Red Lion®

SN/RAM® 6000 & RAM 9000 Software Manual

Firmware Version 3.29/4.29

Software Manual | August 2018

LP0997-E

COPYRIGHT

Red Lion Controls, Inc.

20 Willow Springs Circle

York, PA 17406 USA

CONTACT INFORMATION:

Inside US: +1 (877) 432-9908
Outside US: +1 (717) 767-6511

Website: www.redlion.net

Email: support@redlion.net

Table of Contents

Preface

Disclaimer

Portions of this document are intended solely as an outline of methodologies to be followed during the maintenance and operation of the SN and RAM® equipment. It is not intended as a step-by-step guide or a complete set of all procedures necessary and sufficient to complete all operations.

While every effort has been made to ensure that this document is complete and accurate at the time of release, the information that it contains is subject to change. Red Lion Controls is not responsible for any additions to or alterations of the original document. Industrial networks vary widely in their configurations, topologies, and traffic conditions. This document is intended as a general guide only. It has not been tested for all possible applications, and it may not be complete or accurate for some situations.

Users of this document are urged to heed warnings and cautions used throughout the document.

Purpose

This manual gives specific information on how to apply and use the software functions on the Red Lion Sixnet® Series SN and RAM® Cellular RTUs/Routers. The RAM models are RTUs (with a built-in router) and the SN models are routers.

This manual applies to the following products:

SN-66xx	SN-67xx	SN-68xx	SN-69xx
RAM-66xx	RAM-67xx	RAM-68xx	RAM-69xx
RAM-96xx	RAM-97xx	RAM-99xx	

Audience

The manual is intended for use by personnel who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general Ethernet functions, the Internet Protocol (IP), Simple Network Management Protocol (SNMP), and cellular technology.

Compliance Statements & User Information

FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates uses and can radiate radio frequency energy; and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference to radio communications, in which case the user will be required to correct the interference at their own expense.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Per FCC requirements the antenna gain including cable loss must not exceed 7.5 dBi in the cellular band, 3 dBi in the PCS band, 5.5 dBi for LTE Band 4, and 9 dBi in the LTE Band 17 for RF exposure purposes of 2.1091. The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter evaluation procedures

User Compliance Information

If this equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

In order to meet FCC emissions limits, this equipment must be used only with cables that comply with IEEE 802.3.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions.

The user may find the following booklet prepared by the Federal Communications Commission helpful:

“How to Identify and Resolve Radio-TV Interference Problems”.

This booklet is available from: U.S. Government Printing Office, Washington DC, 20402 Stock No. 004-000-00345-4.

Canadian Compliance Statement

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matérial brouilleur du Canada.

Trademark Acknowledgments

Red Lion Controls, Inc acknowledges and recognizes ownership of the following trademarked terms used in this document.

- Ethernet™ is a registered trademark of Xerox Corporation

All other company and product names are trademarks of their respective owners.

Document History and Related Publications

The hard copy and electronic media versions of this document are revised only at major releases and therefore, may not always contain the latest product information. As needed, Documentation Notes and/or Product Bulletins will be provided between major releases to describe any new information or document changes.

The latest online version of this document and all product updates can be accessed through the Red Lion web site at www.redlion.net/support/documentation.

Publication History

The following information lists the release history of this document.

ISSUE/REVISION	RELEASE DATE	CONTENT DESCRIPTION
2014-03-31	April 2014	Supporting Firmware Version 3.17/4.17
2014-07-29	July 2014	Supporting Firmware Version 3.18/4.18
2014-10-20	October 2014	Supporting Firmware Version 3.19/4.19
2015-02-19	February 2015	Supporting Firmware Version 3.20/4.20
2015-07-21	July 2015	Supporting Firmware Version 3.21/4.21
2015-09-30	September 2015	Supporting Firmware Version 3.22/4.22
2016-02-12	February 2016	Supporting Firmware Version 3.23/4.23
2016-08-12	August 2016	Supporting Firmware Version 3.24/4.24
2017-01-23	January 2017	Supporting Firmware Version 3.25/4.25
2017-08-31	August 2017	Supporting Firmware Version 3.27/4.27
2017-12-22	December 2017	Supporting Firmware Version 3.28/4.28
2018-08-20	August 2018	Supporting Firmware Version 3.29/4.29

Related Documents

Visit the Technical Resources page on the Red Lion website at the following link to view available documents related to this product www.redlion.net/sixnet_documentation.

Additional Product Information

Additional product information can be obtained by contacting the local sales representative or Red Lion through the contact numbers and/or e-mail addresses listed on the inside of the front cover.

Document Comments

Red Lion appreciates all comments that will help us improve our documentation quality. The user can submit comments through the Red Lion Customer Service. Simply email us at customer.service@redlion.net.

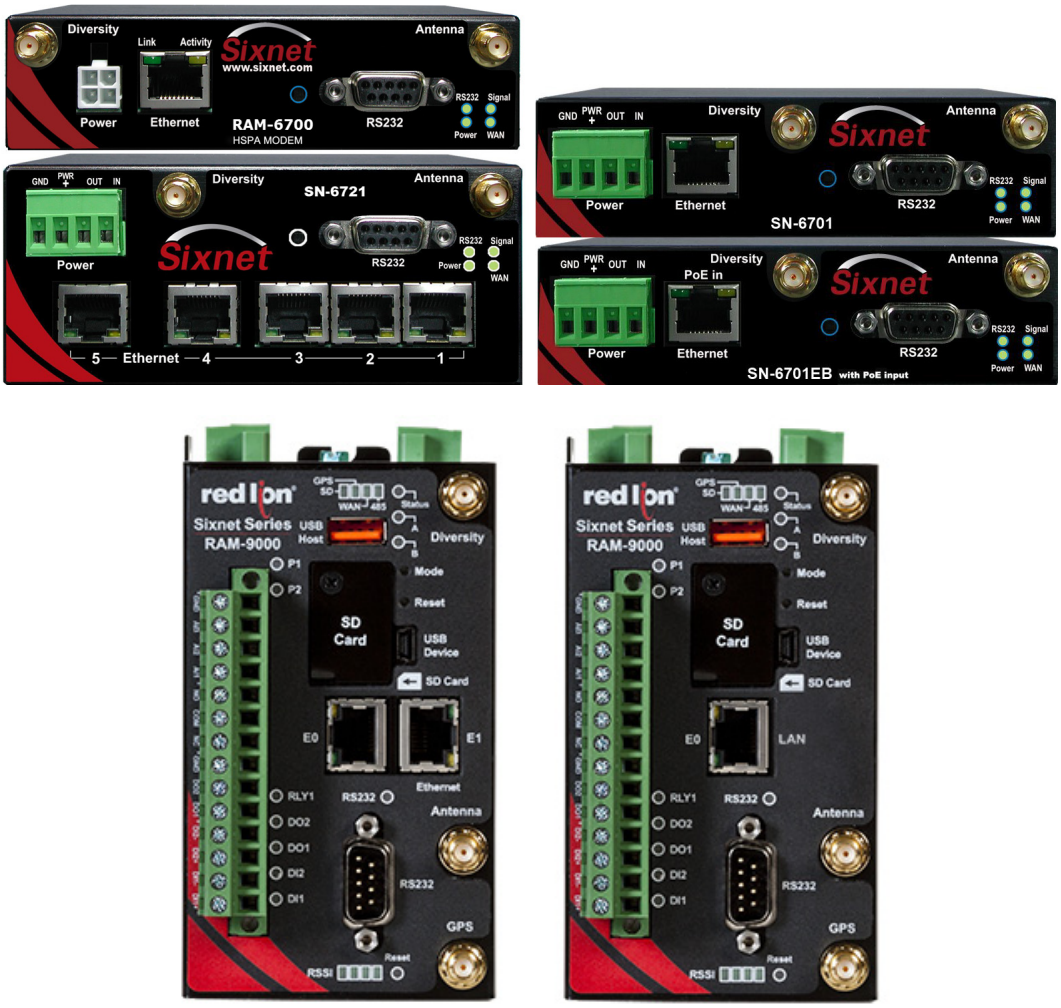
Chapter 1 Accessing the Web User Interface

There are three connection methods available for first time connection to configure your new Red Lion device:

- Autonet (new with version 4.27)
- Ethernet Port(s) with Static IP(s)
- USB Device port

Set Up

Connect a CAT-5 or CAT-6 Ethernet cable between the local PC and the Red Lion RTU or router's Ethernet port(s).



Note: If the Ethernet port's green LED is lit, this indicates that the connection is running at 100Mb speed. If the Ethernet port's green LED is not lit, this indicates that the connection is running at 10Mb speed. The yellow LED indicates the "link" status of the connection.

Yellow steady= Link established. Yellow flashing = Data packets are being transferred.

1.1 Configure Using AutoNet Method

When using AutoNet, connect the eth0 port to any Ethernet network or directly to a PC. It will discover other DHCP networks and will either join automatically or provide a DHCP address to the connected PC.

Inspect the product label on your unit to find the field “Eth0 MAC” and notice the last 6 digits or letters.

If your MAC address was 02-FF-EE-1A-34-5B, then the unit can be accessed by entering http://RAM-1A345B.local in your browser.

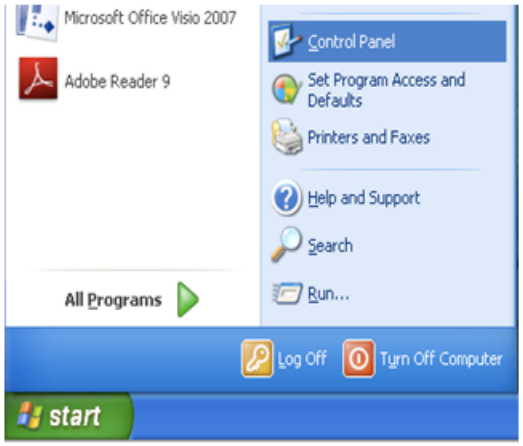
Once you configure your Ethernet port for use in production, AutoNet will be automatically disabled. If AutoNet does not seem to be working in your environment, you can always fall back to the previously supported methods of access described in 1.2 and 1.3.

1.2 Setup PC IP Address

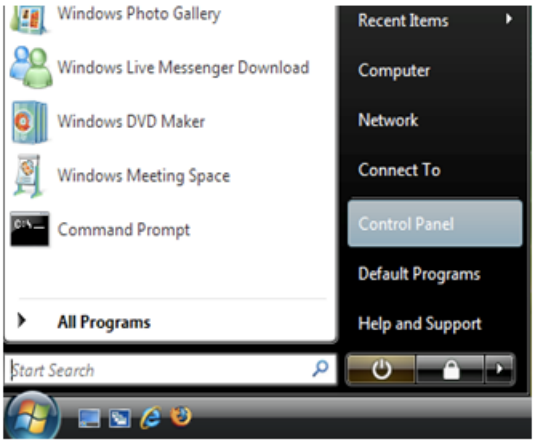
1.2.1 Open the Control Panel

Click on Start and browse the “Control Panel” menu item. The Control Panel should look similar to the following:

XP



Vista/Windows 7



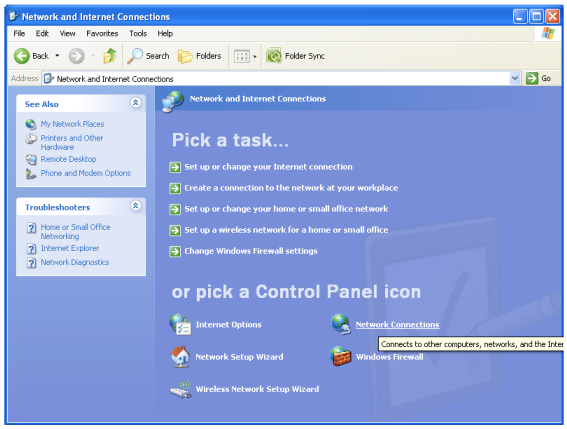
1.2.2 Access Network and Settings

Click on the link to access network and Internet settings

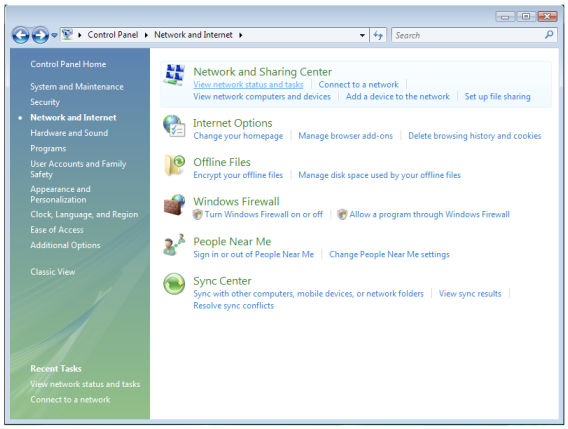
- XP - “Network and Internet Connections”
- Vista/Windows 7 “Network and Internet”

The displays should be similar to the following:

XP



VISTA/WINDOWS 7



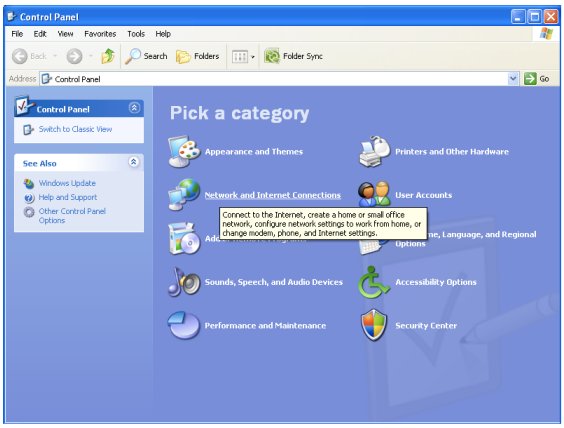
1.2.3 Access Network Connection Settings

Click on the link to access network connection settings.

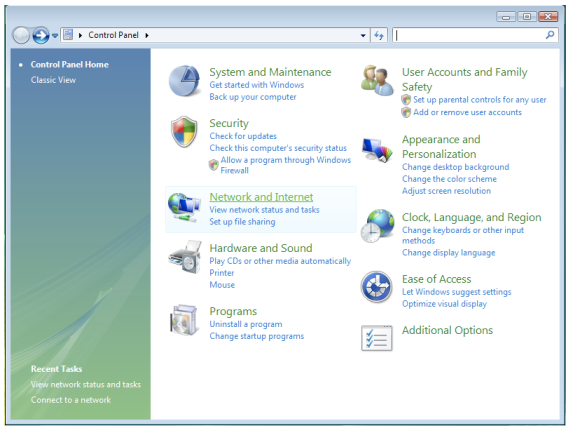
- XP - “Network Connections”
- Vista/Windows 7 - “Network and Sharing Center”

The display should look similar to the following:

XP



VISTA/WINDOWS 7



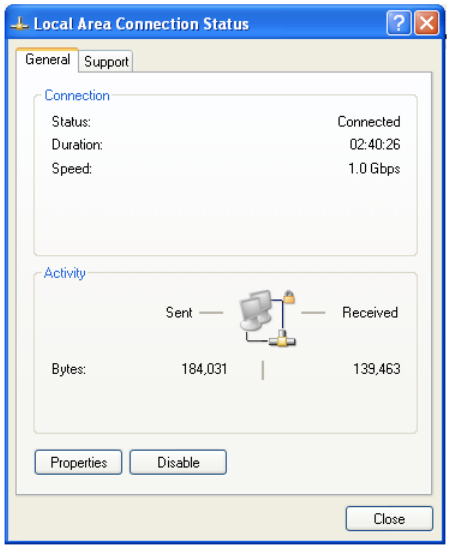
1.2.4 Access Local Area Connection

Click on the link to access the local area connection.

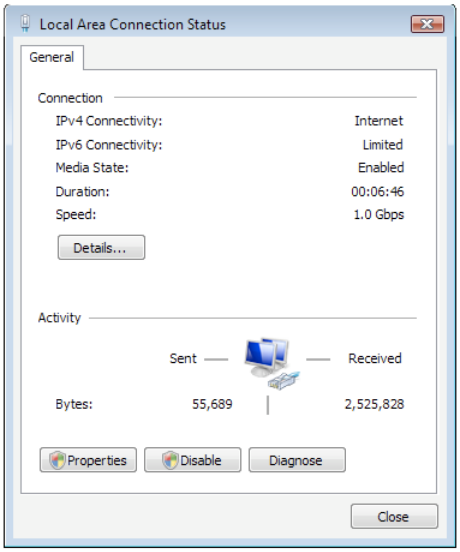
- XP - “Local Area Connection” icon
- Vista/Windows 7 - “View Status” next to Local Area Connection

The display should look similar to the following:

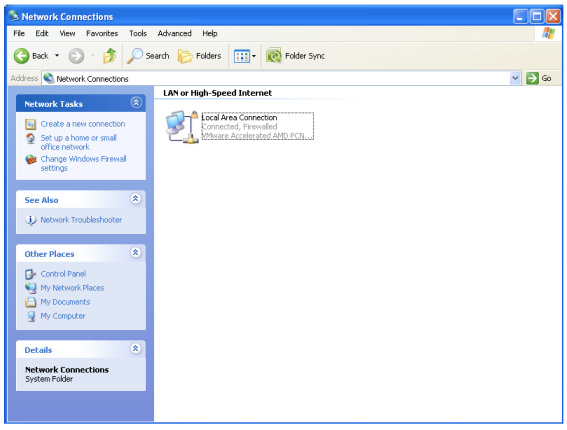
XP



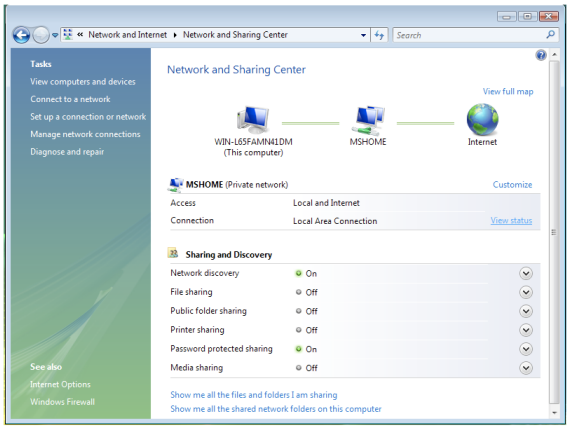
Vista/Windows 7



XP



Vista/Windows 7

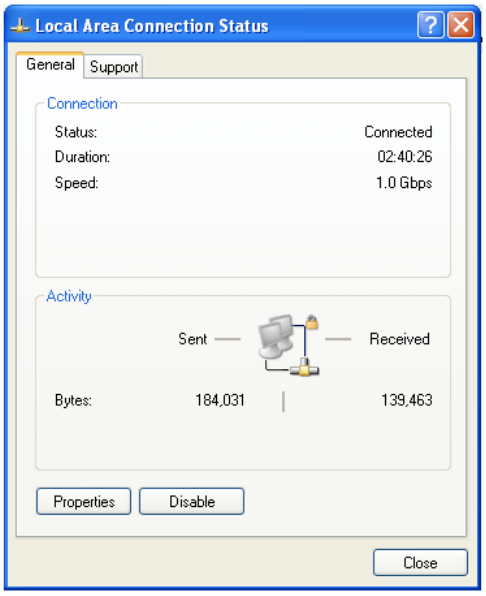


1.2.5 Open Properties

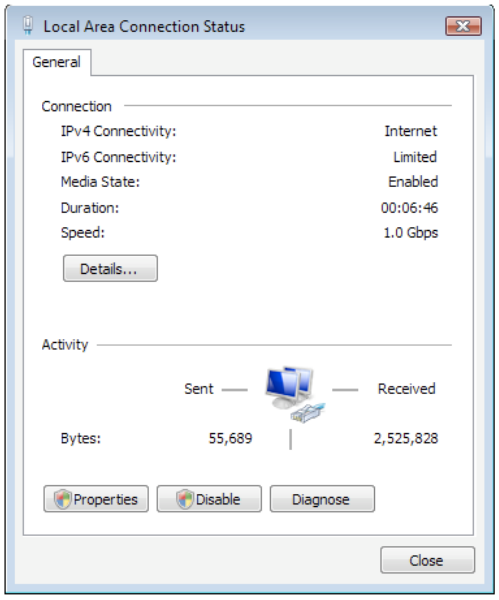
Click on *Properties* button (Vista/Windows 7 will display a popup window asking to confirm the operation).

Click on the *Continue* button. The display should look similar to the following:

XP



Vista/Windows 7



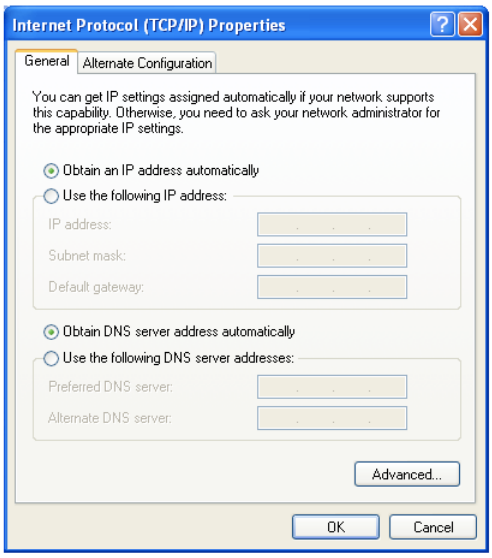
1.2.6 Access Internet Protocol Properties

Click on the Internet Protocol to highlight.

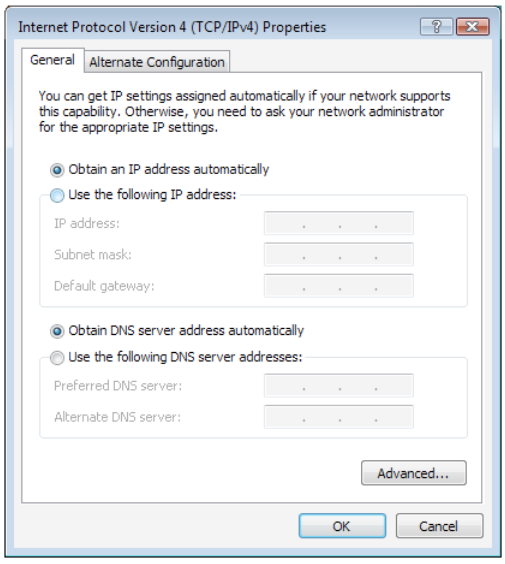
- XP - “Internet Protocol (TCP/IP)”
- Vista/Windows7 - “Internet Protocol Version 4 (TCP/IPv4)”

Click on the *Properties* button. The display should look similar to the following:

XP

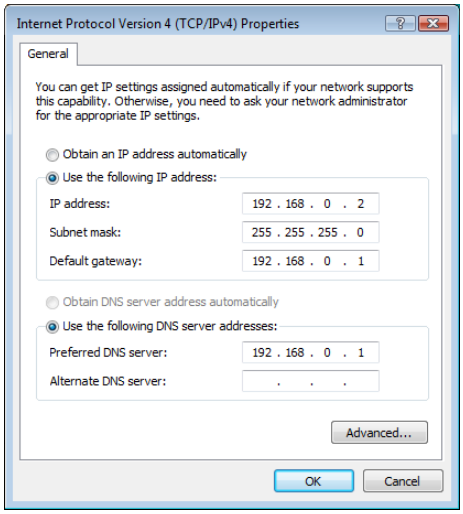


Vista/Windows 7



METHOD 1: PC to: WAN /ETH0, Ethernet on SN/RAM 6000, RAM 9000

Select Use the following IP address and fill in the blank fields with the information below:



- IP address:192.168.0.2
- Subnet mask:255.255.255.0
- Default gateway:192.168.0.1
- Preferred DNS:192.168.0.1

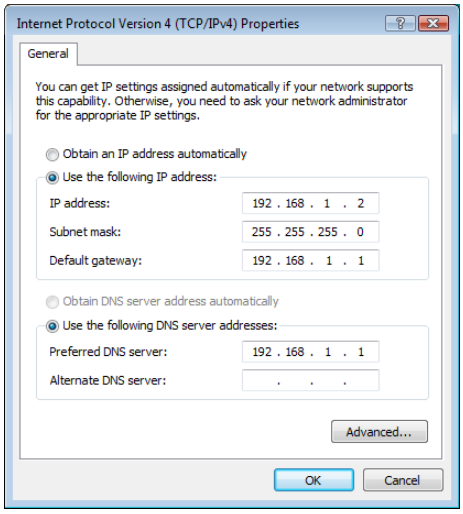
Click OK.

