Ansaldo STS
A Finmeccanica Company
1000 Technology Drive, Pittsburgh, PA 15219
645 Russell Street, Batesburg, SC 29006

Wayside Interface Unit Integrated

ASTS USA Part No.
N17067602
N17067602UP

- **Software**

Copyright© 2015
Ansaldo STS USA, Inc.

Proprietary Notice

This document and the information contained therein are confidential – the disclosure or other communication, copying, reproduction and any use whatsoever is forbidden without the written authorization of Ansaldo STS USA, Inc.

Important Notice

ASTS USA constantly strives to improve our products and keep our customers apprised of changes in technology. Following the recommendations contained in the attached service manual will provide our customers with optimum operational reliability. The data contained herein purports solely to describe the product, and does not create any warranties.

Within the scope of the attached manual, it is impossible to take into account every eventuality that may arise with technical equipment in service. Please consult an ASTS USA local sales representative in the event of any irregularities with our product.

ASTS USA expressly disclaims liability resulting from any improper handling or use of our equipment, even if these instructions contain no specific indication in this respect. We strongly recommend that only approved ASTS USA spare parts are used as replacements.

© Property of Ansaldo STS USA, Inc., 2015 all rights reserved
1000 Technology Drive, Pittsburgh, PA USA 15219-3120
645 Russell Street, Batesburg, SC 29006
www.ansaldo-sts.com

Revision History

REV.	DATE	NATURE OF REVISION
1	February 2015	Initial Release

Table of Contents

List of Figures

List of Tables

1. GENERAL INFORMATION

1.1. Safety Summary

This document provides a description of the software PTC VitalNet Co-Processor PCB that handles Positive Train control (PTC) functionality. See ASTS USA service manual 1D2.0001 for a description of the hardware.

Read and thoroughly understand this manual before attempting any of the procedures listed. Pay particular attention to:

CAUTION

and

WARNING

These headings may appear throughout this manual. Caution statements indicate conditions that could cause damage to equipment. Warning statements indicate conditions that could cause physical harm, serious injury, or loss of life. Always observe standard precautions familiar to trained electrical technicians. Always adhere to all safety regulations stipulated by the railroad.

1.2. Abbreviations and Acronyms

The following are abbreviations and acronyms used in this manual along with their associated meanings.

ACK Acknowledgement

ASTS USA Ansaldo STS USA, Inc. (formerly known as Union Switch & Signal Inc.)

CAT 5 Category 5 cable

CMU Communications Management Unit

CPU Central Processing Unit

CRC Cyclic Redundancy Check

DB D-subminiature (a common type of computer connector)

DCD Data Carrier Detect

DHCP Dynamic Host Configuration Protocol

DNS Domain Name Server

EMP Edge Messaging Protocol

FPGA Field Programmable Gate Array

GMT Greenwich Mean Time

GPS Global Positioning System

HMAC	Hashed Message Authentication Code
IP	Internet Protocol
LED	Light-Emitting Diode
LRM	Launcher Response Message
LRU	Line Replaceable Unit
N/A	Not Applicable
NTP	Network Time Protocol
PC	Personal Computer
PCB	Printed Circuit Board
PTC	Positive Train Control
QoS	Quality Of Service
RC2	Rivest Cipher 2
RS-232	Recommended Standard 232
SCAC	Standard Carrier Alpha Code
SNMP	Simple Network Management Protocol
TCP/IP	Transport Control Protocol/Internet Protocol
TTL	Time To Live
US&S	Union Switch & Signal Inc. (hereinafter ASTS USA)
UTC	Universal Time Code
WCM	Wayside Communication Module
WEU	Wayside Encoder Unit (also known as WIU)
WIU	Wayside Interface Unit (also known as WEU)

2. DESCRIPTION

The Wayside Interface Unit (WIU) is part of a Positive Train Control (PTC) system. The PTC function includes the ability to monitor wayside devices and transmit the status of those devices to a locomotive that requests the information. The train can then react in a safe and timely manner. The WIU sends its information to a Wayside Communication Module (WCM). The WCM communicates with the locomotive.

The Wayside Interface Unit is typically a MicroLok cardfile that is installed at interlocking control points to interface and process with the location's switch machine(s), signal(s), and PTC radio systems.

The VitalNet CPU PCB in the MicroLok cardfile performs core vital logic processing for the MicroLok II system, as well as ongoing diagnostics and event/error logging.

The VitalNet Co-Processor Daughter PCB is attached to the VitalNet CPU PCB. This PCB enables integrated PTC WIU functionality directly within the MicroLok II system.

A PC can be connected to the WIU to access functions and data.

2.1. Features

The main features of the Wayside Encoder Unit are:

- Vital signal control and aspect monitoring
- Dark territory switch position monitoring
- Hazard Detector Warning
- Self-contained and is a line-replaceable unit (LRU)
- Includes a health indicator


Ansaldo STS
A Finmeccanica Company

3. CENTRAL PROCESSOR UNIT

The MicroLok II Central Processor Unit (CPU) with Positive Tran Control capabilities is ASTS USA part number WIUN1706760X. The CPU front panel is shown in Figure 3-1. Refer to Table 3-1 for control/indicator descriptions.

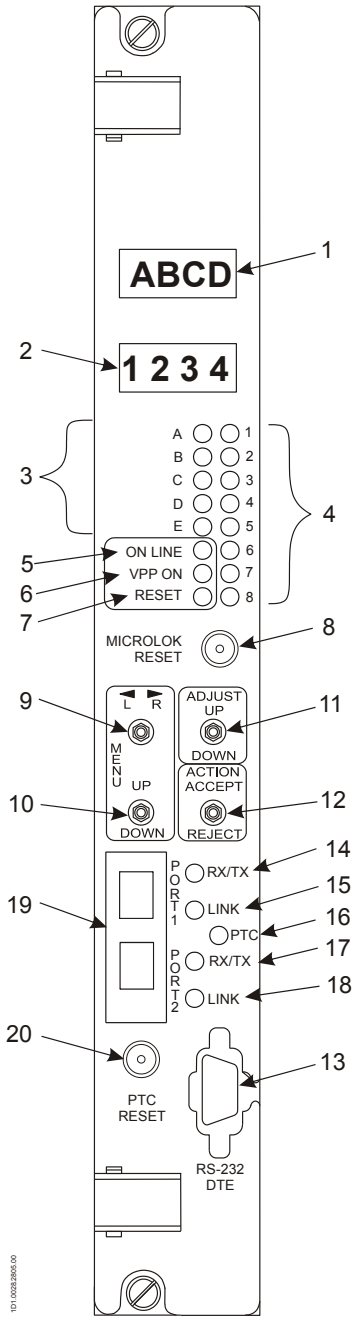


Figure 3-1. CPU Front Panel

Note: Switches 9 through 12 are shown toggled to depict direction of operation. Switches are spring return-to-center at rest.

3.1. User Interface

Table 3-1 lists the user indications and controls on the PTC Central Processor Unit (CPU) PCB ASTS USA part number WIUN1706760X.

Table 3-1. CPU WIUN1706760X Controls and LED Indicators

REF	LABEL	DEVICE	PURPOSE
MicroLok Configuration Functions			
1, 2	**(none)**	Two, four-character alphanumeric displays Top display is Red Bottom display is Green	On-site configuration programming menus and options. Normal operating display is: • The upper four-character display will continuously scroll the phrase US&S MICROLOK II. • The lower four-character display will continuously scroll the Application name.
3	**A, B, C, D, E**	LEDs (Yellow)	*Select serial port with CPU front panel switches (9, 10, 11, &12) via the on-line serial test menu.* A – Selected serial link is transmitting data. B – Selected serial link has received a valid message. C – Selected serial link has recognized the address in a received message. D – Selected serial link is receiving a Data Carrier Detect (DCD) signal. E – Selected serial link has detected a receiver error.
4	**1, 2, 3, 4, 5, 6, 7, 8**	LEDs (Red)	User-defined in Application software. LED #3 lights when CPU is booting-up.
5	**ON LINE**	LED (Green)	Lit indicates normal system operation (successful diagnostics). If out: reset system.
6	**VPP ON** (Voltage Input Flash Programming)	LED (Yellow)	When lit, indicates FLASH +5V programming voltage enabled (via CPU PCB jumper). Lit only during programming on CPUs without PCMCIA card installed. Lit continually on CPUs with PCMCIA card installed.
7	**RESET**	LED (Red)	When lit, indicates that the system is in reset mode. Normal operation = Off
8	**RESET**	Momentary pushbutton	When pressed, reboots the CPU. Also used to clear a CPS fault (VCOR/CPS down condition).

REF	LABEL	DEVICE	PURPOSE
9	**MENU L/R**	Three-position (spring return-to-center) toggle switch	Used to search main program menu items shown on displays.
10	**MENU UP/DOWN**	Three-position (spring return-to-center) toggle switch	Used to select main program menu items shown on displays.
11	**ADJUST UP/DOWN**	Three-position (spring return-to-center) toggle switch	Used to cycle through configuration values shown on displays.
12	**ACTION ACCEPT/ REJECT**	Three-position (spring return-to-center) toggle switch	Executes or cancels menu items shown on displays.
13	**RS-232 DTE** Diagnostic Link Connector	DB9, RS-232 connector Data Terminal Equipment (DTE)	Used for connection to personal computer for system monitoring/diagnosis.
PTC Configuration Functions			
14	**PORT 1 RX/TX**	LED (green)	When lit, indicates activity on Port 1.
15	**PORT 1 LINK**	LED (yellow)	When lit, indicates a link is established on Port 1.
16	**PTC**	LED (green)	When dark, PTC co-processor is not present or the PTC operating system is not (yet) operational. When lit, indicates PTC co-processor is operating properly.
17	**PORT 2 RX/TX**	LED (green)	When lit, indicates activity on Port 2.
18	**PORT 2 LINK**	LED (yellow)	When lit, indicates a link is established on Port 2.
19	**PORT 1** **PORT 2**	RJ-45 connector	Ethernet connections for Ports 1 and 2.
20	**PTC RESET**	Momentary pushbutton	When pressed for longer than 3 seconds, resets the PCB. When pressed for less than 3 seconds, acknowledges the software when prompted through the web interface.

System information can be accessed from the CPU by using the front panel toggle switches and the front panel alphanumeric displays (Items 1 and 2) or via a personal computer running ASTS USA MicroLok II Development System. The personal computer connects via the front panel diagnostics serial port (COM 5) DB9, DTE connector (Item 13).

3.1.1. Loading Software

Executive and Application software is uploaded to the CPU via the front panel diagnostics serial port and a personal computer running the MicroLok II Development System. Application software can be downloaded to the PC (from the CPU) by the same means. Executive software cannot be downloaded from the CPU.

4. CONNECTING TO WEB INTERFACE

4.1. Procedure

Proceed as follows to connect the WIU unit to the Web interface:

1. Connect a standard CAT 5 Ethernet cable from the PC to the Ethernet front panel RJ-45 connector Port 1 or Port 2 (Figure 4–1). The Ethernet port on the WIU is configured as a DHCP server by default and will provide an IP address to the PC.

NOTE

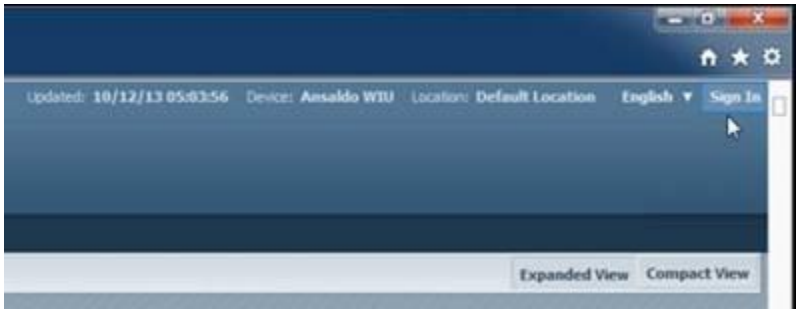
PC firewall software or internet browser proxy server settings may prevent connectivity to the device.

If you are having difficulty connecting, verify your IP address and proxy settings, and disable any firewall software.

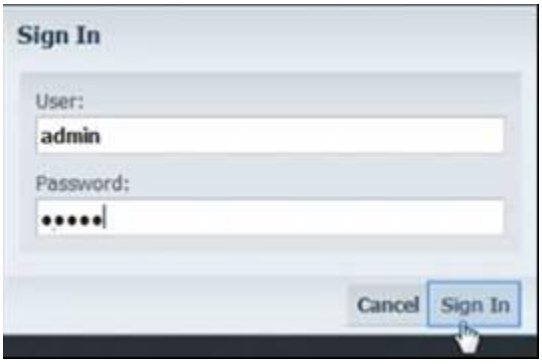
If you have verified the settings above and are still have connection problems, contact your network administrator.

Figure 4–1. PC to WIU Connection

2. Apply power to the unit.
3. Launch any internet browser on the PC, and type the IP address into the address bar on the browser. The factory default IP address for Port 1 is 169.254.1.10. The factory default IP address for Port 2 is 169.254.2.10.
4. Select the Sign In Button located at the upper right of the screen.



5. Log into the WIU device by entering the administrator username and password. The default administrator username and password are both '**admin**'. Select Sign In.



NOTE

When logging into the account for the first time, it is recommended you immediately change the password.

6. Select the Sign In Button located at the upper right of the screen that will now displays your username. A dropdown menu will display.
7. Select User Accounts.
8. The User Account PTC WIU Control screen will display. Enter your password.
9. Select the Select User dropdown menu.
10. Select the account in which to change the password.
11. Enter the previous password for that account in the Your Current Password text box.
12. Enter the changed password in the New Password and Repeat text boxes.
13. Select the Change Password button.

4.2. Connection Verification

Proceed as follows to verify the Web connection of the WIU:

1. After the system boots up (It may take 1-2 minutes from when the WIU is powered on. The 'PTC' LED on the front panel of the WIU will be lit solid green.), navigate to the System Information page on the browser-based maintenance interface:

   http://[ip_of_the_WIU]/system.cgi

2. The page displays the status of the Vital CPUs, model information, as well as version information of the software and FPGA components installed on the system. Make sure the versions match the revision of the firmware tar package that you have uploaded.
3. The "Vital Health Status field in the status bar should indicate GOOD upon successful boot and normal operation. If the health status indication is not GOOD, examine the vital event log in the maintenance interface to pinpoint the cause of the failure.

The VitalNet Co-processor CPU is shipped from the factory loaded with the latest PTC Executive software available at the time of release. As updates occur to the PTC WIU specification due to interoperability requirements, changes in protocol specifications, or new feature releases from ASTS USA, it will be necessary to update the PTC software and firmware running on the device.

4.3. Updating Software and Firmware

To update the Software/Firmware on the device, perform the following steps after logging in as an administrator:

1. Click on the Configuration tab located on the main menu bar of the page (Figure 6–1).
2. Click on the Upload Firmware link on the upper right side of the Configuration screen. The upload firmware screen will display (Figure 6–2).
3. Click on the Choose File button on the Update Device Firmware page to display a standard file-open window.

4. Browse to the latest update file (update files will be provided only by ASTS USA, and will have a .tar file extension). Select the file and click OK to return and close the file-open window.
5. Click on Force Update checkbox.
6. Click on the Update Firmware button to begin the firmware update process. Follow the onscreen instructions to complete the update process.
7. If you are loading a firmware package that is or 2.28 or lower, you must repeats Steps 4 and 6. Do not check the Force Update checkbox (Step 5) during the second upload.

4.4. Troubleshooting

If the event logs page is accessible through the maintenance interface, examine it first. The event logs will provide you with diagnostic information that may aid in troubleshooting.

Table 4-1 can be used as an aid in diagnosing problems.

Table 4-1. Troubleshooting Problems and Solutions

Problem	Possible solution
The PTC LED is not solid green. The PTC and Ethernet port lights cycle on and off light.	This is usually caused by a critical failure. If the browser-based maintenance interface is accessible, navigate to the event logs page, and examine the event log. Events of the critical level may cause the unit to enter a safe-state mode that ceases WSM communication. Most critical events are caused by a hardware failure *(or a software bug)*
The WIU reboots continuously.	This is usually caused by a critical failure. To diagnose this failure, disconnect all voltage and current inputs and outputs.. Disconnect the power from the unit, wait 10 seconds. Once the unit stops the reboot cycle, navigate to the event log page, and examine the events. If the unit is still resetting, further maintenance by Ansaldo team is required.
The unit fails to send wayside messages to the radio.	This can be caused by a faulty application or a critical failure. If the health LED is not solid green, refer to the first Problem above. If the health LED is green and the vital health indication is Good, upload the WIU application package to the WIU. Make sure that you are using a standalone WIU application, and not the MicroLok PTC application.
The unit's time is incorrect	Check the time update settings. The WIU's internal clock ceases operation after 2-18 hours without power. Send five timestamp updates through Class C or configure the WIU to receive time updates through SNTP.

Problem	Possible solution
The maintenance interface is unreachable. The unit doesn't respond to ICMP ping	This is usually caused by a network setting problem. If the WIU's DHCP server is enabled, set the device connected to the WIU to receive its IP configuration through DHCP. If DHCP server is not enabled, try using the default IP configuration: Top Ethernet Port 1: 169.254.1.10 Top Ethernet Port 2: 169.254.2.10 You may also reset the WIU's configuration parameters to factory defaults by powering down the WIU, removing the WIU from the metal casing, and locating the DIP switch bank, and flipping the switch #1 to the ON position.


Ansaldo STS
A Finmeccanica Company

5. WIU MICROLOK II SCREEN DESCRIPTIONS

The following sections describe the screens that are displayed when using the MicroLok II interface.

5.1. HOME/DEVICE STATUS SCREEN

When the web server on the VitalNet Wayside Interface Unit device is first accessed with an Internet Browser, the home page (see Figure 5–1) will be displayed. If an application is already loaded, the home page shows the status of the devices that are configured within the PTC Application. If no application is loaded, the home page will be automatically forwarded to the Application Builder page (Section 6).

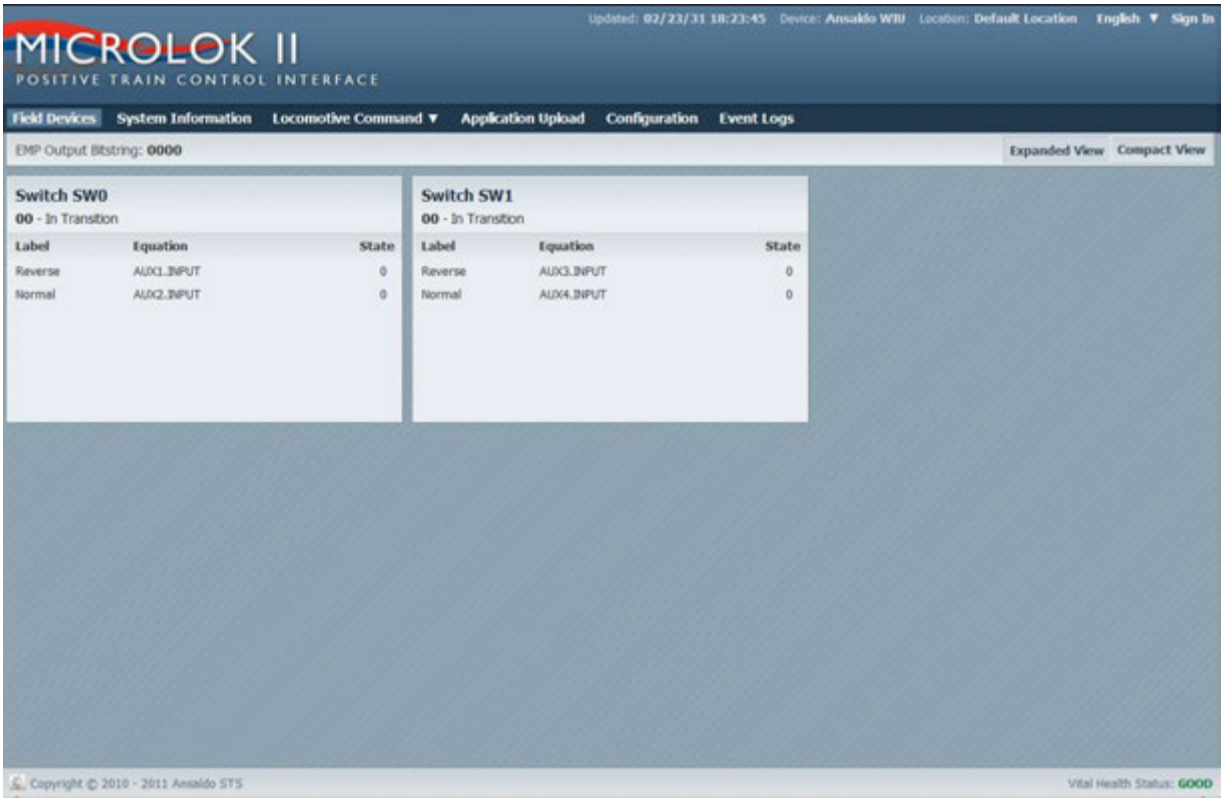


Figure 5–1. Home Page

Changes to the configuration cannot be made until a user login name and password is entered. A Login User Name and Password area is located at the top right corner of the page.

1. Click on the Sign In hyperlink located in the top-right corner of the page, and a Sign-In Screen will be displayed (Figure 5–2).
2. On the Sign-In screen, type in a valid username and password.

If the username and password combination is valid, the tool will return from the Sign-In screen, and the current Signed-In user level will be displayed in the top-right corner of the screen next to the user icon. Once Signed-In, additional configuration options will be made available within the displayed menu bar, relative to the access level granted to the user.

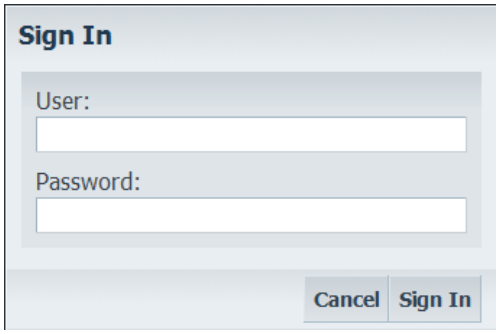


Figure 5–2. Sign-In Screen

5.2. Field Device Status Screen

The Field Device Status screen (Figure 5–3) displays information for WIU system devices. An expanded view or a compact view can be selected from the menu bar. The view can be compacted or expanded by selecting the Expand View and Compact View buttons at the right of the screen. The expanded view is shown in Figure 5–3. The compact view is shown in Figure 5–4.

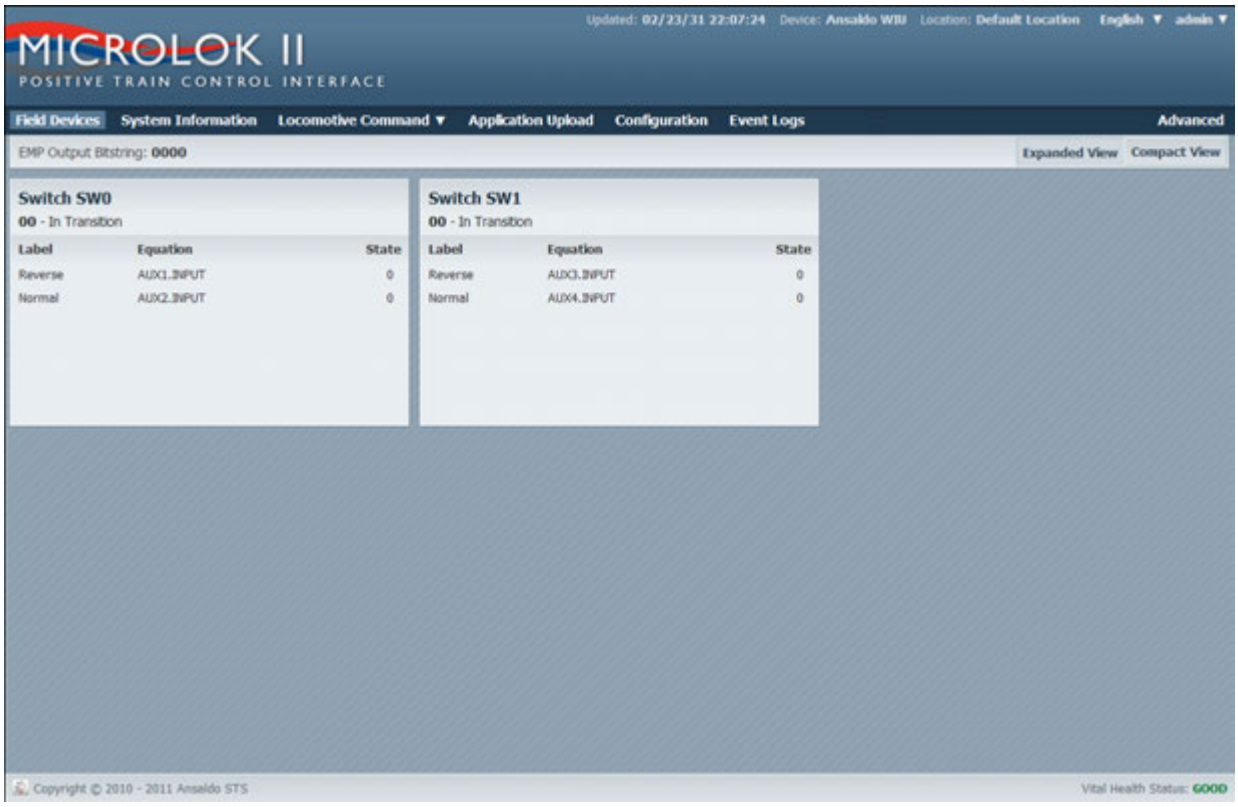


Figure 5–3. Field Device Status Screen Expanded View

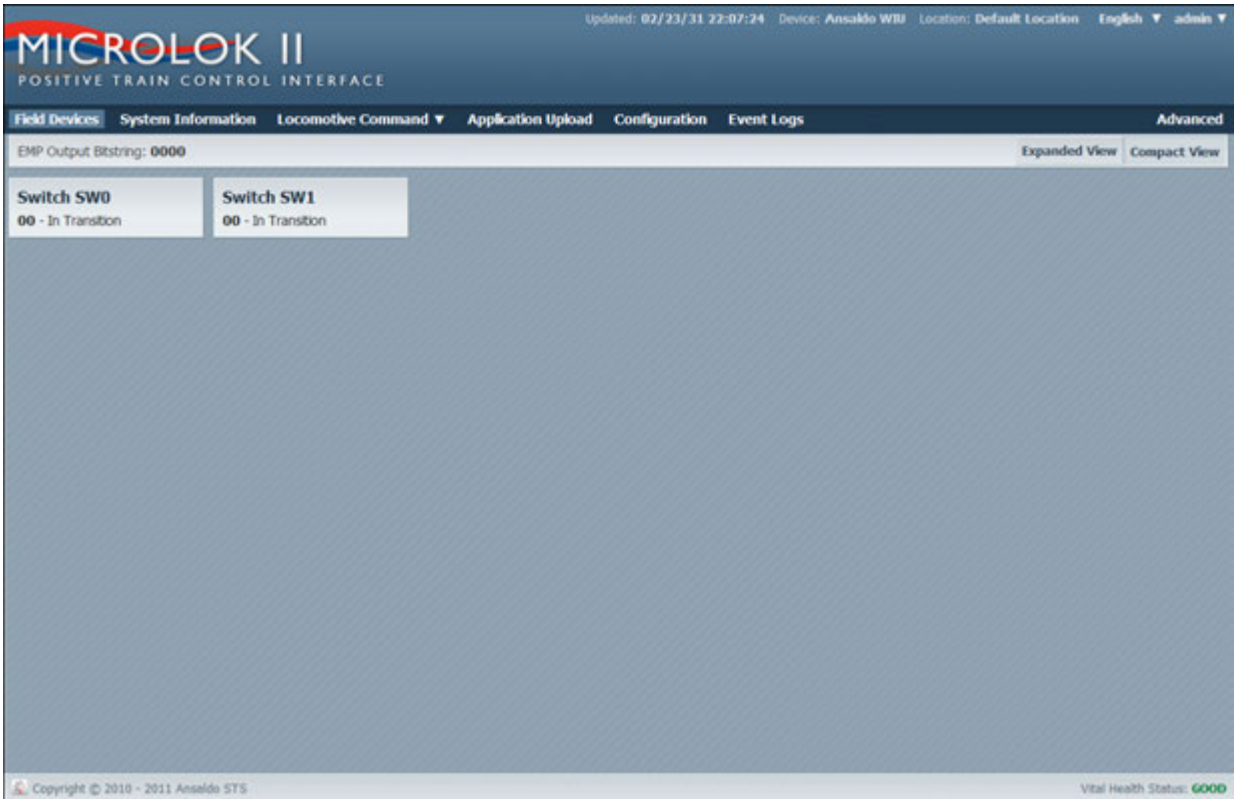


Figure 5–4. Field Device Status Screen Compact View

5.3. Device Configuration Screens

The Device Configuration screens provide information about a particular device. The following screens can be selected:

- Import/Export
- Location
- Network
- Class C
- Class D
- ACSES
- SNMP
- NTP
- ITC Time and Location
- Operating Values
- ITCSM

- Click the Browse button and the Choose File to Upload window opens. Select the new tar package and click open. The .tar package name will appear in the Upload Device Firmware window. From here, you can store or upload the firmware. The stored firmware files are listed in the Preloaded Firmware File window. You can display the MD5 Sum, upload the firmware, or delete the firmware by clicking on the circle under Select next to the .tar file and then selecting the appropriate command at the bottom of the window. See Section 6 for uploading firmware information.

5.4. SYSTEM INFORMATION SCREEN

The System Information screen (Figure 5–5) provides information about a particular system, including hardware model numbers, application information, and software and firmware version information.

After uploading the latest software and firmware to the device, verify that the version numbers match the version of the uploaded software.

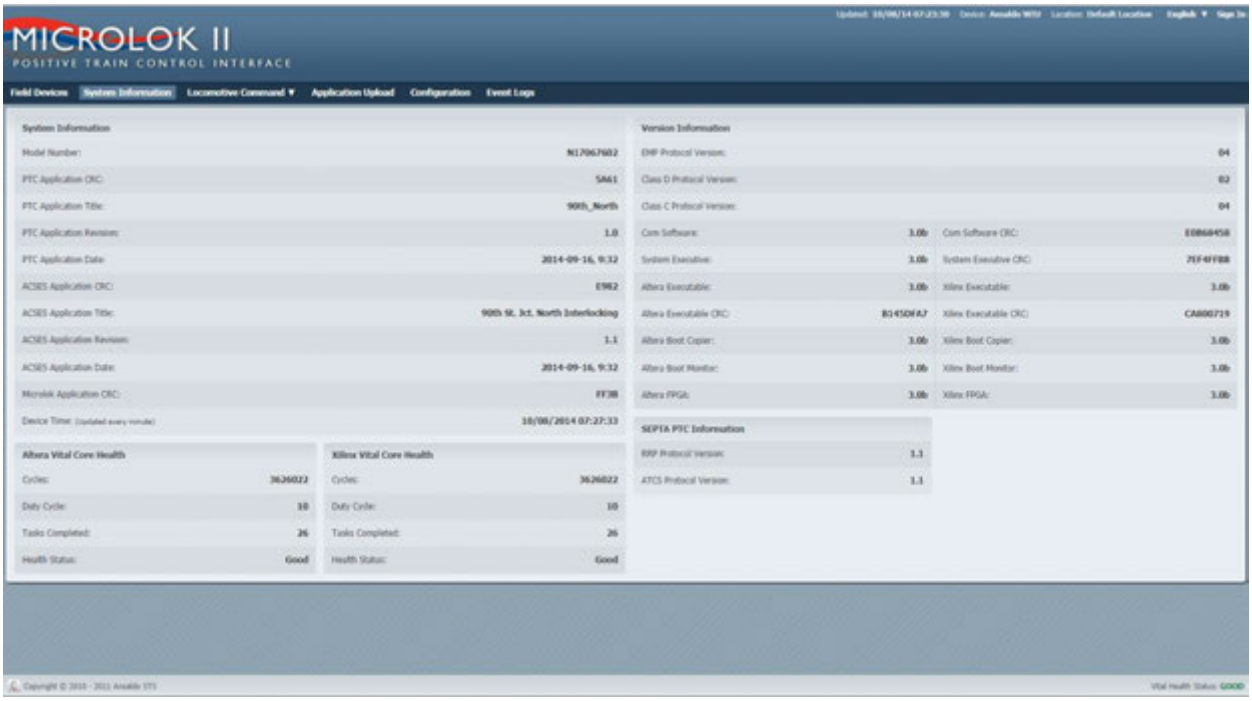


Figure 5–5. System Information Screen

5.4.1. Locomotive Command Screen

The Locomotive Command screen (Figure 5–7) gives the status of the Physical, Network, and Auxiliary bits.

NOTE

The Locomotive Command can only be modified by the PTC Application Builder.

