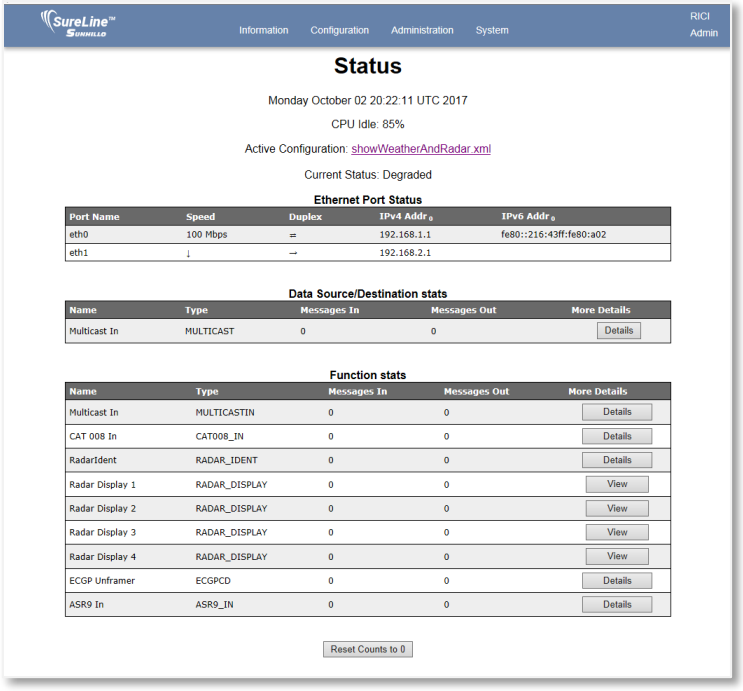
Mission-Critical Data Interoperability

SureLine® Core User's Guide



SureLine Core User's Guide

SUN2353, Revision 2.1 • February 13, 2018

444 Kelley Drive
West Berlin, NJ 08091-9210
www.sunhillo.com
Phone 856.767.7676 • Fax 856.767.9557

Contents

1. INTRODUCTION 1
1.1 Overview 1
1.1.1 How this Manual is Organized 1
1.2 Additional Product Information 2
2. OPERATION AND MAINTENANCE 3
2.1 Graphical User Interface 3
2.1.1 Starting the GUI 4
2.1.2 Logging into the GUI 5
2.1.3 The Menu Bar 8
2.2 Information Menu 9
2.2.1 Status 10
2.2.2 Logs 16
2.2.3 Download Logs 17
2.2.4 Download MIB 18
2.2.5 Radar Display 19
2.2.6 Real-Time Data Display 23
2.3 Reboot/Restart/Shutdown 28
2.3.1 Rebooting the System 29
2.3.2 Restarting the System 29
2.3.3 Shutting Down (SGP Only) 30
2.4 About Option – Verifying System Information 31
3. SYSTEM CONFIGURATION 33
3.1 Network Config Screen 34
3.1.1 Network Address Configuration 36
3.1.2 Routing Configuration 37
3.1.3 DNS Configuration 38
3.1.4 Hostname Configuration 39
3.1.5 GUI Timeout 39
3.1.6 IPv6 Client Configuration 40
3.1.7 NTP Client Configuration 41
3.1.8 Syslog Forwarding Configuration 42
4. FUNCTIONAL CONFIGURATION 43
4.1 Configuration Menu 43
4.2 Configuration Elements 44
4.2.1 Data Flow 44
4.2.2 Node 45

4.2.3 Site/Sensor 47
4.2.4 Data Flow Configuration Restrictions 48
4.3 Configuration Files 49
4.3.1 Getting Started – New vs. Edit 49
4.3.2 Managing Configuration Files 53
4.3.3 Setting Active Configuration File 54
4.4 Create/Edit a Configuration File 56
4.4.1 Configuration GUI Overview 56
4.4.2 Saving Configuration Files 59
4.4.3 Create/Edit Data Flow 60
4.4.4 Data Flow Graphical Elements 61
4.4.5 Sensor Configuration 74
4.4.6 Data Flow UI Controls 76
4.4.7 Edit System Configuration Items 80
5. USER AND RSA KEY ADMINISTRATION 85
5.1 User Account Management 86
5.1.1 User Role Permissions 87
5.1.2 Add a User 88
5.1.3 Delete a User 89
5.1.4 Change Settings 90
5.1.5 Change Password Settings 91
5.1.6 Changing Passwords and Security Questions 92
5.2 Creating and Downloading RSA Keys 95
5.2.1 Download RSA Public Key 96
5.2.2 Download RSA Private Key 97
6. SPECIAL FEATURES 99
6.1 Uploading Data 99
6.2 Activating Licensed Functionality 101
6.3 Flashing the Operating System 103
6.4 Managing ADS-B Receiver Modules in Longport 104
6.5 Accessing the Sunhillo Terminal User Interface (STUI) 106
6.5.1 Technical Support Option 109
7. REDUNDANCY 113
7.1 Unit Redundancy 113
7.1.1 Unit Redundancy Switchover 116
7.2 Network Interface Redundancy 116
7.2.1 Receiving LAN Data 117
7.2.2 Transmitting LAN Data 120
7.3 Preferred Primary Method 121
7.3.1 Unit Redundancy 121

7.3.2 Network Interface Redundancy 122
7.4 Radar Redundancy 122
7.5 Manual Switching 123
8. USB FLASH DRIVE USAGE 125
8.1 RICI USB Update Notification 125
8.1.1 RICI "Update In Progress" Indication 125
8.1.2 RICI "Update Complete" Indication 126
8.1.3 RICI USB "Checksum Error" Indication 126
8.1.4 RICI USB "Error" Indication 127
8.2 Longport USB Update Notification 127
8.2.1 Longport PCM "Update In Progress" Indication 128
8.2.2 Longport PCM "Update Complete" Indication 128
8.2.3 Longport Error Indication 128
8.3 SGP Update Notification 129
8.4 RICI and SGP Software Update 129
8.5 Longport Software Update 130
8.6 Load Configuration File 130
8.7 Download Log Files 131
8.7.1 RICI and Longport Log Files 131
8.7.2 SGP Log File 132
8.8 Install Software Plug-in 132
9. SECURITY FEATURES 135
9.1 Services and Login Options 135
9.1.1 Service Control 136
9.1.2 Login Options 137
9.1.3 Complex Passwords 137
9.1.4 Login Banner 137
9.2 Lock-down Settings 137
10. SNMP SUPPORT 139
10.1 SNMP Management 140
10.1.1 V2 - Communities 140
10.1.2 V3 - Add User 141
10.1.3 V3 - Delete User 142
10.2 SNMP Objects 143
10.3 SNMP Traps 145
10.4 SNMP Get/Set Commands 146
10.5 Common Remote Access and SNMP Usage 149
10.5.1 Recommended SNMP Gets 149
A1. CONFIGURATION EXAMPLES (SERIAL PLATFORMS) 151
A1.1 Example #1: LAN Input to Serial Output (Single Path) 151

A1.2 Example #2: Multiple LAN input to Multiple Serial Output 155
A1.3 Example #3: LAN Input to Multiple Serial Outputs with Site Filtering 158
A1.4 Example #4: Multiple Serial Input to Single LAN output 160
A1.5 Example #5: Serial Input to Multiple LAN Output with Data Conversion . 166
A1.6 Example #6: LAN Input to Multiple LAN Output 169
A2. SGP CONFIGURATION EXAMPLES 172
A3. MARGATE II ADS-B CONFIGURATION 176
A4. ENABLING MSP API OPERATION 178
A5. ACRONYMS 180

List of Figures

Figure 2-1: Status Screen 6
Figure 2-2: Menu Bar 8
Figure 2-3: Checksum Warning Message 9
Figure 2-4: Status Header 10
Figure 2-5: Status Screen Stats Example without Serial Ports 12
Figure 2-6: Status Screen Function Detail Example 13
Figure 2-7: Status Screen Stats 14
Figure 2-8: Status Screen Function Detail 15
Figure 2-9: Event Log Example 16
Figure 2-10: Radar Display Example 19
Figure 2-11: Multiple Radar Display Options 20
Figure 2-12: Four Radar Displays Example 21
Figure 2-13: Filters and Zoom Panel 22
Figure 2-14: Navigation Scroll Bars when Zoomed 22
Figure 2-15: Radar Display Filter Options Dialog 23
Figure 2-16: Real-Time Data Display (no data) 25
Figure 2-17: Real-Time Data Display (with data) 26
Figure 3-1: Extended View of the Network Config Screen 35
Figure 3-2: Network Address Configuration Example 36
Figure 3-3: Add VLAN Configuration Window 36
Figure 3-4: Bond ETH0 & ETH1 Button 37
Figure 3-5: IP Address Aliases Configuration Window 37
Figure 3-6: Routing Configuration Example 38
Figure 3-7: DNS Configuration Example 39
Figure 3-8: Hostname Configuration Example 39
Figure 3-9: GUI Timeout Example 40
Figure 3-10: IPv6 Configuration Example 40
Figure 3-11: NTP Client Configuration Example 41
Figure 3-12: Syslog Forwarding Configuration Example 42
Figure 4-1: Configuration Menu 43
Figure 4-2: Data Flow 44
Figure 4-3: Data Flow that Branches and Merges 45
Figure 4-4: Manage Configurations Window 54
Figure 4-5: Selecting a New Configuration File, “example2” 55
Figure 4-6: New Configuration File Selected Example 55
Figure 4-7: Pending Active and Active Statuses 56
Figure 4-8: Configuration Screen 57
Figure 4-9: Data Flow Graphical Elements 61
Figure 4-10: Node Details 62
Figure 4-11: 13 Bit Radar Out Example 64
Figure 4-12: User Interface Elements Example 64
Figure 4-13: Required Node Type Example 68
Figure 4-14: Greyed Out Node Type Tool Tip 68
Figure 4-15: Node Info Window Example 69

Figure 4-16: Delete a Function Option 70
Figure 4-17: Inactive Delete a Function Option 71
Figure 4-18: Branch the Path Option 71
Figure 4-19: Delete the Branch Option 71
Figure 4-20: Unmerge Option 74
Figure 4-21: An Unmerged Branch 74
Figure 4-22: Undo and Redo Buttons on Data Flow Configuration 77
Figure 4-23: Show Type Checkbox on Data Flow Configuration 78
Figure 4-24: Show Name Checkbox on Data Flow Configuration 79
Figure 4-25: Zoom In and Zoom Out Buttons 80
Figure 4-26: Sys Config and SNMP Buttons 81
Figure 5-1: User Account Management Screen Example 87
Figure 5-2: Invalid User Name or Password Message 94
Figure 9-1: Services and Login Security Options 136
Figure 9-2: Suggested Services and Login Security Options 138
Figure 10-1: SNMP Management Screen 140

List of Tables

Table 2-1: System Status 11
Table 4-1: I/O Node Categories and Descriptions 45
Table 4-2: Function Nodes and Descriptions 46
Table 4-3: Sample Configuration Files and Description 50
Table 4-4: Node Icon Descriptions 63
Table 4-5: Data Recording Control Parameters 83
Table 5-1: User Role Permissions 88
Table 7-1: Unit Redundancy Configuration Parameters 114
Table 7-2: Configuration Parameters for ECGP Unframer Network Redundancy 118
Table 7-3: Configuration Parameters for Three Modes of Network Redundancy 118
Table 7-4: Configuration Parameters for Configuring Network Redundancy 120
Table 7-5: Configuration Parameters for Radar Redundancy 122
Table 8-1: Useful RICI, Longport, and Ventnor Log Files and Locations 131
Table 8-2: Useful SGP Log Files and Locations 132
Table 10-1: Objects Groups Available in SGP MIB Summary 143
Table 10-2: SNMP Traps Issued by System Summary 145
Table 10-3: Available SNMP Commands Summary 146

This page is intentionally left blank.

Section 1

1. INTRODUCTION

In this Section, you gain a general understanding of the purpose and organization of this manual.

This user's manual provides details on the operations of Sunhillo's SureLine® Core software. Hardware that makes use of SureLine Core includes the Real-Time Interface and Conversion (RICI), Longport, Ventnor, Margate II ADS-B, and Surveillance Gateway Processor (SGP) products. This SureLine Core software manual is intended as a companion to the individual hardware manuals for the respective products.

1.1 Overview

The RICI, Longport, Ventnor, Margate II ADS-B, and SGP products share a common software platform, SureLine Core, with each providing different hardware interfaces.

1.1.1 How this Manual is Organized

Section 1 **Introduction** – Provides a brief overview of the relevant software operations and devices, support information, and the contents of this user's manual.

Section 2 **Operation and Maintenance** – Provides a description and instruction for using common features for operating and maintaining the device. These features include starting and logging in to the Graphical User Interface (GUI), status display, using the radar display, viewing and gathering log files, and rebooting/restarting.

Section 3 **System Configuration –** Provides the details for configuring the system network settings and other system-wide items.

Section 4 **Functional Configuration –** Provides a description of the configuration GUI and details and instructions for creating and maintaining configuration files.

Section 5 **User and RSA Key Administration –** Provides information for creating and managing user accounts on the GUI, as well as configuring RSA keys.

Section 6 **Special Features –** Provides a description and instructions for using special, i.e., not commonly used, features of the GUI, as well as provides information on the Sunhillo Terminal User Interface (STUI).

Section 7 **Redundancy –** Provides details on the function of redundancy and network interface redundancy on a device.

Section 8 **USB Flash Drive Usage –** Provides detailed information regarding the USB flash drive and its uses.

Section 9 **Security Features –** Describes the security features available for the device.

Section 10 **SNMP Support –** Describes the Management Information Base (MIB) objects and the Simple Network Management Protocol (SNMP) traps and get/set commands used for accessing these objects.

Appendices Supplemental information to support the contents of this document.

1.2 Additional Product Information

For additional information on this or any of Sunhillo's other products, contact Sunhillo Corporation at:

	**Phone**:	856.767.7676 (Toll Free: 844.977.7676) **Sales** (phone option, press 1) **Technical Support** (phone option, press 2)
	**Fax**:	856.767.9557 (ATTN: Marketing)
	**Web**:	www.sunhillo.com
	**Support Website**:	support.sunhillo.com
	**Email**:	sales@sunhillo.com
	**Mail**:	Sunhillo Corporation ATTN: Marketing 444 Kelley Drive West Berlin, NJ 08091-9210 USA

Section 2

2. OPERATION AND MAINTENANCE

In this section, you gain an understanding of the SureLine Core software's operation and maintenance.

Using an Ethernet cable for a direct LAN connection, the SureLine Core Graphical User Interface (GUI) can be started over an HTTPS Web browser session. The Ethernet Switch Module (ESM) in the RICI and the Ethernet ports in the SGP support auto crossover, meaning a crossover cable is not required for direct connection to these devices. The GUI screens are compliant with most modern Web browsers that have JavaScript enabled and accept cookies, however the system has been tested to run on Windows 7 or higher systems with Microsoft Internet Explorer (v11 or higher) and Firefox.

Note

For low bandwidth connections, you can Secure Shell (SSH) into a supported Sunhillo hardware platform to access the Sunhillo Terminal User Interface (STUI). The STUI allows access to most of the same features as the GUI, save for the Functional Configuration (Section **4**). A unique function, **Technical Support**, described in Section **6.5.1**, is also listed on the STUI menu, allowing for standard shell access in coordination with Sunhillo Technical Support (refer to Section **1.2**) for issues that can't be resolved through normal methods. For information on accessing the STUI, refer to Section **6.5**.

2.1 Graphical User Interface

Working with the GUI is described in the subsections that follow.

Note

JavaScript must be enabled in the Web browser on the system where the GUI is to be run. The browser must also accept cookies for the GUI login to work correctly. Enable these features on the target computer before continuing. Refer to Microsoft's Internet Explorer help site, Mozilla's Firefox help site, or your IT department's support team for assistance with enabling the necessary features.

Note

If you are upgrading to a new software version, you must clear the cache and cookies in your browser.

2.1.1 Starting the GUI

The three subsections that follow describe starting the GUI for the RICI, Longport, Ventnor, Margate II ADS-B, and SGP, respectively.

2.1.1.1 Starting the Configuration Interface

To invoke the device's configuration interface, perform the following:

1. For a direct connection to the device, configure the network settings on the computer to use a static IP address. For the SGP, configure the computer to use the same subnet.
2. For all but the SGP, configure the IP, Netmask, and Gateway addresses on the computer with the correct settings to communicate with the device either through a direct connection or over a network.
3. Plug one end of the Ethernet patch cable into the computer on which the Web browser is installed.
4. Plug the other end of the cable into the RJ45 port labeled **Eth0** (or **Ethernet 1** for SGP) on the chassis.
5. Launch the Web browser and enter the following address:

   https://*Device IP address*/

   Device IP address is the IP address assigned to the device's Ethernet port.

Note

The factory preset IP addresses for the device is 192.168.1.1 for **Eth0** and 192.168.2.1 for **Eth1** (or, for SGP, 192.168.1.100 for **Ethernet 1** and 192.168.2.100 for **Ethernet 2**); to ensure there are no IP conflicts within the Longport chassis, each PCM requires a separate login to a separate IP address. These addresses should be modified using the *Network Config* screen, which is described in Section **3.1**.

Note

Depending upon browser type, you may be presented with a **Certificate error**, **Certificate Invalid**, or other security certificate warning message. When accessing the device, this type of security certificate warning message is safe to ignore.

The following is an example of the network settings for a computer to be connected directly to a Longport with a PCM IP Address of 192.168.1.1:

- Switch to use a Static IP address
- **IP address**: 192.168.1.10
- **Netmask Address**: 255.255.255.0
- **Gateway Address**: 192.168.1.190

2.1.2 Logging into the GUI

Upon launching the GUI, the *Status* screen is displayed, similar to the example shown in **Figure 2-1**:

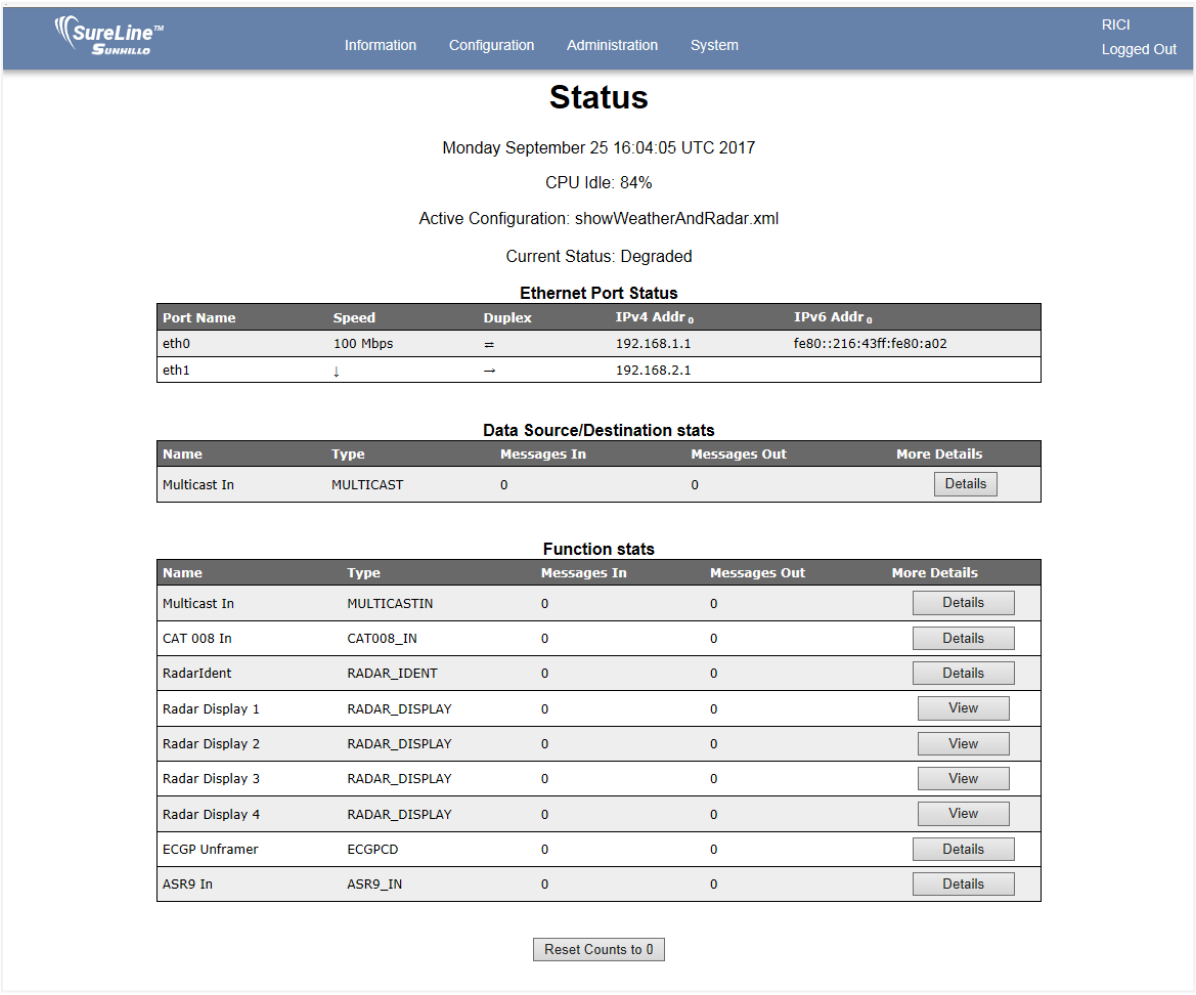
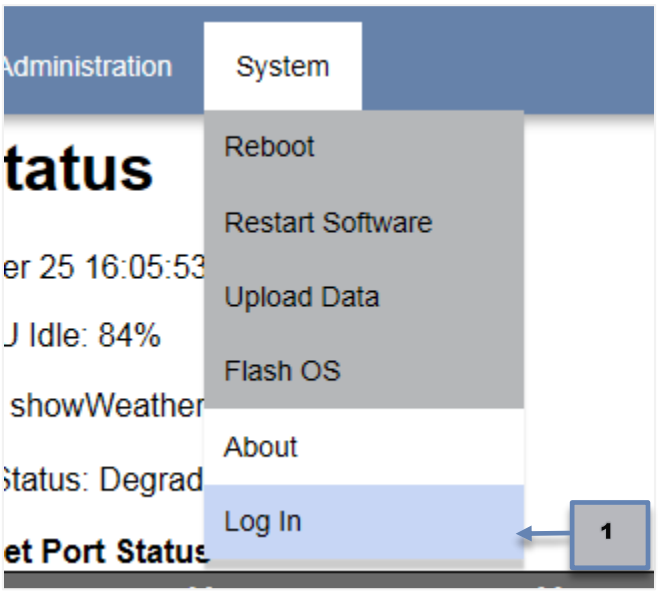


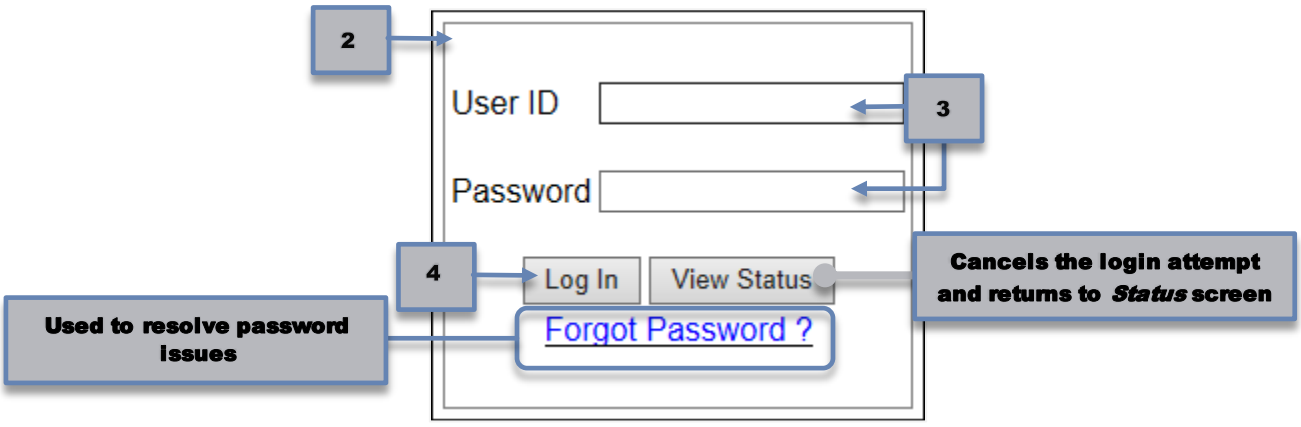
Figure 2-1: Status Screen

To log into the *Configuration* interface, follow these steps:

1. Select **Log In** under the *System* menu in the upper right of the *Status* screen.



2. The *Log In* windows appears.



3. Enter the **User ID** and **Password**. The case-sensitive default values are:

   User ID: Admin

   Password: Sunhillo

Note

The **User ID** and **Password** can be modified. Refer to Section **5.1** for details on user account management.

4. Click the **Log In** button.

By default, a session for a logged in user is active for 20 minutes. If no activity is detected for a particular user, or the browser window closes without logging out the user, the session will be terminated after 20 minutes. This time limit can be modified by changing the **GUI Timeout** option using the **Network Config** option under the *Administration* menu (refer to Section **3.1.5**).

2.1.3 The Menu Bar

The Menu Bar (**Figure 2-2**) runs along the top part of the GUI; to the right, is the log in status, and, to the left, are the four top-level menus: *Information*, *Configuration*, *Administration*, and *System*.

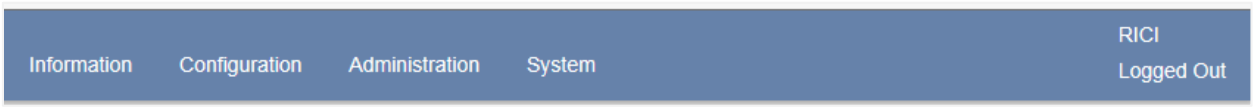


Figure 2-2: Menu Bar

Mousing over any of the top-level menus displays their respective dropdown menus, which provide operations/information associated with the selected item.

Note

The menu options available are specific to the device SureLine is running on. Certain options shown will only appear if it is supported by the device.

The menu options are summarized as follows:

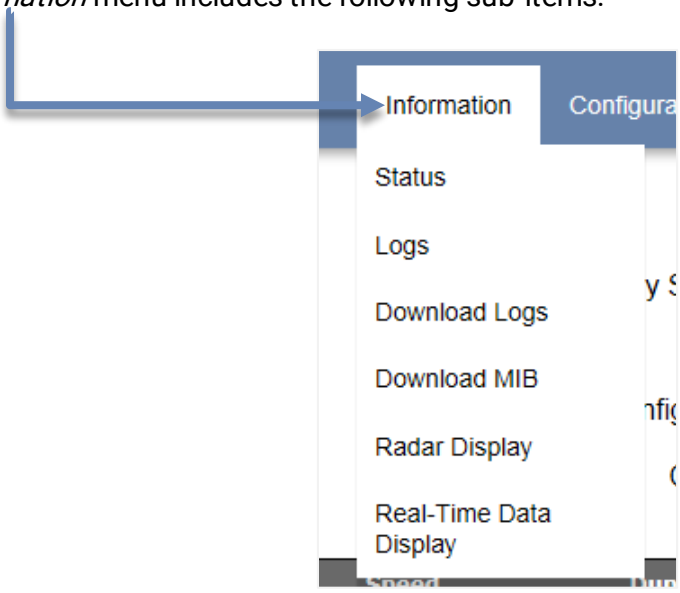
- **Information**—Provides graphical representations of the operational aspects of the device and also provides access to internal data logs. Refer to Section **2.2** for more information.
- **Configuration**—Provides access to the XML-based system configuration files. Refer to Section **3** for more information.
- **Administration**—Allows you to configure the network, security, SNMP, license, and RSA features and options. Refer to sections **3**, **5**, **9**, and **10** for more information of the respective Administration features.
- **System**—Allows you to perform system/software restarts, manage user account information, upload files/software updates, and add features to the system through the use of licensed software. Refer to Section **6** for more information.

In the event that a checksum error occurs during the software installation process, the warning message shown in **Figure 2-3** is displayed directly below the Menu Bar. If this occurs, reinstall the software. If this error persists, contact Sunhillo for technical assistance (see Section **1.2**).

Figure 2-3: Checksum Warning Message

2.2 Information Menu

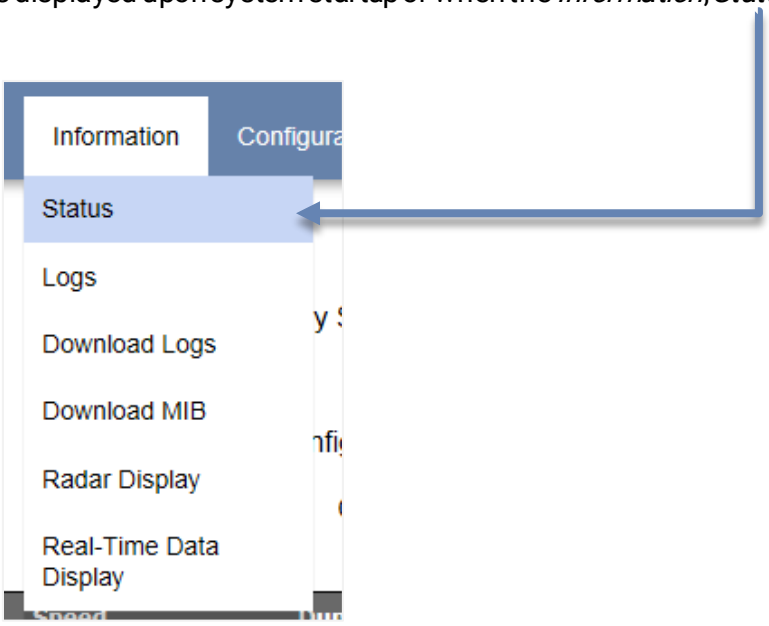
The *Information* menu includes the following sub-items:



The *Status*, *Logs*, *Download Logs*, *Download MIB*, *Radar Display*, and *Real-Time Data Display Information* menu items are described in the subsections that follow.

2.2.1 Status

The *Status* screen (see **Figure 2-1**) is displayed upon system startup or when the *Information*, *Status* menu option is selected.



The *Status* screen displays real-time I/O statistics for the configured ports, data source destination statistics for configured device nodes, and function statistics for configured data flow and conversion functions.

The port statistics include the number of messages received and transmitted for each of the ports. The data source/destination statistics consist of the I/O data counts for device nodes and the function statistics are the message I/O counts for functions and sites utilized in the I/O message data flow.

The current device date and time, CPU activity, the active configuration file name, and current device system status are provided at the top of the device Status screen (**Figure 2-4**):

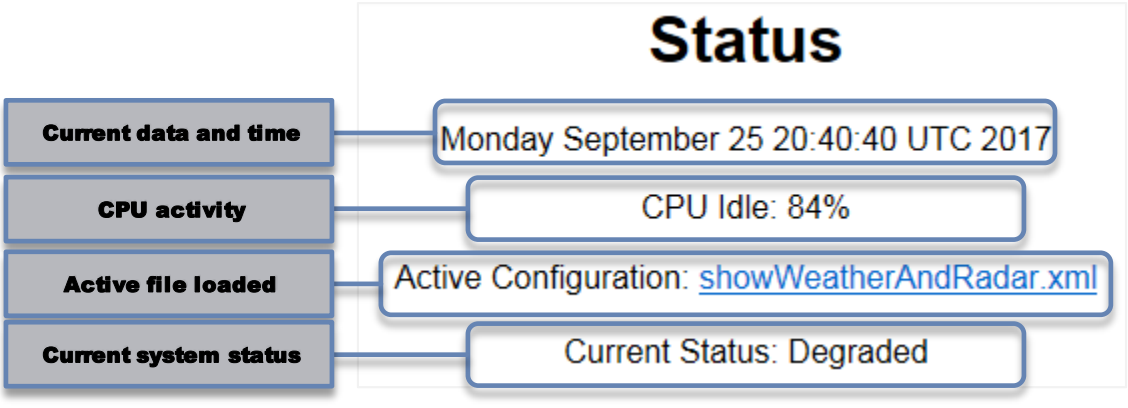


Figure 2-4: Status Header

Table 2-1 describes the three status states found under **Current Status**.

Table 2-1: System Status

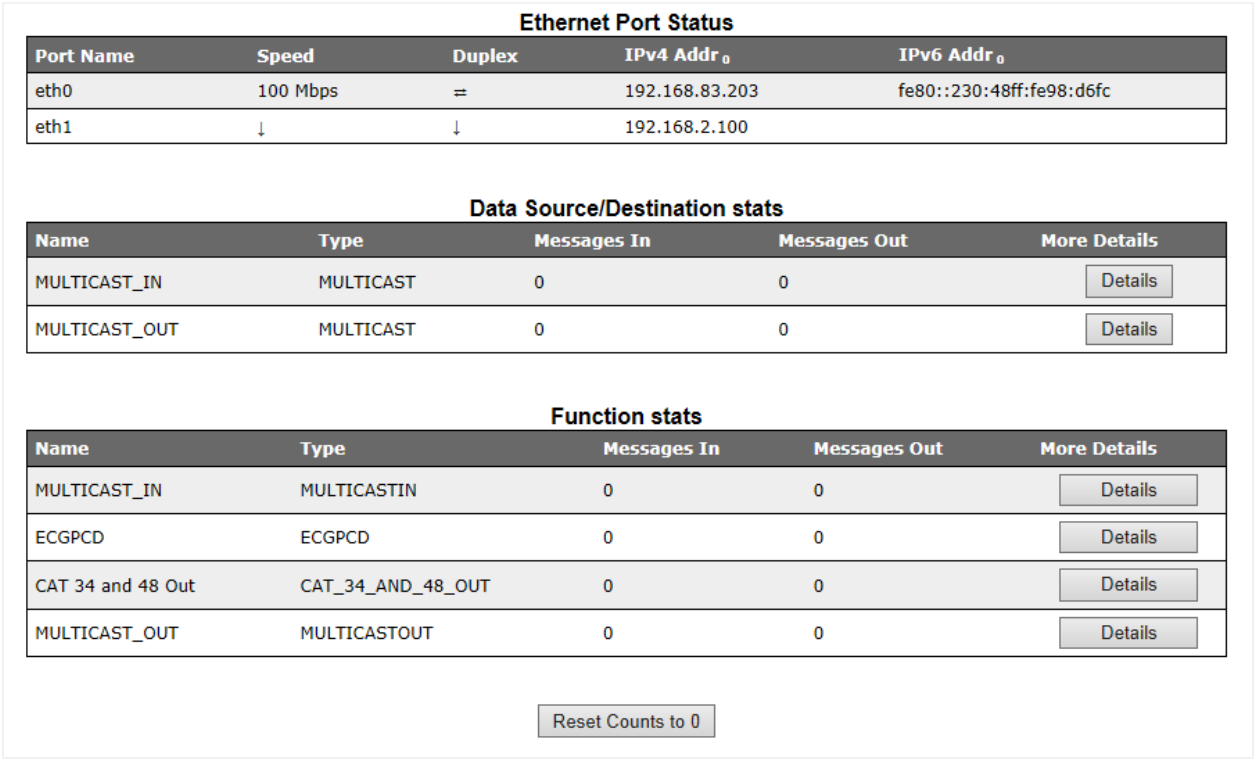
Status	Description
Active	Indicates the device configuration has no errors and the Ethernet ports used in the configuration have connectivity with the LAN.
Degraded	Indicates an Ethernet connection (used in the configuration) is down/does not have connection to the LAN.
Failure	Indicates an error was found in the active configuration file. This usually indicates the active configuration requires a license (Tier 1 or 2) that has not been installed.

2.2.1.1 Status Screen

The *Status* screen displays port statistics under **Ethernet Port Status** and, if available, **Serial Port stats**; physical layer statistics under **Data Source/Destination stats;** and function statistics under **Function stats** (**Figure 2-5**). The information displayed on the *Status* screen is dependent upon the active configuration on the device.

Note

Hovering the mouse pointer on a port name row under **Ethernet Port Status** reveals Tooltip info that provides additional detail. Tooltip info is also available within other areas of the GUI.



Ethernet Port Status

Port Name	Speed	Duplex	IPv4 Addr 0	IPv6 Addr 0
eth0	100 Mbps	=	192.168.83.203	fe80::230:48ff:fe98:d6fc
eth1	↓	↓	192.168.2.100	

Data Source/Destination stats

Name	Type	Messages In	Messages Out	More Details
MULTICAST_IN	MULTICAST	0	0	Details
MULTICAST_OUT	MULTICAST	0	0	Details

Function stats

Name	Type	Messages In	Messages Out	More Details
MULTICAST_IN	MULTICASTIN	0	0	Details
ECGPCD	ECGPCD	0	0	Details
CAT 34 and 48 Out	CAT_34_AND_48_OUT	0	0	Details
MULTICAST_OUT	MULTICASTOUT	0	0	Details

Reset Counts to 0

Figure 2-5: Status Screen Stats Example without Serial Ports

Pressing the **View** button in the **Function stats** section may invoke the graphical radar display or Real Time Data Display associated with whatever data is input in the Display node. Pressing the **Details** command button in any of the status Sections displays a related detailed status screen. A sample detailed status screen for **CAT 008 In** in the **Function stats** Section is shown in **Figure 2-6**.

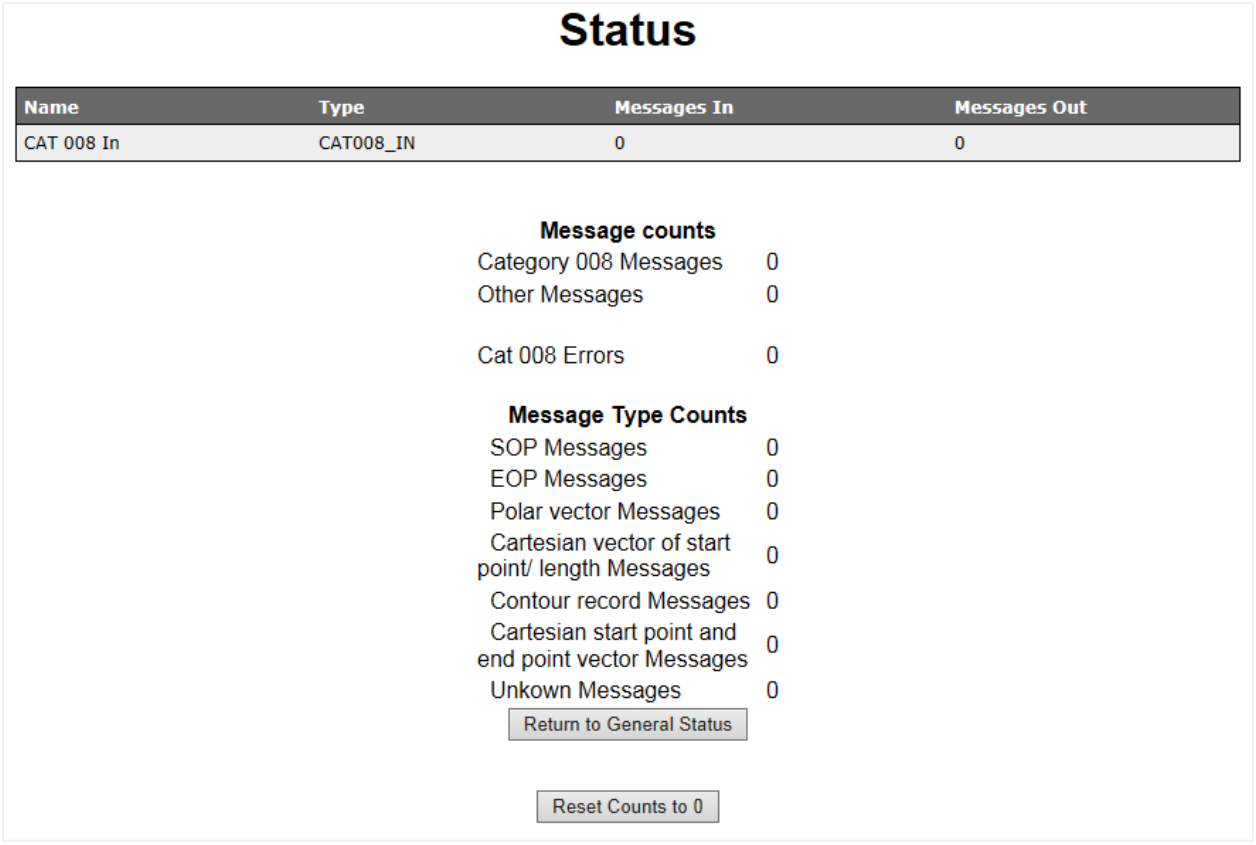
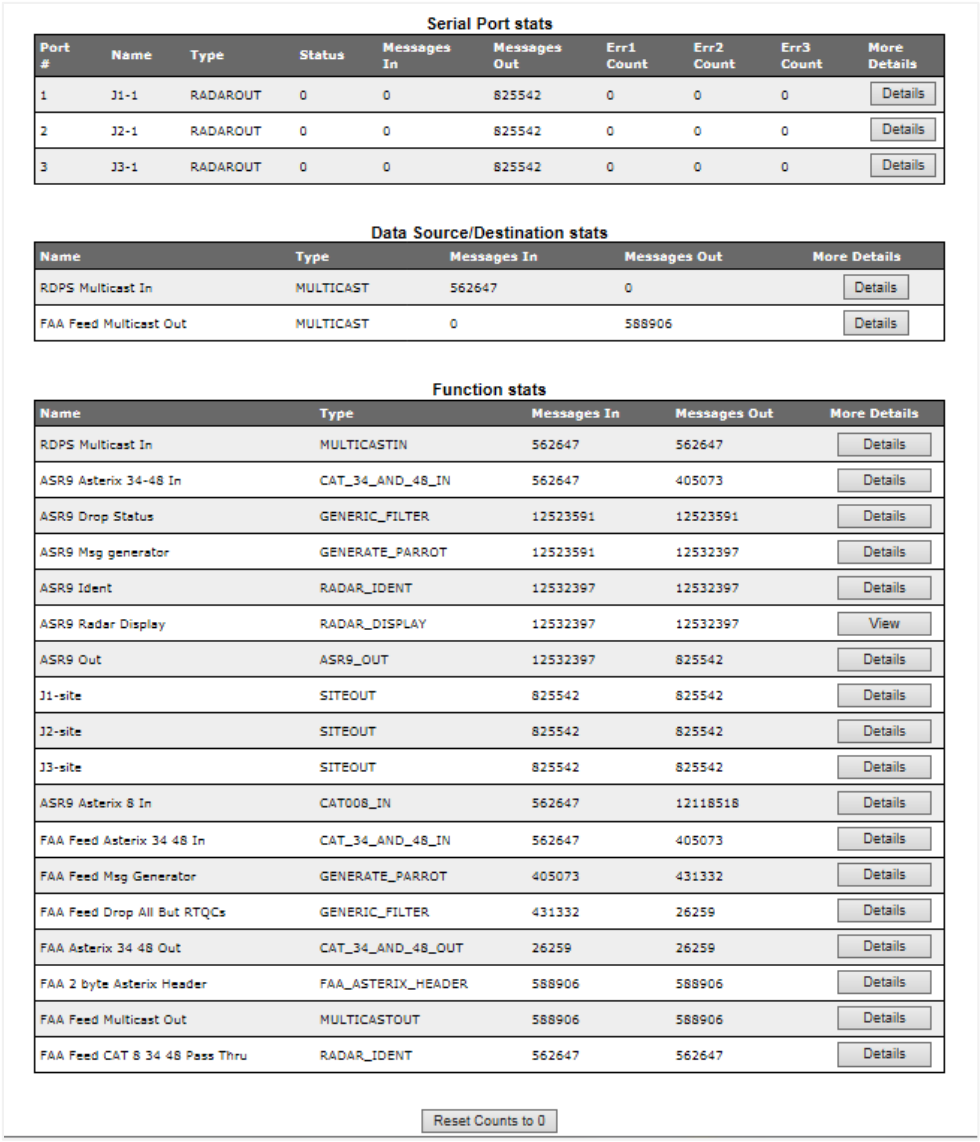


Figure 2-6: Status Screen Function Detail Example

Pressing the **Reset Counts to 0** command button on the main *Status* screen resets all nodes statistics counters to zero. Pressing the **Reset Counts to 0** command button on the detailed screen resets that node's statistics counters to zero. Real-time updates will immediately resume. To return to the main *Status* screen, click the **Return to General Status** command button.

An example of a *Status* screen that displays port statistics under **Serial Port stats**; physical layer statistics under **Data Source/Destination stats;** and function statistics under **Function stats** is shown in **Figure 2-7**.



Serial Port stats

Port #	Name	Type	Status	Messages In	Messages Out	Err1 Count	Err2 Count	Err3 Count	More Details
1	J1-1	RADAROUT	0	0	825542	0	0	0	Details
2	J2-1	RADAROUT	0	0	825542	0	0	0	Details
3	J3-1	RADAROUT	0	0	825542	0	0	0	Details

Data Source/Destination stats

Name	Type	Messages In	Messages Out	More Details
RDPS Multicast In	MULTICAST	562647	0	Details
FAA Feed Multicast Out	MULTICAST	0	588906	Details

Function stats

Name	Type	Messages In	Messages Out	More Details
RDPS Multicast In	MULTICASTIN	562647	562647	Details
ASR9 Asterix 34-48 In	CAT_34_AND_48_IN	562647	405073	Details
ASR9 Drop Status	GENERIC_FILTER	12523591	12523591	Details
ASR9 Msg generator	GENERATE_PARROT	12523591	12532397	Details
ASR9 Ident	RADAR_IDENT	12532397	12532397	Details
ASR9 Radar Display	RADAR_DISPLAY	12532397	12532397	View
ASR9 Out	ASR9_OUT	12532397	825542	Details
J1-site	SITEOUT	825542	825542	Details
J2-site	SITEOUT	825542	825542	Details
J3-site	SITEOUT	825542	825542	Details
ASR9 Asterix 8 In	CAT008_IN	562647	12118518	Details
FAA Feed Asterix 34 48 In	CAT_34_AND_48_IN	562647	405073	Details
FAA Feed Msg Generator	GENERATE_PARROT	405073	431332	Details
FAA Feed Drop All But RTQCs	GENERIC_FILTER	431332	26259	Details
FAA Asterix 34 48 Out	CAT_34_AND_48_OUT	26259	26259	Details
FAA 2 byte Asterix Header	FAA_ASTERIX_HEADER	588906	588906	Details
FAA Feed Multicast Out	MULTICASTOUT	588906	588906	Details
FAA Feed CAT 8 34 48 Pass Thru	RADAR_IDENT	562647	562647	Details

Reset Counts to 0

Figure 2-7: Status Screen Stats

The *Err1 Count*, *Err2 Count*, and *Err3 Count* information under the **Serial Port stats** Section reports the number of times an error has occurred particular to the serial port.

Err1 Count indicates a loss of clock, *Err2 Count* indicates a data overrun, and *Err3 Count* indicates a parity error for radar data receive type ports and a checksum error for synchronous serial and High-level Data Link Communications (HDLC) port types.

The *Status* field under the **Serial Port stats** Section is a hexadecimal representation of the port status bits. Pressing the **View** button in the **Function stats** section may invoke the graphical radar display or Real Time Data Display associated with whatever data is input in the Display node. Pressing the **Details** command button in any of the status Sections displays a related detailed status screen. A sample detailed status screen when selecting **ASR Asterix 34-48 In** (**CAT_34_AND_48_IN**) in the **Function stats** Section is shown in **Figure 2-8**.

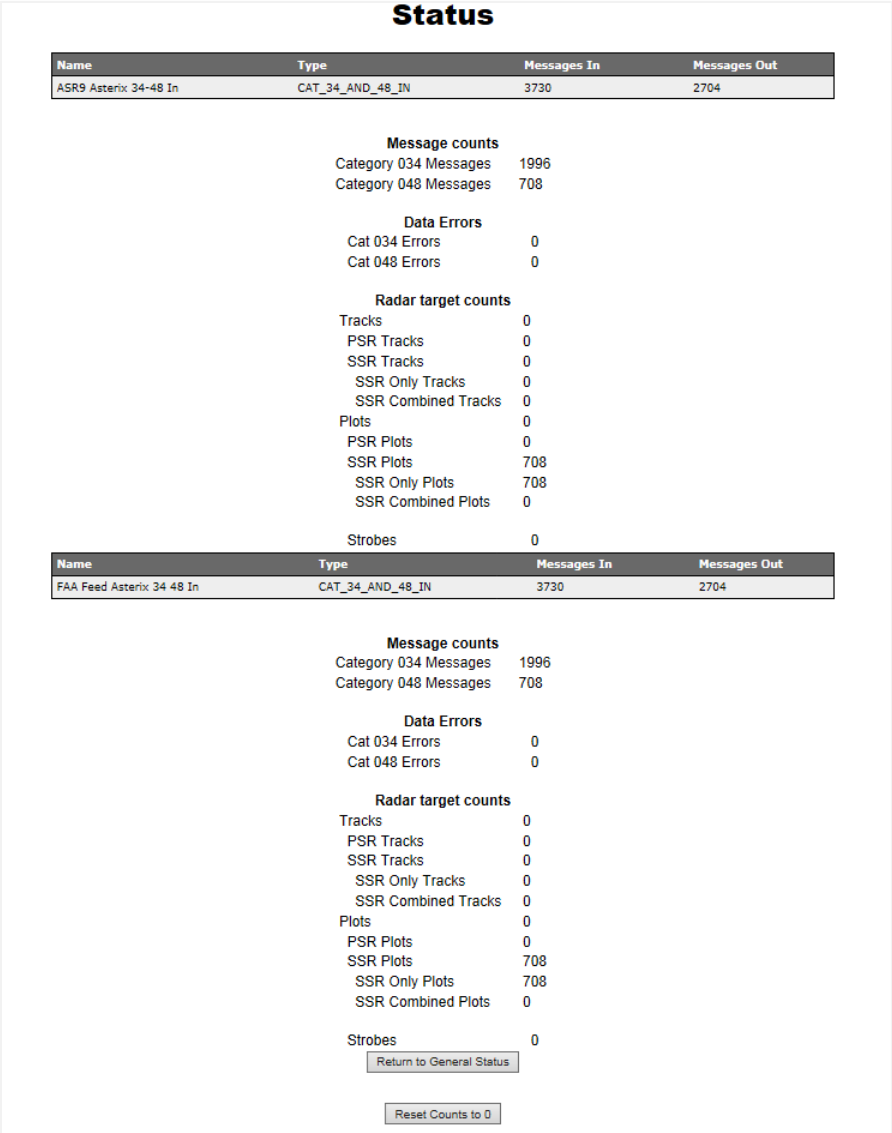
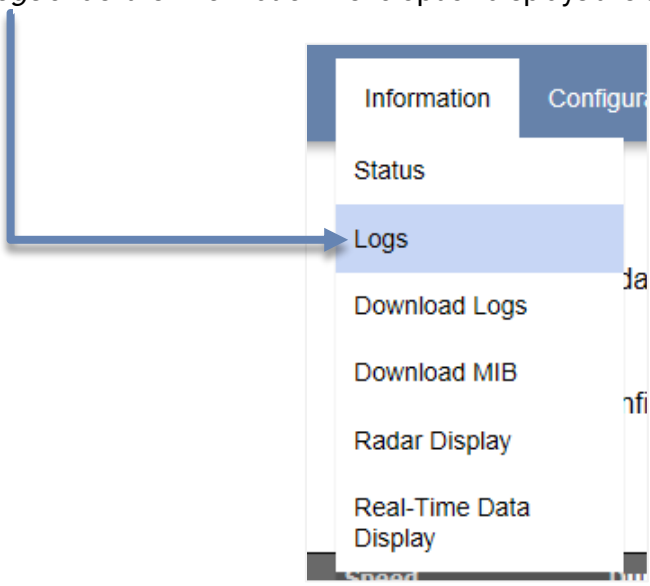


Figure 2-8: Status Screen Function Detail

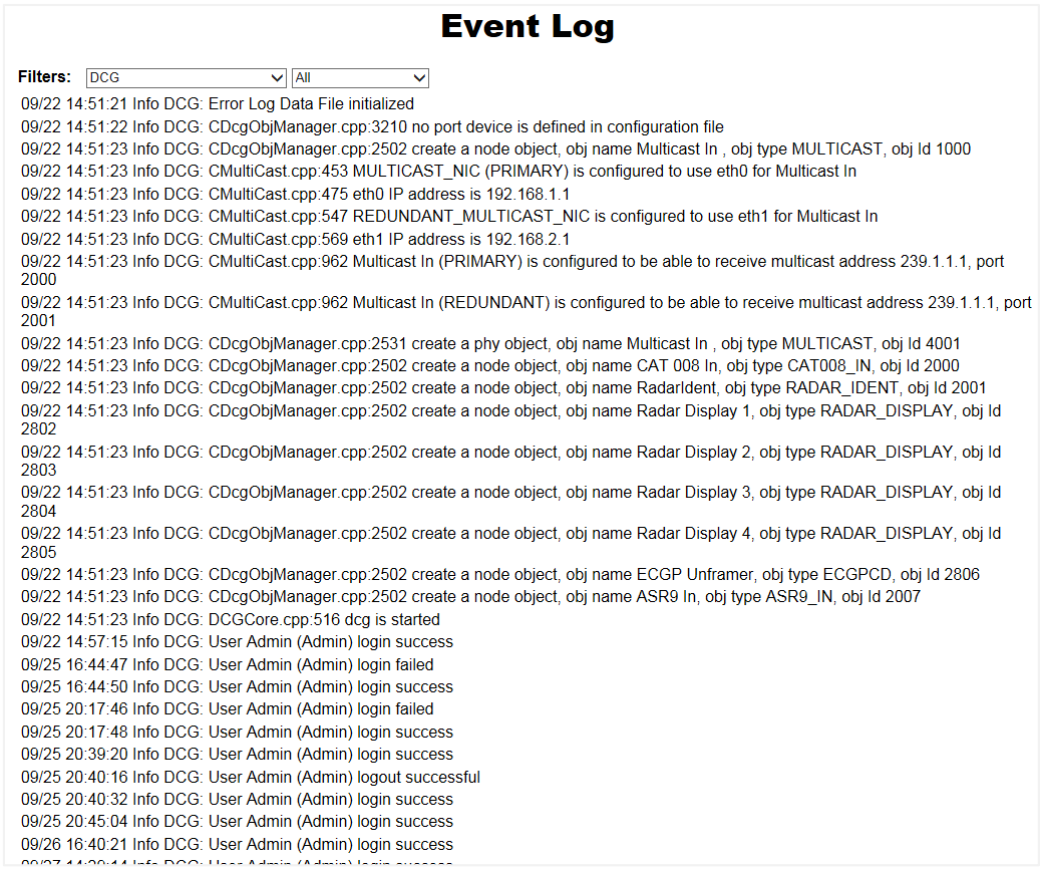
Pressing the **Reset Counts to 0** command button on the main *Status* screen resets all nodes statistics counters to zero. Pressing the **Reset Counts to 0** command button on the detailed screen resets that node's statistics counters to zero. Real-time updates will immediately resume. To return to the main *Status* screen, click the **Return to General Status** command button.