The previous screen appears.

Click OK.

METHOD 2: PC to LAN: ETH1, RAM 9000 Series only

Select Use the following IP address and fill in the blank fields with the information below:



- IP address:192.168.1.2
- Subnet mask:255.255.255.0
- Default gateway:192.168.1.1
- Preferred DNS:192.168.1.1

Click OK.

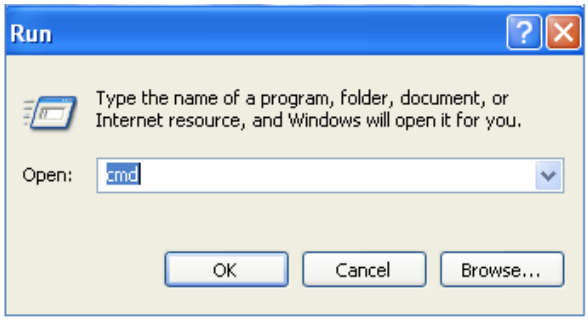
The previous screen appears.

Click OK.

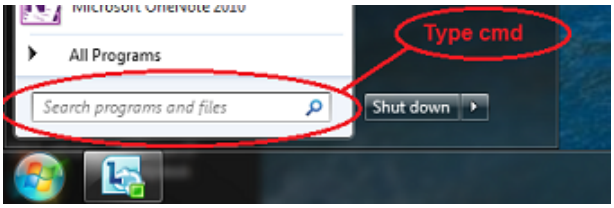
Verify that you are connected to the RTU or router.

Open a Command Prompt window on your laptop.

- XP →Start →Run, type in **cmd** and press the **ENTER** key.



- Vista/Windows 7 →Start →Search window just above the Start icon, type in cmd, wait for Vista/Windows 7 to locate the program, click on the cmd program if finds.

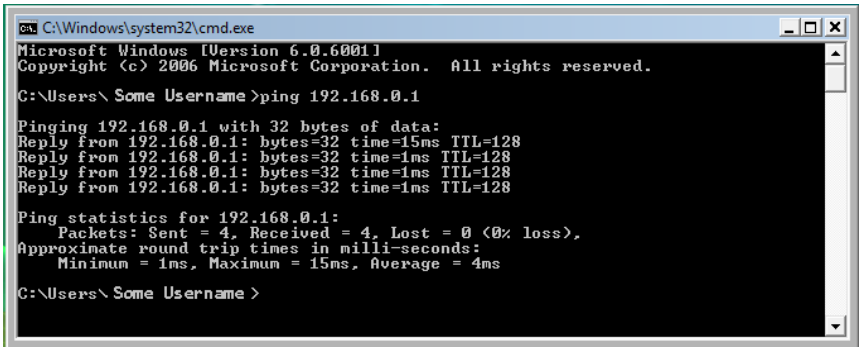


Verify connectivity to the RTU or router by running a “ping” to the IP Address of the Ethernet port you are connected to.

METHOD 1: PC to WAN /ETH0, Ethernet on SN/RAM 6000, RAM 9000

Type in **ping 192.168.0.1** and then press the **ENTER** key

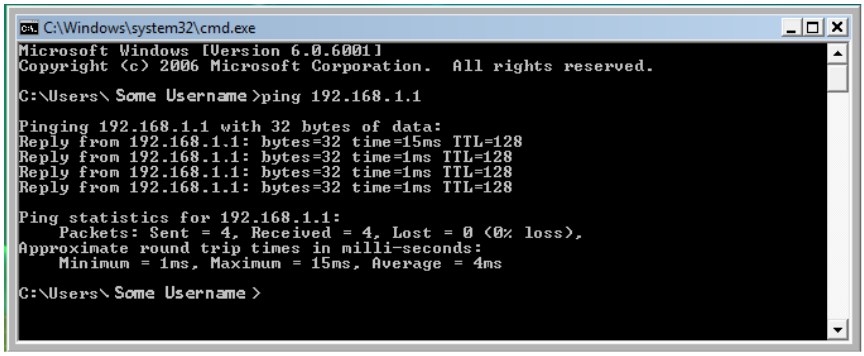
The display should look similar to the following:



METHOD 2: PC to ETH1: LAN on RAM 9000 only

Type in **ping 192.168.1.1** and the press the **ENTER** key

The display should look similar to the following:



This shows the connection is up and functioning.

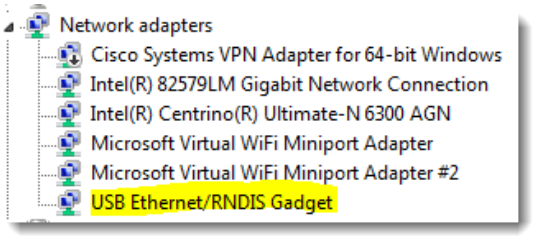
1.3 Installing RNDIS Driver for Ethernet Connectivity over USB

This section outlines the required method to manually install the correct RNDIS driver for your Red Lion device. This will enable the unit to connect via USB and behave as an Ethernet device.

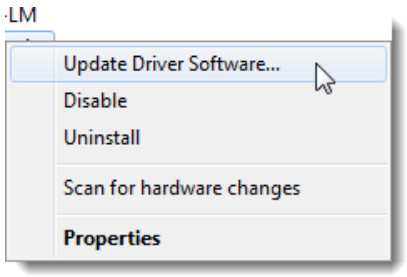
Power on the Red Lion device and connect to your Windows PC via the USB mini cable.

Observe the Microsoft® Windows behavior to see if the unit is properly detected. An audible sound, as the cable is connected, should be heard and Microsoft Windows begins searching for the correct USB driver.

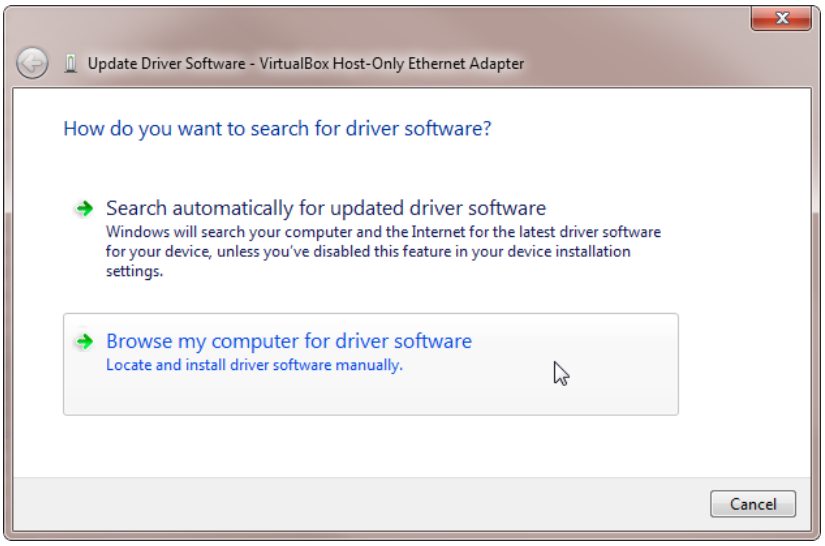
Most Windows systems will automatically locate and install a driver. The device would appear in the Windows Device Manager as seen below:



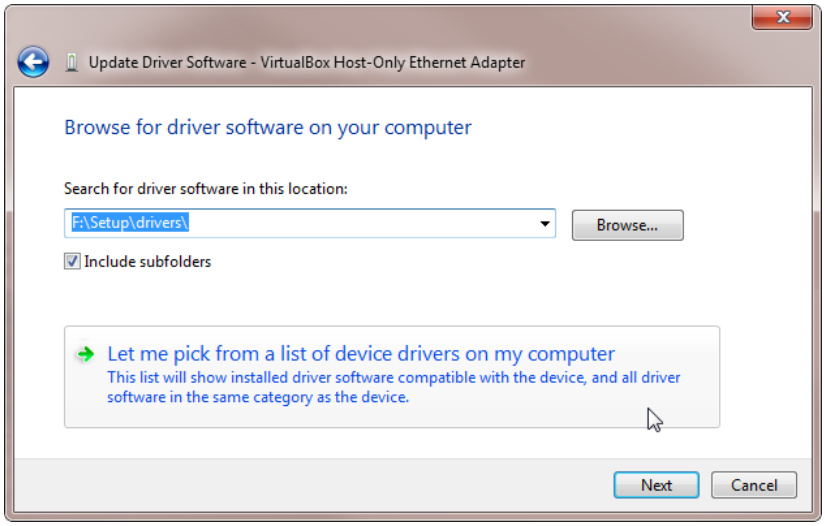
Right-click on the USB Ethernet/RNDIS Gadget adapter, and select Update Driver Software.



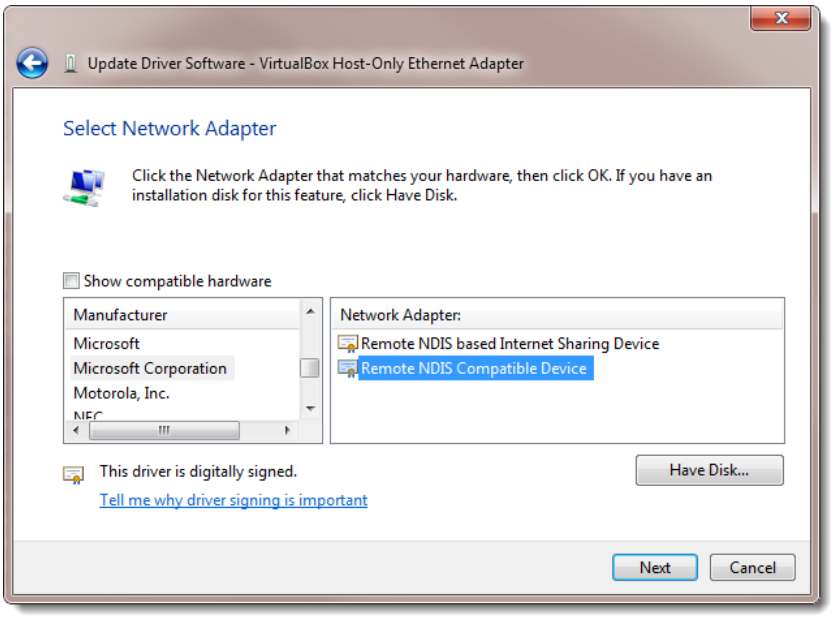
Select Browse my computer for driver software:



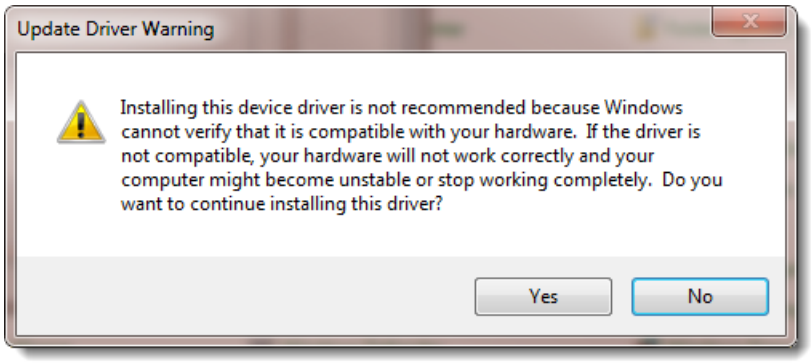
Select *Let me pick from a list...*



Uncheck the *Show Compatible Hardware* check box. In the Manufacturer box, browse to Microsoft Corporation. Then select *Remote NDIS Compatible Device* in the Network Adapter box. Click *Next*.



The Update Driver Warning dialog window shown below appears. Click on Yes.



Once the install is complete, click on *Close*.

The USB Ethergadget driver should now be loaded and you should be able to access the Red Lion device via USB/ Ethernet at 192.168.111.1:10000.

1.4 Access Red Lion Web Server

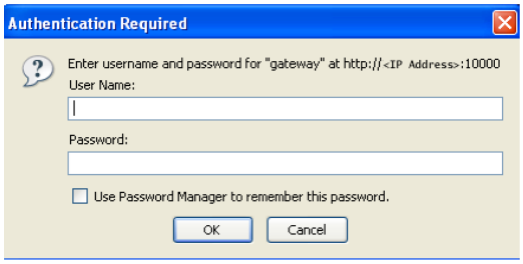
Open a web browser* and enter the following in the address bar:

METHOD 1 (WAN/ETH0):	http://192.168.0.1:10000/
METHOD 2 (LAN/ETH1):	http://192.168.1.1:10000/
METHOD 3 (USB):	http://192.168.111.1:10000/

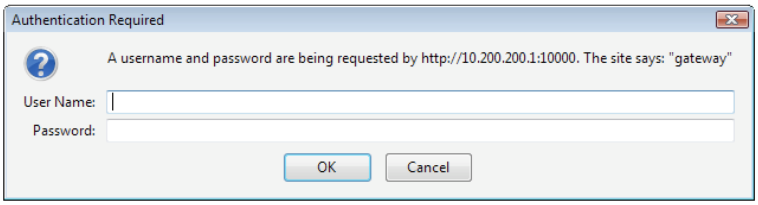
* Browsers currently supported: Internet Explorer 10 & 11, Chrome 42 Through 63.

You will receive a login pop-up screen.

XP



Vista/Windows 7

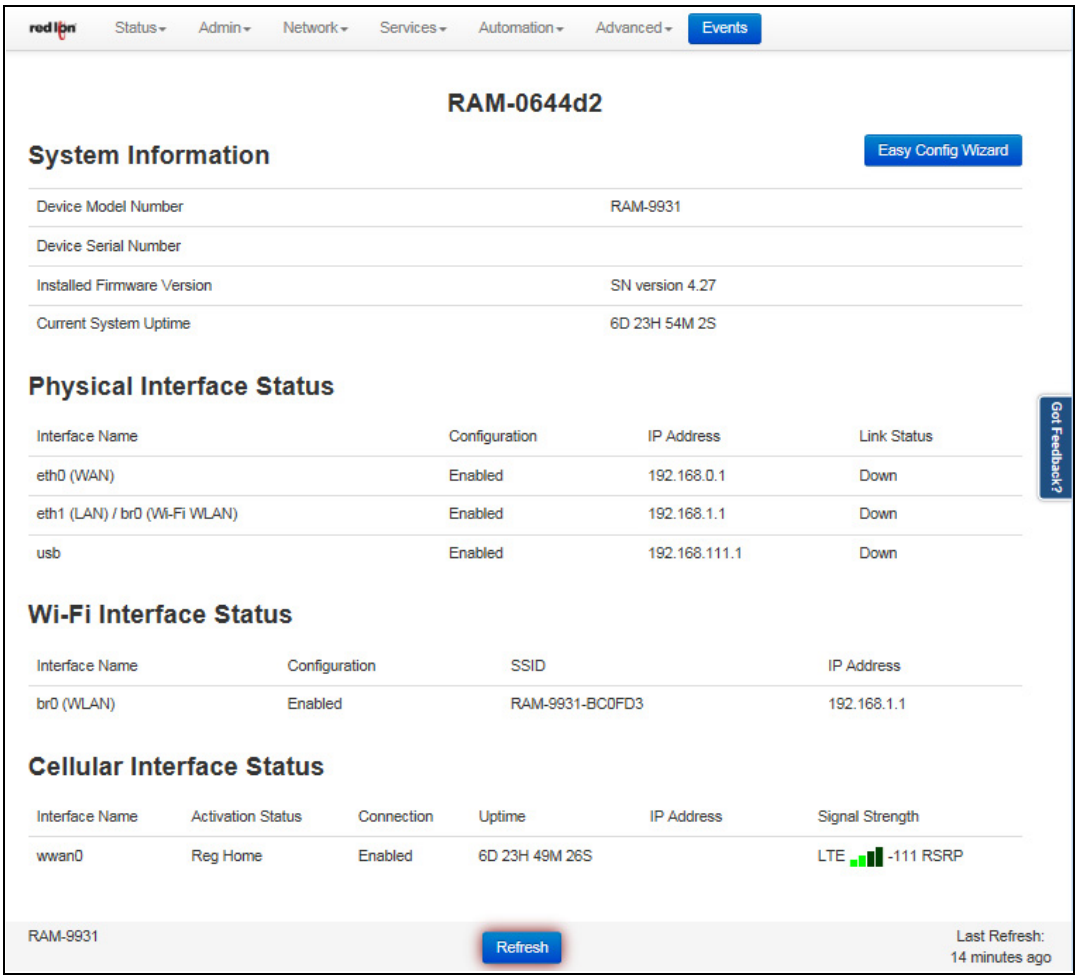


1.4.1 Red Lion RTU or Router Login Instructions

- For the User Name, enter: **admin** (all lowercase)
- For Password, enter the **last six digits of the serial number**, located on the product label (all lowercase)

Upon successfully logging in, the following screen appears:

Note: The following information can be used for all series of RAM RTUs or SN routers. Some models may have reduced options.



At this point, you are connected to the Red Lion RTU or router and can configure it to meet your needs.

If the ppp0 or wwan0 interface do not show an IP address, this could indicate that the internal SIM/Module has not been properly activated. Low or invalid signal strength may also contribute to the issue. Please contact your service provider to ensure proper activation. You may need to enter provisioning information in the Networking→Cellular→Provisioning screen. Consult Section 2.1 for more information.

1.4.2 SSH, Telnet, Serial RS-232 Connections to Red Lion RTUs or Routers

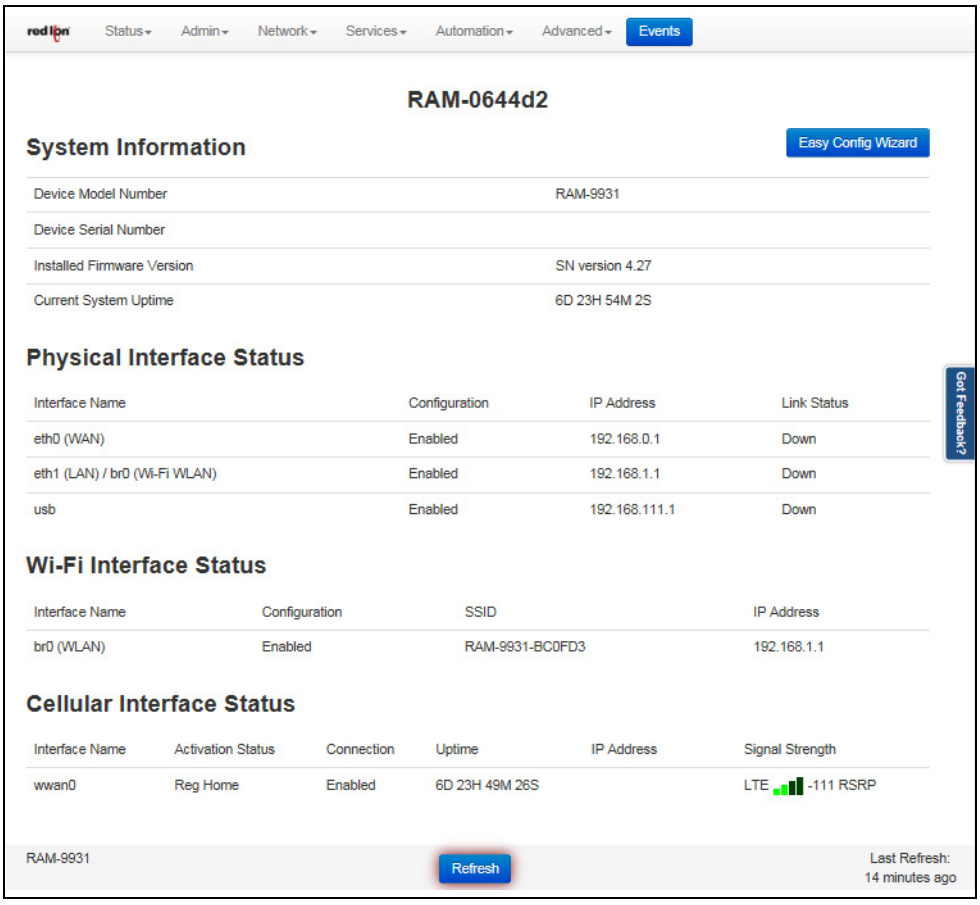
For alternative connections to the Red Lion RTU or router, please contact Red Lion Technical Support for additional documentation.

Note: The SN/RAM 6000 and RAM 9000 series have many modes of operation which can cause the power consumption and corresponding heat dissipation to vary greatly. This factor, along with others, can affect the performance and longevity of the unit. The SN/RAM 6000 series and RAM 9000 series are rated for operation from -40° to 75°C in typical applications where the cellular communication is moderate. Please see the respective hardware guides for more details.

Chapter 2 Cellular Connections

2.1 Cellular Configuration

Cellular connectivity is obtained through the use of an internal (embedded) RF Module.



Your Red Lion RTU or router has an embedded radio that has been detected and may be configured for the intended carrier. If you are using a carrier that supports the use of an Access Point Name (APN), you may have to set your specific APN manually, as covered in the next section. For GSM and LTE service, carriers may provide custom APNs for static IP addresses of VPNs scenarios depending on the type of account.

The 69xx and 99xx model families support switching between multiple carriers. Navigate to the Network → Cellular Connection → Provisioning screen to verify your carrier has been provisioned correctly for these models.

CDMA carriers 3G networks such as Verizon and Sprint do not rely on a SIM card and are activated over the air. See the Cellular Provisioning Section 2.1.3 of the manual for more details on CDMA OTA activations.

Embedded modules for CDMA (Sprint / Verizon) should activate automatically over the air once they are powered on and connected to an antenna. This of course is after you contact your carrier and have an account enabled and connected to the embedded module by providing the ESN / MEID number from the module to your carrier. This is how the carrier will tie your account to the internal cellular radio. For some CDMA based 1xRTT internal modules and Sprint Data-Link connections, additional configuration must be set in the Provisioning screen, detailed later.