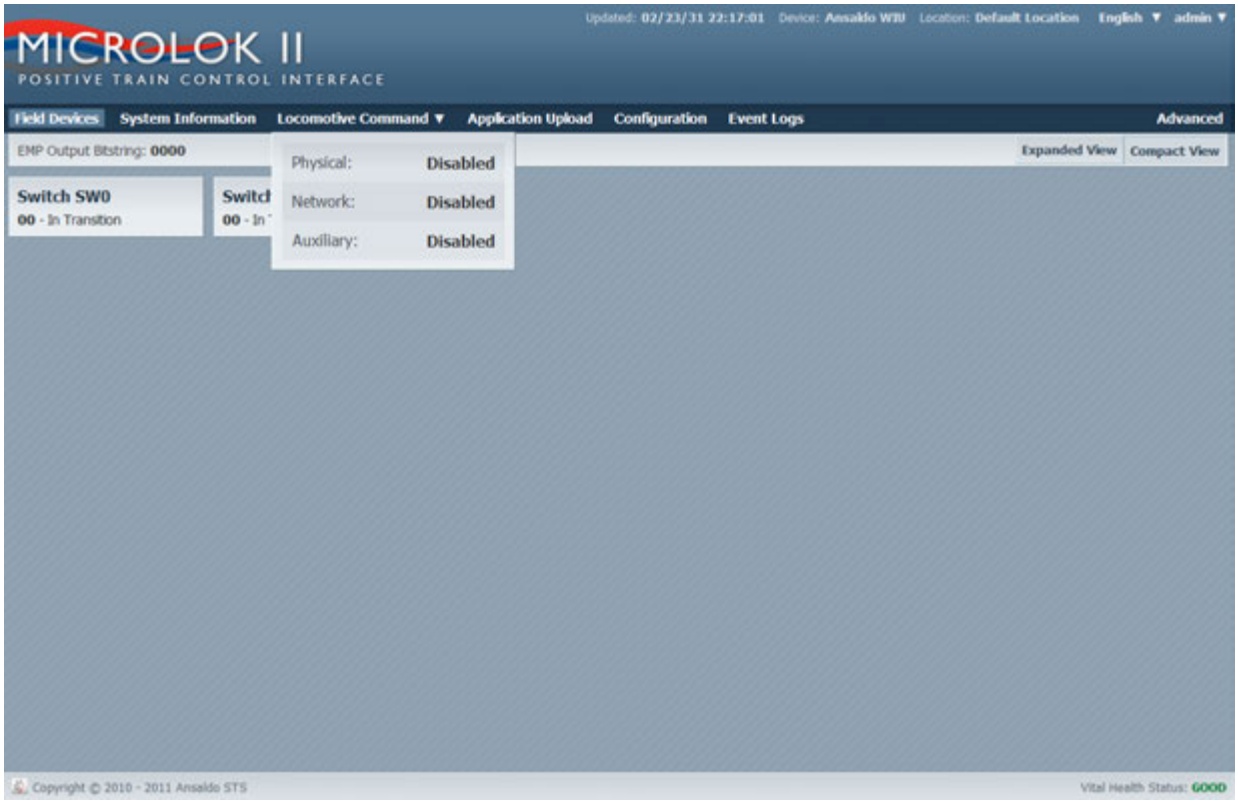


Figure 5–6. Locomotive Command Screen

5.4.2. Application Upload Screen

The Application Upload screen (Figure 5–7) allows you to select a file and upload it.

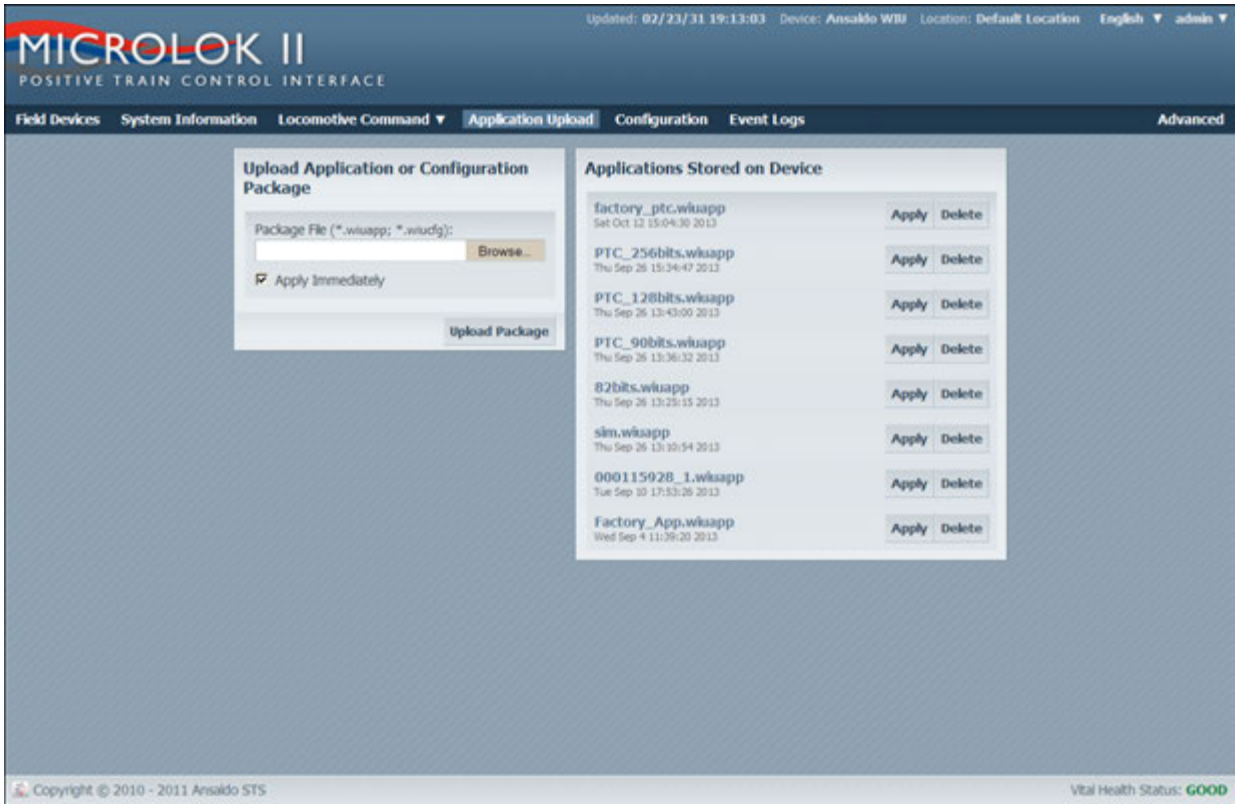


Figure 5–7. Application Upload Screen

5.4.3. Import/Export Screen

The Import/Export screen (see Figure 5–8) allows you to load, export or load a configuration and print a summary. Selecting Load Configuration displays the Application Upload screen (Section 5.4.1). Selecting Export to file downloads the unit's configuration. Selecting Printable Summary displays the Summary screen (Figure 5–9) that can be printed.

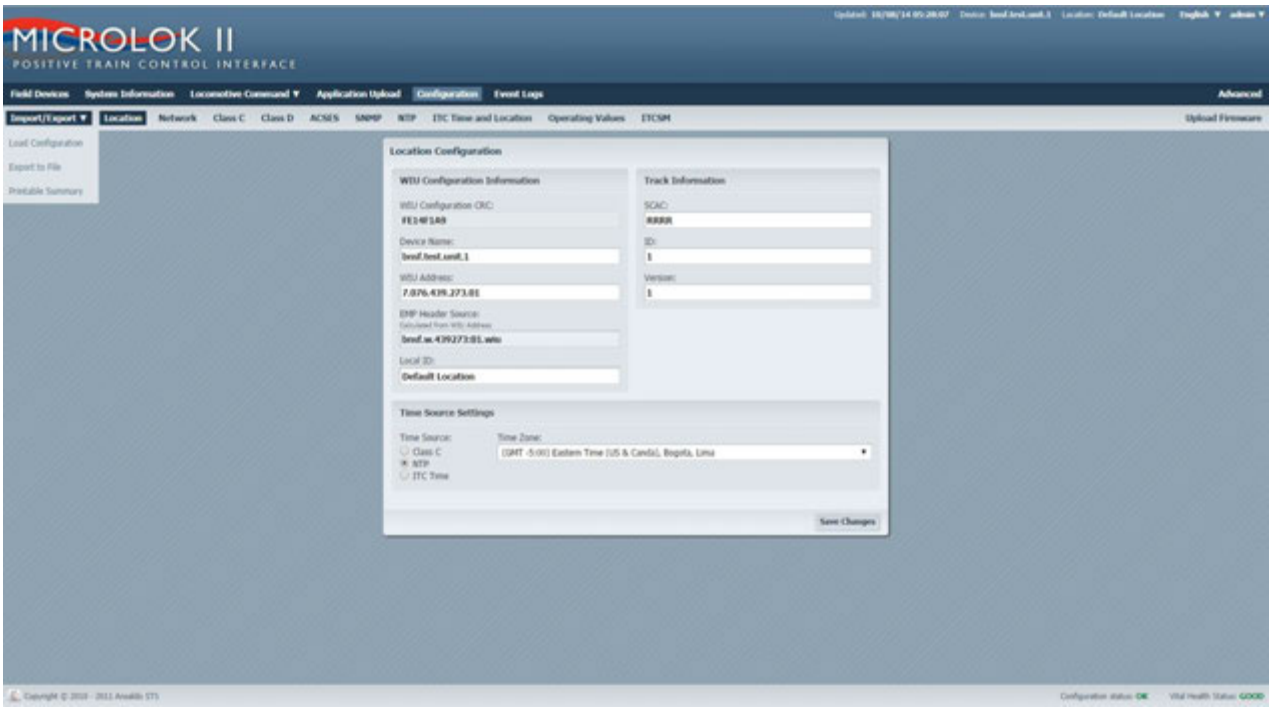
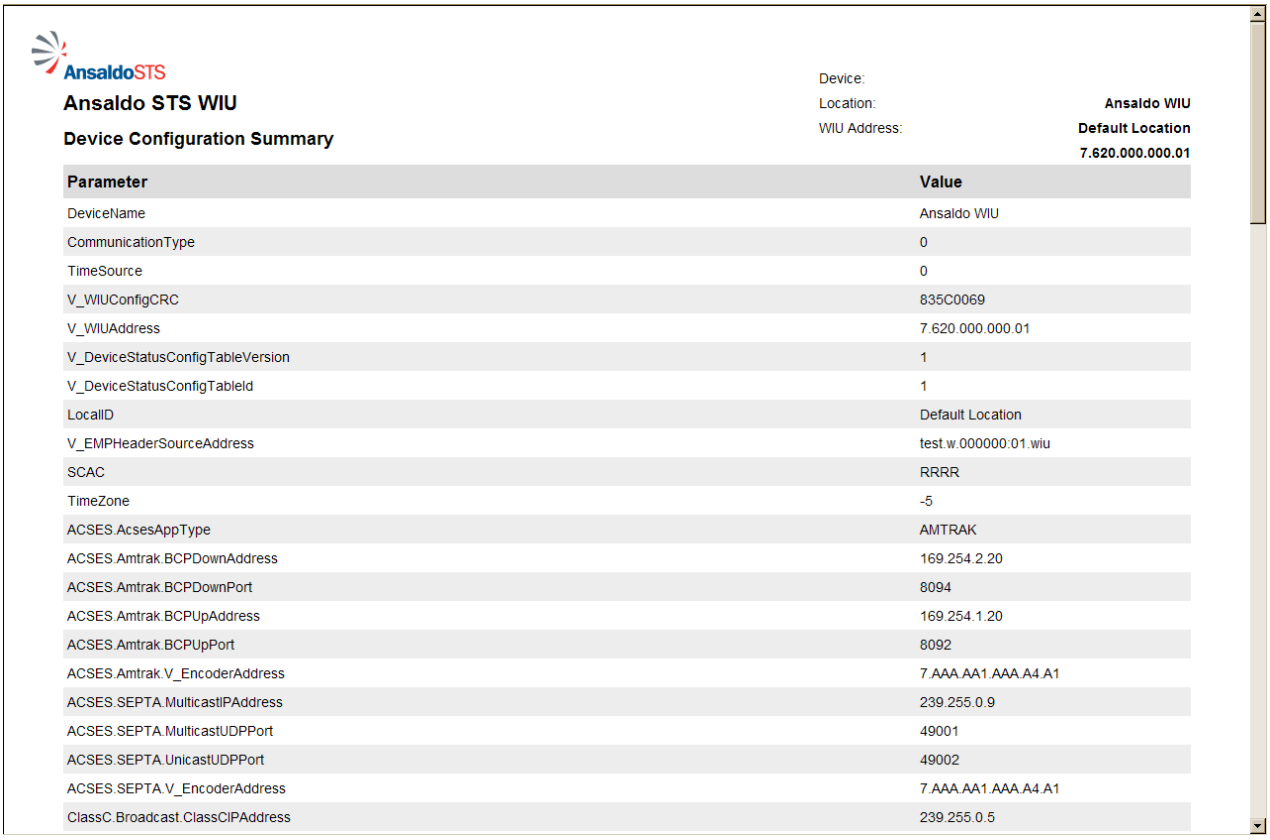


Figure 5–8. Import Export Screen



AnsaldoSTS

Ansaldo STS WIU

Device Configuration Summary

Device:
Location: **Ansaldo WIU**
WIU Address: **Default Location**
7.620.000.000.01

Parameter	Value
DeviceName	Ansaldo WIU
CommunicationType	0
TimeSource	0
V_WIUConfigCRC	835C0069
V_WIUAddress	7.620.000.000.01
V_DeviceStatusConfigTableVersion	1
V_DeviceStatusConfigTableId	1
LocalID	Default Location
V_EMPHeaderSourceAddress	test.w.000000:01.wiu
SCAC	RRRR
TimeZone	-5
ACSES.AcsesAppType	AMTRAK
ACSES.Amtrak.BCPDownAddress	169.254.2.20
ACSES.Amtrak.BCPDownPort	8094
ACSES.Amtrak.BCPUpAddress	169.254.1.20
ACSES.Amtrak.BCPUpPort	8092
ACSES.Amtrak.V_EncoderAddress	7.AAA.AA1.AAA.A4.A1
ACSES.SEPTA.MulticastIPAddress	239.255.0.9
ACSES.SEPTA.MulticastUDPPort	49001
ACSES.SEPTA.UnicastUDPPort	49002
ACSES.SEPTA.V_EncoderAddress	7.AAA.AA1.AAA.A4.A1
ClassC.Broadcast.ClassCIPAddress	239.255.0.5

Figure 5–9. Summary Screen

5.4.4. Location Screen

The Location screen (Figure 5–10) provides WIU location information including WIU configuration information, time settings, and track information. Changes can be made by entering information in the displayed boxes and saved by selecting the Save Changes button.

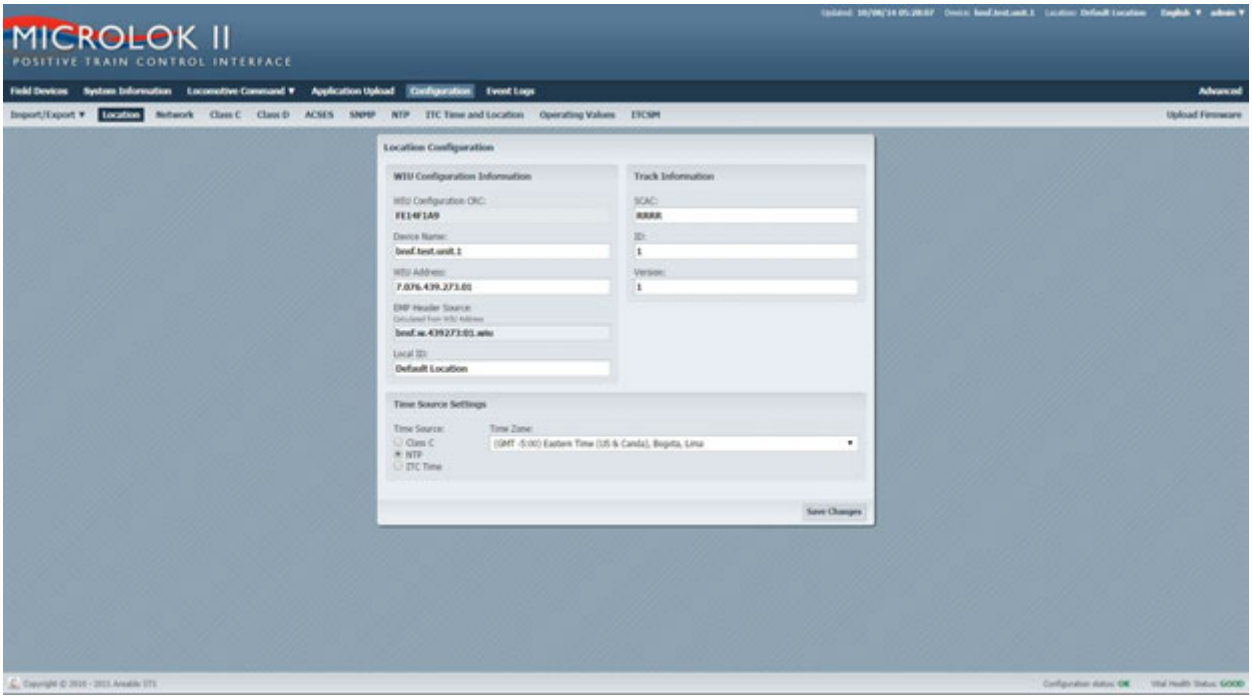


Figure 5–10. Location Screen

5.4.5. Network Screen

The Network screen (Figure 5–11) provides Ethernet Ports 1 and 2 information including connection type, IP address, network mask, gateway, and server information. Changes can be made by entering information in the displayed boxes and saved by selecting the Save Changes button.

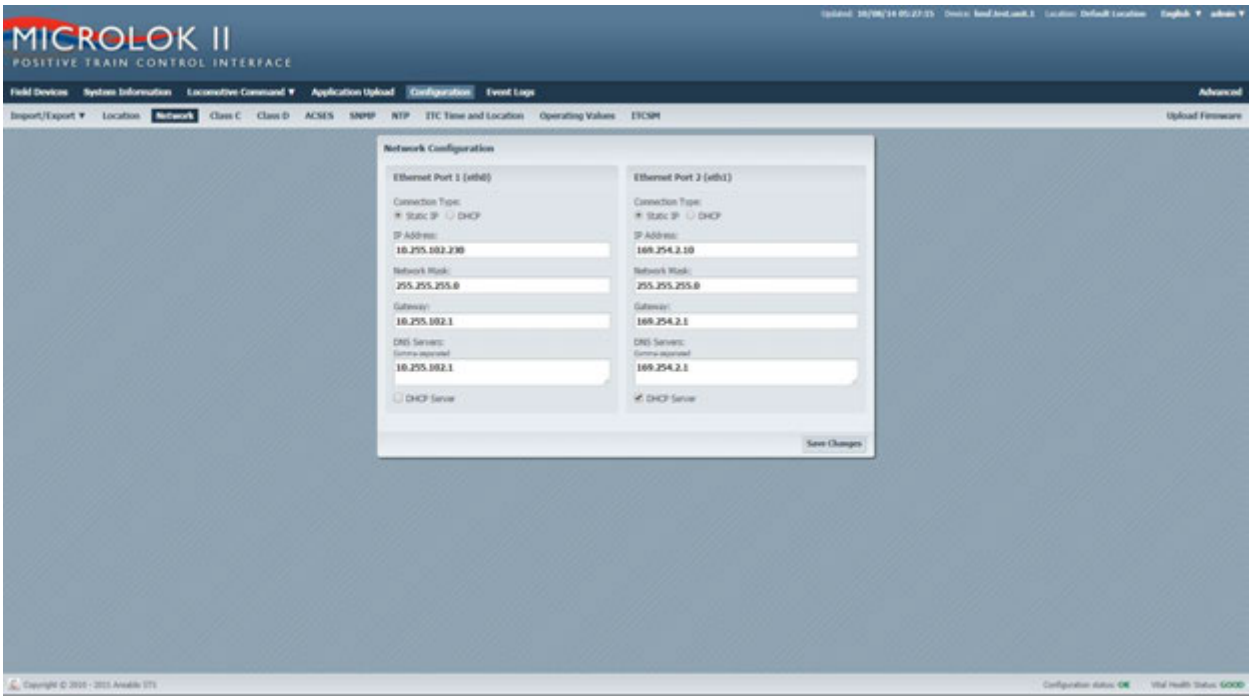


Figure 5–11. Network Screen

.

5.4.6. Class C Screen

The Class C (Figure 5–12) screen provides Class C information including time, address, and port information. Changes can be made by entering information in the displayed boxes and saved by selecting the Save Changes button.

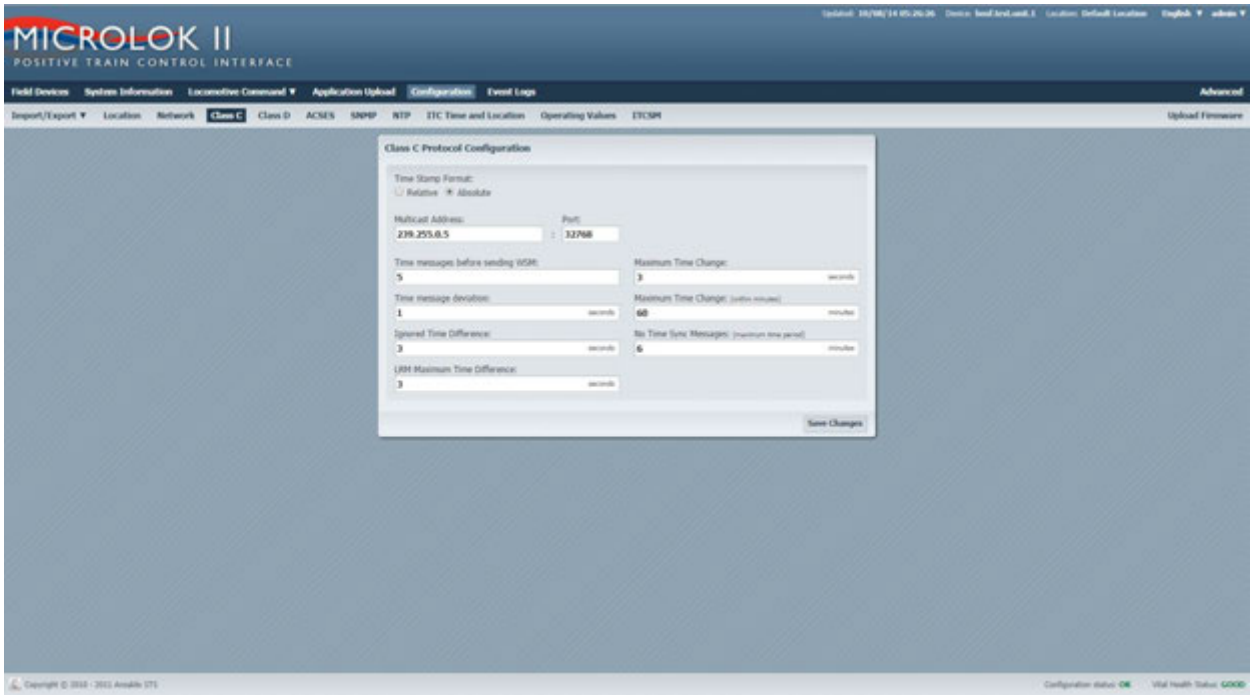


Figure 5–12. Class C Screen

5.4.7. Class D Screen

The Class D screen (Figure 5–13) provides Class D information including link configuration, beacon configuration, protocol attributes, link attributes, beacon attributes and QoS information. Changes can be made by entering information in the displayed boxes and saved by selecting the Save Changes button.

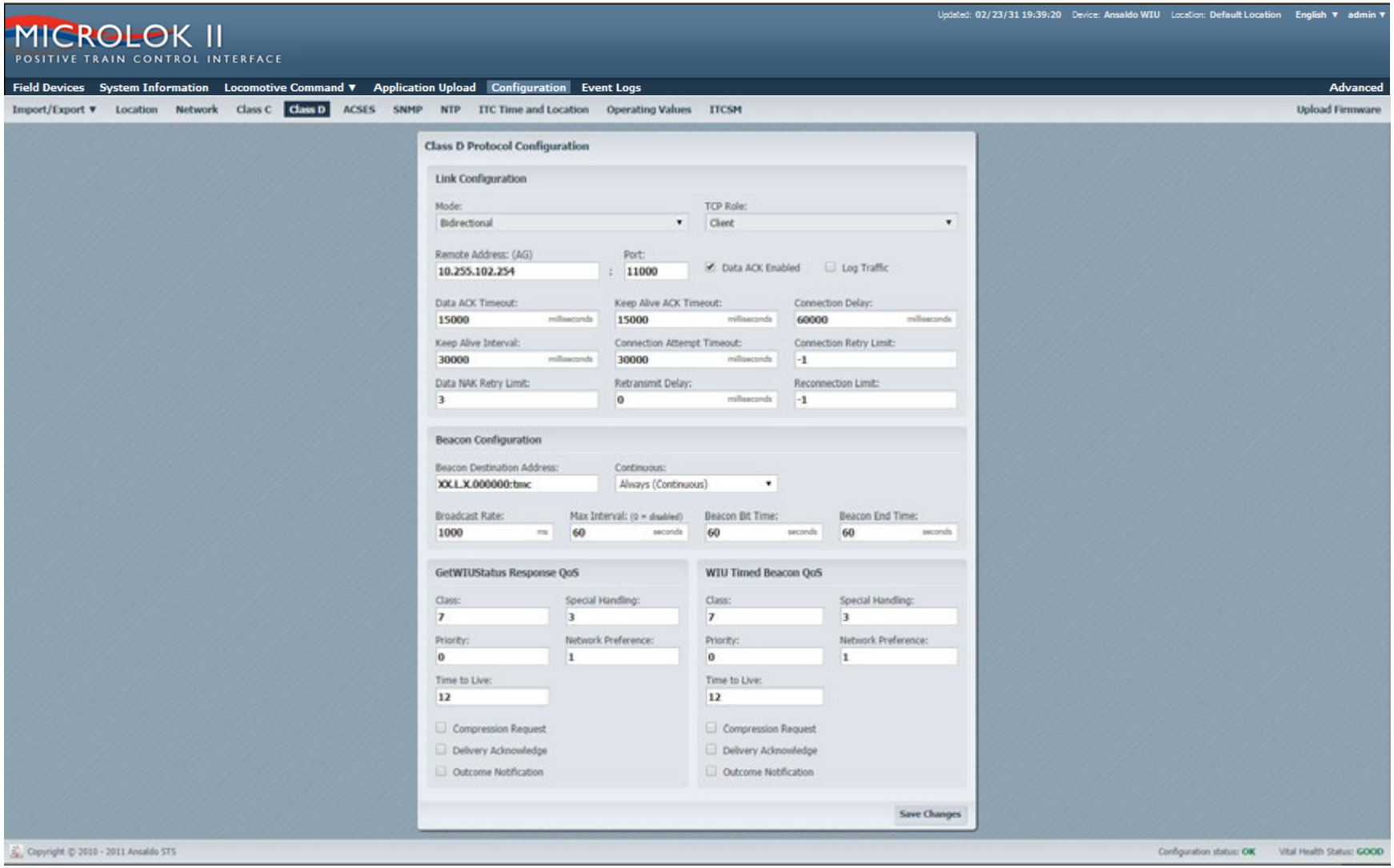


Figure 5–13. Class D Screen

5.4.8. Advanced Civil Speed Enforcement System (ACSES) Screen

The ACSES (Figure 5–14) screen is railroad-specific and provides configuration information for different application types.

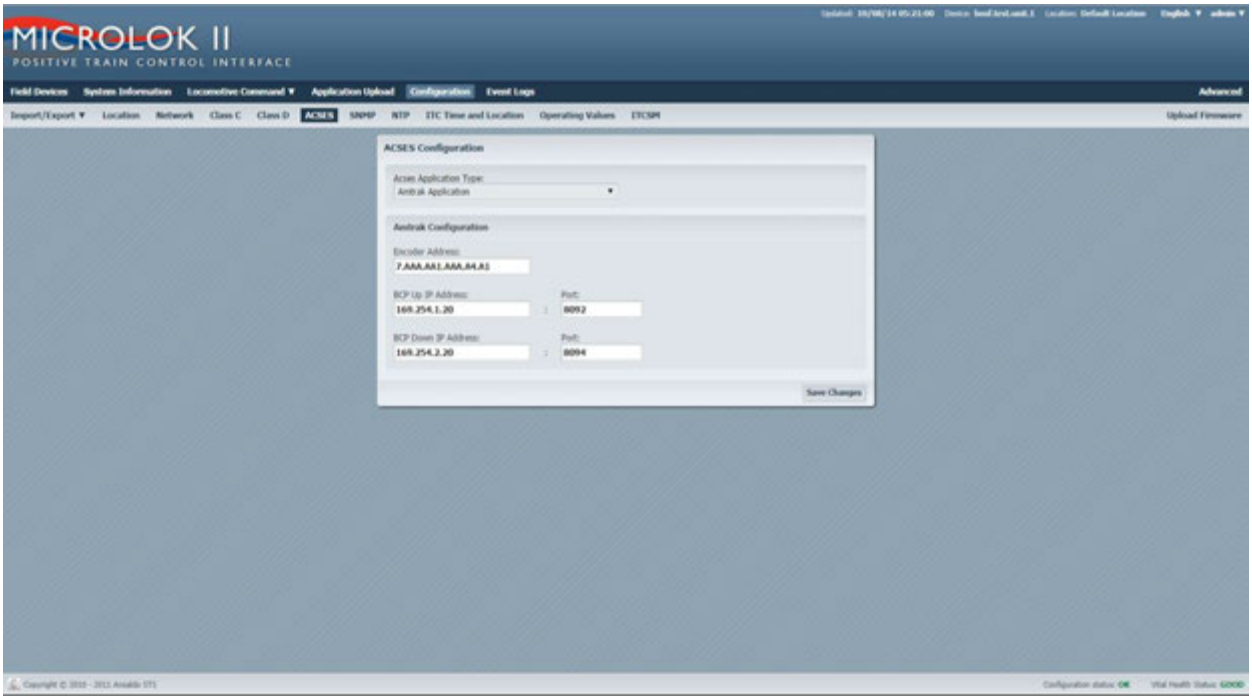


Figure 5–14. ACSES Screen

5.4.9. SNMP Screen

The SNMP screens provide SNMP parameter information and event logs. The SNMP screens are selected via a drop-down menu .The different types of SNMP screens are shown in Figure 5–15 through Figure 5–20. Changes can be made by entering information in the displayed boxes or by checking or unchecking a box(s) and saved by selecting the Save Changes button.