2.2.2 Logs

Selecting *Logs* under the *Information* menu option displays the contents of the system's event log.



The most recent event is listed at the top of the **Event Log**, as shown in the **Figure 2-9** example.



Event Log

Filters: DCG All

09/22 14:51:21 Info DCG: Error Log Data File initialized
09/22 14:51:22 Info DCG: CDcgObjManager.cpp:3210 no port device is defined in configuration file
09/22 14:51:23 Info DCG: CDcgObjManager.cpp:2502 create a node object, obj name Multicast In , obj type MULTICAST, obj Id 1000
09/22 14:51:23 Info DCG: CMultiCast.cpp:453 MULTICAST_NIC (PRIMARY) is configured to use eth0 for Multicast In
09/22 14:51:23 Info DCG: CMultiCast.cpp:475 eth0 IP address is 192.168.1.1
09/22 14:51:23 Info DCG: CMultiCast.cpp:547 REDUNDANT_MULTICAST_NIC is configured to use eth1 for Multicast In
09/22 14:51:23 Info DCG: CMultiCast.cpp:569 eth1 IP address is 192.168.2.1
09/22 14:51:23 Info DCG: CMultiCast.cpp:962 Multicast In (PRIMARY) is configured to be able to receive multicast address 239.1.1.1, port 2000
09/22 14:51:23 Info DCG: CMultiCast.cpp:962 Multicast In (REDUNDANT) is configured to be able to receive multicast address 239.1.1.1, port 2001
09/22 14:51:23 Info DCG: CDcgObjManager.cpp:2531 create a phy object, obj name Multicast In , obj type MULTICAST, obj Id 4001
09/22 14:51:23 Info DCG: CDcgObjManager.cpp:2502 create a node object, obj name CAT 008 In, obj type CAT008_IN, obj Id 2000
09/22 14:51:23 Info DCG: CDcgObjManager.cpp:2502 create a node object, obj name RadarIdent, obj type RADAR_IDENT, obj Id 2001
09/22 14:51:23 Info DCG: CDcgObjManager.cpp:2502 create a node object, obj name Radar Display 1, obj type RADAR_DISPLAY, obj Id 2802
09/22 14:51:23 Info DCG: CDcgObjManager.cpp:2502 create a node object, obj name Radar Display 2, obj type RADAR_DISPLAY, obj Id 2803
09/22 14:51:23 Info DCG: CDcgObjManager.cpp:2502 create a node object, obj name Radar Display 3, obj type RADAR_DISPLAY, obj Id 2804
09/22 14:51:23 Info DCG: CDcgObjManager.cpp:2502 create a node object, obj name Radar Display 4, obj type RADAR_DISPLAY, obj Id 2805
09/22 14:51:23 Info DCG: CDcgObjManager.cpp:2502 create a node object, obj name ECGP Unframer, obj type ECGPCD, obj Id 2806
09/22 14:51:23 Info DCG: CDcgObjManager.cpp:2502 create a node object, obj name ASR9 In, obj type ASR9_IN, obj Id 2007
09/22 14:51:23 Info DCG: DCGCore.cpp:516 dcg is started
09/22 14:57:15 Info DCG: User Admin (Admin) login success
09/25 16:44:47 Info DCG: User Admin (Admin) login failed
09/25 16:44:50 Info DCG: User Admin (Admin) login success
09/25 20:17:46 Info DCG: User Admin (Admin) login failed
09/25 20:17:48 Info DCG: User Admin (Admin) login success
09/25 20:39:20 Info DCG: User Admin (Admin) login success
09/25 20:40:16 Info DCG: User Admin (Admin) logout successful
09/25 20:40:32 Info DCG: User Admin (Admin) login success
09/25 20:45:04 Info DCG: User Admin (Admin) login success
09/26 16:40:21 Info DCG: User Admin (Admin) login success

Figure 2-9: Event Log Example

The dropdown lists under the **Filters** heading allow you to select the log message source (left most dropdown) and the error type (right most dropdown) that you want to display. The source options include: **All** logs, **DCG** (RICI application log), **rsyslogd**, **kernel**, **snmpd**, **xinetd**, **crond**, **ntpd**, **logger**, **mpsmib**, and **CROND**.

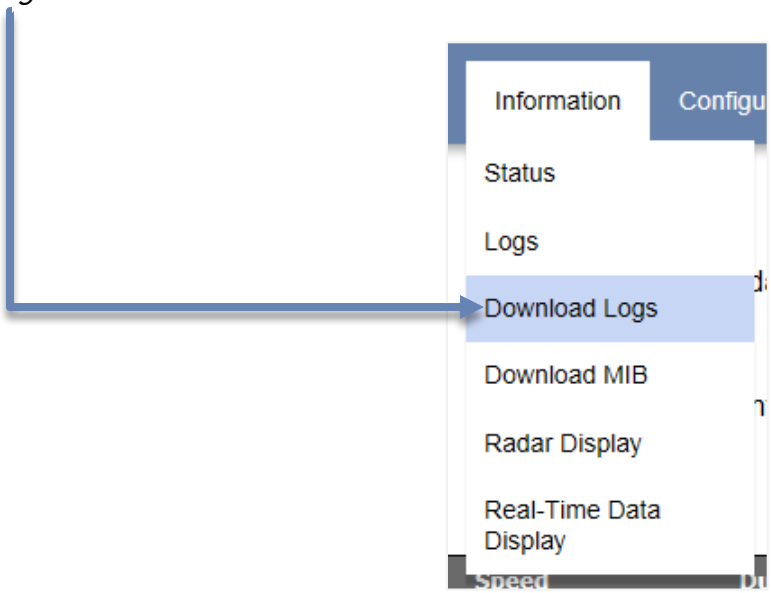
If an error occurs during operation of the device that cannot immediately be diagnosed, the event log should be consulted to locate any internal error conditions.

The event log screen does not update or refresh automatically. In order to view the latest error/warning information, the Web page must be manually refreshed using the refresh button or command on the Web browser.

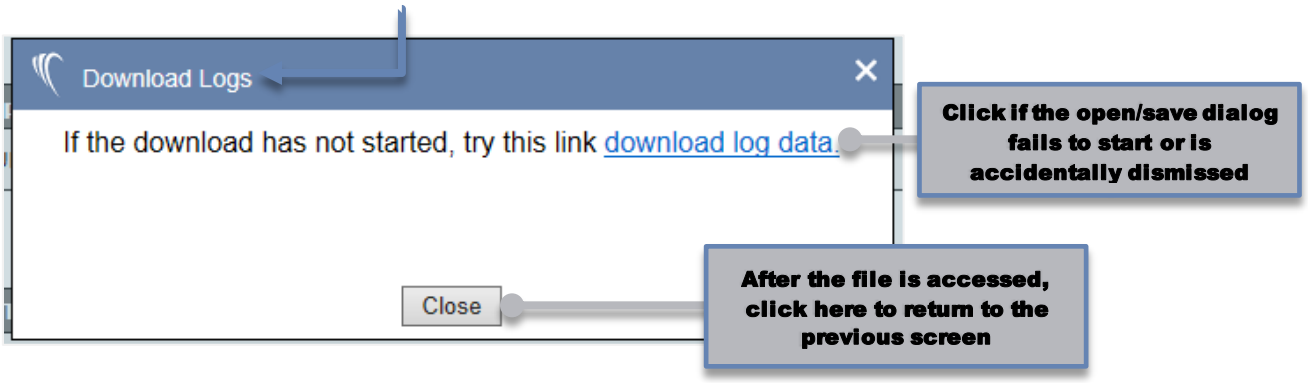
To exit the *Event Log* screen, select a different menu option from the GUI Menu Bar.

2.2.3 Download Logs

The device maintains system log files and configuration files that can be helpful should an unexpected error occur. These files are downloaded to the local workstation by selecting *Download Logs* from the *Information* menu.



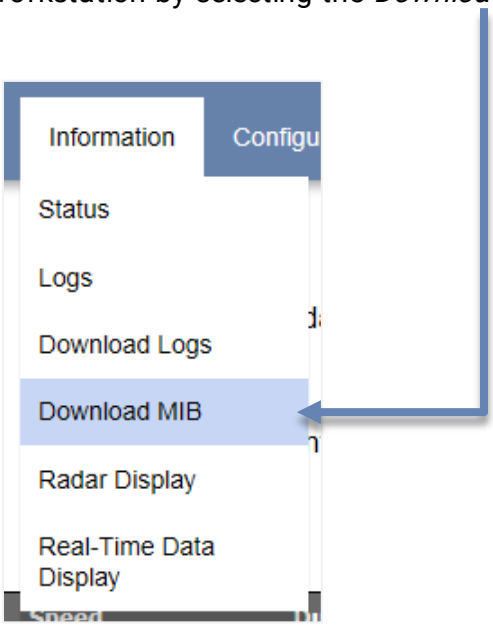
During download, the **Download Logs** dialog appears, then a dialog option to open or save the log file.



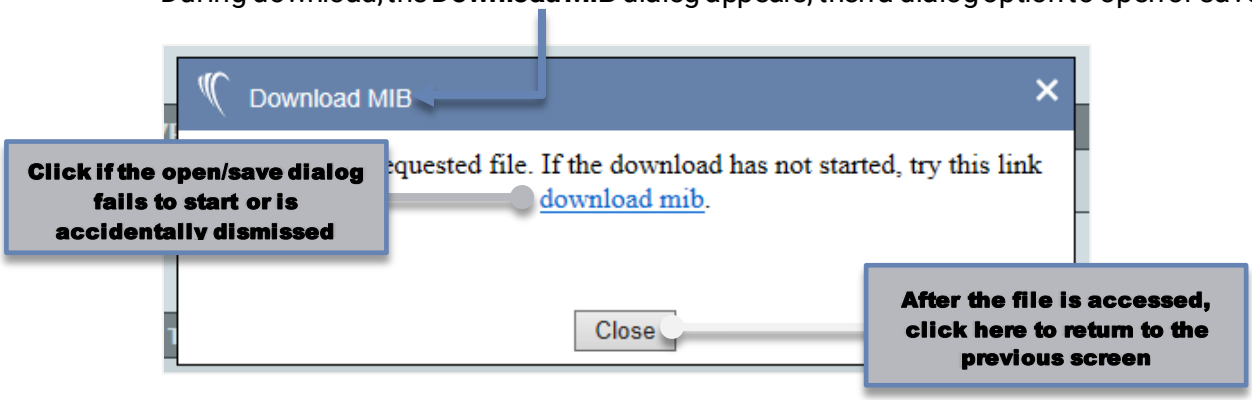
The device's log files are stored in the file, **file.tar*, whose contents can be extracted with any compatible archive extraction software, e.g., *7-Zip* or *WinZip*, and where *** represents *rici* (RICI or Longport), or *dcp* (SGP), depending upon respective device type.

2.2.4 Download MIB

The SNMP MIB can be downloaded so that the file is available for SNMP management tools. These files are downloaded to the local workstation by selecting the *Download MIB* option from the *Information* menu.

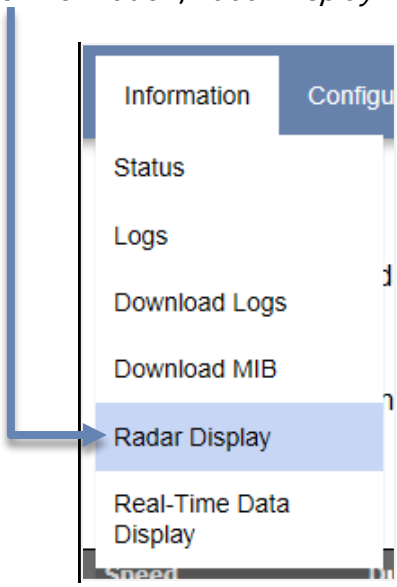


During download, the **Download MIB** dialog appears, then a dialog option to open or save the mib file.



2.2.5 Radar Display

The *Radar Display* option is used to provide a graphical image of radar and weather data (if available). The radar screen (see **Figure 2-1**) is displayed when the **View** button for a specific radar display is selected or when the *Information*, *Radar Display* menu option is selected.



The information on this screen is assigned via the *Radar Display* utility function. **Figure 2-10** shows an example of an unfiltered, single radar display with weather.

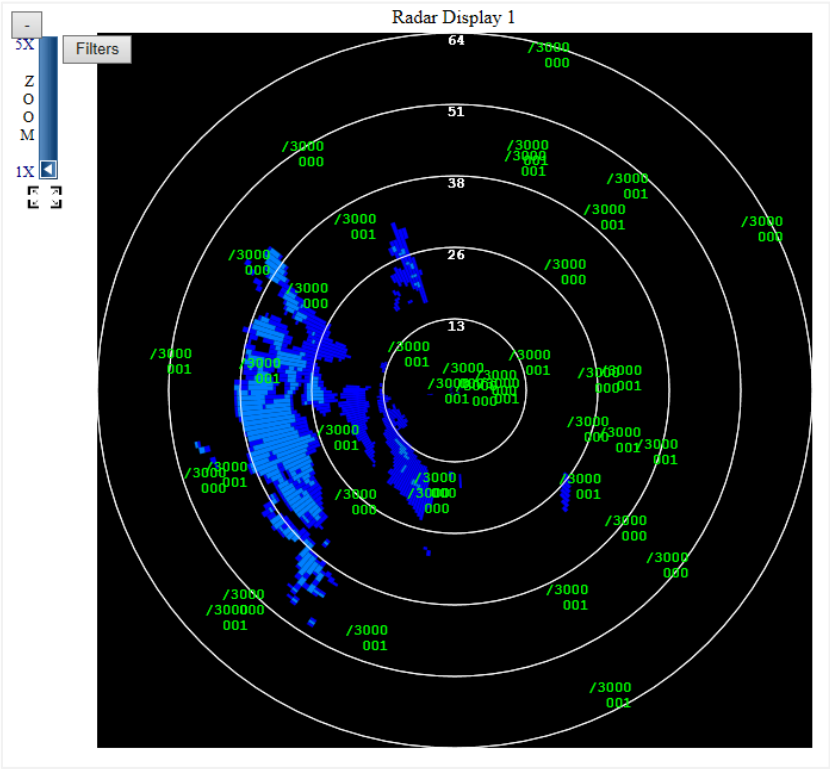


Figure 2-10: Radar Display Example

When multiple radar sites are available, additional button options for one, two, and four displays are shown, like in **Figure 2-11**.

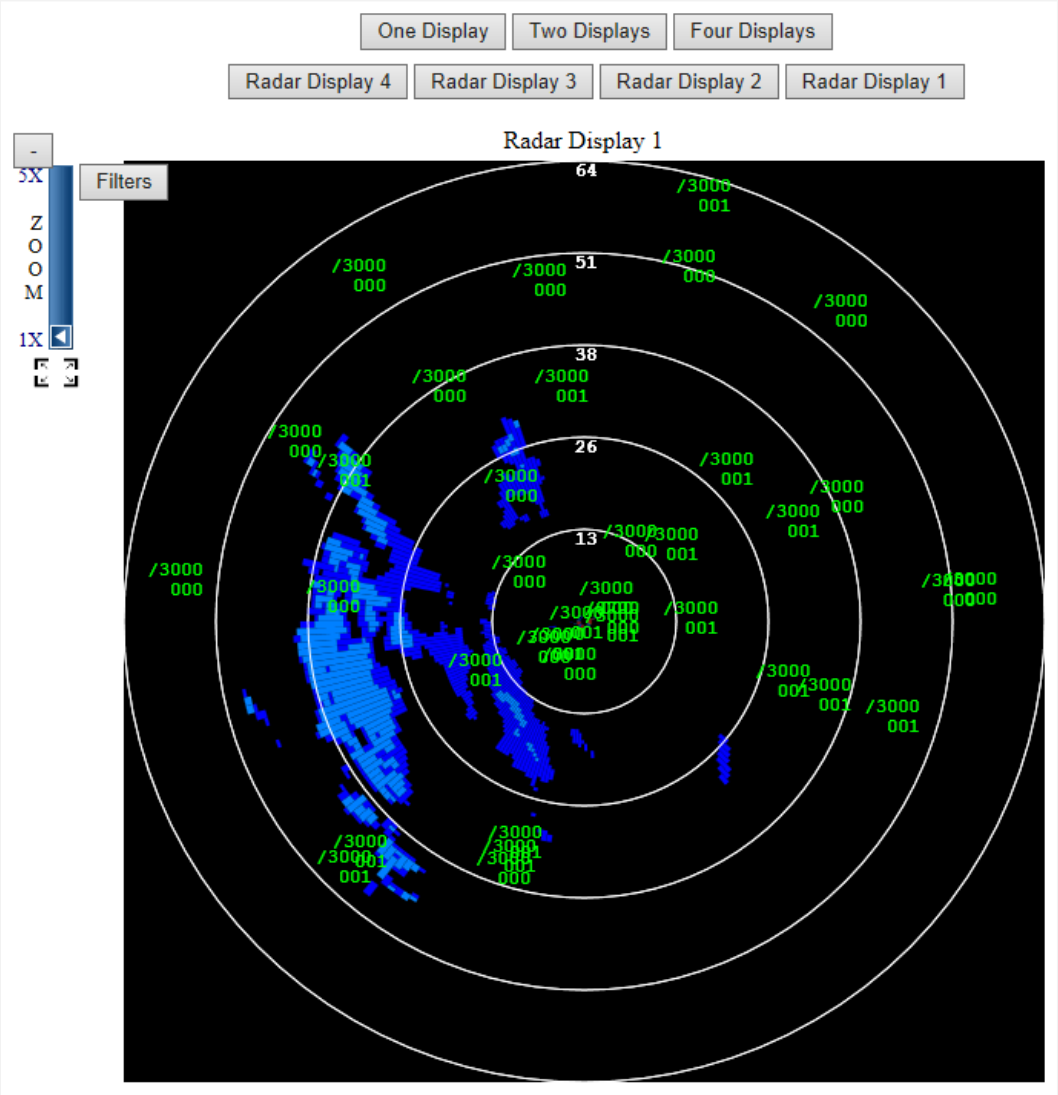


Figure 2-11: Multiple Radar Display Options

The Radar Display uses symbology similar to the FAA Enroute systems. Search and Primary plots are displayed using the plus symbol (**+**). Beacon plots are displayed using a forward slash symbol (**/**), denoting the location followed by the Beacon code. Below the beacon code is the altitude indicator, which is measured in hundreds of feet. For example, Beacon code 1301 with an altitude of 56500 feet is displayed as:

/1301

565

Tracks are displayed using a back slash (****), denoting the location followed by the beacon code. Below the beacon code is the altitude indicator. The third line of the track display is the track number, X Velocity, Y Velocity.

An example of **Four Displays** selected is shown in **Figure 2-12**.

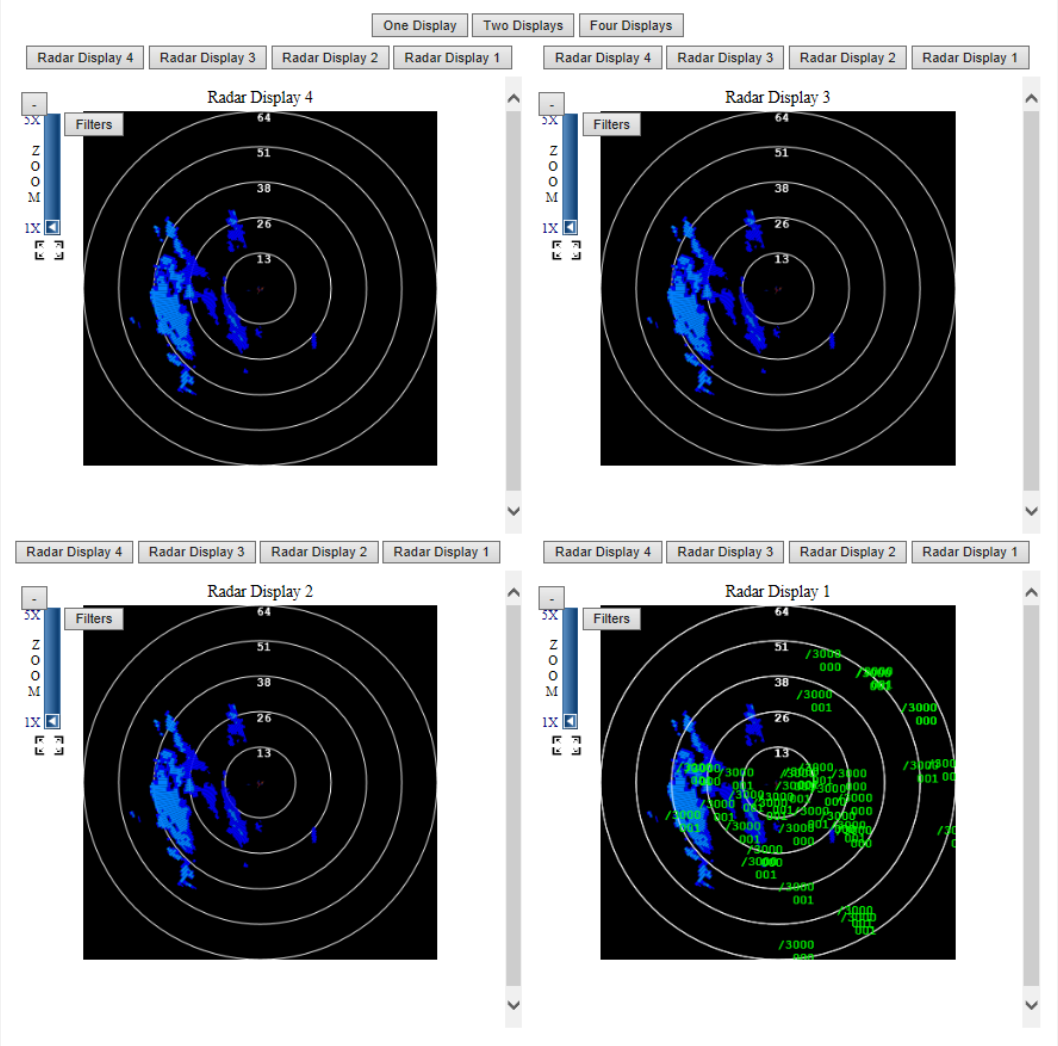


Figure 2-12: Four Radar Displays Example

To change the site being displayed on a radar screen, click the associated site button, like in the example that follows:

Located in the upper left corner of the active radar display is the **Filters** and **Zoom** panel (**Figure 2-13**), which consists of a zoom slider that can zoom up to five times the base resolution, a **Filters** button, and a full screen button (only available for browsers that support HTML5):

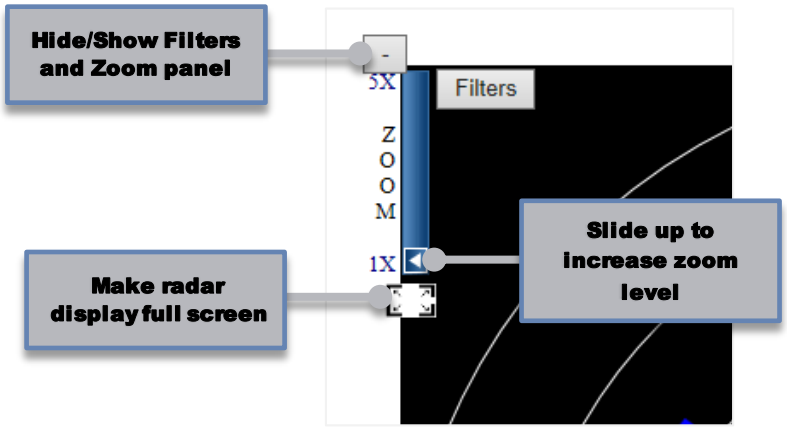


Figure 2-13: Filters and Zoom Panel

When zoomed greater than 1X, scroll bars appear at the bottom and right of the radar display to facilitate navigation, as shown in **Figure 2-14**:

Figure 2-14: Navigation Scroll Bars when Zoomed

Clicking the **Filters** button displays a dialog box, shown in **Figure 2-15**.

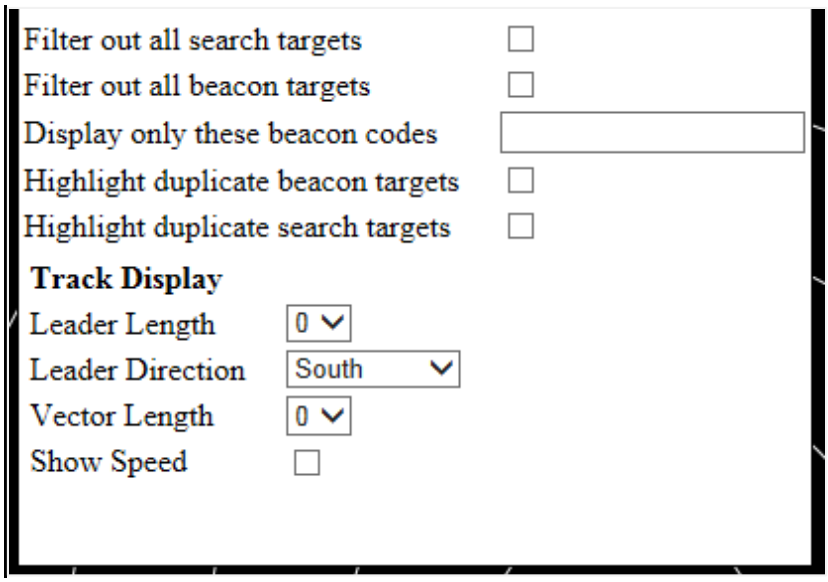


Figure 2-15: Radar Display Filter Options Dialog

The top two checkboxes in the **Filter Options** dialog box are used to filter out search and beacon targets, respectively, from the output radar display data. The **Display only these beacon codes** text entry box is used to enter one or more beacon codes that is shown on the radar output display. Multiple beacon codes must be separated by a space character. If used, only the entered beacon codes will appear on the radar display. The two checkboxes that follow cause duplicate beacon or search targets, respectively, to be highlighted in red on the output radar display.

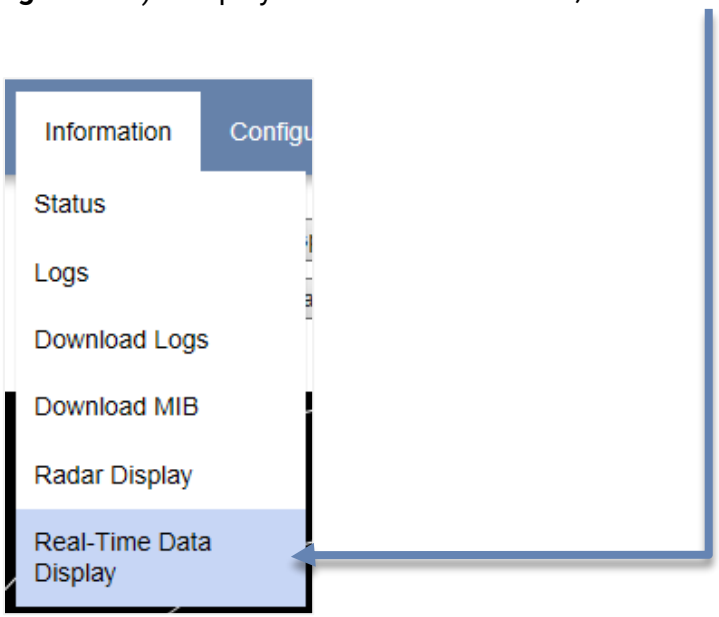
The remaining options are under *Track Display*. These options include **Leader Length** (0 – 5), **Leader Direction** (any cardinal or ordinal direction), **Vector Length** (0 – 5), and a checkbox for **Show Speed**.

To close the **Filter Options** dialog box, click the **X** button in the upper right corner of the box.

2.2.6 Real-Time Data Display

The *Real-Time Data Display* option allows the user to view generic message payloads in real-time when converting from one radar format to another. This utility must be configured in-between an input node and an output node in the configuration dataflow. The generic payload can be viewed in four ways on the GUI: Data, Text, Data+Text, and Generic Fields. The queue length, or maximum number of messages displayed on the GUI before filtering, is configurable from 1 to 1200.

The **Real-Time Data Display** screen (**Figure 2-16**) is displayed when the *Information*, *Real-Time Data Display* menu option is selected.



Without live data from a node or nodes, the default screen allows for the filtering of options, but there is no filtered data displayed under **Messages**.

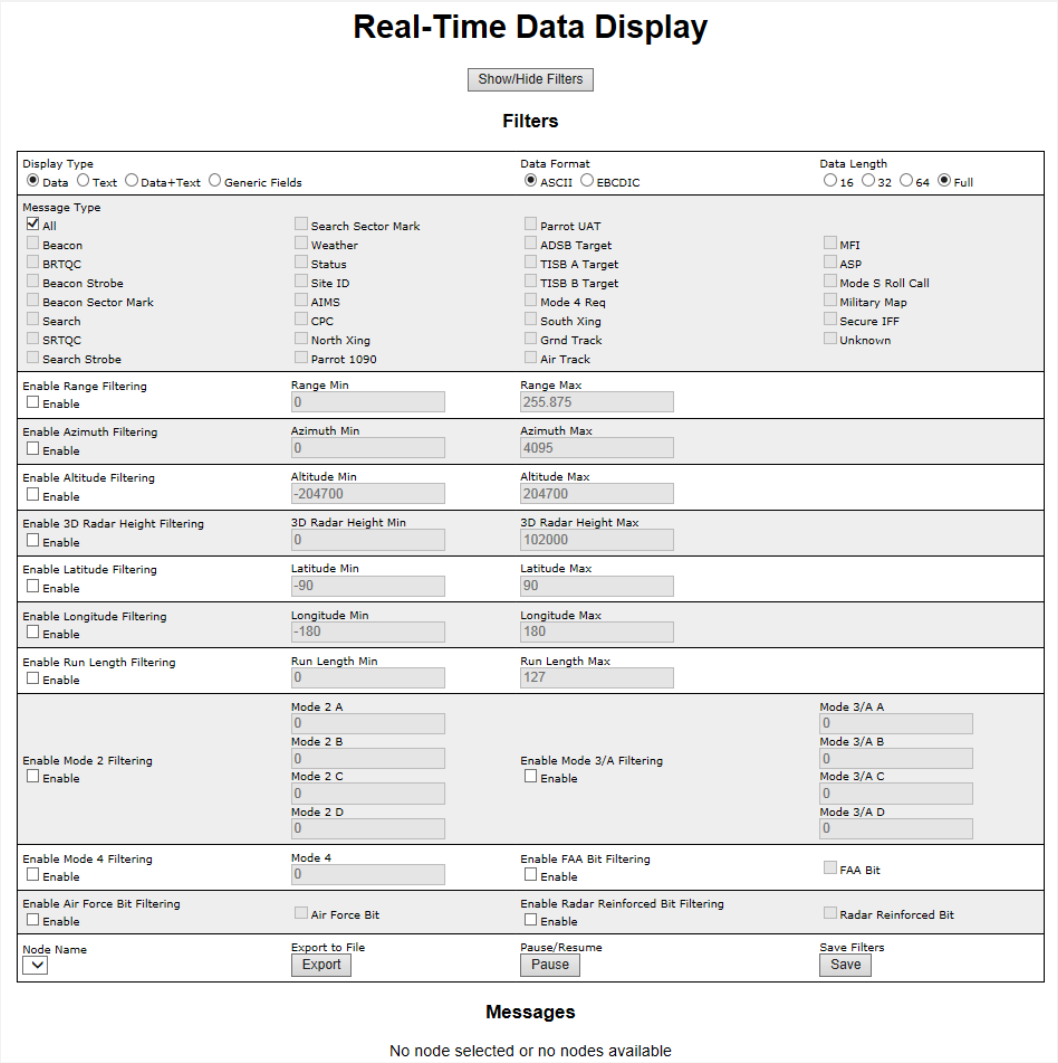
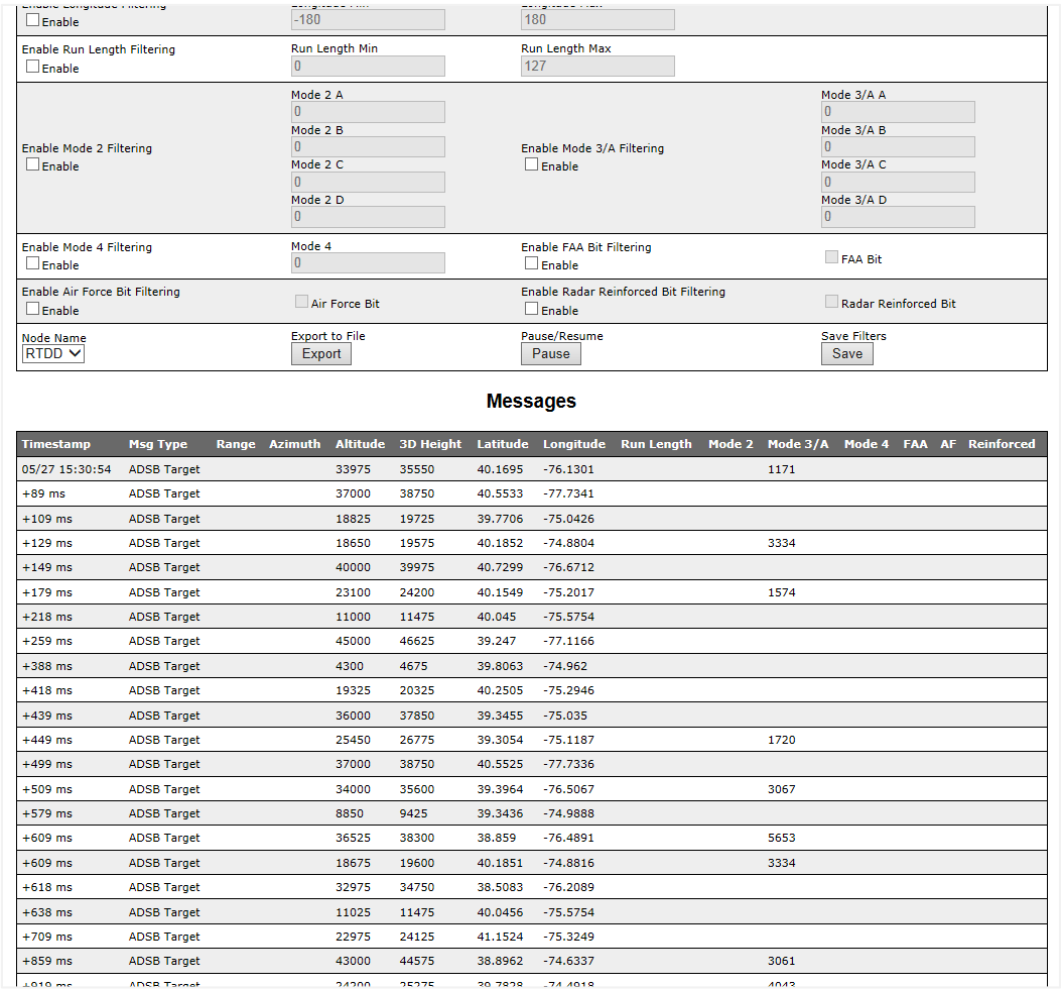


Figure 2-16: Real-Time Data Display (no data)

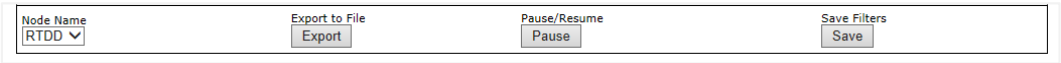
When a node or nodes are present, filtered data is displayed under **Messages**, like in the example shown in **Figure 2-17**.



Timestamp	Msg Type	Range	Azimuth	Altitude	3D Height	Latitude	Longitude	Run Length	Mode 2	Mode 3/A	Mode 4	FAA	AF	Reinforced
05/27 15:30:54	ADSB Target			33975	35550	40.1695	-76.1301			1171				
+89 ms	ADSB Target			37000	38750	40.5533	-77.7341							
+109 ms	ADSB Target			18825	19725	39.7706	-75.0426							
+129 ms	ADSB Target			18650	19575	40.1852	-74.8804			3334				
+149 ms	ADSB Target			40000	39975	40.7299	-76.6712							
+179 ms	ADSB Target			23100	24200	40.1549	-75.2017			1574				
+218 ms	ADSB Target			11000	11475	40.045	-75.5754							
+259 ms	ADSB Target			45000	46625	39.247	-77.1166							
+388 ms	ADSB Target			4300	4675	39.8063	-74.962							
+418 ms	ADSB Target			19325	20325	40.2505	-75.2946							
+439 ms	ADSB Target			36000	37850	39.3455	-75.035							
+449 ms	ADSB Target			25450	26775	39.3054	-75.1187			1720				
+499 ms	ADSB Target			37000	38750	40.5525	-77.7336							
+509 ms	ADSB Target			34000	35600	39.3964	-76.5067			3067				
+579 ms	ADSB Target			8850	9425	39.3436	-74.9888							
+609 ms	ADSB Target			36525	38300	38.859	-76.4891			5653				
+609 ms	ADSB Target			18675	19600	40.1851	-74.8816			3334				
+618 ms	ADSB Target			32975	34750	38.5083	-76.2089							
+638 ms	ADSB Target			11025	11475	40.0456	-75.5754							
+709 ms	ADSB Target			22975	24125	41.1524	-75.3249							
+859 ms	ADSB Target			43000	44575	38.8962	-74.6337			3061				

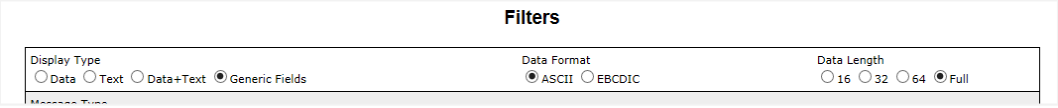
Figure 2-17: Real-Time Data Display (with data)

The last row of options is related to filtering settings and contains the following:



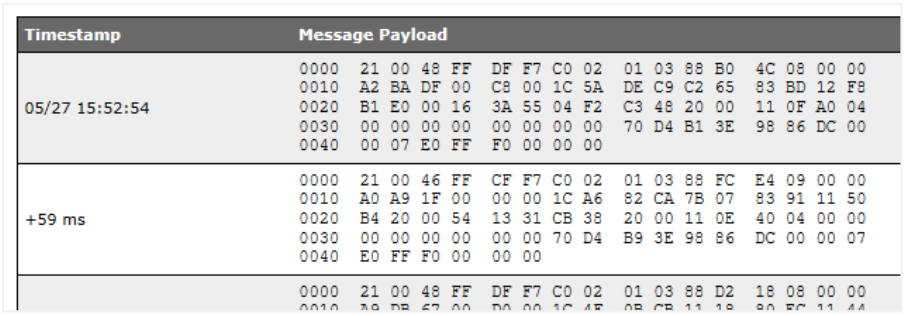
- **Node Name**—Select the active data source. When one or more Real-Time Data Display nodes are present in the active configuration, the list will show the names of these nodes. Otherwise, this field will be empty and no data will display in the **Messages** area.
- **Export to File**—Save the current data table shown under **Messages** as *rtddData.csv* (or any other file name specified) to a drive location of your choosing.
- **Pause/Resume**—Pause or resume the flow of data from the currently selected *Node Name*.
- **Save Filters**—Save the current filter settings configuration directly to the device for the currently logged in user. These saved settings will become the new default settings for all future visits to this page for the current user until new filter settings are saved.

Any changes to the filter settings take immediate effect on the active *Node Name*. While most settings filter specific generic data fields, the first row of settings modify how the data is represented:



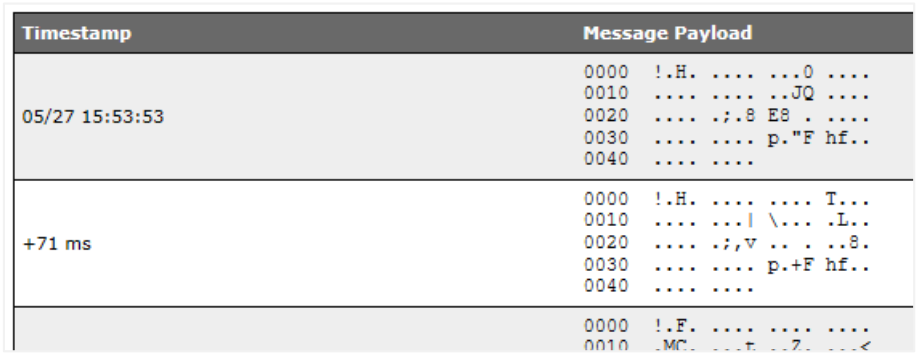
- **Display Type**—The options are *Data*, *Text*, *Data+Text*, and *Generic Fields*.
  - **Data**: Display the message payload only as raw hexadecimal.

    Example:



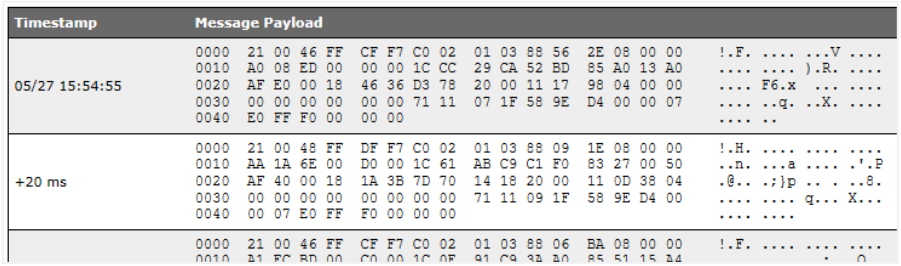
  - **Text**: Display the message payload only as text (format specified under *Data Format*). Note that non-printable characters are replaced with a period.

    Example:



- **Data+Text**: Display the message payload as both raw hexadecimal and text (format specified under *Data Format*).

  Example:



Timestamp	Message Payload
05/27 15:54:55	0000 21 00 46 FF CF F7 C0 02 01 03 88 56 2E 08 00 00 !.F. ....V .... 0010 A0 08 ED 00 00 00 1C CC 29 CA 52 BD 85 A0 13 A0 ....).R. .... 0020 AF E0 00 18 46 36 D3 78 20 00 11 17 98 04 00 00 .... F6.x ... . 0030 00 00 00 00 00 00 71 11 07 1F 58 9E D4 00 00 07 .... ..q. ..X. .... 0040 E0 FF F0 00 00 00 .... ..
+20 ms	0000 21 00 48 FF DF F7 C0 02 01 03 88 09 1E 08 00 00 !.H. .... 0010 AA 1A 6E 00 D0 00 1C 61 AB C9 C1 F0 83 27 00 50 ..n. ...a .... .'.P 0020 AF 40 00 18 1A 3B 7D 70 14 18 20 00 11 0D 38 04 .@.. .;}p .. . ..8. 0030 00 00 00 00 00 00 00 00 71 11 09 1F 58 9E D4 00 .... q... X... 0040 00 07 E0 FF F0 00 00 00 ....
	0000 21 00 46 FF CF F7 C0 02 01 03 88 06 BA 08 00 00 !.F. ....

- **Generic Fields**: Display the values of the generic fields for each generic message.

  Example:

Timestamp	Msg Type	Range	Azimuth	Altitude	3D Height	Latitude	Longitude	Run Length	Mode 2	Mode 3/A	Mode 4	FAA	AF	Reinforced
05/27 15:56:18	ADSB Target			33000	32975	39.5704	-78.3168							
+30 ms	ADSB Target			2000	2250	39.9126	-75.0641							
+50 ms	ADSB Target			10675	11325	40.5114	-73.7131							
+269 ms	ADSB Target			38000	39775	39.877	-77.2157							
+279 ms	ADSB Target			20000	19975	40.2156	-75.7689							
+309 ms	ADSB Target			24425	25700	40.6735	-77.1827							
+402 ms	ADSB Target			22925	24175	39.806	-73.743							
+402 ms	ADSB Target			4600	4700	40.3226	-75.6067			0451				
+402 ms	ADSB Target			38000	39750	40.5117	-75.1741							
+420 ms	ADSB Target			36025	37775	40.4114	-75.6858							
+480 ms	ADSB Target			1800	1900	40.0934	-74.837			1200				

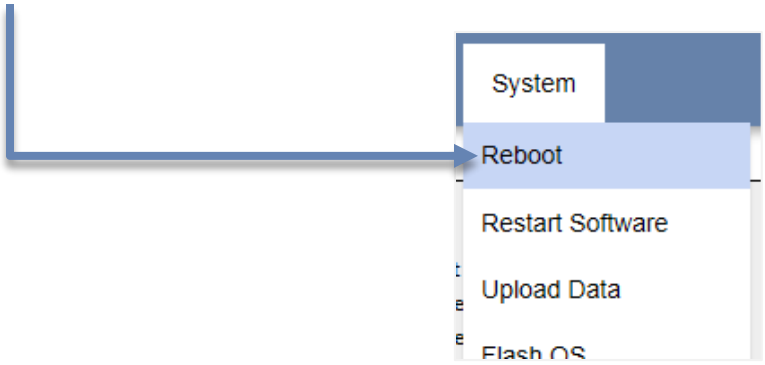
- **Data Format**—Choose between American Standard Code for Information Interchange (ASCII) or Extended Binary Coded Decimal Interchange Code (EBCDIC) text modes.
- **Data Length**—Select between *16*, *32*, *64*, or *Full* data lengths.

2.3 Reboot/Restart/Shutdown

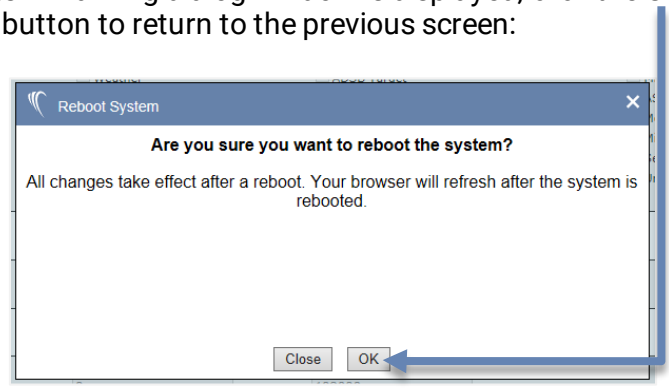
Reboot, restart, and shutdown options are described in the subsections that follow.

2.3.1 Rebooting the System

Some operations require the system to be rebooted in order to take effect. To reboot, select the *Reboot* option from the *System* menu.

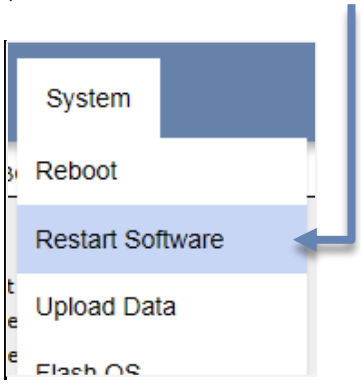


When the **Reboot System** warning dialog window is displayed, click the **OK** button to reboot the system, or the **Cancel** button to return to the previous screen:

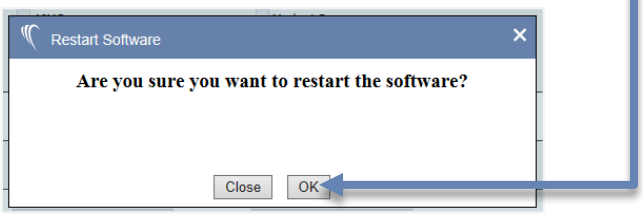


2.3.2 Restarting the System

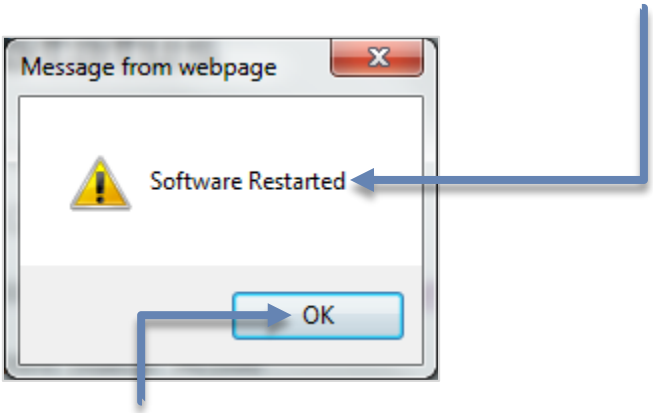
It may be desirable to restart the system software without rebooting the system, e.g., activating a selected configuration file. To restart, select the *Restart Software* option from the *System* menu.



When the **Restart Software** warning dialog window is displayed, click the **OK** button to restart the system software, or the **Cancel** button to return to the previous screen:



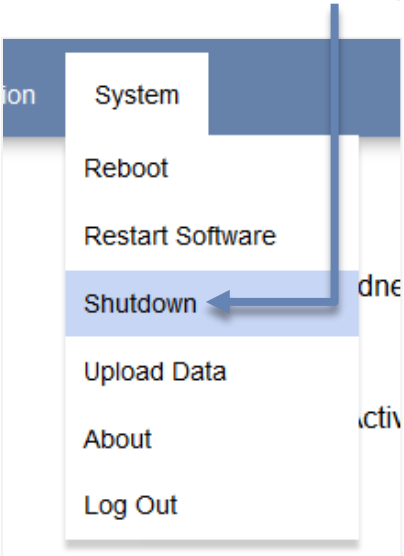
Upon successful restart, the message, “Software Restarted,” is displayed.