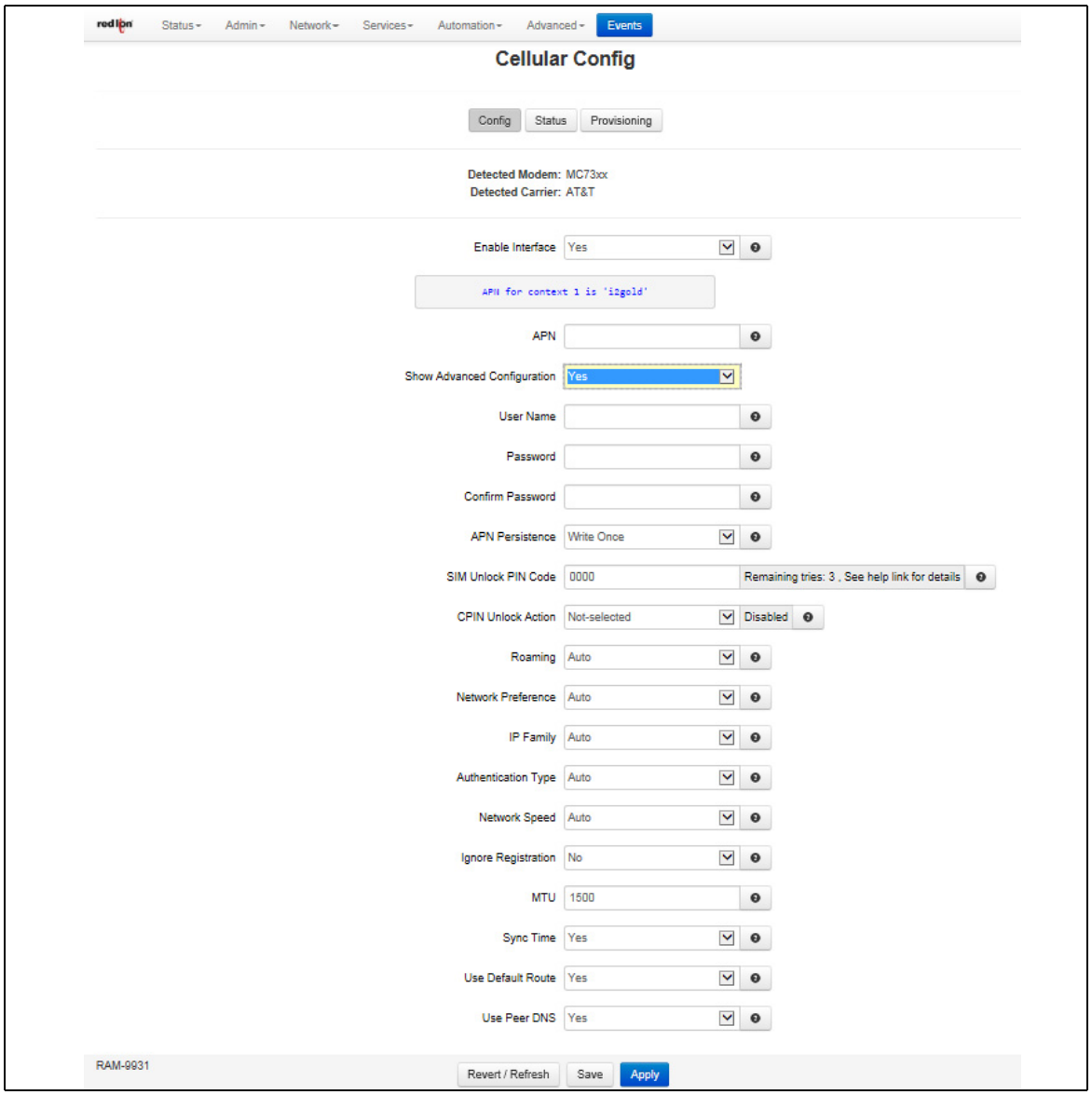
Navigate through the Web UI menu to Networking → Cellular Connection → Configuration screen shown in section 2.1.1. 3G and 4G/LTE GSM based carriers, such as AT&T®, Bell Mobility and Telus will require a SIM card be inserted into the unit and an APN code to be entered to confirm you are the verified user of that SIM. Be sure to only insert and remove the SIM card while the unit is powered off.

You can verify your cellular connectivity by viewing the Status Summary page of the web UI screen and observe if the Cellular Interface status shows an IP Address. On the Home screen you should see: Interface, Activation, Connection, IP Address and Signal Strength. If you do not see an IP Address get populated for the PPP-WWAN interface you may have an issue with your settings or your account has not been correctly activated.

Activation Status column: See table below for a description of the different statuses found in the “Activation Status” column.

CDMA	HSPA/LTE
Running - Connection/Activation is running	Not Reg - Modem not registered
Waiting - Connection/Activation tried and failed. Will retry in 20 mins.	Reg Home - Registered on Home Network
Succeeded - Connection/Activation successful	Searching - Searching for connection
Unavailable - Connection/Activation not supported	Reg Denied - No SIM or SIM no longer activated
Failed - Connection/Activation Failed	Unkn Stat - Unknown status
Available - Activation not running/Module has not tried to connect/Module already activated	Reg Roam - Registered on roaming network

2.1.1 Cellular Interface Configuration



Select Yes to enable the interface so it becomes active after the new settings are applied and upon subsequent system start-up. Select No to disable the cellular connection feature. More information on setting up the unit's cellular connection can be found in Section 3.4.1.

2.1.2 Set the User Name, Password and APN

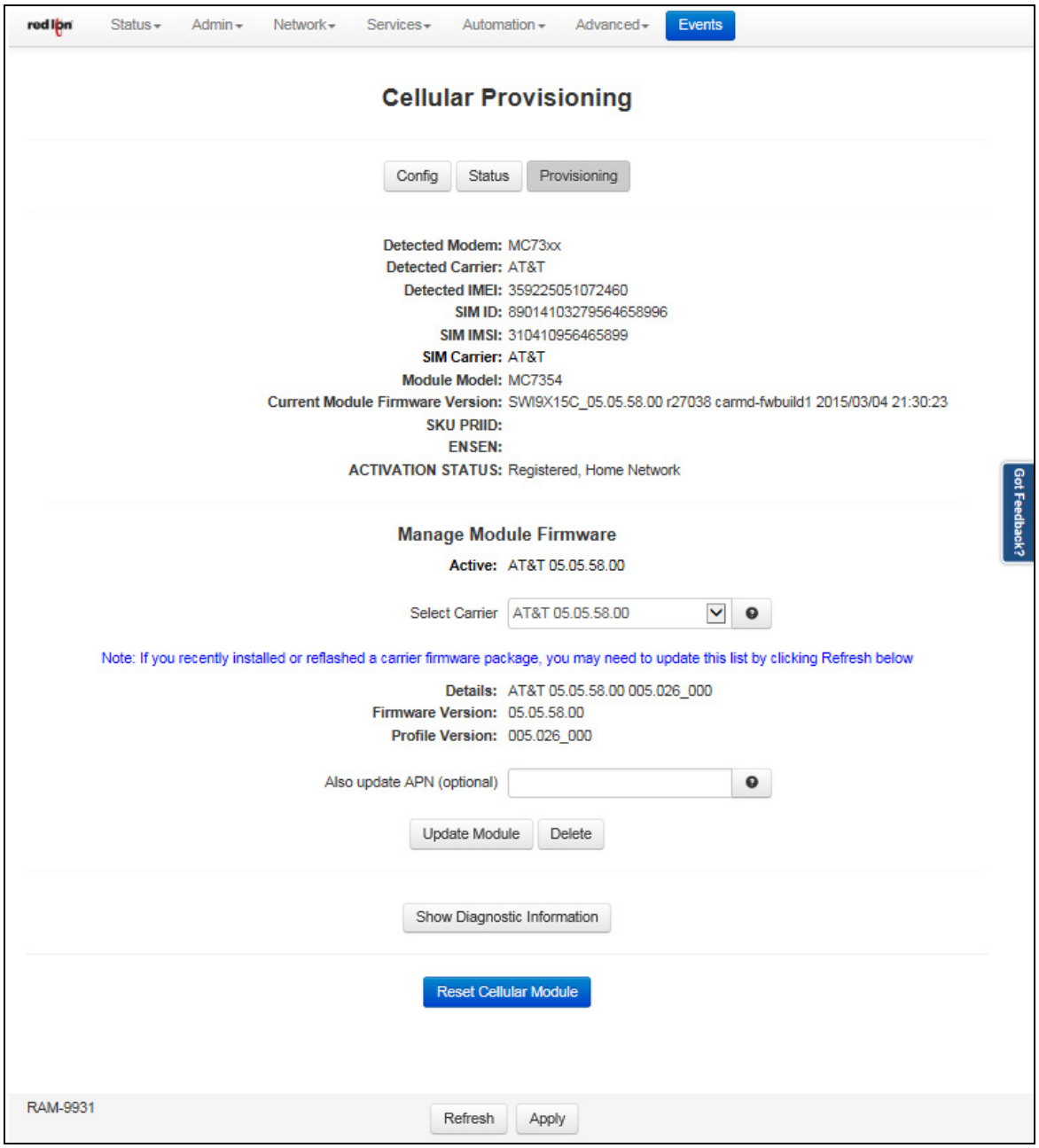
If you are using a GPRS, Edge or HSPA based card, enter the User Name, Password and APN that was provided by your cellular carrier. This information should have been packaged with your SIM chip. If you do not have this information, please contact your carrier's account representative or the carrier's support department before proceeding.

Click the *Apply* button to save and activate the configuration.

Note: The User Name, Password and APN can be case sensitive. Be certain that you use the exact information as provided by your carrier.

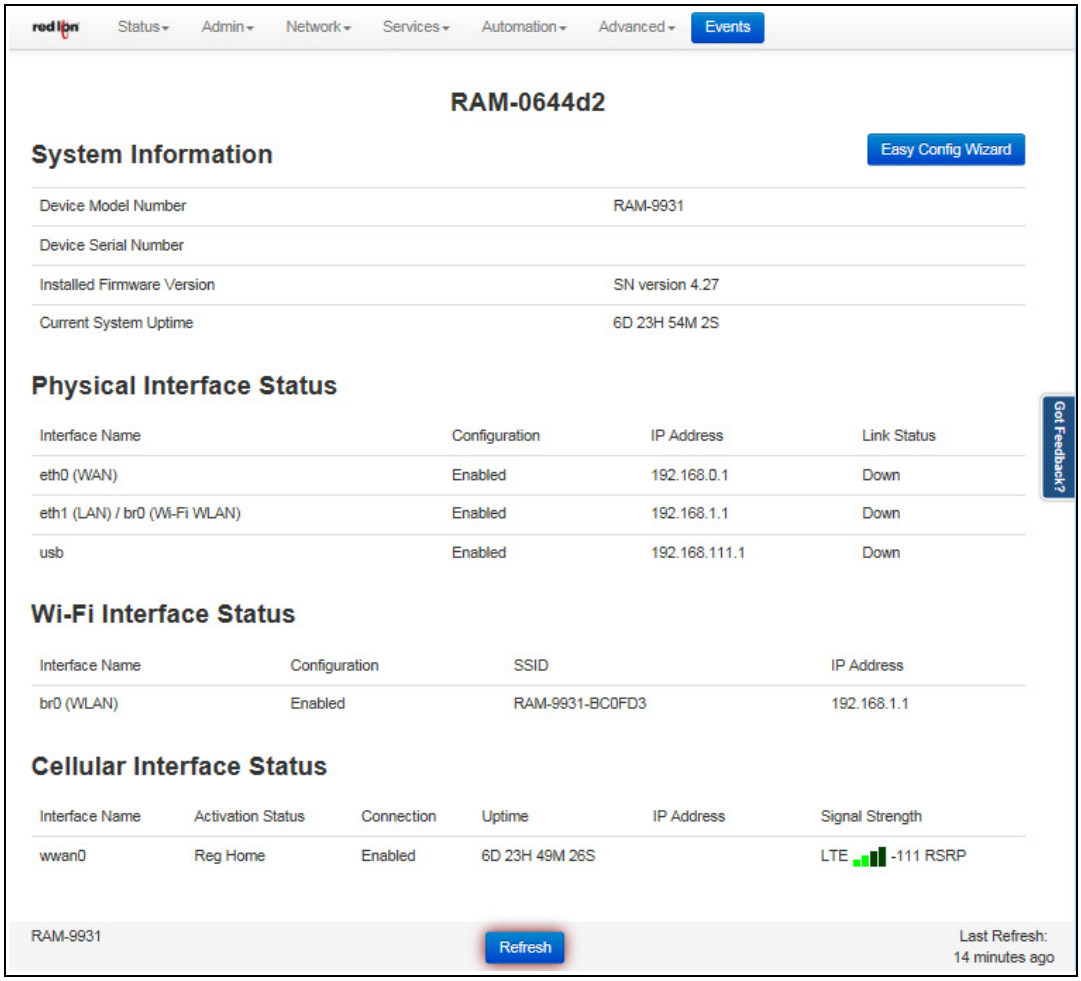
2.1.3 Provisioning

Provisioning should be used on SN/RAM 66xx devices to activate your CDMA based service. Examples of CDMA based 3G carriers are Verizon, Sprint, Bell, Telus and US Cellular. For SN/RAM 69xx and RAM 99xx devices that are able to switch between carriers this page is used to select the correct carrier profile and firmware images for the cellular module to authenticate on the LTE carrier networks. Contact Technical Support for the latest update package for your carrier if you are using one of these models. Navigate to Network → Cellular Connection → Provisioning.



2.1.4 Verify Cellular Connectivity

Browse to the Status screen by selecting Summary → Status. The following dialog window appears:



As shown, the RTU or router is receiving good signal from the cellular network, it is connected and has been issued an IP address.

At this point, if you previously verified that the SIM/Module is activated and have been accessing the web UI to configure your Red Lion interface via it's browser, then you should be able to access the Internet.

Open a browser on the PC/Laptop, and attempt to browse the Internet.

Note: Depending on the provisioning of your module/SIM, particularly in corporate applications in which the unit is providing cellular backup connectivity to wired circuits, your module/SIM may be restricted from Internet access. If this is the case, you may want to test to ensure that you are able to access your corporate network. If you have any questions about your configuration, please check with your network administrator.

If you were able to successfully access the Internet, or your corporate network, your Red Lion unit is up and running. You have successfully completed the Quick Start and you may skip the troubleshooting section.

2.1.5 Cellular Connectivity Troubleshooting

Note: If you were unable to access the Internet, or your corporate network, the section that follows will help you to determine the cause of your difficulties.

If you are reading this section, you have followed all previous instructions and your Red Lion RTU or router is not communicating, this section will provide additional information to isolate the cause of difficulties.

Cellular Reception

Before we get into specifics regarding how to identify and address specific problems that can be encountered, it is important that we spend a moment talking about cellular signal reception, and appropriate expectations.

All of the major cellular carriers expend significant sums insuring that we have excellent signal coverage within their coverage areas. However, they have no control over the environments in which we attempt to place or use our cellular devices.

The principles behind cellular data reception are similar to cellular phone reception. Therefore, our environment has the potential to significantly impact our ability to receive a good quality cellular signal.

You should be aware that it is possible to stand in the parking lot of a building and have perfect reception, but walk just 10 feet inside a concrete and steel building and have absolutely no reception at all.

The important thing to understand is that in many, many instances it is not the cellular network that causes reception problems, but the environment in which we place our cellular devices.

Important Note about Cellular Antennas

For this reason, Red Lion strongly recommends the use of external antennas when deploying cellular devices. It is often the key to a successful implementation. Consult your Red Lion representative if you have questions about the appropriate use of external antennas.

Diversity/MIMO

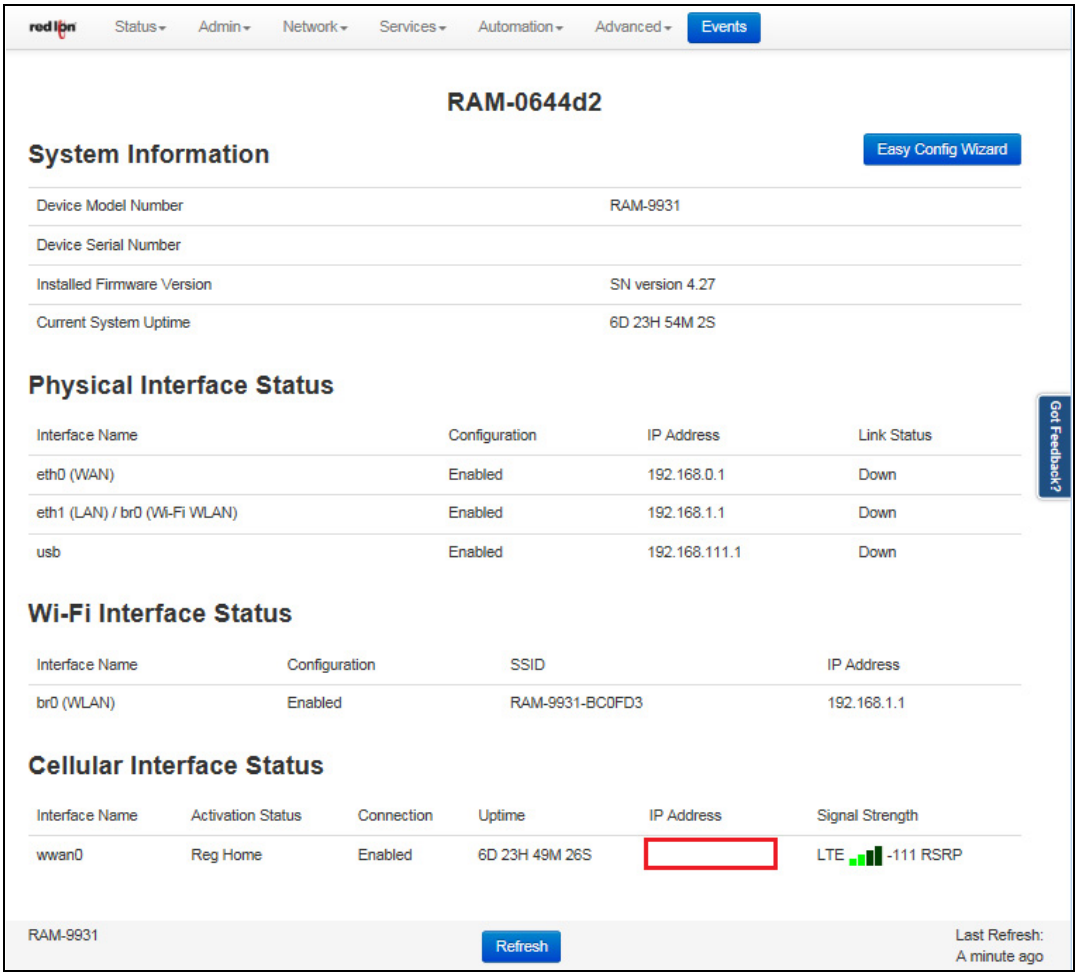
This port is used for RX diversity on 3G connections and MIMO for LTE connections. Receive Diversity or MIMO is a transmission technique that consists of using two separate antennas to achieve the most robust cellular signal possible. Diversity will help achieve fast, reliable data throughput in applications that require a high amount of bandwidth. This antenna is not mandatory for 3G, however it is recommended and will improve throughput in low signal and fringe areas. This antenna is required for compliance with LTE MIMO operation.

To get the best performance, this second antenna should be placed at a minimum of 5/8 of a wave length away from the other antenna. Therefore, the minimum spacing for antennas in the 800 MHz frequency is 5/8 * 13.5” = 8.5”. The diversity antenna can be spaced further away than this, ideally in increments of 13.5”, 22”, 35”, etc. For a 1900 MHz only network, the optimal distance would be 5/8 * 6.2” = 4”. Orienting the antennas differently from one another may also improve performance, particularly when the antennas are close together.

Verifying IP Connectivity

First, check to make sure that your device is connecting to the cellular network and obtaining an IP address.

Navigate to the Web UI Status screen shown below:



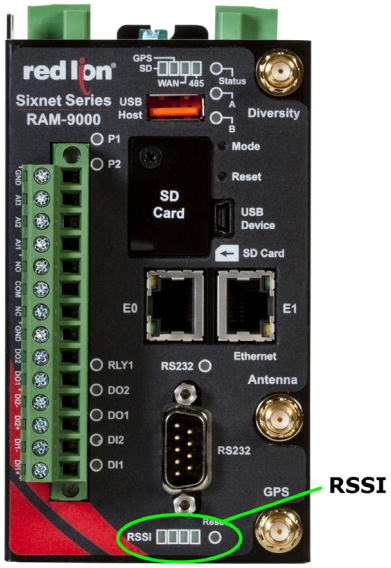
If the Signal Strength on your screen does not look similar to the one shown above, you may be having signal reception difficulties. You can further verify a low signal condition by examining the LED signal meter. See table below for Signal Strength details:

	Low Signal / No service
	≥ - 109 dBm (Low but valid signal)
	≥ - 99 dBm (Lower but valid signal)
	≥ - 89 dBm (Avg signal)
	≥ - 80 dBm (Excellent signal)

SN 6000 units: Observe the signal LED as shown below.

Signal	OFF	No signal available or signal strength is below -100 dBm
	ON	Excellent signal strength = greater than -69 dBm
	FLASH	Fast: Every 300ms = -79 to -70 dBm
		Medium: Every 600ms = -89 to -80 dBm
		Slow: Every 1200ms = -99 to -90 dBm

RAM 9000 units: Observe the RSSI LED as shown below.

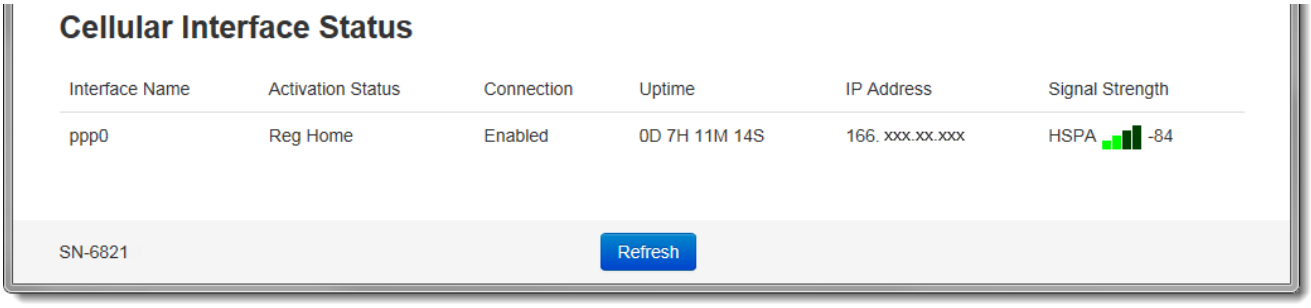


RSSI	RSSI	Low Signal / No service
	RSSI	≥ - 109 dBm (Low but valid signal)
	RSSI	≥ - 99 dBm (Lower but valid signal)
	RSSI	≥ - 89 dBm (Avg signal)
	RSSI	≥ - 80 dBm (Excellent signal)

Minimal Reception

On occasion, you can find yourself in a situation where you have just enough signal to be able to communicate with the cellular tower and obtain an IP address, but not enough reception to be able to sustain a viable connection.