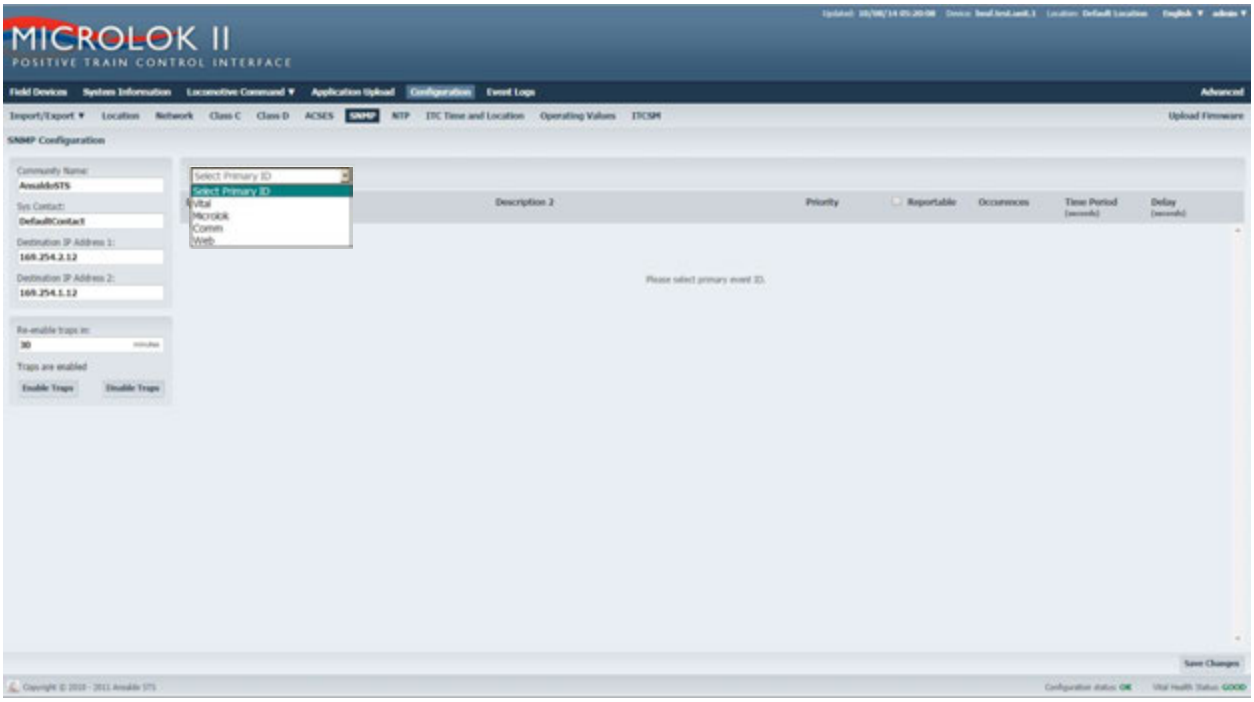


Figure 5–15. SNMP Drop-Down Menu Screen

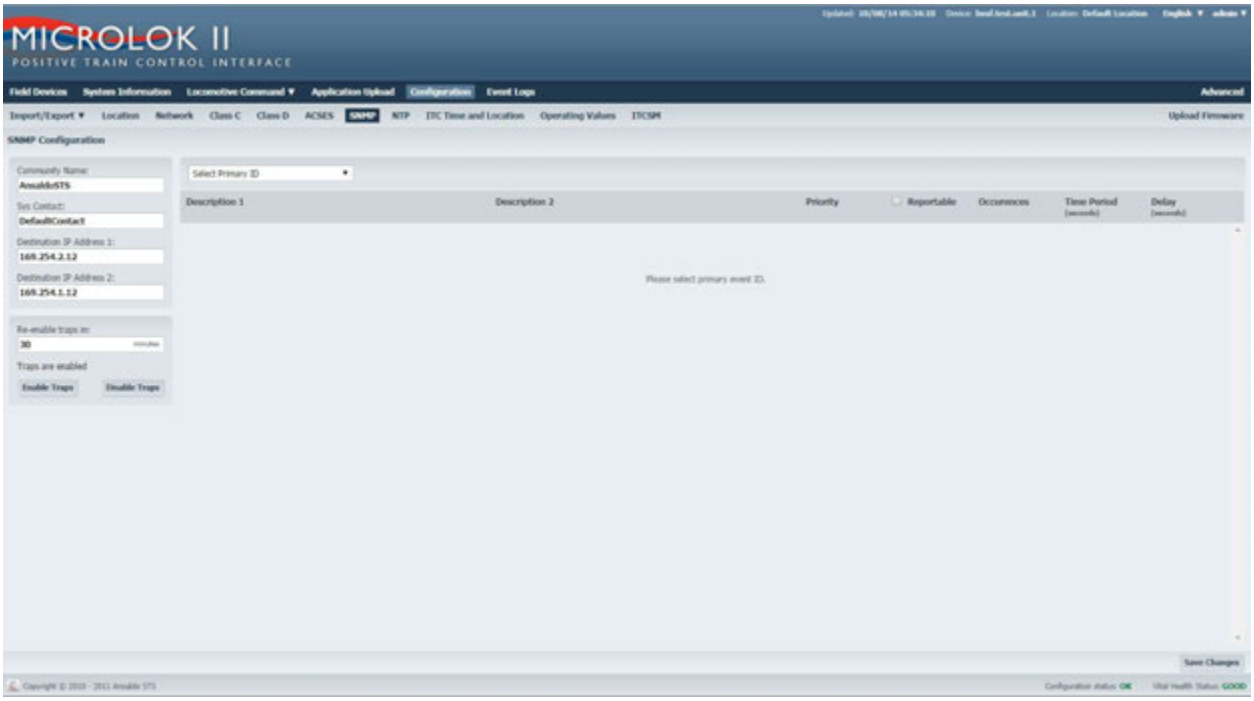


Figure 5–16. SNMP Select Primary ID Screen

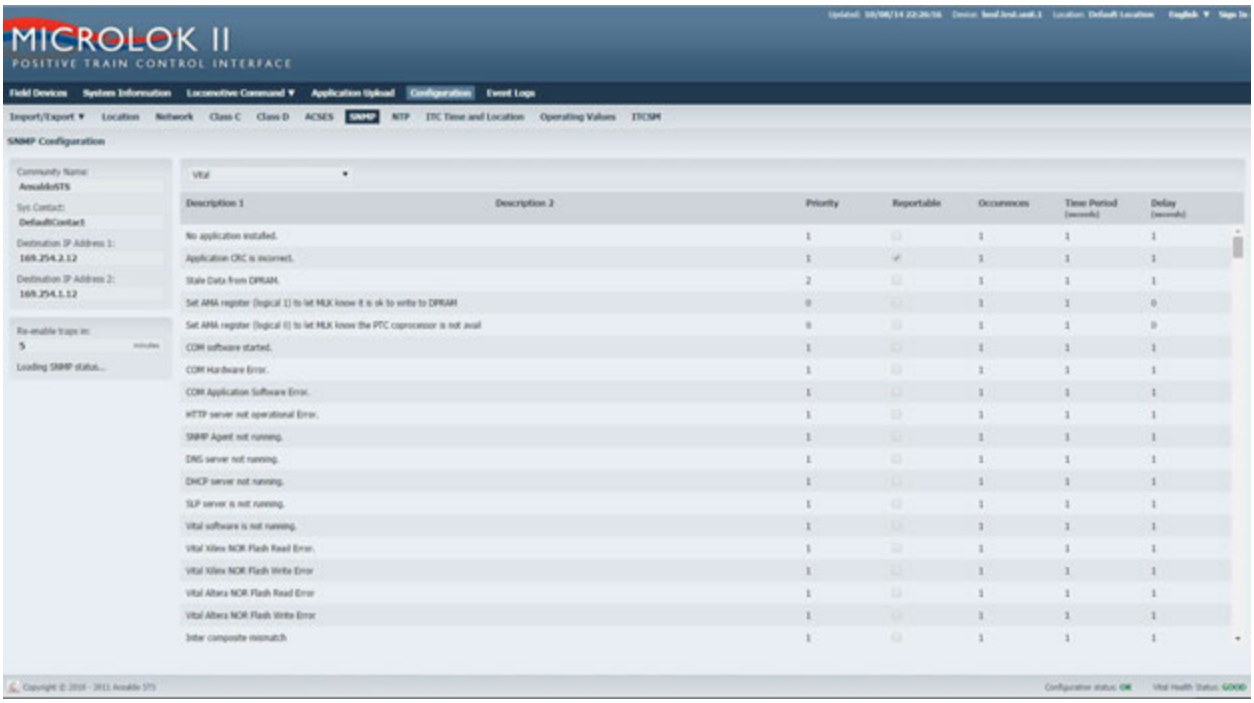


Figure 5–17. SNMP Vital Screen

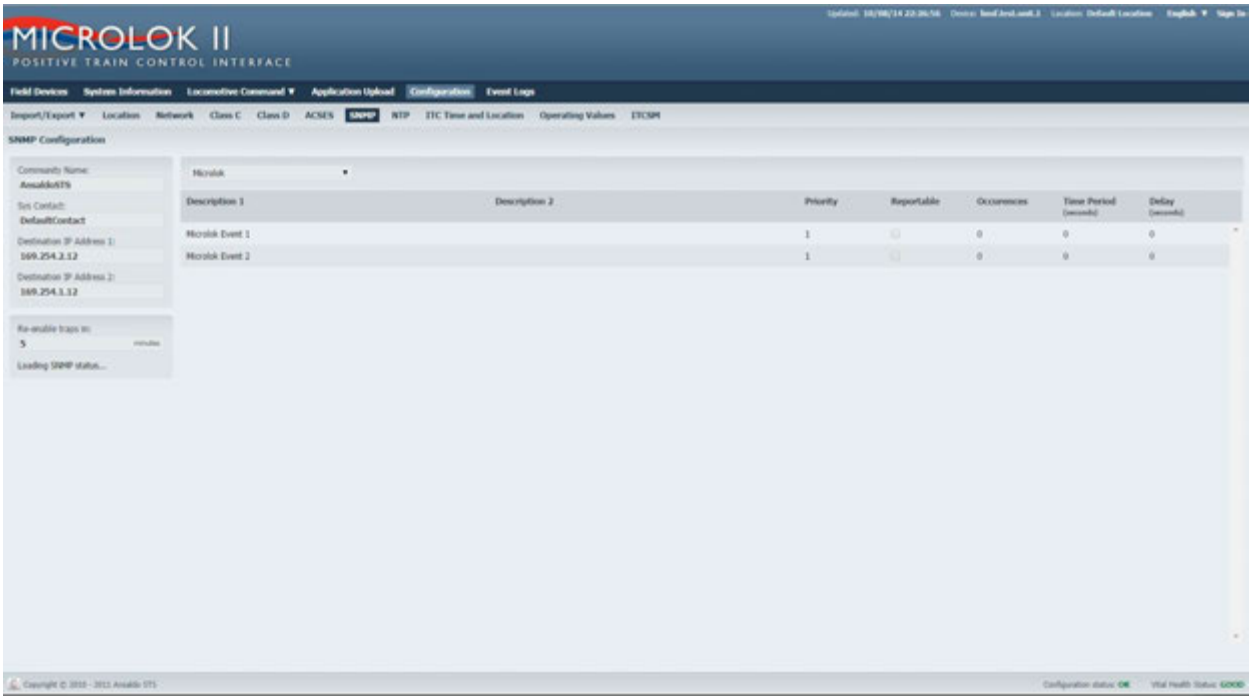


Figure 5–18. SNMP MicroLok Screen

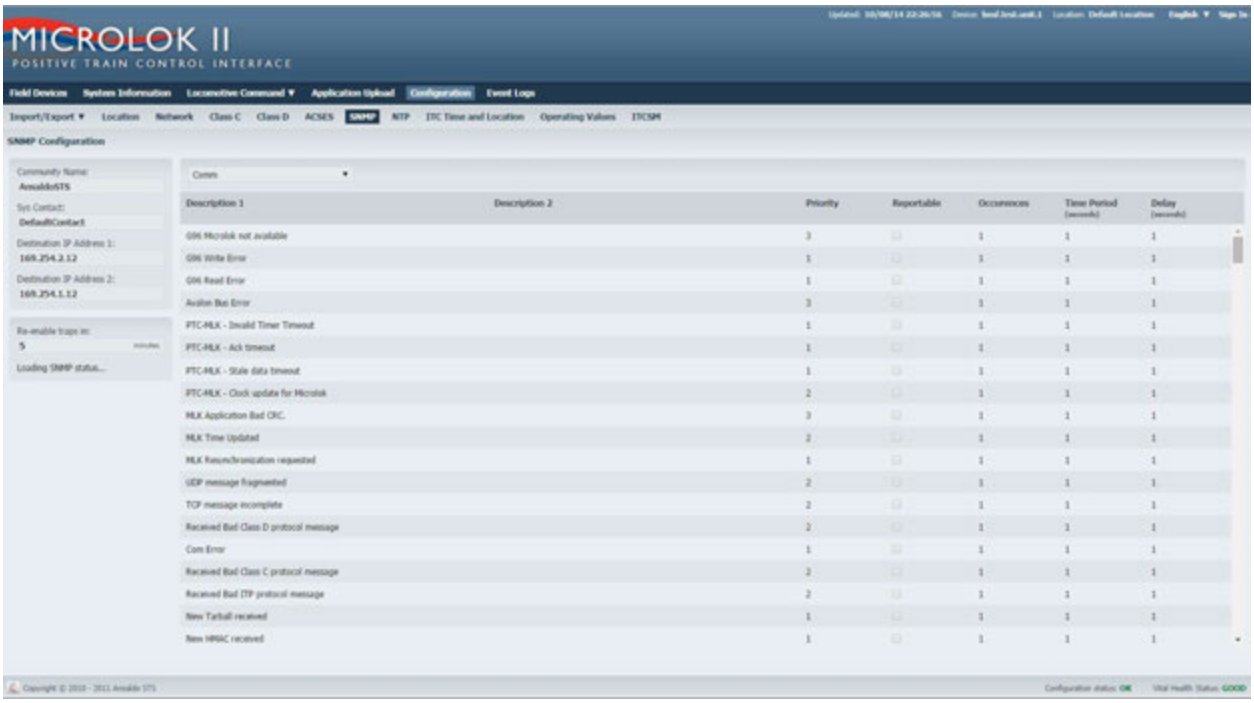


Figure 5–19. SNMP Comm Screen

.

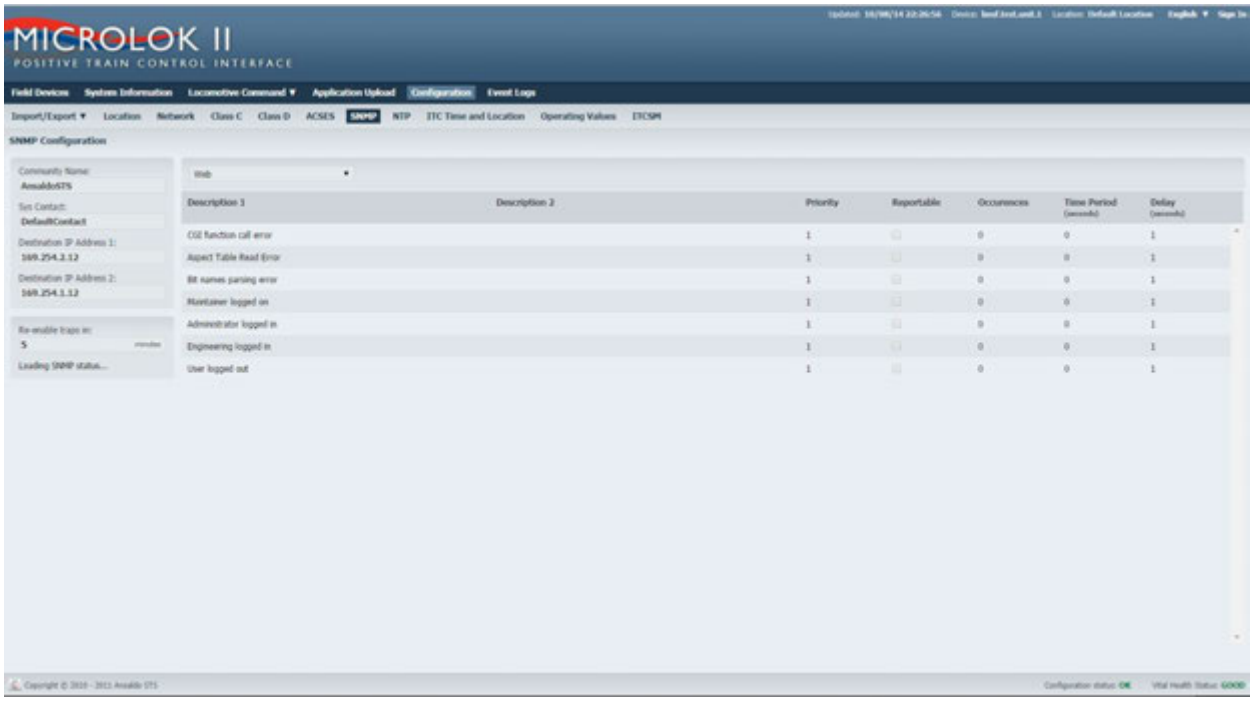


Figure 5–20. SNMP Web Screen

5.4.10. NTP Screen

The NTP (Figure 5–21) screen provides NTP configuration information. Changes can be made by entering information in the displayed boxes and saved by selecting the Save Changes button.

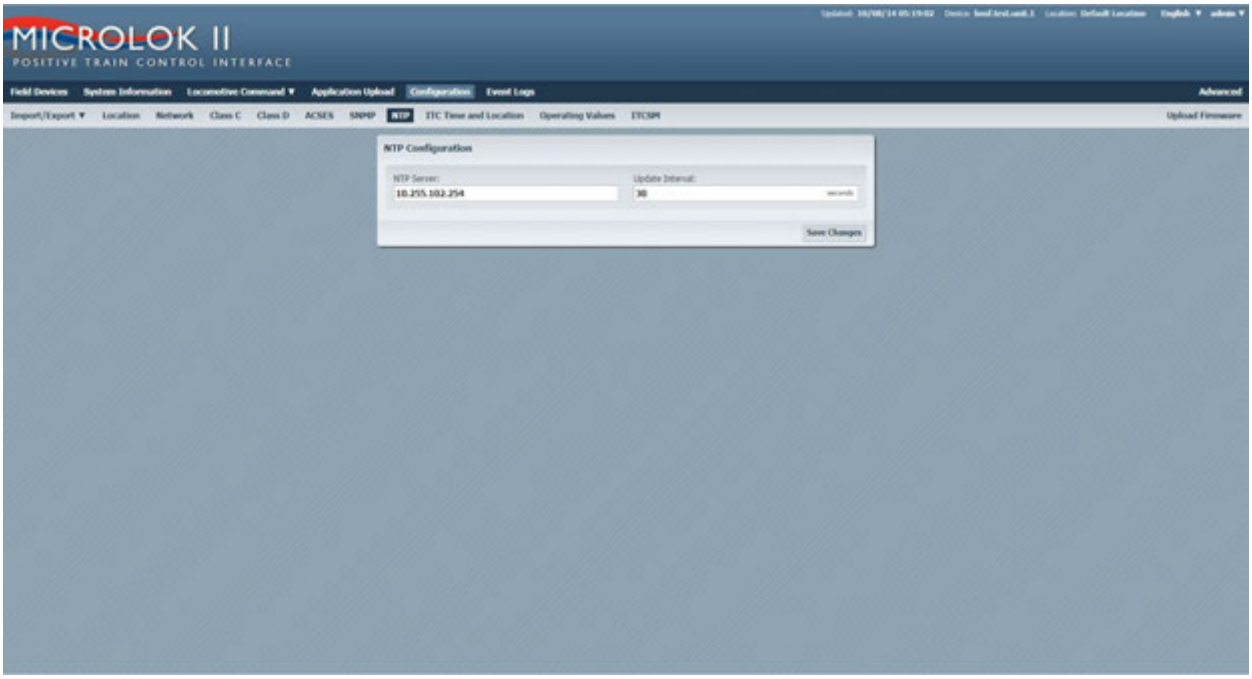


Figure 5–21. NTP Screen

.

5.4.11. ITC Time and Location Screen

The ITC Time and location screen (Figure 5–22) provides the time configuration settings.

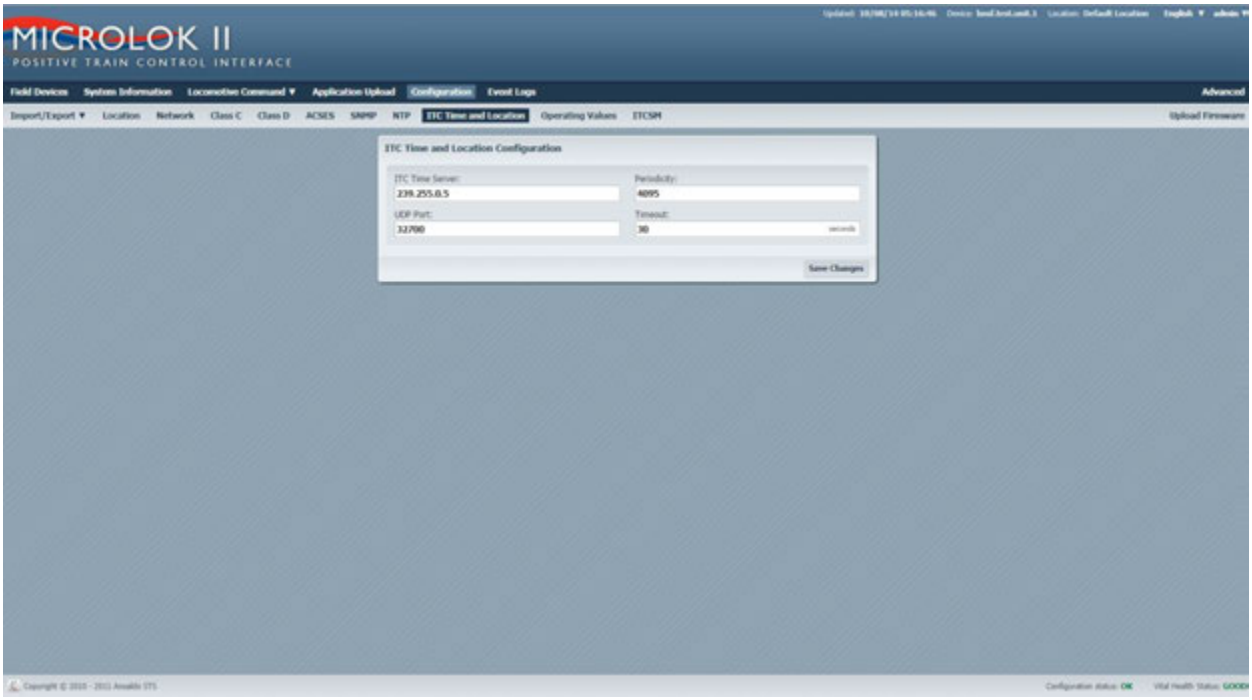


Figure 5–22. ITC Time and Location Screen

5.4.12. Operating Values Screen

The Operating Values screen (Figure 5–23) provides operating value settings.

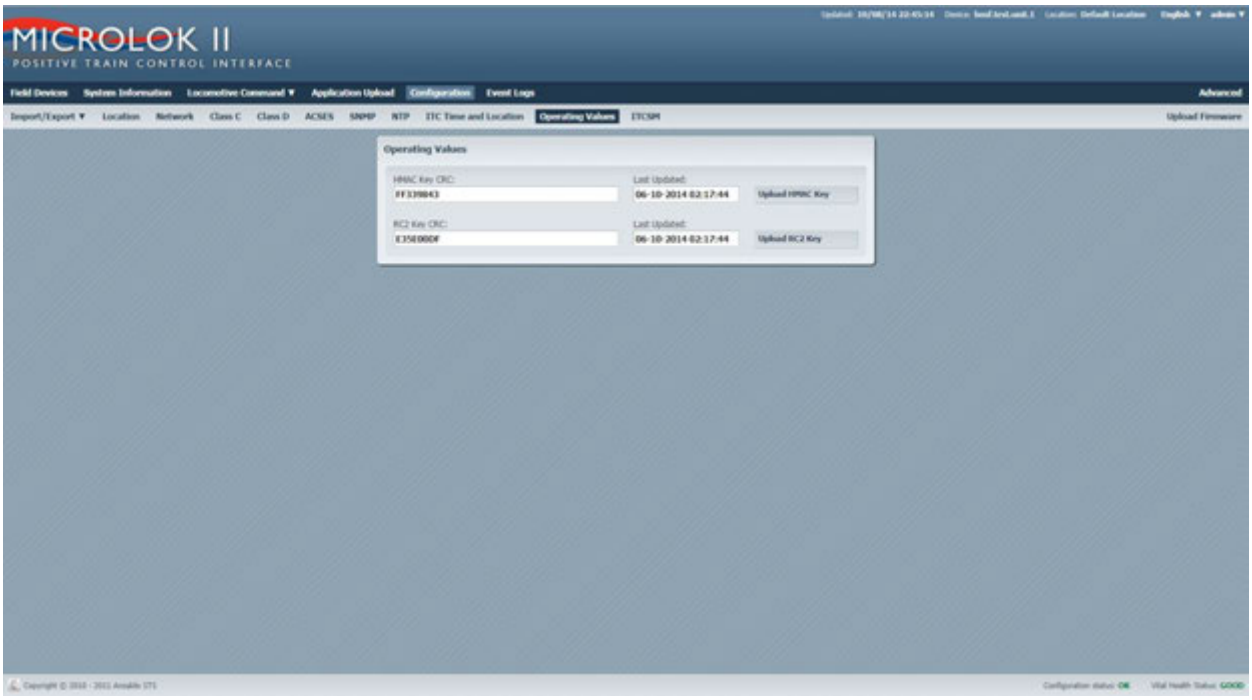


Figure 5–23. Operating Values Screen

5.4.13. ITCSM Screen

The ITCSM (Interoperable Train Control System Manager) screen (Figure 5–24) provides operating value settings.

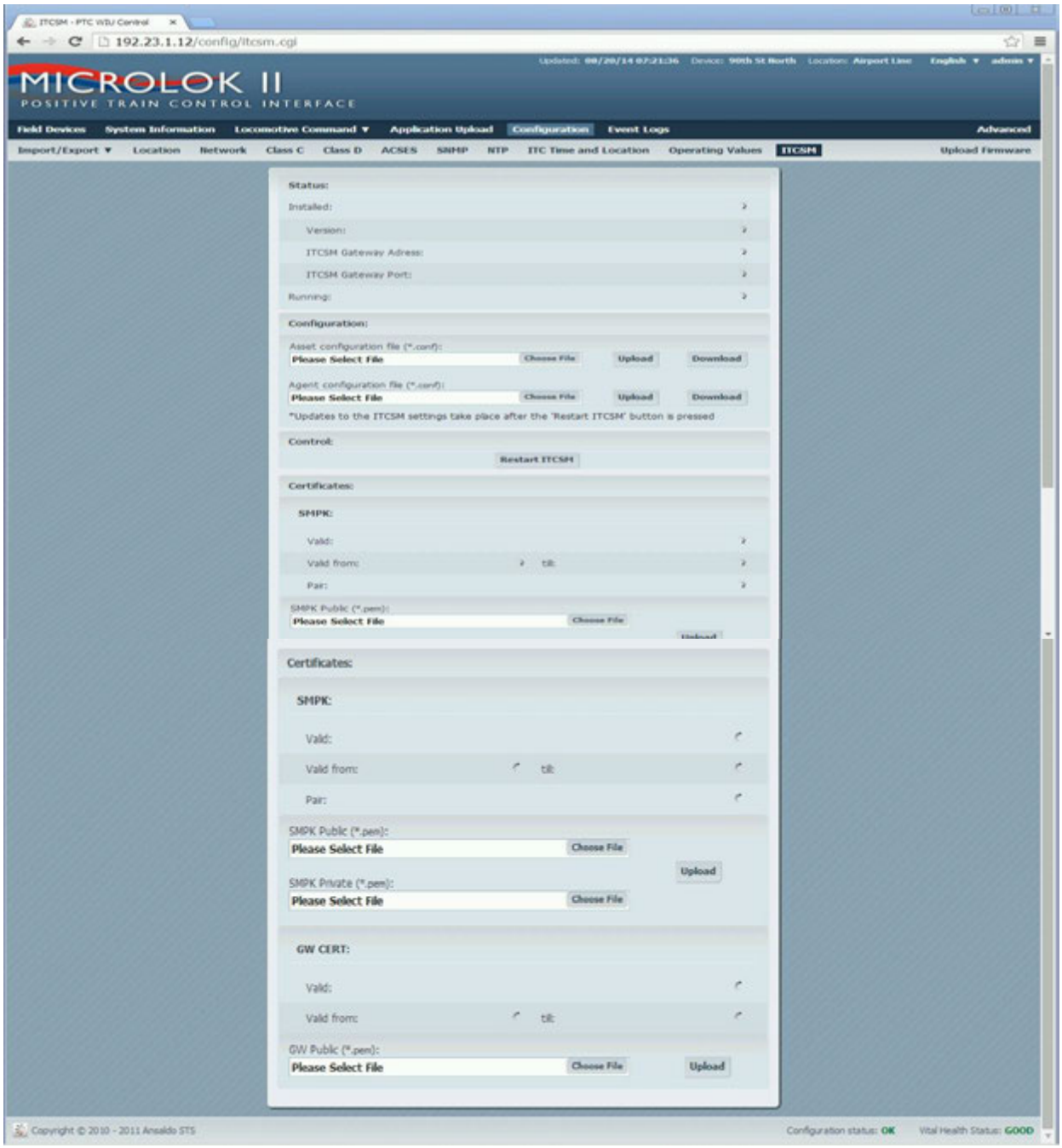


Figure 5–24. ITCSM Screen

5.5. Event Logs Screen

The Event Logs screen (Figure 5–25) provides a listing of system events. Events can be selected from the Source drop-down menu for the Browser Interface, Communication, MicroLok, Vital – Altera events. The log scan be cleared or exported to a file by selecting the Clear Logs or Export to File buttons at the lower right hand of the screen.

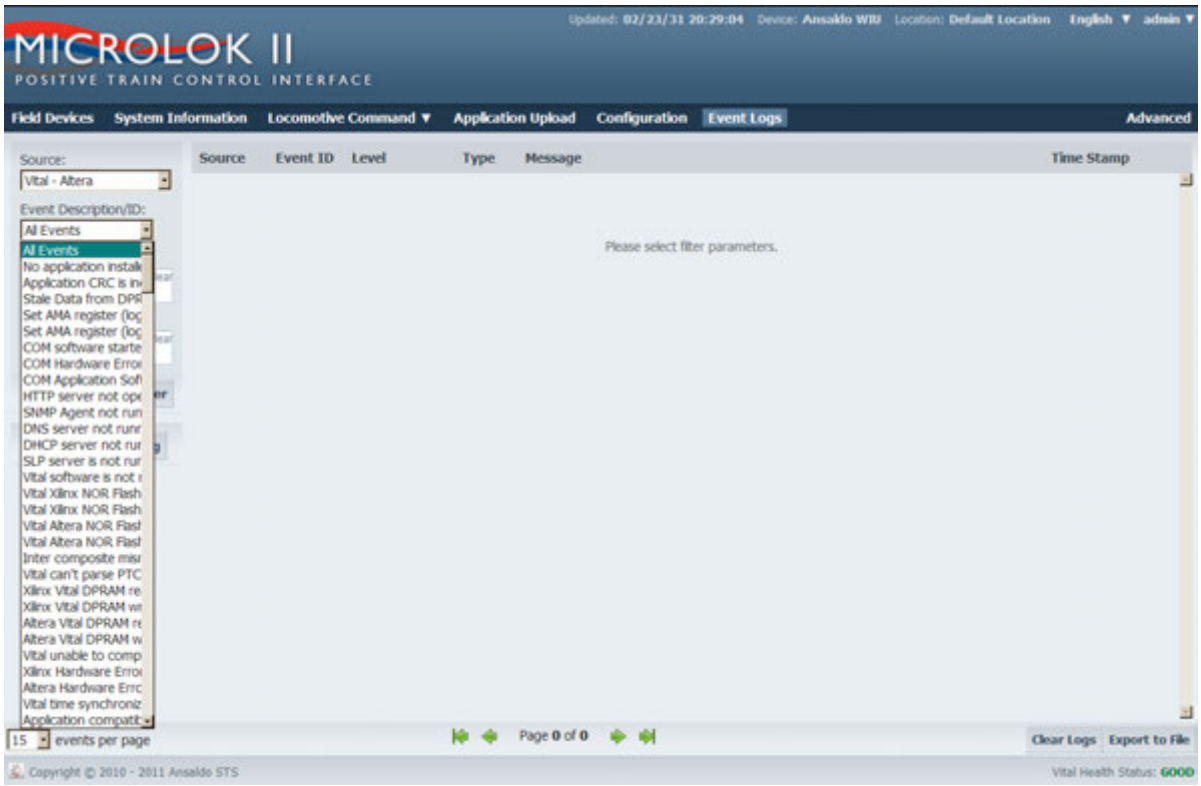


Figure 5–25. Event Logs Event Selection Screen

5.6. Advanced Screen

The Advanced screen (Figure 5–26) displays a list of services, local presence configuration, and user certificate information.

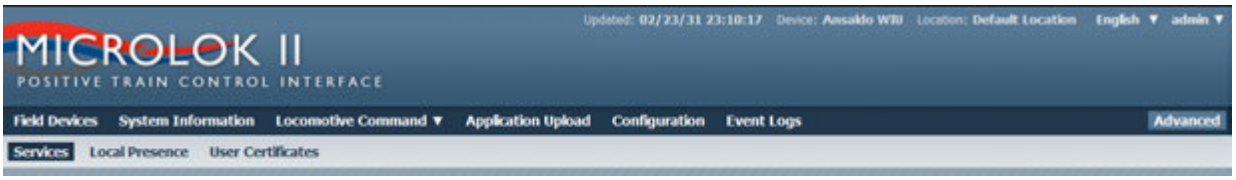


Figure 5–26. Advanced Screen

5.6.1. Services Screen

The Services screen (Figure 5–27) displays SNMP, Class D, SLP service, And TLS service. A checked box indicates that the selection is enabled. Changes can be made by checking or unchecking a box(s) and then selecting the Save Changes button.