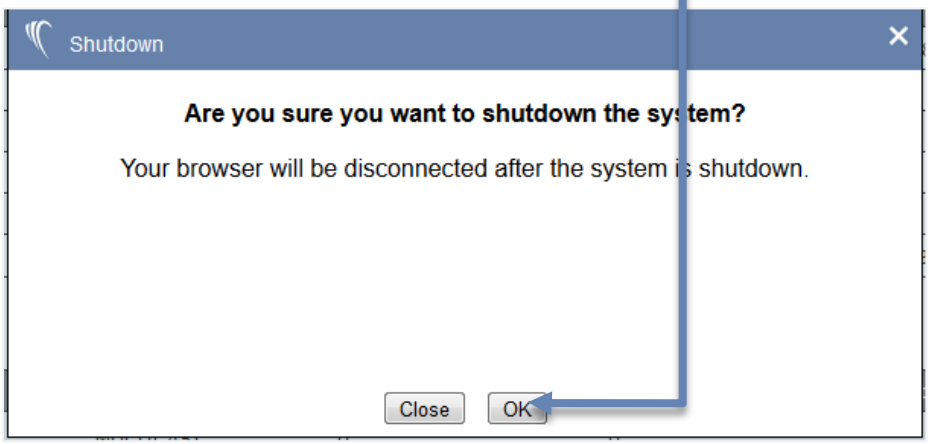
Click the **OK** button to acknowledge the software restart.

2.3.3 Shutting Down (SGP Only)

In order to properly shut down the SGP, select the *Shutdown* option from the *System* menu:

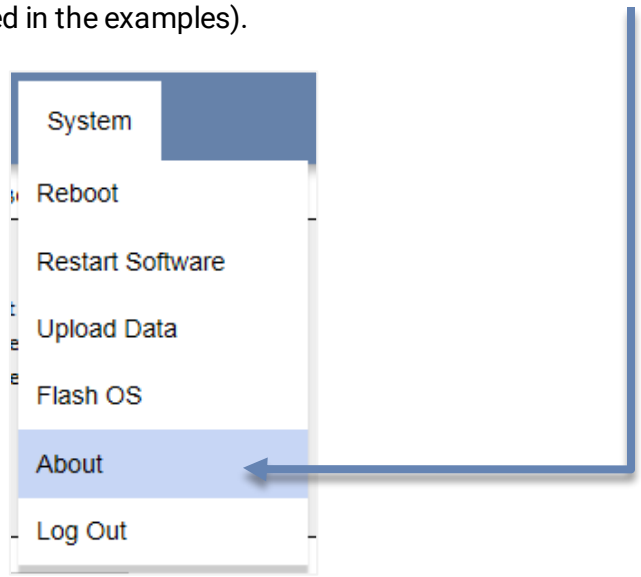


When the **Shutdown** warning dialog window is displayed, click the **OK** button to shut down the SGP, or the **Cancel** button to return to the previous screen.

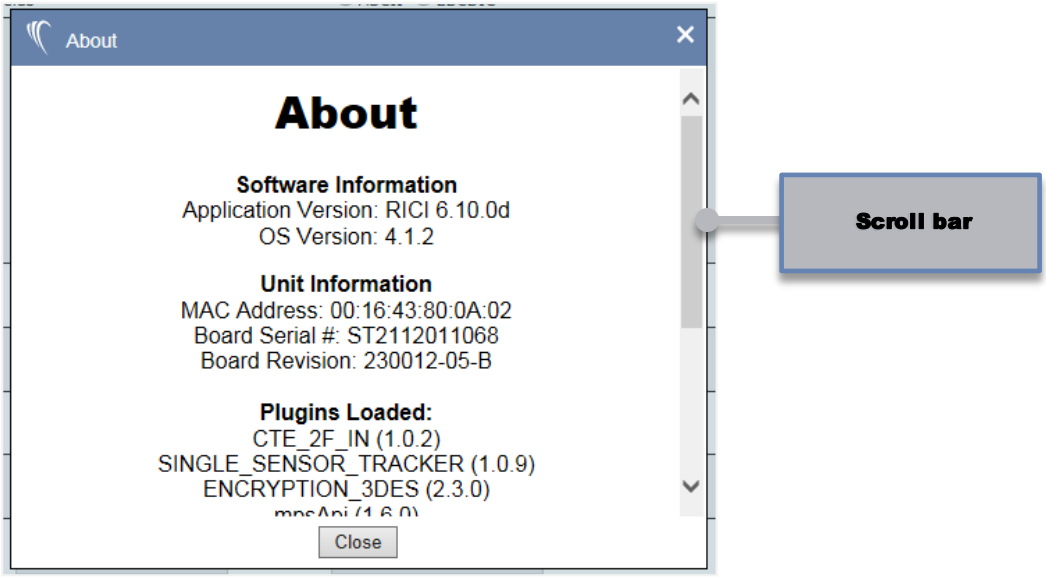


2.4 About Option – Verifying System Information

Information specific to the system that was purchased can be verified by selecting *About* from the *System* menu (RICI screens are used in the examples).



This information is required should you need to contact Sunhillo regarding any issues or requests for software updates. *Applicable Software Information*, *Unit Information*, *Plugins Loaded*, and *License Features* are all presented in the **About** window (generic example follows).



The **Board Serial #:**, found under *Unit Information*, is used by Sunhillo to maintain warranty information on your purchased product. Click the **OK** button to close the *About* window and return to the previous screen.

Section 3

3. SYSTEM CONFIGURATION

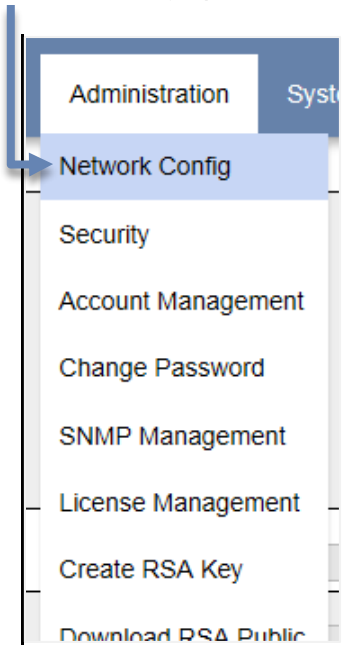
In this Section, you gain an understanding of the SureLine Core's system configuration options.

The SureLine Core's system configuration, which is described in the subsections that follow, consists of the following items:

- Network IP address
- Routing configuration
- DNS configuration
- Hostname configuration
- GUI time out value
- IPv6 settings
- Network Time Protocol (NTP) settings
- Syslog forwarding information (RICI, Longport, and Ventnor only)

3.1 Network Config Screen

The *Network Config* screen is used to modify various system parameters. The system configuration information is displayed when the *Network Config* option is selected from the *Administration* menu.



Note

When changes are made to the parameters under *Network Config* and applied with the **Apply** button, all changes, with the exception of *Hostname* under **Hostname Configuration**, take immediate effect without the need for a reboot.

Each Section of the *Network Config* screen (example shown in **Figure 3-1**; Note that **Syslog Forwarding Configuration** only applies to RICI, Longport, and Ventnor) is described in the subsections that follow.

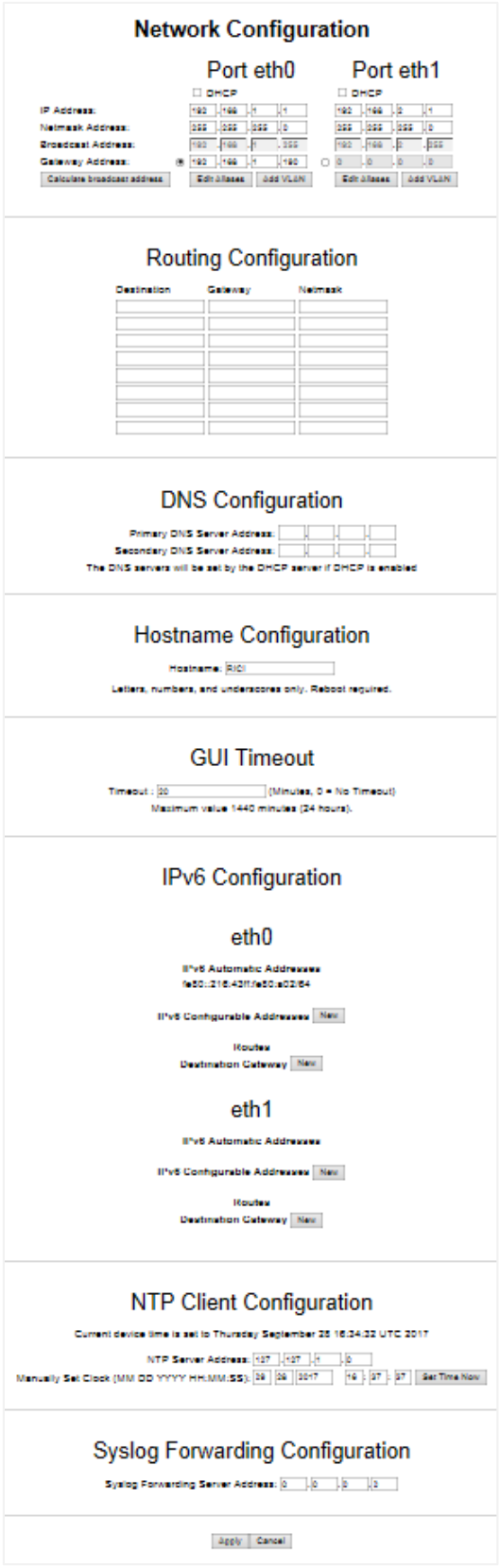


Figure 3-1: Extended View of the Network Config Screen

To accept the displayed settings on the *Network Config* screen as-is, choose another menu option on the Main Menu bar to exit the screen. If modifications are made to this screen, use the **Apply** or **Cancel** buttons located at the bottom of the screen if you want to accept the changes, or reject or undo the changes, respectively. The network and system information configured on the *Network Config* screen are persistent within the device once the changes are applied (saved).

3.1.1 Network Address Configuration

On the *Network Config* screen, the configuration for entries labeled **Port Eth0** and **Port Eth1** (**Figure 3-2**) correspond to Ethernet port 0 and Ethernet port 1, respectively, and, if applicable, continue in that manner for each additional Ethernet port present. For each Ethernet port, the IP, Netmask, Broadcast, and Gateway addresses must be configured. The radio button associated with the Gateway address indicates which gateway is to be used.

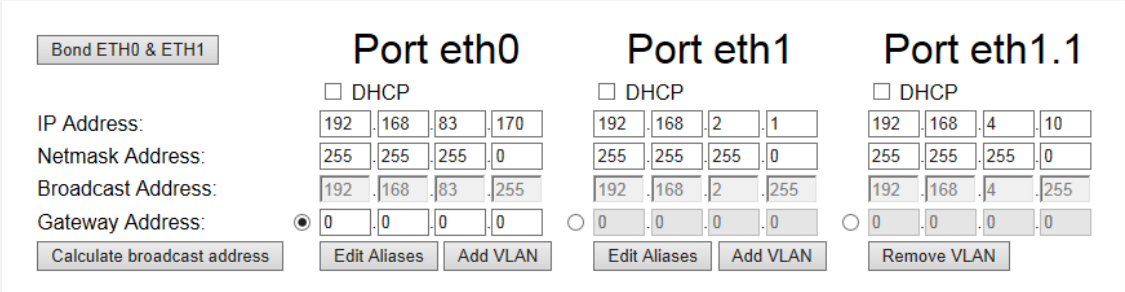


Figure 3-2: Network Address Configuration Example

The **Broadcast Address:** fields are greyed out in order to indicate that the user cannot manually enter an address. The **Calculate broadcast address** command button is provided for informational purposes only. Selecting this button automatically generates the correct broadcast address based on the values entered for the IP and Netmask addresses. This information might be useful if you need to broadcast data to the device.

Click **Add VLAN** if you want to add a new Virtual Local Area Network (VLAN) to one of the Ethernet ports. The VLAN Id, IP Address, and Netmask Address should then be set (**Figure 3-3**).

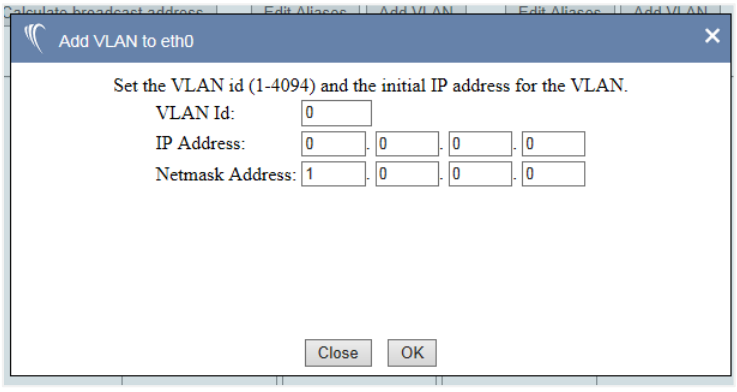


Figure 3-3: Add VLAN Configuration Window

For Ventnor and RICI 5000 devices, click **Bond ETH0 & ETH1** (**Figure 3-4**) if you want to allow the **Eth0**/**Eth1** interfaces to be treated as a redundant pair. This type of redundancy differs from modes that can be configured as shown in Section **7 REDUNDANCY**. When **Eth0** and **Eth1** are bonded, they operate as a single, logical interface. In practical terms, it means that with both **Eth0** and **Eth1** connected to the same network switch, they exist as only one IP address on the network and to remote systems.

Figure 3-4: Bond ETH0 & ETH1 Button

DHCP addressing can be selected on Ethernet using the respective **DHCP** checkbox. Similarly, IP Aliases can be set for any Ethernet port using the respective aliases button (**Figure 3-5**). Note, however, that DHCP and aliasing are not supported in bonding mode.

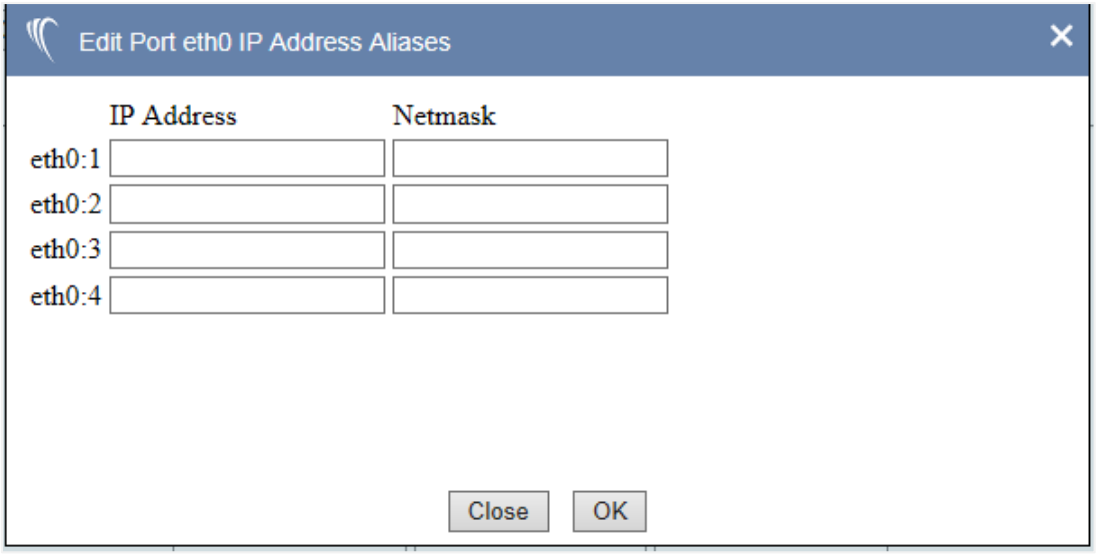


Figure 3-5: IP Address Aliases Configuration Window

3.1.2 Routing Configuration

The *Routing Configuration* Section (**Figure 3-6**) of the *Network Config* screen is used to configure the IP routes necessary for sending/receiving LAN data other than the default routes, which are set by the gateway address. The routing addresses need to be configured if you want to use Unicast, TCP/IP, or access the device via the Internet from the Ethernet port that is not on the default gateway subnet.

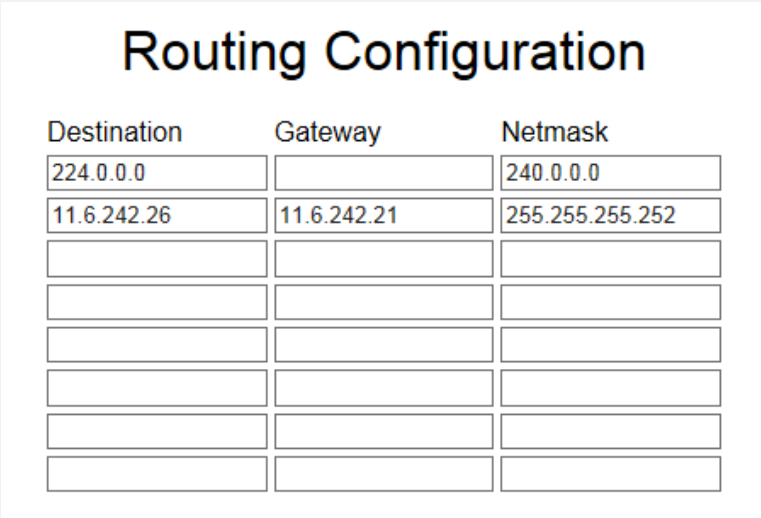


Figure 3-6: Routing Configuration Example

If the device needs to access a particular subnet through a router, use the following steps to configure the routing table:

5. Enter the destination IP address subnet in the **Destination** field
6. Enter the router IP address in the **Gateway** field
7. Enter the netmask in the **Netmask** field

Note

If the OS version on your device has a #XX version number and the device is to receive multicast data through routers (and if the router is configured to remove the unused path periodically), the routing table for the device must be:

- `224.0.0.0` in the **Destination** field
- `240.0.0.0` in the **Netmask** field

3.1.3 DNS Configuration

The *DNS Configuration* section of the *Network Config* screen is used to configure the primary and secondary DNS server addresses if DHCP is not previously enabled (see Section **3.1.1**). If DHCP was previously enabled, the address fields will be greyed out and inaccessible.

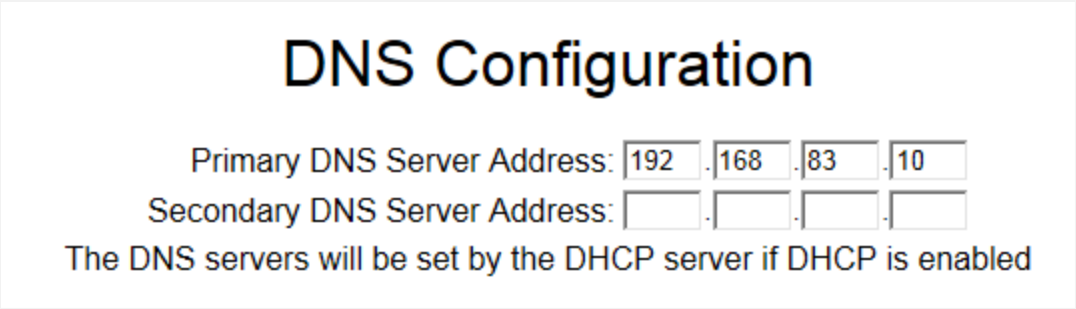


Figure 3-7: DNS Configuration Example

3.1.4 Hostname Configuration

The *Hostname Configuration* Section (**Figure 3-8**) of the *Network Config* screen is used to configure the hostname of the device. The hostname can be up to 32 characters in length and can only include letters, numbers, and underscores. A reboot is required to apply any hostname changes.

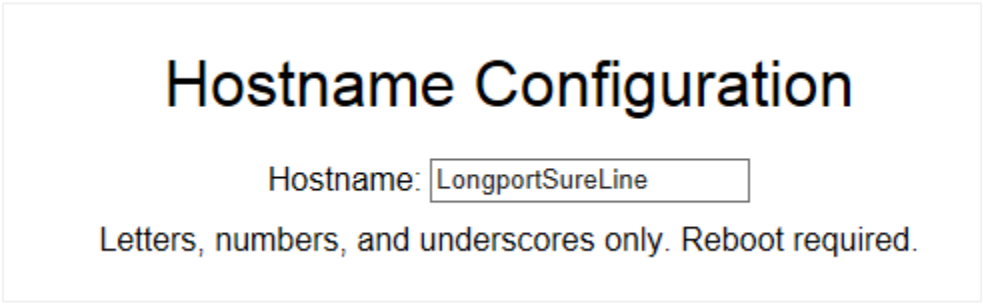


Figure 3-8: Hostname Configuration Example

3.1.5 GUI Timeout

The GUI is configured to time out after 20 minutes of inactivity. To override this default setting, modify the number of minutes designated in the *GUI Timeout* Section (**Figure 3-9**) of the *Network Config* screen. Setting this value to `0` indicates that no timeout should occur.

Note

The new timeout will take effect immediately after the **Apply** button is selected; i.e., it does not require a reboot of the system.

Figure 3-9: GUI Timeout Example

3.1.6 IPv6 Client Configuration

The device supports Internet Protocol version 6 (IPv6) interfaces via its Ethernet port connections. The *IPv6 Configuration* Section (**Figure 3-10**) of the *Network Config* screen is used for address changes.

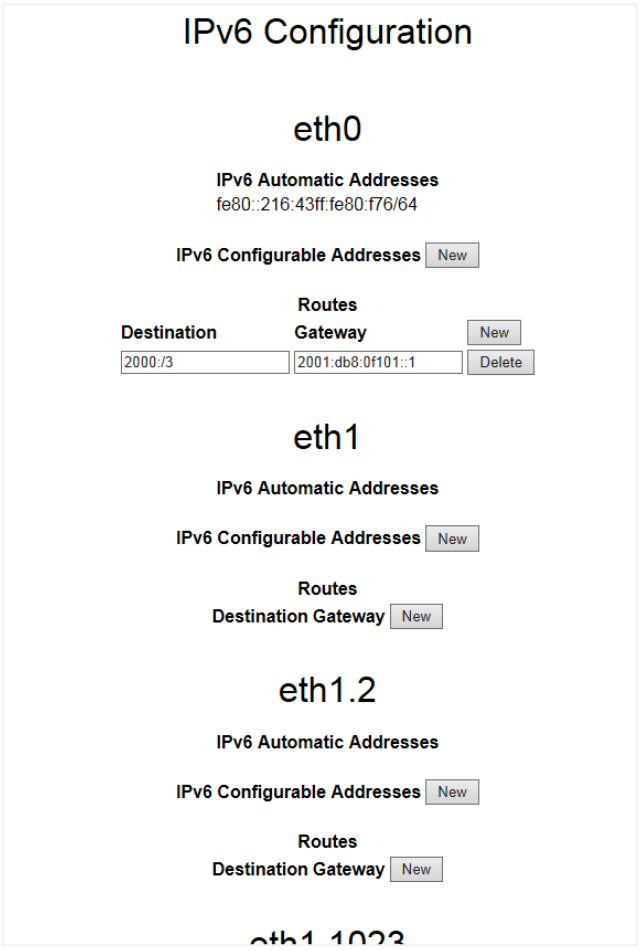
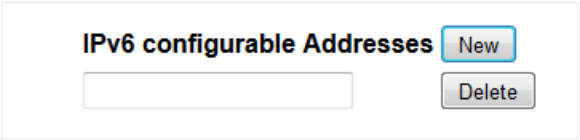


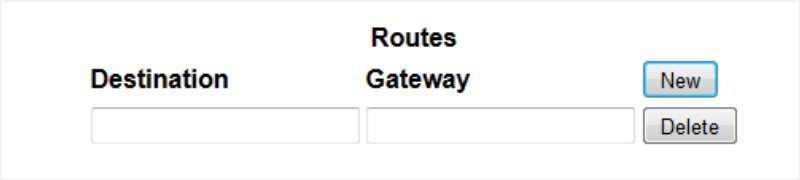
Figure 3-10: IPv6 Configuration Example

To enter a new IPv6 address, click the **New** button associated with the *IPv6 configurable Addresses* field for the given Ethernet port. The input field is displayed as follows:



Type in the new IPv6 address. Multiple addresses can be entered via the **New** button.

To enter a new IPv6 route, click the **New** button associated with the *Destination Gateway* field for the given Ethernet port. The input fields are displayed as follows:



Type in the new IPv6 *Destination* and *Routes Gateway* addresses. Multiple routes can be entered via the **New** button. To remove IPv6 configurable addresses and/or routes, click the **Delete** button to the right of the address.

3.1.7 NTP Client Configuration

When operational, the device functions in Network Time Protocol (NTP) client mode. The *NTP Client Configuration* Section (**Figure 3-11**) of the *Network Config* screen is used to assign the NTP Server address and/or manually set the synchronization clock.

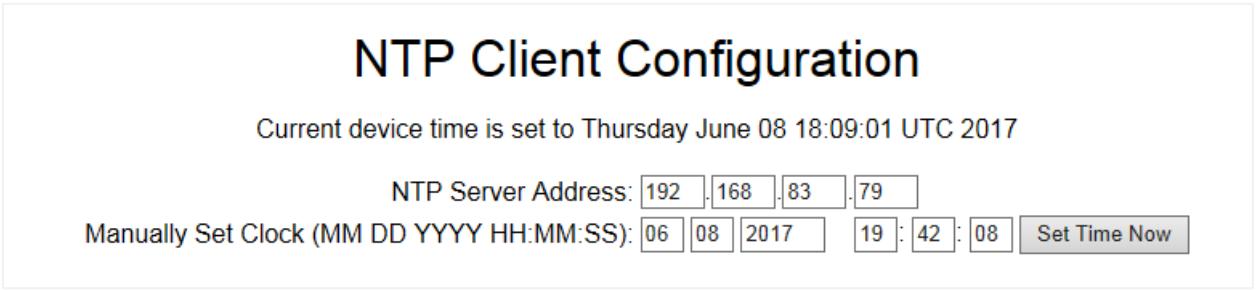


Figure 3-11: NTP Client Configuration Example

To set the clock, type in the time information in the **Manually Set Clock** field, and click the **Set Time Now** button. A reboot of the device is not necessary. The time entered takes effect immediately when the **Set Time Now** button is selected.

3.1.8 Syslog Forwarding Configuration

The *Syslog Forwarding Configuration* Section (**Figure 3-12**) of the *Network Config* screen is used to assign the audit server to which the syslog daemon will forward the system logs. Enter the IP address of the server in the *Syslog forwarding Server Address* field to enable the forwarding. A value of `0.0.0.0`, which is the default setting, disables syslog forwarding.

Figure 3-12: Syslog Forwarding Configuration Example

Section 4

4. FUNCTIONAL CONFIGURATION

In this Section, you gain an understanding of the SureLine Core's functional configuration options.

The concepts behind the operational and functional configuration of a device, as well as elements of its SureLine Core GUI, are described in this Section. In addition, instructions on how to use the GUI to create or edit a device configuration are provided.

4.1 Configuration Menu

On the menu bar, select the *Configuration* menu (**Figure 4-1**). The menu options available under *Configuration*, with the exception of *Network Config*, are discussed in detail throughout this Section. The *Network Config* option is discussed in Section **3**.

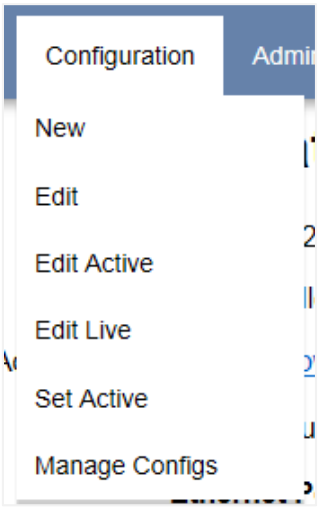


Figure 4-1: Configuration Menu

4.2 Configuration Elements

Before discussing the creation of an active configuration using the GUI, it is important to understand the concepts and define the terms used when creating a system configuration, as well as review the prerequisites and requirements for generating a configuration data flow.

A system configuration consists of the following basic elements:

- Data Flow
- Nodes
- Site/Sensor(s)

The device processes data from serial ports or a LAN by identifying individual messages in the data. These messages are then given specific metadata and passed to functional software nodes that work on the data messages individually by filtering, breaking down into smaller messages, converting, or adding more metadata for use by other software nodes. When this data has been processed by the desired functions, an output software node exports the data onto either a serial port or an Ethernet port.

4.2.1 Data Flow

A data flow consists of various graphical elements that help to visualize conceptually how data is entering and exiting the system for a particular device functional configuration. The data flow determines where and how data is coming into the device and what is to be done with this data, such as conversion and/or filtering. A data flow consists of two or more nodes and ties all nodes together to create the output flow, like is shown in **Figure 4-2**.

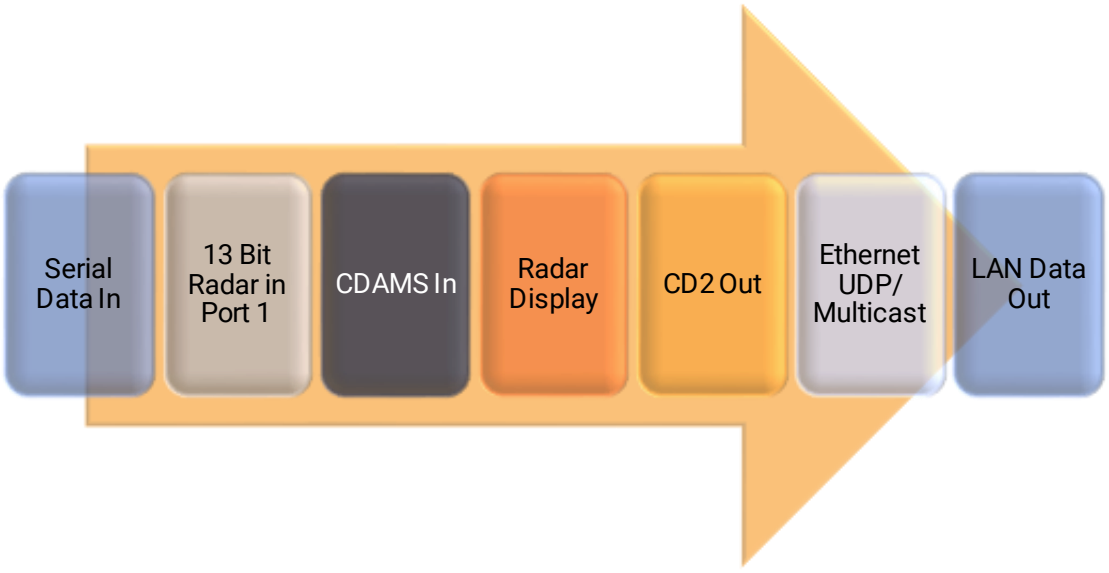


Figure 4-2: Data Flow

A data flow can also be split or "branched" into several paths. A branch in a data flow takes a single source of input data and performs multiple, unique operations on the data to produce unique output on each data path. This data can be transmitted to multiple outputs or "merged" (joined) back into a single path to be transmitted from a single source. **Figure 4-3** shows a conceptual diagram of a data flow that branches and merges.

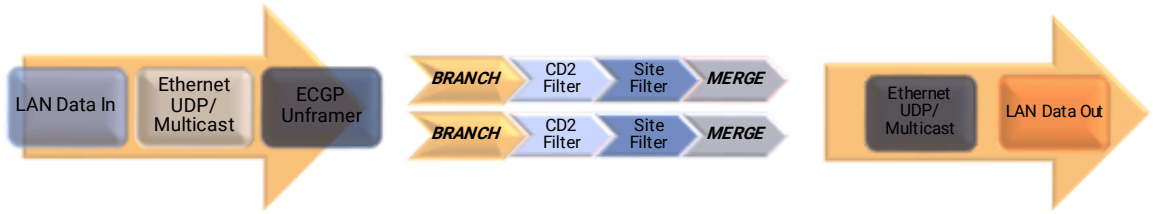


Figure 4-3: Data Flow that Branches and Merges

4.2.2 Node

Conceptually, a node is a system module that performs a specific task on a data message at a particular point in the data flow. Nodes are divided into two basic types: Input/Output (I/O) and Function. Each node type has a set of user configurable parameters particular to that type. These parameters have pre-configured default values that can be modified by the user at any time.

4.2.2.1 Input/Output Nodes

A system configuration must always have at least one input node and one output node. The I/O nodes are further classified into sub-categories based on the source of the input or type of transmission (**Table 4-1**).

Table 4-1: I/O Node Categories and Descriptions

I/O Node Category	Description
Serial	Represent data received (input) or transmitted (output) through the RICI or Longport's DB-25 connectors.
LAN	Depict data received (input) or transmitted (output) through the device's Ethernet ports.
File	Used for input data contained in a file.
Bidirectional	Used to receive and transmit data from a single node within a data path.
RF Receivers	Used for the ADS-B Input on Longport devices.
Other	Reserved for output node types that do not physically transmit data out of the device, but serve as a logical endpoint in the data flow. These node types mark the graphic representation of data when using the *Radar Display* or *KML Display* utility function node.

4.2.2.2 Function Nodes

A function node performs an action on the data input to the node. These "actions" include conversion to another data type or format, filtering out specific information from the data, adding user configured or calculated data to a message, and packing or unpacking data from a particular type of message header.

The device is purchased with standard (base) functions and optional premium functions. The premium functions are licensed by Sunhillo and require a license code for activation. The function nodes are classified into sub-categories based on the action they perform on the data (**Table 4-2**).

Table 4-2: Function Nodes and Descriptions

Function Node Category	Description
Framer/Unframer	Pack/Unpack data from a message header.
Specific Conversions	Convert a specific type of input data to a specific type of output data.
Utilities	Perform unique tasks on the data in order to add/extract data for use in visual displays, which can be either provided by the device or sourced external to the device.
Filter	"Filter out" specific data or messages from the input data stream.
Input Radar Types	Convert specific input data types into a default, generic message format that is used (internally) by the system software.
Output Radar Types	Convert the default, generic message format to a specific output data format.
Plug-in	Separately installed application plug-ins that interface with the system software in order to provide a specific conversion or added functionality.

Several function node types provide unique filtering or display conversion functionality that warrants further detail than is provided through the GUI when clicking on a function node. The details of the unique function nodes are as follows:

- **Mode 3A Range/Azimuth Filter**—The "Mode 3A Range/Azimuth" Filter function node uses a series of message data checks to determine if the received Beacon or BRTQC message should be dropped (filtered). The first check is a Mode3A Code. If the received message Mode3A code matches the Mode3A code of the filter, the associated range, azimuth, and altitude are checked against the configured start and end values of the filter. If any of the checks for range, azimuth, and altitude fail, i.e., if the data in the message is less than the minimum configuration value or greater than the maximum configuration value for range, azimuth and altitude, the Beacon or BRTQC message is processed (not dropped). The radar message is dropped if the Mode3A code matches the filter configuration and the range, azimuth, and altitude all fall within the configured start and end ranges of the filter.

- **Geo Filter**—The *Geo Filter* function node's "Polygon File" configuration parameter is a text file that gets uploaded to the system. This file must contain three or more points listed as single line entries of latitude and longitude, which are separated by a comma. The last latitude/longitude entry must connect back to the first entry of the polygon file. The polygon file must have the extension *.po* and can have end line or single line comments, which are denoted by the # symbol.

  The following is an example of a typical polygon file's contents:

```
34.815, -117.266  #Top Left

31.649, -117.953  #Bottom Left

23.862, -97.423   #Bottom Right

27.687, -95.396   #Top Right
```

- **KML Display**—The *KML Display* utility function node converts received targets to Keyhole Markup Language (KML) for visual display using Google Earth.

  In order to use this function, the display target must have latitude/longitude information. If the input radar format does not have this information as part of its data stream, the coordinates can be added by using the *Add Lat Long* function earlier in the data flow. Additionally, the *KML Display* function uses the radar name configured in it as a filter. If the input radar does not supply this information, the *Radar Ident* function must first be adapted to add a name to the radar.

  In order to use Google Earth, you must make a new network link with a value of `http://<Device_Address>:8080/cgi/getKml.cgi?kml=<KML Display Function>` for a feed with Beacon codes and `http://<Device_Address>:8080/cgi/getKml.cgi?kml=<KML Display Function>-nb` for a feed without Beacon codes.

  For example, if the device is at network address of 192.168.1.1, the "KML Display" name is ZCY_KML, and you wish to subscribe to two feeds – one with Beacon codes and one without Beacon codes – you would need to create two network links with the following values:

  - http://192.168.1.1:8080/cgi/getKml.cgi?kml=ZCY_KML
  - http://192.168.1.1:8080/cgi/getKml.cgi?kml=ZCY_KML-nb

  After setting the link addresses, you should set the display to refresh periodically (every 1 to 3 seconds).

4.2.3 Site/Sensor

A site configuration element provides identifying information about input data used for filtering and radar characteristics about that data. One or more sites can be created for a configuration.

All serial interfaces require a site. A sensor must be associated with a radar data serial input node type. If a serial output node type is selected, the system software can automatically generate a site element that can be further configured for specific data. Sites are needed by several of the system functions that convert or filter the data. Other node types that require a site/senor are described in Section **4.2.3**.

4.2.4 Data Flow Configuration Restrictions

Before creating or editing a data flow, it is important to discuss what information is required and the pre-conditions for adding node types to a data flow path.

4.2.4.1 Required Node Types

Although a data flow can be created with multiple node types, not all node types can be placed in the data flow in any order. Various node types will only function properly if they are preceded in the data flow by particular node types. Each node type performs some function on the data and certain node types expect specific information about the data to be available in order to perform properly.

Example #1

The *Site Filter* node type requires the data to have a site name associated with it. If the incoming data is a raw UDP packet, there is no sensor or site information associated with this raw data. Another node type must be used in the data flow prior to the *Site Filter* node, which will associate a site name with this data. The *Radar Ident* node type allows a site name to be configured and associated with data. One of these two node types is required in the data flow in order to use a *Site Filter* node.

Example #2

In order to output data in CSV format using the *Msg Format CSV* node type, the data coming into this node type must first be received by an input node type. One of the functions from the *Input Radar Types* category of function nodes is necessary in the data flow prior to the *Msg Format CSV* node type.

GUI Feedback

The configuration GUI provides feedback and information when a particular node type cannot be used at a particular point in a data flow and what is required (prerequisites) in order to configure the

4.2.4.2 Unique Node Types

Some node types can only be configured into a data path (or branch) in a data flow one time. In these cases, the GUI provides feedback and details when more than one of a particular node type cannot be inserted into a data flow.

4.2.4.3 Required Sensor

Several node types require a site/sensor in order to function properly. A sensor must be created that is then associated with a particular message based on either the Site name or site ID in the data message received by the node.

The specific node types that require a sensor are:

- All input/output serial node types
- ARTS to CD2
- ARTS Unpacker
- SGF Unframer
- CD to FAA RAPPI
- CD to ASTERIX CAT48/34
- ASTERIX CAT33 to CD2
- Raw Radar File Playback

It is recommended that the desired sensors be created first, each with unique "Radar ID," "Site Name," and "Logical Name" configuration parameter values. When adding/editing these node types in the data flow, you can then associate the appropriate sensor (using the "Radar ID" configuration parameter) with each node. Other Sensor configuration parameters can be configured as desired based on the required data for the data flow.

For RICI and Longport devices, in the case of *Serial Output* node types, the GUI will automatically generate a sensor for each node of that type when the "Radar ID" parameter is set to "Auto." The sensor is created and displayed in the *Sensor Configuration* Section when the configuration file is saved. You will need to edit the sensor to set the configuration information, such as site name and radar ID, if desired.

4.3 Configuration Files

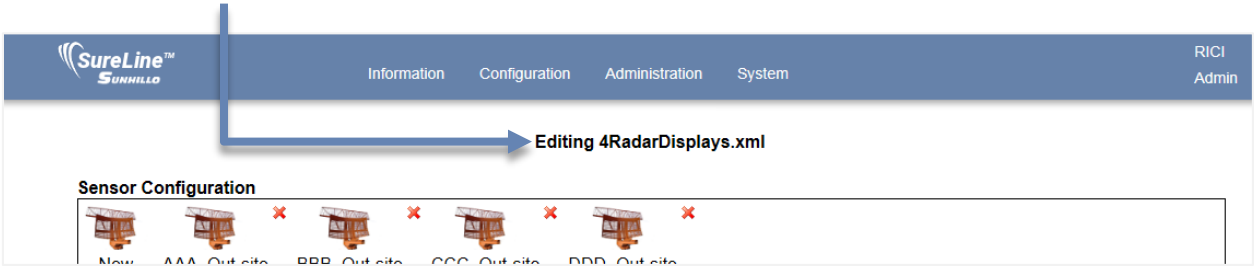
A device configuration is created using the GUI, with the information for the configuration stored in Extensible Mark-up Language (XML) format in a file that resides on the device.

4.3.1 Getting Started – New vs. Edit

A configuration file must always be opened in order to create or edit a configuration. There are four configuration file options under the *Configuration* menu: *New*, *Edit*, *Edit Active*, and *Edit Live*.

Once a file has been selected, the **Data Flow Configuration** screen is displayed. This screen is described in detail in Section **4.2.4**.

The name of the configuration file opened for editing is displayed in the upper center of the screen, like in the example that follows:



4.3.1.1 Creating a New Configuration

You can choose to create a device configuration using a template file provided by the application software. Selecting the *New* option from the *Configuration* menu (**Figure 4-1**) displays a list of available sample files to choose from to provide a template for creating a new, not pre-existing, configuration. Once an appropriate sample is chosen, the node types and configuration parameters of these nodes can be modified as needed. This new configuration file must be saved under a different file name. Sample configuration files, i.e., files with an _ (underscore) in the name, cannot be deleted. A list of those sample files with a description of what each provides is shown in **Table 4-3**. The description of each sample file provides the input data, what other functions (framers, filters, or conversions) are performed on this data, and the output data.

Table 4-3: Sample Configuration Files and Description

RICI	Longport	Ventnor	Margate II ADS-B	SGP	Sample XML File	Description
☑	☑	☑	☐		_1_channel_13_bit_to_lan	**Input**: Four single channel radars (serial data) **Other Functions**: ECGP Framer **Output**: Single LAN destination
☑	☑	☑	☐		_1_channel_sync_serial_to_lan	**Input**: Four single channel data streams (serial data) **Other Functions**: none **Output**: Four different LAN destinations
☑	☑	☑	☐		_4_channel_13_bit_to_lan	**Input**: Single radar with four channels **Other Functions**: ECGP Framer **Output**: Single LAN destination

RICI	Longport	Ventnor	Margate II ADS-B	SGP	Sample XML File	Description
☑	☑	☑	☐	☐	_lan_to_1_channel_13_bit_serial	**Input**: One LAN source (Ethernet UDP/Multicast function) **Other Functions**: One ECGP Unframer Four Site Filter functions **Output**: Radar data (four different sites) over four serial ports
☑	☑	☑	☐	☐	_lan_to_1_channel_sync_serial	**Input**: Four LAN sources (Ethernet UDP/Multicast function) **Other Functions**: None **Output**: Non-Radar data (four different sites) over four serial ports
☑	☑	☑	☐	☐	_lan_to_4_channel_13_bit_serial	**Input**: Single LAN source (Ethernet UDP/Multicast function) **Other Functions**: ECGP Unframer **Output**: One Radar site sending a channel to each of the four serial ports
☑	☑	☑	☐	☐	_sync_lan_serial_bidirectional	Non-radar type data bidirectional LAN to serial/serial to LAN. **Input**: Four different LAN sources Four single channel data streams **Other Functions**: None **Output**: Four LAN destinations (same as input) Four single channel data streams (same as input)
☑	☑	☑	☐	☐	_mps-api-connections	MPS api connection interface from an external MPS host. Since configuration must come from the external MPS host, see *SUN2429 – MPSapi Application Programming Interface User's Guide* for more information.

RICI	Longport	Ventnor	Margate II ADS-B	SGP	Sample XML File	Description
☐	☐	☐	☑	☐	_CAT021	**Input**: ADS-B Antenna source **Other Functions**: None **Output**: LAN-based CAT021 messages containing ADS-B and UAT targets.
☐	☐	☐	☑	☐	_CAT033	**Input**: ADS-B Antenna source **Other Functions**: None **Output**: LAN-based CAT033 messages containing ADS-B and UAT targets.
☐	☐	☐	☑	☐	_SMS	**Input**: ADS-B Antenna source **Other Functions**: None **Output**: LAN-based SDO data which feeds to the Sunhillo Surveillance Monitor System (SMS) display.
☐	☐	☐	☐	☑	_bidirectional	**Input**: UDP LAN data in both directions, separate ports **Other Functions**: None **Output**: Raw LAN data.
☐	☐	☐	☐	☑	_multiplex_2_to_1	**Input**: UDP LAN data on two, separate ports **Other Functions**: ECGP Unframer **Output**: Single LAN data output.
☐	☐	☐	☐	☑	_split_1_in_2_out	**Input**: UDP LAN data in **Other Functions**: ECGP Unframer and Site Name/ID filter **Output**: ECGP LAN data split into UDP outputs based on Site Name.

4.3.1.2 Editing an Existing Configuration

Selecting the *Edit* option from the *Configuration* menu (**Figure 4-1**) displays a list of available user-created files to choose from for editing an existing file. Once the desired file is selected, you can modify the node types and configuration parameters of these nodes as needed. This configuration file can be saved to the existing file or saved to a different file name. All file names listed under the *Edit* option have the suffix *.xml*, which is not shown on the GUI.

Selecting the *Edit Active* option from the *Configuration* menu allows you to make changes to the active configuration of the device. You can modify the node types and configuration parameters of these nodes as needed. This configuration file can be saved to the existing file or saved to a different file name. Although the changes are made to the active configuration file, these changes will not take effect until the device is restarted.

Selecting the *Edit Live* option from the *Configuration* menu allows you to make changes to the current active configuration of the device, although you cannot change the flow or modify any options that are greyed out. When changes are made to the active configuration file with this option, they take effect immediately after the **Live Update** or **Update & Save** buttons are clicked without the need to restart the software. The **Live Update** button commits changes to the current active configuration, but does not save changes to the file, while the **Update & Save** button commits the changes to the current active configuration and saves changes to the file. To cancel changes, click the **Revert to Saved** button, which will restore the most recent saved file.

4.3.2 Managing Configuration Files

Existing user-created configuration files can be copied, renamed, or deleted. These actions are provided under the *Manage Configs* option under the *Configuration* menu (**Figure 4-1**).

Use the mouse to select a configuration file from the list. The scroll bar on the right side of the **Select A file** display will show more files that cannot be shown in the list due to the limitations of the display area size. Once a file is selected with a left mouse-click, a menu pops-up with options to *Copy*, *Delete*, *Rename*, or *Download* (**Figure 4-4**).

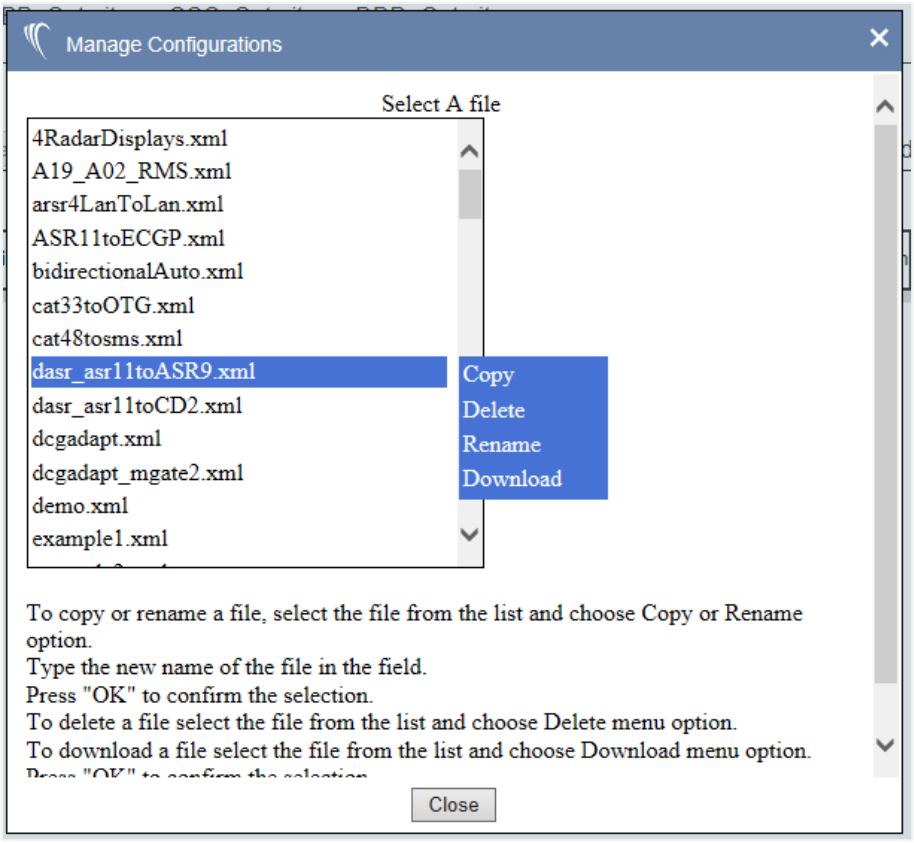


Figure 4-4: Manage Configurations Window

If *Copy* or *Rename* is selected, type the new file name in the data field after the **to**. Press the **ok** button to complete this action. If the selected file is to be deleted, select **Delete** from the options. Confirm the deletion of the selected file by pressing the **ok** button. To download a file, select *Download* and then confirm with the **ok** button. Selecting the **Close** button at the bottom of the screen closes the *Manage Configurations* window.

4.3.3 Setting Active Configuration File

To set a configuration file as the active configuration, i.e., the configuration to be run on the device, select the *SetActive* option from the *Configuration* menu (**Figure 4-1**). Locate the desired configuration file in the dropdown list. Highlight and select the desired option (**Figure 4-5**).

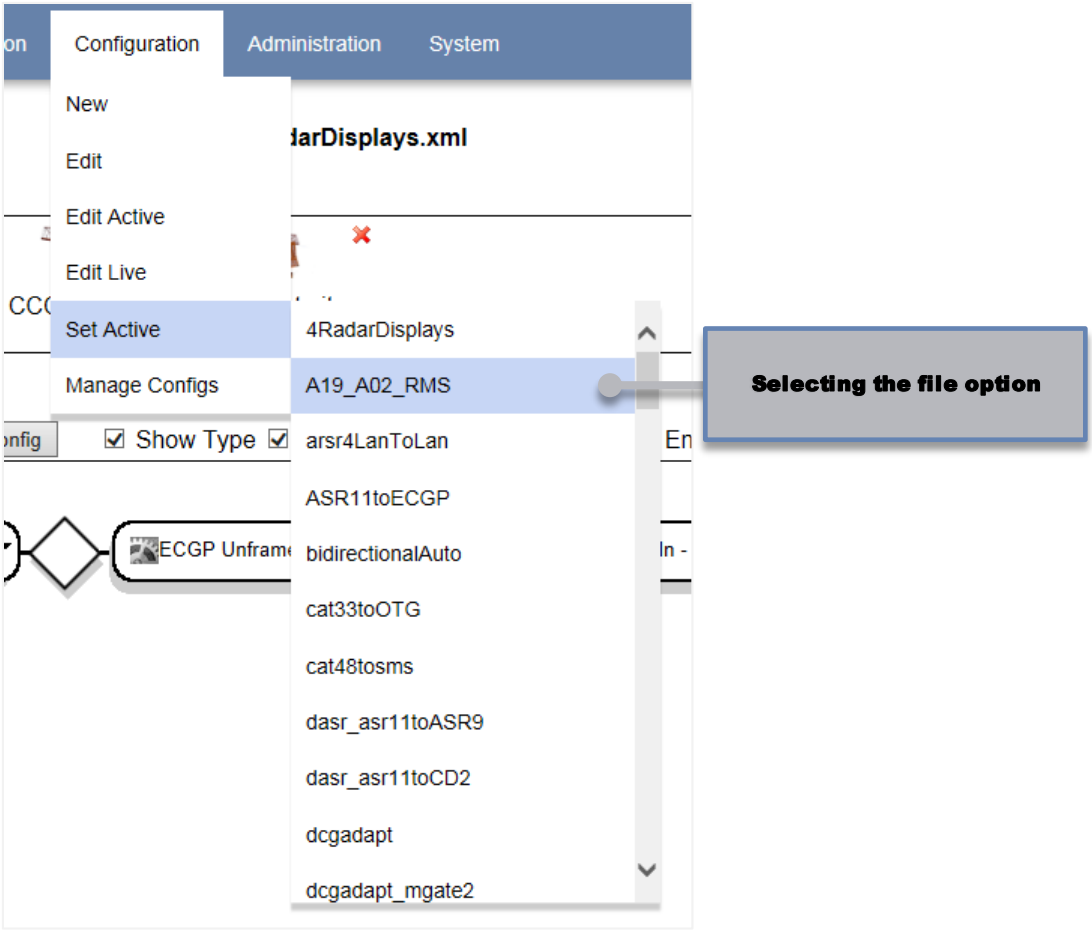


Figure 4-5: Selecting a New Configuration File, "example2"

When a new configuration file has been selected, a dialog box with the message "*filename*.xml is set as active configuration, please restart the software for it to take effect," is displayed (**Figure 4-6**).