If your cellular card is using dynamically assigned IP addresses, you can determine if you are in a situation like this by watching the “Cellular Interface” field from the Home screen (Summary → Status) as shown below:

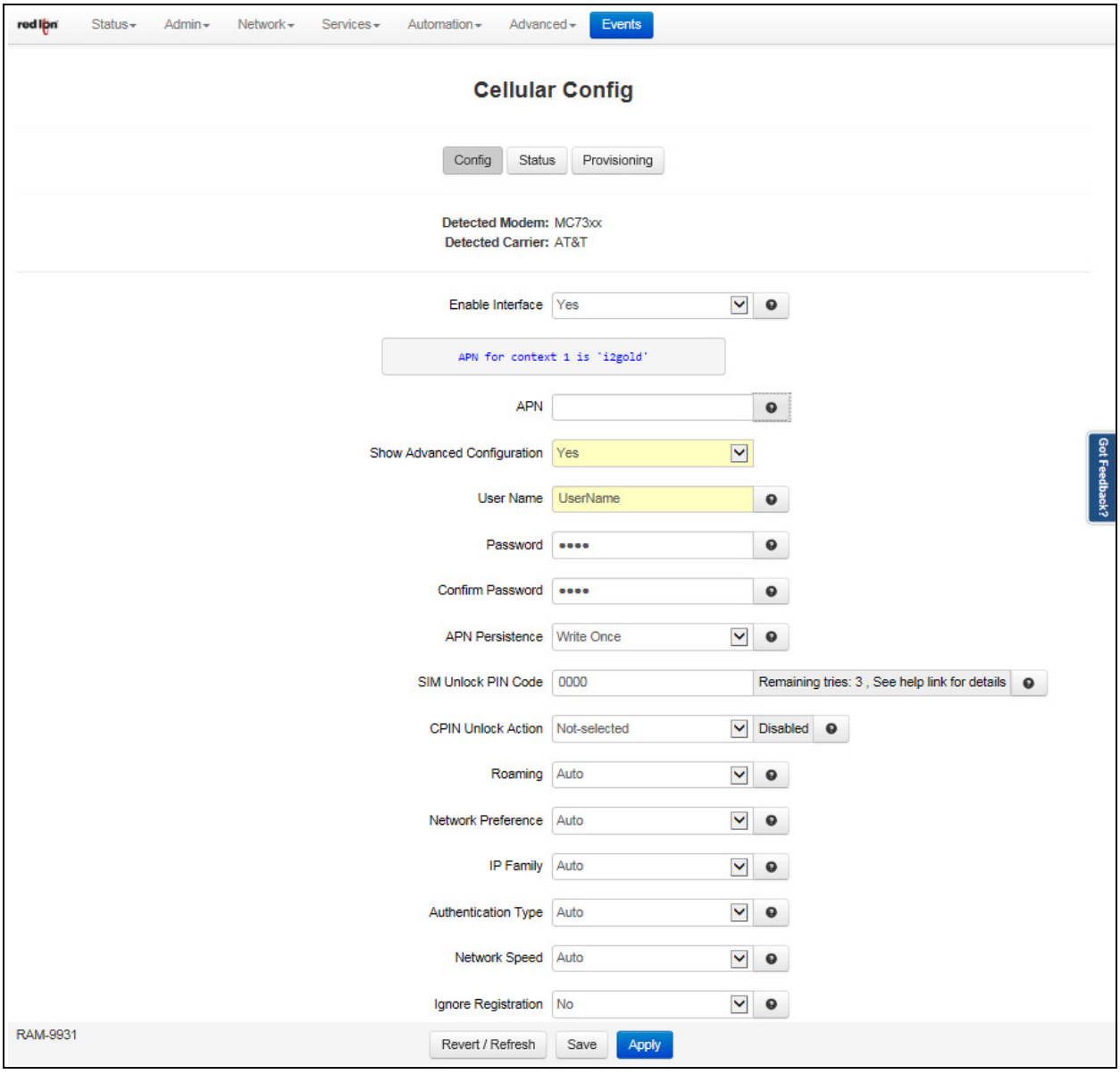


If you refresh this screen every few minutes and notice that the IP address is changing frequently, it is possible that the RTU or router is connecting to the network and obtaining an IP address and then the connection to the cellular network is being dropped. When the connection is re-established, the device is then issued a different IP address.

Authentication Issues

If you are using a GPRS/EDGE/HSDPA card, and have at least three LEDs of signal on the front panel signal meter, your radio connection to the network may be just fine. The problem may lie in logging onto the cellular network.

Navigate to the Cellular Connection dialog window (Network → Cellular Connection → Configuration)



Verify your user name, password, and APN information. All three of these items can be case-sensitive and must be entered exactly in order to properly log in to the cellular network.

Click on the *Save* button for changes to be saved without activating the interface, the *Apply* button will save your settings and apply them immediately. To revert to the previous settings, click on the *Revert* button.

Red Lion Technical Support

If you have followed all of the instructions up to this point, have satisfied yourself that you are not having an authentication problem, are convinced that you have sufficient reception, and your RTU or router is still not communicating, then please call Red Lion Technical Support at 1-877-432-9908. Live support is available from 8:00 a.m. - 5:30 p.m. EST. If you call after hours, please leave your contact information and a detailed description of your problem and we will respond to you the following business day. We will be happy to assist you in getting your RTU or router operational.

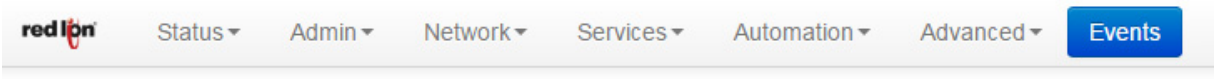
When submitting a support question, it is most helpful to have a GatherStats from the unit in question. Please obtain one from the Status → GatherStats screen. Choose the Download Option, and save the resulting file to your PC. You may attach it to an email to support@redlion.net, describing your issue.

Chapter 3 Web User Interface

3.1 Web User Interface Introduction

3.1.1 Organization

The Red Lion Web UI is comprised of six major sections. *(Click on a link to get an in-depth description of each topic)*



- Status: The Status tab presents information on the RTU or router. This tab is organized into six (6) sections: Summary, Easy Config, Network, Diagnostics, Syslog and Gather Stats.
- Admin: The Admin Tab is used to configure how the Red Lion RTU or router is accessed, update the firmware, reset the system defaults, set the system time and reboot the RTU or router remotely. This tab is organized into eight (8) sections: Access Settings, System Time, Certificate Manager, Firmware Update, Configuration Manager, Package Installation, Factory Defaults/Reboot and Job Control.
- Network: The Network Tab is used to configure settings that connect the RTU or router to external interfaces. The Network tab is organized into eight (8) major categories: Cellular Connections, Interfaces, Firewall, Tunneling, DNS Settings, Static Routes, DMNR/NEMO and TCP Global Settings.
- Services: The Services tab is used to configure the various features of the Red Lion RTU or router. These services include DHCP Server, DHCP Relay, Dynamic DNS, SN Proxy Settings, SixView Manager, GPS Settings, SSH/TELNET Server, SSL Connections, SNMP Agent, Ping Alive, Crimson Connect, Email Client, SMS Handling, RAMQTT Client, SD Card Manager and Serial IP.
- Automation: The Automation menu contains all aspects of managing your Modbus and DNP3 based I/O. The Autmation tab is organized into the following categories: Local Station, Serial Ports, Tags, Data Logger, Modbus, DNP3 and I/O Settings.
- Advanced: The Advanced Tab is used to configure the advanced features of the Red Lion RTU or router, which include IP Fallback, IP Transparency, Out-of-Band Management, VRRP, Expert Mode, GWLNX, Classic View and About.
- Events: Events are used to apply a series of logic checks to a register(s) that allows the user to program an action based on the content of a specific register.

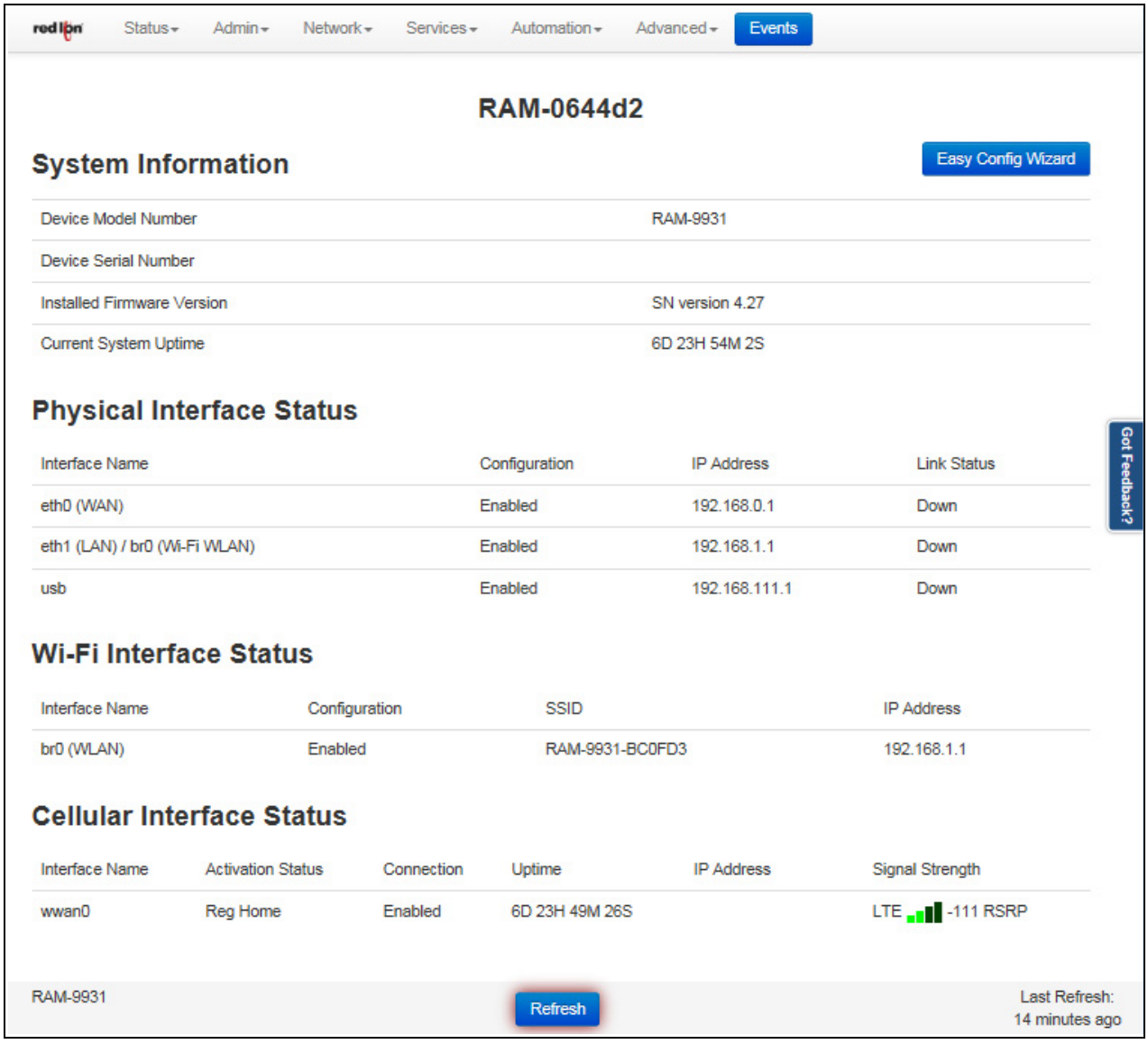
All tabs are described further in the manual along with the functionality of each dialog window.

3.2 Status Tab

The Status Tab allows you to review the state of the RTU or router functions, such as network connections, interfaces, system processes, services running, and system information. It also allows review of the syslog, update history, and under diagnostic tools, permits testing connectivity through the use of 'ping' and 'traceroute'.

3.2.1 Summary

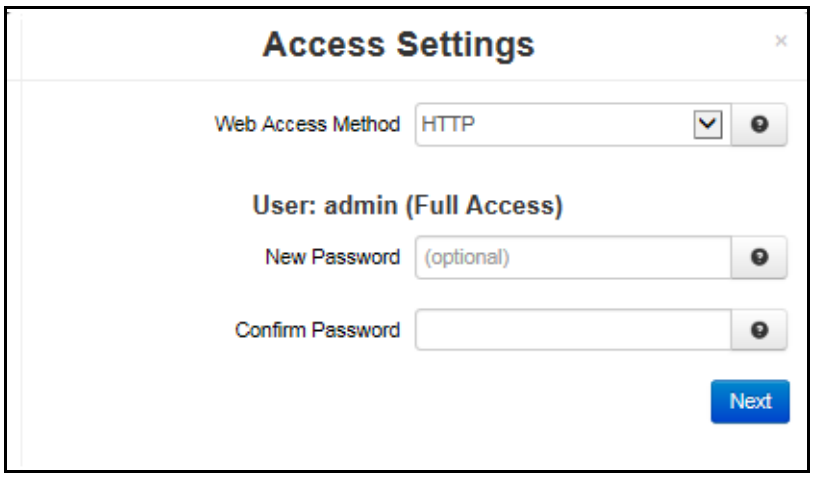
This option will return the user to the System Summary (home) page. On this page, the system information and physical interface status are easily viewed.



3.2.2 Easy Config Wizard

The Easy Config Wizard is used to setup your Ethernet IP without having to navigate through multiple dialog windows. The Easy Config Wizard is situated on the Summary page and accessed by clicking on the blue Easy Config Wizard button.

Click on the *Easy Config Wizard* button.The Access Settings dialog window will open:



Web Access Method: Select the method by which you would like to access the Web UI. You do not need to enter the password in order to change the access method.

> **Note:** The HTTP method can result in better performance and faster page load times; however, it is less secure than the HTTPS method, which uses data encryption to provide a secure connection.

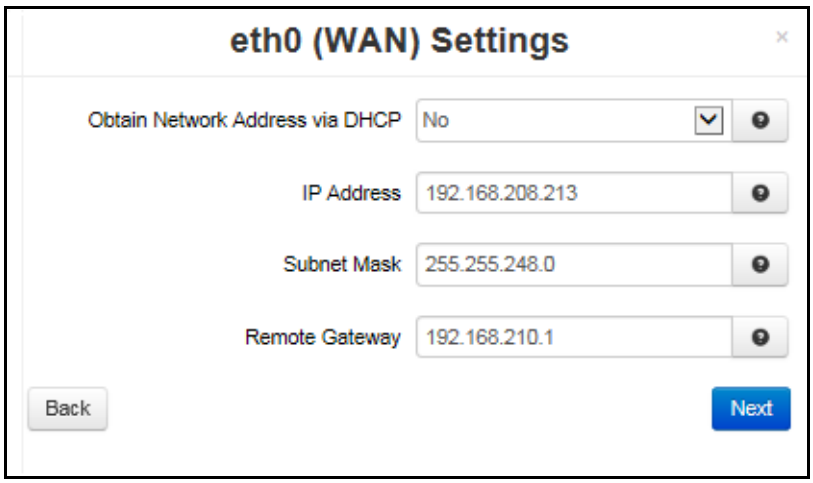
New Password: Enter the new password in this field.

> **Note:** Password Limitation, Single quote (‘) character is not a valid character for password.

Recommended Setting for a secure password, choose one that is at least six characters long, which is not a common word and comprised of a mixture of upper and lower characters and numbers.

Confirm Password: Enter your current password in this field (required).

Click on the *Next* button.The Eth0 (WAN) Settings dialog window will open:



Obtain Network Addresses via DHCP: Select *Yes* to allow the interface to obtain address information via a DHCP server. The device will obtain its IP address, netmask and remote gateway as the default route. It can also, optionally, obtain DNS server address via DHCP.

Select *No* to prevent the interface from obtaining address information via a DHCP servers.

You will be required to enter the IP address, netmask and remote gateway addresses. DNS information can be provided by navigating to the Network>DNS Settings menu.

IP Address (Required): Enter the desired interface IP address. This field is only available when the "Obtain Network Addresses via DHCP" is set to *No*.

The IP address identifies a device on a TCP/IP network. Every device on a network must have a unique address. The range of valid addresses for a given network is determined by the value of the Netmask. Some addresses are reserved for special uses such as network and broadcast.

For example, if a netmask is 255.255.255.0, the assigned IP address must be within the range of 192.168.1.1 to 192.168.1.254 as 192.168.1.255 is reserved as the broadcast address.

> **Recommended Setting:** This address should have been provided by your Network Administrator. It must be an address valid for the network described by the value contained in the Subnet Mask field and must not conflict with any other device on the target network.

Subnet Mask (Required): Enter the desired interface IP address into this field. This field is only available when "Obtain Network Addresses via DHCP" has been set to *No*.

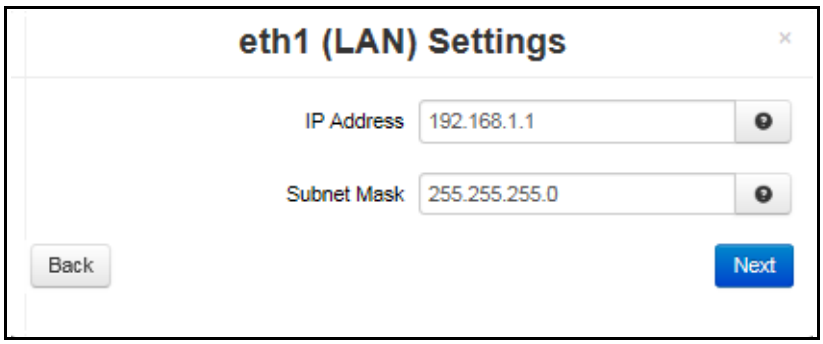
> **Recommended Setting:** Your network administrator should be able to provide an appropriate value. This value determines the valid range of IP addresses allowed in the "Enter IP Address" field.

Remote Gateway: Enter the IP Address for the gateway device. This field is only available when "Obtain Network Addresses via DHCP" has been set to *No*.

A gateway is a device (typically a RTU or router) used to gain access to another network. For example, if a device is attached to a LAN whose network address is 192.168.1.0 with a netmask of 255.255.255.0, then it can communicate directly with any other device on that network with a range of addresses of 192.168.1.1 through 192.168.1.254 (with 192.168.1.255 reserved for broadcast). An address outside of that range is on a different network which would need to be accessed indirectly through a RTU or router. That RTU or router would be the gateway to the network on which the remote target device resides. In order to communicate with it, it would mean sending and receiving via the gateway device. This also requires either defining a static route (defined through the Network>Static Routes menu) via that gateway or making it the default route by setting "Use Remote Gateway as Default Route" to *Yes*.

Recommended Setting: Your network administrator should be able to provide an appropriate value. The address must be one within the valid range for the network.

Once the desired settings have been entered in the Eth0 (WAN) Settings dialog window, click on the *Next* button and the following eth1 (LAN) Settings dialog window appears:



IP Address (Required): Enter the desired interface IP address into this field. This field is only available when the "Obtain Network Addresses via DHCP" is set to *No*.

The IP address identifies a device on a TCP/IP network. Every device on a network must have a unique address. The range of valid addresses for a given network is determined by the value of the Netmask. Some addresses are reserved for special uses such as network and broadcast.

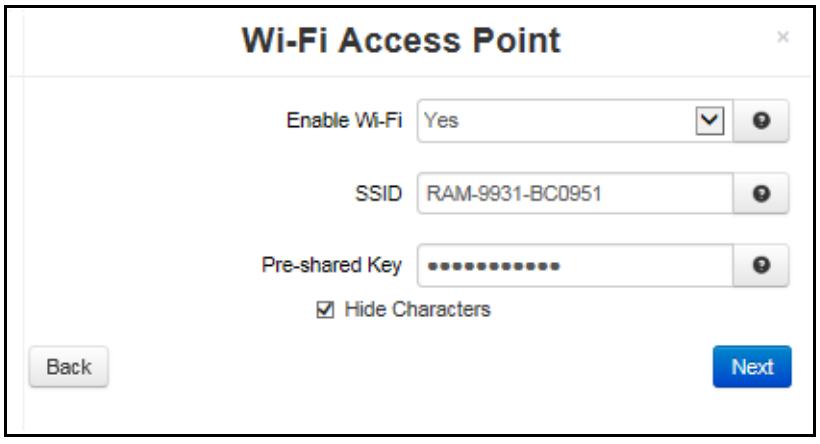
For example, if a netmask is 255.255.255.0, the assigned IP address must be within the range of 192.168.1.1 to 192.168.1.254 as 192.168.1.255 is reserved as the broadcast address.

Recommended Setting: This address should have been provided by your Network Administrator. It must be an address valid for the network described by the value contained in the Subnet Mask field and must not conflict with any other device on the target network.

Subnet Mask (Required): Enter the desired interface IP address into this field. This field is only available when "Obtain Network Addresses via DHCP" has been set to *No*.

Recommended Setting: Your network administrator should be able to provide an appropriate value. This value determines the valid range of IP addresses allowed in the "Enter IP Address" field.

Once the desired settings have been entered in the Eth1 (LAN) Settings dialog window, click on the *Next* button and the following Wi-Fi Access Point dialog window appears:



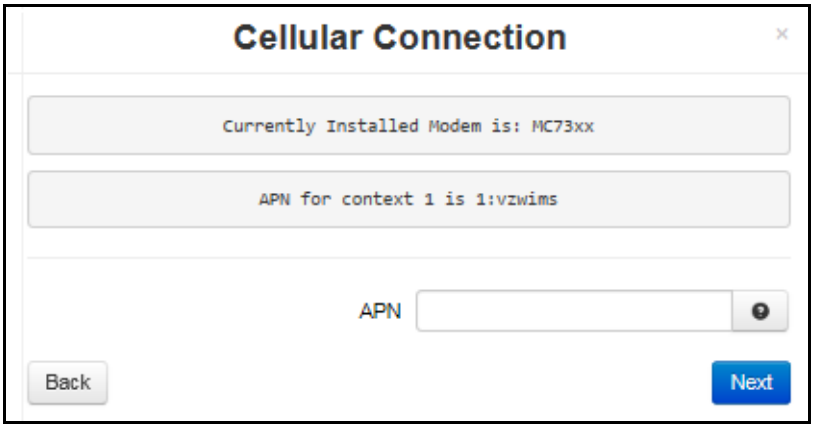
Enable Wi-Fi: Select YES to configure the parameters for wireless LAN clients which may connect to your Access Point. You may change wireless encryption settings as well as wireless network parameters.

SSID: The SSID is a unique name for your wireless network. It is case sensitive and must not exceed 32 characters. All wireless devices in your network must use the same SSID.

Pre-shared Key: This option is available when **WPA** types are selected as an option for **Encryption** and allow the user to specify the encryption key to be used. For WPA, this should be a pass phrase of 8-63 printable ASCII characters. This option allows the sender and recipient to share a secret key.