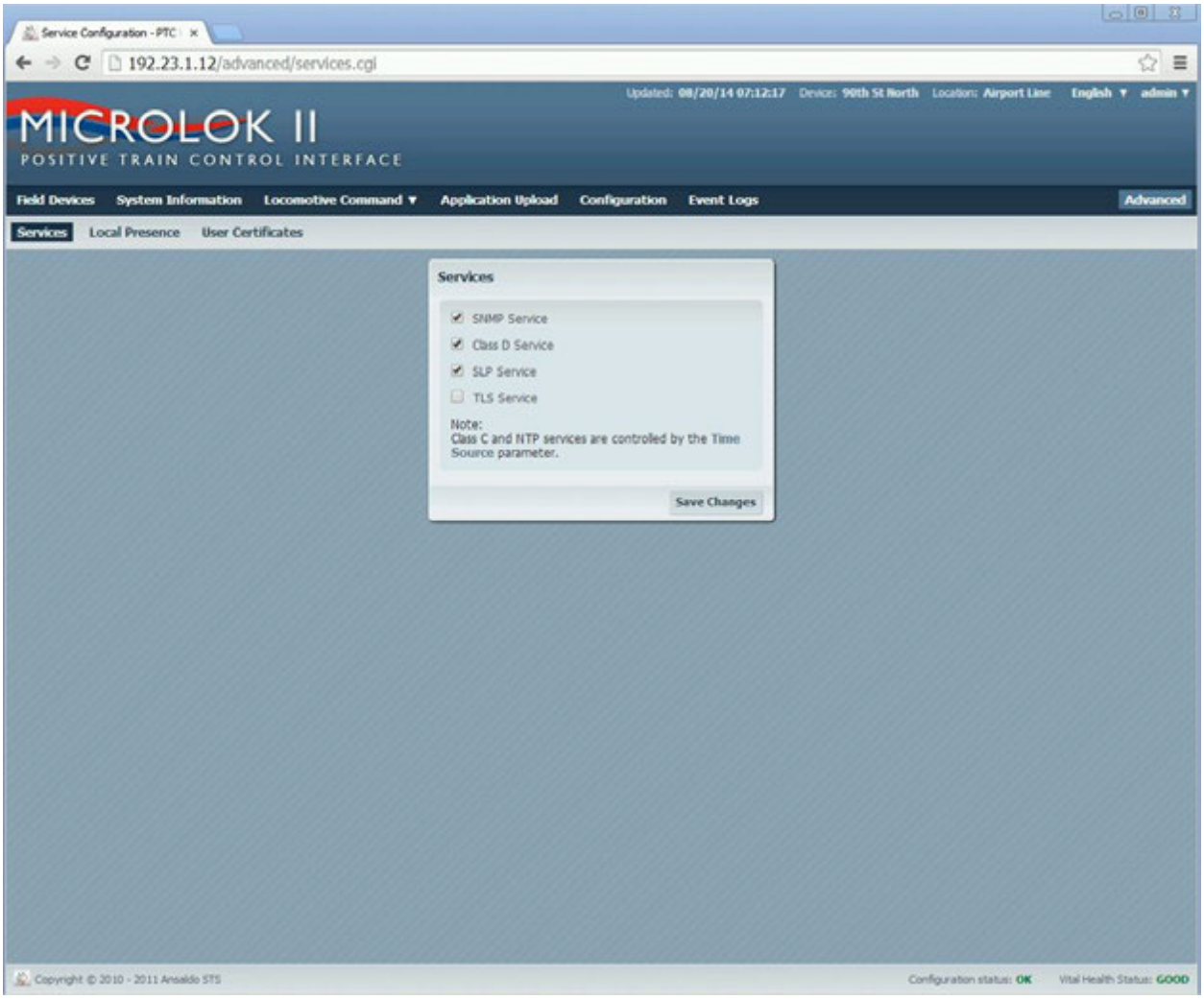


Figure 5–27. Services Screen

5.6.2. Local Presence Screen

The Local Presence screen (Figure 5–28) provides a list of local presence configuration parameters. A checked box indicates that you will be prompted to reset the WIU before the parameter can be enabled.

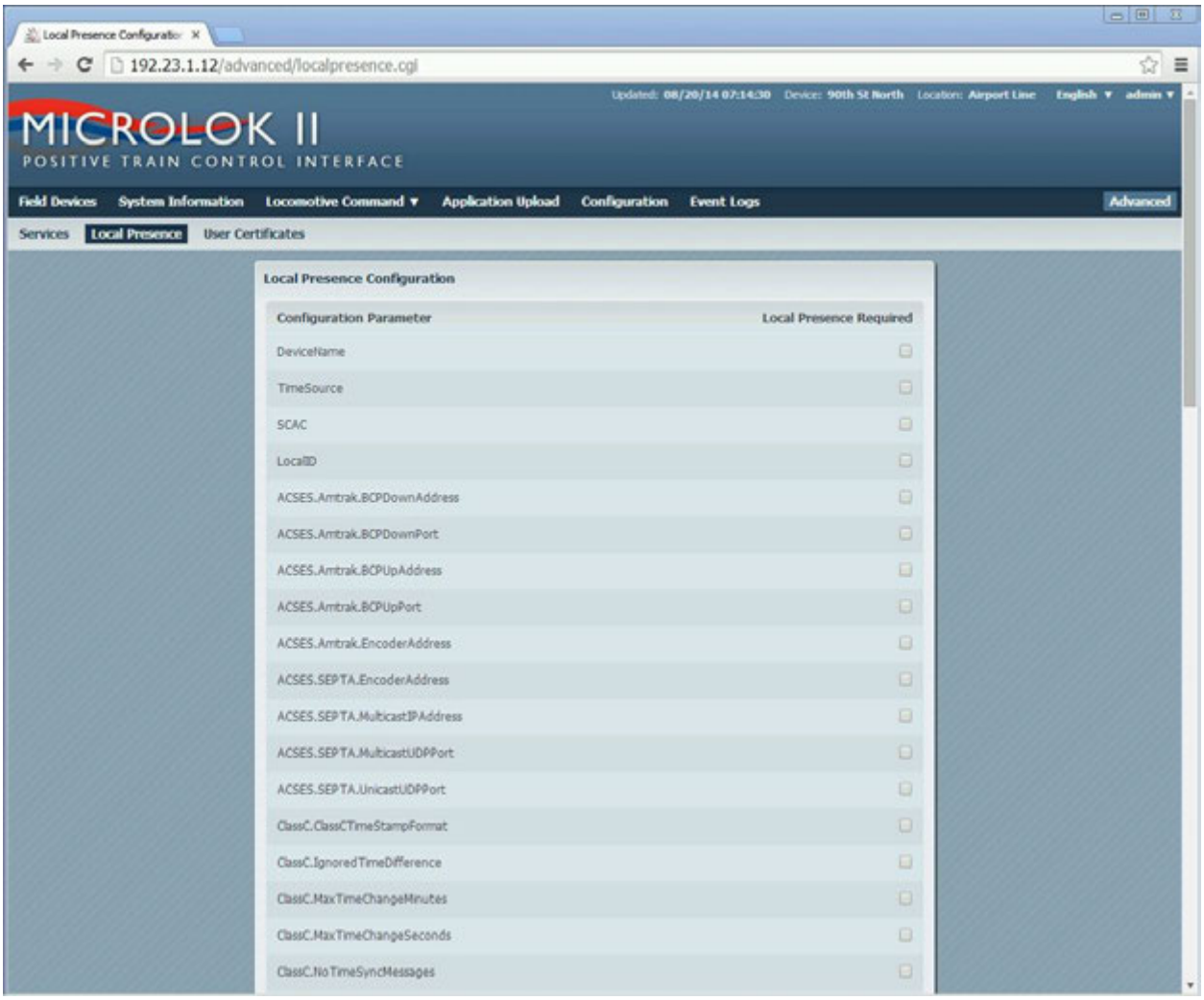


Figure 5–28. Local Presence Screen

5.7. User Certificates Screen

The User Certificates screen (Figure 5–29) allows the user to upload a new certificate.

Proceed as follows to upload a new certificate:

1. Click on the Choose File button on the User Certificates screen to display a standard file-open window.
2. Browse to the latest update file. Select the file and click OK to return and close the file-open window.
3. Click on the Upload button to begin the certificate upload process. Follow the onscreen instructions to complete the upload process.

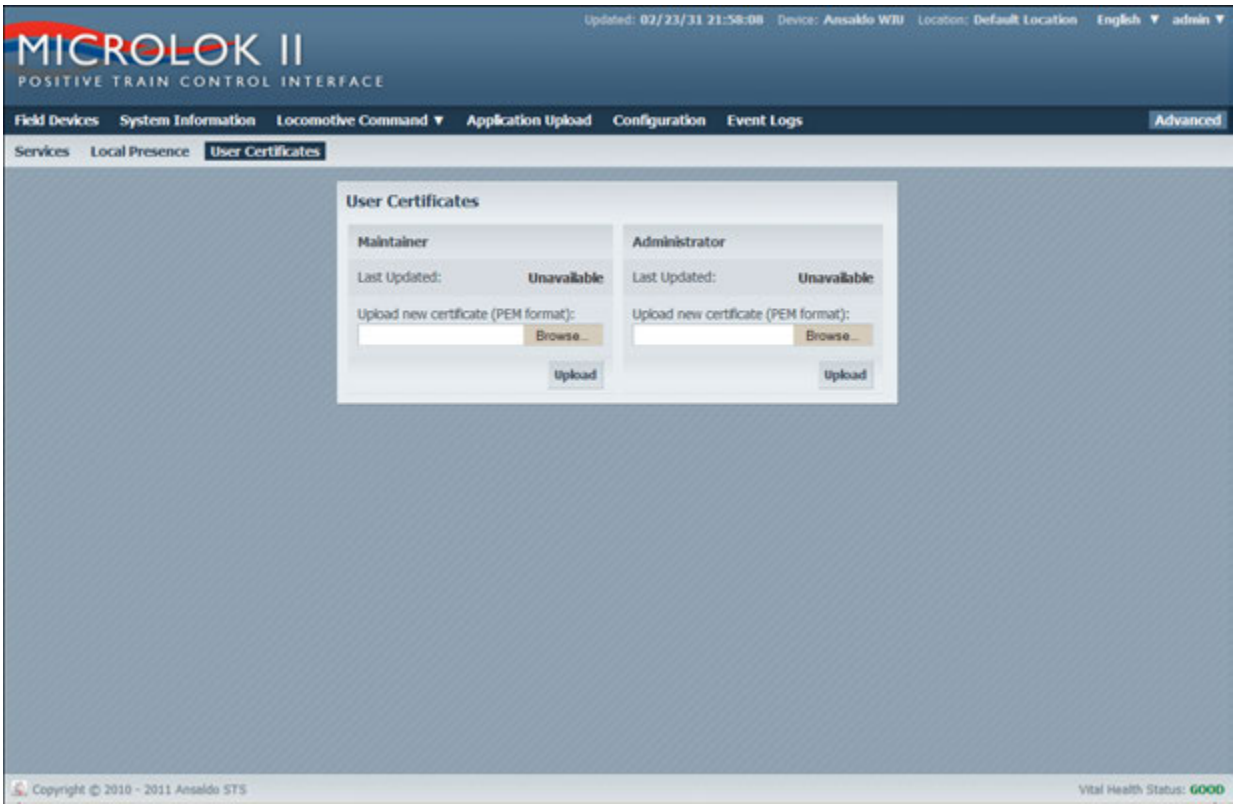


Figure 5–29. User Certificates Screen

6. UPLOADING FIRMWARE THROUGH THE WEB INTERFACE

The VitalNet Co-processor CPU is shipped from the factory loaded with the latest PTC Executive software available at the time of release. As updates occur to the PTC WIU specification due to interoperability requirements, changes in protocol specifications, or new feature releases from ASTS USA, it will be necessary to update the PTC software and firmware running on the device.

To update the Software/Firmware on the device, perform the following steps after logging in as an administrator:

1. Click on the Configuration tab located on the main menu bar of the page (Figure 6–1).
2. Click on the Upload Firmware link on the upper right side of the Configuration screen. The upload firmware screen will display (Figure 6–2).
3. Click on the Choose File button on the Update Device Firmware page to display a standard file-open window.
4. Browse to the latest update file (update files will be provided only by ASTS USA, and will have a .tar file extension). Select the file and click OK to return and close the file-open window.
5. Click on Force Update checkbox.
6. Click on the Update Firmware button to begin the firmware update process. Follow the onscreen instructions to complete the update process.
7. If you are loading a firmware package that is or 2.28 or lower, you must repeats Steps 4 and 6. Do not check the Force Update checkbox (Step 5) during the second upload.

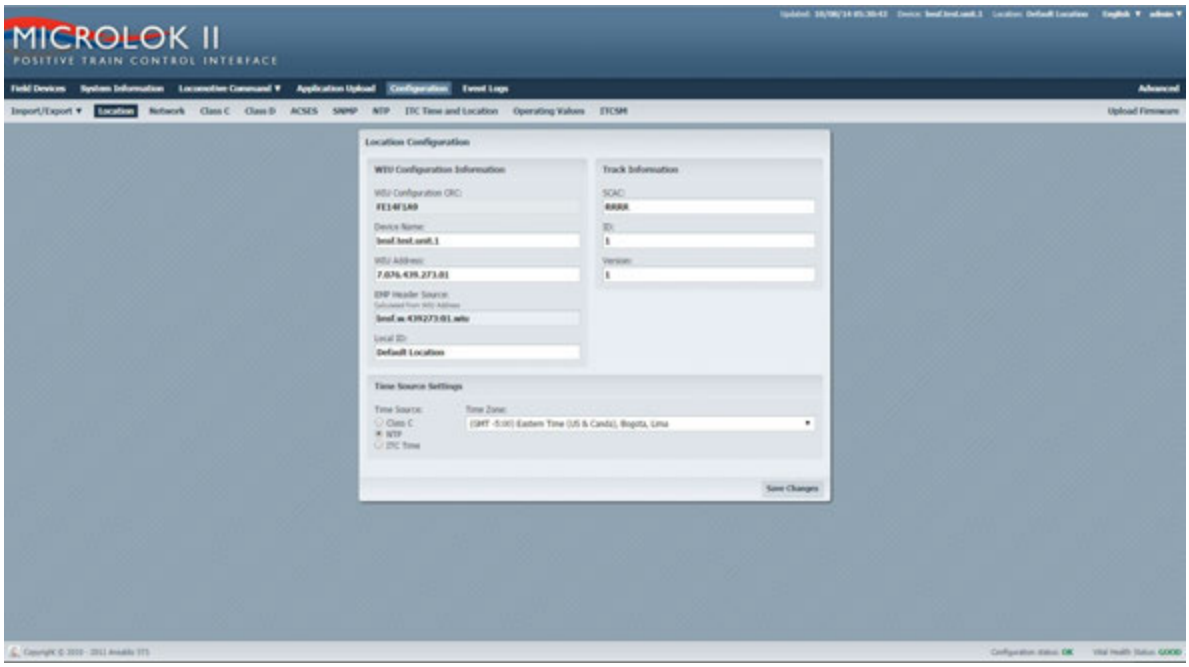


Figure 6–1. Configuration Screen

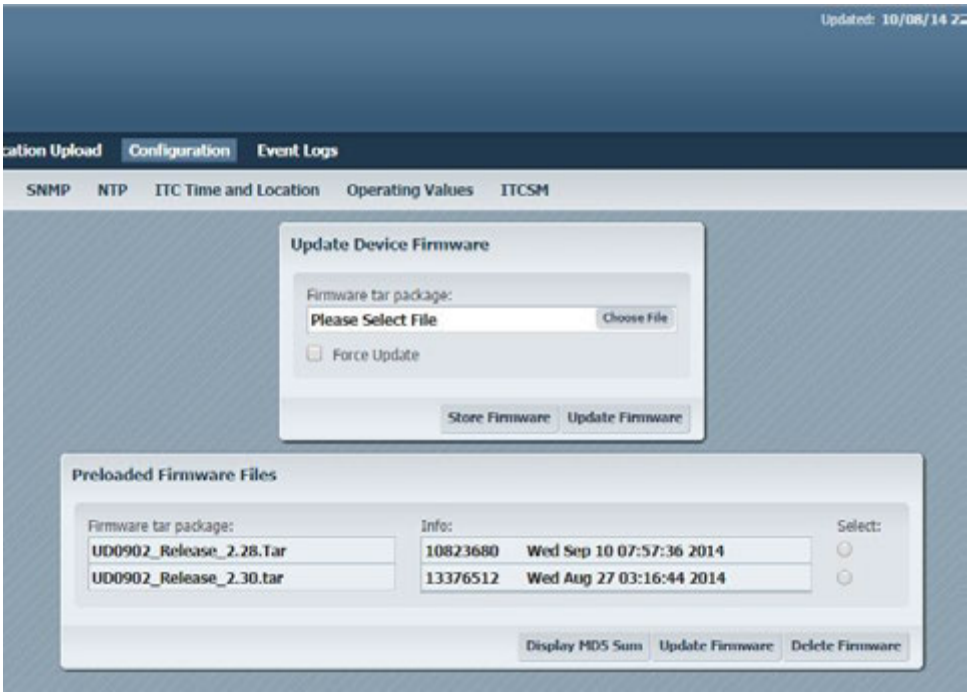


Figure 6–2. Upload Firmware Screen

- Click the Browse button and the Choose File to Upload window opens. Select the new tar package and click open. The .tar package name will appear in the Upload Device Firmware window. From here, you can store or upload the firmware. The stored firmware files are listed in the Preloaded Firmware File window. You can display the MD5 Sum, upload the firmware, or delete the firmware by clicking on the circle under Select next to the .tar file and then selecting the appropriate command at the bottom of the window. See Section 6 for uploading firmware information.

6.1. Firmware Storage

The WIU has the ability to store multiple firmware packages through the firmware upload screen. To do so perform the following steps when signed in as an administrator:

1. Click the Browse button and the Choose File to Upload window opens.
2. Select the new tar package and click open. The .tar package name will appear in the Upload Device Firmware window.
3. From here, you can store or upload the firmware. Choose the upload option.

Once uploaded, the stored firmware files are listed in the Preloaded Firmware File window. There are multiple options with these stored firmware packages which is accomplished by clicking on the circle under Select next to the .tar file and then selecting the appropriate command at the bottom of the window.

- Display the MD5 Sum of any of the stored firmware packages
- Upload one of the stored firmware packages to the WIU
- Delete any of the stored firmware packages

7. ANSALDO STS WIU APPLICATION BUILDER

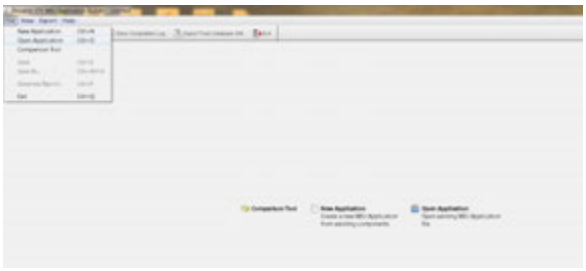
When building an application, the application can be configured to use Advanced Civil Speed Enforcement System Encoding (ACSES) encoding. ACSES encoding requires a CSV logic table. The table is railroad-specific and includes all switch positions and signal aspects within the span of track that the WIU unit is monitoring. An existing table can be selected by using the Browse button. A new Aspect Logic Table can be created by selecting the Create New button.

Figure 7–1. Create New WIU Application Screen

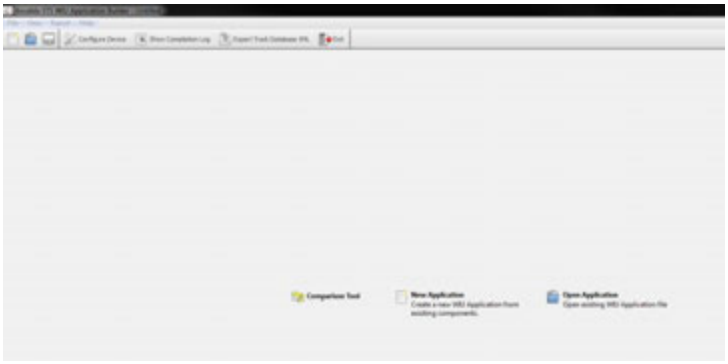
7.1. Opening an Existing Application

To begin setup on a WIU application, you must first create a new application. Proceed as follows:

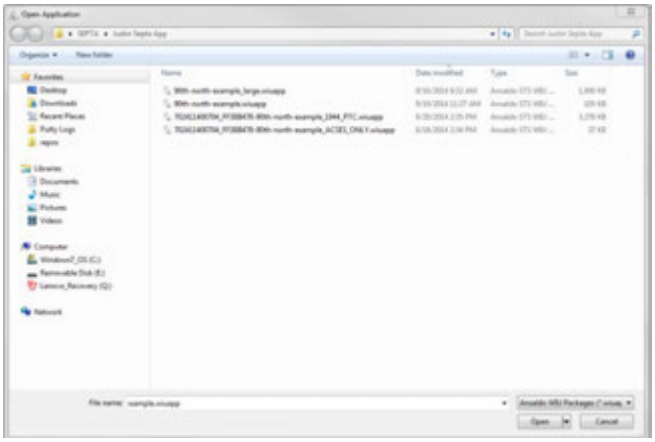
1. Select File/Open Application drop down menu in the top left of the application builder.



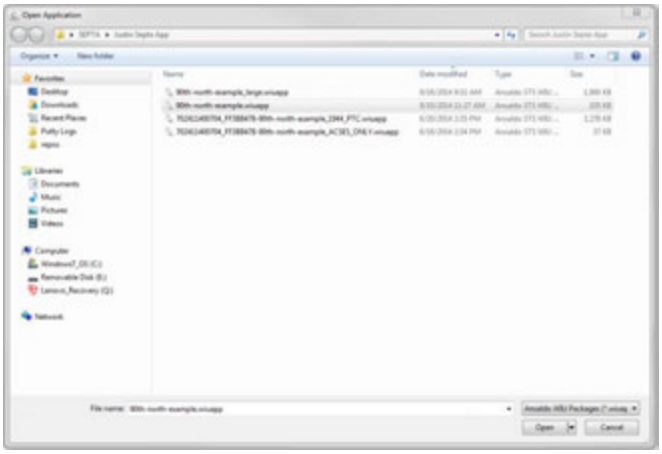
Or select the Open Application button in the center of the application builder window.



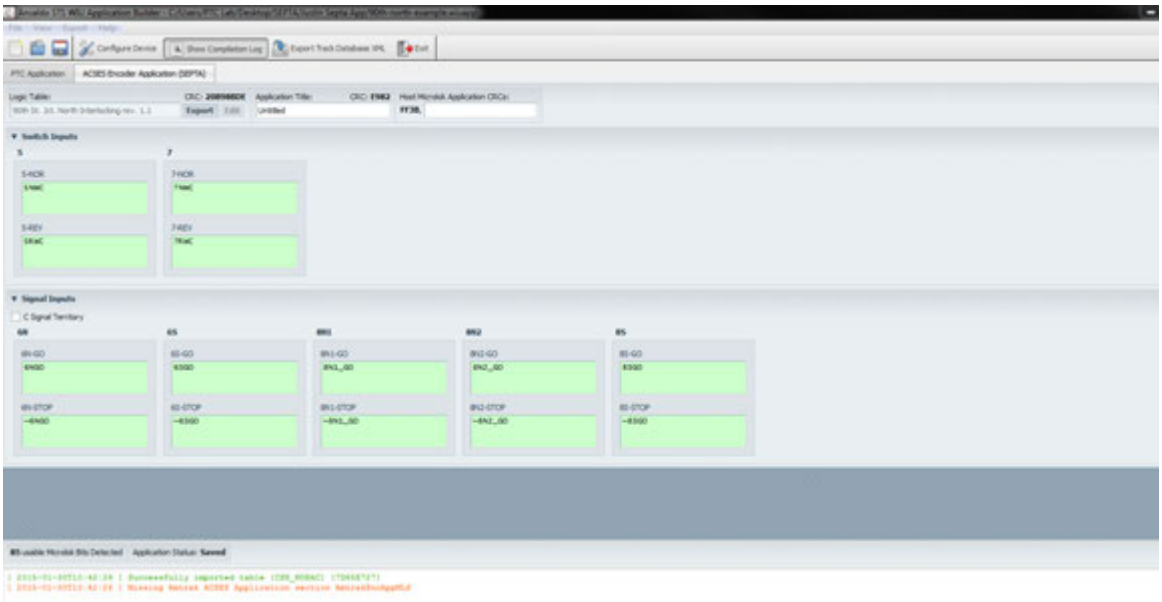
2. The window will appear for you to browse to the location on your computer where the application is stored.



3. Select the file and then select Open.

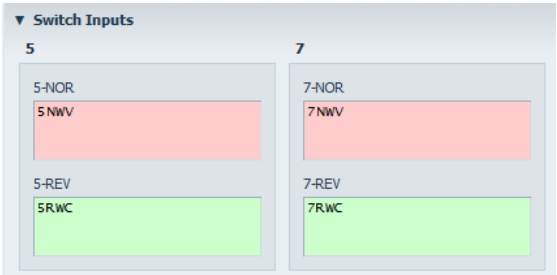


4. The selected file will open.

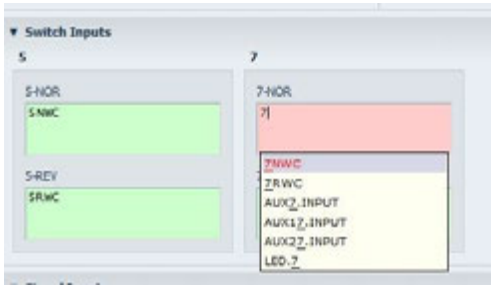


A green background for a device indicates a valid item. A red background indicates and invalid item. Messages will appear in green or red text at the bottom of the screen. The text will be green for a valid item. The text will be red for an invalid item.

If you type invalid text in a device window, the background will turn red.



As you begin to type information in a device window, a list of bits from the MicroLok .mlp file will display. Click on one of these bits to assign it to the device.



7.2. WIU Application Builder Software Creation

The WIU Application Builder is a tool used to create application files that will be uploaded to the WIU to set what actions it will take in certain situations. The application builder is on a disc as part of the WIU X-kit. Proceed as follows to install the WIU Application Builder:

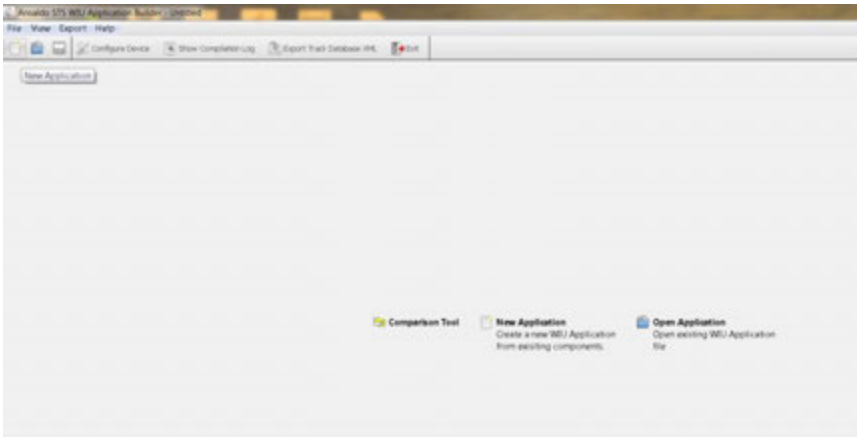
1. Insert the application builder disc into the computer.
2. Open the Start menu and click on the Computer menu item.
3. Double-click on the CD\DVD Drive. This will open up the drive where the App Builder Setup is located.
4. Double-click on the App Builder Setup to open the WIU Application Builder Setup Wizard.
5. Click the Next button, and after reading the license agreement, select I agree.
6. Make sure the check box next to Run WIU Application Builder is selected and click Install.
7. Once completed, click Finish, and the Ansaldo STS WIU Application Builder will open (Figure 7–2).

Figure 7–2. Application Builder Home Page

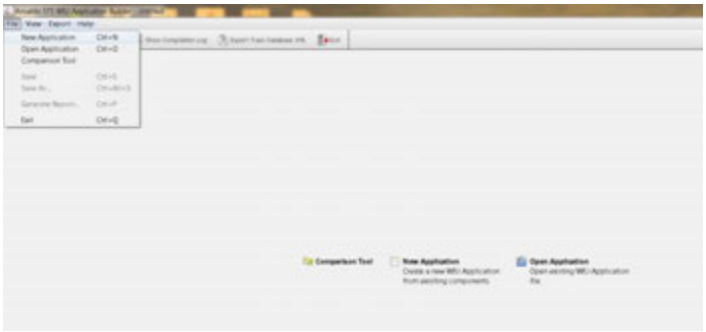
7.3. Starting a New Application

To begin setup on a WIU application, you must first create a new application. Proceed as follows:

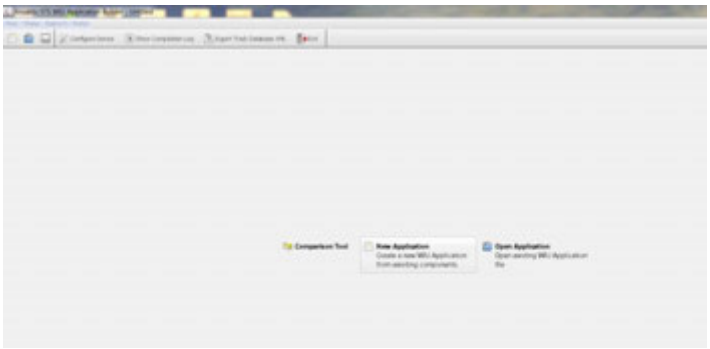
1. Select the New Application icon in the center of the application builder.



Or select the File dropdown menu in the upper left of the menu bar, and then click New Application



Or select the New Application button in the center of the application builder window.



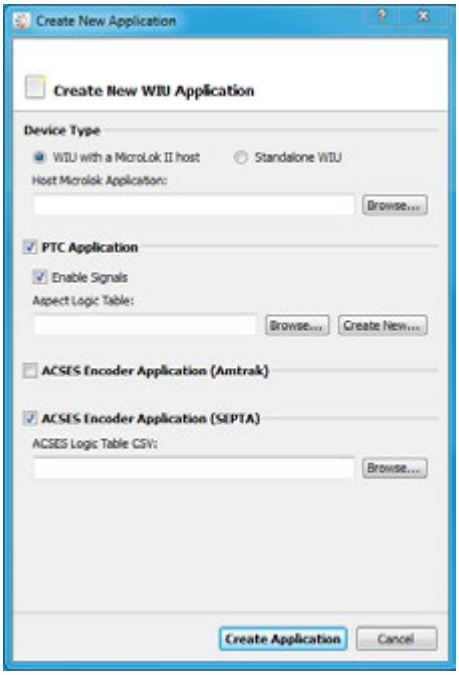
2. The Create New Application window will display.

3. You can choose to either set up an application for a WIU with a MicroLok II host or a Standalone WIU. Choose WIU with a MicroLok II host.
4. Select the desired file and choose Open. If the incorrect .mlp file is selected, the error screen shown in will appear when Create Application is selected.

Figure 7–3. .mlp Selection Error Screen

7.3.1. Creating a New SEPTA Application

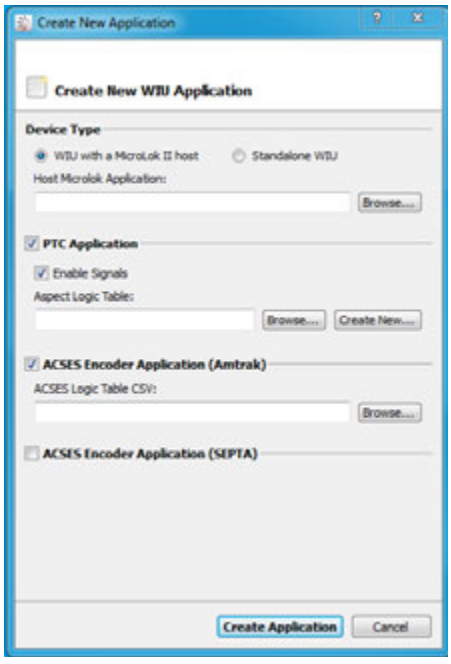
Refer to the procedure in Section 7.3 to create a new SEPTA application. When the Create New WIU Application window appears, browse and select the appropriate Device Type, PTC Application, and ACSES Encoder Application (SEPTA).check the ACSES Encoder Application (SEPTA) checkbox.



Select Create Application after all of the parameters have been selected.

7.3.2. Creating a New AMTRAK Application

Refer to the procedure in Section 7.3 to create a new AMTRAK application. When the Create New WIU Application window appears, browse and select the appropriate Device Type, PTC Application, and ACSES Encoder Application (AMTRAK).check the ACSES Encoder Application (AMTRAK) checkbox.



Select Create Application after all of the parameters have been selected.

7.4. Saving an Application

Proceed as follows to create a new application:

1. Select Save icon in the top left or the application builder or select the File dropdown menu and then select Save (**Error! Reference source not found.**).
2. If the save was successful, text messages that indicate a successful save will appear at the bottom of the window. An example of a successful save message is shown in Figure 7–4.

```
[ 2015-02-05T10:28:22 ] Generating MLP...
[ 2015-02-05T10:28:22 ] Processing Compiler Output...
[ 2015-02-05T10:28:22 ] Vital Logic Compiler Log:

                        MICROLOK II Compiler Version 8.50 (N800102-0001)

                        Wednesday April 23, 2014 12:25:29

                        Compiling C:\Users\PTCLAB~1\AppData\Local\Temp\ptcapp.ml2
                        Image size: 0x23C6
                        Application Image Checksum: 04c2

                        Compile complete. 0 errors, 0 warnings.
                        Compilation log written to C:\Users\PTCLAB~1\AppData\Local\Temp\ptcapp.mll

[ 2015-02-05T10:28:22 ] WIU Configuration PTC CRC : 835C563C
[ 2015-02-05T10:28:22 ] WIU Configuration ACSES CRC : 835C3407
[ 2015-02-05T10:28:22 ] Successfully compiled selected components.
[ 2015-02-05T10:28:22 ] Saving to C:\Users\PTC Lab\Desktop\SEPTA\Factory Merged Apps\Merged Factory App.wiuapp...
[ 2015-02-05T10:28:22 ] WIU Package Saved.
[ 2015-02-05T10:28:22 ] Available sections:  WIU Configuration, PTC Application.
```

Figure 7–4. Successful Save Text Messages

3. If the save was unsuccessful, text messages that indicate an unsuccessful save will appear at the bottom of the window. An example of an unsuccessful save message is shown in Figure 7–5.

```
[ 2015-02-05T10:28:31 ] ================================
[ 2015-02-05T10:28:31 ] Initiated application generation.
[ 2015-02-05T10:28:31 ] Compiling PTC Application...
[ 2015-02-05T10:28:31 ] Generating ML2...
[ 2015-02-05T10:28:31 ] Compiling SEPTA ACSES Encoder Application...
[ 2015-02-05T10:28:31 ] ACSES ENCODER: Processing Compiler Output...
[ 2015-02-05T10:28:31 ] ACSES ENCODER: MLP Generation Error:

                        MICROLOK II Compiler Version 8.50 (N800102-0001)

                        Wednesday April 23, 2014 12:25:29

                        Compiling C:\Users\PTCLAB~1\AppData\Local\Temp\encapp.ml2

                        Compile complete. 1 errors, 0 warnings.
                        Compilation log written to C:\Users\PTCLAB~1\AppData\Local\Temp\encapp.mll

[ 2015-02-05T10:28:31 ] ACSES Encoder Application failed to compile. Changes will not be saved.
```

Figure 7–5. Unsuccessful Save Text Messages

7.5. Device Configuration SETUP

The Configure Device selection window (Figure 7–6) in the PTC Application Builder gives the user the ability to set the various configuration options that are necessary for proper setup of the device.