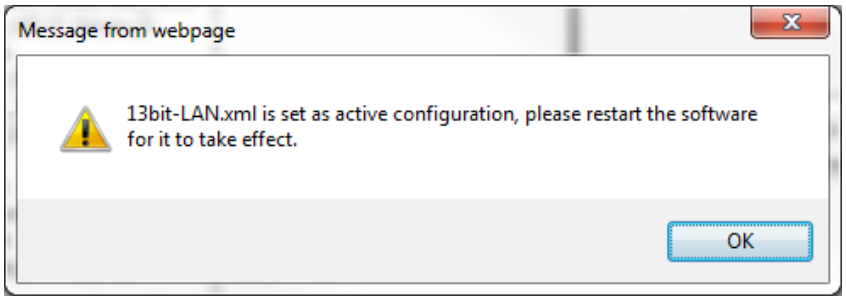


Figure 4-6: New Configuration File Selected Example

A **(pending active)** status appears in the dropdown list after the selected file to indicate this file will be the next active file after a system reboot or a software restart (**Figure 4-7**). The **(active)** status is shown in the list after the current, working system configuration.

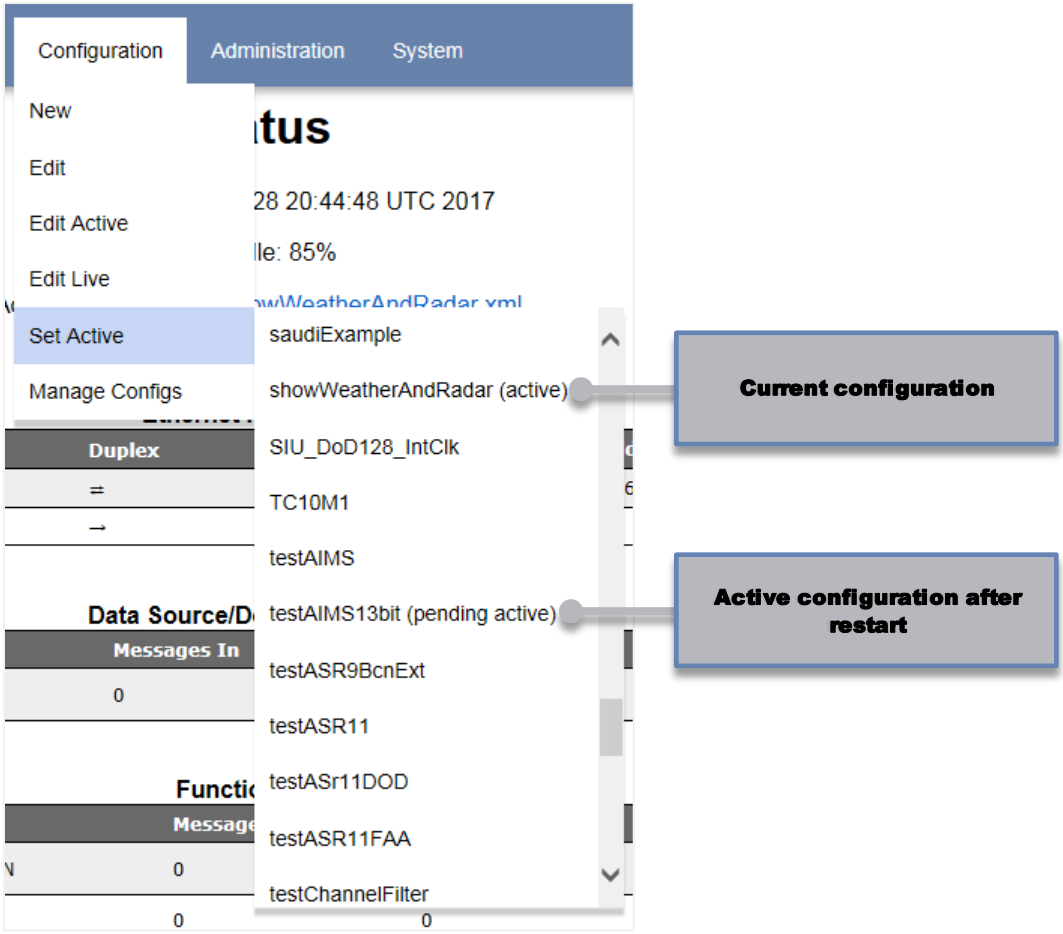


Figure 4-7: Pending Active and Active Statuses

4.4 Create/Edit a Configuration File

The subsections that follow provide details on the use of the configuration GUI to create a new, or edit an existing, configuration file. The different elements on the GUI itself and particular actions you might take when editing configuration files are also defined in this Section.

4.4.1 Configuration GUI Overview

Once a file has been selected (as described in Section **4.3.1**), the configuration screen in displayed (**Figure 4-8**).

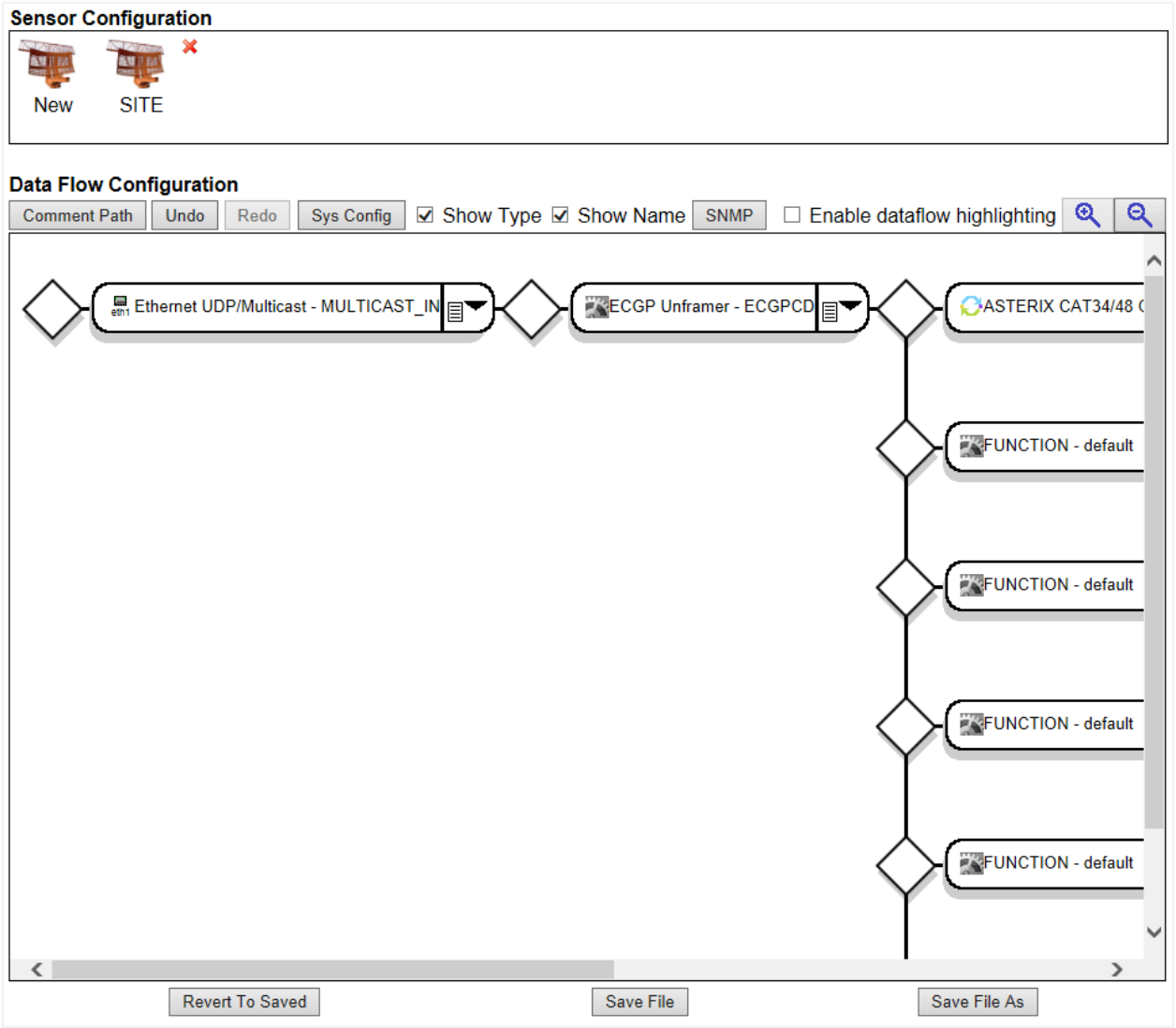
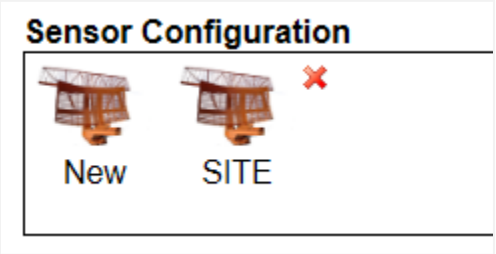


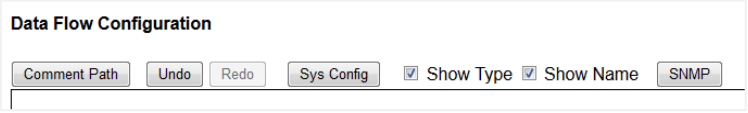
Figure 4-8: Configuration Screen

The components of the configuration screen are as follows:

- **Sensor Configuration**—The *Sensor Configuration* Section of the configuration screen displays the sensors or sites (as defined in Section **4.2.3**) for the configuration file. A sensor labeled **New** will always be displayed in the *Sensor Configuration* Section for every configuration file.

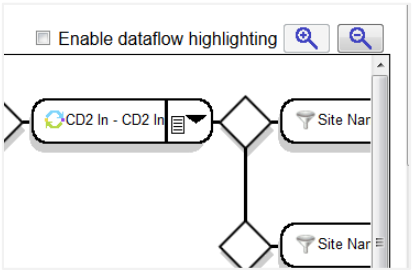


- **System Configuration Items**—The **Sys Config** button provides the configuration parameters that are used to configure unit redundancy, message throttling, and enhanced data recording. The **SNMP** button provides the configuration parameters to setup the SNMP traps sent from the RICI.

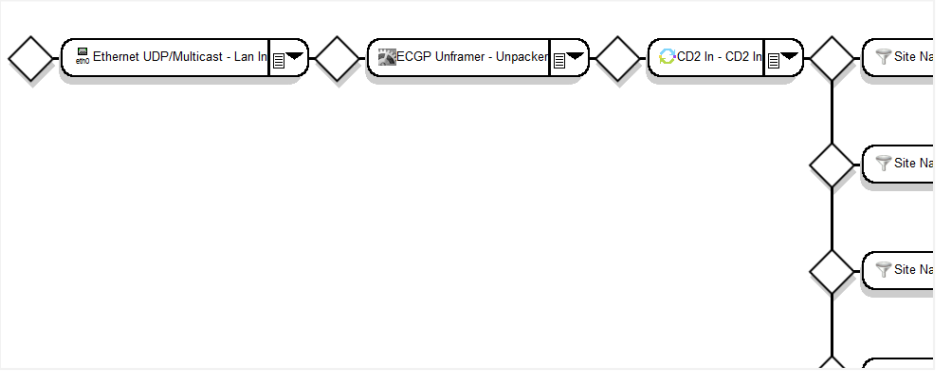


These configuration parameters are stored in the XML configuration file along with a particular data flow. A different, unique set of system configuration items can be created per configuration file. These configuration items are described in further detail in Section **4.4.2**.

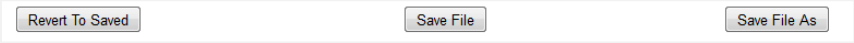
- **Data Flow GUI Controls**—The data flow UI controls provide a set of options that can be used to change/control what is displayed and how the data flow is shown on the user interface screen. The controls available are described in further detail in Section **4.4.1**.



- **Data Flow Configuration Window**—The *Data Flow Configuration* window Section of the screen is used to generate and edit the actual data flow for the configuration.



- **Save File Controls**—The save file controls, found on the bottom of the *Data Flow Configuration* screen, are used to either save the configuration to a file or get back to a last known good version of the configuration file currently open for editing. Refer to Section **4.4.2** for more information.



4.4.2 Saving Configuration Files

It is important that a configuration that is being edited or created on the GUI be saved to a configuration file. Although the changes performed on the GUI to a data flow, node type configuration parameter, system configuration item, or sensor are persistent on the screen, these changes are not automatically saved to the configuration file until you explicitly select the **Save File** or **Save File As** buttons found on the bottom of the screen.

Note

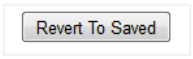
Do not press the Refresh button on the Web browser while editing a configuration file since all changes will be lost. You must save all changes to the configuration file before exiting the *Configuration* screen or selecting another menu option from the GUI menu bar (e.g., *Log Out* or *Status*). All unsaved changes to the configuration are lost when leaving the *Configuration* screen.

If there is an error with the current configuration while attempting to save a configuration file, a pop-up message is displayed stating the error and the node(s) in which the errors occur, highlighted in red. An example of an error is a node which does not have a unique Logical name, i.e., either it is the same as another node in the data flow or has not yet been defined.

4.4.2.1 Revert to Saved

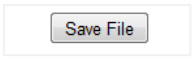
The **Revert To Saved** button restores to the GUI screen the configuration currently saved in the configuration file that is open for editing (this includes data flow and all configuration parameters).

This option is useful if several changes were made to a configuration during an edit session on the GUI, but these changes need to be backed out. Instead of trying to remove all the changes manually, **Revert To Saved** displays on the GUI a last known good or last saved configuration found in the file itself.



4.4.2.2 Save File

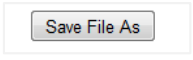
The **Save File** button saves the configuration information on the GUI to the current file open for editing. A dialog box appears to confirm or cancel overwriting the contents of the current contents of the open configuration file with the configuration data on the GUI.



This option is not available to new configuration files. If the *New* menu option is selected to use a template configuration file for creating a configuration, the changes must be saved to another file name first. Template configuration files cannot be overwritten.

4.4.2.3 Save File As

The **Save File As** button saves the configuration information on the GUI to a file of another name. Once selected, a dialog box appears where you can enter a new or existing file name in which to save the configuration. You do not need to include the *.xml* file extension; this is done automatically by the software.



4.4.3 Create/Edit Data Flow

The data flow and other configuration parameters for a configuration file are edited within the *Data Flow Configuration* window on the configuration screen. This subsection provides the details on how to use the GUI to perform specific actions in editing a data flow.

Step-by-step examples for using the Configuration GUI to create various configurations is provided in **Appendix A (RICI and Longport)** and **Appendix B (SGP)**.

4.4.4 Data Flow Graphical Elements

The data flow consists of the following elements (**Figure 4-9**):

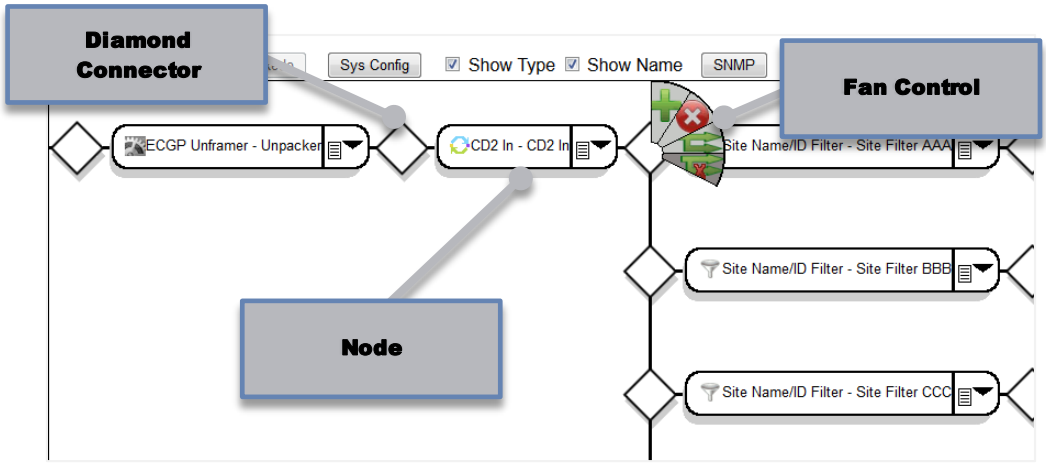
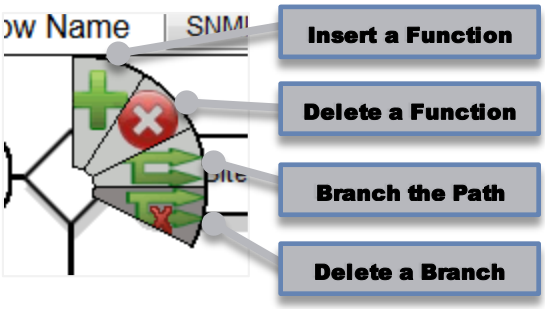


Figure 4-9: Data Flow Graphical Elements

- **Diamond Connector**—The diamond connector is used to show how and where nodes in a data flow are connected. A diamond connector shows:
  - Connection between nodes in a single data flow path
  - Where a branch from a path starts in a data flow
  - Where a branch in a data flow merges back into another path
- **Fan Control**—A mouse-over on a diamond connector brings up the fan control. A fan control is used to make a decision about what comes next in the data flow at that connector. The four possible choices are: **Insert a Function**, **Delete a Function**, **Branch the Path**, and **Delete the Branch**.



A mouse-over on each option on the control provides a short tool-tip on what each selection does.

On any given connector, the fan control only allows you to select the options that are valid for that location/connector in the data path. Valid options are shown in a light grey background and change to white when the mouse is on that option. Invalid options are shown in a dark grey background, e.g., in the previous figure, **Delete a Branch** option is not valid; the remaining three options are valid selections.

- **Node**—A data flow is a specific combination of nodes. A data flow can consist of one data path or multiple data paths that can branch and/or merge. A data path must have an input type node and an output type node. The input type node is always the first node and the output type node is always the last node in a data path (**Figure 4-10**).

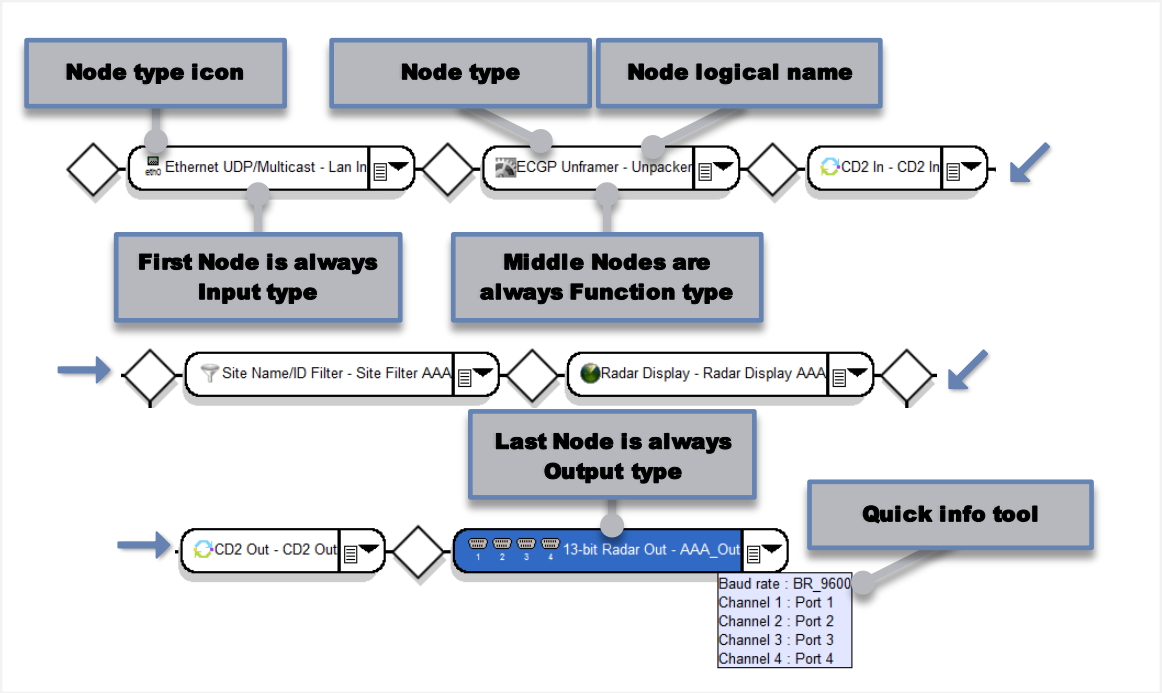


Figure 4-10: Node Details

- **Node Type Icon**—Each node type is represented graphically by an icon to give a simple visual indication of what function the node in the data flow is performing (**Table 4-4**).

Table 4-4: Node Icon Descriptions

Node Icon	Description
	Serial Port (RICI and Longport only). The port number(s) configured to the node appears below the icon.
	Ethernet port. The port number configured to the node appears below the icon.
	Utility
	Conversion
	Filter
	Graphical Display

- **Node Type**—Each node is identified with the actual node type as described in Section **4.2.2**.
- **Node Logical Name**—The node logical name is the unique, identifying name given to this particular node by the user. This name is entered in the *Logical Name* configuration parameter of every node. Every node must have a unique name.
- **Node Dropdown Menu**—This dropdown menu is where the actual node type for each node is selected.
- **Quick Info Tool Tip**—A mouse-over on each node will pop-up a tool tip that provides a quick view of a few of the configuration settings of that node. The tool-tip only provides some of the particular configuration parameters. All of the configuration parameters can be viewed by selecting the node with a mouse click.

4.4.4.1 Changing the Parameters for a Node/Sensor

A set of configuration parameters is associated with each node type and sensor. You will need to set the configuration parameters for each node and/or sensor according to your particular application in which the device is being used.

The configuration parameters for a specific node or sensor can be accessed via mouse-click. An example for the *13 Bit Radar Out* node type is shown in **Figure 4-11**.

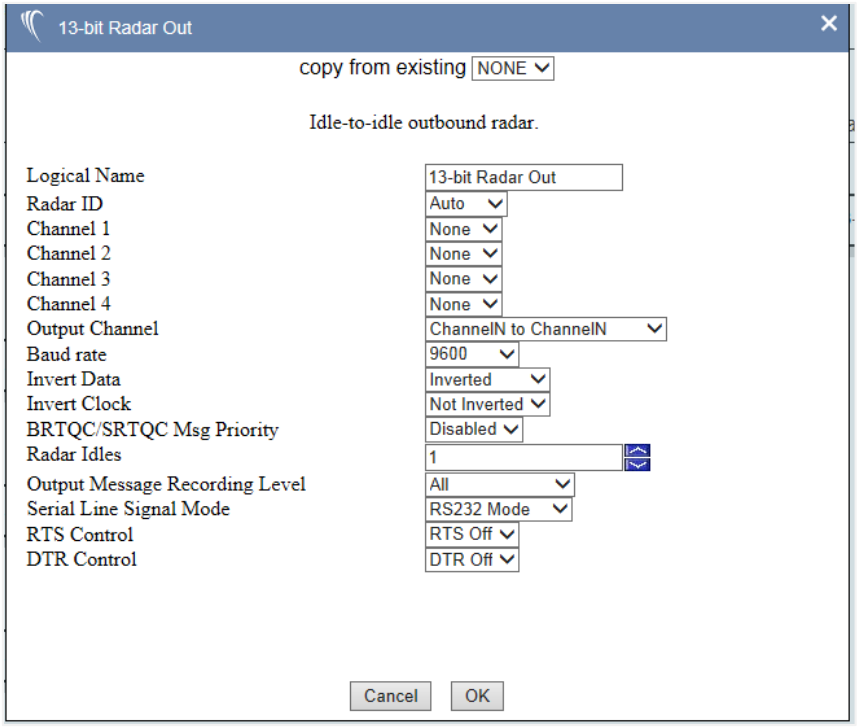


Figure 4-11: 13 Bit Radar Out Example

Additional details for a selection of node types are provided in Section **4.2.2**.

4.4.4.2 Edit Configuration Parameters User Interface Elements

The user interface provided for a given operation can contain any or all of the following elements (**Figure 4-12**):

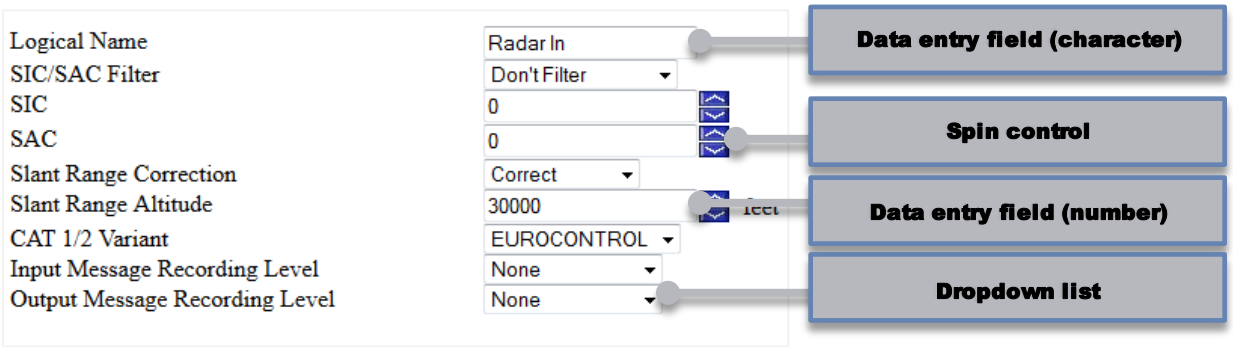


Figure 4-12: User Interface Elements Example

- **Data Entry Fields**—A data entry field is used to enter either characters or numbers for the given configuration item. The information is entered in a data entry field by placing the cursor over the existing data and overwriting its contents. The backspace or delete keys on the keyboard can be used to remove data from a data entry field.

- **Spin Controls**—A spin control provides a data entry field for a number. A spin control has an up arrow to increment that number by a pre-defined value and a down arrow to decrement that number by the same pre-defined value. The value of the increment or decrement is provided in the tool-tip for the particular configuration parameter. The user can also type over the data in the data entry field to enter a different value for that configuration parameter.

- **Dropdown Lists**—A dropdown list provides a fixed set of valid entries for the given configuration item. To choose an entry from a dropdown list, click the down arrow to the far right and move the cursor to the desired entry. Click the entry to highlight it. The highlight entry is now selected.

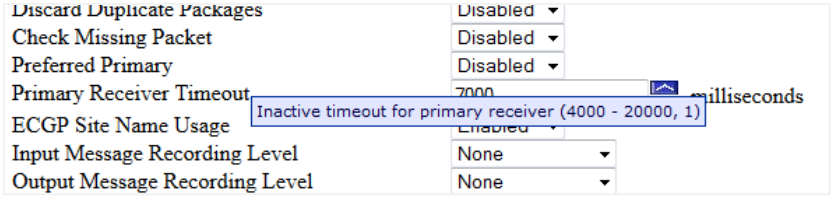
- **Checkboxes**—An additional element, which is not shown in the example in **Figure 4-12**, is a checkbox. A checkbox is used to select/deselect or enable/disable the associated element. A checkmark symbol appears for a selected/enabled item.

4.4.4.3 Common Features

Each configuration parameter screen has configuration parameters that are specific to that type of node or sensor. Common features for all configuration parameter screens are:

- **Parameter Description Tool-tip**—A mouse-over a configuration for a node type or sensor displays a pop-up tool tip. This tool-tip provides a description of the configuration parameter and, if applicable, other helpful information for how to use this parameter.

  In the case of configuration parameters that require a numerical value, the acceptable range and the increment value for its data entry field spin control are provided in parenthesis at the end of the tool-tip description. For example, the valid range for the **Primary Receiver Timeout** configuration item shown below is 4000 to 20000 and it increments by 1:



- **Copy from Existing**—The **copy from existing** dropdown list is available on each sensor or node on the top center of the parameter screen. This option is useful when creating multiple nodes of the same type with the exact or similar configuration parameter settings. Rather than enter all the values for each parameter multiple times, the **copy from existing** option provides a short-cut to setting the parameter values for a node type.

The dropdown list is populated with the (logical) names of all other nodes of the same type as the node you are editing. Selecting a name from the list automatically sets the configuration values identical to the selected node name. Choosing **NONE** from the list means you will need to set all configuration parameters as desired for the node/sensor.

- **Logical Name**—Every node in a configuration data flow must have a unique name that identifies that particular node compared to any other. As well as helping the user distinguish between nodes visually on the GUI, this name is also used internally by the software to uniquely identify this node and the data it will process.

- **Cancel/OK/Delete**—Selecting the **Cancel** button on the bottom of a configuration parameter screen closes the pop-up window without saving any changes to the parameters for that node.

  Selecting the **OK** button saves any changes to the configuration parameters and closes the pop-up window.

Note

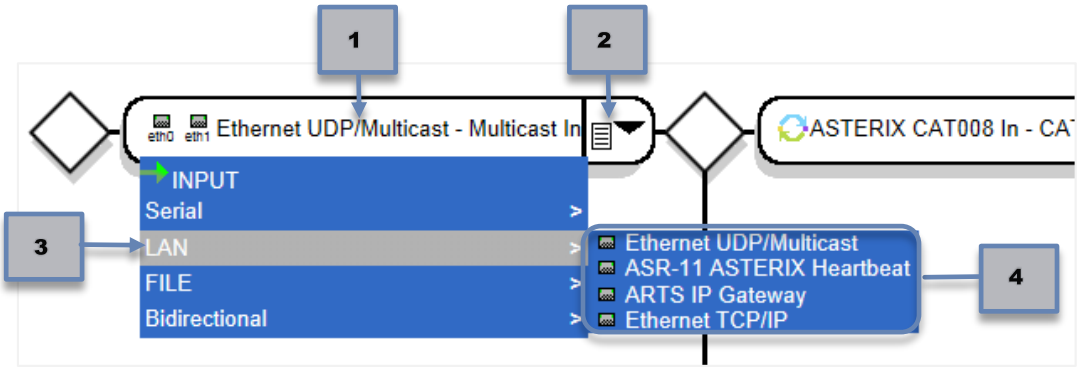
The changes are only saved to the GUI, i.e., persistent on the GUI, as long as the configuration editor is open. None of the changes are actually saved to a configuration file until the **Save** or **Save As...** buttons are used. If changes are made and you exit without saving, a pop-up warning will provide one last chance to discard (**OK**) or keep (**Cancel**) changes.

A **Delete** button is only available on the configuration parameter screen of a sensor. Selecting the **Delete** button will permanently remove the sensor from the configuration.

4.4.4.4 Change Node Type

The Node Dropdown Menu is used to select the node type for a node in a data flow. A mouse click on the dropdown menu produces a list of the available node types for the node of interest. The title on each dropdown menu of a node indicates the overall category of node: **INPUT**, **FUNCTION**, or **OUTPUT**. Based on this category, the node type selections will vary.

To change the node type on a node in a data flow, perform the following steps:



1. Locate the node within the data flow path to change.
2. Select the node's dropdown menu.
3. Move the mouse through the menu options to find the desired node type, which will be highlighted in grey.
4. Click on the desired node name. The node type and name changes on the GUI.

4.4.4.5 Cannot Select a Node Type

You may find some node types in the dropdown list are greyed-out, i.e., unavailable for selection for a particular node.

As shown in **Figure 4-13**, several of the possible selections from the node types are greyed out to indicate they cannot be chosen at this point in the data flow. These node types are unavailable because they require other node types to be present in the data flow to allow for their use.

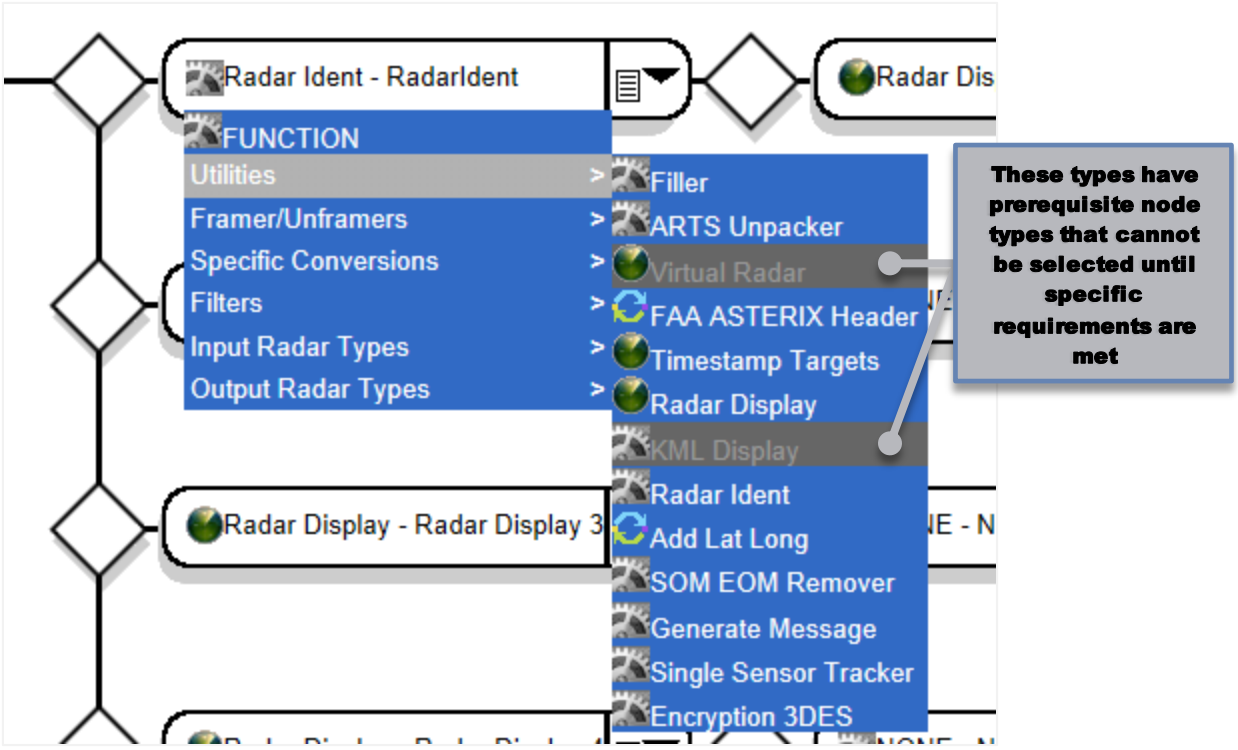


Figure 4-13: Required Node Type Example

A mouse-over on any greyed out selection displays a tool tip with information stating: **This node type requires a prerequisite node type earlier in the data flow. Double-click for more details** (**Figure 4-14**).

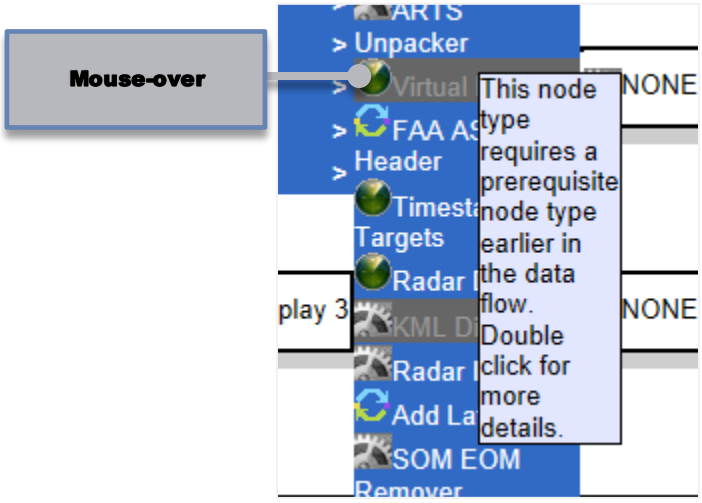


Figure 4-14: Greyed Out Node Type Tool Tip

A double-click on a greyed out node type displays more information regarding what is required in the data flow in order to configure the selected node type (**Figure 4-15**).

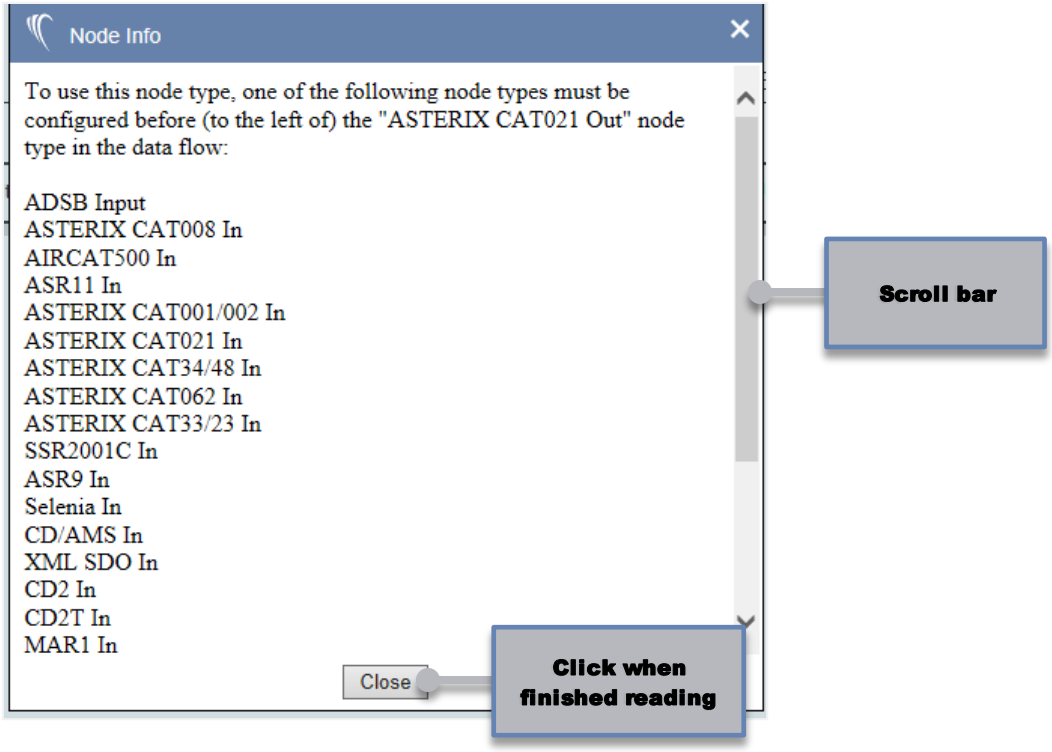


Figure 4-15: Node Info Window Example

The unique node types that cannot be configured a second time are similarly greyed-out from the node type selection list. A mouse-over on a greyed-out node type produces a tool-tip stating: **This node type conflicts with a node type earlier in the data flow. Double click for more details.** A double mouse-click on a node type displays a dialog box with further details and lists all the node types that cannot be configured in the data flow more than one time.

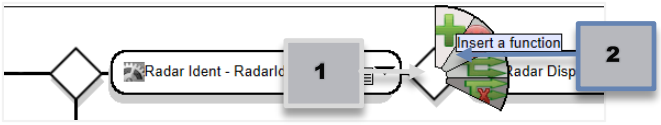
4.4.4.6 Adding a Function Node

The **Insert a function** option on the Fan Control adds a new function type node into the data flow after the diamond connector. A default, generic function type node is inserted, and this element can be configured to the desired node type.

Inserting a node is valid only on the diamond connectors after an input type node. The **Insert a function** selection is unavailable and greyed out before an input node and on the last diamond connecter of a merged data path.

To add a new node into a data path, perform the following steps:

1. Move the mouse to the diamond connector where the node should be inserted.



2. Select the **Insert a function** option from the Fan Control.
3. The node is inserted to the right of that connector.

4. The added node is a default, generic Function type node and must be configured to a specific type of node. Use the *Node Dropdown Menu* to select the required node type from the menu lists.
5. Configure the function parameters as per Section **4.4.3**.

4.4.4.7 Deleting a Function Node

The **Delete a function** option on the fan control removes an existing node from the data flow (**Figure 4-16**). The function attached to the right of the selected diamond connector is deleted.

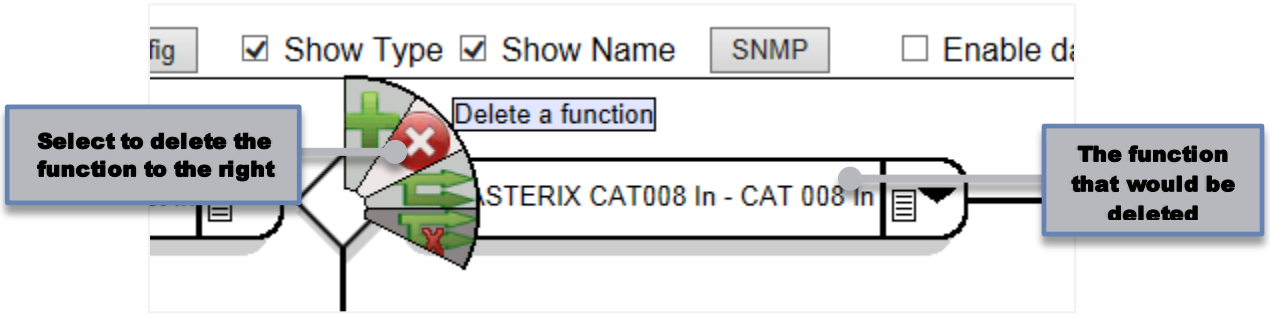


Figure 4-16: Delete a Function Option

The **Delete a function** option is not valid (greyed-out) on the first diamond connector in a data path (**Figure 4-17**), as well as the last diamond connector in the data path. As such, you cannot delete an INPUT type node or an OUTPUT type node from a data flow path.

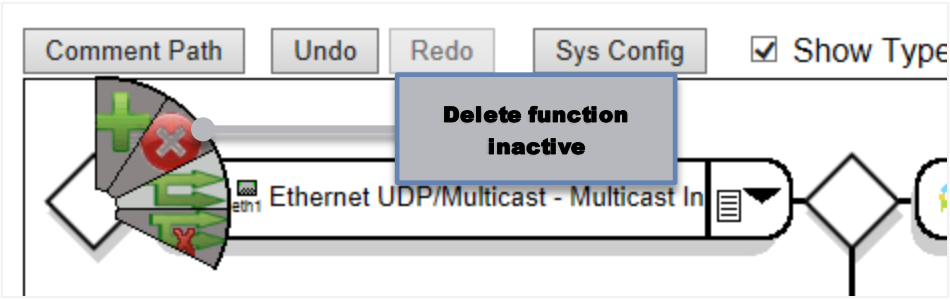


Figure 4-17: Inactive Delete a Function Option

4.4.4.8 Branching a Data Path

The **Branch the path** option (**Figure 4-18**) on the fan control creates a default, generic data path branching from the diamond connector where the selection was made.

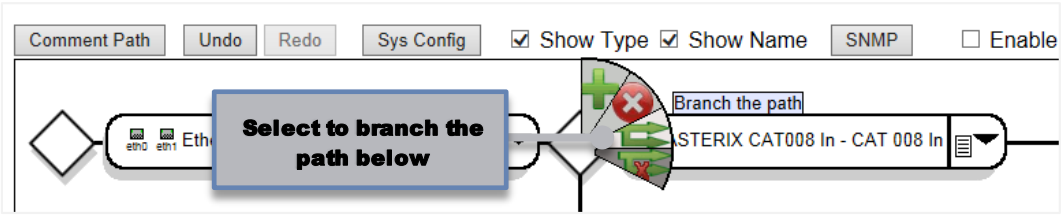


Figure 4-18: Branch the Path Option

This default, generic data path mimics the path above from which it was branched in the number of nodes, but the node types themselves are not copied. The automatically generated data path must be configured with the desired node types and further output or merging options. A path branch is valid on all diamond connections in a data path.

4.4.4.9 Deleting a Branch

The **Delete the branch** fan control option (**Figure 4-19**) removes the entire data path that branches from the chosen diamond connector.

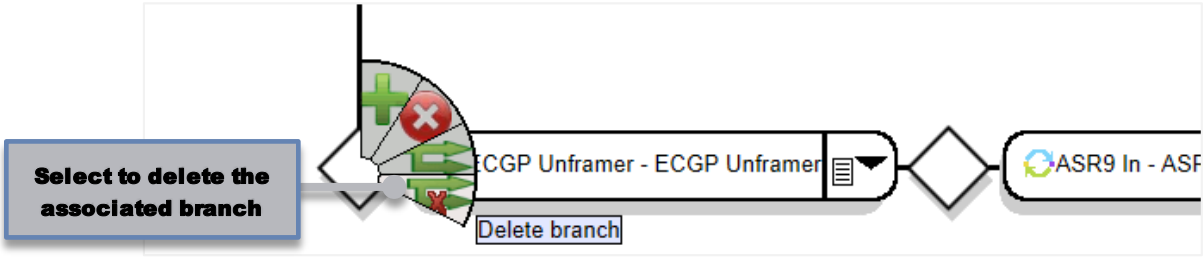


Figure 4-19: Delete the Branch Option

This selection is only valid for a diamond connector that has a data path branch associated with it. If there is no branch from a connector, there is nothing to delete.

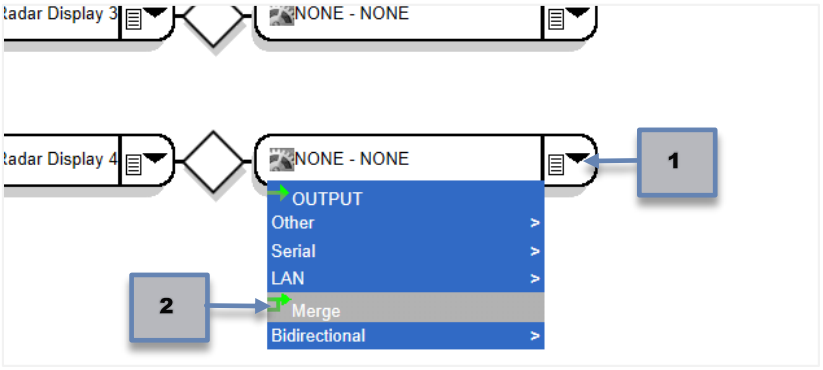
4.4.4.10 Merging Data Paths

Merging a data path into another path is done using the node dropdown menu. The **Merge** option is available only on an OUTPUT type node, which is always the last node in a data path.

A data path can only be merged into a data path above it in the *Data Flow Configuration* window. The merge into the data path can occur at any of the diamond connectors, except the first one in the path.

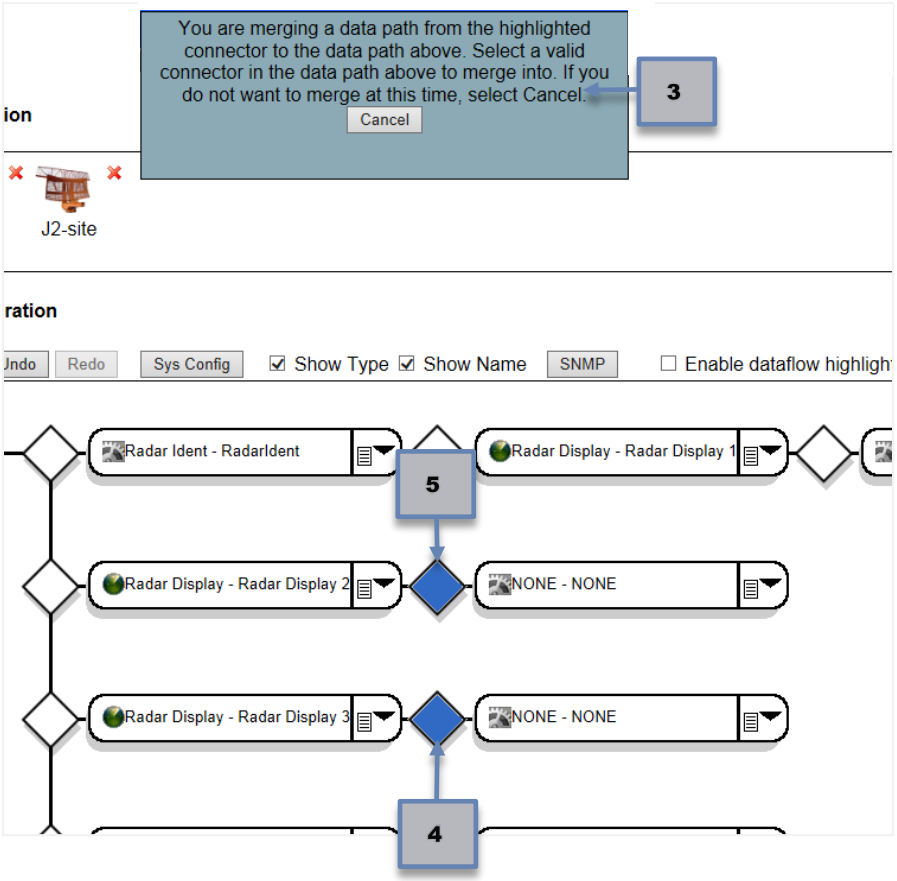
To merge a data path into another path, perform the following steps:

1. On the merging data path, select the node dropdown list on the OUTPUT node.



2. Select **Merge**.

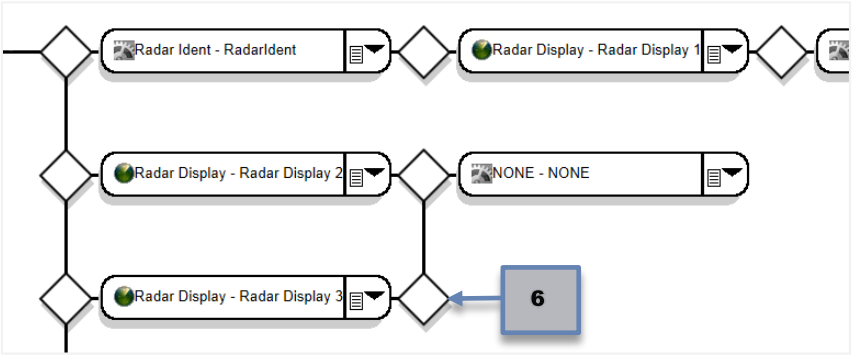
3. A pop-up with instructions, as well an option to **Cancel** the merge, appears.



4. The diamond connector from the merge from location is highlighted in blue.

5. Click on the desired location (diamond connector) for the from data path to be merged into. The merge to location changes to blue.

6. The OUTPUT node of the merge data path disappears from the GUI and a connection from the lower data path to the upper is displayed.



If necessary, a merge can be undone by using the **Undo** button (refer to Section **4.4.6.2** for details).

4.4.4.11 Deleting Data Path Merges

A merge into a data path can be deleted using the fan control. The **Unmerge** is initiated from the data path that merged into the other path. Visually on the GUI, this is a lower data path than where the merge ends. A mouse-over on the diamond connector where the merge starts displays a fan control with an **Unmerge** option (**Figure 4-20**).