Note: The following six characters are not supported: ( ) ` ' " =

Once the desired settings have been entered in the Wi-Fi Access Point dialog window, click on the *Next* button and the following Cellular Connection dialog window appears:

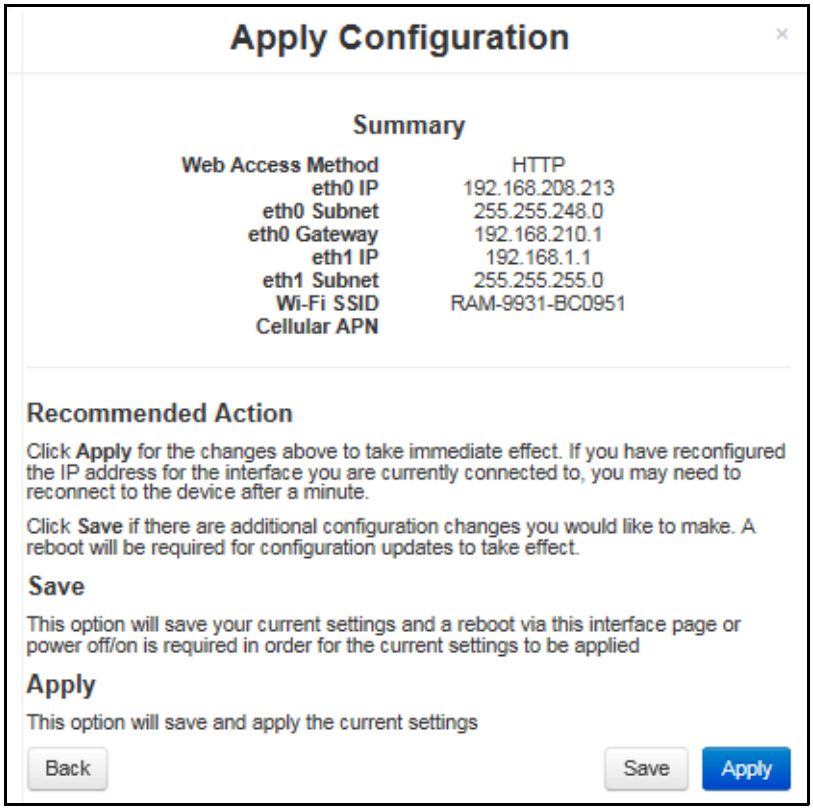


APN (Optional): Enter the APN used to access your cellular wireless data service in this field. This information should have been given to you by your service provider when service was established.

Note: Maximum allowable characters for this field are 104 characters.

Note: Entering an APN value in this field will overwrite any APN stored in the modem for the selected context.

Once the desired settings have been entered, click on the *Next* button and a Apply Configuration dialog window appears.



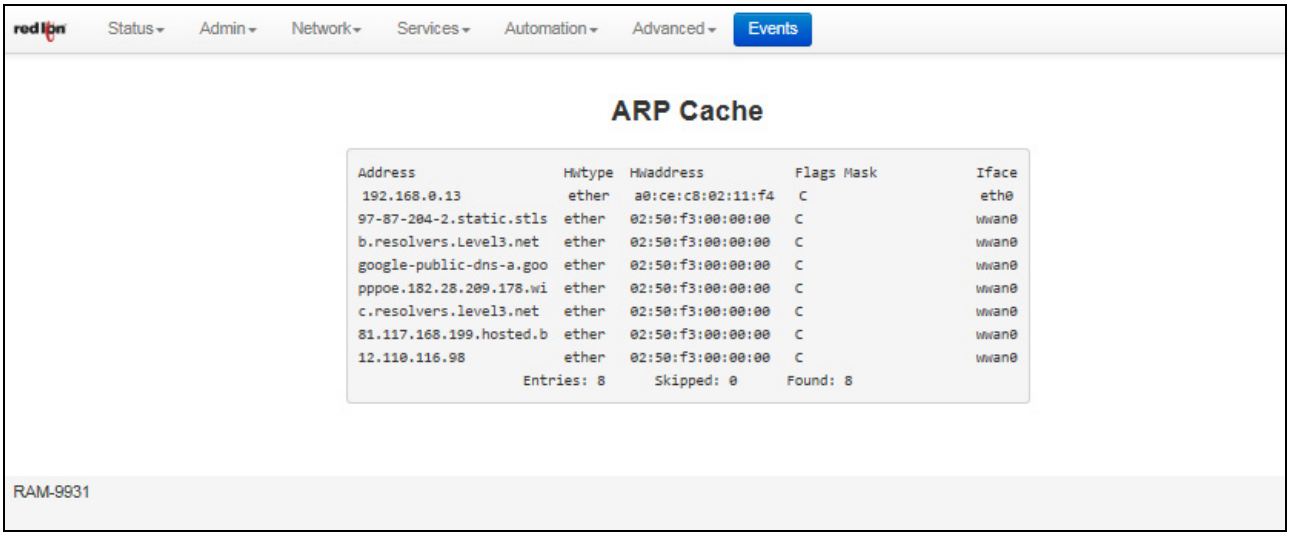
Click on *Back*, *Save* or *Apply* (*see explanation of each setting in dialog window above*).

3.2.3 Network

The Network menu contains the following sub-menus: Arp Cache, Firewall Rules, Interfaces, Routing Tables, Socket Statuses and Traffic.

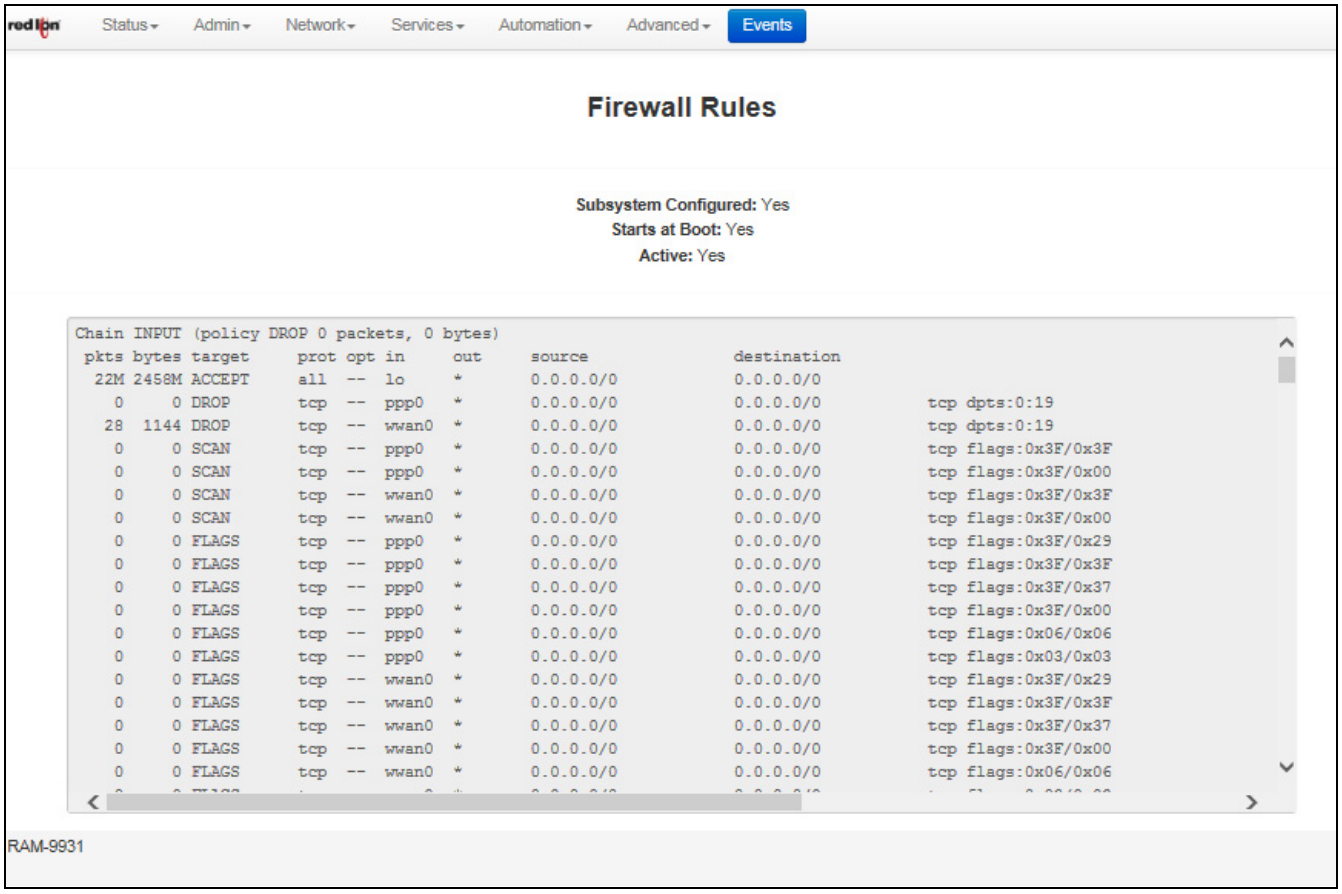
ARP Cache

The ARP Cache is a table which stores mappings between Data Link Layer (OSI Layer 2) addresses and Network Layer (OSI Layer 3) addresses. This important information shows what connections are established to the RTU or router. When you click on the ARP Cache menu item, the ARP Cache dialog window will open.



Firewall Rules

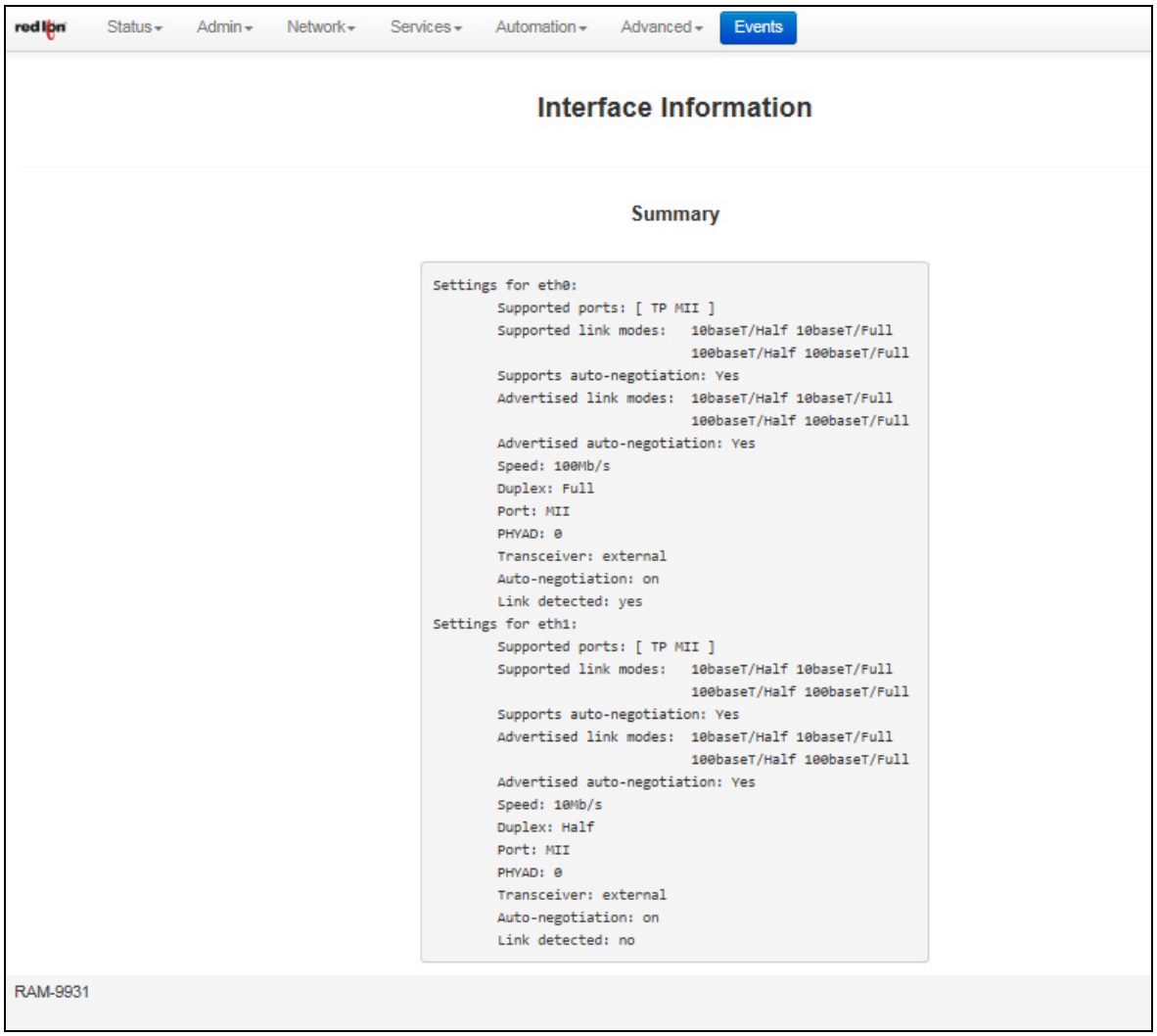
The Firewall Rules menu item displays a complete listing of the rules used within the firewall for the Red Lion RTU or router. If you are familiar with Linux and IPTables, this will be of great use.



Scroll through the list of rules to review the entire IPTABLES listing. This information is used to track traffic being allowed and traffic being denied access to and through the Red Lion RTU or router.

Interfaces

The Interfaces dialog window is divided into three sections. Summary, Details and Multicast.



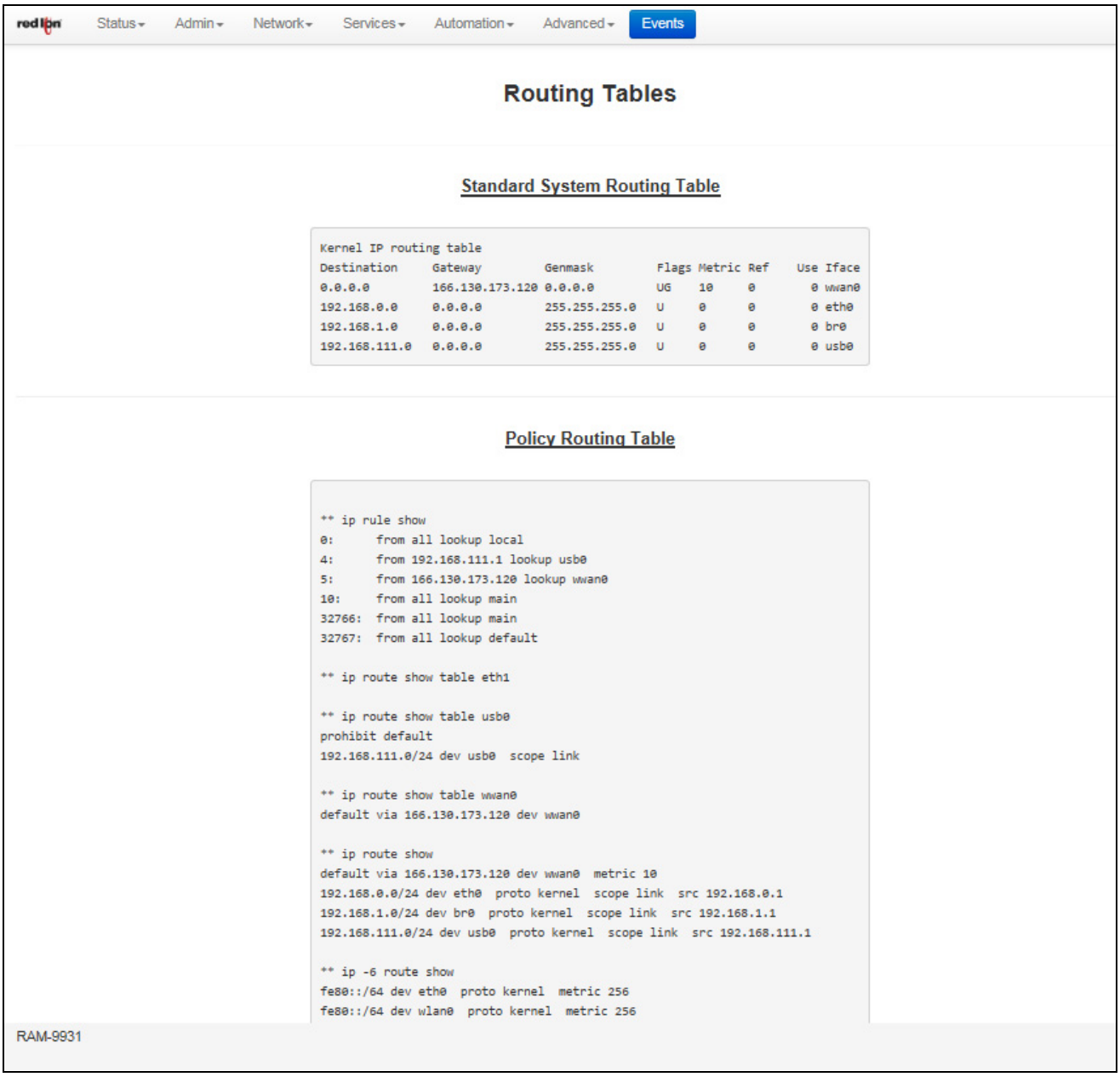
The Summary table displays a brief description of the interfaces of the Red Lion RTU or router.

The Details table displays a system specific description of the interfaces on the Red Lion RTU or router.

The Multicast table displays the current multicast settings for various interfaces.

Routing Tables

The Routing Tables dialog window contains both the Standard System Routing Table and the Policy Routing Table.



The Standard System Routing Table displays the current routes for the Red Lion RTU or router and the static routes that have been configured for the RTU or router.

The Policy Routing Table displays information on the policy rules, the route tables for each individual interface and the general routes for the Red Lion RTU or router.

Socket Statuses

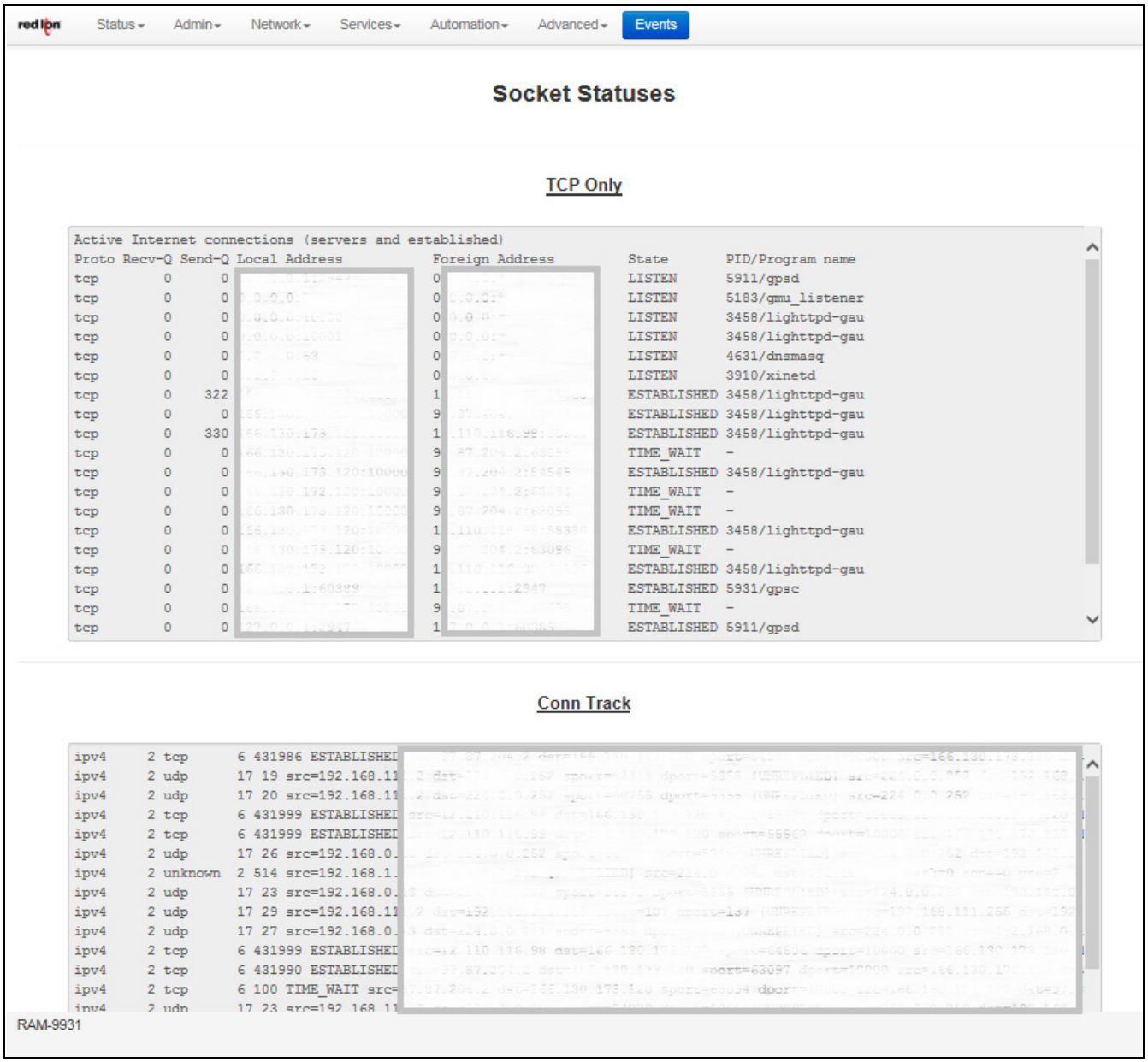
Sockets are end-points to communication over the Internet. Much like PBX phone systems, where the IP address is the phone number and the port is the extension. Every paired (connected) socket has a source IP/port and a destination IP/port.

There are three tables in the Socket Statuses dialog window: TCP Only, Conn Track and Socket Statuses All.

The TCP Only table displays the sockets that are connection-oriented (Also known as stream sockets).