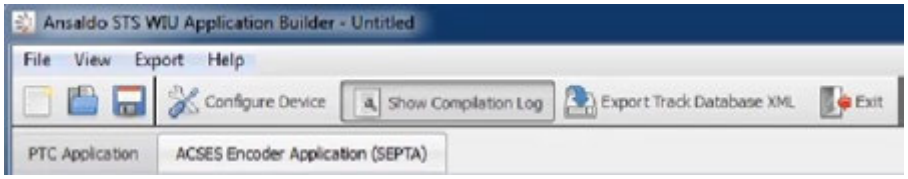


Figure 7–6. Configure Device Screen

7.5.1. Location Properties

The Location Properties section (Figure 7–7) contains general configuration parameters that must be set for each Ansaldo VitalNet WIU installation. These parameter values are used to uniquely identify each WIU device, and assist in Configuration Management of the device throughout the customer's PTC network. See Table 7-1 for a description of the Location Configuration parameter settings.

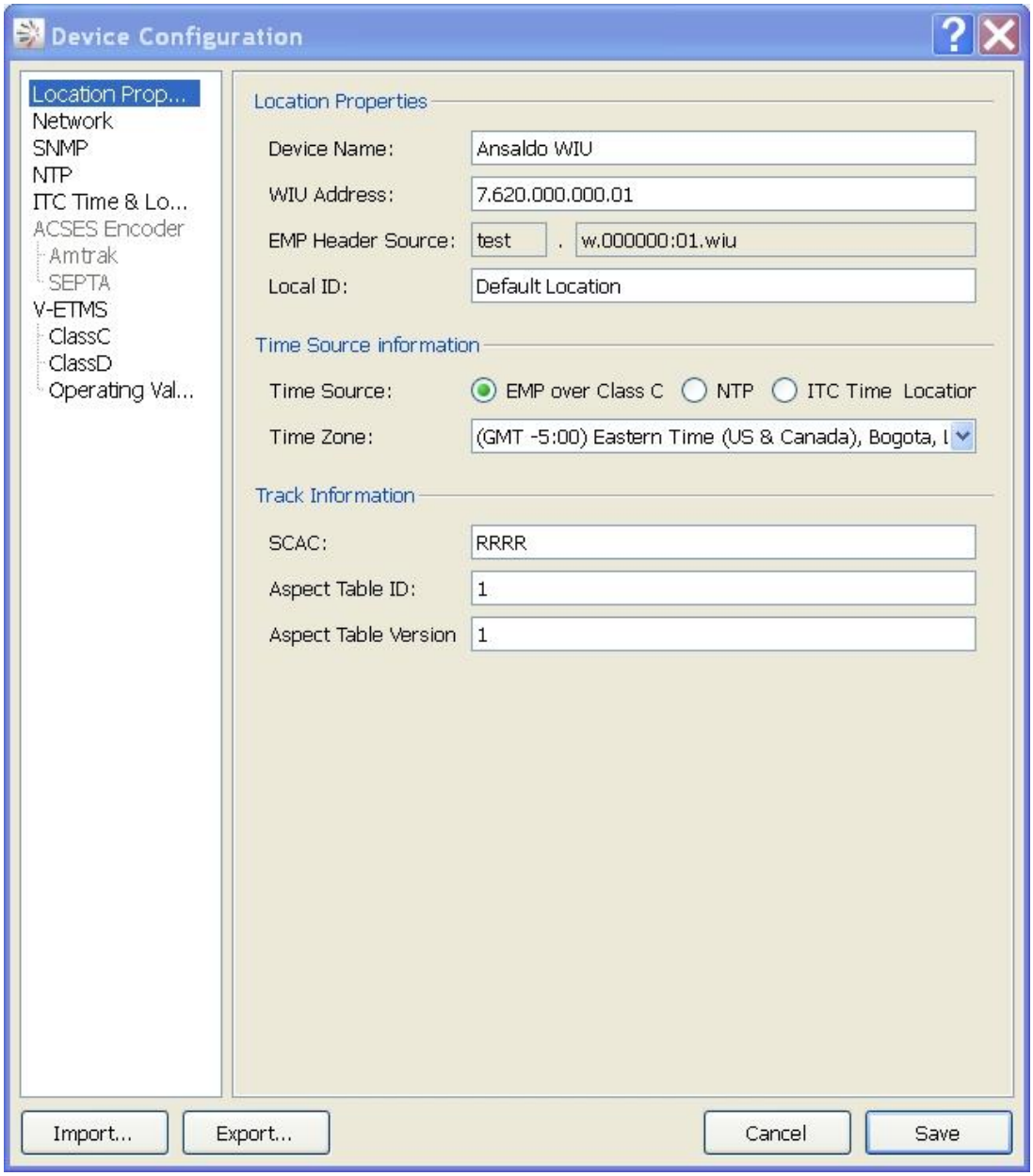


Figure 7–7. Location Settings

Table 7-1. Location Properties Parameters

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Device Name	This is the user-configured name displayed at the top of the PTC Configuration tool, so that remote users can verify that they have accessed the correct device	**Free-text** (50 alphanumeric characters) **Default Value** *Ansaldo WIU*	N/A	N/A
WIU Address	The unique 48-bit WIU Address field is in the format 7.RRR.LLL.GGG.DD, where: • 7 = WIU address type identifier • RRR = Railroad Number • LLL = Routing Region Code • GGG = Location Code • DD = Device Number	**Free-text** (numeric values only) **Default Value** *7.000.000.000.00*	N/A	N/A
EMP Header Source Address	This field identifies the WIU source address used when sending Wayside Status Messages from the WIU (Refer to Appendix A of the EMP Message Format Specification for more details on the format of this field)	**Free-text** (null-terminated string with a limit of 64 bytes.) **Default Value** *"null"*	N/A	N/A
Local ID	This is the user-configured device location displayed at the top of the PTC Configuration tool, so that remote users can verify that they have accessed the correct device location	**Free-text** (50 alphanumeric characters) **Default Value** *"Location ID"*	N/A	N/A
Time Source	This parameter specifies whether the WIU will obtain its time update messages via Class C messages from the EMP, or whether time updates will be provided from and NTP Server on a network	**Radio Button** • EMP • NTP **Default Value** *EMP*	N/A	N/A
Time Zone	This parameter specifies the Hour offset from Greenwich Mean Time which is used for display within the web configuration screens and used for error/event log timestamps. The time zone setting has no effect on communications to the Wayside Communications Module.	**Drop-down List** **Default Value** *GMT-5:00 (Eastern)*	N/A	N/A

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
SCAC	This is the user-configured Standard Carrier Alpha Code (SCAC) – a unique two-to-four-letter code used to identify transportation companies – used to populate information in the track database .xml export file. The SCAC value does not have any other effects on settings for the device	**Free-text** (4 alpha characters) **Default Value** *blank*	N/A	N/A
Aspect Table ID	This field displays the name and CRC of the currently loaded aspect table being used for PTC application design. If no aspect table is being used (dark territory location), this field will show "N/A"	**Read-only** **Default Value** *N/A*	N/A	N/A
Aspect Table Version	This field displays the version number of the currently loaded aspect table being used for PTC application design. If no aspect table is being used (dark territory location), this field will show "N/A"	**Read-only** **Default Value** *N/A*	N/A	N/A

7.5.2. Network

The Network section (Figure 7-8) in the Device Configuration Setup gives the user the option to modify network controls, and view the relevant network information within the configuration. The IP address, subnet mask, gateway, and DNS Server are all viewable in the network configuration window if the user is using a static connection type; if the user is using a dynamic host configuration protocol, then this information is disabled (irrelevant). The options are repeated for Ethernet Port 1 (eth0) and Ethernet Port 2 (eth1). See Table 7-2 for a description of the network configuration parameter settings.

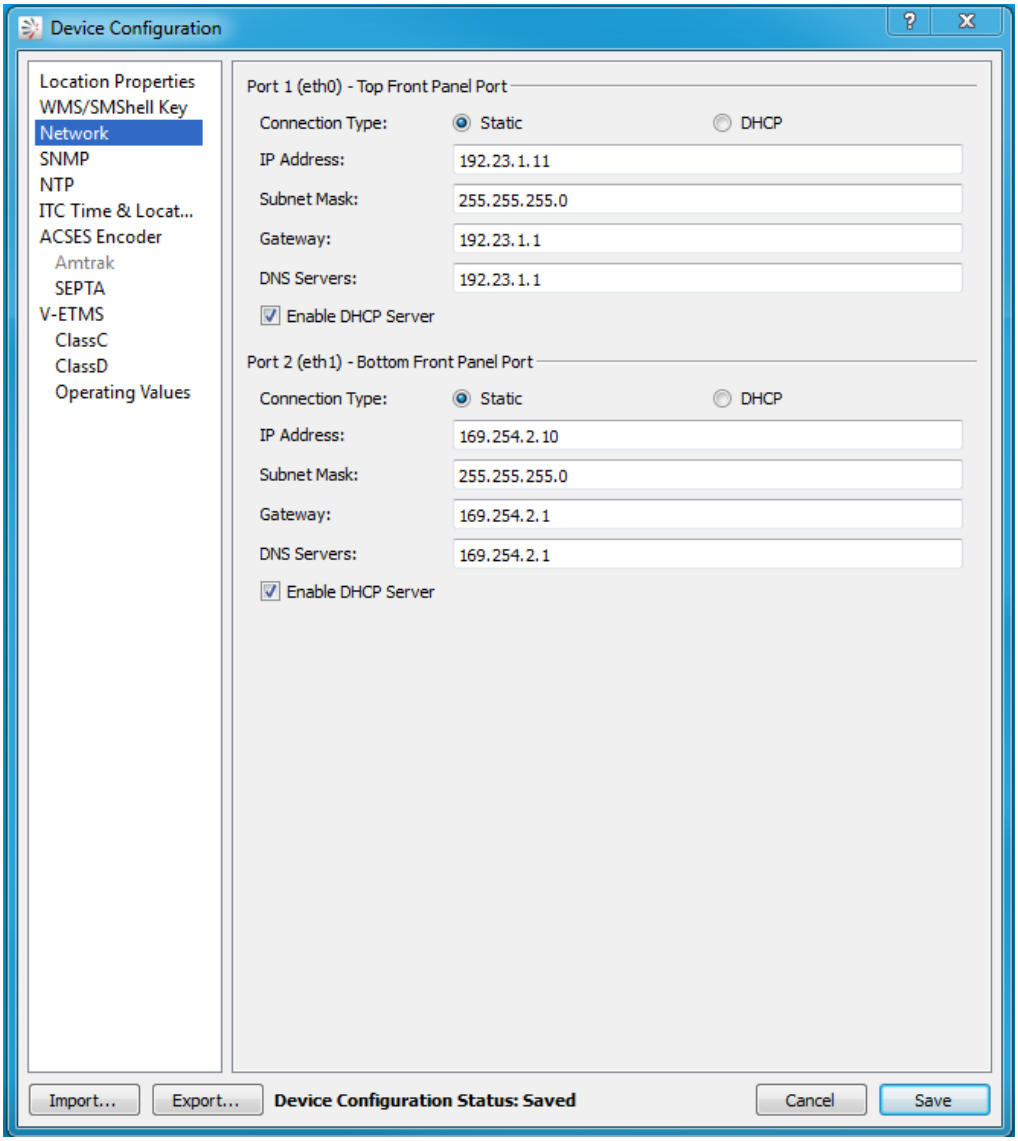


Figure 7-8. Network Settings

Table 7-2. Network Parameters

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Connection Type	This value specifies whether the device uses a user-specified static IP address, or if it will acquire an IP address from an external DHCP Server	**Radio Button** • Static IP • Automatic Configuration (DHCP) **Default Value** *Static IP*	N/A	N/A
IP Address	IP Address of the device must be entered when Static IP is selected for the Connection Type	**Masked Text Entry** (Valid IPv4 Address) **Default Value** *169.254.1.10* *(Ethernet Port 1)* *169.254.2.10* *(Ethernet Port 2)*	N/A	N/A
Subnet Mask	Device Network Subnet Mask	**Masked Text Entry** (Valid IPv4 Address) **Default Value** *255.255.255.0* *(Ethernet Port 1)* *255.255.255.0* *(Ethernet Port 2)*	N/A	N/A
Gateway	IP Gateway address for the connected network	**Masked Text Entry** (Valid IPv4 Address) **Default Value** *169.254.1.1* *(Ethernet Port 1)* *169.254.2.1* *(Ethernet Port 2)*	N/A	N/A
DNS Servers	Domain Name Server Address	**Free Text** (Valid IPv4 Address or DNS name) **Default Value** *0.0.0.0* *(Ethernet Port 1)* *0.0.0.0* *(Ethernet Port 2)*	N/A	N/A

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Enable DHCP Server	Allows the user to obtain the IP address from the WIU unit.	**Check-box** • Unchecked (DHCP server disabled) • Checked (DHCP server enabled) **Default Value** *DHCP server enabled (checked)*	N/A	N/A

7.5.3. SNMP

The SNMP section (Figure 7–9) in the Device Configuration Setup allows the user to specify the settings of the SNMP protocol. See Table 7-3 for a description of the SNMP configuration parameter settings.

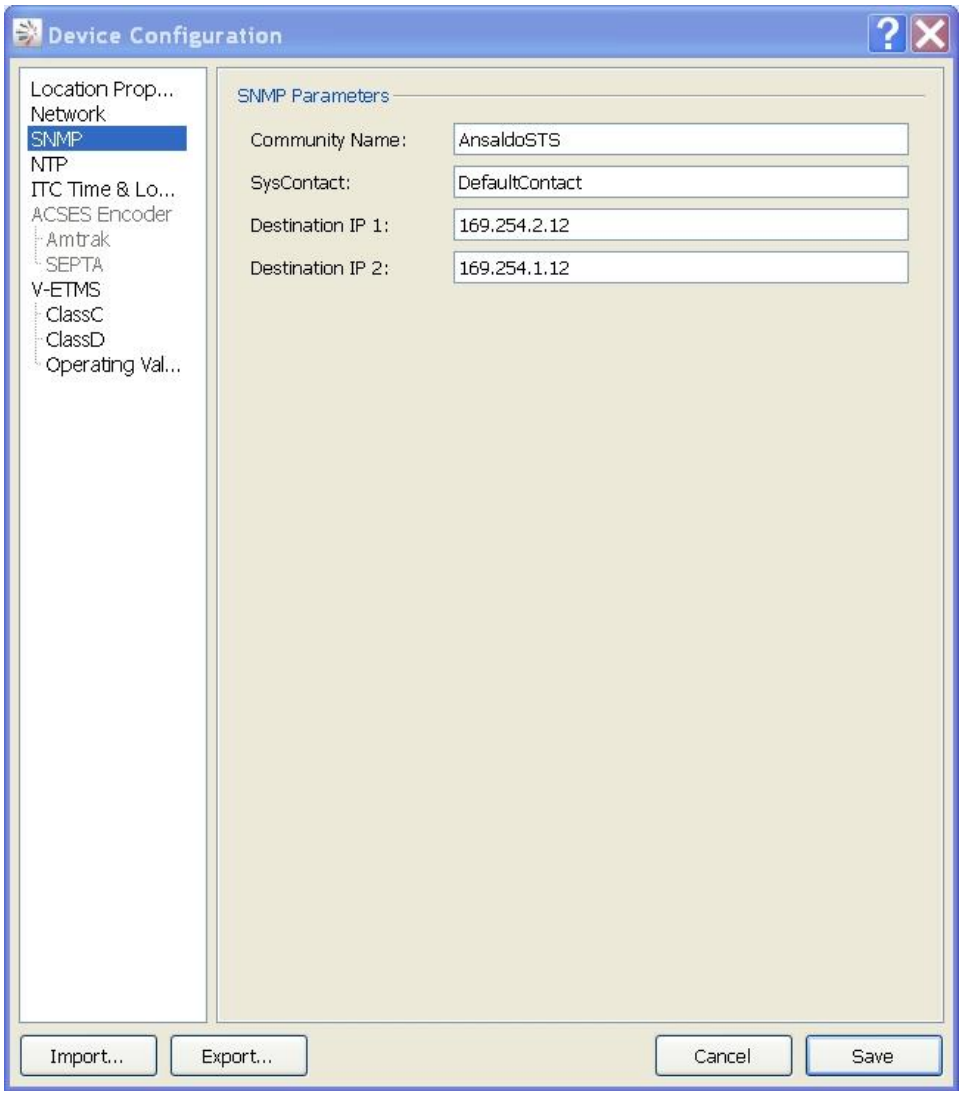


Figure 7–9. SNMP Settings

Table 7-3. SNMP Settings

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Community Name	Specifies the name of the community where traps are sent. This is any character string with no spaces in it.	**Free-text** (up to 50 characters) **Default Value** *"AnsaldoSTS"*	N/A	N/A
SysContact	The textual identification of the contact person for this managed node, together with information on how to contact this person.	**Free-text** (up to 50 characters) **Default Value** *"DefaultContact"*	N/A	N/A
Destination IP1 IP Address 1	This is the address used for Ethernet Port 1 for sending traps and informs.	**Free Text** (Valid IPv4 Address or DNS name) **Default Value** *169.254.2.12*	N/A	N/A
Destination IP2 IP Address 2	This is the address used for Ethernet Port 2 for sending traps and informs.	**Free Text** (Valid IPv4 Address or DNS name) **Default Value** *169.254.1.12*	N/A	N/A

7.5.4. NTP

The NTP configuration section (Figure 7–10) in the Device Configuration Setup allows the user to specify the settings of the NTP server being used for time update messages – if the device is configured to receive time update messages from NTP, rather than from the WCM. See Table 7-4 for a description of the NTP configuration parameter settings.

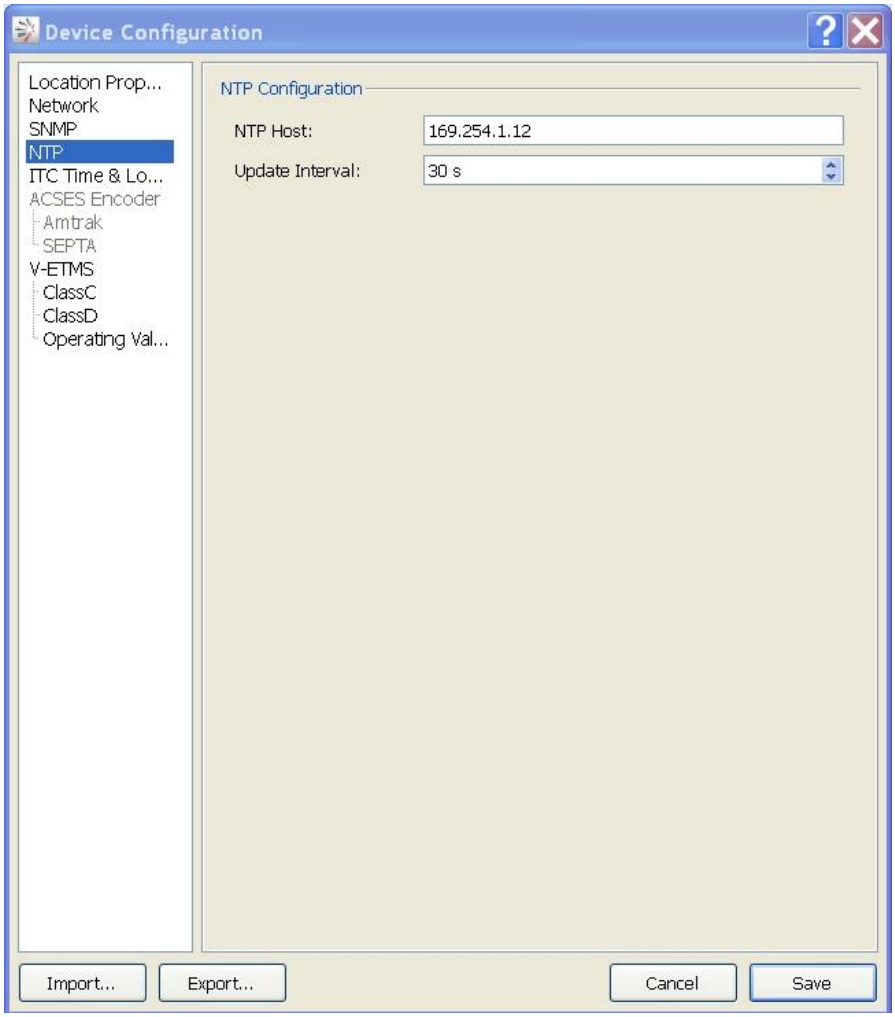


Figure 7–10. NTP Settings

Table 7-4. NTP Settings

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
NTP Host	IP Address of the NTP Server	**Free Text** (Valid IPv4 Address or DNS name) **Default Value** *time.windows.com*	N/A	N/A
Update Interval	Frequency at which the WIU device will request time updates from the NTP Server	**Numerical Entry** **Default Value** *30*	1 – 300	seconds

7.5.5. ITC Time and Location Configuration

The ITC Time and Location Configuration section (Figure 7–10) in the Device Configuration Setup allows the user to specify the settings. See Table 7-5 for a description of the ITC configuration parameter settings.

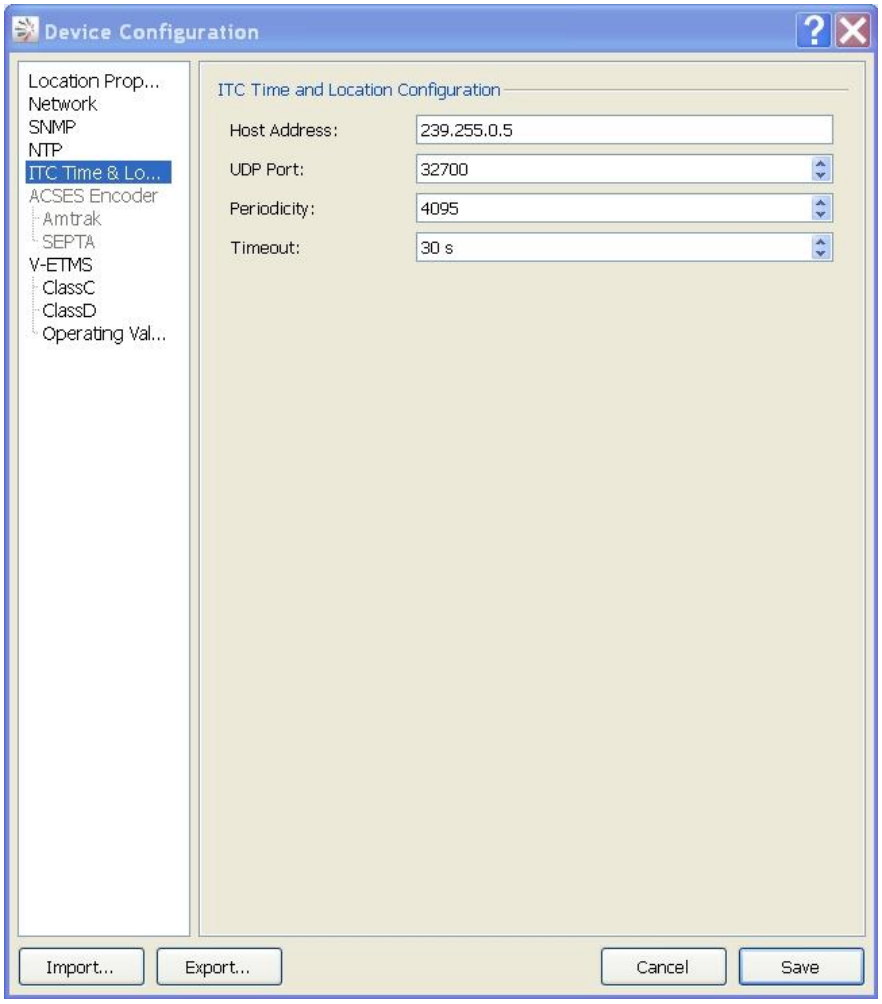


Figure 7–11. ITC Time and Location Configuration Settings

Table 7-5. ITC Time and Location Settings

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Host Address		**Free-text** (up to 50 characters) **Default Value** *"239.255.0.5"*	N/A	N/A
UDP Port		**Numerical Entry** (up to 50 characters) **Default Value** *"32700"*	N/A	N/A
Periodicity		**Numerical Entry** (Valid IPv4 Address or DNS name) **Default Value** *4095*	N/A	N/A
Timeout		**Numerical Entry** (Valid IPv4 Address or DNS name) **Default Value** *30*	N/A	seconds

7.5.6. SEPTA ACSES Encoder

The SEPTA section (Figure 7–13) in the ACSES Encoder allows the user to specify the settings for the SEPTA ACSES Encoder. See Table 7-5 for a description of the SEPTA encoder parameter settings.

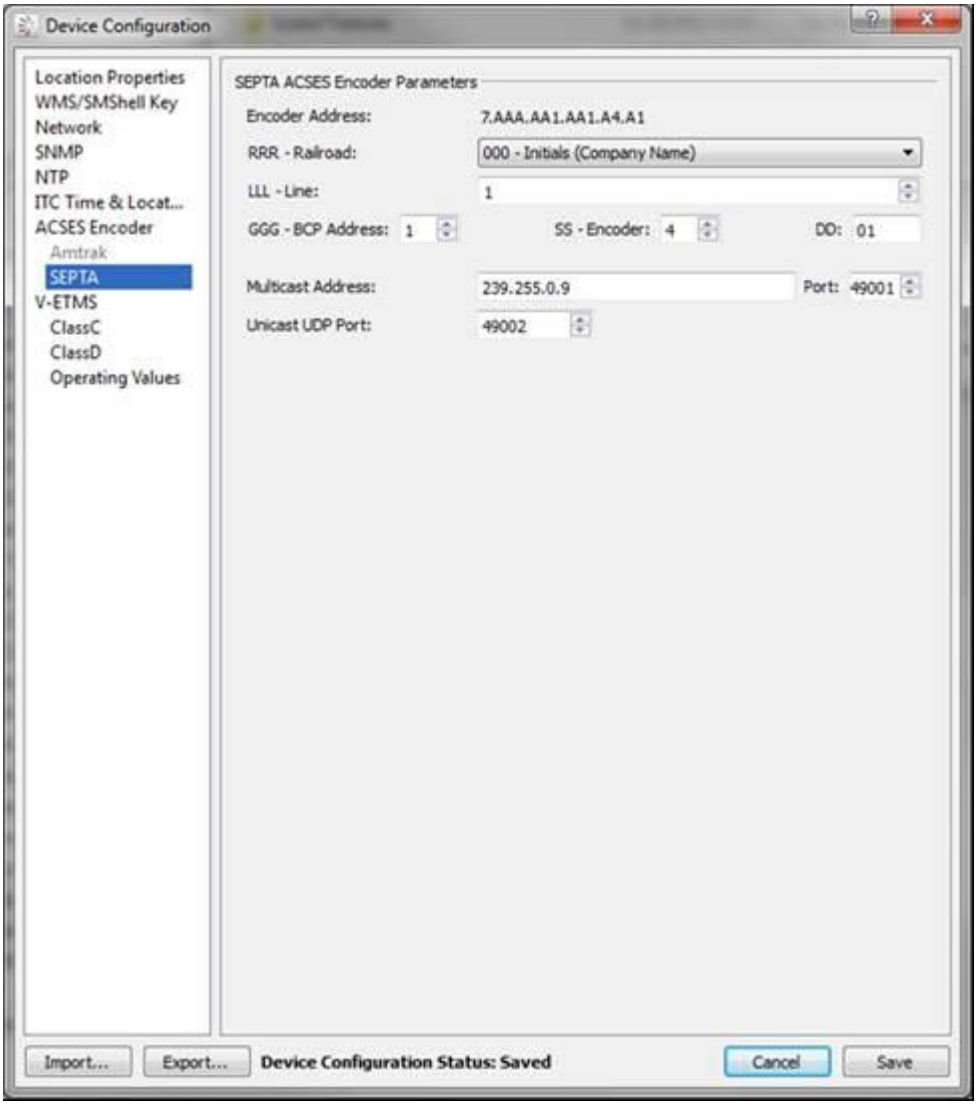


Figure 7–12. SEPTA ACSES Encoder Settings

Table 7-6. SEPTA ACSES Encoder Parameters

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Encoder Address	The IP address of the encoder	**Free-text** (up to 50 characters)	N/A	N/A
RRR - Railroad	The name of the railroad	**Drop Down Selection Entry**	N/A	N/A
LLL – Line:	The railroad line number	**Numerical Entry**	999	N/A
GGG – BCP Address	Control point number	**Free-text**	N/A	N/A
SS - Encoder	Type of equipment	**Free-text**	N/A	N/A
DD	Specific instance of equipment	**Free-text**	N/A	N/A
Multicast Address	The IP address of the multicast Port	**Free-text** (up to 50 characters)	N/A	N/A
Port	Port number for the multicast address	**Numerical Entry**	0 - 6535	N/A
Unicast UDP Port	Port number for the unicast port	**Numerical Entry**	0 - 6535	N/A

7.5.7. Class C

The Class C section (Figure 7–13) in the Device Configuration Setup gives the user the option to configure the WIU to accept an EMP-based time message transported over Class C. The user can specify the parameters to be used when these Class C messages are being used to obtain Time Update Messages from the WCM. See Table 7-7 for a description of the Class C parameter settings.