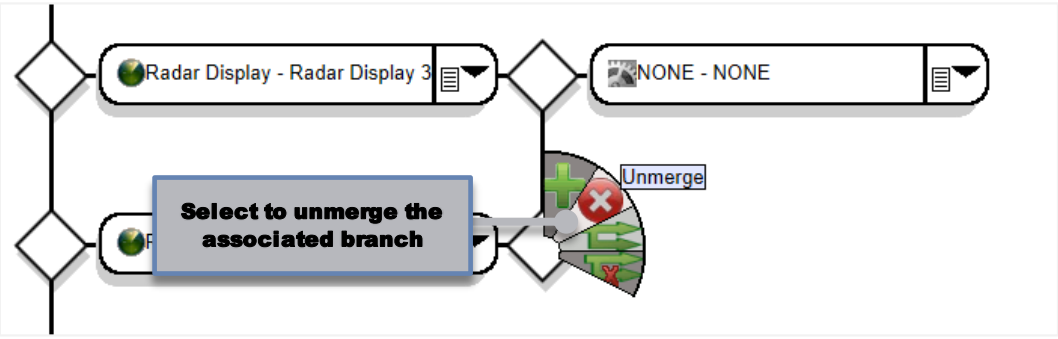


Figure 4-20: Unmerge Option

Selecting the **Unmerge** option from the fan control removes the visual connection between the lower data path and the diamond connector in the other data path. An OUTPUT type node with default configuration information is available for this data path (**Figure 4-21**). The OUTPUT node must be configured to a valid output node type.

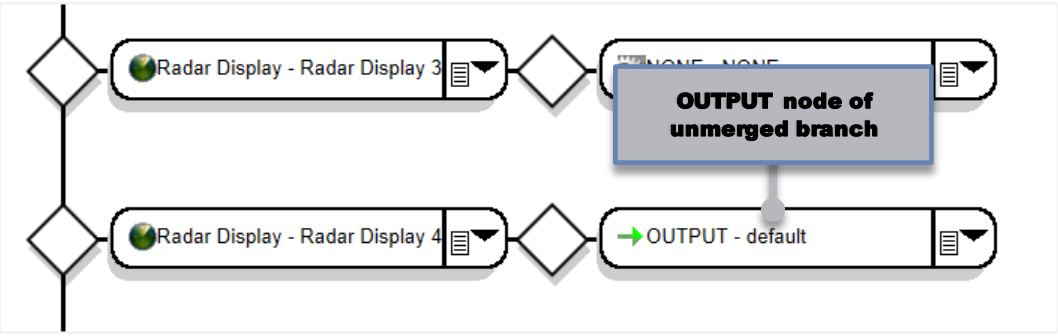


Figure 4-21: An Unmerged Branch

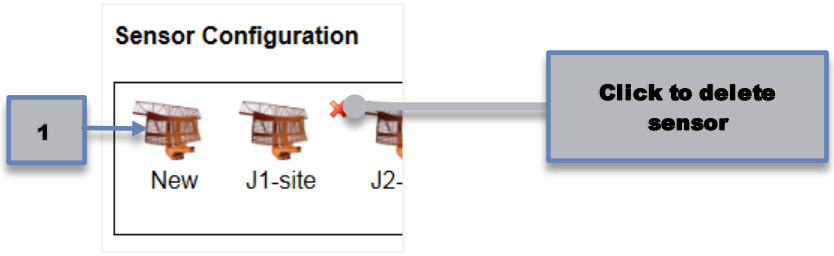
4.4.5 Sensor Configuration

If a sensor/site is necessary for the configuration, i.e., a node type that depends on site information to function properly, a sensor can be created via one of the following ways:

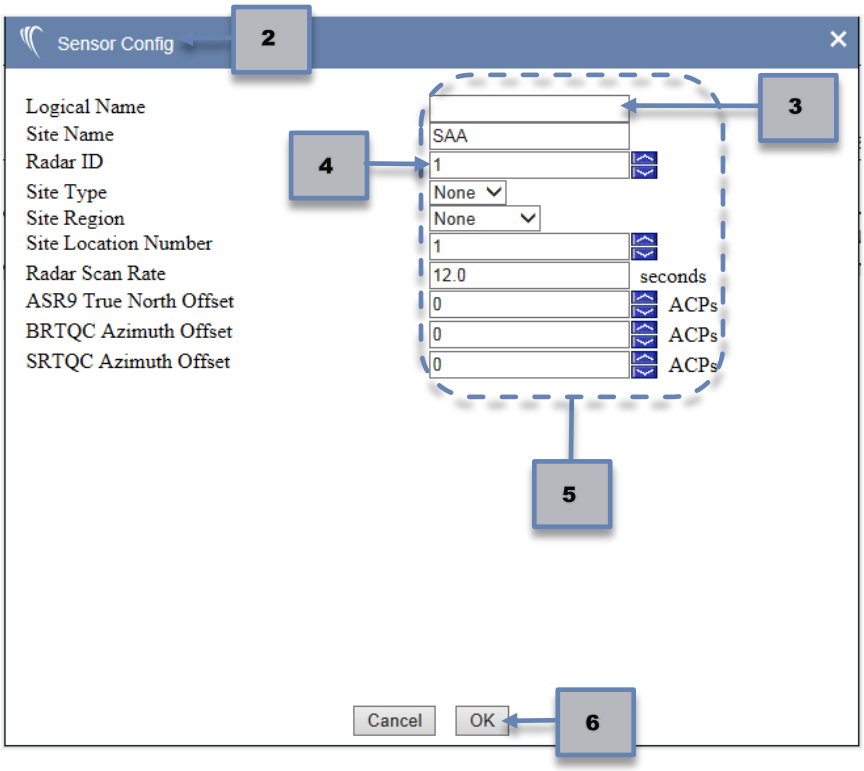
- Selecting the **New** sensor on the display and manually configuring the sensor parameters.
- The GUI will automatically create a sensor for you when a Serial Output node type is used and the file is saved.

To create a new sensor, perform the following steps:

1. Click on the sensor labeled **New** in the Sensor Configuration Section.



2. The *Sensor Config* screen is displayed.



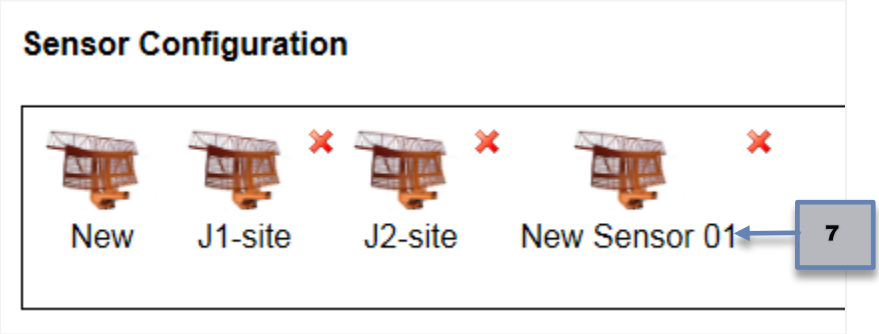
3. Enter a unique,meaningful name of at least one character to distinguish this sensor from other sensors in the **Logical Name** data field.

4. Choose a unique identification number in the **Radar ID** parameter.

5. Change other configuration parameters as desired for the sensor.

6. Click **OK** to confirm changes.

7. The new sensor with the name provided in step 2 appears in the *Sensor Configuration* Section.



A sensor in the *Sensor Configuration* Section can be associated with a particular serial input or function node by selecting the name of the sensor from the **Radar ID** dropdown list in the input or function node configuration.

4.4.6 Data Flow UI Controls

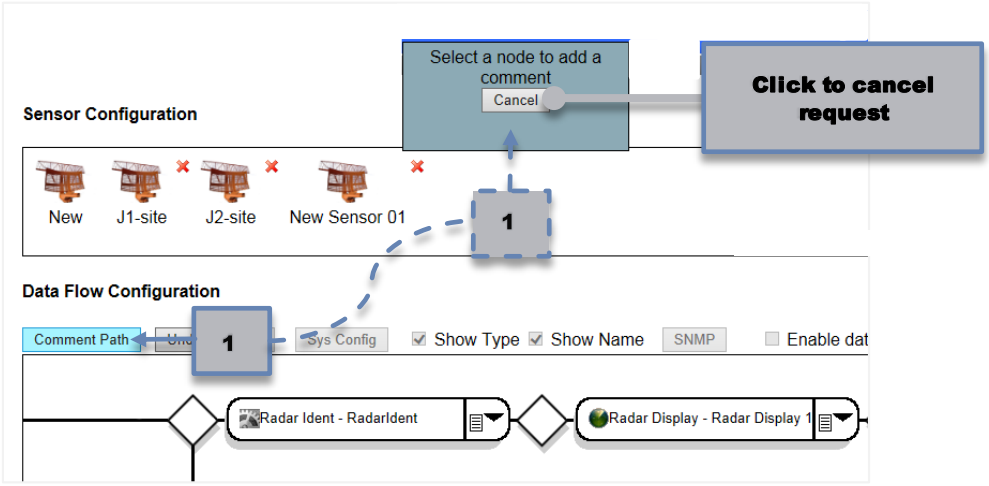
The data flow UI controls provide a set of options that can be used to change/control what is displayed and how the data flow is shown on the user interface screen.

4.4.6.1 Comment Path Button

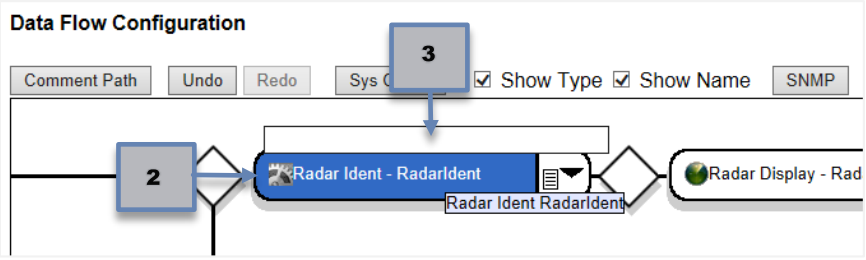
The **Comment Path** button allows you to annotate a node of your choice within a data path. The annotations are displayed above the node.

To enter an annotation, do the following:

1. Click on the **Comment Path** button. A pop-up message stating, **Select a node to add a comment**, appears.



2. Click the desired node.



3. Type in the desired comment. Press **Enter** when finished.

To edit an existing comment on a data path, repeat the steps above, or double-click on the comment. The comment can be deleted by double-clicking on the comment, deleting the text, and pressing **Enter**.

4.4.6.2 Undo and Redo Buttons

The **Undo** and **Redo** buttons (**Figure 4-22**) allow the user to undo an action or revert the undo, respectively. These buttons toggle between each other.

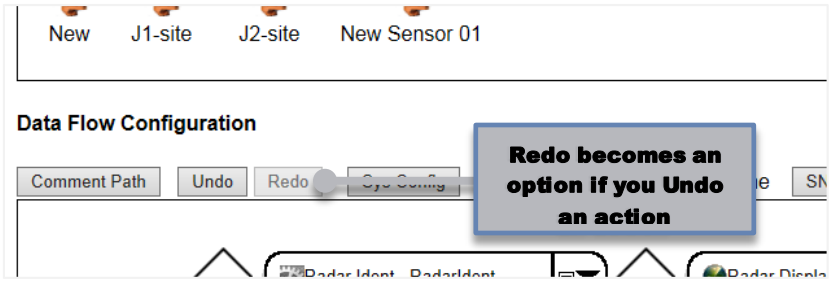


Figure 4-22: Undo and Redo Buttons on Data Flow Configuration

If an action was undone, the **Redo** button is available, while the **Undo** button is greyed-out. If an action was re-applied, the **Redo** button is greyed-out, while the **Undo** button is available.

Example: A function node is deleted from a data path by mistake. The Undo button is available for selection and pressing this option causes the node to appear in the data flow again.

An undo is five actions deep, meaning you can press the **Undo** button up to five times to undo or back-out the last five changes to the data flow.

The following actions can be undone with **Undo**:

- Deleting a node from a data path
- Adding a node to a data path
- Branching a data path

- Deleting a branch
- A data path merge
- Unmerging a data path

Note

Modifying the configuration parameters of a node in the data flow deletes all previous actions possible for an undo on a data flow. You cannot undo a previous action if the configuration parameters have been edited.

4.4.6.3 Show Type Checkbox

The **Show Type** checkbox is used to display (checked) or not display (unchecked) the node type in each node on the GUI. This option is applied to all nodes in the data flow. By default, the **Show Type** control is checked (**Figure 4-23**).

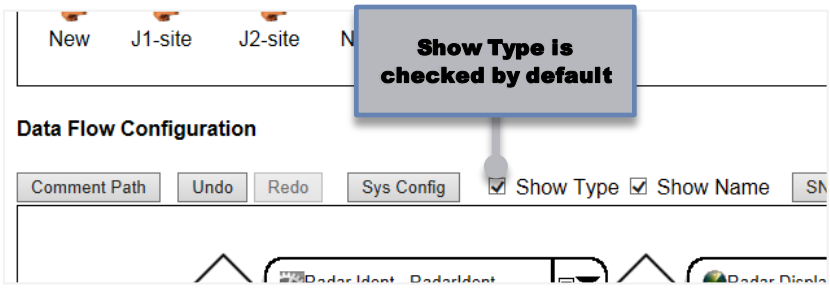


Figure 4-23: Show Type Checkbox on Data Flow Configuration

This option can be used to shorten the length of data flow paths when viewing longer data flows to avoid having to scroll right or left to view the entire path in the data flow window.

4.4.6.4 Show Name Checkbox

The **Show Name** checkbox is used to display (checked) or not display (unchecked) the node name, which is the logical name provided by the user to identify that particular node in each node on the GUI. This option is applied to all nodes in the data flow. By default, the **Show Name** control is checked (**Figure 4-24**).

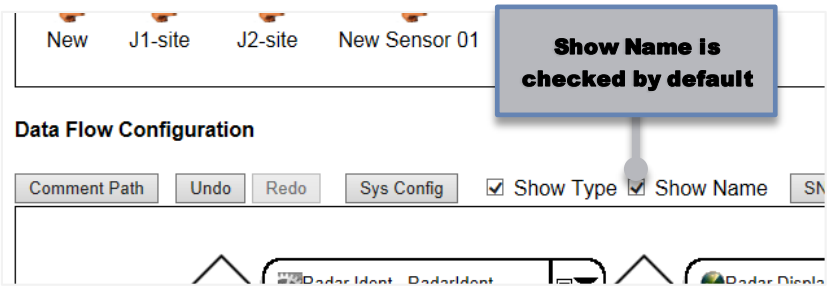


Figure 4-24: Show Name Checkbox on Data Flow Configuration

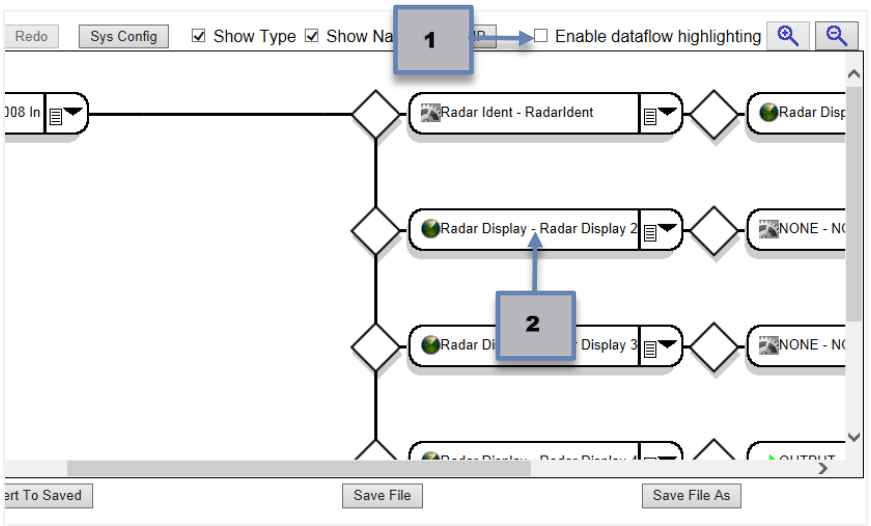
This option can be used to shorten the length of data flow paths when viewing longer data flows to avoid having to scroll right or left to view the entire path in the data flow window.

4.4.6.5 Enable Data Flow Highlighting Checkbox

For a long, complicated data flow with multiple inputs with branching and/or merging, it can be difficult to follow the flow of data from one node to another when viewing it all on the GUI. The **Enable Data Flow Highlighting** control can aid in visualizing how data moves through a path by displaying a cyan color highlight starting at a selected node until the output node for the data. By default, the **Enable Data Flow Highlighting** control is unchecked.

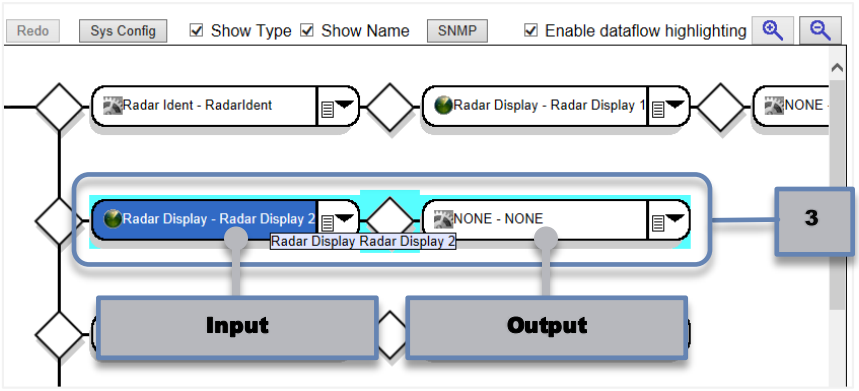
To enable the highlighting, do the following:

1. Click the checkbox control.



2. Move the mouse pointer onto a node in the data flow path.

3. The cyan colored highlight appears from that node to the corresponding output node.



4.4.6.6 Zoom In and Zoom Out Buttons

The *Data Flow Configuration* window is a fixed display size on the GUI. Longer data paths with multiple nodes may not be visible in the provided window and scrolling left-right or up-down may be necessary to view the entire data flow. The **Zoom In** and **Zoom Out** controls (**Figure 4-25**) enlarge or shrink the visuals in the *Data Flow Configuration* window to enhance visibility.

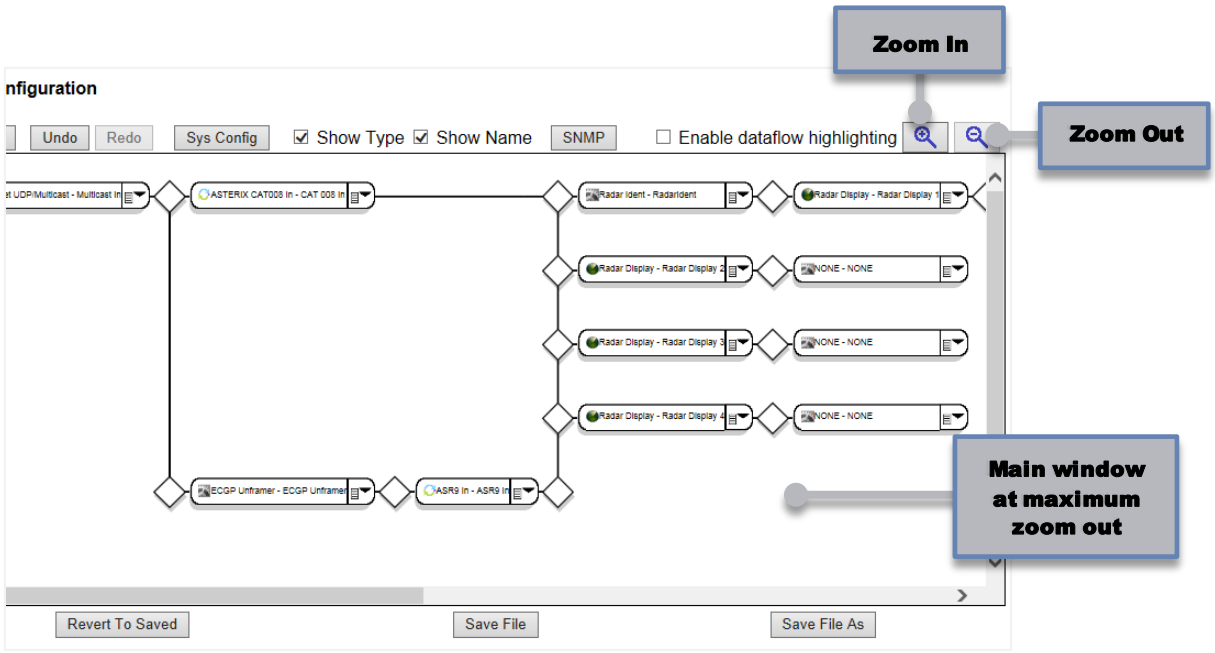


Figure 4-25: Zoom In and Zoom Out Buttons

4.4.7 Edit System Configuration Items

The **Sys Config** and **SNMP** buttons (**Figure 4-26**) provide the configuration parameters that can be used to configure a wide range of options, including the following:

- Unit redundancy
- Message throttling
- Enhanced data recording
- SNMP traps

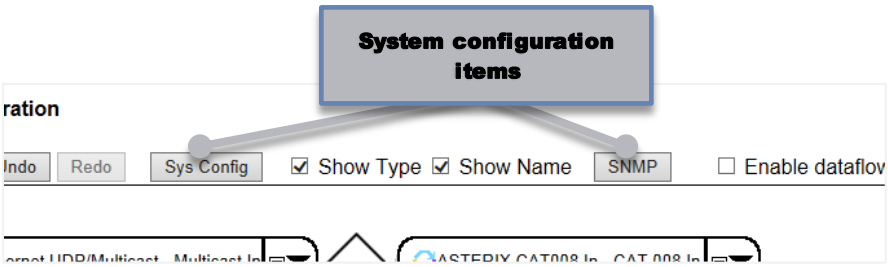


Figure 4-26: Sys Config and SNMP Buttons

These configuration parameters are stored in the XML configuration file alongside the data flow. A different, unique set of system configuration items can be created per configuration file.

The subsection that follows describes the configuration items provided under the **Sys Config** and **SNMP** buttons on the *Configuration Screen*.

4.4.7.1 Unit Redundancy

Unit redundancy is configured by selecting the **Sys Config** button on the configuration GUI when editing or creating a configuration file. Refer to Section **7.1** for additional information.

4.4.7.2 Message Throttling

The message throttling feature is configured by selecting the **Sys Config** button on the configuration GUI when editing or creating a configuration file. By default, message throttling is disabled. To enable this feature, set the *Message Throttling* parameter to **Enabled**.

The configuration parameters for message throttling and queue monitoring include *Message Throttling*, *Message Throttling Site ID*, *Message Throttling Trap Report Interval*, *TIS Threshold*, *Preoverload Threshold*, *Overload Threshold*, *Return to Normal Threshold*, and *Return to Preoverload Threshold*.

Message throttling involves monitoring a fixed size First In First Out (FIFO) queue and dropping incoming messages based on 1) priority and 2) queue depth overload conditions. Additionally, messages will be dropped based on their configured time in storage (TIS) value.

Messages are designated as having one of four priorities, with Priority 1 being the highest. The messages, based on priority are:

- *Priority 1* – Beacon Real Time Quality Control (BRTQC), Search Real Time Quality Control (SRTQC), Status, Strobe, Beacon Emergency.

- *Priority 2* – Non-emergency Beacon.
- *Priority 3* – Search.
- *Priority 4* – All other messages (including Weather).

Priority 1 and *Priority 2* messages are never dropped, and *Priority 1* messages are transmitted ahead of *Priority 2* messages. *Priority 3* messages will be throttled if, and only if, throttling the lowest priority messages (*Priority 4*) does not return the message throttling queue to its pre-overload condition.

The overload (including pre-overload) configuration parameters control both the application software and the SNMP traps that are generated when the overload condition changes. For a description of the SNMP traps related to message throttling, please refer to Section **4.4.7.4**.

The *Preoverload Threshold* parameter indicates the queue depth full percentage at which Priority 4 message throttling commences. An SNMP trap notification is sent in order to notify the user that this condition has been met. Throttling of *Priority 3* messages will commence upon reaching the Overload Threshold (and an SNMP trap notification is sent).

The *Return to Preoverload Threshold* parameter indicates the queue depth full percentage at which the cessation of *Priority 3* message throttling occurs. An SNMP trap notification is sent upon reaching this threshold. The *Return to Normal Threshold* parameter indicates the queue depth full percentage at which message throttling of *Priority 4* messages will cease. An SNMP trap notification is sent upon reaching this threshold.

4.4.7.3 Data Recording

The data recording capability of the device supports Peripheral System Analysis and Recording (PSAR), raw (binary), and packet capture (PCAP) data recording formats.

The recording format is set with the *Data Recording File Type* parameter, and may be any of the following:

- *Raw* – Creates a *.dat* binary recording file.
- *PSAR Flat* – Creates a non-circular (flat) *.psar* recording file.
- *PSAR Circular* – Creates a single, circular *.psar* recording file.
- *PCAP (Wireshark/TCPDump)* – Creates a *.pcap* recording file.

All files, regardless of format, are created with the filename *sunlogDDMMYYYY-HHMMSS*, where *DDMMYYY-HHMMSS* is replaced by the day/month/year-hour/minute/second of the recording (in 24 hour format). This filename can be prefixed with customizable text by setting the *Data Recording File Prefix* parameter.

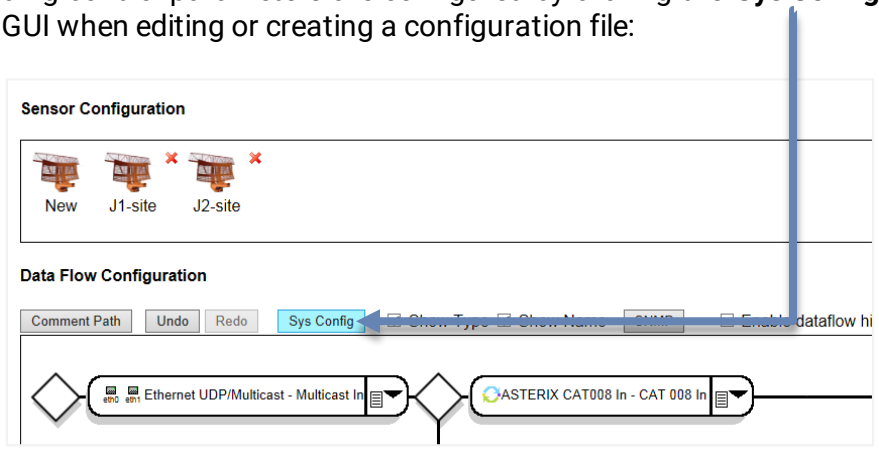
By default, the maximum recording file size is 2 MB. For all file types except the circular PSAR file, the file will be closed upon reaching its maximum file size, and a new recording file will be created.

On devices with an OS version of 3.x.x or higher, the file size and the ability to automatically upload the data log file to a separate server location are also configurable. The maximum log file size is modified by changing the *Data Recording File Size* parameter. The server upload settings are configured through the *Data Recording Upload* series of parameters. Currently, the only upload mechanism supported is File Transfer Protocol (FTP). With this feature enabled, all recorded data files will be included in the logs and sent to the FTP server when the system software is restarted or when the maximum file size is reached, except for the circular PSAR files, which are only uploaded when the system software is restarted.

Note

The current OS version can be found on the **About** page (refer to Section **2.4**).

The data recoding control parameters are configured by clicking the **Sys Config** button on the configuration GUI when editing or creating a configuration file:



The data recording options are described in **Table 4-5**.

Table 4-5: Data Recording Control Parameters

Configuration Parameter	Description
Data Recording File Prefix	The file name prefix.
Data Recording File Size	The file size. Values are between 2000 – 10,000,1.
Data Recording File Type	File type options are: • Raw • PSAR Flat • PSAR Circular • PCAP (Wireshark/TCPDump)
Data Recording Upload Type	Options are FTP or SFTP.
Data Recording Upload User Name	The upload user name.
Data Recording Upload Password	The upload password.
Data Recording Upload Server	Address of the server to upload recordings to (format: #.#.#.#).
Data Recording Upload Location	The upload path.
Data Recording Upload2 Type	The secondary upload user name.

Configuration Parameter	Description
Data Recording Upload2 User Name	The secondary upload password.
Data Recording Upload2 Server	Address of the secondary server to upload recordings to (format: #.#.#.#).
Data Recording Upload2 Location	The secondary upload path.

4.4.7.4 TCP/IP Retries

There are two entries for TCP/IP Retries: *TCP/IP Retries 1* and *TCP/IP Retries 2*. *TCP/IP Retries 1* is the number of times TCP will attempt to retransmit a packet normally, with a Linux default of 3, and range of 1 – 100 in increments of 1. *TCP/IP Retries 2* is the maximum number of times a TCP packet is retransmitted before giving up, with a Linux default of 3, and range of 1 – 100 in increments of 1.

4.4.7.5 SNMP

The SNMP management station IP addresses and system traps are configured by selecting the **SNMP** button on the configuration file editing screen. For a discussion about the SNMP features and Management Information Base (MIB) contents, refer to Section **10**.

Up to seven different SNMP management stations can be configured by entering a valid IP address in dot notation in the *SNMP Mgt Station IP Address* data entry fields. You can also enable or disable the SNMP traps generated by the system.

Section 5

5. USER AND RSA KEY ADMINISTRATION

In this Section, you gain a deeper understanding of SureLine Core user accounts and RSA keys, and their management.

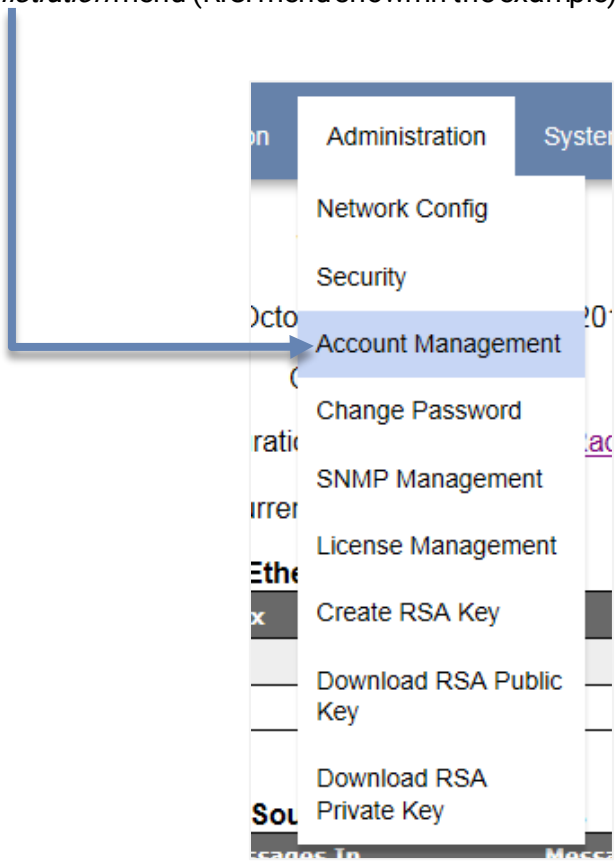
User accounts, user account administration, related user account security concerns and login issues, and RSA key administration are described in this Section.

Note

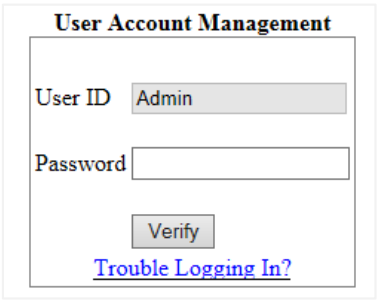
Account Management options in the SureLine Core GUI menu are specific to the GUI. In other words, user accounts created or modified in the SureLine Core STUI do not apply to the GUI, and vice-versa.

5.1 User Account Management

To add or delete users who have access to the device, reset a user's password or password expiration (timeout), or set the minimum required password length, select **Account Management** from the *Administration* menu (RICI menu shown in the example). Only an **Admin** user has access to this function.



Once **Account Management** is selected, the login window is displayed:



Once the **Admin** user enters their password and presses the **Verify** button, the **User Account Management** screen is displayed (**Figure 5-1**).

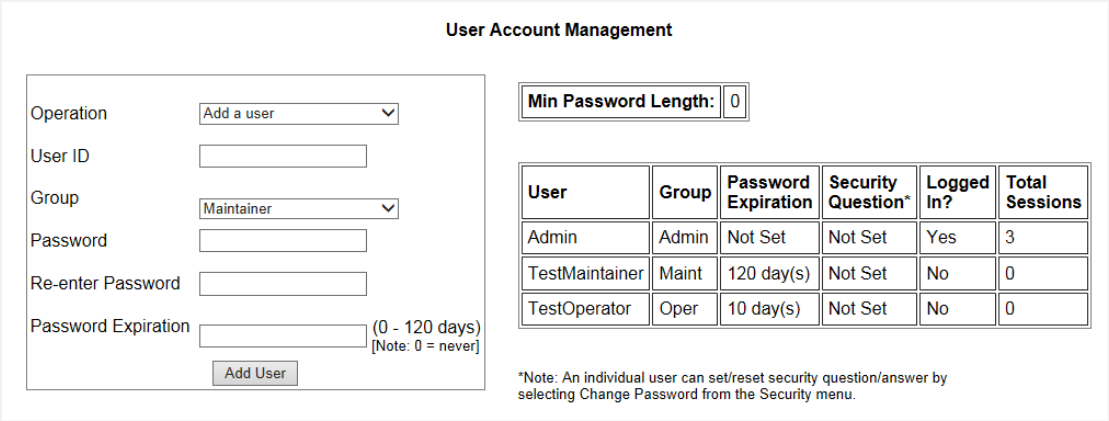


Figure 5-1: User Account Management Screen Example

The **User Account Management** screen displays current system users, user groups (user role permissions), password expiration status, login status, and the total number of associated login sessions on the right side of the screen. User account management functionality is provided by the options located on the left side of the screen.

5.1.1 User Role Permissions

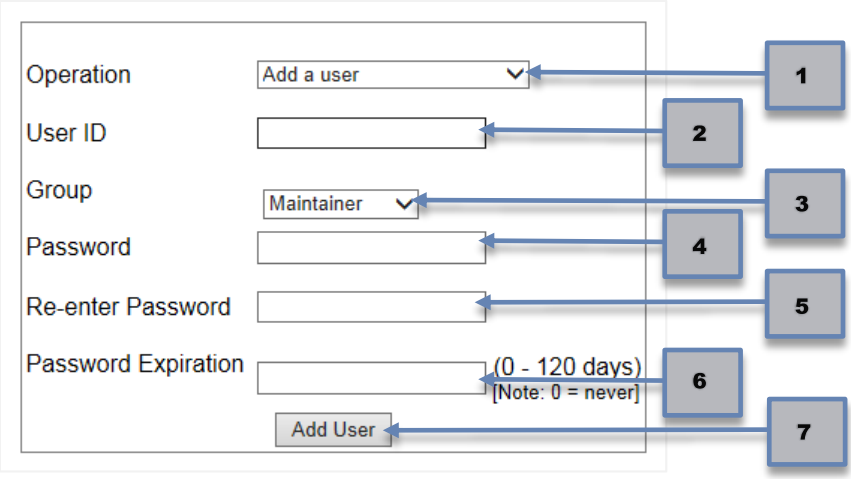
Role permissions define what GUI items are accessible for any given login. **Table 5-1** provides a summary of the user role permissions associated with each user type.

Table 5-1: User Role Permissions

User Permission Group	Administrator (Admin)	Maintainer	Operator
Information Menu	Yes	Yes	Yes
Status	Yes	Yes	Yes
Logs	Yes	Yes	Yes
Download Logs	Yes	Yes	No
Download MIB	Yes	Yes	Yes
Radar Display	Yes	Yes	Yes
Real-Time Data Display	Yes	Yes	Yes
Configuration Menu	Yes	Yes	Yes
New	Yes	No	No
Edit	Yes	No	No
Edit Active	Yes	No	No
Edit Live	Yes	No	No
Set Active	Yes	Yes	No
Manage Configs	Yes	No	No
Administration	Yes	Yes	Yes
Network Config	Yes	Yes	No
Security	Yes	No	No
Account Management	Yes	No	No
Change Password	Yes	Yes	Yes
SNMP Management	Yes	No	No
License Management	Yes	Yes	No
Create RSA Key	Yes	No	No
Download RSA Public Key	Yes	No	No
Download RSA Private Key	Yes	No	No
Manage ADSB (Longport and Margate II ADS-B only)	Yes	Yes	No
System Menu	Yes	Yes	Yes
Go Standby/Go Active	Yes	Yes	No
Reboot	Yes	Yes	No
Restart Software	Yes	Yes	No
Shutdown (SGP only)	Yes	Yes	No
Upload Data	Yes	Yes	No
Flash OS (Does not apply to SGP)	Yes	No	No
About	Yes	Yes	Yes
Log In	Yes	Yes	Yes

5.1.2 Add a User

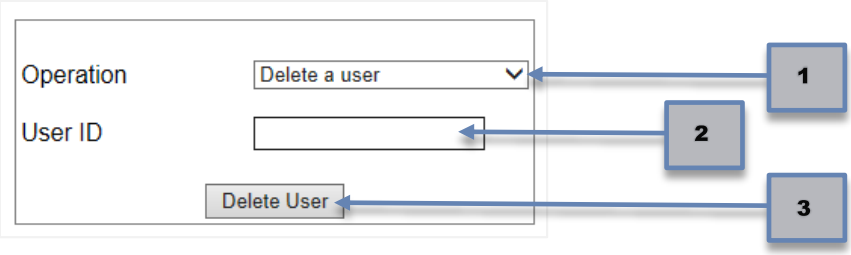
The default operation on the **User Account Management** screen is the **Add a user** selection. To add a new user, do the following:



1. Select *Add a user* from the **Operation** pull-down.
2. Enter the user ID. The user ID is case sensitive and much be between four and 16 characters in length.
3. Select the user's group: Administrator, Maintainer (default), or Operator. Refer to **Table 5-1** for each role's permissions.
4. Enter the password. The password is case sensitive and must be at least the length of the **Min Password Length** value (refer to Section **5.1.5**).
5. Re-enter the password.
6. Set the password expiration, which is units of days from the moment the new user is created. A value of **0** sets the password to never expire. If the user password is reset or changed at some point in the future, the expiration timer is also reset.
7. Select **Add User**. The message "New user account successfully created!" appears and the user name is shown in the user list along with all of the other existing user names.

5.1.3 Delete a User

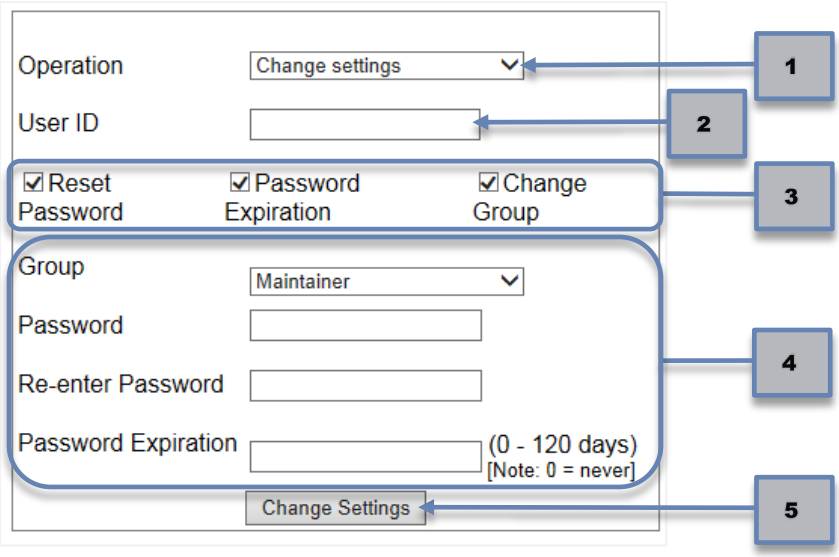
The second operation on the **User Account Management** screen is the **Delete a user** selection. To delete an existing user, do the following:



1. Select *Delete a user* from the **Operation** pull-down.
2. Enter the user ID to delete.
3. Select **Delete User**. The message "User account successfully deleted!" appears and the user name is removed from the user list.

5.1.4 Change Settings

The third operation on the **User Account Management** screen is the **Change settings** selection, which allows you to change a user's associated group (permissions), reset a user's password, or change a user's password expiration:



By default, all three options are selected: **Reset Password**, **Password Expiration**, and **Change Group**. Unchecking **Reset Password** removes the *Password* and *Re-enter Password* options, unchecking **Password Expiration** removes the *Password Expiration* option, and **Change Group** removes the *Group* option.

To change a user's settings, do the following:

1. Select *Change settings* from the **Operation** pull-down.
2. Enter the user ID whose settings you wish to modify.

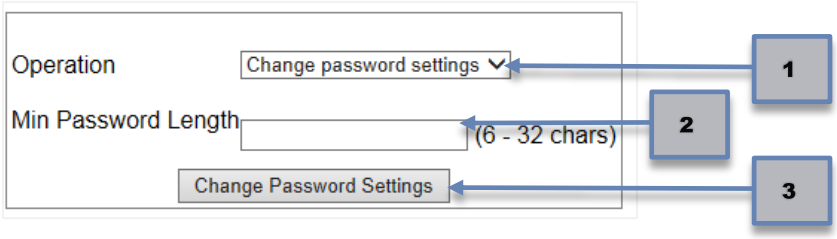
3. Uncheck any user properties you do not wish to change at this time (**Reset Password**, **Password Expiration**, or **Change Group**).

4. Fill in the applicable information.

5. Select **Change Settings**. The message "User account setting(s) successfully changed!" appears and the user's updated settings are reflected in the user list.

5.1.5 Change Password Settings

The fourth and final operation on the **User Account Management** screen is the **Change password settings** selection, which changes the minimum password length for all newly created users.



Note

If *Complex Passwords* is enabled from the **Security** pull-down, additional password criteria will be required. Refer to Section **9.1.3** for details.

To change a user's settings, do the following:

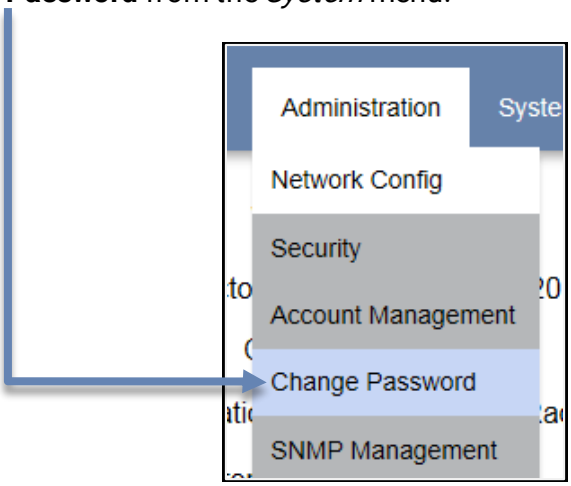
1. Select *Change password settings* from the **Operation** pull-down.

2. Enter the new minimum password length as a number between 6 and 32 (characters).

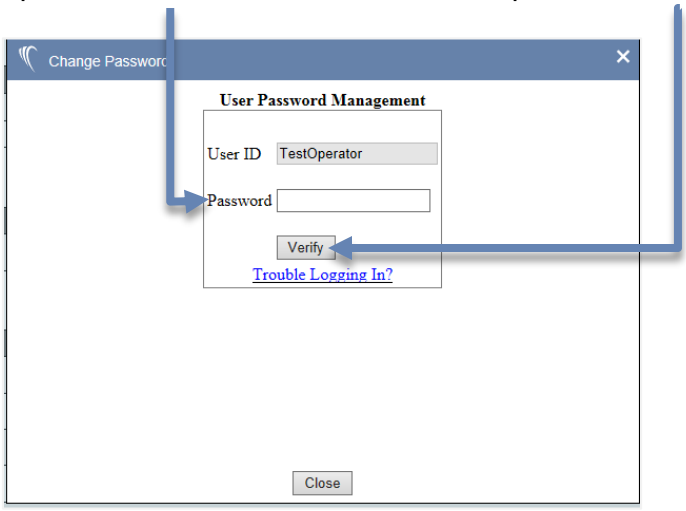
3. Select **Change password settings**. The message "Minimum password length successfully changed!" appears and the **Min Password Length** indicator above the user list is updated with the value entered.

5.1.6 Changing Passwords and Security Questions

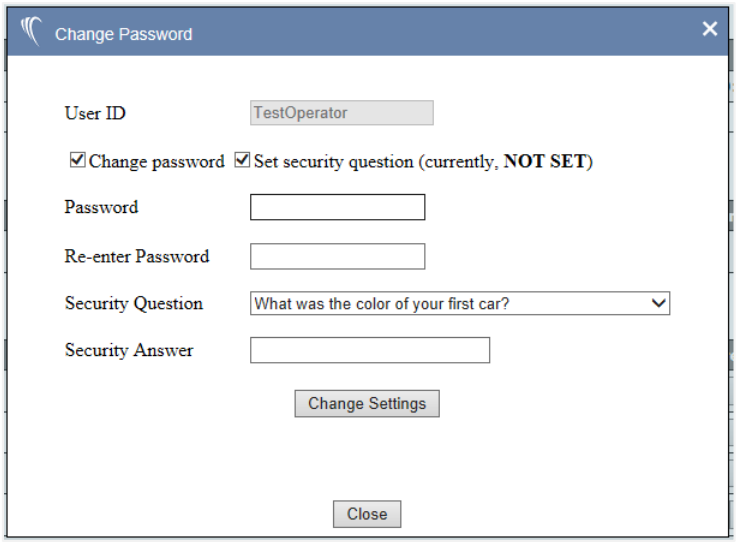
Maintainers and **Operators** are able to change their own passwords and security questions by selecting **Change Password** from the *System* menu.



Once **Change Password** is selected, the *User Password Management* login window appears. The user enters their current password in the **Password** field, then presses the **Verify** button:



Once verification is successful, the *Change Password* screen appears:



Two options are available. The first option is disabling the ability to change the password in that moment by unchecking **Change password**. The second option is disabling the security question requirement by unchecking **Set security question**.

Note

If a security question is not set, then the user will not be able to recover their password, if needed, in the future.

Once any modifications to those two options have been made, if **Change password** is still checked, the user then enters their new password, re-enters it for verification, then confirms with the **Change Settings** button.

Once all changes are confirmed, the message "User account setting(s) successfully changed!" appears. The *Change Password* screen can then be closed by pressing the ✕ or the **Done** buttons.

5.1.6.1 Login Issues – Incorrect User ID or Password

If an invalid **User ID** or **Password** is entered on the login screen, a message indicating "User name or password invalid." is shown (**Figure 5-2**).

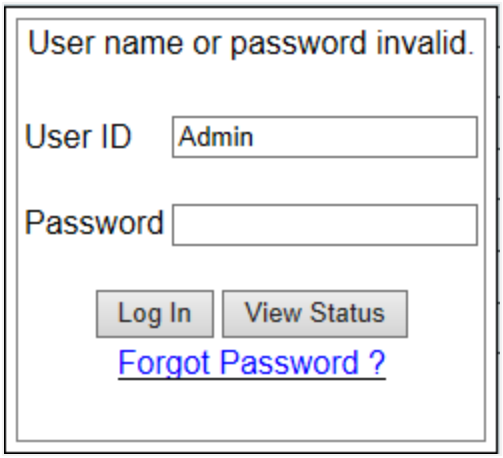


Figure 5-2: Invalid User Name or Password Message

If the password has been forgotten and a security question has previously been set (refer to Section **5.1.6** for instructions on setting a security question), click the **Forgot Password?** link. A series of three prompts walks the user through the process for entering a new password by answering a security question.

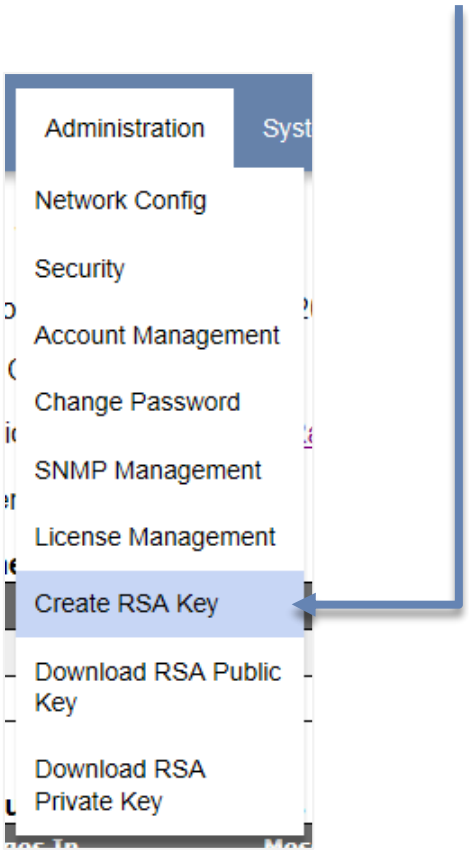
5.1.6.2 Login Issues – Password Expired

A password expiration time can be configured for each user via the **Account Management** option (Section **5.1**). If the user password has expired, a prompt indicating "Your password has expired! Please reset password" is displayed on the login screen.

To reset the login password, click the **Reset Password** link, then follow the remaining instructions. Upon success, the message "User password successfully reset!" is displayed.

5.2 Creating and Downloading RSA Keys

If RSA public and private keys need to be created, select the *Create RSA Keys* option from the *Administration* menu.

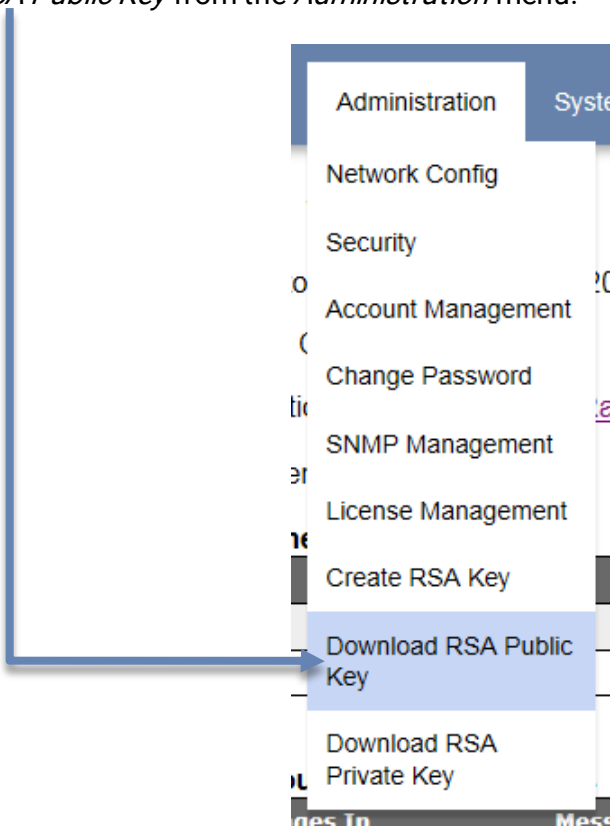


Once selected, a confirmation screen is displayed:

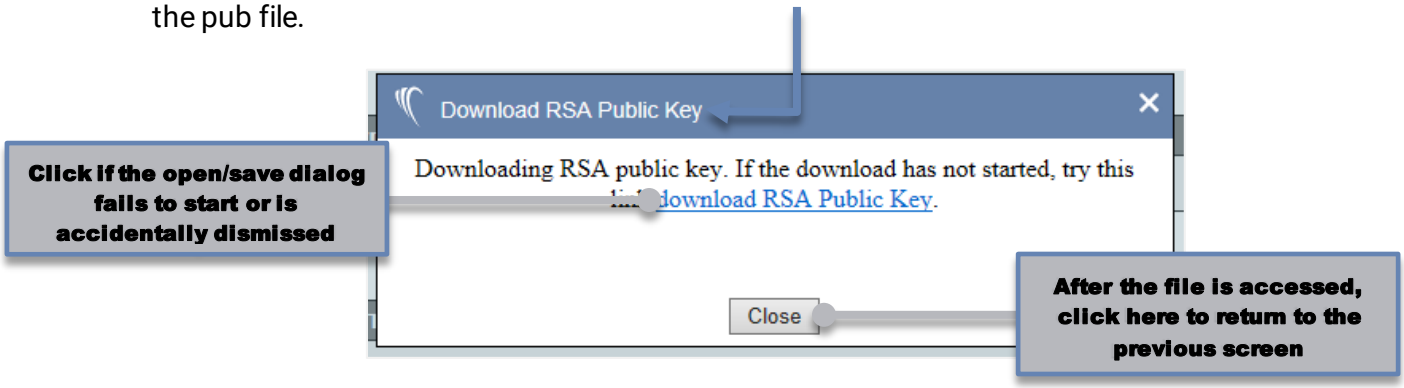
After the confirmation screen is displayed, click **Close** to return to the *Status* screen.