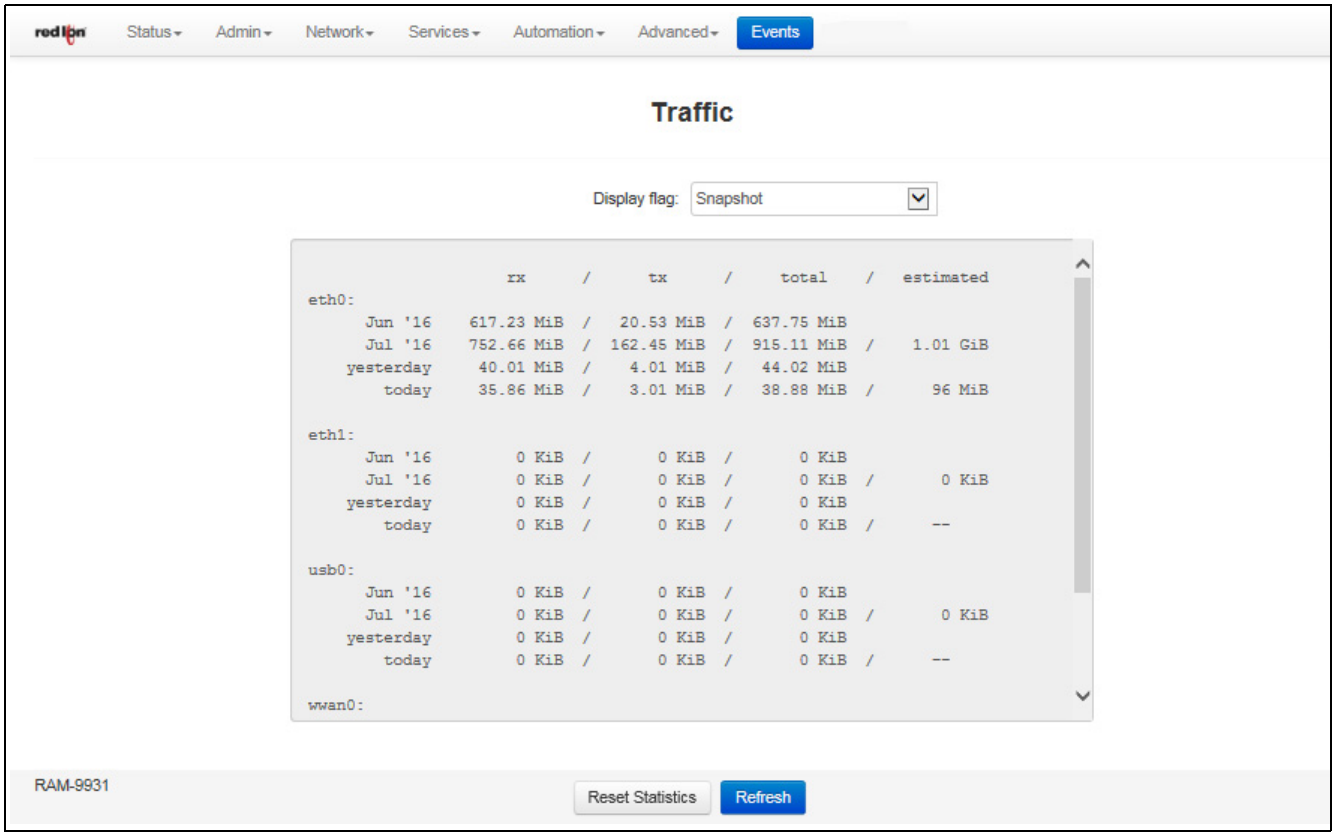
Conn Track is a connection tracker that displays more thorough information about the current socket connections. Connection tracking allows the kernel to keep track of all logical network connections or sessions, and thereby relate all of the packets which may make up that connection. NAT relies on this information to translate all related packets in the same way, and IPTABLES can use this information to act as a stateful firewall.

The Socket Statuses All table displays the sockets that are considered connection-oriented and connectionless (also known as datagram sockets).



Traffic

The Traffic dialog window shows the unit's traffic history. From the Display Flag drop-down list, select which information is desired and which Interface is to be viewed. The information will then be shown in the dialog window.

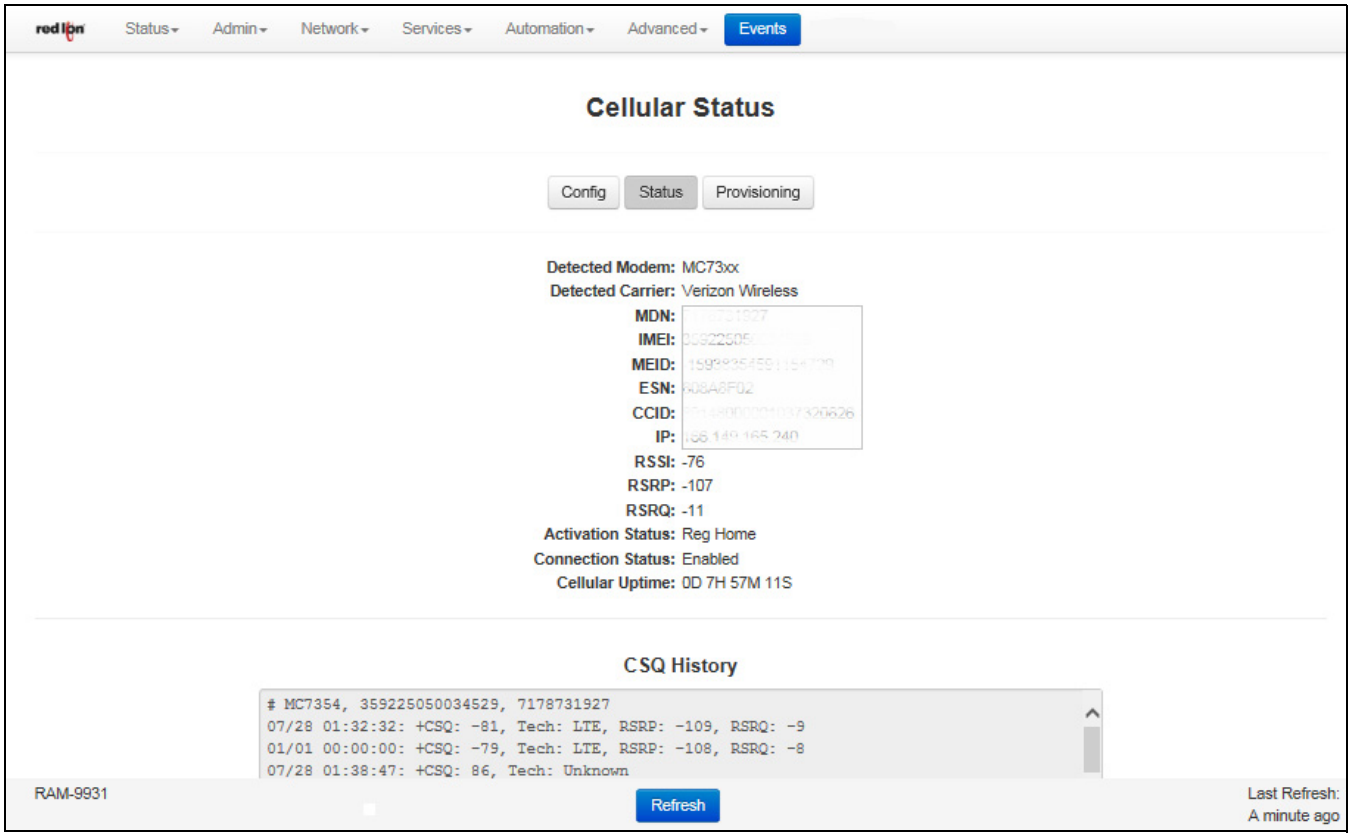


3.2.4 Diagnostics

The Diagnostics menu is sub-sectioned into Cellular Status, Ping, Traffic Capture, Socket Test, Traceroute and System Info sub menus. This information is useful in troubleshooting connectivity between the Red Lion RTU or router and the Internet or Network connection.

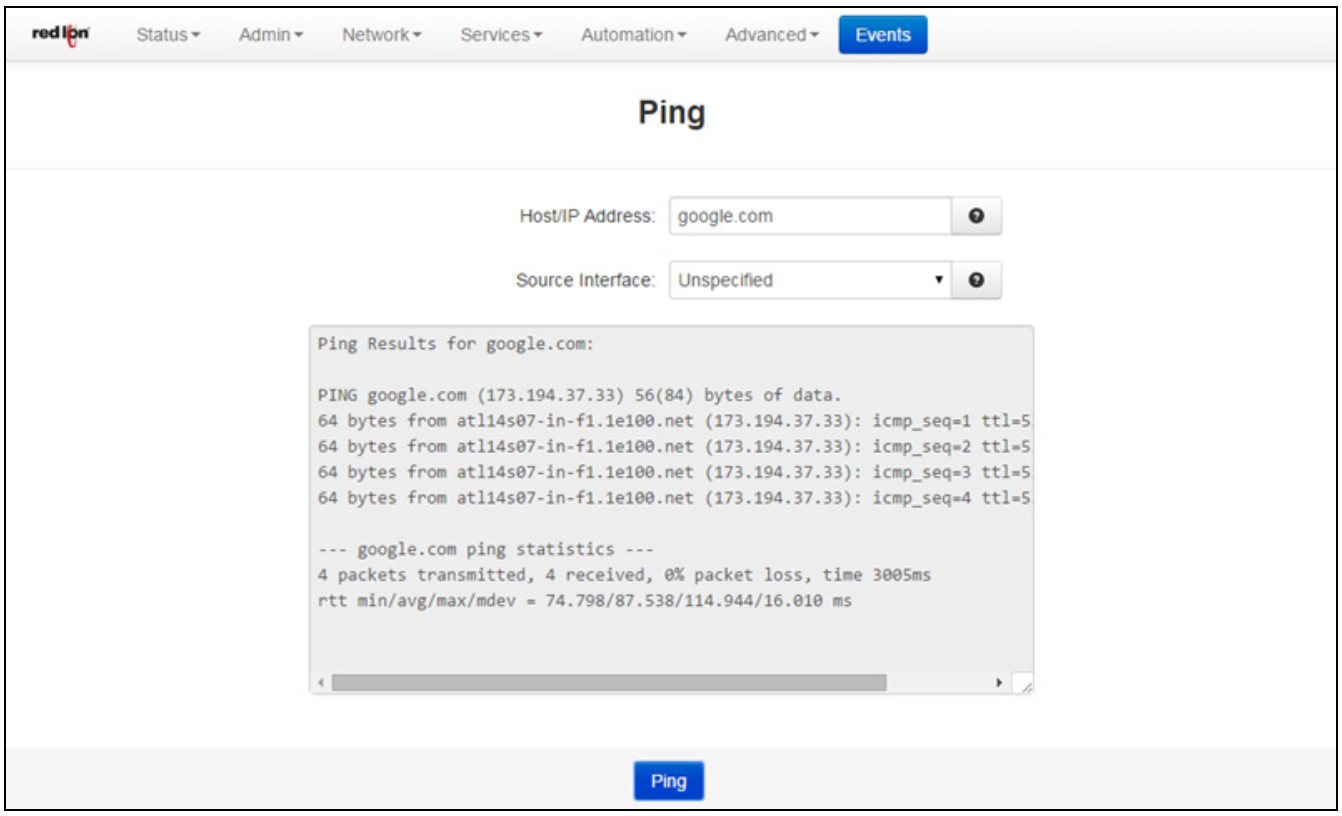
Cellular Status

The Status menu item brings up a dialog window displaying the status of the cellular connection. From here, you can get information such as the type of modem, carrier, MDN, IMEI, ESN, CCID (SIMID), IP, RSSI, RSRP, RSRQ, Activation Status, Connection Status, Cellular Uptime, CSQ History and Card Stats.



Ping

The Ping menu item allows you to input an address either as an IP Address or a URL for testing the availability of the defined destination.



Host/IP Address field: Type in the IP Address or URL you wish to Ping. It is recommended you start with a locally accessible IP address to confirm communication to an interface's local subnet. Then proceed to addresses on distant networks. Your local default gateway is a good test, and this IP can be found in the your routing table. Also, a commonly available internet server available to test against is 4.2.2.2

Source Interface: The Source Interface offers the option of using different interfaces to send the Ping through. This is useful if you have a VPN Tunnel in place. Testing the connection through the VPN Tunnel is required to verify connectivity through the tunnel.

Choose the interface that the VPN Tunnel has listed for the Local Subnet end-point, i.e. if the Left Subnet is 10.100.100.0/24 and eth1 has 10.100.100.1 as its IP Address, then choose Source Interface eth1.

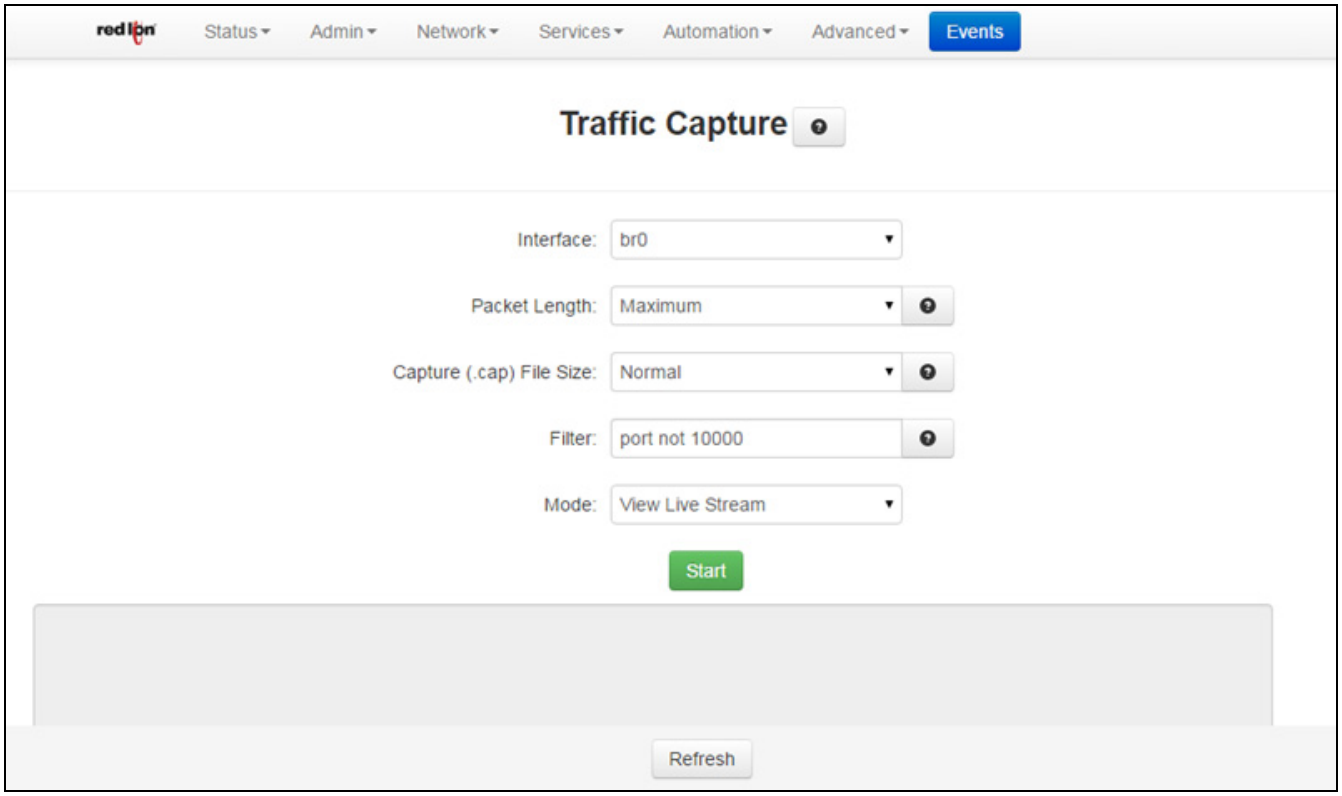
Specify a Host/IP Address at the head-end to Ping through the tunnel.

Click on the *Ping* button to see the result.

Traffic Capture

Traffic Capture uses the tool *tcpdump* to perform network traffic captures and generate a widely compatible .cap file.

A series of rotating capture files will be generated to prevent exhausting local resources and all may be downloaded for post-capture analysis in the viewer of your choice. Capturing the most relevant information may require trial and error to obtain the best filter for specific investigations.



Interface: Select which interface is to be used to generate the capture file.

Packet Length: Select which type of packet to be created. The recommended setting for this option is *Truncated* unless a deep packet inspection is required.

Truncated: If this option is selected, the packet headers and the first few bytes of the start of the data packet will be included. Use this option to trace network and connection behavior.

Maximum: If *Maximum* is selected, the entire packet, with its contents, will be captured. Use this option to investigate the contents of the data exchange, such as Serial IP packets.

Capture (.cap) File Size: Cap files are generated on a rotating basis. This sets the maximum size for each of three individual files. The recommended setting for this field is *Normal* to ensure a minimal amount of system resources are used.

Normal: 1 Megabyte

Large: 3 Megabytes

Maximum: 1/6 system memory

Filter: Create filters by typing the options listed below. The recommended setting for this field is *port not 10000*.

To ignore browser traffic while capturing: *port not 10000*

To ignore traffic to/from a specific host: *host not 192.168.1.2*

To capture only traffic from a specific port: *port 1234*

To combine these filters use: *host not 192.168.1.2 and port 1234*

Mode: Select whether you want to generate a capture file or view the live stream of the network traffic.

Socket Test

The Socket Test menu will allow you to "Telnet" to the desired destination IP and Port addresses to verify the socket availability.

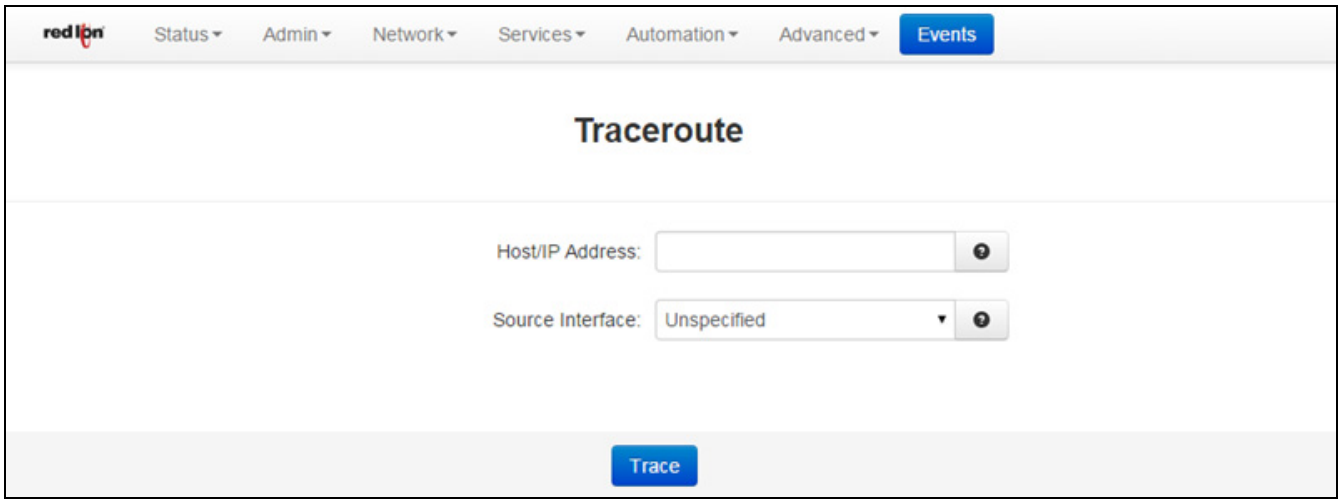
Host/IP Address field: Enter the IP Address or URL you wish to connect to via Telnet.

Destination Port field: Enter the Destination port of the server to which you would like to connect.

Click on the *Test* button at the bottom of the dialog window to proceed with the TCP socket test to verify socket availability.

Traceroute

The Traceroute menu item allows you to watch the route taken through the Internet to the specified IP Address or URL.



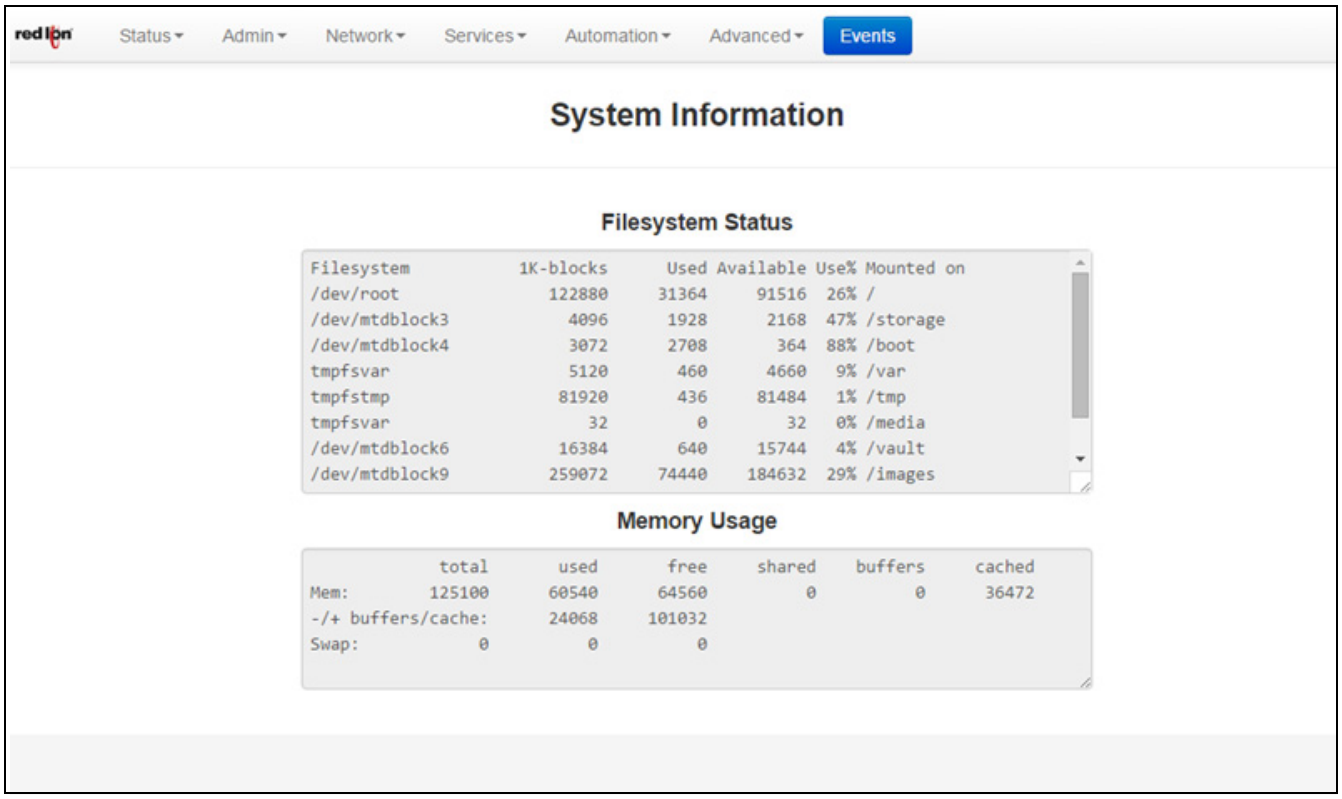
Host/IP Address field: Enter the IP Address or domain name (if DNS enabled) you wish to trace. It is recommended to start with a locally accessible IP address to confirm communications to an interface's local subnet. Then proceed to addresses on distant networks. You local default gateway is a good test, and this IP can be found in your routing table. A commonly available Internet server available to test against is 4.2.2.2.

Source Interface field: Select the interface to be used from which to originate the Traceroute test. The recommended setting for this field is "Unspecified", as it will let the system choose the first interface found with a route to the destination.

Click on the *Trace* button at the bottom of the dialog window and a table describing the Trace Route results appears in the dialog window.