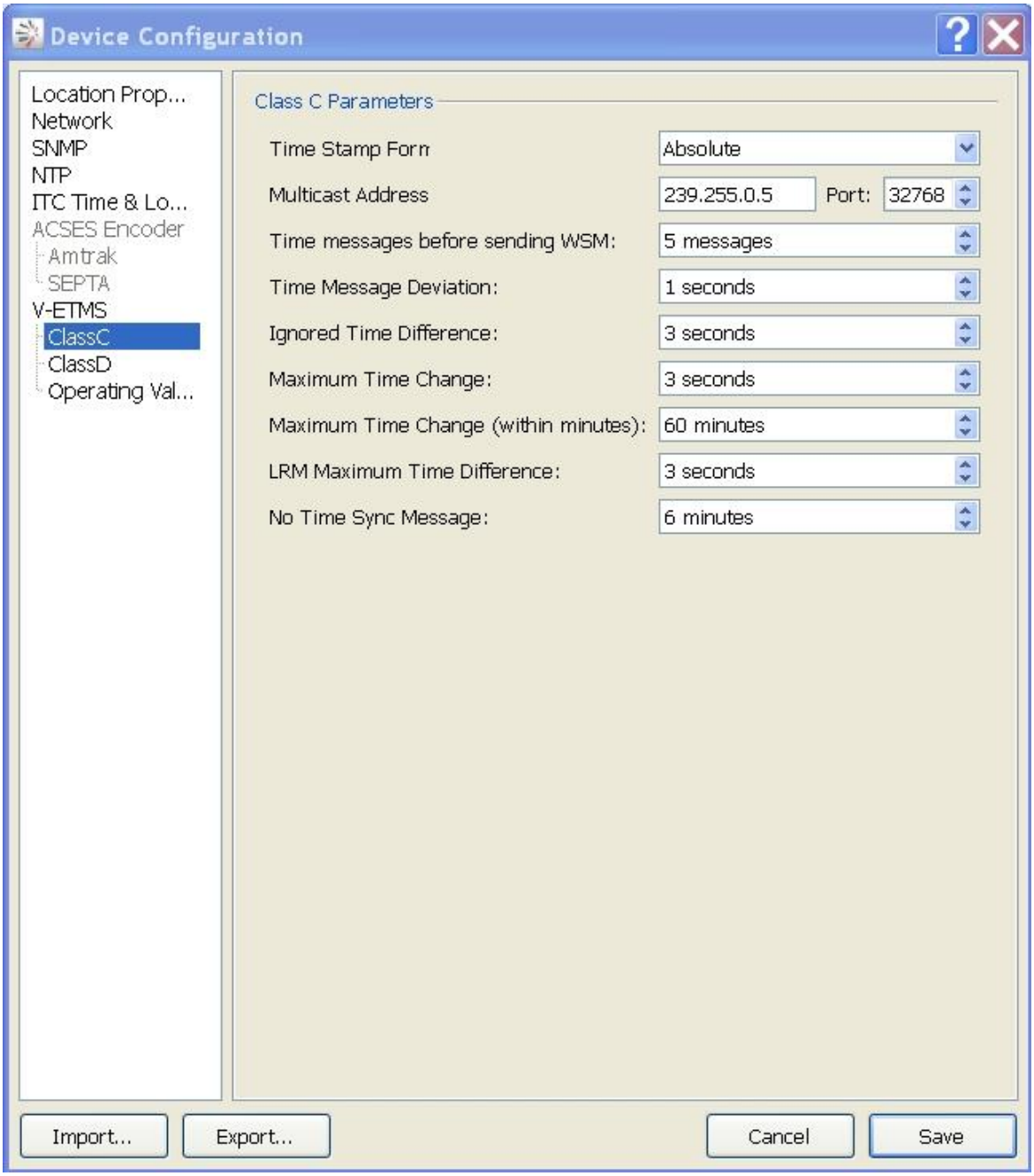


Figure 7–13. Class C Settings

Table 7-7 Class C Parameters

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Time Stamp Format	The format of the time message received from Class C protocol will always be received as Absolute Time	**Drop-down box** • Relative Time (elapsed time since last message creation) • Absolute Time (UTC time expressed as the absolute number of seconds since 00:00, 1/1/1970) **Default Value** *Absolute Time*	N/A	N/A
Multicast Address	The IP multicast address used to receive time sync messages	**Masked Text Entry** (Valid IPv4 Address) **Default Value** *239.255.0.5*	N/A	N/A
Port	The port used to receive time sync messages	**Free-text** (4 - 5 numeric characters) **Default Value** *32768*	1024 - 65535	N/A
Time Messages Before Sending WSM	WIU shall not send WSM's until this configured number of valid GPS time messages are received (unless configured for NTP)	**Numerical Entry** **Default Value** *5*	1 – 10	N/A
Time Message Deviation	The allowable +/- time deviation from the current internal WIU time, used to determine validity of consecutively received GPS messages – corresponds to “Time Messages Before Sending WSM”	**Numerical Entry** **Default Value** *1*	0 - 3	Seconds
Ignored Time Difference	The configured +/- time difference window for received time messages – messages received with time updates outside of this allowable window will be ignored by the WIU	**Numerical Entry** **Default Value** *3*	1 – 10	Seconds

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Maximum Time Change	The maximum allowable internal WIU clock drift (+/-), caused by cumulative effects of time update messages	**Numerical Entry** **Default Value** *3*	1 – 10	Seconds
Maximum Time Change (Within Minutes)	The specified time period over which the allowable internal WIU clock drift is calculated	**Numerical Entry** **Default Value** *60*	1 - 120	Minutes
LRM Maximum Time Difference	The allowable time difference of received LRM messages compared to the internal WIU time	**Numerical Entry** **Default Value** *3*	0 – 20	Seconds
No Time Sync Message	The allowable period of time for the WIU to wait for a time sync message after booting up	**Numerical Entry** **Default Value** *6*	1 – 6	Minutes

7.5.8. Class D

The Class D section (Figure 7–14) in the Device Configuration Setup contains four section; each section specifies the arguments passed to a Class D object. Those four sections are the Protocol Attributes, Link Attributes, Beacon Attributes, and Quality of Service (QoS).

7.5.8.1. Protocol Attributes

The Protocol Attributes section (Figure 7–14) allows the user to view general Class D protocol options. These options are used in constructing the headers used in the framing of EMP-formatted messages which are transmitted over Class D from the WIU device. See Table 7-8 for a description of the Protocol Attributes parameter settings.

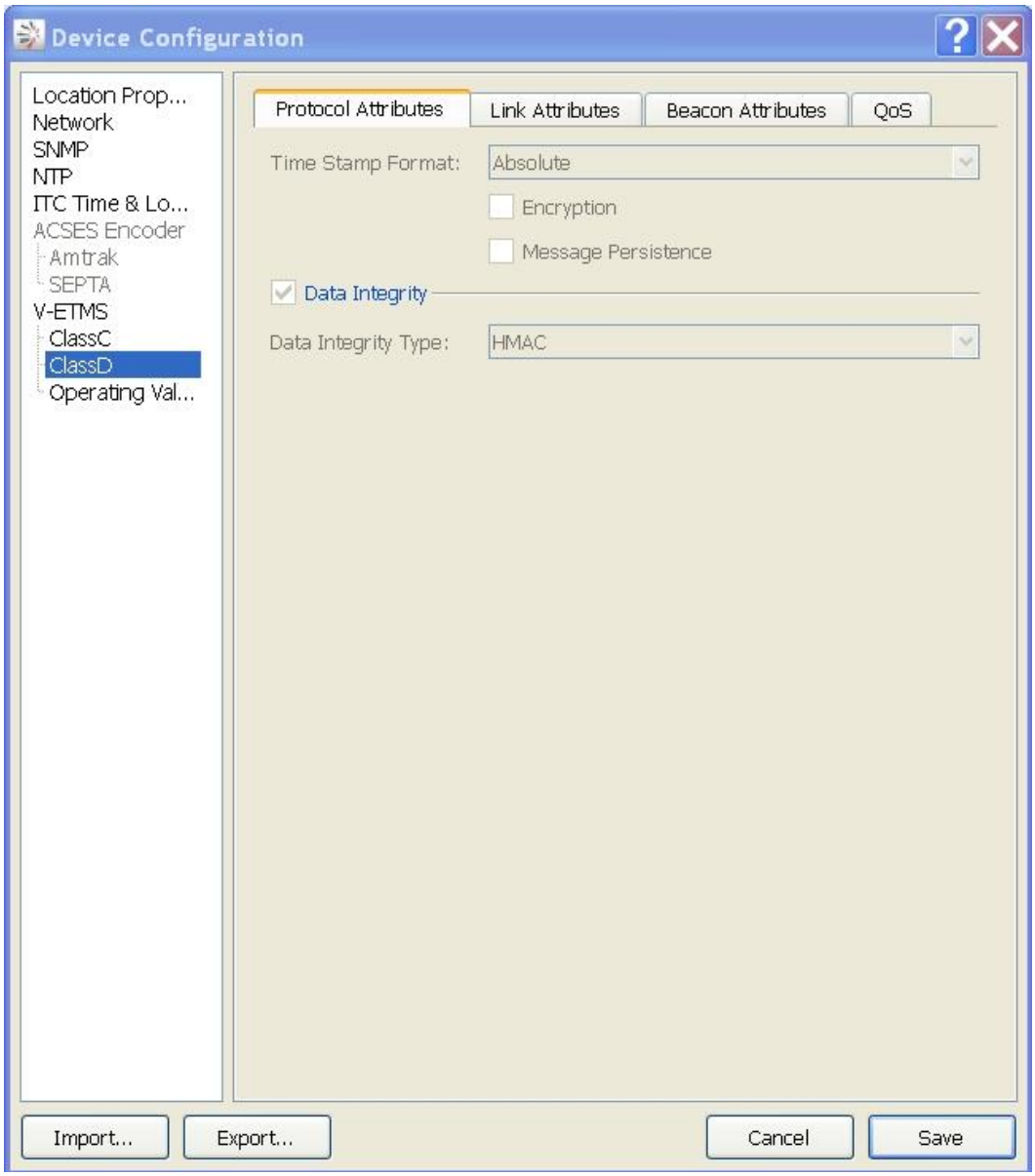


Figure 7–14. Class D Protocol Attribute Parameters

Table 7-8. Class D Protocol Attribute Parameters

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Time Stamp Format	The timestamp format to be used by the WIU device when transmitting WSMs	**Drop-down box** • Relative Time (elapsed time since last message creation) • Absolute Time (UTC time expressed as the absolute number of seconds since 00:00, 1/1/1970) **Default Value** *Absolute Time*	N/A	N/A
Encryption	The encryption flag indicates that the messages being sent by the WIU will be encrypted. This is different from the QoS service indicators requesting that an intermediate gateway encrypt the message	**Check-box** • Unchecked (Body is not encrypted) • Checked (Body is encrypted) **Default Value** *Not Encrypted (unchecked)*	N/A	N/A
Message Persistence	The message persistence flag is disabled	**Check-box** • Unchecked (Persistence is not enabled) • Checked (Persistence is enabled) **Default Value** *Not enabled (unchecked)*	N/A	N/A

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Data Integrity	The data integrity option indicates whether the WIU will use data integrity when constructing the WSMs	**Check-box** • Unchecked (Do not use Data Integrity) • Checked (Use Data Integrity) **Default Value** *Use Data Integrity (checked)*	N/A	N/A
Data Integrity Type	Specifies the data integrity type to use to ensure that the message header and payload delivered to the final destination are exactly the same as the EMP header and payload generated by the WIU	**Drop-down box** • CRC • HMAC **Default Value** *HMAC*	N/A	N/A

7.5.8.2. Link Attributes

The Link Attributes section (Figure 7–15) allows the user to specify TCP/IP communications-related Class D protocol options. These options are used in handling the TCP/IP communications link to the WCM. See Table 7-9 for a description of the Link Attributes parameter settings.

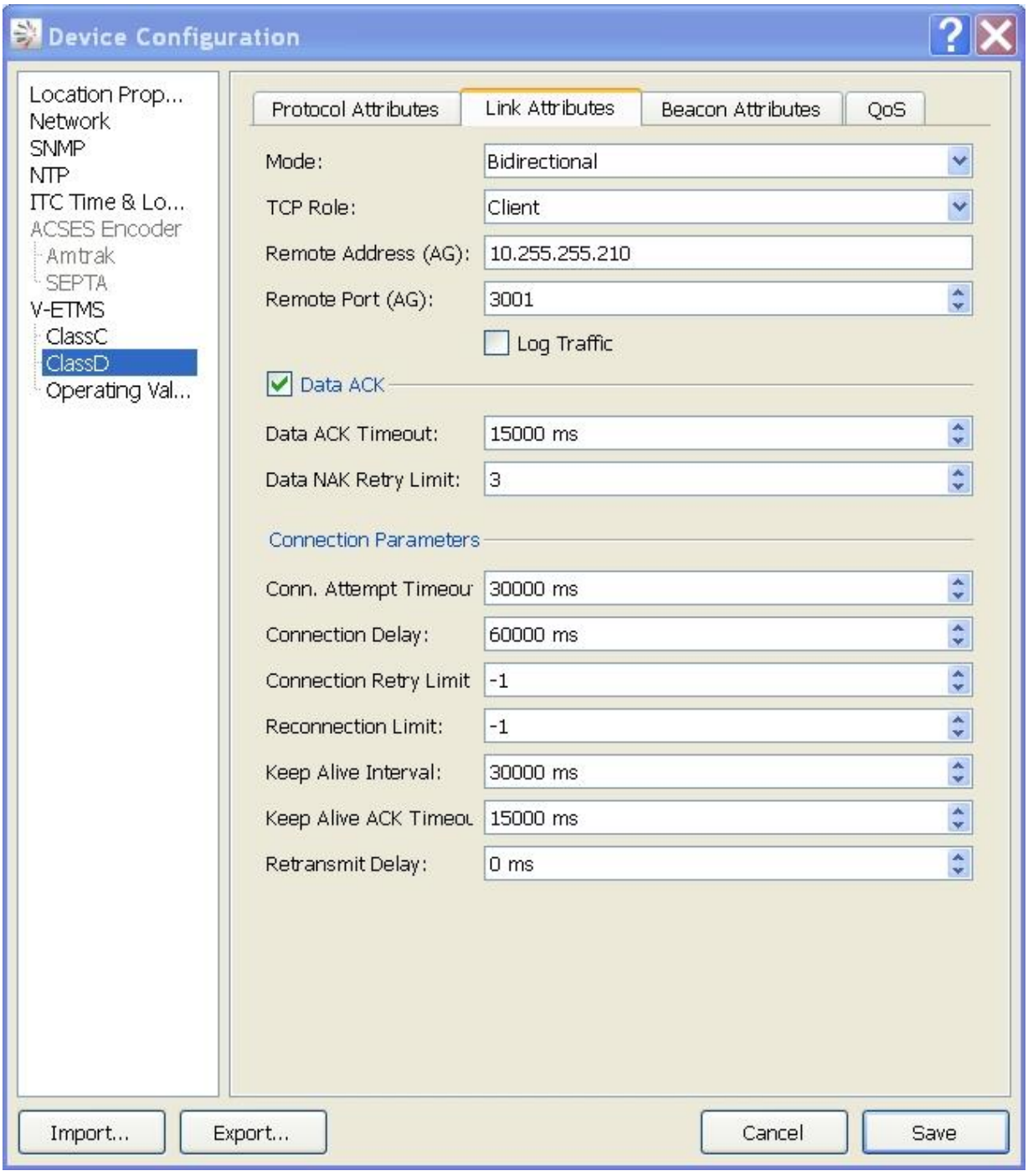


Figure 7–15. Class D Link Attribute Settings

Table 7-9. Class D Link Attribute Parameters

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Mode	This parameter indicates the direction in which data messages are permitted for the link	**Drop-down box** • Bidirectional **Default Value** *Bidirectional*	N/A	N/A
TCP Role	This parameter indicates whether the node shall act as a TCP client or TCP server	**Drop-down box** • Client **Default Value** *Client*	N/A	N/A
Remote Address (AG)	This parameter indicates the Application Gateway address to which the node shall be bound for the link	**Free Text** (Valid IPv4 Address or DNS name) **Default Value** *10.255.255.210*	N/A	N/A
Remote Port (AG)	This parameter indicates the TCP port to which the node shall be bound for the link	**Free-text** (4 or 5 numeric characters) **Default Value** *3001*	1024 - 65535	N/A
Log Traffic	This optional parameter indicates whether or not link traffic should be logged for debugging purposes. If this attribute is set to yes, all link traffic shall be logged by the node in a human readable format	**Check-box** • Unchecked (Do not log traffic) • Checked (Log traffic) **Default Value** *Do not log traffic (unchecked)*	N/A	N/A
Data ACK Enabled	This required attribute indicates whether or not acknowledgments (and negative acknowledgments) shall be sent or expected in response to data messages. The data ACK enabled attribute must be configured the same on both ends of a link	**Check-box** • Unchecked (Data ACK disabled) • Checked (Data ACK enabled) **Default Value** *Data ACK enabled (checked)*	N/A	N/A
Data ACK Timeout	The amount of time that a Class D node will wait for an acknowledgement of a data message, before timing-out	**Numerical Entry** **Default Value** *60,000*	1 – 60000	milli-seconds

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
NAK Retry Limit	The NAK retry limit specifies the maximum number of times that the node will retransmit a message because of negative acknowledgements before the node terminates the link	**Numerical Entry** **Default Value** *3*	1 – 10	Retries
Connection Attempt Timeout	This parameter indicates how much time shall be allowed to elapse while making a single attempt to establish a connection to the AG	**Numerical Entry** **Default Value** *30,000*	1 – 60000	milli-seconds
Connection Delay	This parameter indicates how much time the node shall wait before retrying a connection to the AG after the previous attempt failed	**Numerical Entry** **Default Value** *15,000*	1 – 60000	milli-seconds
Connection Retry Limit	This parameter indicates how many times an attempt shall be made to establish a connection to the AG in the event that connection attempts are failing ***NOTE:*** *A value of "-1" indicates that the WIU should retry forever*	**Numerical Entry** **Default Value** *-1 (Retry forever)*	-1 - 10000	Retries
Reconnection Limit	This parameter indicates the number of times that shall be allowed to reconnect to the AG before giving up ***NOTE:*** *A value of "-1" indicates that the WIU should retry forever*	**Numerical Entry** **Default Value** *-1 (Retry forever)*	-1 - 10000	Retries
Keep Alive Interval	This parameter indicates the rate at which keep alive messages shall be sent to the AG ***NOTE:*** *A value of "0" indicates that no keep alive messages will be used – must be configured the same on both ends of the link*	**Numerical Entry** **Default Value** *60,000*	1 – 60000	milli-seconds
Keep Alive ACK Timeout	This parameter indicates how long the node shall wait for an acknowledgment to a keep alive message before terminating the link	**Numerical Entry** **Default Value** *30,000*	1 – 60000	milli-seconds
Retransmit Delay	This parameter indicates the amount of time to wait before retransmitting a message after receiving a NAK from the receiver	**Numerical Entry** **Default Value** *0 (no delay)*	0 – 10000	milli-seconds

7.5.8.3. Beacon Attributes

The Beacon Attributes section (Figure 7–16) allows the user to specify the settings related to the Beacon messages broadcasted by the WIU. See Table 7-10 for a description of the Beacon Attributes parameters settings.

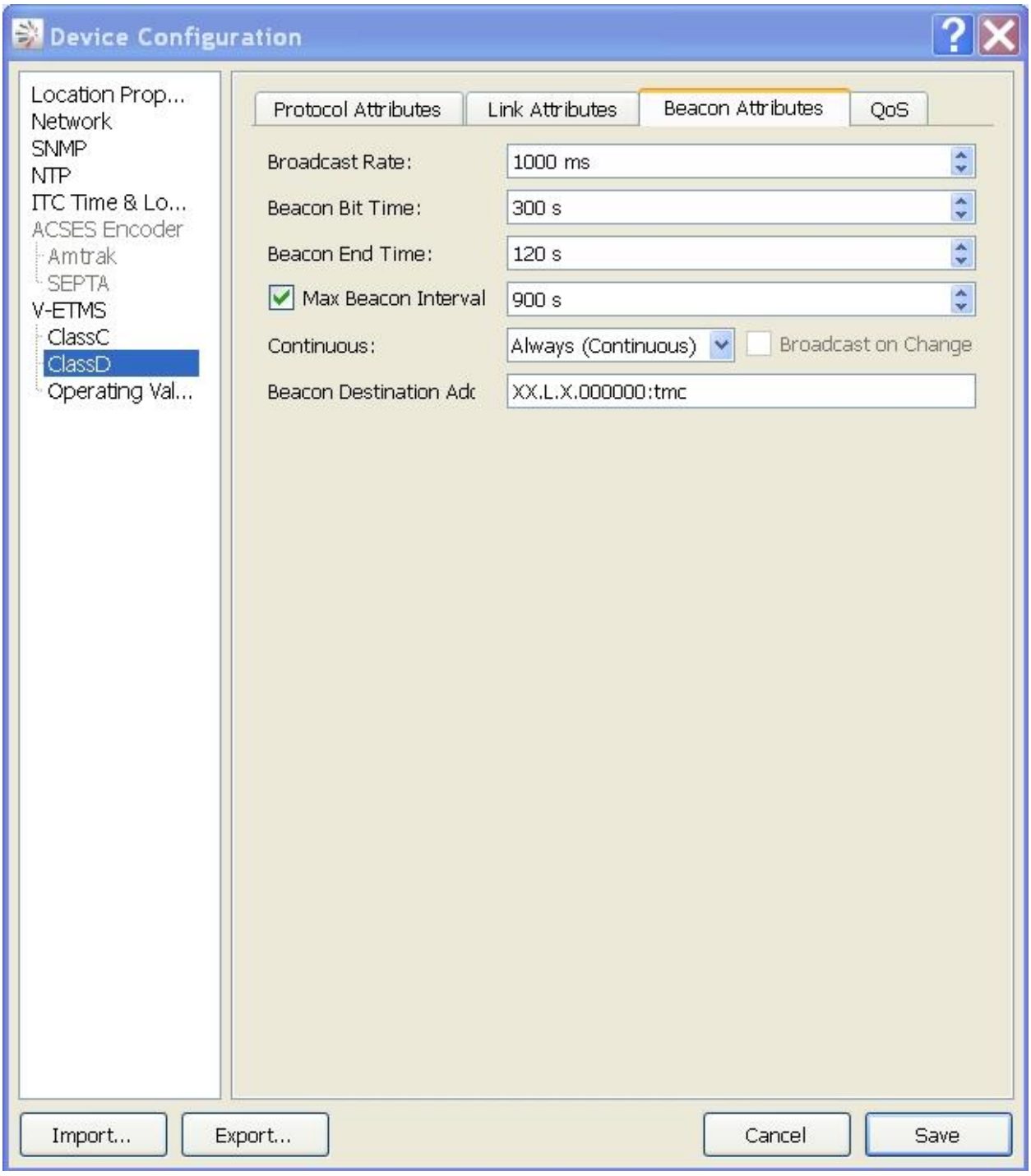


Figure 7–16. Class D Beacon Attribute Settings

Table 7-10. Class D Beacon Attribute Parameters

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Broadcast Rate	This parameter indicates the rate at which the WIU will broadcasts wayside status messages (beacons)	**Numerical Entry** **Default Value** *1,000*	0 – 60000	milli-seconds
Beacon Bit Time	This parameter indicates the length of time that the WIU will send beacon messages with the BeaconTTL flag set HIGH	**Numerical Entry** **Default Value** *300*	60 – 1800	seconds
Beacon End Time	This parameter indicates the length of time that the WIU will continue to send beacon messages (after the expiration of the BeaconBitTime) with the BeaconTTL flag set LOW. If a new request is not received from the requestor, the WIU will cease broadcasts at the end of this timeout period	**Numerical Entry** **Default Value** *120*	60 – 1800	seconds
Max Beacon Interval	When the WIU is configured to *not* beacon continuously, this parameter specifies the length of time for the WIU to wait before sending a "heartbeat" message to the beacon destination address **NOTE:** This parameter is irrelevant if Beacon Continuous is set to "Always (Continuous)"	**Numerical Entry** **Default Value** *900 (if enabled)*	60 – 86400	seconds
Continuous	The parameter indicates whether the WIU will continuously (always) send beacon messages to the beacon destination address. If configured to only send when requested, the WIU communications will "sleep" until a request is received, or the Max Beacon Interval expires (if enabled)	**Drop-down box** • Always (Continuous) • Only When Requested (Times Out) **Default Value** *Always (Continuous)*	N/A	N/A

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Broadcast on Change	This parameter indicates whether a WIU will broadcast a device status change in a WIU Status message immediately after it occurs (e.g. event driven) when it is *not* set to Beacon Continuous **NOTE:** This parameter is not available if Beacon Continuous is set to "Always (Continuous)"	**Check-box** • Unchecked (Do not broadcast on change) • Checked (Broadcast on change) **Default Value** *Do not broadcast on change (unchecked)*	N/A	N/A
Beacon Destination Address	This parameter indicates the EMP-formatted destination address to which all beacon messages will be sent by the WIU (Refer to Appendix A of the EMP Message Format Specification for more details on the format of this field)	**Free-text** (null-terminated string with a limit of 64 bytes.) **Default Value** *"null"*	N/A	N/A

7.5.8.4. Quality of Service (QoS)

The Quality of Service (QoS) section (Figure 7–17) allows the user to specify parameters that relate to the EMP message's variable message header and flags, for each type of message sent by the WIU. These parameters help specify the priority levels and routing information to the wireless messaging infrastructure, to ensure proper message delivery. Each message type (Timed Beacon or GetWIUStatus Response), has its own configurable parameter settings. See Table 7-11 for a description of the Quality of Service parameters settings.

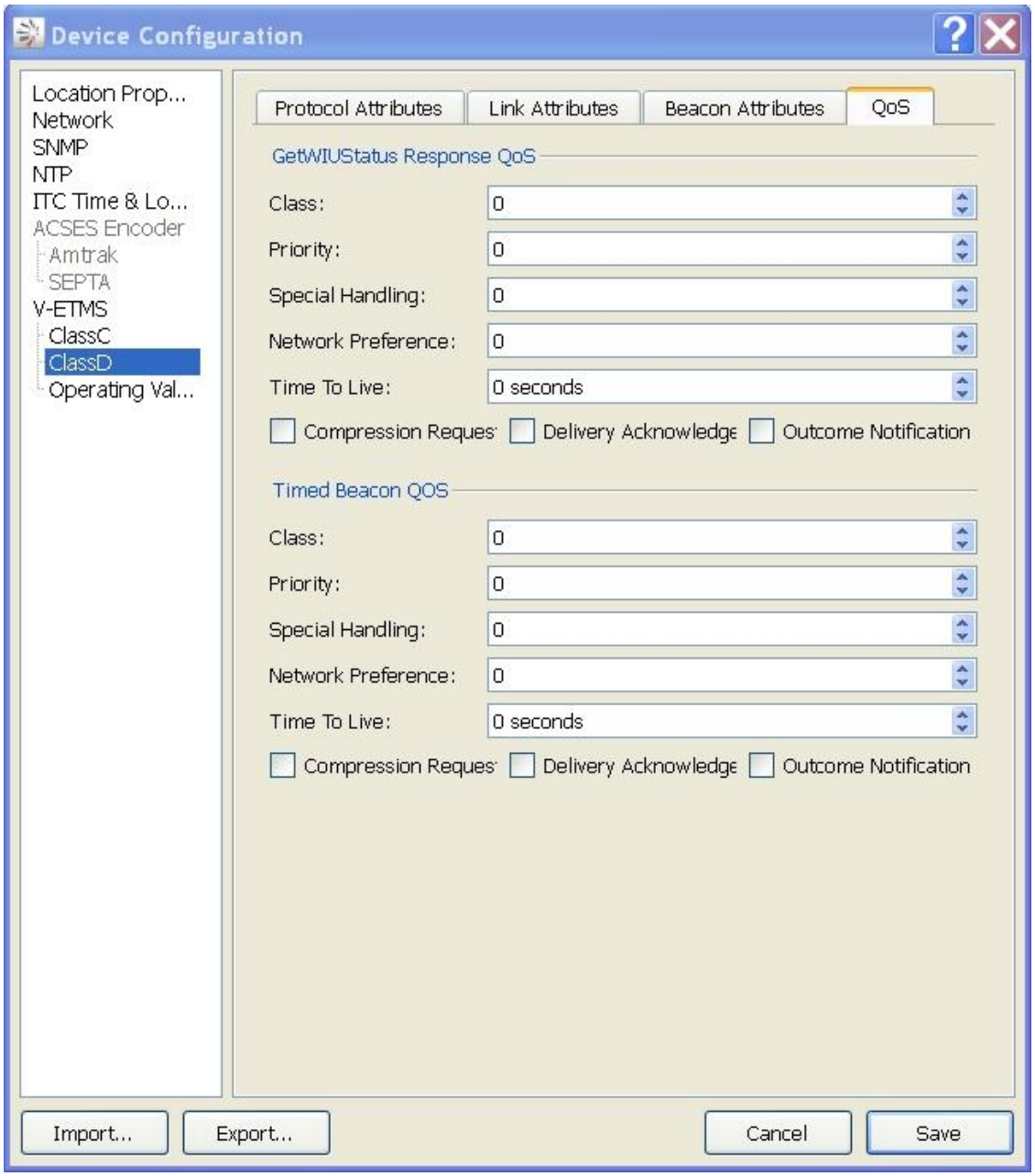


Figure 7–17. Class D QoS Settings

Table 7-11. Class D QoS Parameters

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Class	The parameter specifies which one of eight classes is assigned to the EMP message type, and determines message eligibility for various transport methods	**Numerical Entry** **Default Value** *1*	0 - 7	N/A
Priority	This parameter specifies which one of eight priority levels which are used to indicate to the underlying messaging system the priority of the message type relative to all other messages in the system	**Numerical Entry** **Default Value** *1*	0 – 15	N/A
Special Handling	This parameter specifies any special handling instructions for the message type, which are used by the messaging system to perform non-standard processing for that message	**Numerical Entry** **Default Value** *0 (no special handling)*	0 – 31	N/A
Network Preference	The parameter indicates a transport network preference for the message type which is used to override the default network selection behavior of the messaging system	**Numerical Entry** **Default Value** *0 (no preference)*	0 – 15	N/A
Time To Live	Determines the amount of time allowed by the sender to transmit the message	**Numerical Entry** **Default Value** *0 (no preference)*	0 – 9999	seconds
Compression Request	This parameter specifies whether compression will be requested for the message type - if supported by the Message Gateway / CMU, those functions shall compress the message prior to transmission	**Check-box** • Unchecked (Do not request compression) • Checked (Request Compression) **Default Value** *Do not request compression (unchecked)*	N/A	N/A

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Delivery Acknowledgement	This parameter specifies whether delivery notification will be requested for the message type – if supported by the Message Gateway / CMU, those functions shall implement delivery acknowledgement for the specified messages **NOTE:** Can only be requested if outcome notification is also requested	**Check-box** • Unchecked (Do not request delivery acknowledgement) • Checked (Request delivery acknowledgement) **Default Value** *Do not request* delivery acknowledgement *(unchecked)*	N/A	N/A
Outcome Notification	The parameter specifies whether outcome notification is requested for the message type – if supported by the Message Gateway / CMU, those functions shall asynchronously send the sender an EMP message indicating the outcome of the transmission attempt	**Check-box** • Unchecked (Do not request outcome notification) • Checked (Request outcome notification) **Default Value** *Do not request* outcome notification *(unchecked)*	N/A	N/A

7.5.9. Operating Values

This Operating Values page (Figure 7–18) in the Device Configuration Setup allows the user to specify the PTC operating values to be used for the WIU device, including the HMAC Encrypted Key and the RC2 Decryption Key. These values are entered in plain-text, but the RC2 Decryption Key is masked and then encrypted, so that it is only readable by the WIU device to which the value is uploaded.

The user can export the keys into separate files to be individually uploaded to the WIU unit through its browser-based configuration interface. The payload of the .rc2 file is encrypted and only visible to the WIU Application builder and WIU devices.

The user may also import the cryptographic keys from other WIU Application files and .HMAC and .rc2 files generated via exporting the keys from the WIU Application Builder.

See Table 7-12 for a description of the operating Values configuration parameters settings.

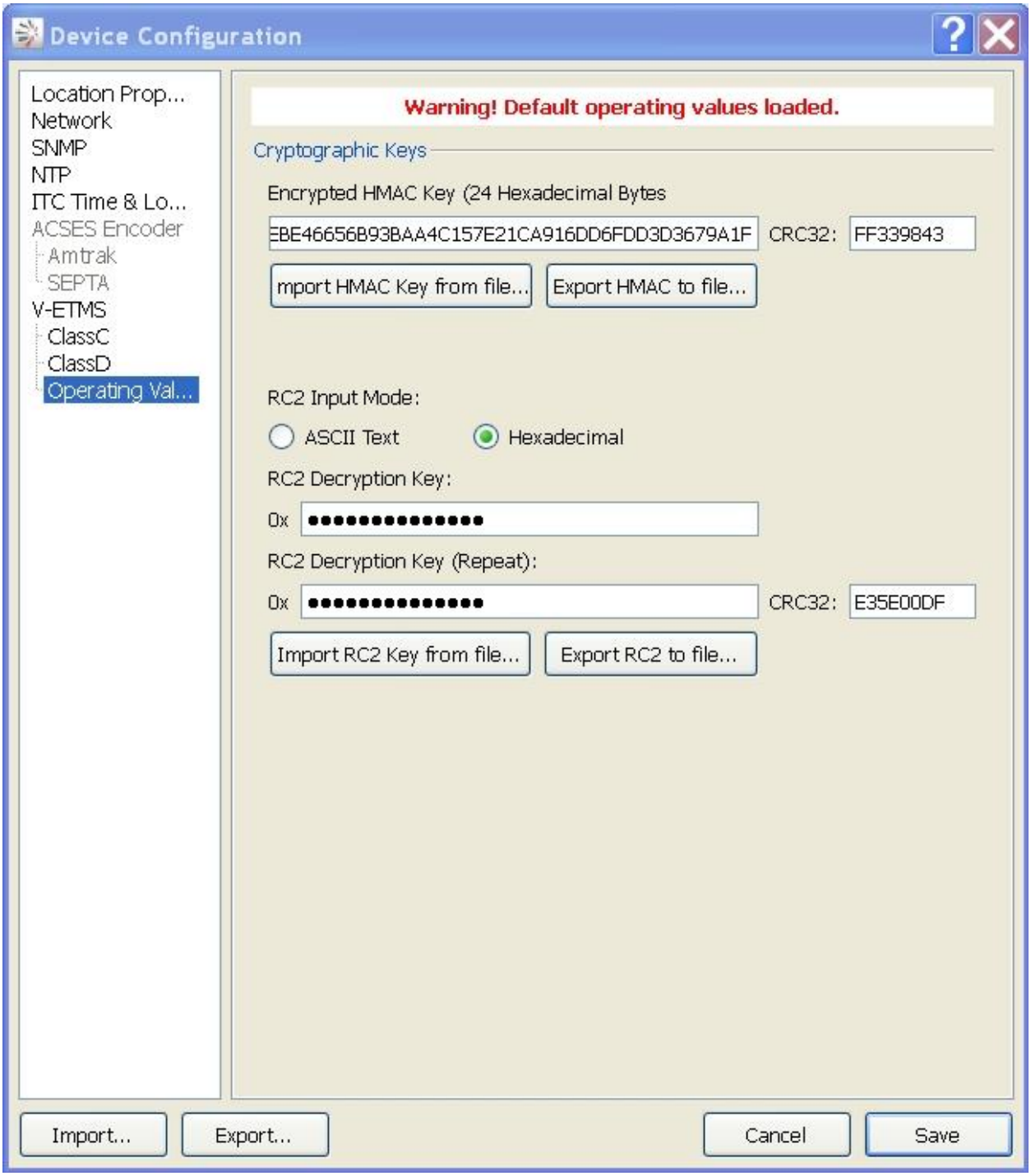


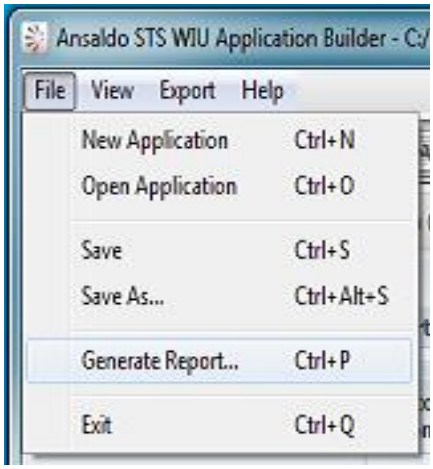
Figure 7–18. Cryptography (HMAC Operating Value) Settings

Table 7-12. Operating Values Settings

NAME	DESCRIPTION	ENTRY TYPE	RANGE	UNITS
Encrypted HMAC Key	Encrypted key necessary to support the HMAC calculations	**Free Text** (24 bytes) **Default Value** *N/A*	N/A	N/A
RC2 Input Mode	The RC2 input mode sets the mode of how the RC2 decryption key will be entered	**Radio Button** • ASCII Text • Hexadecimal **Default Value** *Hexadecimal*	N/A	N/A
RC2 Decryption Key	The RC2 embedded password used to decrypt keys used in the HMAC calculations. This value is hidden and encrypted so that this Key is not made available to field personnel	**Free Text** (20 bytes) **Default Value** *N/A*	N/A	N/A

7.5.10. Generate Report

To generate a listing of all the WIU parameters, elect Generate Report form the File menu.