5.2.1 Download RSA Public Key

After creation of the RSA keys (see Section **5.2**), you can download the public key by selecting *Download RSA Public Key* from the *Administration* menu.



During download, the **Download RSA Public Key** dialog appears, then a dialog option to open or save the pub file.

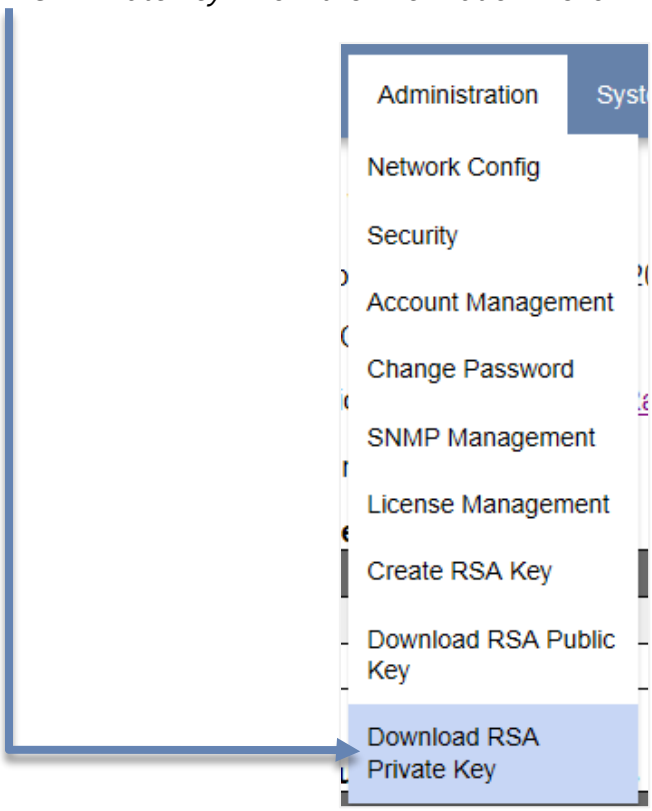


The public key, once created and downloaded from the device, needs to be uploaded to the target Linux server in order to exchange the data recordings. After downloading *id_rsa.pub*, consult your server documentation to install the public key on your file server.

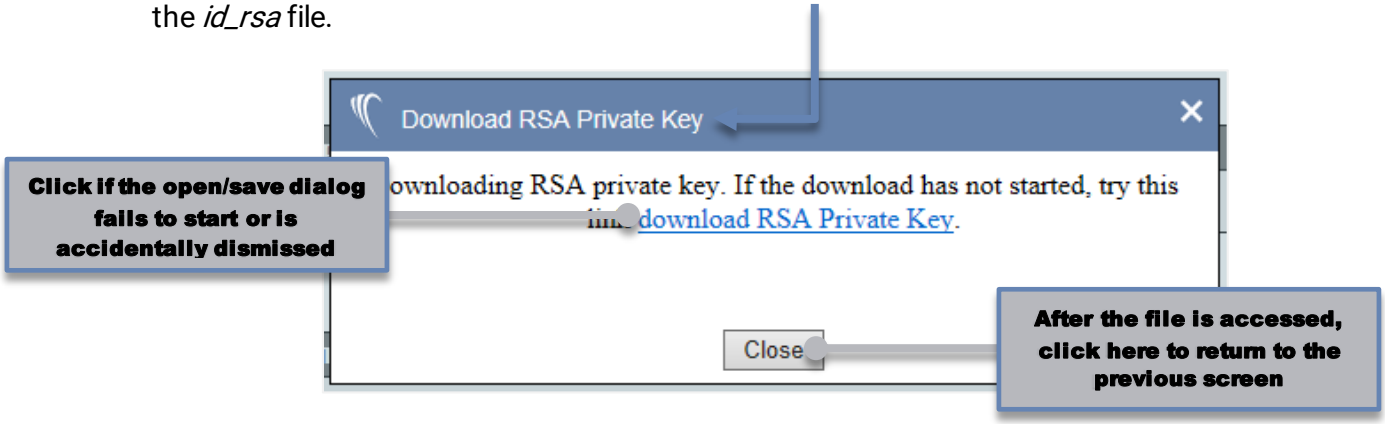
Under **sysconfig** on the **Data Flow Configuration** screen (see Section **4.4.1**), there are entries for *Data Recording Upload Server* and *Data Recording Upload Location* for up to two server addresses. This is the IP address of the Linux server and the directory where the data recordings will transfer to via SFTP.

5.2.2 Download RSA Private Key

After creation of the RSA keys (see Section **0**), you can download the private key by selecting *Download RSA Private Key…* from the *Information* menu.



During download, the **Download RDA Private Key** dialog appears, then a dialog option to open or save the *id_rsa* file.



The private key (*id_rsa*), once created and downloaded from the device, needs to then be uploaded via **Upload Data** to either the same device or any other unit performing SFTP data recording file transfers to a Linux server.

Under **sysconfig** on the **Data Flow Configuration** screen (see Section **4.4.1**), there are entries for *Data Recording Upload Server* and *Data Recording Upload Location* for up to two server addresses. This is the IP address of the Linux server and the directory where the data recordings will transfer to via SFTP.

Section 6

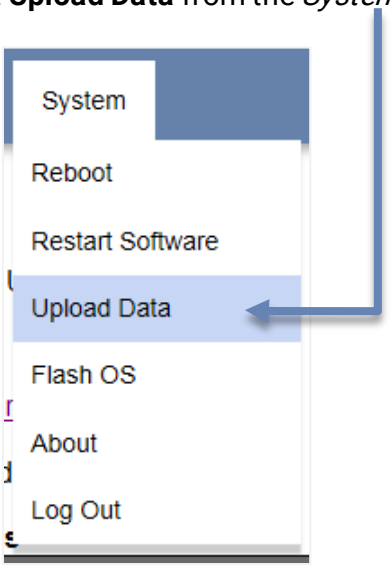
6. SPECIAL FEATURES

In this Section, you learn about some of the less frequently used, secondary features of SureLine Core.

Special features, which are described in this Section, including uploading select data, updating the operating system, and activating licensed functionality (new or additional features).

6.1 Uploading Data

To transfer files to the device, select **Upload Data** from the *System* menu.



The files are placed in their proper location based on the type of file being uploaded. The allowable file types are:

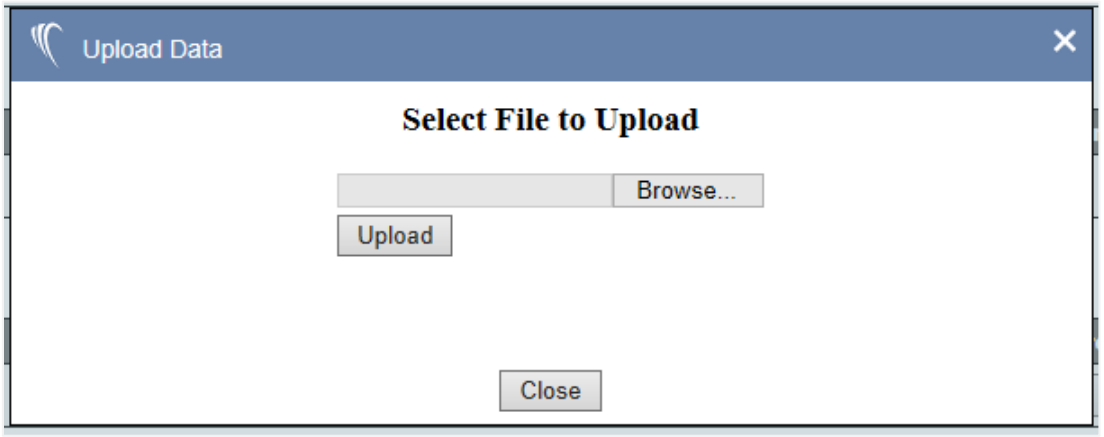
- Geographical filter description files (*.pol*)
- Configuration files (*.xml*)

- Software updates (*upd_fs.tar*, or, for versions 6.0.0 and above, *platform_#_#_#.sun*, where *platform* represents *rici*, *longport*, *ventnor*, or *sgp*, respectively, and *#* indicates version number)
- Plug-ins (*.so*)
- Raw data recordings (*.dat*)
- Radar definition file (*radar.ini*)

Note

Network profile export/import is supported using the *systemConfig.xml*, download logs, and data upload features. This is saved when the logfile is downloaded and can be extracted from the *.tar* file, modified in a text editor, and re-uploaded to the device. This provides the ability to copy or quickly modify the network configuration page's contents offline for field deployments from unit-to-unit.

Once **Upload Data** is selected, the *Upload Data* window appears:

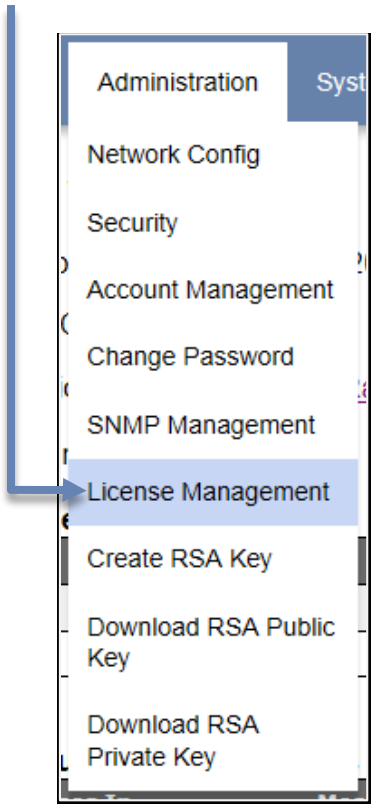


Use the **Browse** button to search on the connected workstation for the file to upload. After selecting the file, click the **Upload** button to transfer the file to the device. Should an attempt be made to upload an invalid file type, the message "**Error *filename.ext* is an invalid file to upload**" is displayed, and buttons to **Upload another file** or to close the dialog (**Done**) are provided.

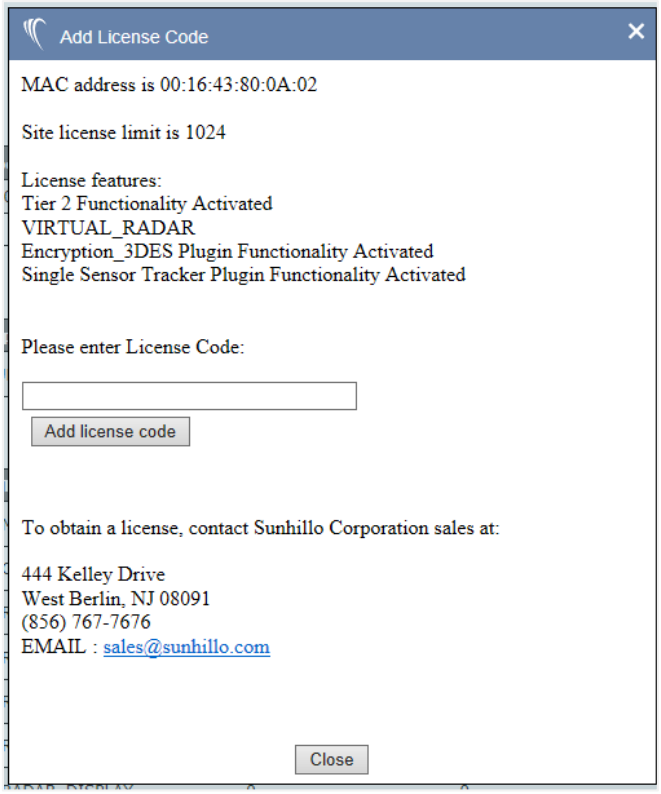
For software updates, after the file has been successfully uploaded to the device, you must reboot the system in order for the software update to take effect.

6.2 Activating Licensed Functionality

Several data conversions and other functionality (e.g., CV4400 emulation) require license codes to be activated. This activation requires interaction with Sunhillo's technical support team. To activate a licensed function, select **License Management** from the *Administration* menu.



Once **License Management** is selected, the *Add License Code* window appears:

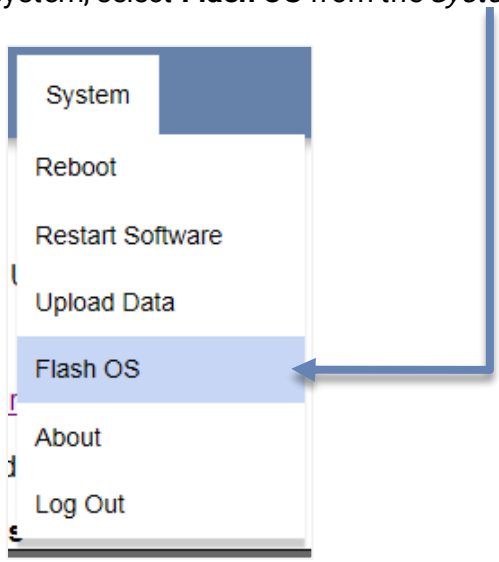


The *License features* field displays the active license features on your system. If you purchased Tier licensing, then the text "**Tier *x* Functionality Activated**" (where *x* = 1 or 2) is displayed.

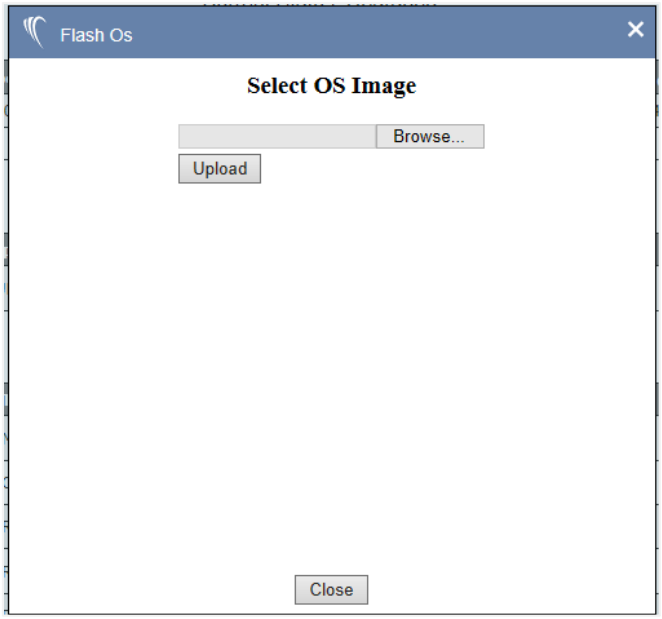
The license code is a unique, encrypted key. Once you have obtained your license code, enter it into the field below the *Please enter License Code* text, then click the **Add license code** button. If an invalid license code is entered, the message "**Failed to add License Code: *code***" is displayed before returning to the *Add License Code* window.

6.3 Flashing the Operating System

To re-flash (update) the operating system, select **Flash OS** from the *System* menu.



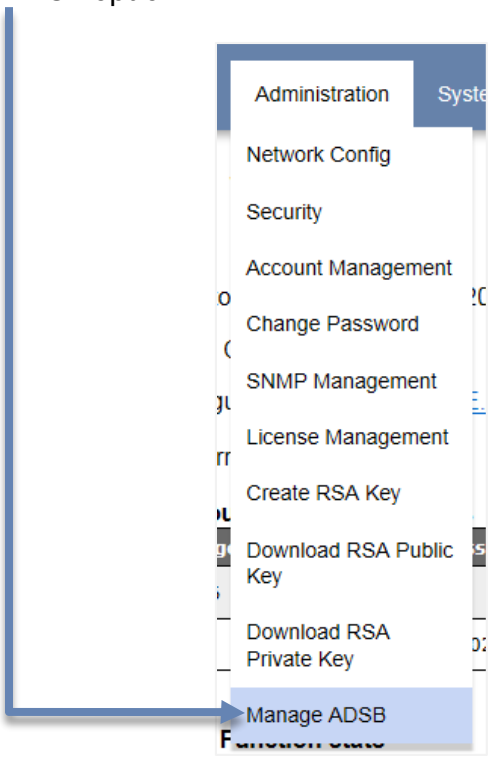
Once **Flash OS** is selected, the *Flash OS* window appears:



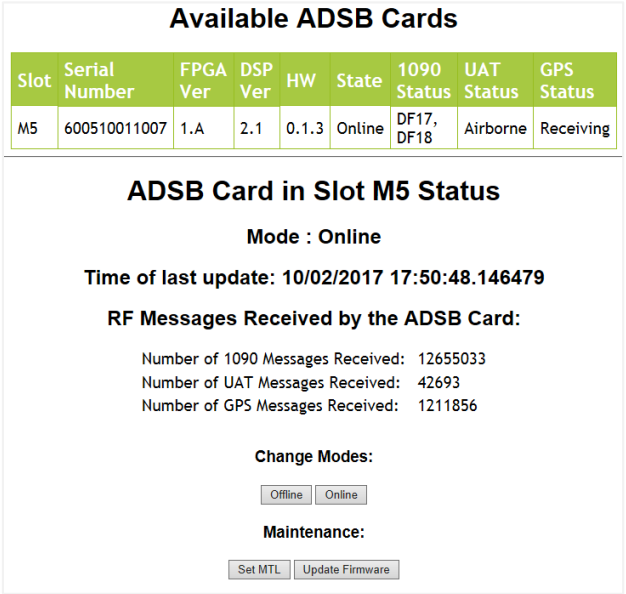
The file to be uploaded can be typed in the text entry field next to the **Select File** button, or the **Browse** button can be used to search for the file on the drive of the connected computer. Once the filename has been entered, click the **Upload** button to transfer the OS file to the device. Should an attempt be made to upload an invalid OS image, the message "**File Upload Failed**" is displayed.

6.4 Managing ADS-B Receiver Modules in Longport

If a Sunhillo ADS-B receiver module is present in the Longport chassis, the *Administration* menu displays the **Manage ADSB** option.



The ADS-B receiver module is controlled by one or more PCMs, and this relationship and the ADS-B module itself are configured through the *Manage ADSB* screen:



Note

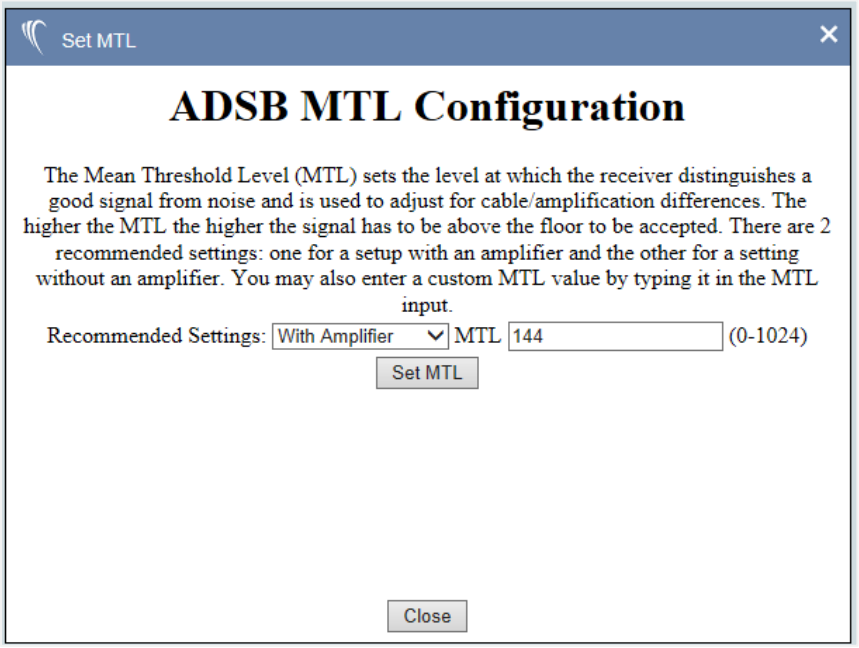
Details regarding the installation of the ADS-B receiver module are provided in the ADS-B receiver installation manual, *SUN2905_2 – ADS-B Receiver Processor Card Module Operations Manual*, which was shipped with the module.

The top portion of the *Manage ADSB* screen presents status as reported by the ADS-B receiver. The **Slot** information denotes the Longport chassis slot number (reading from left to right from the front side of the chassis) in which the receiver resides (note that slot information is omitted on the Margate II ADS-B page).

The bottom portion of the screen has buttons for controlling the ADS-B receiver. To take a card offline, click the **Offline** button. A warning dialog is displayed. Click **OK** to take the card offline or **Cancel** to retain its online status.

To bring a card online, click the **Online** button. A warning dialog is displayed. Click **OK** to take the card offline or **Cancel** to retain its online status.

The Mean Threshold Level (MTL) sets the level at which the receiver distinguishes a good signal from noise and is used to adjust for cable/amplification differences. The higher the MTL value, the higher the signal has to be above the floor to be accepted. In order to adjust this value, click the **Set MTL** button to display the *Set MTL* dialog:



There are two default recommended settings, one for an antenna with an amplifier and one for an antenna without an amplifier. These are selected by clicking the dropdown arrow in the **Recommended Settings** field. A third option, *Other*, appears in this dropdown. If this option is selected, the value entered into the **MTL** field is used.

Updates to the ADS-B receiver firmware are managed by Sunhillo and are delivered electronically to customers in the event of a bug fix or if the card is under warranty and is eligible for firmware enhancements. The firmware is loaded onto the ADS-B receiver under the control of the Longport PCM.

To update the ADS-B firmware:

1. Click the **Update Firmware** button.
2. A dialog window appears warning that the receiver will go offline. Click **OK**.
3. In the *Upload Firmware* dialog, type in or browse to the *. *adsb* file to be downloaded to the ADS-B receiver module.
4. Click the **Upload** button. The *Upload Firmware* dialog displays with a progress bar showing the download file progress.

Upon completion, the *Upload Firmware* dialog displays "Upload Successful" (in place of the "Flash phase" message). Click the **Done** button to exit the *Upload Firmware* dialog.

6.5 Accessing the Sunhillo Terminal User Interface (STUI)

For low bandwidth connections or as an alternative to the GUI, you can use a serial connection, Telnet, or SSH into the device to access the STUI. The STUI allows access to most of the same features as the GUI, save for the Functional Configuration (Section **4**). A unique function, **Technical Support**, described in Section **6.5.1**, is also listed on the STUI menu, allowing for standard shell access in coordination with Sunhillo Technical Support (refer to Section **1.2**) for issues that can't be resolved through normal methods.

Note

Account Management options in the STUI menu are specific to the STUI. In other words, user accounts created or modified in the GUI do not apply to the STUI, and vice-versa.

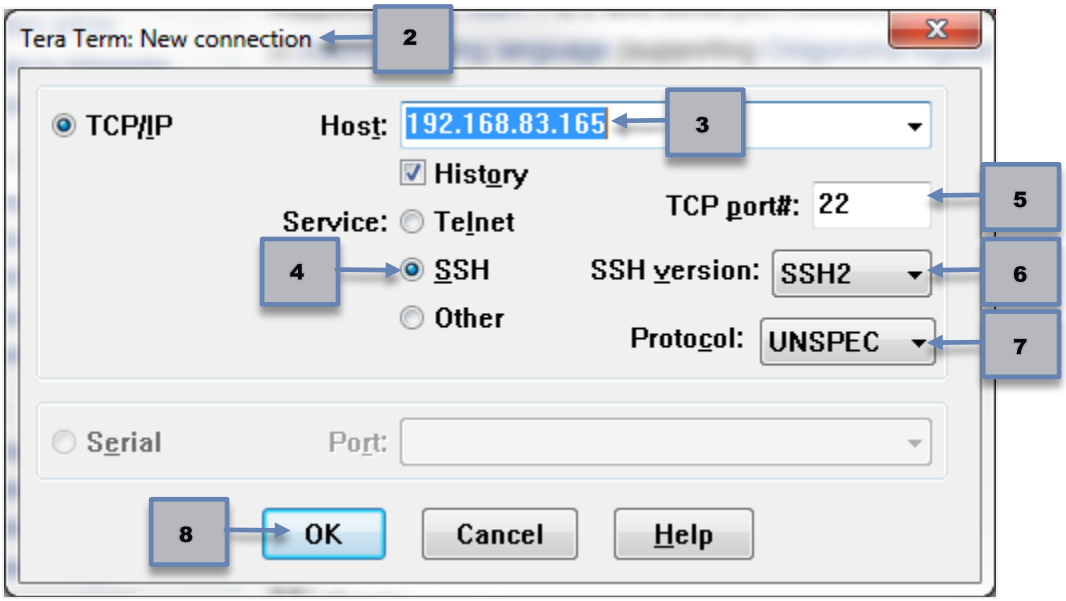
If enabled through the GUI (see Section **9.1**), Telnet or SSH connections are available on the Ethernet ports, as well as a serial connection through the Maintenance (**Maint**) port. While most terminal programs should work, file transfers require a terminal program that supports the ZMODEM file transfer protocol.

Note

On RICI, Longport, and Ventnor devices, if an Ethernet connection isn't an option, a USB to miniUSB cable can be used to allow for the same type of connection options. On a Margate II ADS-B, a USB to USB cable can be used. In the terminal software, the baud rate should be set to 115200 and the local PC's applicable COM port should be selected.

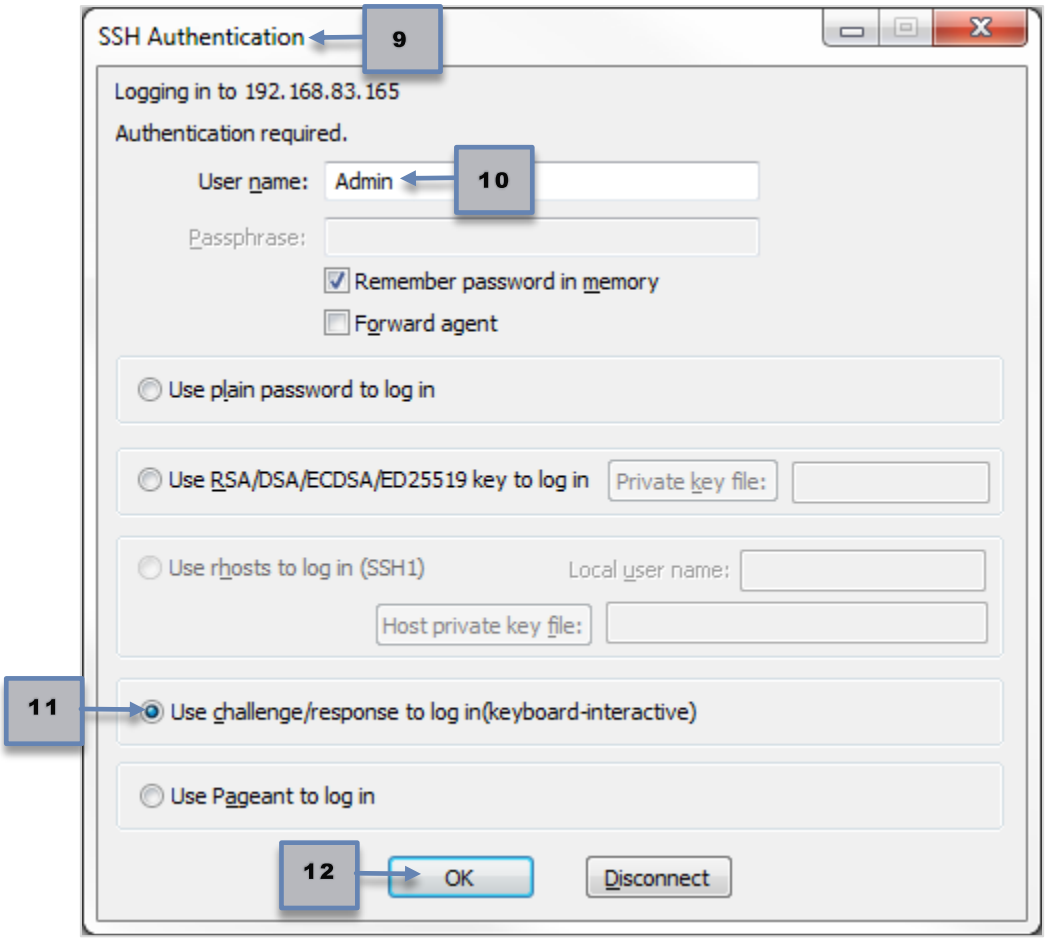
Example steps for connecting over SSH with the free, open source terminal emulator, *Tera Term*, are as follows:

1. Start *Tera Term*.
2. The *Tera Term: New Connection* window appears.



3. Enter the IP address of your device under **Host:**.
4. Verify **SSH** is selected under **Service:**.
5. Verify the **TCP port#:**.
6. Verify the **SSH version:**.
7. Set the protocol to unspecified (**UNSPEC**).
8. Click **OK**.

9. The *SSH Authentication* window appears.

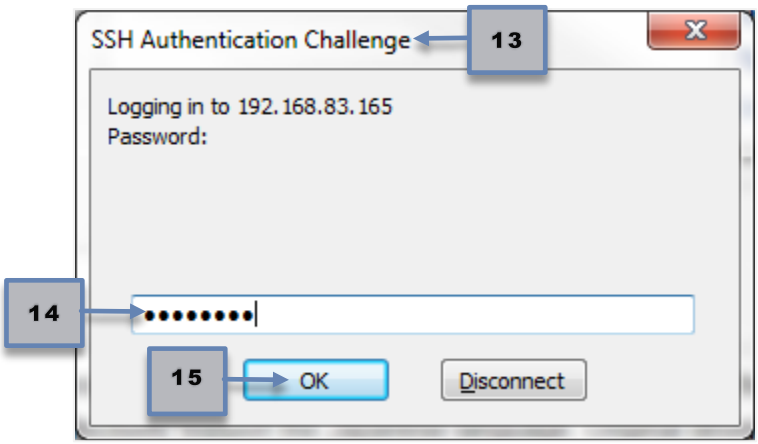


10. Enter **Admin** under user name.

11. Select **Use challenge/response to log in(keyboard-interactive)**.

12. Click **OK**.

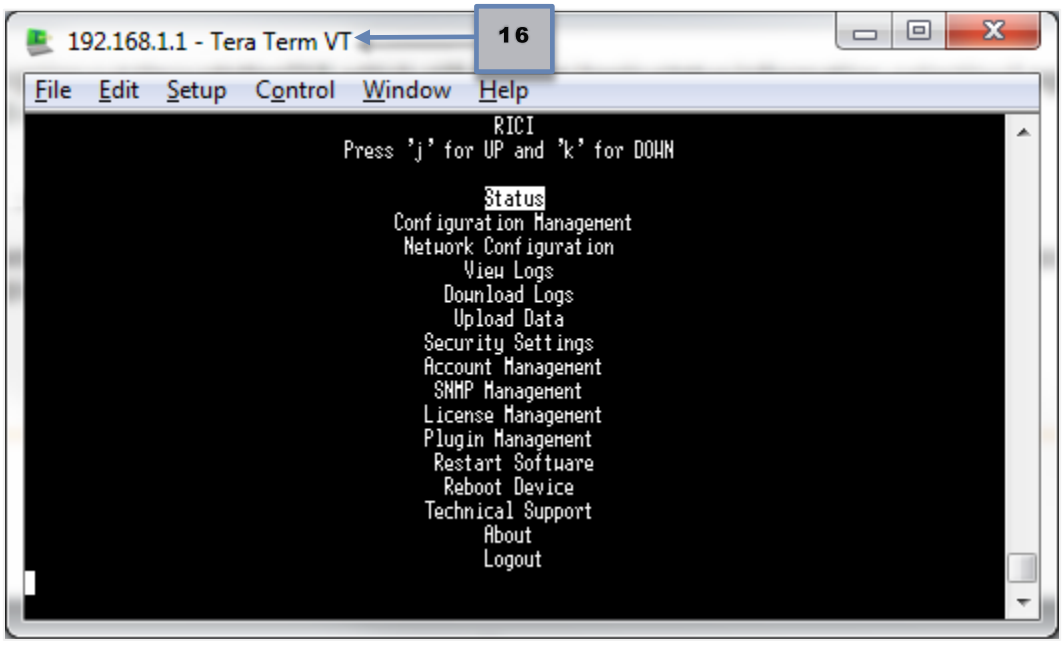
13. The *SSH Authentication Challenge* window appears.



14. Enter **Sunhillo** (password).

15. Click **OK**.

16. The terminal window appears, with all STUI menu options accessible.

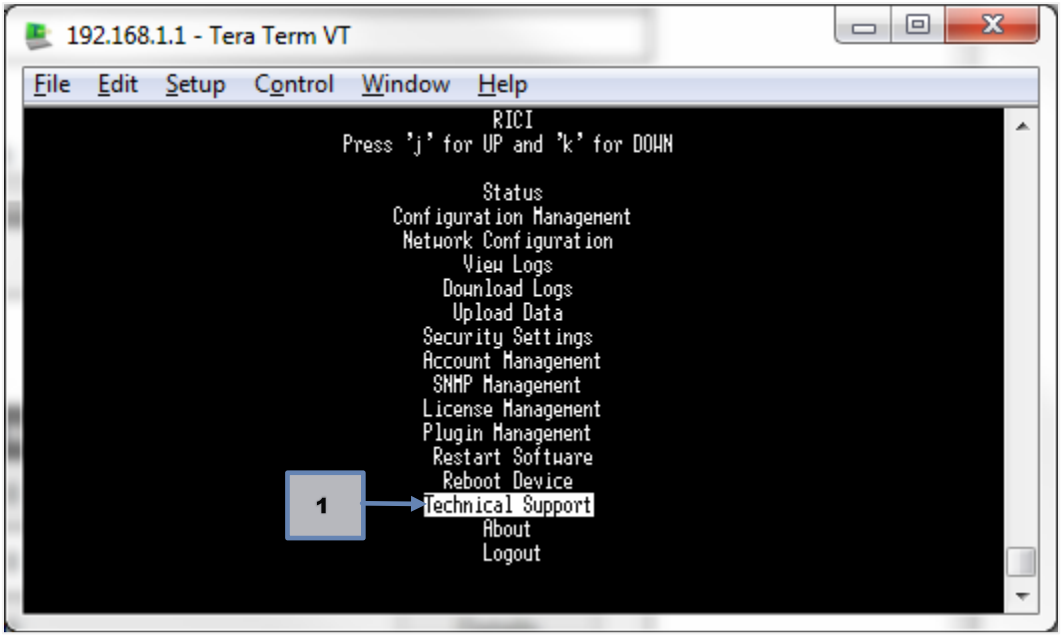


Unlike logging out through the GUI, which still displays basic status information, selecting **Logout** on the STUI menu terminates the connection.

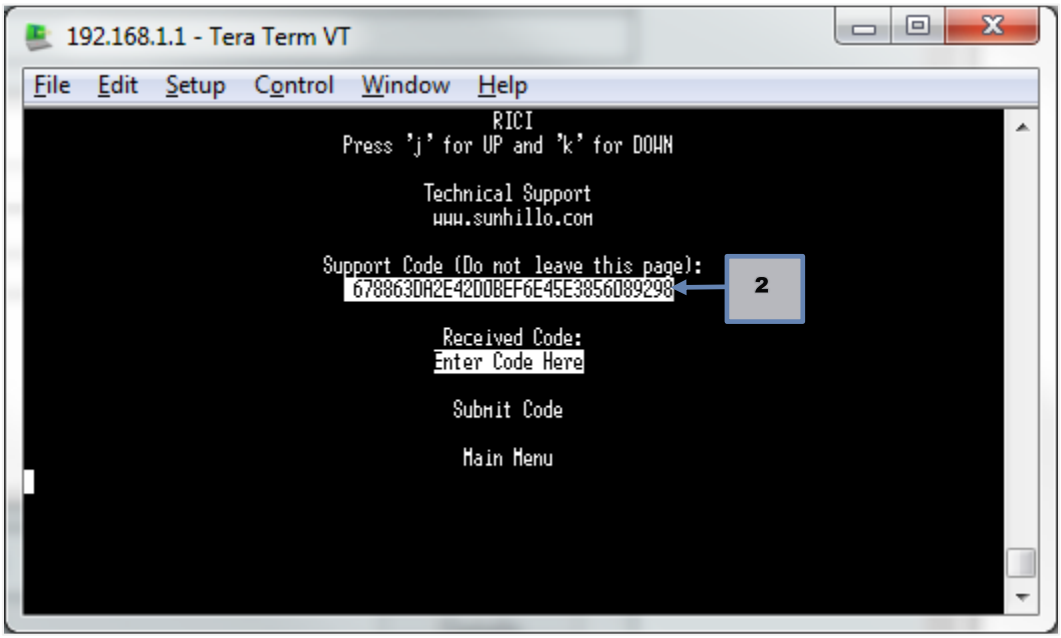
6.5.1 Technical Support Option

For issues that can't be resolved through normal methods, you will need to gain access to the standard shell prompt. Do the following:

1. Highlight **Technical Support** on the STUI menu and then press **Enter**.



2. Use your mouse to left-click on and select **Support Code** until all of the letters and numbers are highlighted.



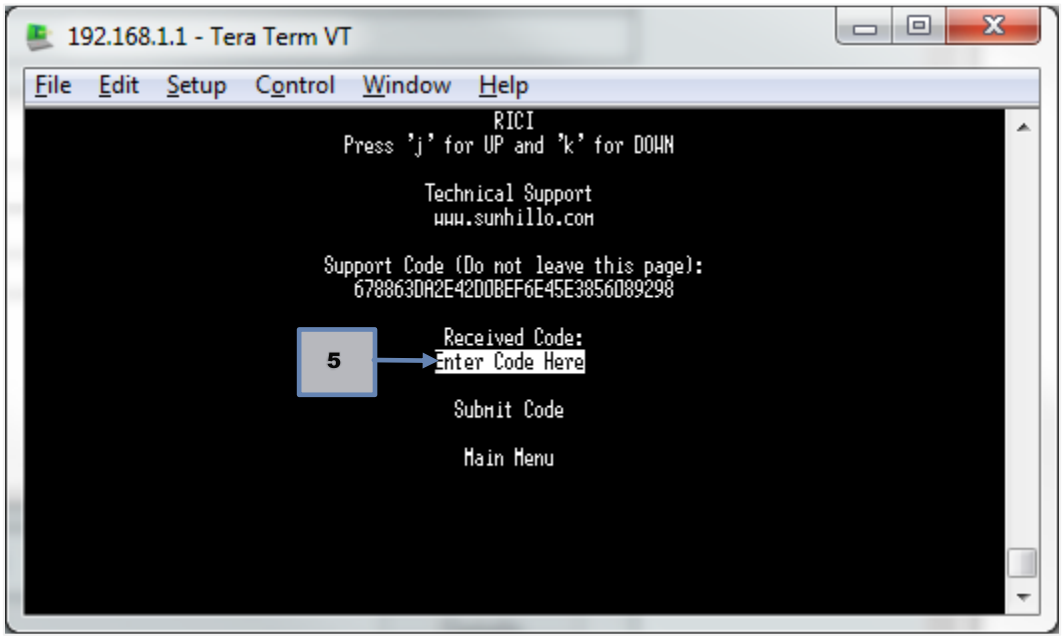
3. To copy the code, highlight it with the mouse. This will allow it to be pasted into an email or other document for Sunhillo technical support.

Note

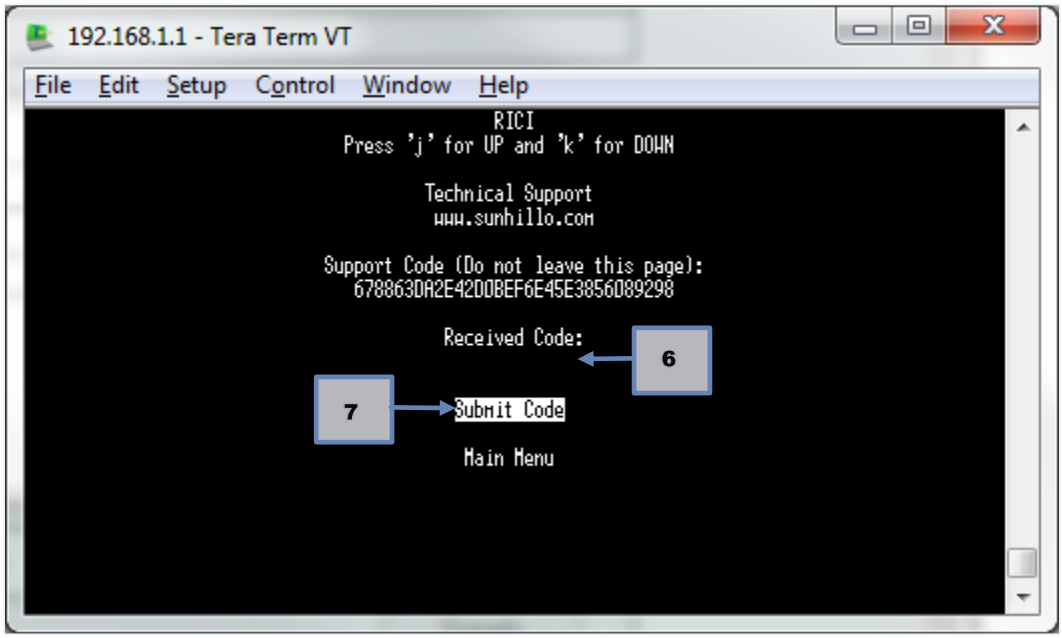
The **Support Code** is only valid for the current session. Once you exit out of the menu option, a new code will need to be generated.

4. Contact Sunhillo technical support via email or phone (refer to Section **1.2**) and provide the **Support Code** from step 2 to receive a code in return.

5. Highlight **Enter Code Here** and press **Enter**.



6. Under **Received Code**, paste the code received from Sunhillo technical support in step 4 by right-clicking with the mouse.



7. Highlight **Submit Code** and press **Enter**. You now have access to the standard shell prompt and can continue troubleshooting.

Section 7

7. REDUNDANCY

In this Section, you gain a general understanding of unit and network interface redundancy.

Redundancy can be classified into two categories: *unit* (or, for Longport, *PCM*) redundancy and *network interface* redundancy. This Section describes the two categories of redundancy, along with the associated configuration parameters needed to achieve these.

7.1 Unit Redundancy

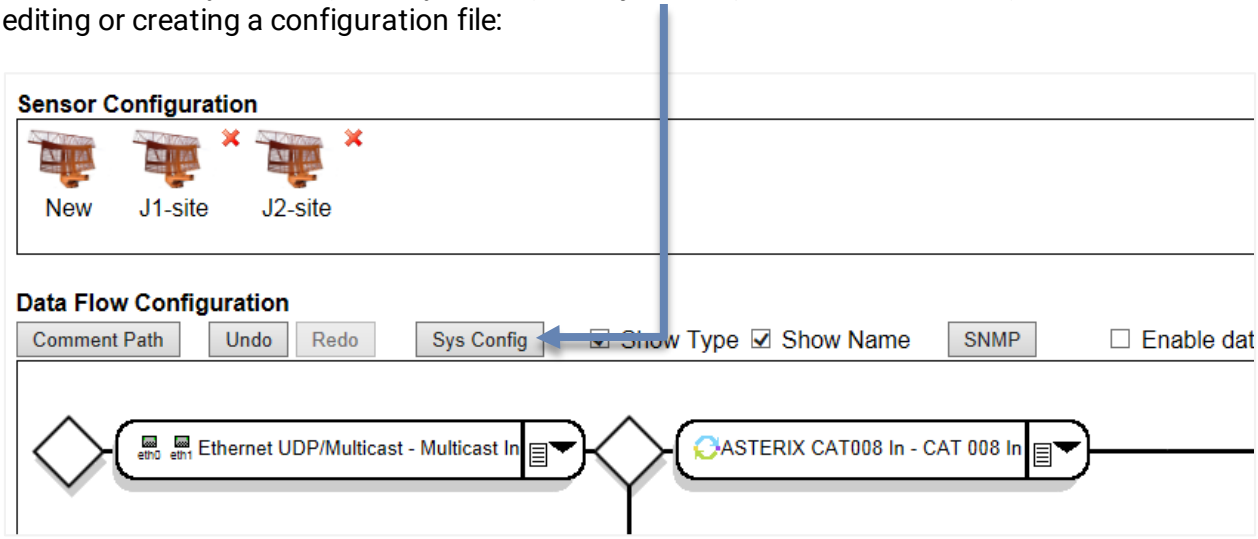
Unit redundancy means a pair of devices is configured to operate in a mode where one unit is the primary and the other unit is the backup (refer to Section **7.3.1**).

Note

For Longport redundancy, redundant PCMs can be located within the same chassis or in two different Longport chassis that are connected on the same network.

The primary and backup units communicate through a system health message, which is not configurable. Each device in a redundant pair is monitoring the other device through the health messages. The UDP health message can be sent between the units by unicast or multicast. A redundant network can also be configured for unit redundancy in which a primary and redundant network interface are used for sending and receiving the health messages. In a redundant device configuration, only one device is processing data ("active") at any given time; the other device of the redundant pair is monitoring, but not processing, data ("standby").

Unit redundancy is configured by clicking the **Sys Config** button on the configuration GUI when editing or creating a configuration file:



The configuration parameters necessary for unit redundancy are described in **Table 7-1**.

Table 7-1: Unit Redundancy Configuration Parameters

Configuration Parameter	Description
Processor Number	Unique number identifying which unit is primary and which is the backup. Valid values are 0 - 15, in increments of 1, e.g., primary processor number = 0 and backup processor number = 1.
Primary/Backup Processor	Valid values are: • **None** – Disable unit redundancy feature • **Primary** – Unit is primary • **Backup** – Unit is backup If the preferred primary method is enabled (see Section **7.3**), this value determines which device unit will be the primary unit and which unit the backup unit. If the preferred primary method is disabled, this value only sets the initial unit redundancy state upon system startup. If switchovers occur, a device will alternate between being the primary unit or the backup unit.

Configuration Parameter	Description
Multicast Port Number	The port number for transmitting the UDP health message to the other unit. The port number is bidirectional and does not depend on whether a unit is primary or backup. Valid range is 1 to 65535.
Multicast IP	The multicast or unicast address used for transmitting UDP multicast health messages to backup unit (if primary) or to primary (if backup) for the primary network interface.
Multicast NIC	The name of the Ethernet interface used for transmitting health messages from the unit (either primary or backup) on the primary network interface. Valid values, which are selected using the dropdown list, are the device names of each Ethernet port.
Multicast Receive IP Address	The multicast or unicast address on the primary network interface used for receiving UDP multicast health messages from the backup unit (if primary) or from primary (if backup).
Redundant Multicast Port Number	The port number for transmitting the UDP health message on the redundant network interface to the other unit. The port number is bidirectional and does not depend on whether a unit is primary or backup.
Redundant Transmit Multicast Address	The multicast or unicast address used for transmitting UDP multicast health messages to backup unit (if primary) or to primary (if backup) on the redundant network interface.
Redundant Multicast Data Ethernet Port	The name of the Ethernet interface used for transmitting health messages from the unit (either primary or backup) on the redundant network interface.
Redundant Receive Multicast Address	The multicast or unicast address on the redundant network interface used for receiving UDP multicast health messages from the backup unit (if primary) or from primary (if backup).
Redundant Processor IP Version	The IP version of the redundant network interface data.

Configuration Parameter	Description
Network Time To Live (TTL)	The TTL is a limit on the number of transmissions or a limit on the period of time a data packet on a computer network can exist before it should be discarded. *This parameter should be configured to a value that best supports the architecture of the network on which the device will be transmitting data to ensure the data packets will reach the intended destination(s) without being discarded. This parameter limits the number of routers a packet can traverse.*
Preferred Primary	This parameter enables or disables the use of a preferred primary method when selecting which unit (primary or redundant) to process data from or which unit to make "active." Selectable values are: • Enabled • Disabled If set to "Enabled," the preferred primary method is used to ensure the primary unit is always processing incoming data if possible. If set to "Disabled," the preferred primary method is not used and possible unwanted switchovers between redundant and primary units are reduced.

7.1.1 Unit Redundancy Switchover

A health check failure between the active unit and the inactive unit will cause a switchover. The inactive unit becomes active and starts processing data. A health check failure could occur due to a system failure, the unit being powered down, or network failure. The *Preferred Primary* configuration parameter indicates how the active unit, whether it is the primary or backup unit, is determined. A detailed description of *Preferred Primary* functionality is provided in Section **7.3**. If the redundant network interface is configured, both the primary and redundant health checks must fail on the active unit for the inactive unit to become active and start processing data.

If the device is configured to send SNMP traps (see Section **10.3**), an SNMP trap is generated when the device state changes from active to inactive or vice-versa.

7.2 Network Interface Redundancy

A device can be configured for network interface redundancy in which a primary and redundant network interface are used for the processing of input and output LAN data streams. The configuration parameters vary depending on if the unit is receiving LAN data or transmitting data onto the LAN.

7.2.1 Receiving LAN Data

Device network redundancy for receiving LAN data can operate in three different modes:

- Dual Data Input
- Primary and Redundant Input
- Preferred Primary Input

The Dual Data Input redundancy mode is when the device is configured to receive and process LAN data from both Ethernet ports. The device is configured to receive two sources of the same LAN data.

In the **Primary and Redundant Input** mode, the device monitors both the primary and redundant LAN sources. However, the data from only one of those sources will be processed. The **Preferred Primary Input** mode is determined by the *Preferred Primary* configuration parameter, which indicates how this processing should be performed. A detailed description of the preferred primary method is provided in Section **7.3**.

The network interface redundancy configuration for receiving LAN data is done in the *Ethernet UDP/Multicast* node type. The exception to this configuration is when the incoming data is in En Route Communications Gateway Protocol (ECGP) format. Although the primary and redundant network interfaces are configured in the *Ethernet UDP/Multicast* node type, it is the *ECGP Unframer* function node type of the software that monitors the redundant network. There are configuration parameters specific to the *ECGP Unframer* function that must be configured for network redundancy to operate with incoming ECGP data.

If the incoming LAN data is in ECGP format, some elements of the network interface redundancy are configured in the configuration parameters for the *ECGP Unframer* function. The configuration parameters and descriptions related to network redundancy for ECGP Unframer are described in **Table 7-2**.

Table 7-2: Configuration Parameters for ECGP Unframer Network Redundancy

Configuration Parameter	Description
Preferred Primary	This parameter enables or disables the use of a preferred primary method when selecting which LAN input (primary or redundant) to process data from or which Ethernet port to make "active". Selectable values are: • Enabled • Disabled If set to "Enabled," the preferred primary method is used to ensure the primary network interface is always processing incoming data if possible. If set to "Disabled," the preferred primary method is not used, and possible unwanted switchovers between redundant and primary network interfaces is reduced.
Primary Receiver Timeout	This is the number of milliseconds the device will wait before switching to the alternate LAN source if ECGP data from the interfacing Air Route Traffic Control Center (ARTCC) is no longer received.

The primary and redundant network interface, such as address, port, and NIC, for ECGP and all other incoming LAN data is configured in the *Ethernet UDP/Multicast* node type. Refer to Section **4.4.4.1** for the details on setting configuration parameters for a node type. The configuration parameters and descriptions related to configuring the three modes of network redundancy are listed in **Table 7-3**. These configuration parameters are used by the software only if the *Primary and Redundant LAN* input parameter is set to "Enabled."

Table 7-3: Configuration Parameters for Three Modes of Network Redundancy

Configuration Parameter	Description
Primary and Redundant LAN Input	Enables or disables the network interface redundancy for incoming LAN data. Selectable values are: • **Enabled** – Process data between two LAN sources (*primary* and *redundant*). • **Disabled** – Only the primary network interface is used; no network interface redundancy. **NOTE**: The parameters that follow in this table are used only if this parameter is set to "Enabled."
Primary Receiver Timeout	This is the number of milliseconds the device will wait before switching to the alternate LAN source if data is no longer being received on the current LAN source.