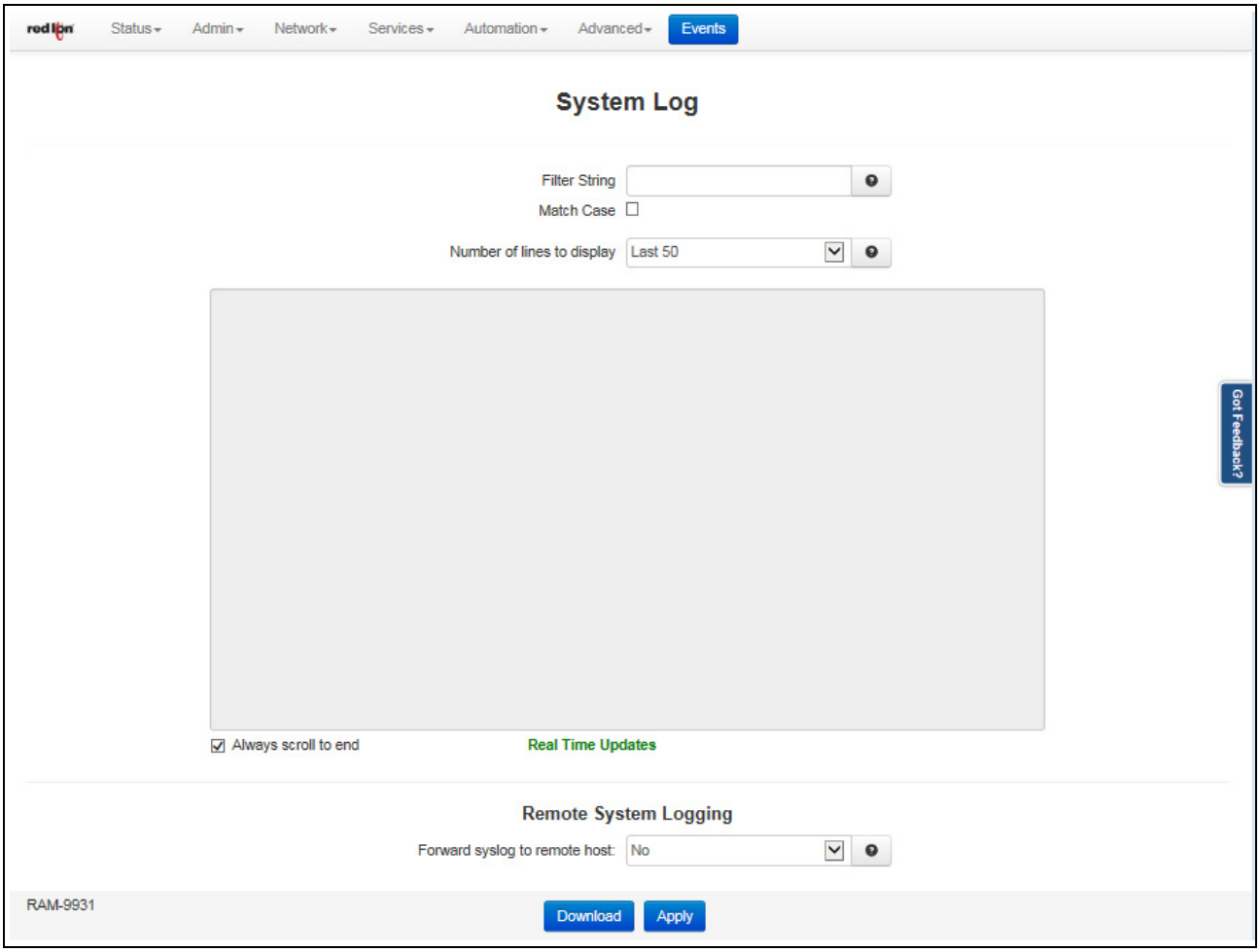
System Info

The System Info menu item will display the current usage of the file system in both the directory size and the memory utilization.



3.2.5 Syslog

The Syslog window will display the current syslog of the Red Lion RTU or router.



Customize your search by configuring the following fields:

Filter String (optional): Enter a filter string in the space provided. Only lines containing the filter value(s) will be displayed via a grep (Global Regular Expression Parser) style filter mechanism.

Match Case: Check this box if you want the Filter String field to be case sensitive.

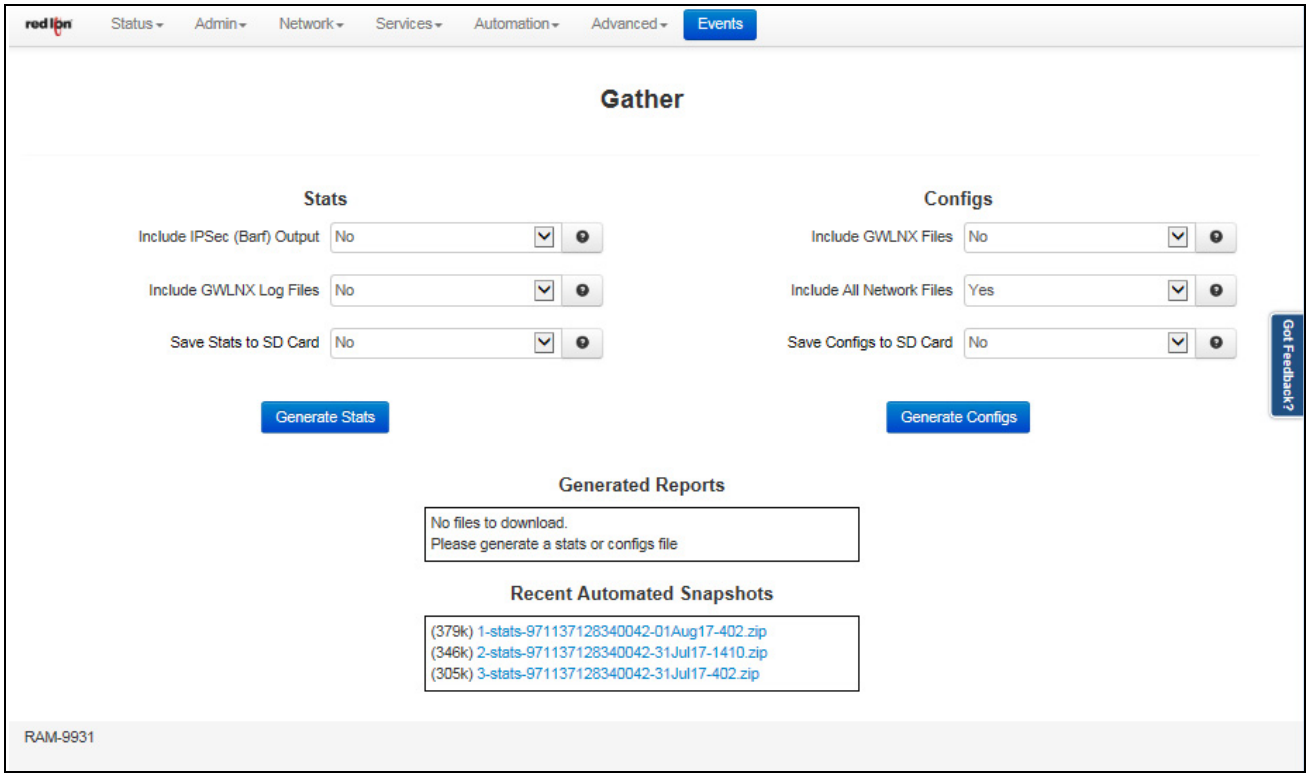
Number of lines to display: Select the number of lines to be displayed from one of the choices in the drop-down list provided.

Forward syslog to remote host (Required): Select YES to enable forwarding of syslog messages to another host. The recommended setting for this field is NO.

Click on the *Download* button and a download window appears prompting whether to save or open the file. The download interface will be different depending on the browser used.

3.2.6 Gather Stats

The Gather Stats feature creates a collection of system log, configuration and status files for use as a troubleshooting tool when contacting Technical Support to research a reported issue. The device takes an automatic Gather Stats snapshot every night around 4AM and will rotate at three days of snapshots.



Include IPSec (Barf) Output: Select YES to include all IPSec (Internet Protocol Security) debug information. The recommended setting for this field is YES if a VPN connection is used on this unit.

Include GWLNX Log Files: Select YES to include all GWLNX related logs. Choose YES for this option if you are running GWLNX for protocol conversion. Be aware that this will increase the size of the resulting .zip file.

Include GWLNX Files: Select YES to include all the GWLNX protocol conversion application file. Be aware that this will considerably increase the size of the resulting .zip file. Only choose YES for this option if directed by Technical Support, or if you have installed a custom GWLNX protocol engine.

Include All Network Files: Select YES to include all networking related configuration files. If using "gatherconfigs" to clone a unit, note that this option will cause the network interfaces (Including static IP addresses) to be cloned as well. If performing a gatherconfigs for review by Technical Support, please choose YES for this option.

Save Stats to SD Card: Select YES to save all Statistics to an SD card. This feature is only available on the RAM-9xxx series (6xxx does not have an SD Card, only 9xxx does).

Save Configs to SD Card: Select YES to save all Configuration data to an SD card. This feature is only available on the RAM-9xxx series (6xxx does not have an SD Card, only 9xxx does).

To create the files for the Stats and/or Configs, click on the **Generate Stats** and/or **Generate Configs** buttons. The newly generated file will be shown in the Generated Reports table while the Recent Automated Snapshots table will list previously generated files.

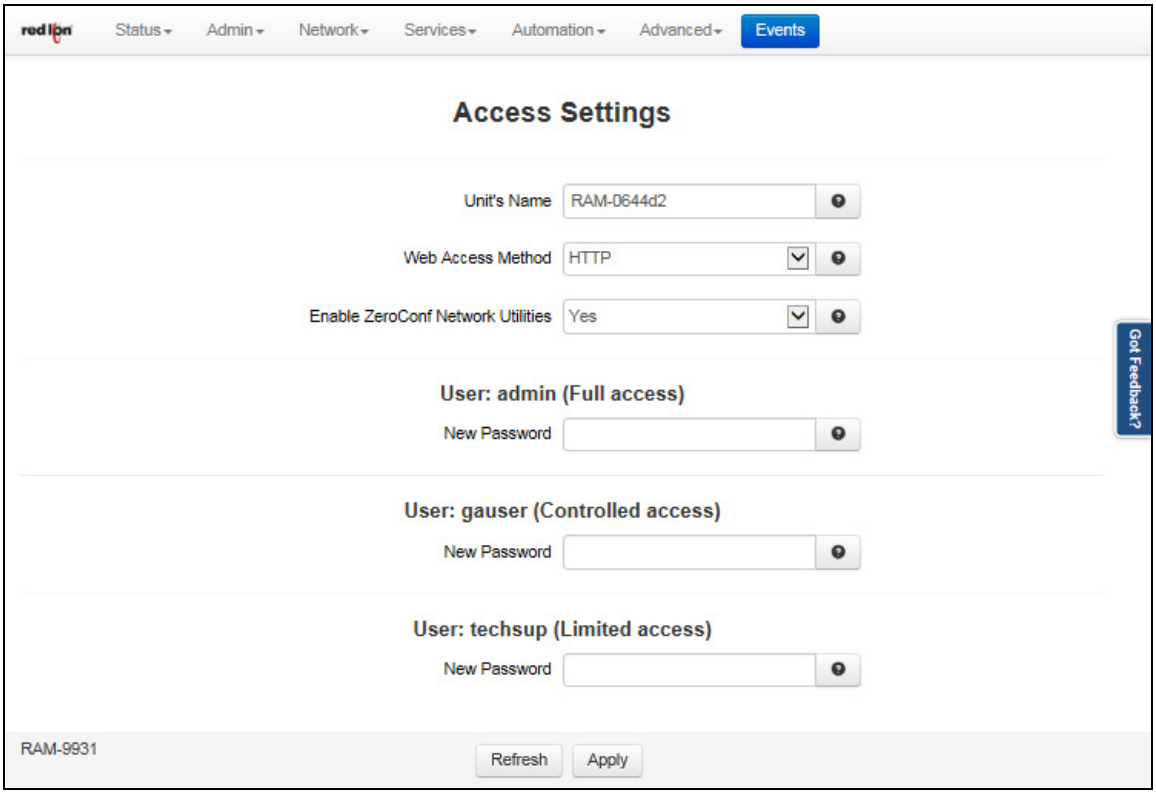
3.3 Admin Tab

The Admin Tab is where you configure web access methods, manage SSL/IPSec certificates, set passwords, update firmware, manage configurations and set factory defaults.

3.3.1 Access Settings

The Access Settings menu item allows you to change how the unit's Web UI is accessed, either by HTTP, HTTPS or HTTPS/redirect. You can also change the passwords used to access the Web User Interface. For security purposes, it is recommended that the admin password be changed according to your internal policies.

Click on the *Access Settings* menu item and the following window appears.



Unit's Name: Enter a description to identify the unit. This field is not required to support functionality. It is only for unit identification. This information appears on the Summary screen when logging into the device.

Note: Maximum length of this field is 32 and supported characters are alphanumeric plus the following special characters.: + -._

Recommended Setting: Optional

Web Access Method: Select the method you would like to use to access the Web UI. You do not need to enter the password in order to change the access method. Use the HTTPS/Redirect option if you are currently using the HTTP method and want to redirect existing users to the new HTTPS port.

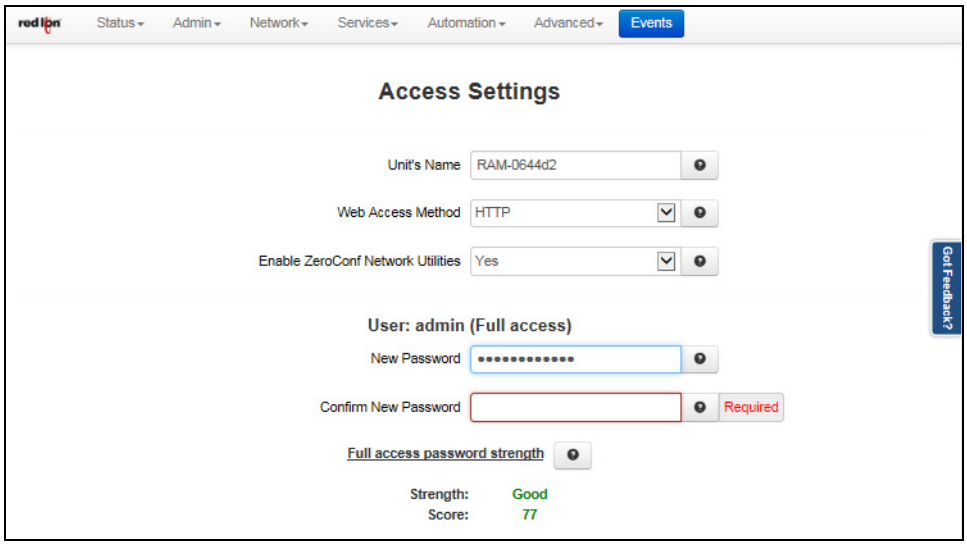
Note: The HTTP method can result in better performance and faster page load time; however, it is less secure than the HTTPS or HTTPS/redirect methods, which use data encryption to provide a secure connection.

Enable ZeroConf Network Utilities: Enabling this option will make this device available on the network via unitname/hostname without a central DNS server.

User: admin (Full access)

Permissions: This user level has full save and apply privileges in addition to CLI access via Telnet and/or SSH if enabled.

New Password: Enter the new password in the “New Password” field. For a secure password, choose one that is at least six characters long, which is not a common word and comprised of a mixture of upper and lower case characters and numbers as well as special characters. The relative strength of the password you create is displayed on the visual password strength indicator. Please note that the single quote (‘) character is not a valid character. *For security purposes, it is recommended that the admin password be changed according to your internal policies*.



Confirm New Password: Re-enter the password entered in the New Password field.

User: gauser (Controlled access)

Permissions: This user level has save and apply access to all systems of the GUI interface except for changing the passwords of the user accounts and no Telnet of SSH access.

New Password: Enter the new password in the “New Password” field. For a secure password, choose one that is at least six characters long, which is not a common word and comprised of a mixture of upper and lower case characters and numbers as well as special characters. The relative strength of the password you create is displayed on the visual password strength indicator. Please note that the single quote (‘) character is not a valid character. *For security purposes, it is recommended that the admin password be changed according to your internal policies*.

Confirm New Password: Re-enter the password entered in the New Password field.

User: techsup (Limited access)

Permissions: This user level has view only access to the deviceGUI and cannot save or apply configuration changes.

New Password: Enter the new password in the “New Password” field. For a secure password, choose one that is at least six characters long, which is not a common word and comprised of a mixture of upper and lower case characters and numbers as well as special characters. The relative strength of the password you create

is displayed on the visual password strength indicator. Please note that the single quote (‘) character is not a valid character. *For security purposes, it is recommended that the admin password be changed according to your internal policies*.

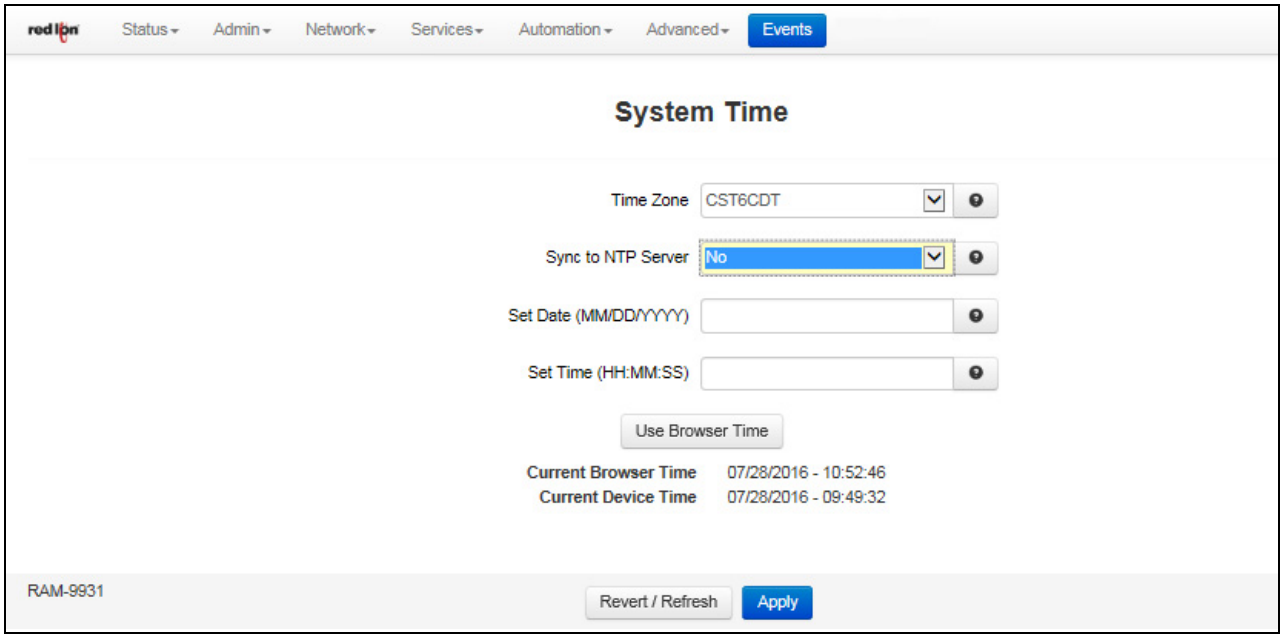
Confirm New Password: Re-enter the password entered in the New Password field.

Click on the *Save* button for changes to be saved without activating the interface, the *Apply* button will save your settings and apply them immediately. To revert to the previous settings, click on the *Revert* button.

3.3.2 System Time

The System Time menu item is used to configure the time zone on the Red Lion RTU or router to correspond to your location.

Click on the *System Time* menu time and the following window appears.



Time Zone: Select the time zone corresponding to your geographical location by choosing one of the values available on the drop down list provided.

To configure the date and time for your Red Lion RTU or router there are three options:

Option 1:

Sync to NTP Server: Select Yes to enable synchronizing the system clock to an NTP server.

Option 2 - Manual Configuration:

Current Date (MM/DD/YYYY) (Required): Set the Sync to NTP Server field to No and enter the Current Date using the shown format.

Current Time (HH:MM:SS) (Required): Set the Sync to NTP Server field to No and enter the Current Time using the shown format.

Note: The Hour field in on the 24-hour time clock, range 00-24. This page verifies that the month, day, year, hour, minute and seconds conform to expected inputs. For example, month range from 01-12, days range from 01-31 (checks for limit according to month, i.e. January has 31 days, February has 28 or 29 depending on year, etc.)

Option 3:

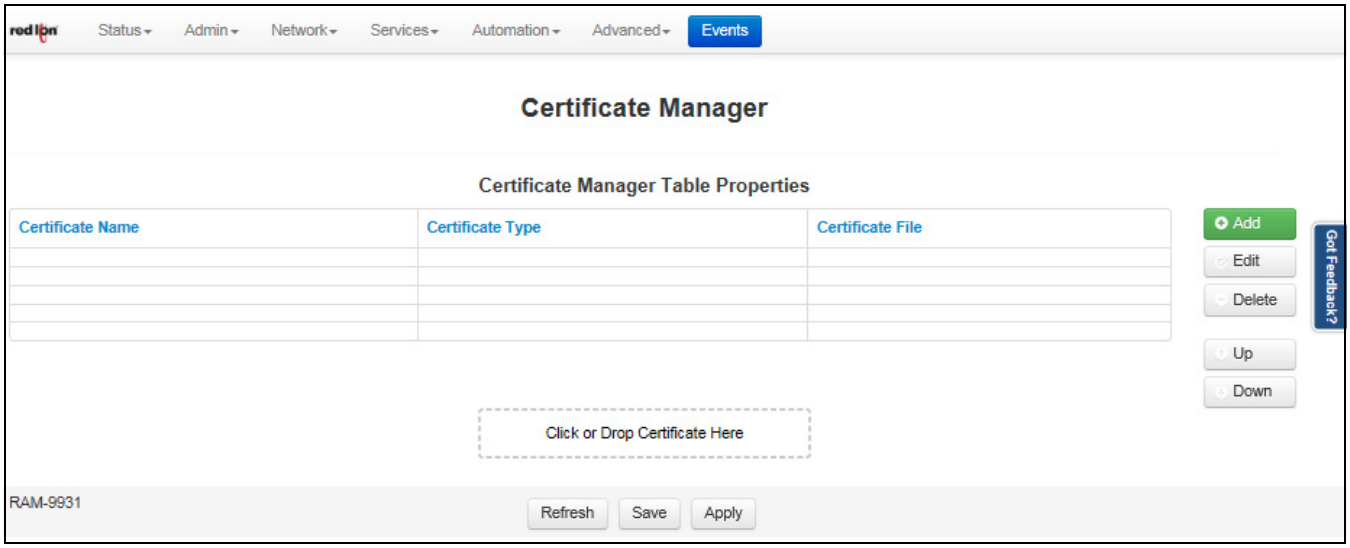
Use Local System Time: Set the Sync to NTP Server field to No and click on the Use Local System Time button. The local time as referenced from your browser is used to populate the settings.

Click on the *Apply* button to save your settings and apply them immediately. To revert to the previously saved defaults, click on the *Revert* button.

3.3.3 Certificate Manager

The Certificate Manager gives the option of adding a certificate, deleting or editing an existing one.

Click on the *Certificate Manager* menu item and the following dialog window appears:



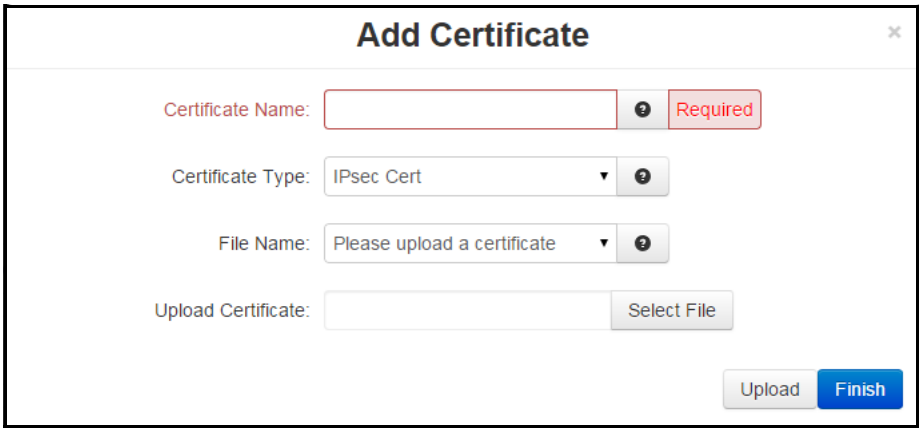
There are two ways to add a certificate to the Certificate Manager Table. One way is by using the “Click or Drop Certificate Here” hot spot and the second is by creating a new certificate.