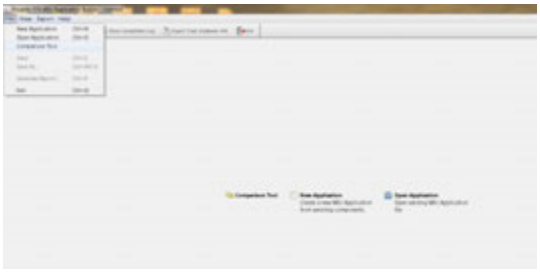


A pdf file will be generated that lists all of the WIU's parameters. A window will open where you will be required to name the file and select a location to save the file.

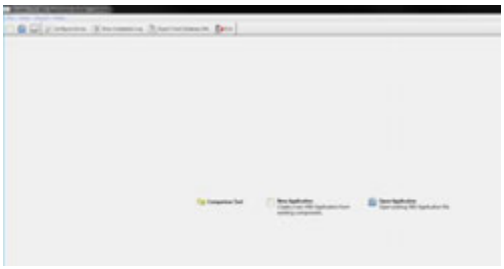
7.6. Comparing Application Files

The comparison tool allows you to compare two files. Proceed as follows to compare files:

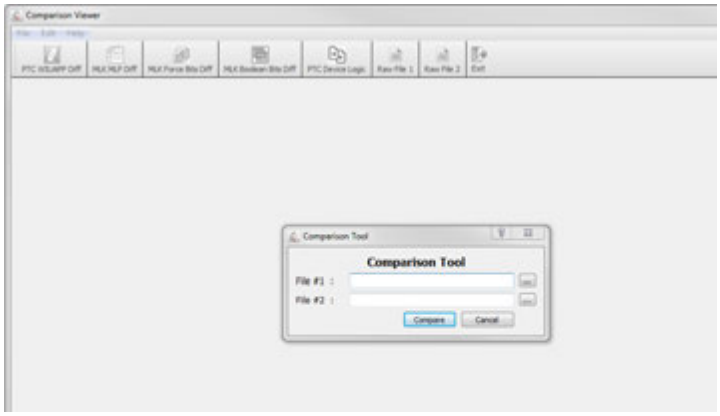
1. Select File/Comparison Tool drop down menu in the top left of the application builder.



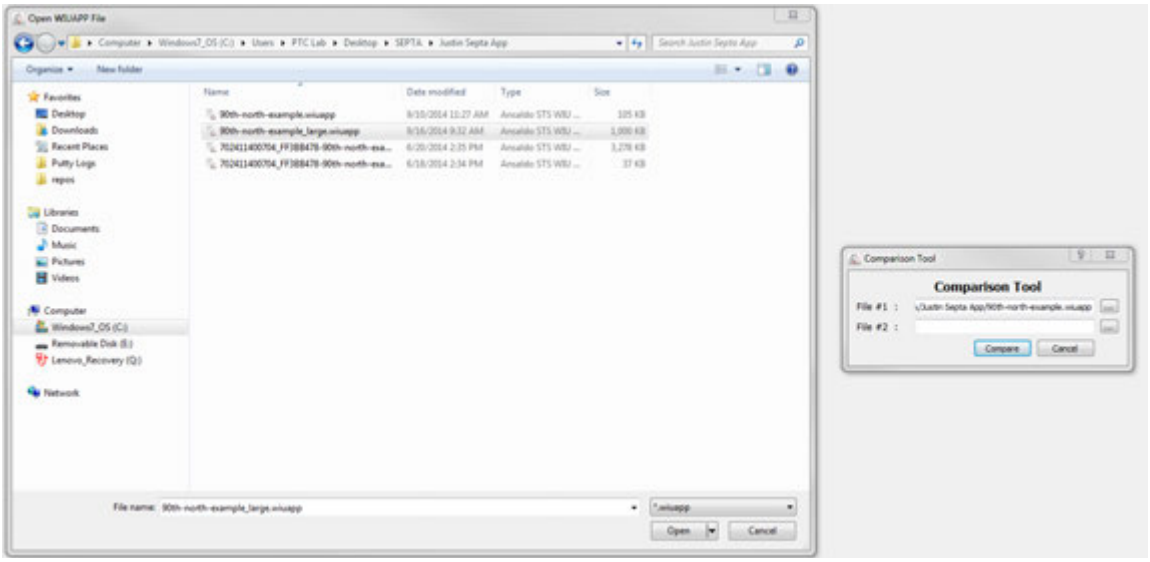
Or select the Comparison Tool button in the center of the application builder window.

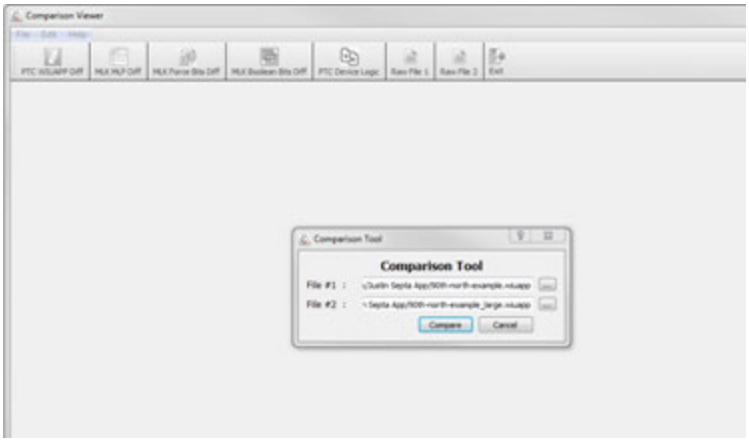


2. The window will appear for you to browse to the locations on your computer where the applications are stored.

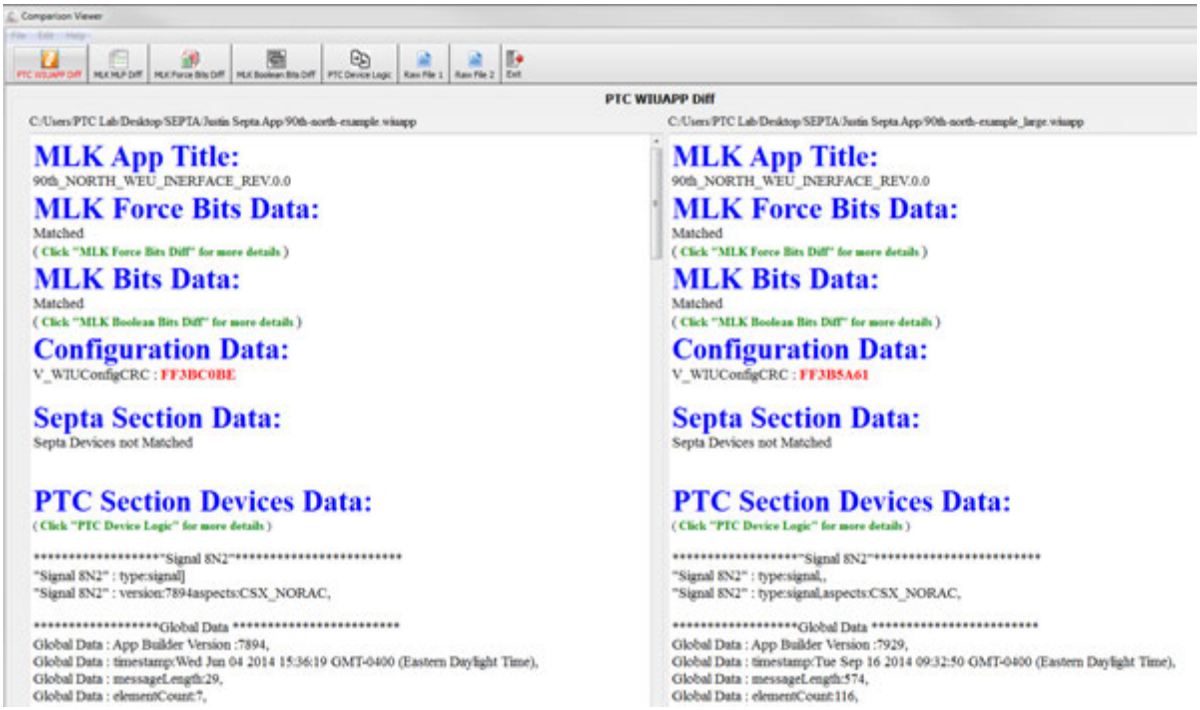


3. Browse and Select the files.





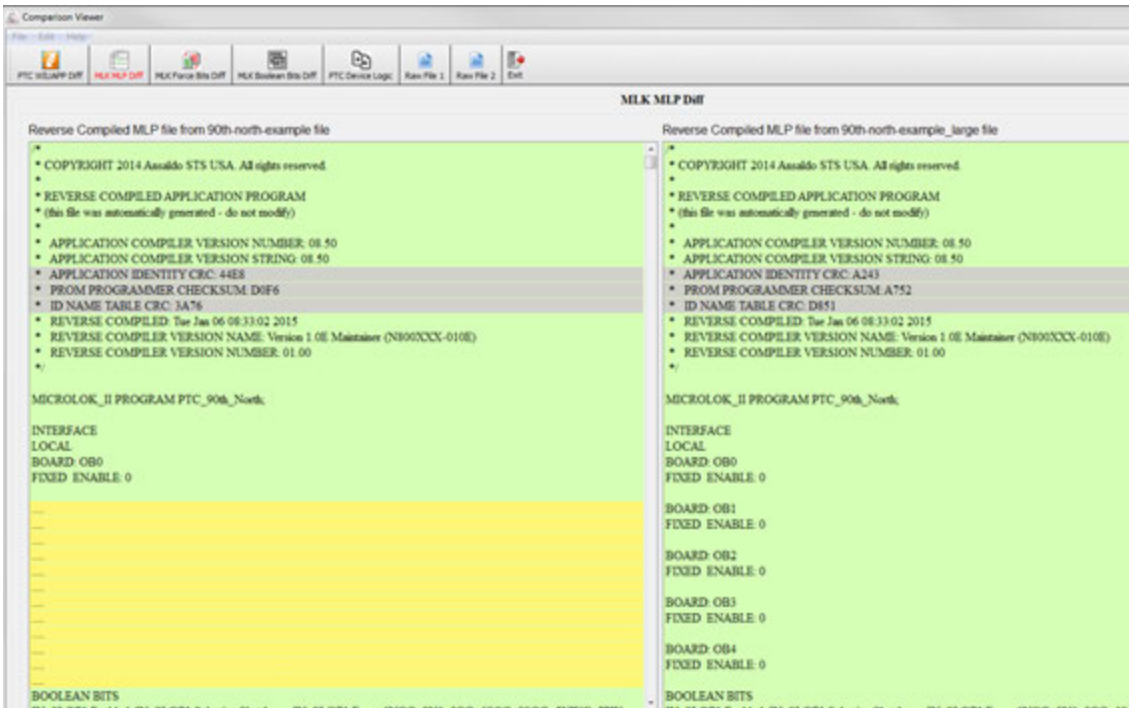
4. After both files to compare are opened, select Compare.
5. The comparison window will open. The parameters for the selected files will be displayed side by side. The file names of the files appear at the top of each list.



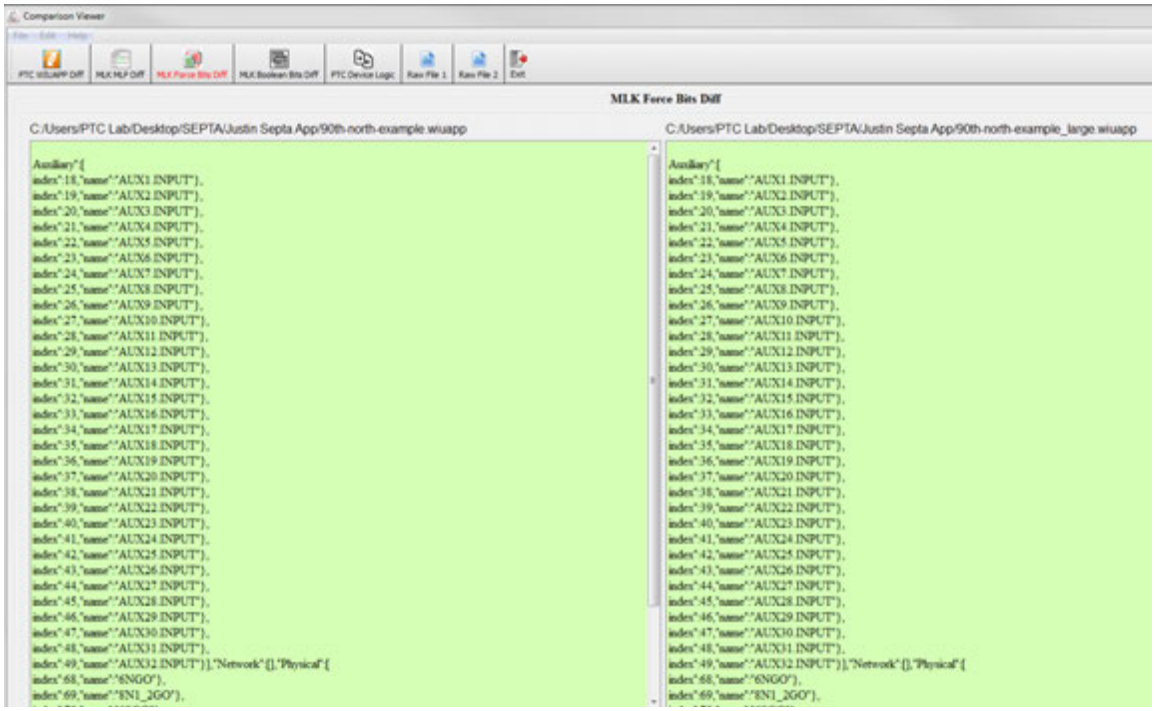
NOTE

The background colors in the comparison screens indicate a match or not matched parameter. A green background indicates that the parameters match. A gray or yellow background indicates that the parameters do not match.

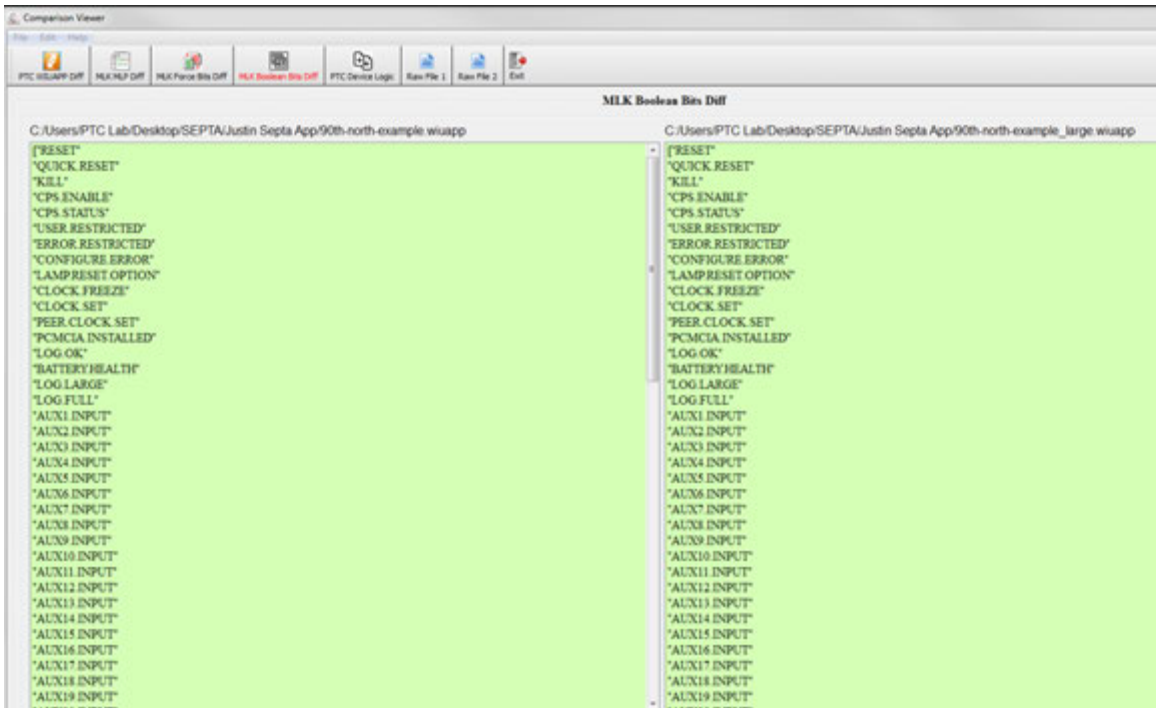
6. To compare the MicroLok II .mlp files, select the MLK MLP Diff icon from the main menu. The .mlp comparison screen will display.



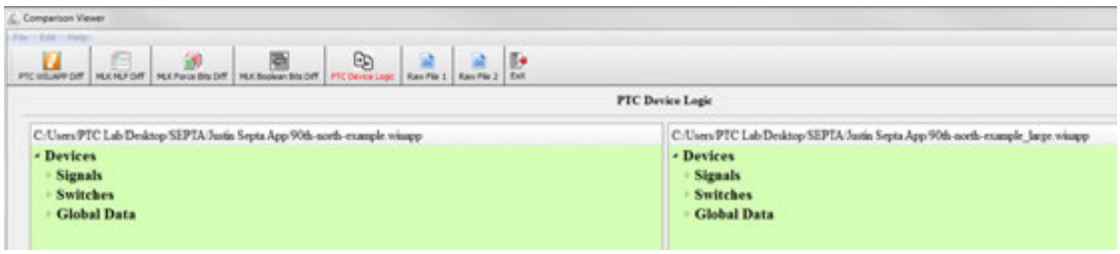
7. To compare the MicroLok II forced bits, select the MLK Force Bits Diff icon from the main menu. The MicroLok forced bits comparison screen will display.



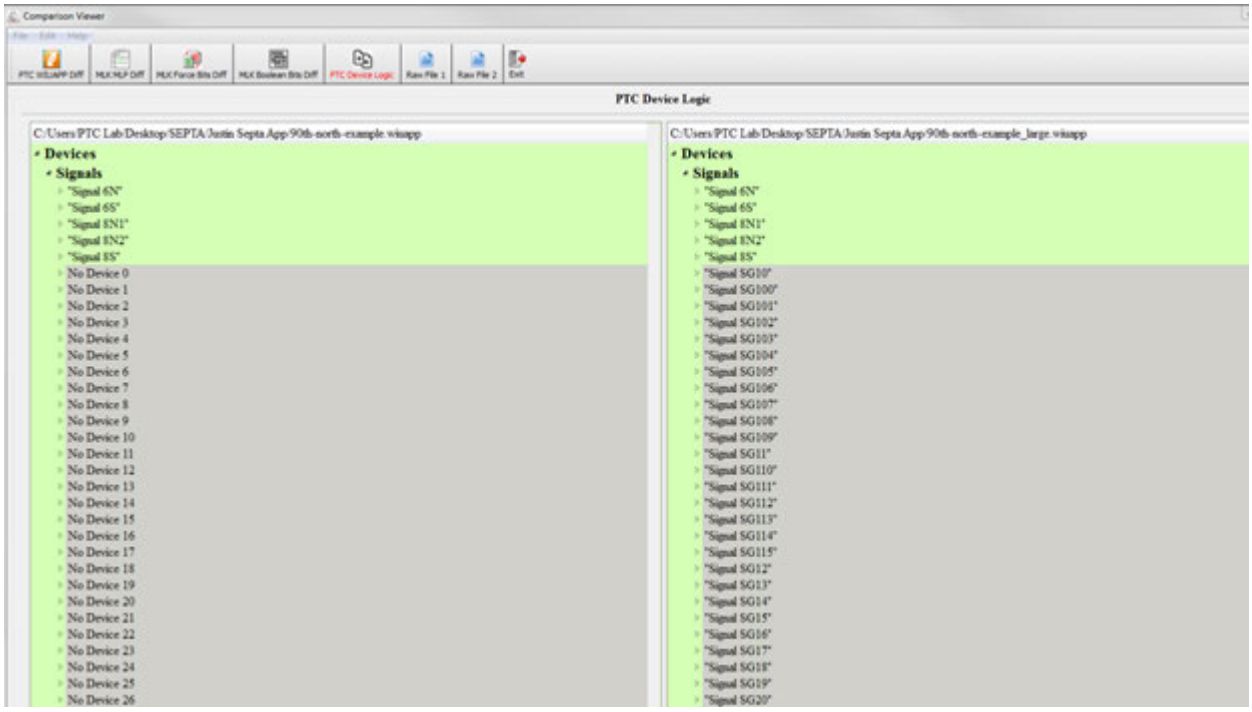
8. To compare the MicroLok II Boolean bits, select the MLK Boolean Bits Diff icon from the main menu. The MicroLok Boolean bits comparison screen will display.



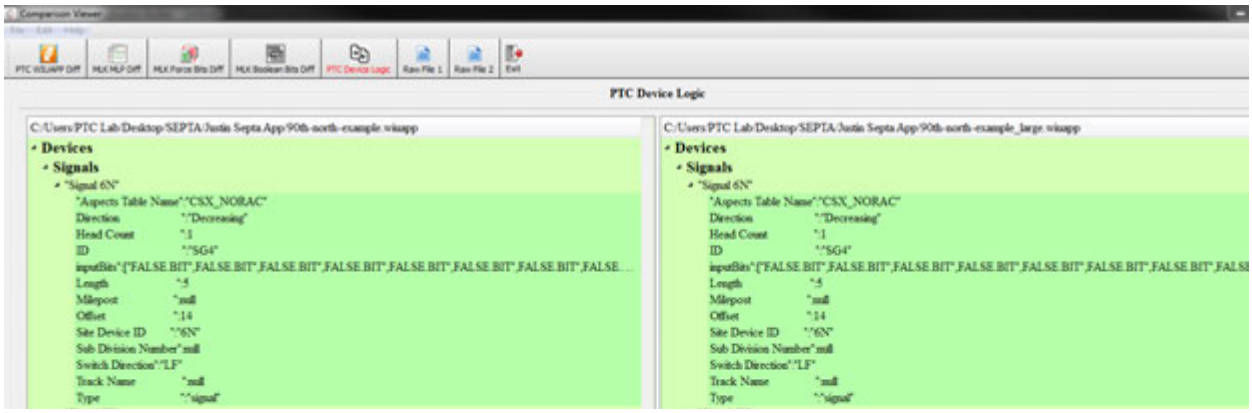
9. To compare the PTC device logic, select the PTC Device Logic icon from the main menu. The PTC device logic comparison screen will display.

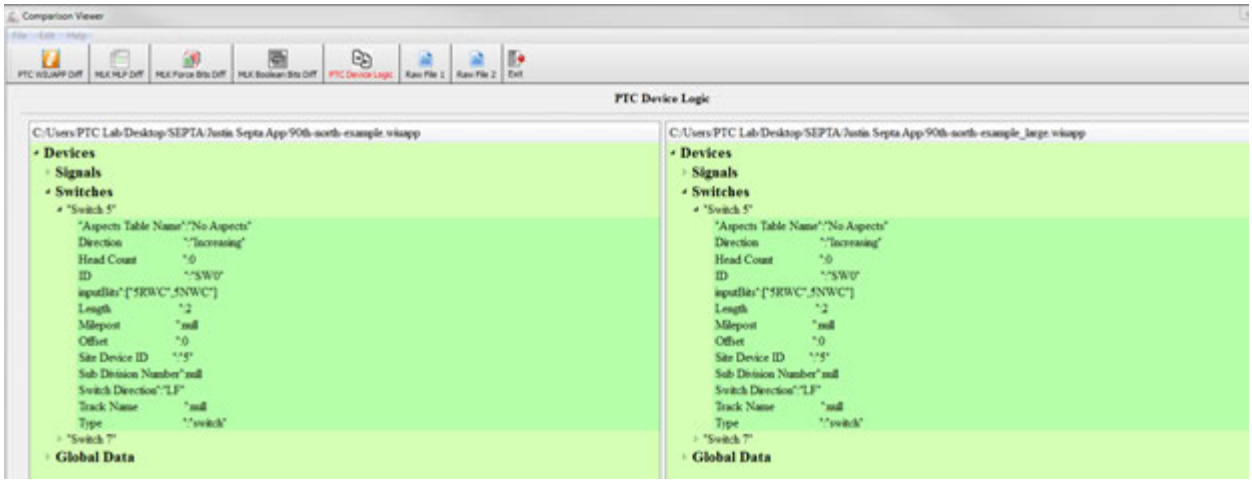


10. This screen lists the devices that are contained in the application program. To select a list of devices for a type of device, select the arrow next to each device category. A listing of the devices will display.

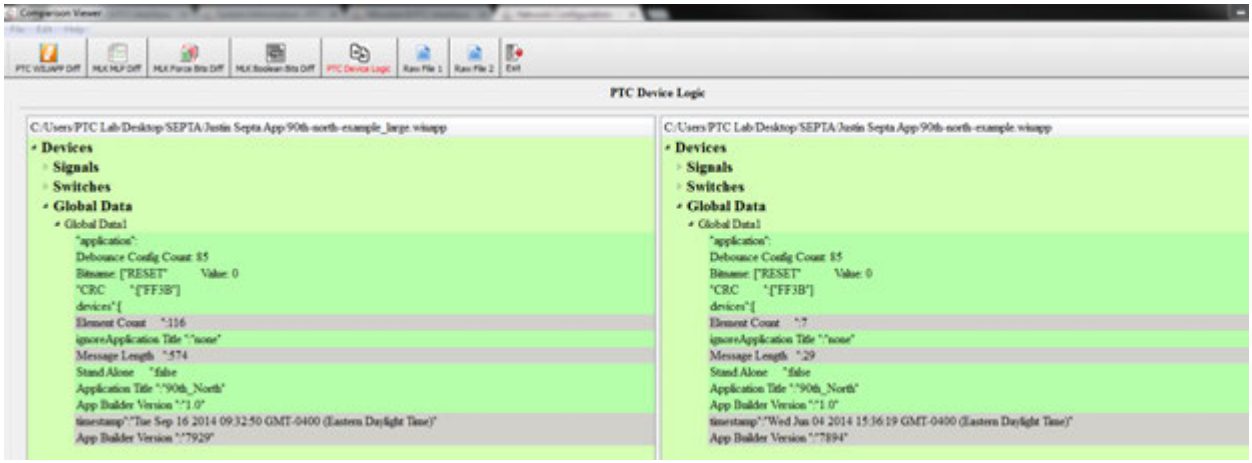


11. To compare a specific device in a category, select the arrow next to the specific device. The comparison list for the device will display.

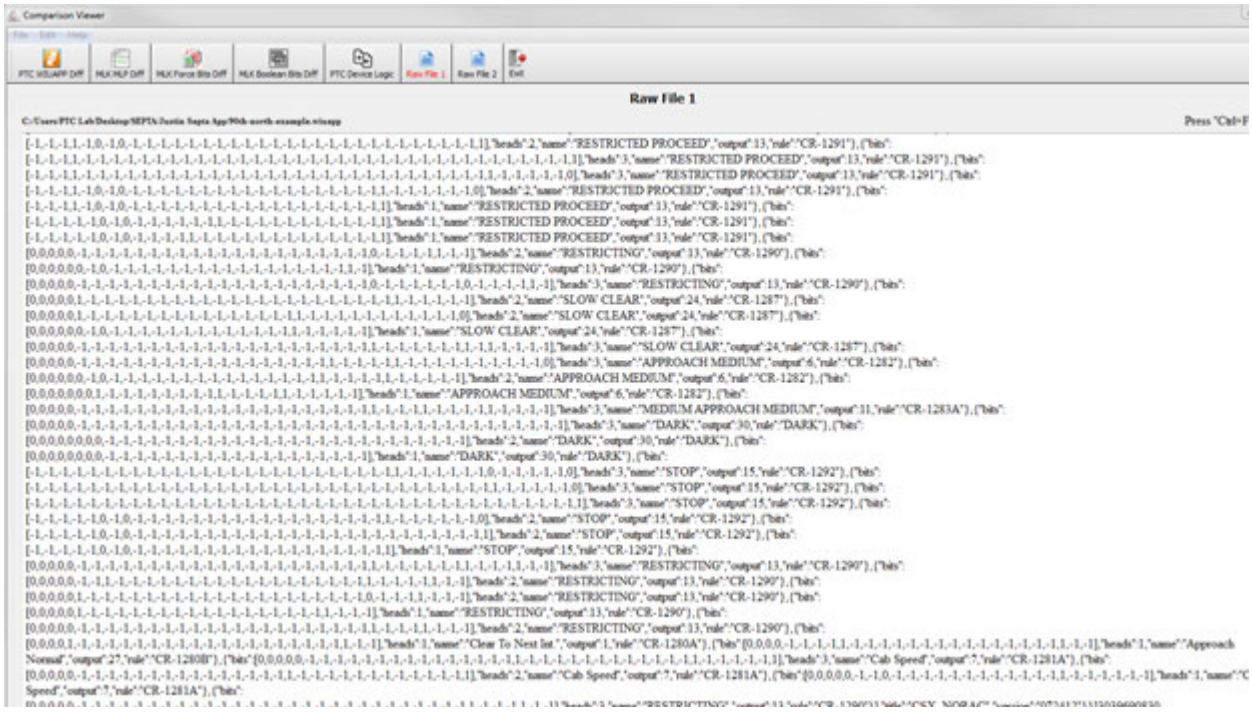




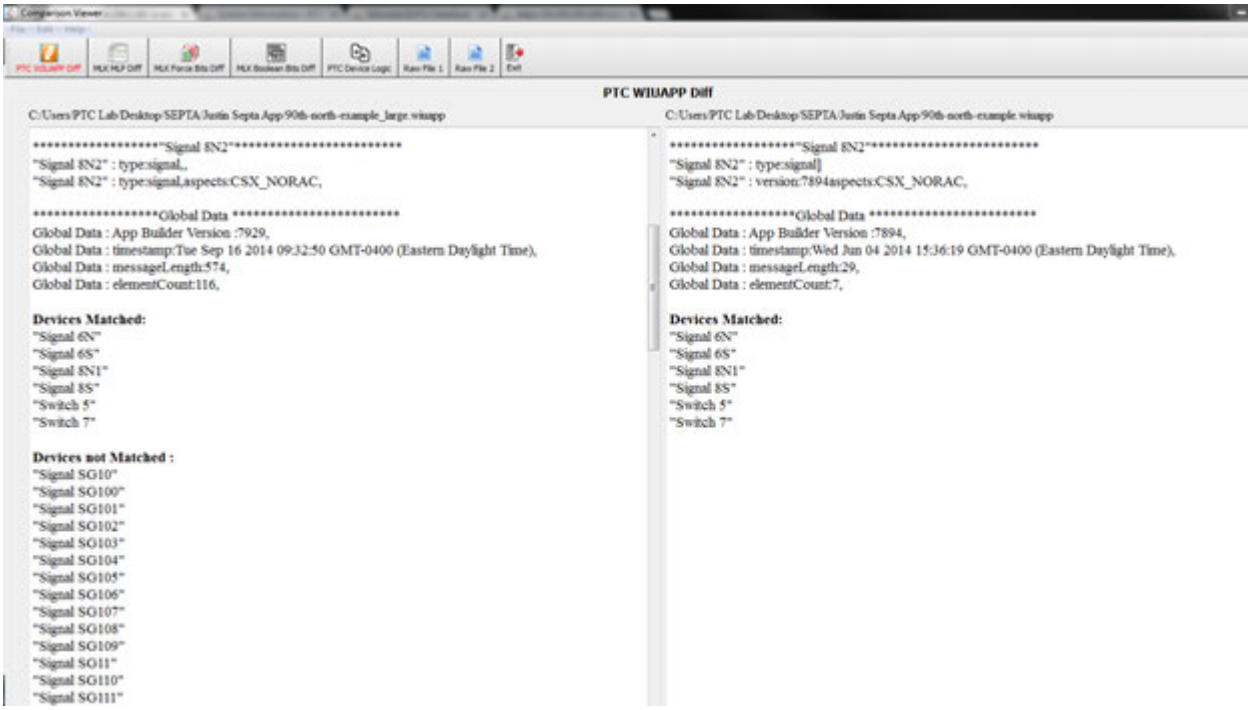
12. To compare the app builder program's global data, select the arrow next to Global Data category. A comparison of the global data will display.