Configuration Parameter	Description
Preferred Primary	This parameter is only used if *Dual LAN Data Filter* and *Primary and Redundant LAN Input* are set to "Enabled."
Dual LAN Data Filter	Selectable values are: • Enabled • Disabled If enabled, the device will process data from only one LAN input source, while the other is monitored for data and/or active LAN connection. If the current (either primary or redundant) LAN source has a loss of data, the device will switch to the other source to continue processing data. If disabled, the device will process both the primary and redundant sources of LAN data. The device will receive and process two input sources of LAN data. This parameter should be enabled only when the incoming data is not in ECGP format and redundant LAN sources are configured.
Redundant Receive Multicast Address	The IP address used for receiving UDP multicast, unicast, or broadcast data on the redundant network interface. If this entry is blank, the *Ethernet UDP/Multicast* node type will function in UDP broadcast mode and will receive all UDP data.
Redundant Processor IP Version	IP version of the redundant interface – IPv4 or IPv6.
Redundant Multicast data Ethernet Port	The name of the Ethernet port used for receiving the UDP multicast, unicast, or broadcast data on the redundant network interface.
Redundant Multicast Port Number	The port number for receiving UDP multicast, unicast, or broadcast data on the redundant network interface.

7.2.1.1 Network Redundancy Switchover

Either a loss of data on a network interface for an amount of time designated by the *Primary Receiver Timeout* parameter or a loss of network link on the interface will cause a switchover to the alternate network interface. A loss of data could occur due to a hardware failure of the network interface itself, IP connection problems, or simply the data from the source no longer being transmitted to the device. In the case of the *ECGP Unframer* function, loss of data also means that data from a particular ARTCC is no longer detected on the incoming LAN data stream.

If the incoming data is in ECGP format, the *ECGP Unframer* function is used to perform the selection of data from either the primary or redundant LAN sources. If the incoming data is not ECGP format, the *Dual LAN Data Filter* parameter configures the device to select the data between the primary and redundant LAN sources. The device will monitor both LAN sources, but process only one source at a time. The *Preferred Primary* configuration parameter indicates how this processing should be performed. A detailed description of the *Preferred Primary* functionality is provided in Section **7.3**.

If the device is configured to transmit SNMP traps, an SNMP trap is generated when the device switches to a different LAN data source.

7.2.2 Transmitting LAN Data

Network interface redundancy for transmitting LAN data from the device is configured in the *Ethernet UDP/Multicast* node type. The configuration parameters and descriptions related to configuring network redundancy are listed in **Table 7-4**. The configuration parameters in **Table 7-4** are used by the software only if the *Primary/Redundant Ethernet Devices* parameter is set to "Enabled."

Table 7-4: Configuration Parameters for Configuring Network Redundancy

Configuration Parameter	Description
Primary/Redundant Ethernet devices	Enables or disables the network interface redundancy data transmit function for multiple Ethernet devices. Selectable values are: • Enabled • Disabled When enabled, the device will send the same data to the primary and redundant Ethernet devices. When disabled, the device will use only the primary Ethernet device for transmitting data; network interface redundancy is disabled.
Redundant Processor IP Version	IP version of the redundant processor – IPv4 or IPv6.
Redundant Transmit Multicast Address	The IP address used for transmitting UDP multicast, unicast, or broadcast data on the redundant network interface. If this entry is blank, the MULTICAST node will broadcast on the system subnet.
Redundant Multicast Data Ethernet Port	The name of the Ethernet port used for sending the redundant UDP multicast, unicast, or broadcast data. Valid values, which are selected using the dropdown list, are the device names of each Ethernet port.
Redundant Multicast Port Number	The port number for sending UDP multicast, unicast, or broadcast data for the redundant data.

Configuration Parameter	Description
Single Multicast Destination	Enables/Disables transmitting multicast data to a single LAN destination in a system configured for redundancy. When enabled, the device will multicast data on the primary LAN. If the primary LAN is not active (connected), the redundant LAN is used. The primary LAN is always used by default, regardless of whether the data source was from the primary LAN, redundant LAN or serial ports. When disabled and redundancy is configured, the same data is transmitted on both primary and redundant LANs.

7.3 Preferred Primary Method

The term *Preferred Primary* refers to how switchovers are performed in redundant configurations. For unit redundancy, the switchover is between the primary and backup units. For network interface redundancy, the switchover is between the primary and redundant network interfaces receiving LAN data.

7.3.1 Unit Redundancy

If the *Preferred Primary* parameter is set to "Enabled," the method to determine which unit is to be active, i.e., processing data, is done on a "Preferred Primary" basis. As a result, the primary unit will always be the active unit when it is operational. If the primary unit has failed in some way, the backup unit will encounter a health check error. The backup unit then becomes the active unit and starts processing data. When the primary unit is operational, the backup unit will detect this through successful health checks. The primary unit becomes the active unit and the backup unit returns to a "monitor only" mode.

If the *Preferred Primary* parameter is set to "Disabled," the active unit, regardless of whether it is primary or backup, will remain active until a failure occurs on that unit and a switch-over to the alternate unit is necessary. If a failure occurs on the primary unit, the backup unit becomes the active unit. When the primary unit is operational again, the backup unit will remain the active unit and the primary unit will be inactive. Only a failure on the backup unit will cause the primary unit to become active.

7.3.2 Network Interface Redundancy

If the *Preferred Primary* parameter is set to "Enabled," the processing of the data is done on a "Preferred Primary" basis. The device will monitor both primary and redundant sources of data, but always use the primary network interface until a loss of data is detected. If data is no longer detected on the primary source, the device will automatically switch to the redundant network interface and process the data. If data returns on the primary network interface, the device will switch back to use the data from the primary source. If data is not found on either primary or redundant data sources, the device will remain on the primary network interface.

If the *Preferred Primary* parameter is set to "Disabled," the device will monitor both primary and redundant network interfaces and use the source, whether primary or redundant, (only one) which provides data. A switch to the other data source will only occur if a loss of data on the current source is detected.

If the device is configured to send SNMP traps, an SNMP trap is generated when the device switches to a different network interface.

7.4 Radar Redundancy

The device can be configured to monitor redundant input radar data sites. The input source of these radar sites could be two serial interfaces, two LAN sources, or a mix of serial and LAN. The device will monitor both sources (serial and/or LAN) for a particular radar site and switch to the valid source of that radar data if one input should fail to deliver that radar site data. Radar redundancy is configured in the *Site Filter* node type. The configuration parameters and descriptions related to configuring radar redundancy are listed in **Table 7-5**.

Table 7-5: Configuration Parameters for Radar Redundancy

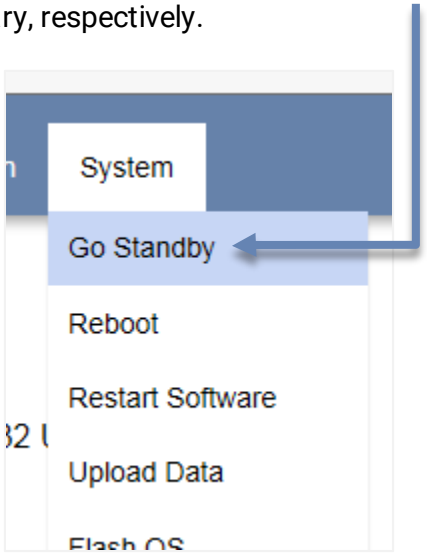
Configuration Parameter	Description
Radar Redundancy Type	This parameter sets the type of radar redundancy for the particular radar site. Selectable values are: • **NONE** – Disables radar redundancy. • **Last Good** • **Preferred Primary** If set to "Last Good," the valid input source of the radar site data, regardless of primary or redundant, will always be used. If set to "Preferred Primary," the preferred primary method is used to ensure the primary source of the radar site is always processing incoming data if possible. Refer to Section **7.3**.
Radar Timeout	This is the number of seconds the device will wait before switching to the alternate source of the radar site data when that data is no longer present on the current input source.
Site Name	The radar data 3 - 4 letter name that identifies the site.
Radar ID	A numeric value that identifies the site.

Configuration Parameter	Description
Site Filter Type	The parameter determines which information the filter should use to identify the particular radar data. Selectable values are: • Site Name • Radar ID

7.5 Manual Switching

If the radar data source is over the network, the device can be configured to drop duplicate data packets using the *ECPG Unframer* node type using the configuration parameter "Drop Duplicate Packets."

For redundant device setups, you can switch between **Go Standby** or **Go Active** to make the selected device either secondary or primary, respectively.



This page is intentionally left blank.

Section 8

8. USB FLASH DRIVE USAGE

In this Section, you learn about the USB flash drive interface features.

The USB slot(s) on the device is used to apply updates, copy over configuration files, download log files, or set other configuration parameters via a USB flash drive. Note that not all device platforms support a USB flash drive interface. These devices are identified in the subsections that follow.

8.1 RICI USB Update Notification

The RICI provides visual feedback when applying updates via a USB flash drive. The **TD/RD**, **RD/TD**, and **SYNC** LEDs are employed to provide an indication of the status of the update(s).

Note

Ventnor, RICI 5000, and Margate II ADS-B devices do not have front facing USB ports, and, as a result, do not support these features.

The LED indications apply to the following USB-based operation: RICI software update (*rici_[version].sun*).

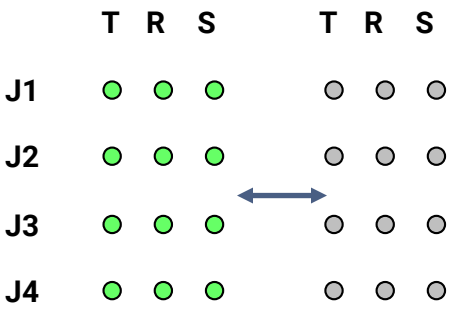
When the USB-based operation listed above is performed, the RICI software is automatically stopped for the update process. The RICI will need to be rebooted as the last step of the procedure for each of these USB operations, at which time the RICI software will automatically restart.

The LED indications do not apply to XML-only updates or to copying data files to the USB drive.

In the subsections that follow, diagrams depict how the LEDs for each row (**J1** - **J4**) and column (**TD/RD**, **RD/TD**, **SYNC**) are lit – green, red, or off (shown in grey in each diagram) – for the USB update notification.

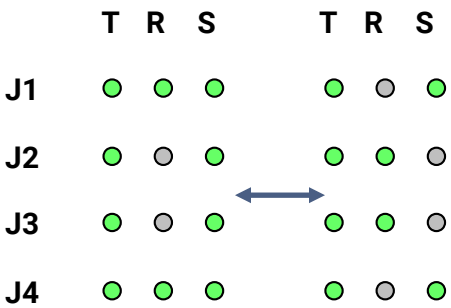
8.1.1 RICI "Update In Progress" Indication

LEDs alternate between all ON and all OFF when an update via USB flash drive is in progress:



8.1.2 RICI "Update Complete" Indication

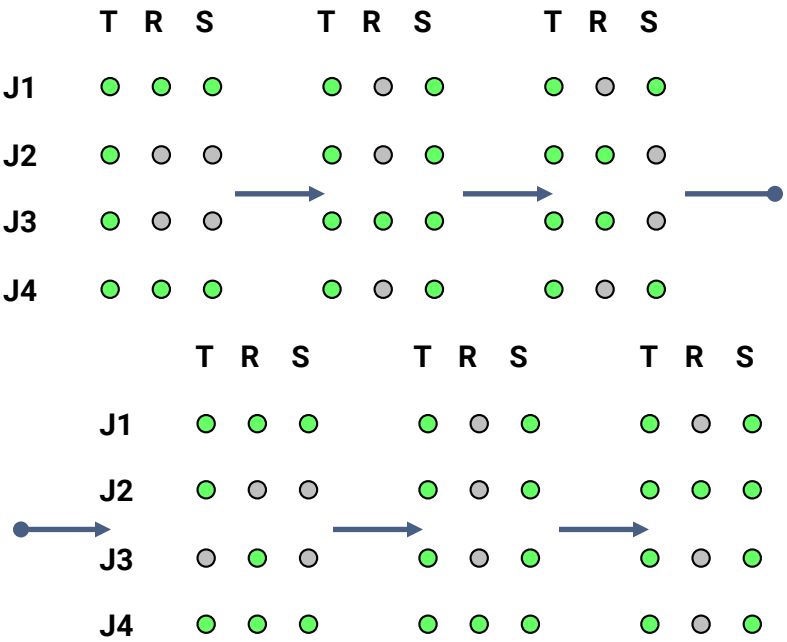
When the contents of the USB have been copied successfully, the LEDs alternate between **O** and **K** ("**OK**"):



8.1.3 RICI USB "Checksum Error" Indication

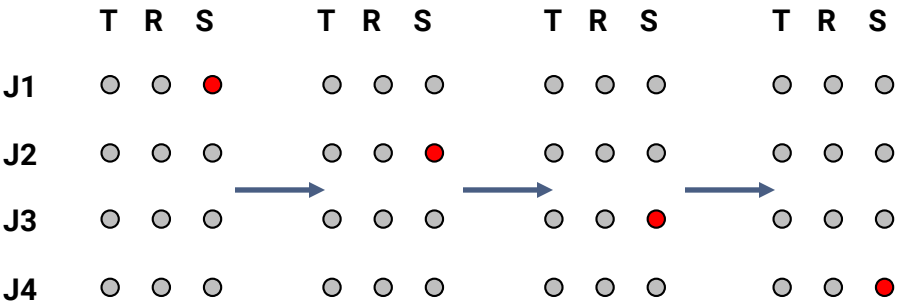
The checksum works by concatenating all the files together in the build and creating a single MD5 checksum, which is also included in the build. When this file is installed, the installation script concatenates only the files that were in the tar file (so that user-added files are not counted), and creates the *install_chksum* file.

If the two files do not match on the initial boot up, the LEDs will continually display **C**, **H**, **K**, **S**, **U**, and **M** ("**CHKSUM**") until the RICI is rebooted. If the files do not match on subsequent reboots, the letters in "**CHKSUM**" are displayed five times, and then the RICI will attempt to start:



8.1.4 RICI USB "Error" Indication

If an error other than a checksum error occurs, the SYNC LEDs alternately walk a RED pattern from top to bottom:



8.2 Longport USB Update Notification

The Longport PCM provides visual feedback when applying updates via a USB flash drive. The **CH*x*RX and CH*x*TX** LEDs are employed to provide an indication of the status of the update(s).

The LED indications apply to the following USB-based operation: Longport software update (*longport_[version].sun*).

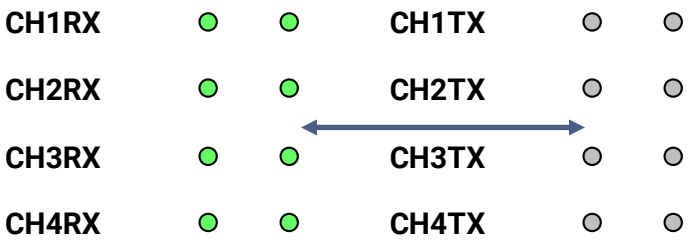
When the USB-based operations listed above are performed, the PCM software is automatically stopped for the update process. The PCM will need to be rebooted as the last step of the procedure for each of these USB operations, at which time the PCM software will automatically restart.

The LED indications do not apply to XML-only updates or to copying data files to the USB drive.

In the subsections that follow, diagrams depict how the LEDs for each row (**CH1*x*X**) and column are lit – green, red, or off (shown in grey in each diagram) – for the USB update notification.

8.2.1 Longport PCM "Update In Progress" Indication

LEDs alternate between all green and all off when an update via USB flash drive is in progress:

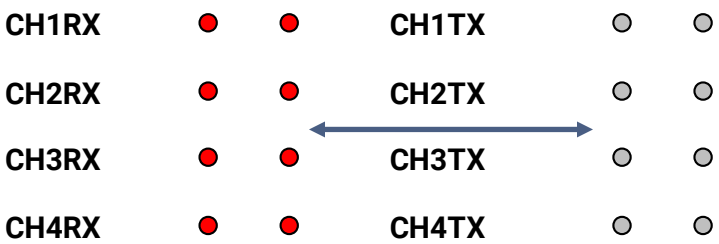


8.2.2 Longport PCM "Update Complete" Indication

When the contents of the USB have been copied successfully, the LEDs blink green in alternating columns:

8.2.3 Longport Error Indication

If an error other than a checksum error occurs, the transmit (**CH*x*TX**) and receive (**CH*x*RX**) LEDs alternate between all red and all off. If a checksum error occurs, only the receive LEDs alternate between all red and all off:



8.3 SGP Update Notification

USB flash drives are inserted into either of the USB slots located on the rear of the SGP. Though both USB ports are available, both ports should not be used concurrently to perform USB-based operations.

The following USB-based operations are available on the SGP:

- SGP software update (*upd_dcg.tar*, or, for version 6.0.1 or greater, *sgp_#_#_#.sun*, where *#* represents the version number)
- Configuration file updates (**.xml*)
- Download Log files (*dcgfile.tar*)
- Install software plug-in (**.so)*

When the software update and configuration file update USB-based operations are performed, the SGP will need to be rebooted as the last step of the procedure. The SGP software will automatically start after the hardware has been rebooted.

8.4 RICI and SGP Software Update

If a software update is issued by Sunhillo, a *platform_#_#_#.sun* file, where *platform* represents *rici* or *sgp*, respectively, and *#* indicates version number, is delivered to customers. The *sun* file can then be used to initiate an update as follows:

1. If necessary, copy the *platform_#_#_#.sun* file into the root directory of the USB drive (do not create a subfolder/directory on the USB flash drive for this file).
2. Insert the flash drive that contains the *platform_#_#_#.sun* file into the USB slot.
3. The LEDs will indicate the status (in progress, complete, or error) of the software update.
4. Remove the USB flash drive from the USB slot once the update is complete as indicated by the LEDs.
5. Reboot the device by powering off and then powering it back on.

For an alternate method of updating the software that does not involve the use of the USB flash drive, please refer to Section **6.1**.

8.5 Longport Software Update

If a PCM software update is issued by Sunhillo, a *longport_#_#_#.sun* file, where *#* indicates version number, is delivered to Longport customers. The tar file can then be used to initiate an update as follows:

1. If necessary, copy the *longport_#_#_#.sun* file into the root directory of the USB drive (do not create a subfolder/directory on the USB flash drive for this file).
2. Insert the flash drive that contains the *longport_#_#_#.sun* file into the USB slot.
3. The LEDs will indicate the status (in progress, complete, or error) of the software update.
4. Remove the USB flash drive from the USB slot once the update is complete as indicated by the LEDs.
5. Reboot the PCM by pressing the **Reset** button on the front panel.

The application software on the PCM is stopped during the software update process. Therefore the PCM will not process any serial or LAN data until the module is manually rebooted. The version of the application software can be verified using the Longport GUI.

For an alternate method of updating the Longport software that does not involve the use of the USB flash drive, please refer to Section **6.1**.

8.6 Load Configuration File

If a new configuration file is supplied by Sunhillo or created by the user, the configuration file (with file extension *.xml*) can be copied to the device as follows:

1. If necessary, copy the **.xml* file into the root directory of the USB drive, i.e., do not create a subfolder/directory on the USB flash drive for this file.
2. Insert the flash drive that contains the **.xml* file into the USB slot and wait approximately 10 seconds. The USB light will be steady ON when the load is complete.
3. Remove the USB flash drive from the USB slot.

If a configuration file created on a device is to be used on other of the same device type, the configuration file can be retrieved from the *DATA.tar* file, which was downloaded from the device using the GUI option (refer to Section **2.2.3**) or by inserting a blank USB flash drive into the device. The desired configuration file can be loaded on other device of the same type using the steps detailed earlier.

8.7 Download Log Files

If the *platform_#_#_#.sun* or **.xml* file is not present on the USB flash drive – which is true of the flash drive originally shipped with the device – the USB flash drive is considered to be in "download" mode. In download mode, the log files will automatically be written to the USB flash drive once it is inserted into the USB port. The file download process takes approximately 10 seconds, at which time the USB flash drive should be removed from the USB port.

8.7.1 RICI and Longport Log Files

The *ricifile.tar* log file contains useful log files for troubleshooting the unit. The log files can be downloaded from the GUI or by inserting a blank USB stick into the respective port on device and waiting 30 seconds for the download to complete. The log file can be downloaded via the STUI on the device or from the GUI. The *ricifile.tar* can be opened for file extraction with free, third party tools on Windows such as *WinRAR* or *7-Zip*.

Table 8-1 shows particularly useful files in *ricifile.tar* and their purpose.

Table 8-1: Useful RICI, Longport, and Ventnor Log Files and Locations

File and Location	Description
/home/dcg/version	Current Installed Software Version
/home/dcg/sys.ver	Current Installed Operating System Version and Model Identification
/home/dcg/activeFile	Current Active XML Configuration File
/home/dcg/*.xml	All XML files loaded on the unit exist in the log file
/home/dcg/SystemConfig/systemConfig.xml	Exportable Network Profile of the Unit (can be imported to another unit to copy over or clone *Network Config* settings to another unit via **Upload Data** feature)
/home/dcg/radar.ini	Custom Tracker tuner file (the *radar.ini* file's contents will vary depending on the customer's tracker requirements—it is a custom setup by Sunhillo)
/var/tmp/.psar *or* .dat *or* .pcap	Data Recording files
/var/tmp/POST_LOG.log	POST results
/var/tmp/license.log	License Codes installed on unit
/tmp/sn.txt	Unit Serial Number and Board Revision
/tmp/netinfo.txt	Network Settings Information (IP addresses of the unit)
/proc/mpsprotem	MPS debug information when configured in MPS mode
/etc/hosts	DNS settings (if configured)
/etc/network/interfaces	Network configuration

8.7.2 SGP Log File

The *dcgfile.tar* log file contains useful log files for troubleshooting the unit. The log files can be downloaded from the GUI or by inserting a blank USB stick into the device and waiting 30 seconds for the download to complete. The log file can be downloaded via STUI or from the GUI. The *dcgfile.tar* can be opened for file extraction with free, third party tools on Windows such as *WinRAR* or *7-Zip*.

Table 8-2 shows particularly useful files in *dcgfile.tar* and their purpose:

Table 8-2: Useful SGP Log Files and Locations

File and Location	Description
/home/dcg/version	Current Installed Software Version
/home/dcg/activeFile	Current Active XML Configuration File
/home/dcg/*.xml	All XML files loaded on the unit exist in the log file
/home/dcg/SystemConfig/systemConfig.xml	Exportable Network Profile of the Unit (can be imported to another unit to copy over or clone *Network Config* settings to another unit via **Upload Data** feature)
/home/dcg/radar.ini	Custom Tracker tuner file (the *radar.ini* file's contents will vary depending on the customer's tracker requirements—it is a custom setup by Sunhillo)
/var/tmp/.psar *or* .dat *or* .pcap	Data Recording files
/var/tmp/POST_LOG.log	POST results
/var/tmp/license.log	License Codes installed on unit
/tmp/sn.txt	Unit Serial Number and Board Revision
/var/tmp/osversion	Operating System version currently installed on the SGP
/etc/sysconfig/network-scripts/ifcfg-eth* (where * is 0 up to 5)	IP Address info currently configured on the SGP for each NIC)
/etc/sysconfig/route-eth* (where * is 0 up to 5)	Routes configured on the SGP for each NIC

8.8 Install Software Plug-in

If a software plug-in is to be installed on the device, the specific plug-in file, with file extension *.so*, is provided by Sunhillo. The plug-in can be installed on the device using a USB flash drive as follows:

1. Copy **.so* into the root directory of the flash drive, i.e., do not create a subfolder/directory on the USB flash drive for this file.

2. Insert the flash drive that contains **.so* the file into the USB slot and wait approximately 10 seconds. The USB light will be steady ON when the load is complete.

3. Remove the flash drive from the USB slot when the light on the flash drive is no longer flashing.

To verify the plug-in was installed successfully, perform the following steps:

4. Login to the device's GUI.
5. From the main menu, select **About** from the *System* menu.
6. Verify the plug-in is shown on the screen under the *Plugins Loaded* Section.

Refer to the manual that was provided with the software plug-in for configuration details and usage information. Once the plug-in has been configured as per the instructions in the manual, the device will need to be rebooted.

This page is intentionally left blank.

Section 9

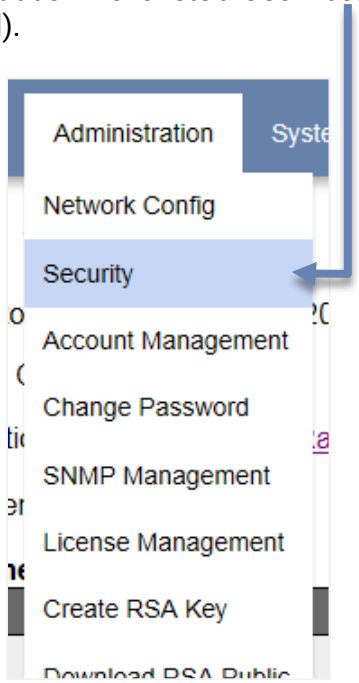
9. SECURITY FEATURES

In this Section, you learn about SureLine Core's services, login options, and other features related to security and Information Assurance.

The SureLine Core device may be used in an environment where access via the LAN must be limited and secure. The device provides security features and integrity checking for secure environments. Although the device does not have a National Information Assurance Partnership (NIAP) certification, the security features are modeled after the Common Criteria Network Device Protection Profile (NDPP).

9.1 Services and Login Options

Selecting **Security** from the *Administration* menu lists the services and login options that are enabled (checked) or disabled (not checked).



Under **Services** (**Figure 9-1**), the options are: **FTP**, **HTTPS**, **KML**, **SSH/SFTP**, **NTP**, **Telnet**, **SNMP**, and **USB**. Under **Login Options**, the options are: **Complex Passwords**, which requires that all users create strong passwords (refer to Section **9.1.3**), and **Login Banner**, which displays the text specified under *Banner Text* after a user clicks the **Log In** link (refer to Section **2.3.2**). Any changes are saved after click the **Save** button.

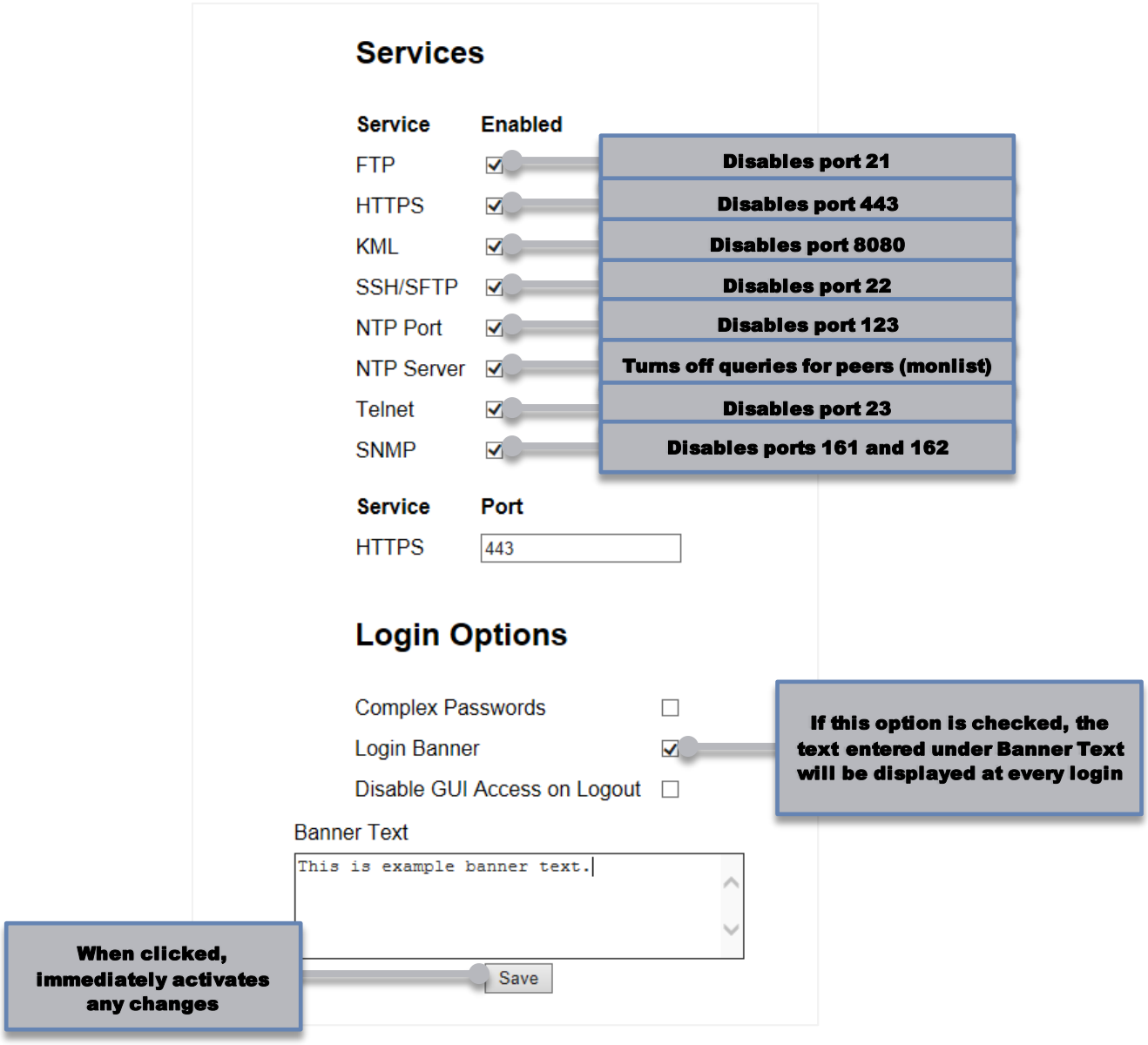


Figure 9-1: Services and Login Security Options

9.1.1 Service Control

The services shown in **Figure 9-1** control how the device can be accessed remotely. The administrator of the device can determine how the unit can be accessed by only enabling those services deemed acceptable in a particular environment. Care must be taken when selecting services to disable as it is possible to make the device non-accessible if all options are disabled.

Note

Disabling HTTPS eliminates access to the Web displays normally used for configuration.

9.1.2 Login Options

The **Login Options** shown in **Figure 9-1** provide additional control on how the device handles logins.

9.1.3 Complex Passwords

Enabling complex passwords ensures the following rules are met for new passwords entered:

- Minimum length (based on setting; see Section **5.1.5**)
- One lower case letter (alphabetic: **a b c d**, etc.)
- One upper case letter (alphabetic: **A B C D**, etc.)
- One number (numeric: **0 1 2 3**, etc.)
- One special character (**! @ # $ % ^ & * , +**)

9.1.4 Login Banner

The login banner feature is enabled or disabled via the **Login Banner** check box. If enabled, the text in the **Banner Text** will be displayed each time a user selects **Login**. Banner text can be up to 1,023 characters.

9.2 Lock-down Settings

The default shipping configuration leaves the security settings open for general use and setup. This section provides suggested security feature settings for secure environments.

The settings shown in **Figure 9-2** indicate the suggested lock-down configuration. In this configuration, the only means of access to the device is through the HTTPS GUI. In addition, the HTTPS port should be changed to something other than 443 and, if SNMP is required, SNMP V3 should be enabled (see Section **10**). Alternatively, for low bandwidth environments, SSH can be checked to provide a text user interface over a secured connection terminal (see Section **6.5** for more information on STUI).

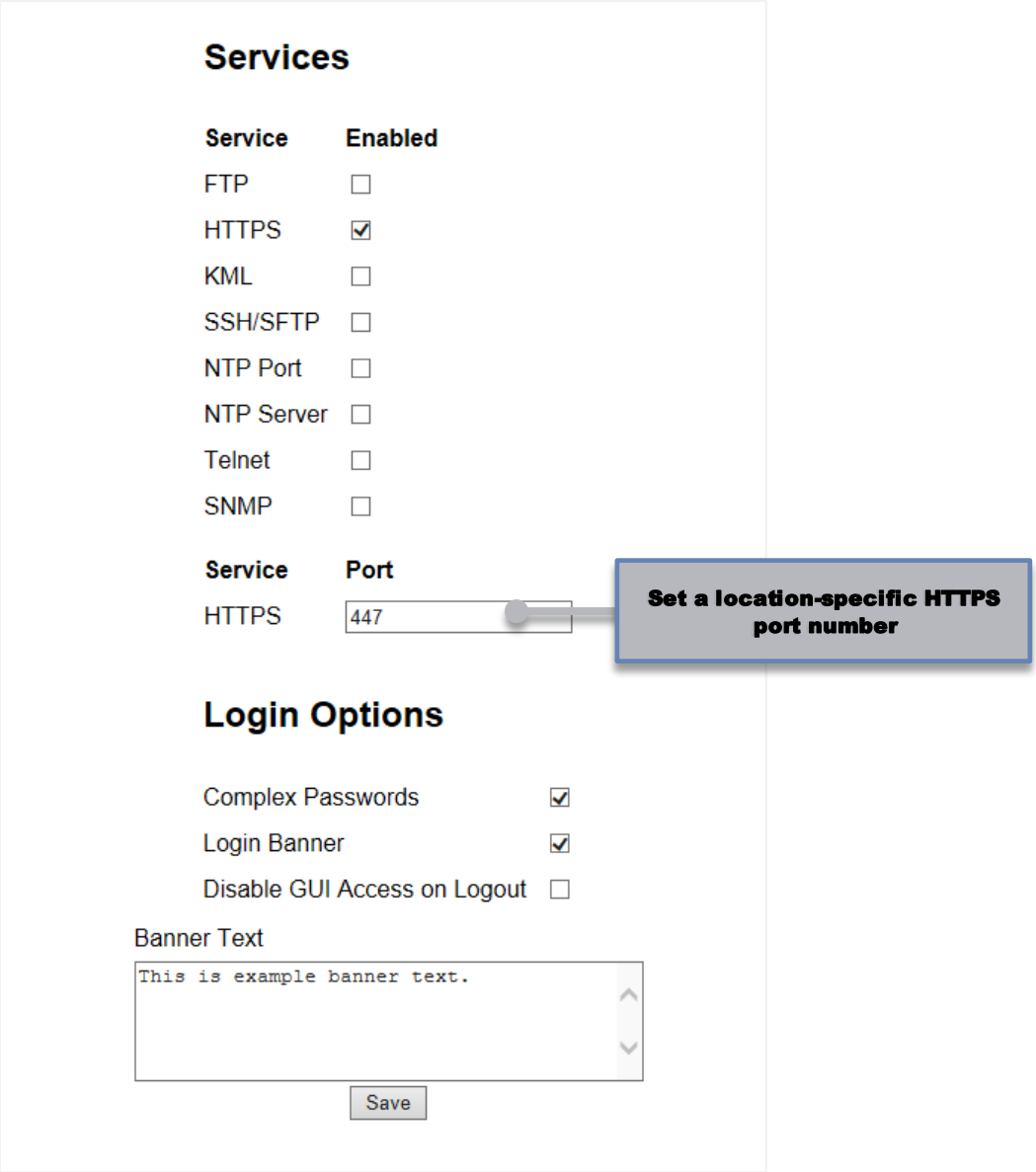


Figure 9-2: Suggested Services and Login Security Options

The final aspect of securing the device environment requires that User Management be accessed. Here the primary factors to consider are:

- Minimum Password Length – Established by local security group
- Password Expiration – Should be non-zero
- User Group – Established by local security group

Refer to Section **5.1.5** for more information on changing password settings.

Section 10

10. SNMP SUPPORT

In this Section, you learn about remote interactions with the SureLine Core device in SNMP.

The SureLine Core device may be used in an environment in which physical access to the hardware or access via the LAN network is, or must be, limited. The device provides software tools and an SNMP agent to allow the user to interact with the device remotely.

An SNMP manager can poll the unit for device/network statistics and information, and run a set of commands. Traps are generated (if configured) for changes in status of the unit, network, and serial devices.

The device MIB, *SUNDCGR-MIB.txt*, is provided with the software release in the *upd_fs.tar* or *platform_#_#_#.sun* file provided by Sunhillo. The *SUNDCGR-MIB.txt* file should be downloaded from the Web GUI using the **Download MIB** button (see Section **2.2.4**). Each time a new software version is released, the device MIB file should be updated on the user's SNMP manager also.

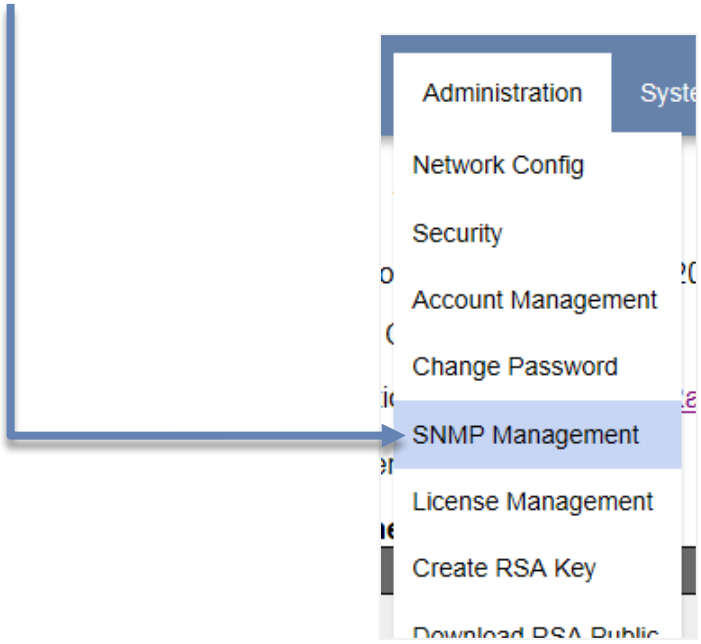
The default community names for SNMP access are:

- **public** – read-only. This is for SNMP **get** commands.
- **sunhillo** – read-write. This is for SNMP **get** and **set** commands.

The community names must be configured on the user's SNMP manager. The community names can be changed (for security reasons) by using an SNMP **set** command.

10.1 SNMP Management

SNMP V2 and V3 communities and users, respectively, can be modified or created by selecting **SNMP Management** from the *Administration* menu.



After selection, the *SNMP Management* screen, shown in **Figure 10-1**, is displayed.

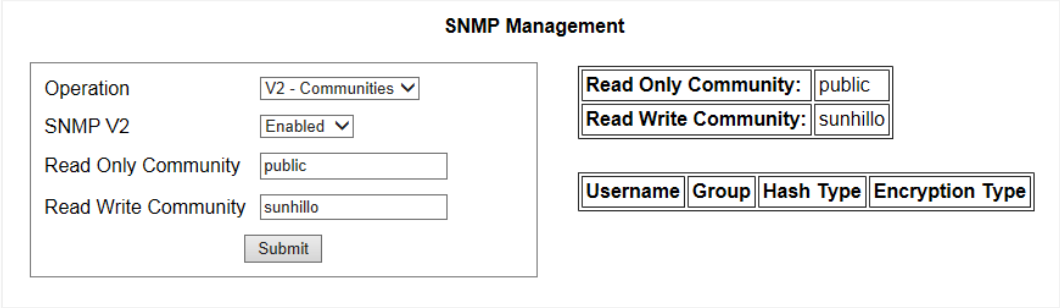


Figure 10-1: SNMP Management Screen

The available options under **Operation**, *V2 - Communities*, *V3 - Add User*, and *V3 - Delete User* are described in the subsections that follow.

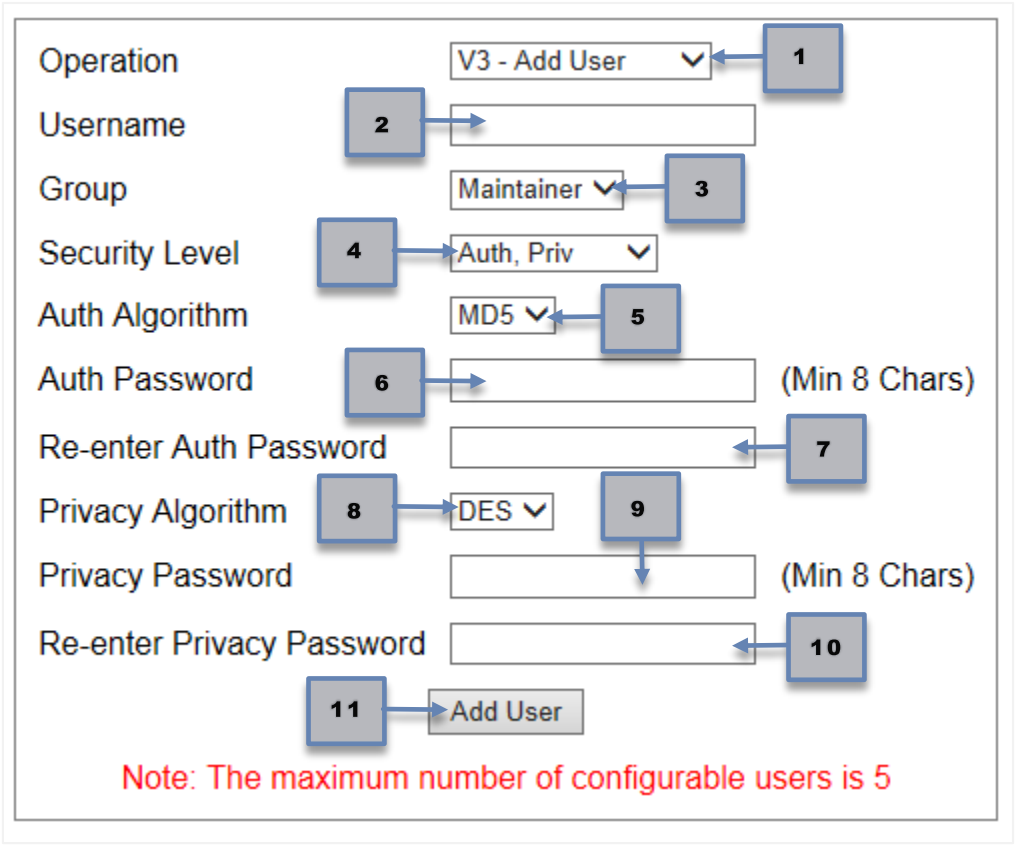
10.1.1 V2 - Communities

For the *V2 - Communities* **Operation** (**Figure 10-1**), the SNMP V2 **Read Only Community** and **Read Write Community** names can be changed from the respective defaults of **public** and **sunhillo**.

By default, **SNMP V2** is set to **Enabled**. If set to **Disabled**, it will no longer be possible to do any *gets* or *sets* using SNMP V2 communities.

10.1.2 V3 - Add User

For SNMP V3 to work, at least one user must be added. To add a new SNMP V3 user – up to a maximum of 5 – do the following:

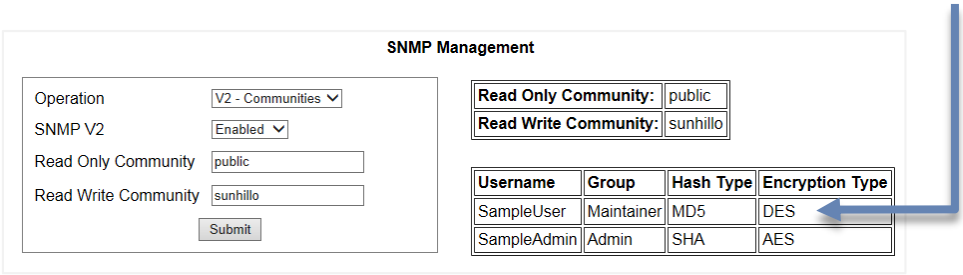


1. Select *V3 - Add User* under **Operation**.
2. Using only letters or numbers, enter a **Username**.
3. Select **Group** between the following:
   - *Admin*—Unrestricted. Can perform *gets* and *sets* across entire device.
   - *Maintainer*—Can only do *gets* and *sets* on device MIB.
   - *Operator*—Can only do *gets* on device MIB.
4. Select **Security Level**:
   - *Auth, No Priv*—Basic user password authentication.
   - *Auth, Priv*—Adds encryption and hashing to basic user password authentication.
5. Select **Auth Algorithm** between *MD5* or *SHA*.

6. Select **Auth Password**, which needs to be a minimum of eight characters.
7. Enter the same password from step **6** under **Re-enter Auth Password**.
8. Select a **Privacy Algorithm** between *DES* or *AES*.
9. Set a **Privacy Password**, which needs to be a minimum of eight characters.
10. Enter the same password from step **9** under **Re-enter Privacy Password**.
11. Click **Add User**.

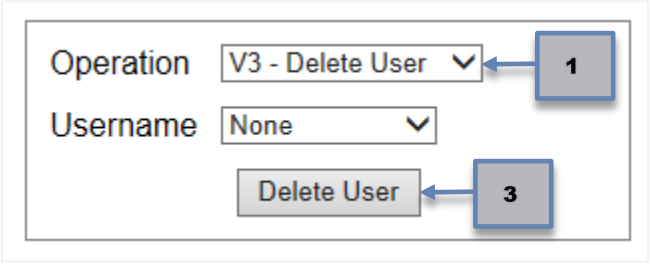
10.1.3 V3 - Delete User

To delete an SNMP V3 user, at least one user must have been previously added.

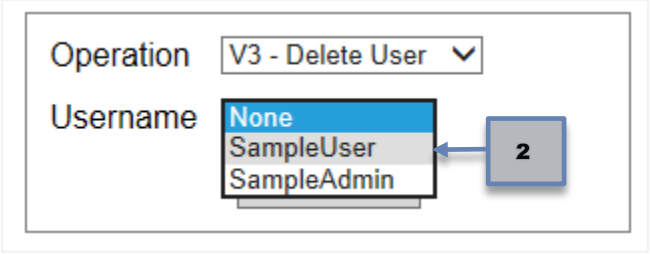


To delete an SNMP V3 user do the following:

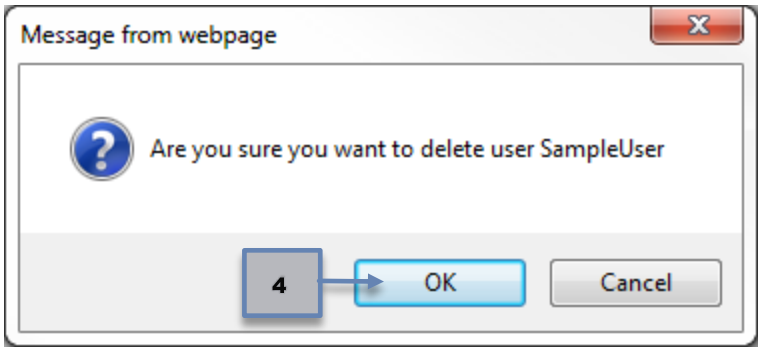
1. Select *V3 - Delete User* under **Operation**.



2. Select a user to be deleted under *Username*.



3. Click **Delete User**.
4. Click **OK**.



The user is now deleted from the table.

10.2 SNMP Objects

Table 10-1 summarizes the object groups available in the device MIB.

Note

Items marked in *italics* are for compatible Sunhillo equipment that provide serial port connectivity, but are not applicable on the SGP.

Table 10-1: Objects Groups Available in SGP MIB Summary

Object Number	Object Name	Detail
1	dcgStatusAndIdentity	This group of objects provides the status of the system, the SW version, and configuration file currently in use. This group of objects also provides commands to restart, and set the system online or offline.
2	*dcgDeviceInfo*	This group of objects provides identification, status and accumulated statistics of each serial port device in the current configuration. For each serial port device the accumulated totals of number of messages in, number of messages out, bytes in, bytes out, and error counts are available.

Object Number	Object Name	Detail
3	dcgNetworkInfo	This group of objects is for identification, address, state, accumulated statistics and status of the Ethernet devices. For each Ethernet device the accumulated totals of number of messages in, number of messages out, bytes in and bytes out are available.
4	dcgLog	Generated when a message is written to the error log that is classified as requiring SNMP manager notification. This information is sent with a trap.
5	dcgTrap	This group of objects defines the fields used in the SNMP traps. See the table on the following page for a list of SNMP traps.
6	dcgGlobal	This group of objects refer to the entire system and define fields for use in statistics
7	dcgNetworkInterval	This group of objects is for network statistics and identification. The statistics are provided in intervals over a 24 hour period of time. The statistics available for the Ethernet devices are: number frames in, number of frames out, bytes in, and bytes out.
8	*dcgDeviceInterval*	This group of objects is for serial port device statistics and identification. The statistics are provided in intervals over a 24-hour period of time. The statistics available for each serial port device are: number of messages in, number of messages out, bytes in, bytes out, and errors counts.
9	dcgMiscOperations	This group of objects is for miscellaneous operations. These operations include transferring files to the system and supporting the sending of text commands to the operational software (dcgOperationalCmd). dcgOperationalCmd – GET – Shows the last command processed. dcgOperationalCmd – SET – Allows the user to send text commands to the operational software.

10.3 SNMP Traps

The SNMP traps issued by the system and described in the MIB are summarized in **Table 10-2**.

Table 10-2: SNMP Traps Issued by System Summary

Trap #	Trap Name	Description	Detail
1	dcgSystemStatusChange	On its own, this trap is generated when the DCG completes initialization. Sending simulates this change.	Generated when the device completes initialization or system is goes down.
2	*dcgDeviceStateChange*	On its own, this trap is generated when there is a change in status of a device. Sending simulates this change.	Generated when a device (serial ports J1-J4) changes status.
3	dcgNICStateChange	On its own, this trap is generated when there is a change in state of a NIC. Sending simulates this change.	Generated when there is a change in the status of a NIC.
4	dcgErrorInfo	On its own, this trap is generated when there is a message written to the RICI/DCG error Log, and it is classified as an event that requires that notification be sent to the SNMP Manager.	Generated when a message is written to the error log that is classified as requiring SNMP manager notification. NOTE: This trap is not currently implemented.
5	dcgPrimaryRedundantLanChange	On its own, this trap is generated when a primary/redundant LAN data source is changed. Sending simulates this change.	Generated when primary/redundant LAN data source changes.

Trap #	Trap Name	Description	Detail
6	dcgSiteNoDataTimeOut	On its own, this trap is generated when a site does not receive any data after timeout. It is also generated when a site starts to receive data again. Sending simulates this timeout.	Generated when any of the configured Sites is no longer receiving data within the defined timeout. The text "site <SITENAME> is down" is reported. If data resumes on the site, this trap is sent with the text "site <SITENAME> is up"
7	dcgGeneralInfo	On its own, this trap is generated for events such as security issues, etc. Sending simulates this scenario.	Generated for security issues (such as, file integrity check).

10.4 SNMP Get/Set Commands

Table 10-3 summarizes the SNMP commands available in the MIB.

Table 10-3: Available SNMP Commands Summary

Get/Set	Command Name	Description
Get	dcgConfiguration	Returns the name of the configuration file in use.
Set		Commands the system to use the configuration file sent in the command. The configuration file must already reside on the system. The system must be set OFFLINE and ONLINE in order for the new configuration to become active.
Set	dcgCountReset	Sets ALL counts to zero.
Get	dcgFileTransfer	Returns the status of the file transfer operation with a timestamp.
Get	dcgMessageThrottling	Returns the enable (1)/disable(0) status of message throttling.
Set		Enables/Disables message throttling.
Get	dcgMessageThrottlingLanInput	Returns the Ethernet port used for input messages subject to message throttling. 0 = Eth0, 1 = Eth1.

Get/Set	Command Name	Description
Set		Sets the Ethernet port – 0 or 1 – used for input messages subject to message throttling.
Get	dcgMessageThrottlingPortsDisable	Returns the disabled ports: port 1 = 1, port 2 = 2, port 3 = 4, and port 4 = 8.
Set		Disables a port(s): port 1 = 1, port 2 = 2, port 3 = 4, and port 4 = 8.
Get	dcgMessageThrottlingPortsEnable	Returns the enabled ports: port 1 = 1, port 2 = 2, port 3 = 4, and port 4 = 8.
Set		Enables a port(s): port 1 = 1, port 2 = 2, port 3 = 4, and port 4 = 8.
Get	dcgMessageThrottlingStats	Returns the queue depth, message drop counts, and TIS message drop counts (in that order).
Get	dcgOperationalCmd	The dcgOperationalCmd portion of the MIB is used when Command Processor is Enabled under the SNMP dialog of software to control RTS: dcgOperationalCmd Syntax for SET: RTS <COMMAND> <PORT 1-4> <ON/OFF> **Example 1**: RTS STATUS 1 (ON/OFF not needed here – get status of port 1). **Example 2**: RTS OVERRIDE 1 ON (turns override for port 1 on – turns RTS on). **Example 3**: RTS SET 1 OFF (turns off the RTS signal for port 1).
Set		
Get	dcgPreOverloadThreshold	Returns the pre-overload threshold value (queue monitoring).
Set		Sets the pre-overload threshold value (queue monitoring).
Set	dcgRestart	Commands the application to perform a hardware reboot.
Get	dcgReturnToNormalThreshold	Returns the queue monitoring return to normal threshold.
Set		Sets the queue monitoring return to pre-overload threshold.
Get	dcgReturnToPreoverloadThreshold	Returns the queue monitoring return to pre-overload threshold.
Set		Sets the queue monitoring return to normal threshold.
Get	dcgROCommunity	Returns the read-only community name.

Get/Set	Command Name	Description
Set		Sets the read-only community name to new string value (a single word). The system must be restarted in order for the new community name to take effect. The read-only community name must be different from the read-write community name.
Get	dcgRWCommunity	Returns the read-write community name.
Set		Sets the read-write community name to new string value (a single word). The system must be restarted in order for the new community name to take effect. The read-write community name must be different from the read-only community name.
Set	dcgSetOffline	Commands the system to the OFFLINE state. The application SW will stop running.
Set	dcgSetOnline	Commands the system to the ONLINE state. The application SW will execute.
Get	dcgStatus	Returns an integer value that describes the current status of the application software. Values are: • dcgStatusOffline(0) – Application SW is not running • dcgStatusStandby(1) – Processor is functioning as a backup system, SW is running but as backup system. • dcgStatusOnline(2) – Application SW is running • dcgStatusDegraded(3) – Application SW is running, but errors were encountered • dcgStatusFailed(4) – Application SW failed to initialize or configuration file error detected on software startup.
Set	dcgSwitchOverMode	Returns the current processor type in switchover mode. Values are: • dcgSwitchOverModeNone(0) • dcgSwitchOverModePrimary(1) • dcgSwitchOverModeBackup(2)
Get	dcgTisThreshold	Returns the TIS threshold value (seconds).
Set		Sets the TIS threshold. Value is in seconds.
Get	dcgTrapCommunity	Returns the trap read-write community string.

Get/Set	Command Name	Description
Set		Sets the trap read-write community name to new string value (a single word). The system must be restarted (**dcgRestart** command) in order for the new community name to take effect.
Get	dcgUpTime	Returns the time in seconds since the system was last re-initialized.
Get	dcgVersion	Returns the application SW version. Only valid when system status is Online or Standby.

10.5 Common Remote Access and SNMP Usage

This Section details the steps for how to use the remote access tools and SNMP for particular scenarios and recommended usage.

10.5.1 Recommended SNMP Gets

The SNMP agent provides numerous commands to retrieve (get) information and statistics about the device and the data in and out of the system. This subsection documents a few of the recommended get commands that can be used to monitor the device for proper function and information. The user is not limited to only these commands, having, if desired, access to the full functionality of the device MIB.

10.5.1.1 System Status

The system status can be polled via SNMP can be polled every 5 - 10 seconds to monitor overall system status. The SNMP get command is **dcgStatusAndIdentity**, **dcgStatus**.

The status values of "Online" or "Standby" indicate the device is functioning properly with no detected errors. The application software is running either as PRIMARY or standalone ("online"), or BACKUP ("standby") system.

The status value of "Offline" indicates the system application software is not running, although the hardware is powered on and functioning. The device is in this state due to some user interaction and the software application can be started using the **dcgStatusAndIdentity**, **dcgSetOnline** command.

If the status is "degraded," meaning either the serial or NIC device has encountered an error:

- More information on serial devices can be obtained by polling each device and obtaining the following information:
  - Get serial device state to check if error condition is set.
  - Get serial device status to check for the cause of the error.

- More information on the NIC devices can be obtained by polling each device and obtaining the following information:
  - Get NIC device state to check if error condition is set.
  - Get NIC device status to check for the cause of the error.
- If configured for Traps, a trap, i.e., **dcgDeviceStatusChange** or **dcgNICStatusChange**, was also sent from the device to indicate some kind of error. Further information can be obtained from these trap messages about the cause of the device status change.

The "failed" status indicates a fatal software application error has occurred and is not running. This usually occurs because the active configuration file contains errors. The Event Log will contain details on the reason for the failure.

10.5.1.2 Data Message Counts

The message counts in and out on the serial and NIC devices are a means to verify proper data processing of the device. The system status may indicate the software and hardware is well, but it is recommended to verify data is being received and processed by the device.

The applicable serial and NIC devices message in and out counts can be polled every five to 10 minutes to verify data is being received and processed, i.e., the counts are increasing, and the amount of data being processed is acceptable.

The message count information for the serial devices can be found in the **dcgDeviceInfo** MIB object. The message count information for the NIC devices can be found in the **dcgNetworkInfo** MIB object.

Appendix A

A1. CONFIGURATION EXAMPLES (SERIAL PLATFORMS)

This Section provides several examples of creating from scratch or editing existing configuration files on SureLine Core serial platforms, including RICI, Longport, and Ventnor. Each example mirrors common user data flow configurations and demonstrates some of the features and functionality available from the configuration GUI to create/edit the data flow. Each example will walk through, step-by-step, what is needed to create a data flow. Figures are provided when necessary to highlight a specific operation or clarify a step in the process.

The samples provided here are provided as examples only. If you desire, you can walk through these examples step-by-step using the GUI as an exercise to gain understanding and increase your familiarity in editing configuration files, and particularly, a data flow.

The follow examples are provided:

- LAN data in – Serial data out (Single data path).
- Multiple LAN data inputs – Multiple serial data output (two data paths).
- LAN data in with Site Filtering to multiple serial data outputs.
- Multiple serial data in – Single LAN data output.
- Single serial data in with data conversion – Multiple LAN data out.
- LAN data in with site filtering – Multiple LAN data out.

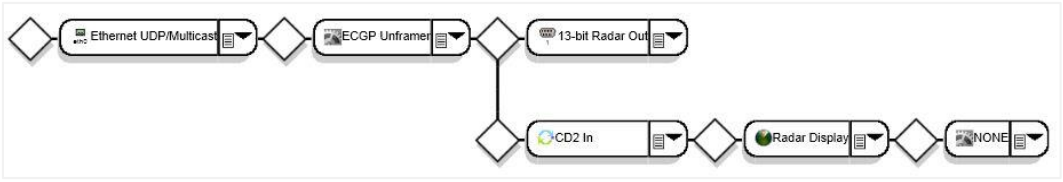
A1.1 Example #1: LAN Input to Serial Output (Single Path)

The configuration in example #1 should contain the following elements:

- Multicast LAN data input on Ethernet port 0 from 239.1.1.6 port 9507

- Incoming CD-2 radar data in ECGP format from ARTCC ZNY
- Data from site XYZ should be displayed using the Radar Display feature
- Radar output channel 1 in 13 bit radar format on serial port #1
- External baud rate

The final data flow will look like this:



To create the data flow described above the following steps are performed:

1. From the menu bar, select **Configuration**, **New**. Choose the *_lan_to_4_chan_13_bit_serial* file.

   This file provides the following template:

2. Click on the first node of type *Ethernet UDP/Multicast*. Change the following configuration parameters:

   a) Type “LAN_in” for the **Logical Name**.

   b) Enter “9507” for **Multicast port number**.

   c) Enter “239.1.1.6” for **Multicast Receive IP Address**.

   d) Choose “Eth0” for **Multicast NIC**.

   e) Click **OK** to exit the configuration parameters screen.

3. Mouse-click on the second node of type *ECGP Unframer*. Change the following configuration parameters:

   a) Type “ECGP_from_ZNY” for **Logical name**.

   b) Type “ZNY” for **ARTCC Name**.

   c) Choose “ARTCC Name” for **ARTCC Filter**.

   d) Click **OK** to exit the configuration parameters screen.

Note

The template file has all 4 serial ports in use. This configuration only uses a single port. The OUTPUT node is the correct node type, but the configuration parameters must be edited.

4. Click on the *13 Bit Radar Out* node. Change the following configuration parameters:

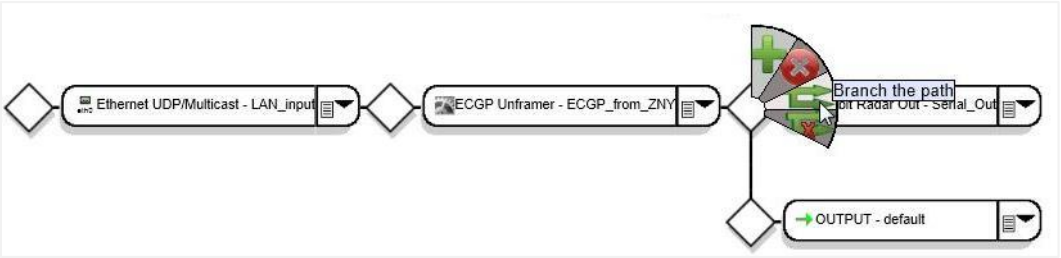
   a) Choose "None" for **Channel 2**, **Channel 3**, and **Channel 4**.

   b) Choose "External" for **Baud Rate**.

Note

The current data flow does not have a *Radar Display* node type; therefore, another node must be added to the existing data flow. It is recommended that a graphical display type node, such as *Radar Display*, be added to the data flow in a separate branch of data path which is not in the critical data processing stream.

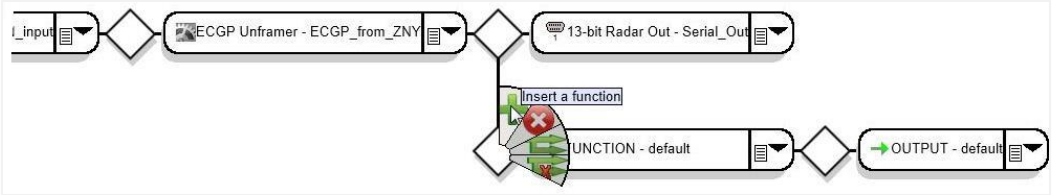
5. Mouse-over on the diamond connector after *ECGP Unframer* node. Select the "Branch the path" option. A duplicate of the data path from where the branch was initiated is created. This path is populated with "dummy" nodes, which must be configured.



Note

The new data path does not have a FUNCTION node type; therefore, another node must be added to the existing data path.

6. Mouse-over on the diamond connector before the OUTPUT node. Select the "Insert a function" option. A generic node of FUNCTION type with default name is inserted in the data flow.



Note

The *Radar Display* node type requires a prerequisite node type prior to it in the data flow. Before a *Radar Display* can be added to the data flow, the node type *CD2 In* must be configured.

7. Select the node dropdown list on the new node. Choose **Input Radar Types**, **CD2 In**.

8. Click on the node. Enter "for_display" for **Logical name**. Click **OK** to exit the configuration parameter screen and save the settings.

Note

The *Radar Display* node can be inserted into the data flow now. You may have to scroll to the right to see all the nodes in the data flow path.

9. Mouse-over on the diamond connector after "CD2 In" node. Select the "Insert a Function" option. A generic node of FUNCTION type with default name is inserted in the data flow.

10. Select the node dropdown list on the new node. Choose **Utilities**, **Radar Display**.

11. Click on the node. Enter "site_xyz" for **Logical name**. Type "XYZ" for **Site Name** to display. Click **OK** to exit the configuration parameter screen and save the settings.

Note

For this data path there is no actual data output. Though, be design, each data path has to have an OUTPUT node. In this case, the OUTPUT node type must be set to "NONE" to indicate this is the end of this data path.

12. On the OUTPUT node, select the node dropdown list. Choose **Other**, **NONE**.

Note

Saving a configuration often is recommended. Though not specifically performed during this example, a configuration should be saved to a file during editing/creating so as not to lose any information.

13. Select **Save File As** button at the bottom of the screen. Enter the file name “doc_example1” and click **OK**.

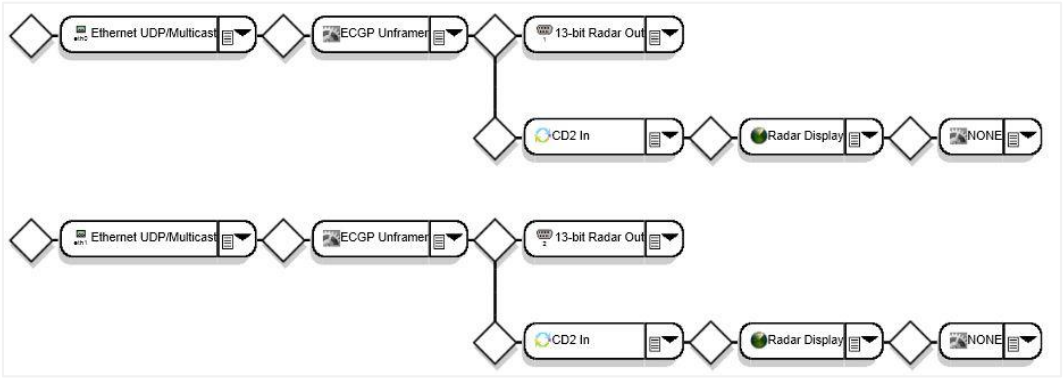
A1.2 Example #2: Multiple LAN input to Multiple Serial Output

This example is an exercise in creating a data flow with multiple inputs to multiple outputs. This example is based on example #1 to create two different data paths for the data flow.

The configuration in example #2 should contain the following elements:

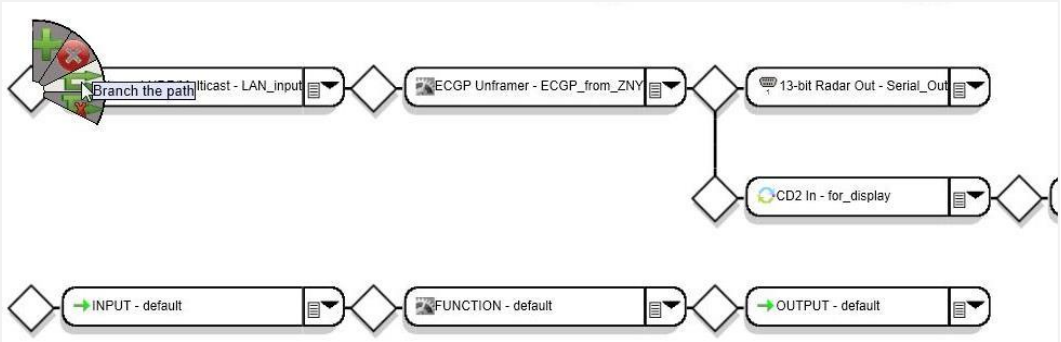
- Configuration from example #1.
- Multicast LAN data input on Ethernet port 1 from 239.1.1.5 port 9510.
- Incoming CD-2 radar data in ECGP format from ARTCC ZOB.
- Data from site PHL should be displayed using the Radar Display feature.
- Radar output channel 1 in 13 bit radar format on serial port #2.
- External baud rate.

The final data flow will look like this:



To create the data flow described above the following steps are performed:

1. From the menu bar, select **Configuration**, **Edit**. Choose the file *doc_example1*.
2. Mouse-over the first diamond connector. Select “Branch” from the fan control. The GUI creates a duplicate of the data path from where the branch was initiated. The nodes are setup with “dummy” values and must be configured by the user.



3. Select the node dropdown list on the INPUT node. Choose **LAN**, **Ethernet UDP/Multicast**.
4. Click on the node. Change the following configuration parameters:
   a) Type “LAN_input2” for the **Logical Name**.
   b) Enter “9510” for **Multicast port number**.
   c) Enter “239.1.1.5” for **Multicast Receive IP Address**.
   d) Choose “Eth1” for **Multicast NIC**.
   e) Click **OK** to exit the configuration parameters screen.
5. Select the node dropdown list on the second node in the path (a FUNCTION node). Choose **Framers/Unframers**, **ECGP Unframer**.
6. Mouse-click on this node and change the following configuration parameters:
   a) Type “ECGP_from_ZOB” for **Logical name**.
   b) Type “ZOB” for **ARTCC Name**.
   c) Choose “ARTCC Name” for **ARTCC Filter**.
   d) Click **OK** to exit the configuration parameters screen.
7. Select the node dropdown list on the third node (OUTPUT node). Choose **Serial**, **13 Bit Radar Out**.
8. Click on the *13 Bit Radar Out* node. Change the following configuration parameters:
   a) Choose “Port2” for **Channel 1**.
   b) Choose “External” for **Baud Rate**.
   c) Click **OK** to exit parameter screen.

9. Mouse-over on the diamond connector after *ECGP Unframer* node. Select the "Branch the path" option. A duplicate of the data path from where the branch was initiated is created. This path is populated with "dummy" nodes which must be configured.

Note

The new data path does not have a "Radar Display" node type; therefore, another node must be added to the existing data path.

10. Mouse-over on the diamond connector before the OUTPUT node. Select the "Insert a function" option. A generic node of FUNCTION type with default name is inserted in the data flow.

Note

The *Radar Display* node type requires a prerequisite node type prior to it in the data flow. Before a *Radar Display* can be added to the data flow, the node type *CD2 In* must be inserted.

11. Select the node dropdown list on the new node. Choose **Input Radar Types**, **CD2 In**.

12. Click on the node. Enter "for_display2" for **Logical name**. Click **OK** to exit the configuration parameter screen and save the settings.

Note

The *Radar Display* node can be inserted into the data flow now. You may have to scroll to the right to see all the nodes in the data flow path.

13. Mouse-over on the diamond connector after *CD2 In* node. Select the "Insert a Function" option. A generic node of FUNCTION type with default name is inserted in the data flow.

14. Select the node dropdown list on the new node. Choose **Utilities**, **Radar Display**.

15. Click on the node. Enter "site_phl" for **Logical name**. Type "PHL" for **Site Name** to display. Click **OK** to exit the configuration parameter screen and save the settings.

Note

For this data path there is no actual data output. Though, by design, each data path has to have an OUTPUT node. In this case, the OUTPUT node type must be set to "NONE" to indicate this is the end of this data path.

16. On the OUTPUT node, select the node dropdown list. Choose **Other**, **NONE**.

17. Select **Save File As** button at the bottom of the screen. Enter the file name "doc_example2" and click **OK**.

Note

After the configuration file has been saved, another Sensor is automatically created by the GUI. This sensor is necessary for the serial port node type to operate correctly.

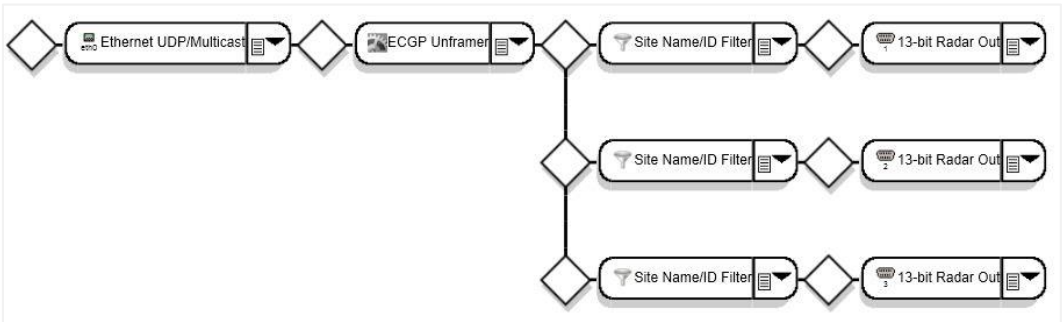
A1.3 Example #3: LAN Input to Multiple Serial Outputs with Site Filtering

This example is an exercise in creating a branch to send data from a single source to multiple outputs.

The configuration in example #3 should contain the following elements:

- Multicast LAN data input on Ethernet port 0 from 239.1.1.6 port 9507.
- Incoming CD-2 radar data in ECGP format from ARTCC ZNY.
- Radar site XYZ output channel 1 in 13 bit radar format on serial port #1.
- Radar site QRS output channel 1 in 13 bit radar format on serial port #2.
- Radar site KLM output channel 1 in 13 bit radar format on serial port #3.
- External baud rate.

The final data flow will look like this:



To create the data flow described above the following steps are performed:

1. From the menu bar, select **Configuration**, **Edit**. Choose the file *doc_example1*.

Note

The first two nodes in the data flow are configured correctly (refer to example #1). No changes are necessary. This data flow does not use a *Radar Display.* Therefore, the *CD2 In* function can be removed from the data path.

2. Mouse-over the diamond connector after the *ECGP Unframer* node. Select the "Delete a Function" option. The *CD2 In* function node type is removed from the data path.

Note

In order to send only data from a particular site out a serial port a *Site Name/ ID Filter* Function node must be used in the data path prior to the output.

3. On the fourth node in the data path, which is currently a *Radar Display* node type, select the node dropdown list. Choose **Filters**, **Site Name/ID Filter**.

4. Click on the node. Enter to following:

   a) Type "site_XYZ" for **Logical name**.

   b) Type "XYZ" for **Site Name**.

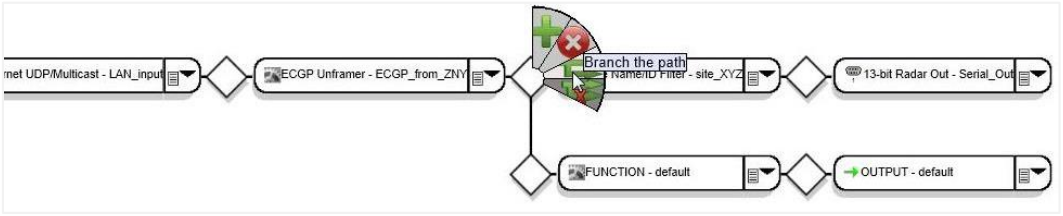
   c) Choose "Site name" for the **Site filter type**.

   d) Click **OK** to exit the configuration parameter screen and save the settings.

Note

To send particular sites to the other two serial ports, the data path must be branched after the ECGP data with a Site Name/ID Filter function for each serial output.

5. Mouse-over on the diamond connector after *ECGP Unframer* node (the third diamond connector). Select the "Branch the path" option. The GUI creates a duplicate of the data path from where the branch was initiated. The nodes are setup with "dummy" values and must be configured by the user.



6. Select the node dropdown list on the first node in the new branch. Choose **Filters**, **Site name/ID Filter**.

7. Click on the node. Enter to following:

   a) Type "site_QRS" for **Logical name**.

   b) Type "QRS" for **Site Name**.

   c) Choose "Site name" for the **Site filter type**.

   d) Click **OK** to exit the configuration parameter screen and save the settings.

8. Select the node dropdown list on the OUTPUT node (second node). Choose **Serial**, **13 Bit Radar Out**.

9. Click on the "13 Bit Radar Out" node. Change the following configuration parameters:

   a) Choose "Port2" for **Channel 1**.

   b) Choose "External" for **Baud Rate**.

   c) Click **OK** to exit parameter screen.

10. Repeat steps 5 - 9 to create another branch for site KLM for output on serial port #3.

11. Select **Save File As** button at the bottom of the screen. Enter the file name "doc_example3" and click **OK**.

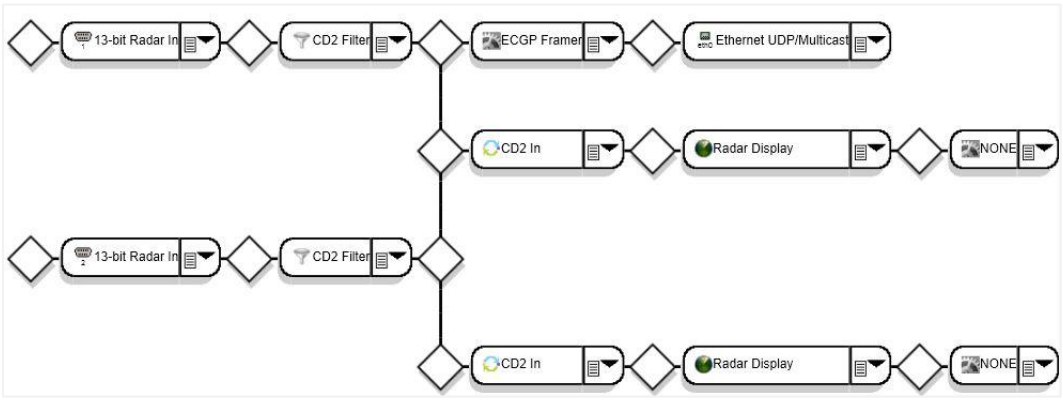
A1.4 Example #4: Multiple Serial Input to Single LAN output

This example is an exercise in creating sensors and merging data from multiple inputs to a single output.

The configuration in example #4 should contain the following elements:

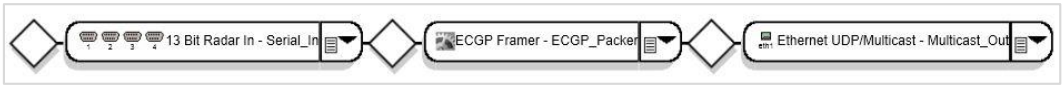
- Two CD-2 13 bit radar data serial input on port 1 and 2 (channel 1 only).
- Filter out Search messages from CD-2 data on port 1.
- Filter out status, AIM, and weather messages from CD-2 data on port 2.
- A GUI Radar Display to show both radar inputs – sites XYZ and TUV.
- Format data in ECGP headers from ARTCC ABV.
- Multicast all data on LAN to 239.1.1.7 port 9507.

The final data flow will look like this:



To create the data flow described above the following steps are performed:

1. From the menu bar, select **Configuration**, **New**. Choose the file *_4_channel_13_bit_to_lan*. This file provides the following template:



2. In the *Sensor Configuration* Section of the screen, mouse-click the **New** sensor. . Enter "XYZ" for **Site Name**. Choose "CD-2" for **Site Type**. Change the **Logical Name** to "Radar In 1 - site". Click **OK** to exit the configuration parameters screen.

3. In the *Sensor Configuration* Section of the screen, mouse-click the **New** sensor. Enter "TUV" for **Site Name**. Choose "CD-2" for **Site Type**. Change the **Logical Name** to "Radar In 2 - site". Click **OK** to exit the configuration parameters screen.

4. Click on the first node of type *13 Bit Radar In*. Change the following configuration parameters:

   a) Type "Radar In 1" for the **Logical Name**.

   b) Choose "9600" for the **Baud Rate**.

c) Choose "Radar In 1 – site" for **Radar ID**.

d) Click **OK** to exit the configuration parameters screen.

Note

The current data flow does not have a *CD2 Filter* node type; therefore another node must be added to the existing data path.

5. Mouse-over on the diamond connector after 13 Bit Radar In node. Select the "Insert a Function" option. A generic node of FUNCTION type with default name is inserted in the data flow.

6. Select the node dropdown list on the new node. Choose Filters, CD2 Filter.

7. Click on the node. Enter "filter searches" for Logical name. Check the box next to: Search, Search Strobe, and SRTQC messages. Click OK to exit the configuration parameter screen and save the settings.

Note

The ECGP Framer node is needed, but the configuration parameters are changed to match the desired output information.

8. Click on the *ECGP Framer* node type. Enter "ABV" for the **ARTCC Name**.

9. Click **OK** to exit the configuration parameter screen and save the settings.

10. Click on the *Ethernet UDP/Multicast* node. Change the following configuration parameters:

a) Enter "9507" for **Multicast port number**.

b) Enter "239.1.1.7" for **Multicast IP**.

c) Choose "Eth0" for **Multicast NIC**.

d) Click **OK** to exit the configuration parameters screen.

Note

Another serial port input is required for the configuration. Another branch to process serial data from port #2 must be created.

11. Mouse-over on the first diamond connector in the data path. Select the "Branch the path" option. The GUI creates a duplicate of the data path from where the branch was initiated. The nodes are setup with "dummy" values and must be configured by the user.

12. Each node in the branched data path must be configured with a particular type. Using the node dropdown menu on the following nodes, select the correct node type:

    a) First node: *13 Bit Radar In*.

    b) Second node: *CD2 Filter*.

13. For each of the nodes configured in step 15. Click on each node type and configure the following parameters:

    a) First node: Type "Radar In 2" for the **Logical Name**. Choose "9600" for the **Baud Rate**. Choose "Port 2" for **Channel 1**. Choose "Radar In 2 – site" for **Radar ID**.

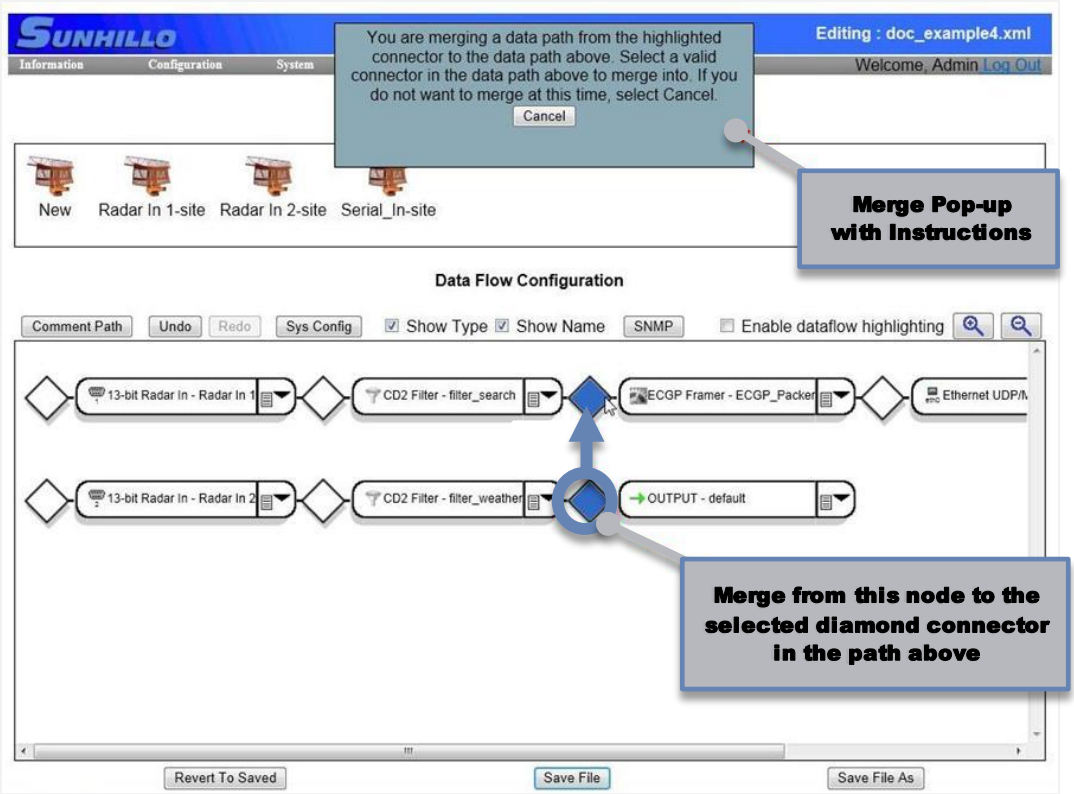
    b) Second Node: Type "filter_weather" for the **Logical Name**. Filter out AIMS, Status, and Weather messages.

Note

The data flow is to send both radar inputs to a single LAN output. At this point in the data path, the second path must be merged into the top data path to use the *ECGP Framer* and *Ethernet UDP/Multicast* nodes for the data in the second path. The third node is not necessary in the second data path row.

14. Mouse-over on the third diamond connector in the data path. Select the "Delete a Node" option. The FUNCTION node will be removed from the data path.

15. Select the node dropdown list on the OUTPUT node. Choose Merge. A pop-up dialog box will give instructions for choosing the connector in the data path above with which to merge. Click on the node before the "ECGP Framer" type node.



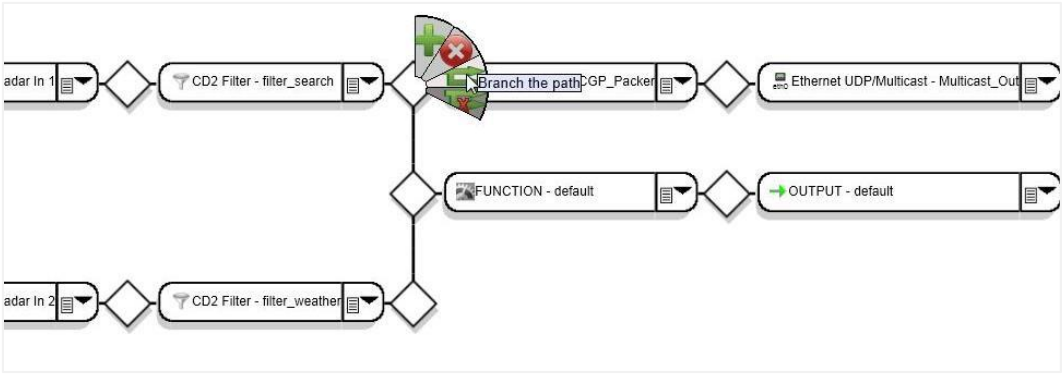
Note

The current data flow does not have a *Radar Display* node type. It is recommended that a graphical display type node, such as *Radar Display*, be added to the data flow in a separate branch of data path which is not in the critical data processing stream.

Note

For this example, a *Radar Display* is desired for BOTH sources of serial radar data after the CD2 filter. The location of the branch for the *Radar Display* must be chosen after the *CD2 Filter* node in the data path.

16. Mouse-over on the diamond connector after "CD2 Filter – filter search" node. Select the "Branch the path" option. A duplicate of the data path from where the branch was initiated is created. This path is populated with "dummy" nodes which must be configured.



Note

The *Radar Display* node type requires a prerequisite node type prior to it in the data flow. Before a Radar Display can be added to the data flow, the node type *CD2* In must be inserted.

17. Select the node dropdown list on the FUNCTION node. Choose **Input Radar Types**, **CD2 In**.

18. Click on the node. Enter "for_display1" for **Logical name**. Click **OK** to exit the configuration parameter screen and save the settings.

Note

The *Radar Display* node can be inserted into the data flow now. You may have to scroll to the right to see all the nodes in the data flow path.

19. Mouse-over on the diamond connector after *CD2 In* node. Select the "Insert a Function" option. A generic node of FUNCTION type with default name is inserted in the data flow.

20. Select the node dropdown list on the new node. Choose **Utilities**, **Radar Display**.

21. Click on the node. Enter "site_XYZ" for **Logical name**. Type "XYZ" for **Site Name** to display. Click **OK** to exit the configuration parameter screen and save the settings.

Note

For this data path there is no actual data output. By design, each data path has to have an OUTPUT node. In this case, the OUTPUT node type must be set to "NONE" to indicate this is the end of this data path.

22. On the OUTPUT node, select the node dropdown list. Choose **Other**, **NONE.**

Note

Another *Radar Display* must be added to the data flow for the serial data from Port 2 after the *CD2 Filter – filter weather* node.

23. Repeat steps 14 – 20 to create a data path branch for a *Radar Display* for site name "TUV".

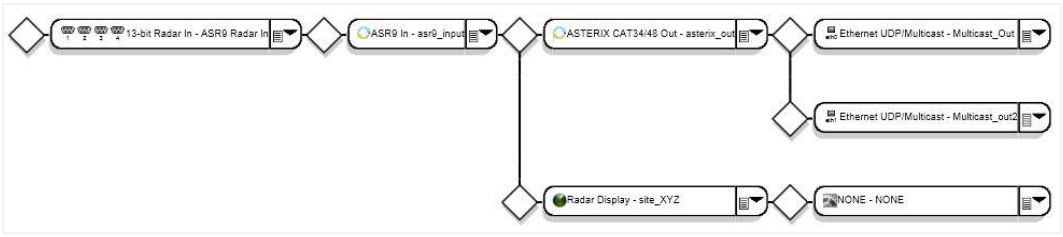
24. Select **Save File As** button at the bottom of the screen. Enter the file name "doc_example4" and click **OK**.

A1.5 Example #5: Serial Input to Multiple LAN Output with Data Conversion

The configuration in example #5 should contain the following elements:

- Receiving ASR-9 formatted radar data.
- 4 channel 13 bit radar data serial input using 4 ports using external clock.
- A GUI Radar Display to show radar input – site XYZ.
- Convert ASR-9 data to ASTERIX CAT034/48.
- Multicast all data on LAN to 239.1.1.7 port 9507 and 239.1.1.8 port 9508.

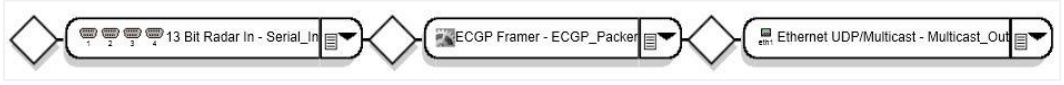
The final data flow should look like this:



To create the data flow described above the following steps are performed:

1. From the menu bar, select **Configuration**, **New**. Choose the file *_4_channel_13_bit_to_lan*.

   This file provides the following template:



2. Click on the first node of type *13 Bit Radar In*. Change the following configuration parameters:

a) Type “ASR9 Radar In” for the **Logical Name**.

b) Choose “External” for the **Baud Rate**.

c) Click **OK** to exit the configuration parameters screen.

Note

The site data associated with this radar must be configured. This information is stored in the Sensor associated with the *13 Bit Radar In* node named “Serial_In-site”.

3. Click on the “Serial_In-site” in the Sensor configuration window. Enter “XYZ” for **Site Name**. Choose “Asr9” for **Site Type**. Click **OK** to exit the configuration parameters screen.

Note

The current data flow does not need an *ECGP Framer* as provided by the template; therefore, this node can be changed to the necessary conversion node type. However, the *ASTERIX CAT34/48 Out* node type requires a prerequisite node type prior to it in the data flow. An “Input Radar Type” node must be inserted first.

4. Mouse-over on the diamond connector after *13 bit Radar In* node. Select the “Insert a Function” option. A generic node of FUNCTION type with default name is inserted in the data flow.

5. Select the node dropdown list on the new node. Choose **Input Radar Types**, **ASR9 In**.

6. Click on the node. Enter “asr9_input” for **Logical name**. Click **OK** to exit the configuration parameter screen and save the settings.

Note

The ECGP Framer node can now be changed to the proper conversion function type.

7. Select the node Dropdown list on the *ECGP Framer* node. Choose **Output Radar Types**, **ASTERIX CAT34/48 Out**.

8. Click on the node. Enter “asterix_out” for **Logical name**. Change other settings if necessary. Click OK to exit the configuration parameter screen and save the settings.

9. Click on the *Ethernet UDP/Multicast* node. Change the following configuration parameters:

a) Enter “9507” for **Multicast port number**.

b) Enter “239.1.1.7” for **Multicast IP**.

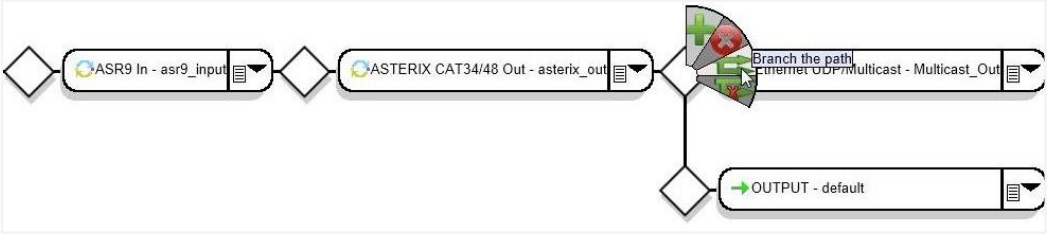
c) Choose “Eth0” for **Multicast NIC**.

d) Click **OK** to exit the configuration parameters screen.

Note

Another Multicast LAN output is required for the configuration. Another branch to transmit LAN data must be created.

10. Mouse-over on the fourth diamond connector in the data path. Select the “Branch the path” option.



11. Select the node dropdown list on the new OUTPUT node. Choose **LAN**, **Ethernet UDP/Multicast**.

12. Click on the new node. Change the following configuration parameters:

a) Enter “9508” for **Multicast port number**.

b) Enter “239.1.1.8” for **Multicast IP**.

c) Choose “Eth1” for **Multicast NIC**.

d) Click **OK** to exit the configuration parameters screen.

Note

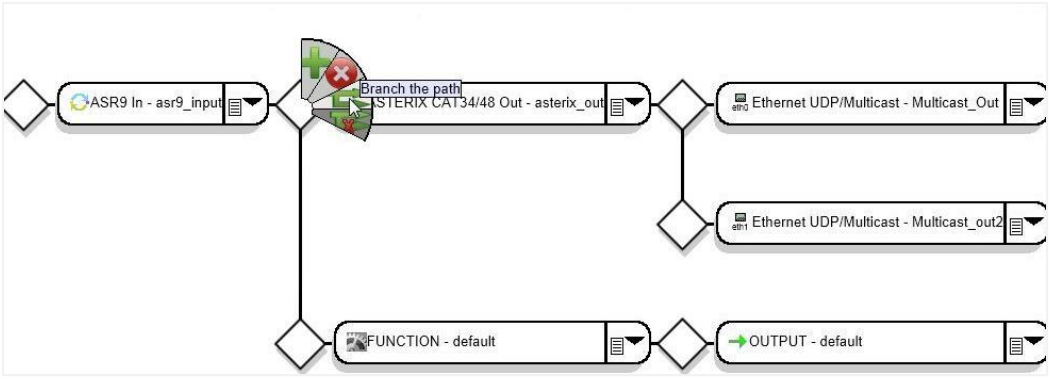
The current data flow does not have a *Radar Display* node type. It is recommended that a graphical display type node, such as *Radar Display*, be added to the data flow in a separate branch of data path which is not in the critical data processing stream.

Note

The *Radar Display* node type has a prerequisite that a node of the Input Radar Type be present in the data flow before the Radar Display utility node. The location of the

branch for the Radar Display must be chosen after the *ASR9 In* node in the data path.

13. Mouse-over on the diamond connector after *ASR9 In* node. Select the "Branch the path" option. A duplicate of the data path from where the branch was initiated is created. This path is populated with "dummy" nodes which must be configured.



14. Select the node dropdown list on the FUNCTION node. Choose **Utilities**, **Radar Display**.

15. Click on the node. Enter "site_xyz" for **Logical name**. Type "XYZ" for **Site Name** to display. Click **OK** to exit the configuration parameter screen and save the settings.

Note

For this data path there is no actual data output. By design, each data path has to have an OUTPUT node. In this case, the OUTPUT node type must be set to "NONE" to indicate this is the end of this data path.

16. On the OUTPUT node, select the node dropdown list. Choose **Other**, **NONE**.

17. Select **Save File As** button at the bottom of the screen. Enter the file name "doc_example4" and click **OK**.

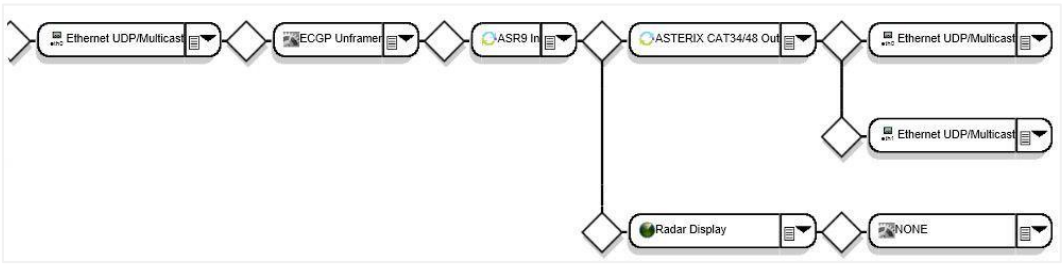
A1.6 Example #6: LAN Input to Multiple LAN Output

The configuration in example #6 should contain the following elements:

- Receiving ASR-9 formatted radar data.
- Multicast LAN data input from 239.1.1.12 port 9512 in ECGP format from ARTCC ABV.
- A GUI Radar Display to show both radar input – site XYZ.
- Convert ASR-9 data to ASTERIX CAT034/48.

- Multicast all data on LAN to 239.1.1.7 port 9507 and 239.1.1.8 port 9508.

The final data flow should look like this:



To create the data flow described above the following steps are performed:

1. From the menu bar, select **Configuration**, **Edit**. Choose the file *doc_example5*.
2. Select the node dropdown list on the first node to change the type from a serial input to LAN input. Choose **LAN**, **Ethernet UDP/Multicast**.
3. Click on the node. Enter "ASR9 ECGP In" for **Logical name**. Change the following configuration parameters:
   a) Enter "9512" for **Multicast port number**.
   b) Enter "239.1.1.12" for **Multicast Receive IP address**.
   c) Choose "Eth0" for **Multicast NIC**.
   d) Click **OK** to exit the configuration parameters screen.

Note

The current data flow does not have an *ECGP Unframer* node type; therefore, another node must be added to the existing data path.

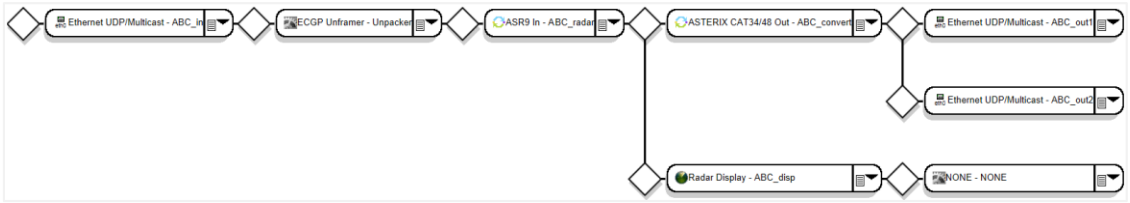
4. Mouse-over on the diamond connector after the *Ethernet UDP/Multicast* node. Select the "Insert a Function" option. A generic node of FUNCTION type is inserted in the data flow.
5. Select the node dropdown list on the new node. Choose **Framer/Unframers**, **ECGP Framer**.
6. Click on the node. Enter "unframer" for **Logical name**. Enter "ABV" for **ARTCC Name**.
7. Click **OK** to exit the configuration parameter screen and save the settings.
8. Select **Save File As** button at the bottom of the screen. Enter the file name "doc_example6" and click **OK**.

A2. SGP CONFIGURATION EXAMPLES

This Section provides a step-by-step example of creating a configuration file using one of the template files shipped with the SGP product. The configuration in this example contains the following elements:

- Receiving ASR-9 formatted radar data and converting it to ASTERIX CAT034/048
- Multicasting LAN data input from 239.1.1.12 port 9512 in ECGP format from ARTCC ABC
- Displaying radar data graphically
- Multicasting output data on the LAN to addresses 239.1.1.7 port 9507 and 239.1.1.8 port 9508

The final data flow will be:



To create the described data flow, the following steps are performed:

- **Create the Input Flow**

1. From the menu bar, select **Configuration**, **New**. Choose the file *_split_1_in_2_out.xml*.
2. Click the **Save File As** button and enter the file name *my_asr9in* at the prompt.
3. Click the **OK** button to save the template file as *my_asr9in.xml*. This new file name appears in the upper right corner of the screen.
4. Click on the first node in the data flow, change the following parameters, and then click **OK**:
   a) **Logical Name** = ABC_in
   b) **Multicast Port Number** = 9512
   c) **Multicast Receive IP Address** = 239.1.1.12
5. Mouse over the diamond connector before the SBB-Filter node and select the **Delete branch** fan option. The lower branch is now removed from the data flow.
6. Mouse over the diamond connector after the ECGP Unframer node and select the **Insert a function** fan option. A default FUNCTION node is inserted into the data flow.

7. Select the FUNCTION node's dropdown list and **choose Input Radar Types, ASR9 In**.
8. Click on the FUNCTION node and change the Logical Name to *ABC_radar*.
9. Click **OK**.

Create the Output Flow

1. Mouse over the diamond connector after the ABC_radar function and select the **Branch the path** option. A new path is created containing a FUNCTION node and an OUTPUT node.
2. Select the new Function node's dropdown list and choose **Utilities, Radar Display**.
3. Click on the Radar Display node, change the following parameters, and then click **OK**:
   a) **Logical Name** = ABC_disp
   b) **Site Name** = ABC
4. Select the default OUTPUT node's dropdown list and choose **Other, NONE**.
5. On the upper data path, select the SAA-Filter node's dropdown list and choose **Output Radar Types, ASTERIX CAT34/48 Out**.
6. Click on this Output node and change the Logical Name to *ABC_convert*.
7. Click **OK**.
8. Mouse over the diamond connector after the ABC_convert node and select the **Branch the path** fan option. A new OUTPUT node is created.
9. Click on the topmost Output node (**OUT_1**), change the following parameters, and then click **OK**:
   a) **Logical name** = ABC_out1
   b) **Multicast Port Number** = 9507
   c) **Multicast Port** = 239.1.1.7
10. Select the new (default) Output node's dropdown list and choose **LAN, Ethernet/UDP Multicast**.
11. Click on this Output node, change the following parameters, and then click **OK**.
    a) **Logical name** = ABC_out2
    b) **Multicast Port Number** = 9508
    c) **Multicast Port** = 239.1.1.8

12. Click the **Save File** button.

This page is intentionally left blank.

A3. MARGATE II ADS-B CONFIGURATION

Margate II ADS-B devices provide templates for the most popular configurations (see Section **4.3**). The basic concepts described in Appendices **A** and **B** can also be applied to Margate II ADS-B devices.

This page is intentionally left blank.

A4. ENABLING MSP API OPERATION

To configure a SureLine Core device to use the MPS API, a valid MPS API data flow must be used. As such, the software comes with a preconfigured template. To use this template, follow these steps:

1. From the menu bar, select **Configuration**, **New**. Choose the file *_mps-api-connections*.
2. On the configuration screen, click the **Save File As** button and enter a file name at the prompt. Click **OK**.
3. From the menu bar, select **Configuration**, **SetActive**. Choose the file name saved in step 2. Click **OK**.
4. From the menu bar, select **System, Restart software…**. Once restarted, the device operates as an MPS and is controlled by the MPS API.

With the MPS API configuration running, proceed to attaching and using the MPS API calls described in *SUN2298 – MPS WAN Protocol User's Guide*.

This page is intentionally left blank.

A5. ACRONYMS

The acronyms that follow have been used throughout this document.

Acronym	Expansion
ADS-B	Automatic Dependent Surveillance – Broadcast
AIMS	ATCRBS Identification Friend-or-Foe Mark XII System
ANSI	American National Standards Institute
API	Application Programming Interface
ARTCC	Air Route Traffic Control Center
ARTS	Automated Radar Terminal System
ASCII	American Standard Code for Information Interchange
ASR	Airport Surveillance Radar
ASTERIX	All Purpose Structured Eurocontrol Surveillance Information Exchange
ATCRBS	Air Traffic Control Radar Beacon System
bps	bits per second
BRTQC	Beacon Real Time Quality Control
BTU	British Thermal Unit
CD	Common Digitizer
CRC	Cyclic Redundancy Check
CSA	Canadian Standards Association
CTS	Clear to Send
DTR	Data Terminal Ready
EBCDIC	Extended Binary Coded Decimal Interchange Code
ECGP	En Route Communications Gateway Protocol
EIA	Electronic Industries Alliance
ESD	Electrostatic Discharge
ESM	Ethernet Switch Module
EUROCONTROL	European Organisation for the Safety of Air Navigation
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FIFO	First In First Out
FTP	File Transfer Protocol
GUI	Graphical User Interface
HDLC	High-level Data Link Communications
IEC	International Electrotechnical Commission
IP	Internet Protocol
KML	Keyhole Markup Language
LAN	Local Area Network
LED	Light Emitting Diode
LRU	Lowest Replaceable Unit
Mbps	Megabits Per Second
MIB	Management Information Base
MPS	Multi-Protocol Server
MTBF	Mean Time Between Failure

Acronym	Expansion
MTL	Mean Threshold Level
NDPP	Network Device Protection Profile
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NTP	Network Time Protocol
PCAP	Packet Capture
PCM	Processor Card Module
POST	Power On System Test
PSAR	Peripheral System Analysis and Recording
PSM	Power Supply Module
RAG	Range Azimuth Gate
RAPPI	Random Access Plan Position Indicator
RD	Receive Data
RICI	Real-Time Interface and Conversion Item
RoHS	Restriction of Hazardous Substance
RTS	Request to Send
SGF	Sensis Generic Format
SGP	Surveillance Gateway Process
SNMP	Simple Network Management Protocol
SRTQC	Search Real Time Quality Control
SSH	Secure Shell
STUI	Sunhillo Terminal User Interface
TCP	Transmission Control Protocol
TIS	Time In Storage
TTL	Time To Live
UDP	User Datagram Protocol
UL	Underwriters Laboratories
USB	Universal Serial Bus
VLAN	Virtual Local Area Network

End of Document