13. To view a raw data file, select Raw File 1 or Raw File 2 icon from the main menu. The raw data file for the application will display.



14. There is no icon in the main menu for the Septa Section Data. Use the scroll bar in the middle of the screen to scroll down the page to view the Septa Section Data comparison list.



To return to any of the comparison screens, select the appropriate icon from the main menu.

8. WIU APPLICATION UPLOAD THROUGH A WEB INTERFACE

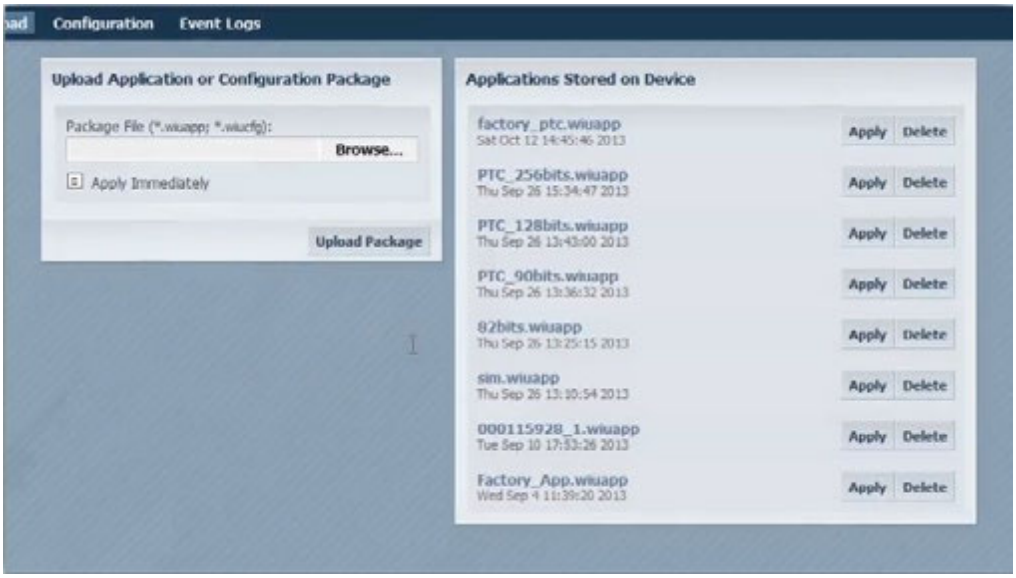
After successfully creating a WIU application as specified in Section 7, upload the WIU application as instructed below.

8.1. Uploading an Application and Monitoring the Unit

To successfully upload a new application and or configuration to the WIU you will need to make sure that you or someone else can locally press the reset button on the front of the WIU when prompted.

Once connected to the web interface and logged in on the unit, select the Application Upload tab.

In this tab you can upload a file that you have created using the WIU Application Builder, or load a previously stored application.



The box on the right displays any applications that are already stored on the unit. To load one of these applications, select the apply button. This will then prompt you to press the PTC reset button on the front panel of the CPU PCB. You have approximately 20 seconds to push the button before it times out. Once pushed, the unit will take the necessary steps to load the application and will prompt you when it is complete.

Select the Delete button to delete any previously loaded applications.

Click the Browse button to upload a new application. Browse to the appropriate file

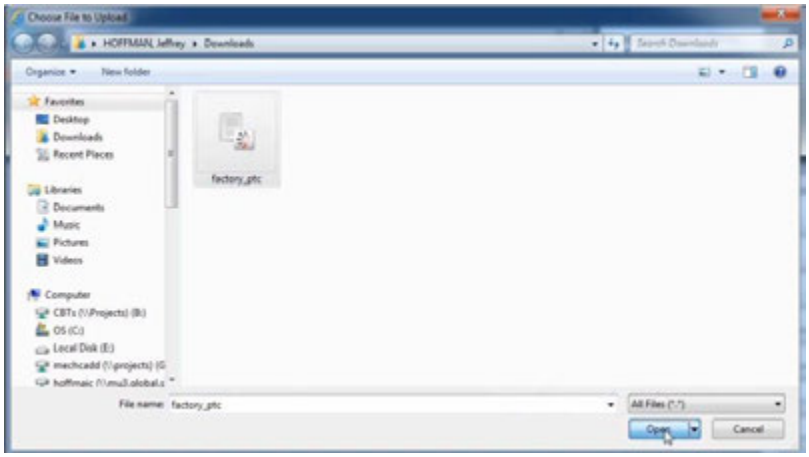
This will open the Choose File to Upload window. You can then browse for the desired file you wish to upload.

The uploader is compatible with either the .wiuapp or .wiucfg file extensions, which allows you to upload either an application or configuration file. If uploading a .wiucfg file your devices will not be changed, but only your configuration of the WIU itself.

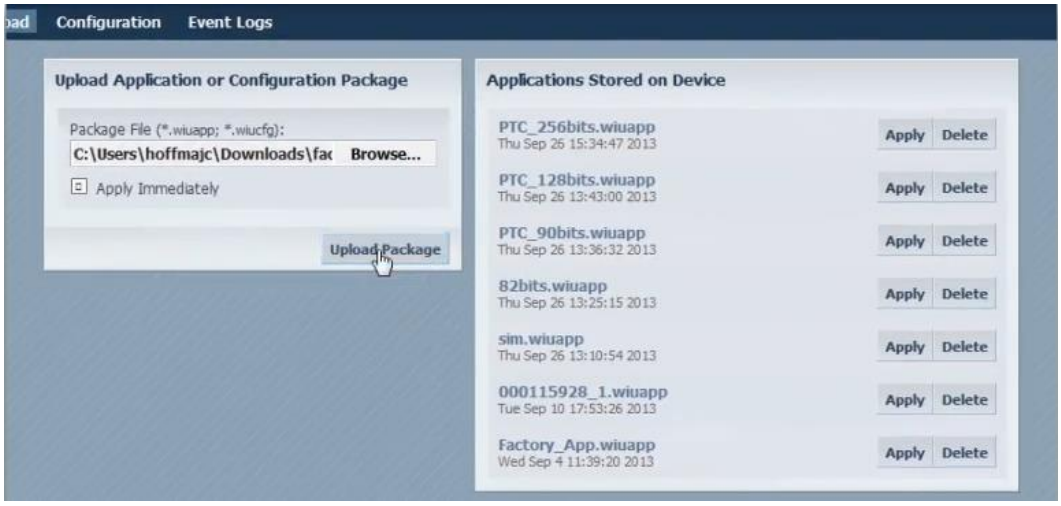
8.1.1. Uploading an Application File Example

Proceed as follows to upload an application file:

Browse to the appropriate file and select the Open button.



Select the Upload Package button.



Press the WIU's front panel reset button.

If the reset button is not pressed within 20 seconds, the dialogue box will disappear. The dialog box counts down to indicate the amount of time remaining.

When reset button is pressed, the WIU will go through a series of steps to complete the upload process.

The Package Processing Finished screen will appear stating that the application has been successful.

8.2. Monitoring and Checking the Configuration Settings

Select the Configuration tab to monitor the unit and to check configuration settings.

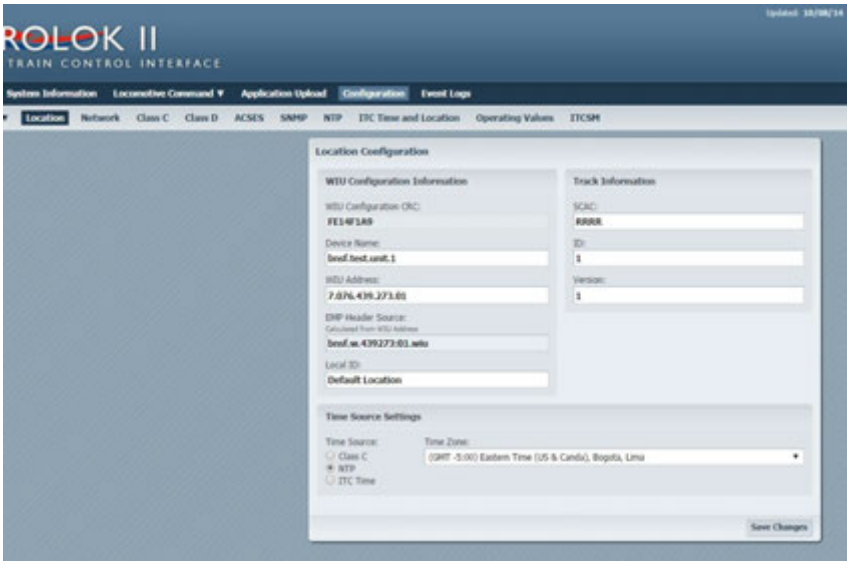
This opens the configuration settings. You can access various settings from the set of sub-tabs that appear below the main navigation. These tabs configure the parameters that you can configure using the application builder without having to have installed the application builder to the machine you are working from.

Select the Import Export tab. This will open a dropdown menu that displays three items:

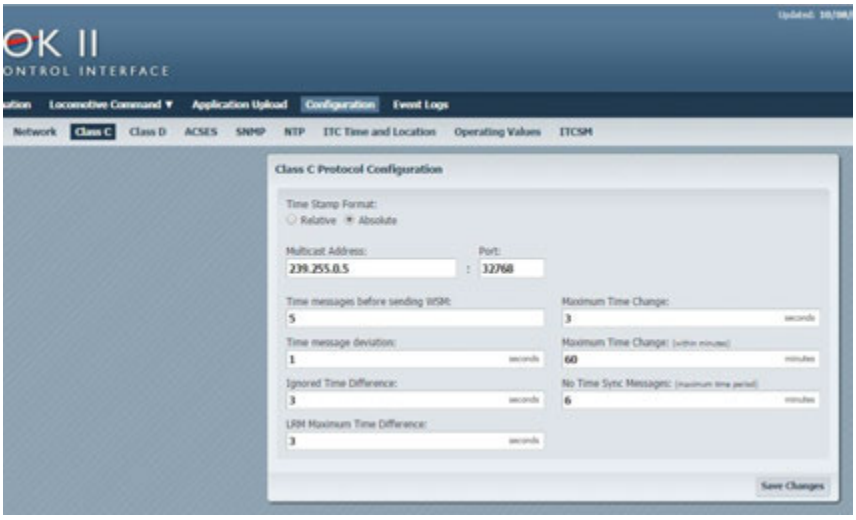
- Load configuration, which will open the Application Upload tab.
- Export to File, which allows you to save the configuration settings just as you would in the application builder. Select, Export to file. The browser will prompt you to open or save the file. Choose save, save as, and pick your desired location and file name for this file. You can export these settings as a WUICFG file for use in the application builder or on a different unit.
- Printable Summary, which will print all of the configurable values in your system, similar to the functionality of the generate report feature in the application builder.

The tab to the right of the Locomotive Command tab is the Network tab. The Network tab allows you to configure the IP addresses of your ports. Take precautions when doing this over the network, as it is possible to lose access to your device if an improper change is made.

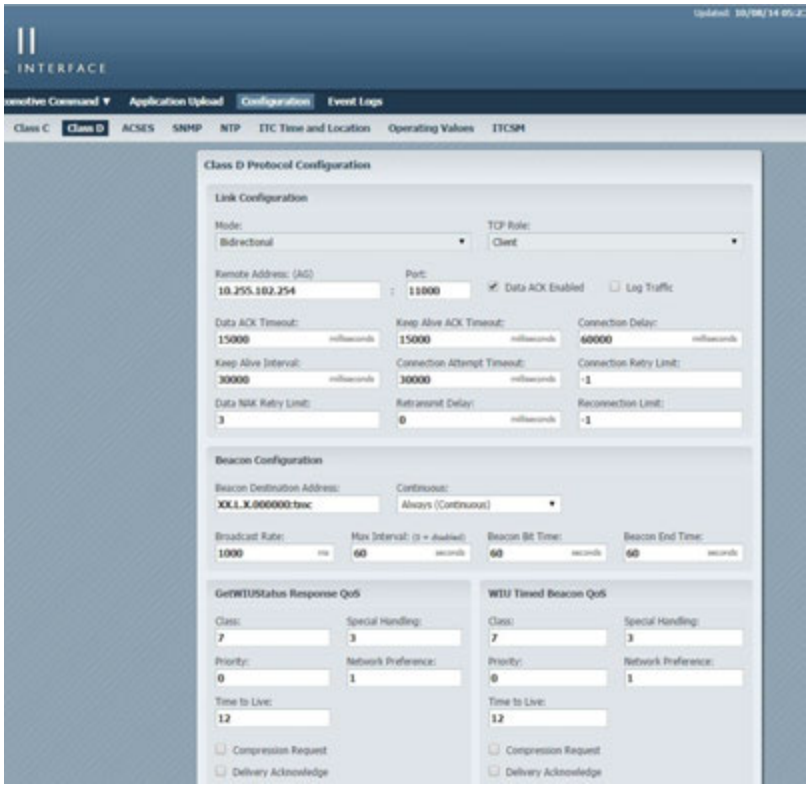
The Location, Class C, Class D, and NTP tabs are the same as in the application builder (Section 7.2).



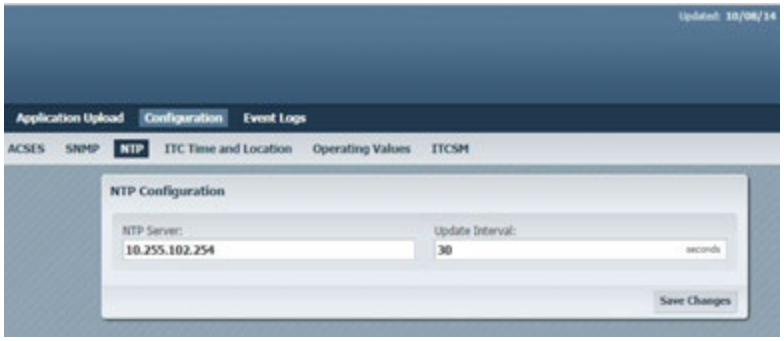
Location Tab



Class C Tab



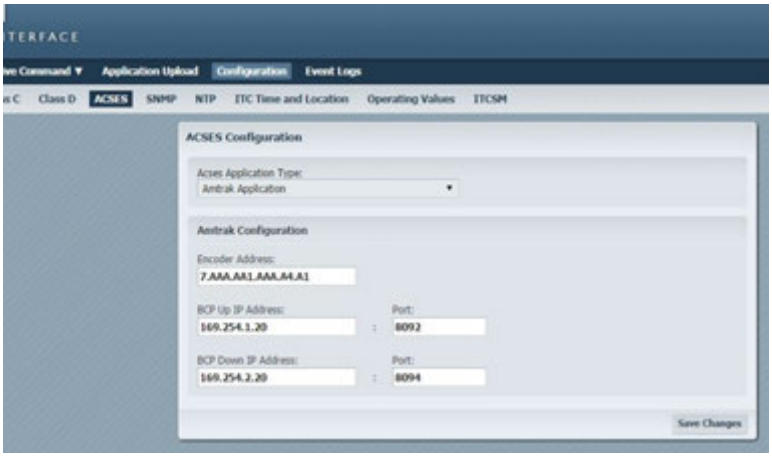
Class D Tab



NTP Tab

8.2.1. ACSES Configuration

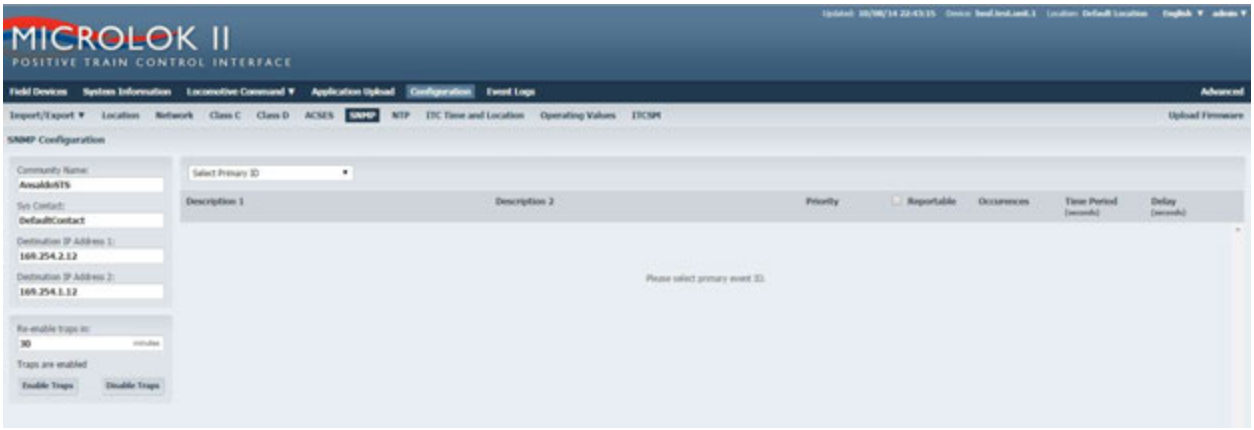
Select the ACSES tab. If your unit is configured for Advanced Civil Speed Enforcement System, ACSES, you can view some ACSES configuration settings in this window.



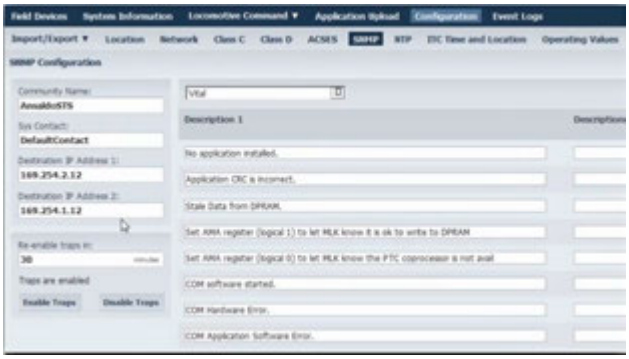
It allows you to see the application type and Encoder Address. This screen allows you to change these addresses and ports without having to build and upload a new application.

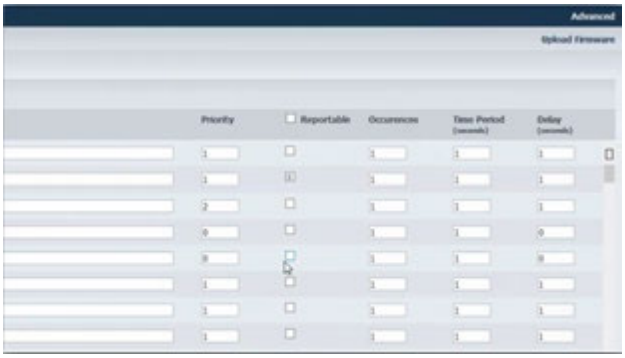
8.2.2. SNMP Configuration

Select the SNMP tab. This opens the SNMP Configuration window.



Click the Select Primary ID dropdown menu and select Vital.





Here you can select which event you want to be reported by SNMP by clicking the check boxes under the Reportable column.

All of this SNMP data is stored on the unit. The left panel with Server information is set up in the app builder under the SNMP field. These servers are typically located in the Central Office. You can select which messages are to be sent to Central office from the right side of the page by checking the Reportable box.

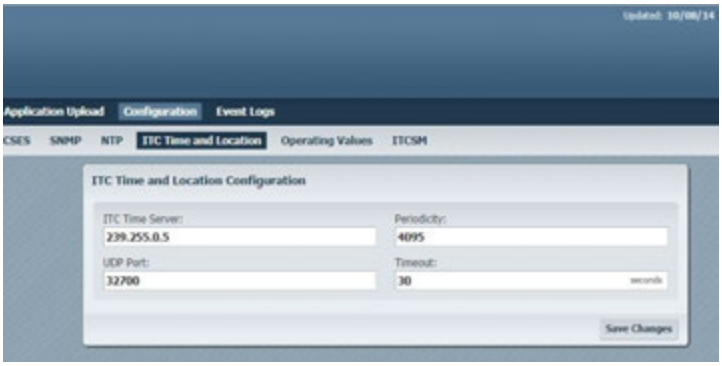
Select the Save Changes button at the bottom right of the page. This will save all changes you have made in the interface.

Any items with checked boxes will be reportable by SNMP to the destination IP address specified on the left of the interface.

The Disable Traps button disables all the SNMP traps for a specified period of time. In this case, the traps would be re-enabled in 30 minutes.

8.2.3. ITC Time and Location

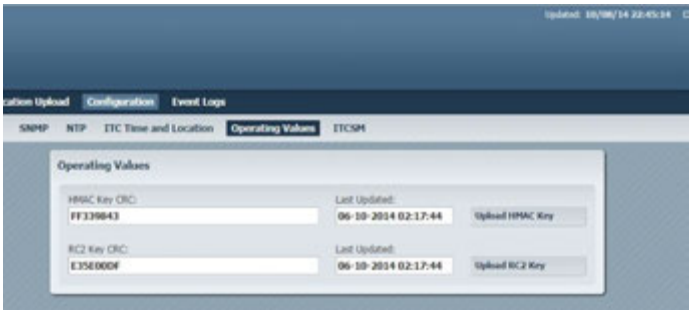
Select the ITC Time and Location tab.



This tab allows you to check and modify the IP address of the ITC time server and the Periodicity. It also shows the UDP port and timeout in seconds.

8.2.4. Operating Values

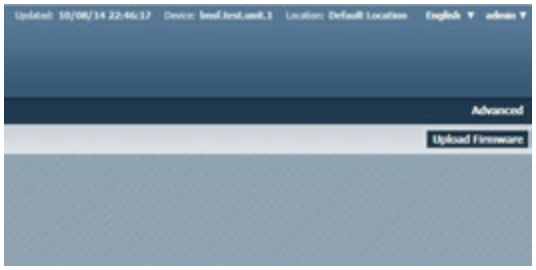
Select the Operating Values tab.



Here you can upload HMAC and RC2 keys directly to the unit via the web interface without having to build another application with the application builder. These would be changed for security purposes and it is much easier to update the values via the web interface rather than building and uploading a new application with the new HMAC and RC2 keys. For security purposes these keys are only visible to the administrator user. To change these keys click the Upload HMAC key or click the Upload RC2 key.

The HMAC key must be input in its encrypted form as it would be in the app builder. Once the key is in select Upload HMAC Key. A successfully uploaded box will appear. The RC2 key will be uploaded in the same manner, although it does not have to be encrypted.

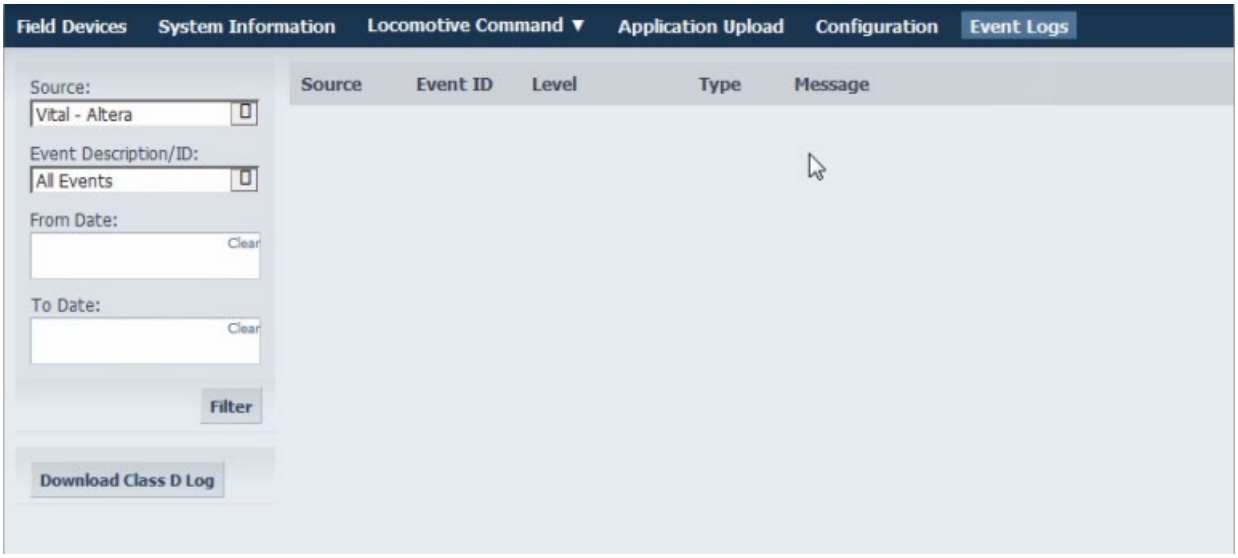
Select the Upload Firmware tab.



This tab is only visible if you are an administrator user. It allows you to update your unit's firmware by uploading a tar package specifically made for the WIU. A tar package is a software upgrade for the processors in the WIU. These updates are necessary to keep the unit running up to par.

8.2.5. Events Log

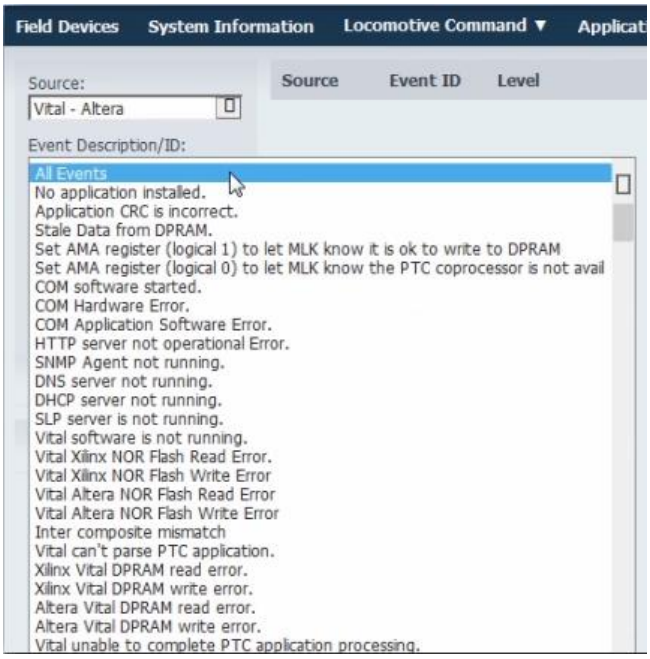
Select the Event Logs tab.



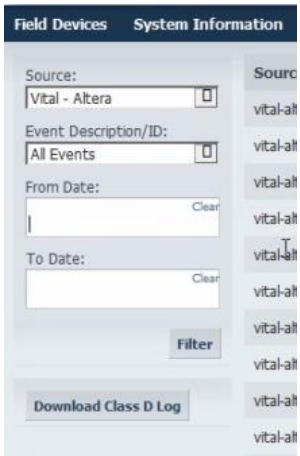
This will display a live view of what events the unit is reporting. If an event occurs, it will be displayed in the log.

Select the Source dropdown menu on the left of the interface to filter which event sources are displayed

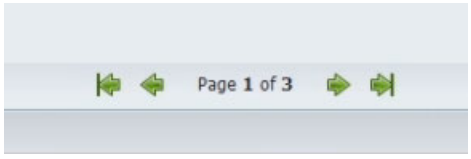
Select the Event Description ID dropdown menu to filter events by their description.



Select the From Date and To Date items to select a period of time to display only those events that occurred during the selected period.



Use the green arrows at the bottom of the screen to navigate through the pages of event.



To download the class D log, click the Download Class D log button in the left panel. This feature allows you to download a .txt file of the traffic logs for all the class D messages.

Select the Export to File button at the bottom right of the interface. The Export Events window will appear.

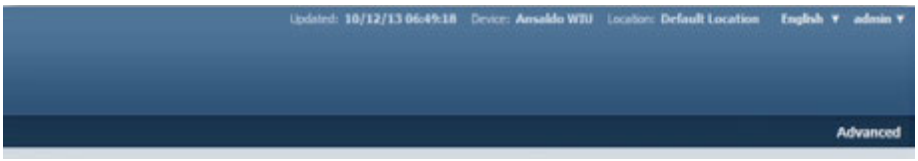
The number of events that you wish to export and download can be entered in this window. To export all of the records, enter -1 and select the Download button.

A Success window will appear where you can download these records. Select the Download Records button to download the records.

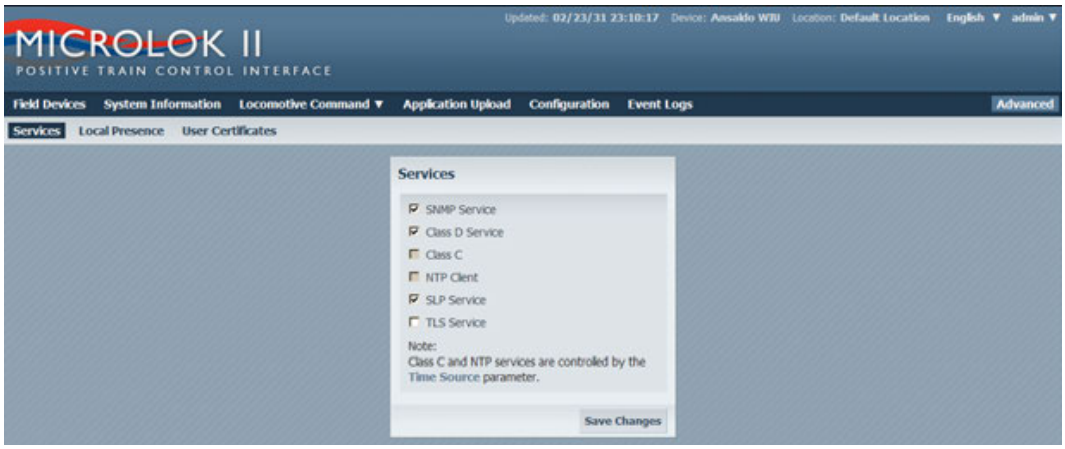
This will create a csv file containing however many logs you have specified to export. This file will open with Microsoft excel. The file can then be printed, if necessary. When done with the file, save and close the excel document and to return to the PTC web interface.

8.2.6. Advanced Screen Displays

Select the Advanced tab at the upper right side of the screen. This tab is only visible if you are an administrator user.



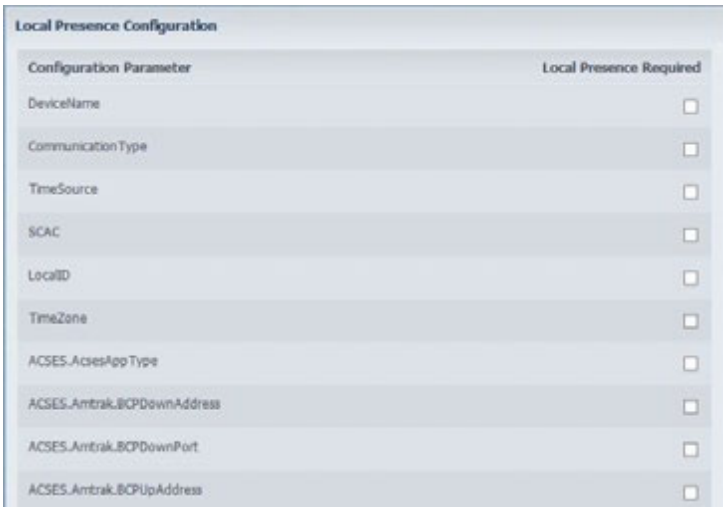
The first tab shown is Services.



Here you can start and stop different services that are running on the device. If the box next to a service is checked, the service is running. If it is not, the service is not currently running.

Select the Local Presence tab.

All vital parameters require local presence at the unit. You can configure non-vital parameters to require local presence also.



If the box to the right of a parameter is checked, it requires local presence to be configured. This means that to make any change to that specific parameter, you would need to manually press the button on the front panel of the unit to prove you are accessing it locally. If the check box next to a parameter is not checked, it does not require a local presence.

Select the User Certificate tab.

Here you can browse for single sign-on certificates if, for example, you wish for a password to not be necessary when any users are logging on.

The certificate files are in a PEM format. You can only change the certificates for yourself and any users beneath you.

To browse for a certificate, select the Browse button. Here you can locate and select the PEM file. Once done, select the Open button.

Select the Upload button to initiate the use of the selected certificate.

After any session in the PTC interface, be sure to sign out before exiting. To do this, select the Admin dropdown at the top right of the screen.

Select the Sign Out link. This may bring you to a Please Sign In window.

From this point, you or someone else can sign in, or you can exit out of the interface.

9. RAIL TEAM AND TECHNICAL SUPPORT

The Rapid Action Information Link Team (RAIL Team) is a group of experienced product and application engineers ready to assist the user to resolve any technical issues concerning this product. Contact the RAIL Team in the United States at 1-800-652-7276 or by e-mail at railteam@ansaldo-sts.us.

End of Manual