To add a new certificate using the hot spot:

You can drag and drop a certificate on “Click or Drop Certificate Here” to add the certificate to the table or click on “Click or Drop Certificate Here” to navigate to and select the certificate file to be added.

To create a new certificate:

Click on the *Add* button and the following dialog window appears:



Certificate Name: Enter a descriptive name to be associated with the Certificate File to be uploaded. This name can be used later in fields where selection of a certificate is required. The descriptive name can contain only upper and/or lower case **letters** and **digits**.

Certificate Type: Select the type of certificate that you will be uploading. Each certificate is stored in a unique repository, depending on the service that will be using it. The certificate file name can contain only upper and/or lower case letters, digits, '-', '_' and must end with *.ca*, .cert, *.cer*, *.crt*, *.csr*, *.srl*, *.cnf*, *.key*, or *.pem*.

Possible choices include:

HTTPS: This certificate is used for the HTTPS engine, and replaces the onboard automatically generated self-assigned HTTPS cert. This should be a key and cert, together in the same pem format certificate file. The key should not be password protected. If the new cert is unable to be loaded by the HTTPS engine, it will revert to an onboard generated HTTPS certificate.

IPsec Cert: This will specify a certificate to be used to authenticate a VPN connection. A server and client certificate will be required.

IPsec Key: An RSA key must be provided for any client certificate uploaded. If this is signed with a password, that will need to be entered in the IPsec as well.

IPsec CA: This specifies a Certificate Authority. Please include a CA valid for each signed certificate.

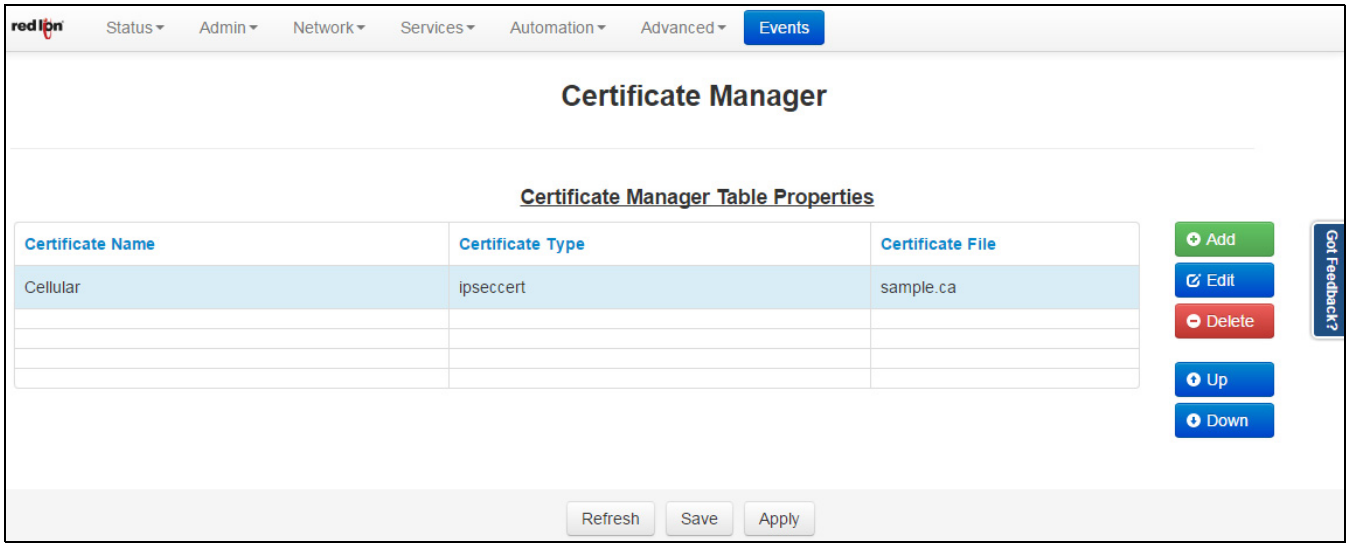
SSL: This certificate will be available for SSL Connections as a Server Certificate, or a Client Certificate.

SSLVPN: This certificate will be available for SSL VPN tunnels.

File Name: This field will be populated with files previously selected in the Upload Certificate field for quick access.

Upload Certificate: Click on the Select File button to browse to the location where the certificate file is saved. The certificate file name can contain only upper and/lower case letters, digits, '-', '_' and must end with *.ca*, .cert, *.cer*, *.crt*, *.csr*, *.srl*, *.cnf*, *.key*, or *.pem*. ***Note:*** SSL type certificates must include the key and cert portions, and the key must not be password encrypted.

Click on the *Finish* button and you will be directed to the Certificate Manager dialog window and the table will be populated with the entered data.



To delete an existing certificate, select it in the table and click on the *Delete* button. To edit an existing certificate, select it in the table and click on the *Edit* button.

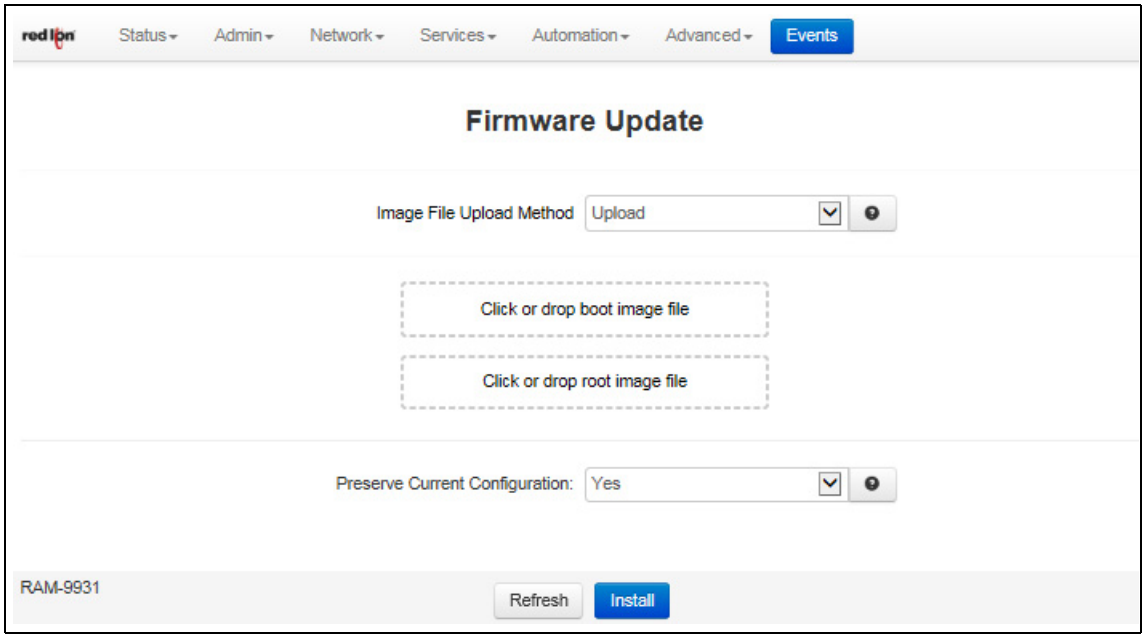
To move a certificate up or down in the table properties, use the Up and Down buttons.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

3.3.4 Firmware Update

The Firmware Update menu item is used to upgrade the firmware of the Red Lion RTU or router.

Click on the *Firmware Update* menu item and the following window appears:



To upgrade the firmware of the Red Lion RTU or router:

Click or drop boot image file: Click on to select the file that will perform the kernel update or drag and drop into this area the file that will perform the kernel update.

Click or drop root image file: Click on to select the file that will perform the system update or drag and drop into this area the file that will perform the system update.

Preserve current configuration: Select YES to save the device's current configuration and restore it after the firmware image is installed.

Image File Upload Method: Select the method that will perform the image file upload including a SD Card source option.

Note: The Image File Upload Method from SD Card option is only available on the 9xxx series (SD Card model).

Click on the *Install* button.

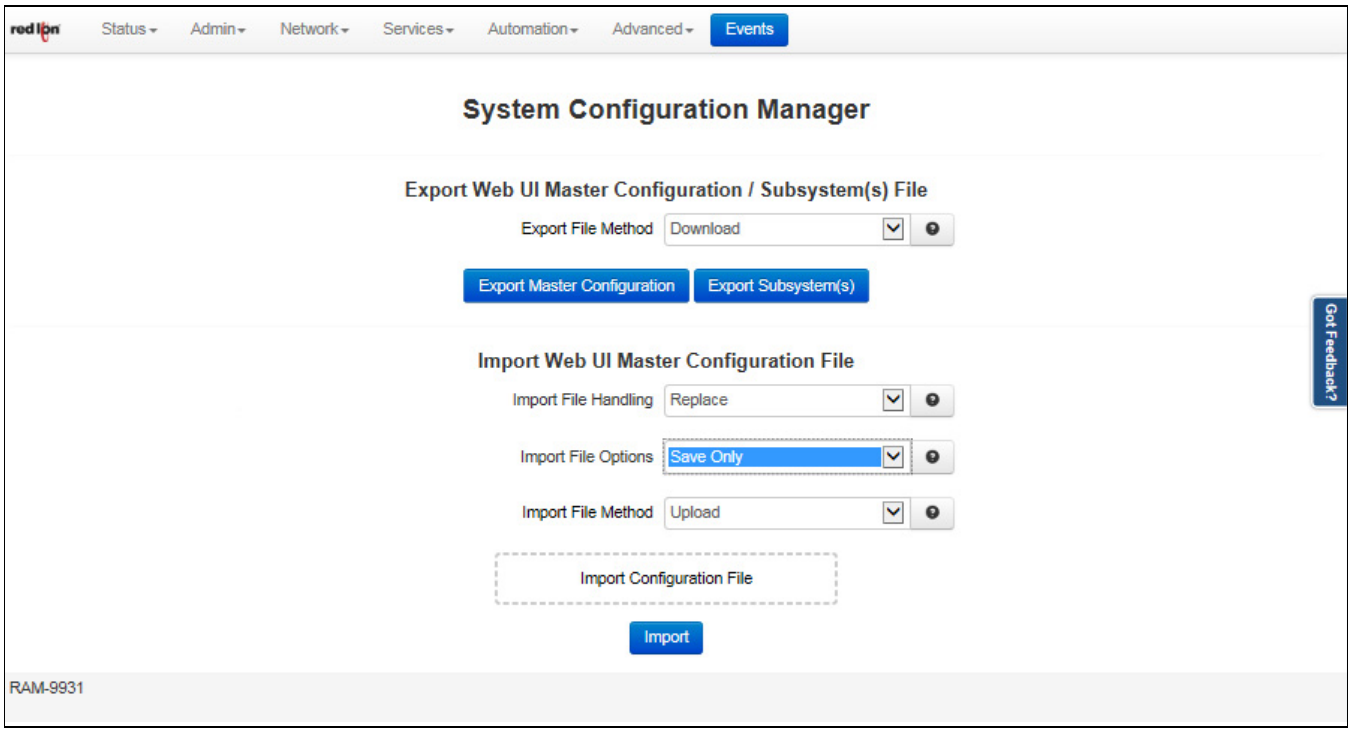
Note: This procedure can take anywhere from 6-10 minutes to complete.

Warning: It is important that the power to the unit is **not** interrupted at any time during the upgrade process, as this could cause the unit to become corrupt and require shipment back to the factory to correct.

3.3.5 Configuration Manager

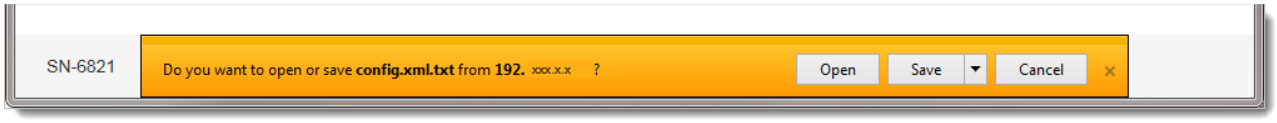
The Configuration Manager menu item saves a copy of the current system configuration, i.e., Export. This is useful when a confirmed good configuration is operational. A backup can be exported for use should the configuration become corrupt or re-configured in error.

Click on the *Configuration Manager* menu item and the following window appears:



Export File Method: Select the method (Download or SD Card) by which you would like to download the master or multi subsystem configuration file.

Export Web UI Master Configuration File: To save a copy of the Red Lion RTU or router configuration, click on the “Export” button. The pop-up window below asking you to save or open the file appears. Select the desired option.



Note: Please note the directory where the file was saved in order to retrieve it when needed to put the file back onto the Red Lion RTU or router.

Import Web UI Master Configuration File: Set your defaults for importing the configuration file.

Import File Handling: Select Replace to completely replace the device configuration file with your import.

Import File Options: If you want to save the new configuration without immediately applying it, simply select *Save Only.*

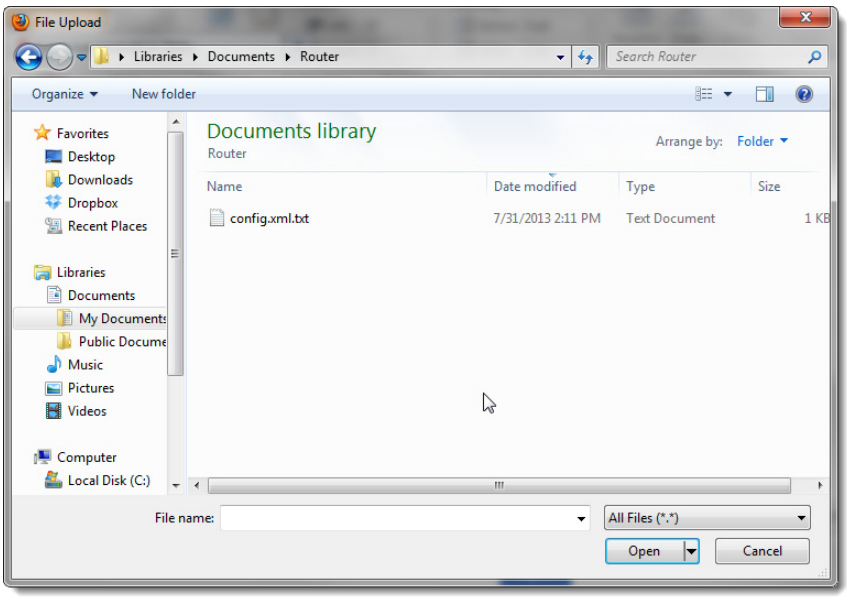
If *Apply* is selected to apply the settings, any imported configuration sections will be applied ONLY if they have changed values. If imports sections are identical to the current configuration, that section will not be applied.

If you select *Forced Apply* to apply the settings, every section imported will be applied immediately. This is not frequently required.

Warning: If the configuration file has many sections, the *Forced Apply* option can take a long time to process.

To apply the settings, you will need to visit the configuration page for each supported sub-system and click its Apply button. This is unusual, but useful for when you are importing a configuration from one unit to another and need to make additional settings before applying them.

Import Configuration File: Click on *Import Configuration File*, and the dialog window below appears.



Browse to the directory where the config.xml.txt file is located.

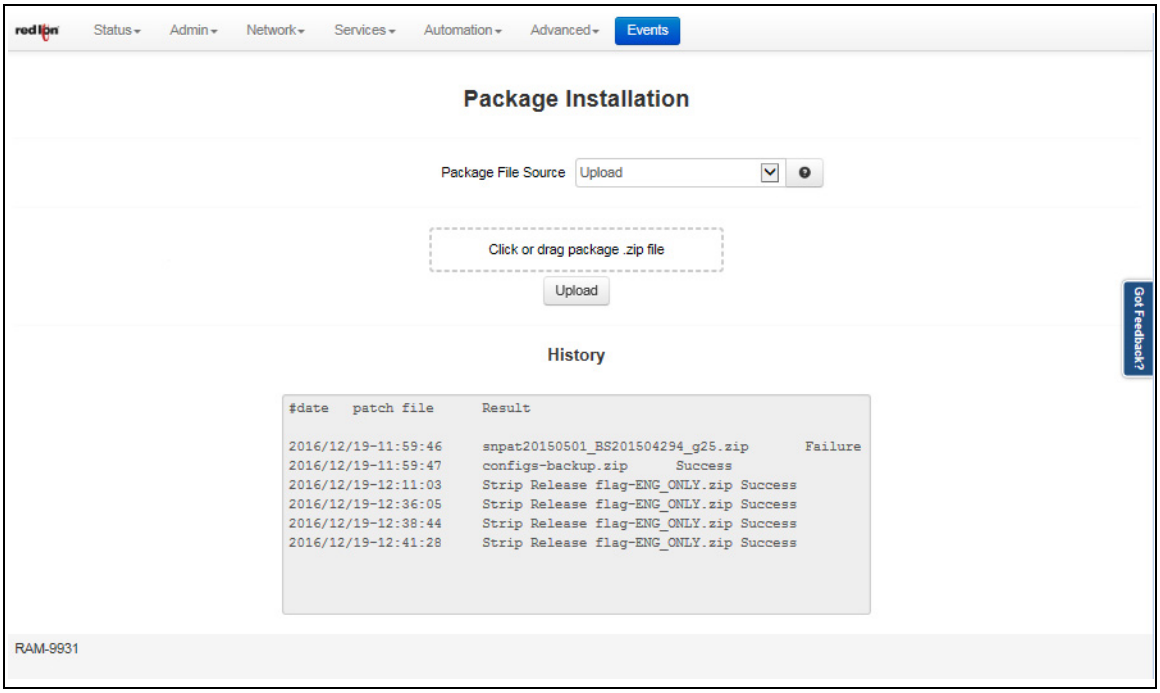
Select the config.xml.txt file and click on the *Open* button to populate the Browse window. If needed, you can change the file or remove it from the field by clicking the appropriate button

Click on the *Import* button. When import is complete, a table appears at the bottom of the dialog window listing the modified files.

3.3.6 Package Installation

The Package Installation feature allows you to upload and install patches from Red Lion.

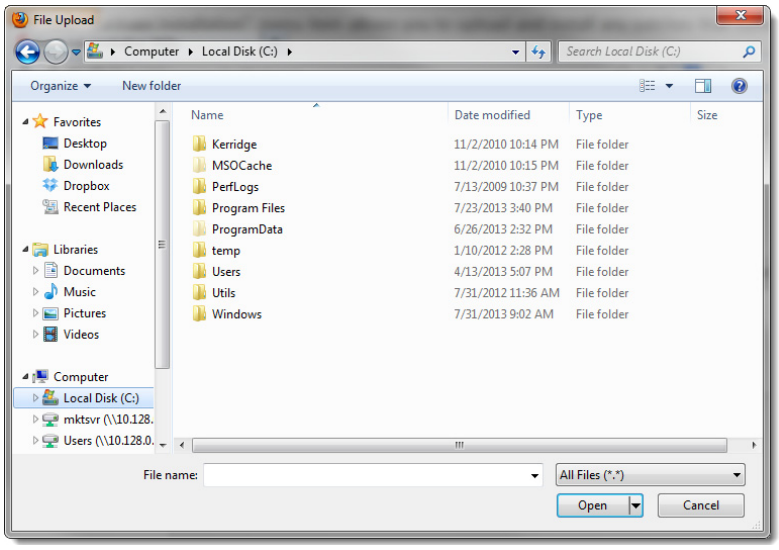
Click on the *Package Installation* menu item and the following dialog window appears:



Package File Source: Select the method (Upload or SD Card) by which you would like to upload the package zip file.

Click or drag package .zip file: Click on to select the package .zip file that will be installed or drag and drop into this area the package .file that will be installed.

Clicking on the field will display the a dialog window similar to the following:



Browse to the directory where the package .zip file is located.

Select the filename to select the file.

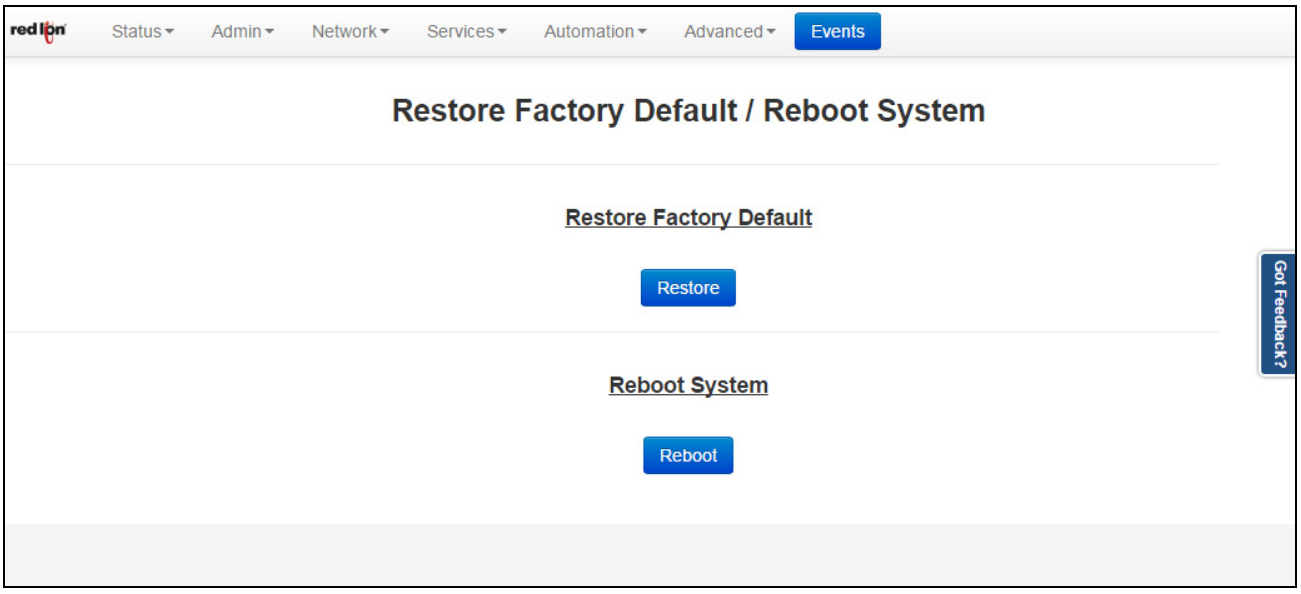
Note: Be sure to use only genuine Red Lion provided packages in the form of filename.zip.

Click on the *Open* button to populate the Package File field and click on the *Upload* button. When install is complete, a table appears at the bottom of the dialog window listing the results.

3.3.7 Factory Defaults/Reboot

The Factory Defaults/Reboot menu item allows you to restore the configuration back to factory default settings.

Click on the *Factory Defaults/Reboot* menu item and the following window appears:

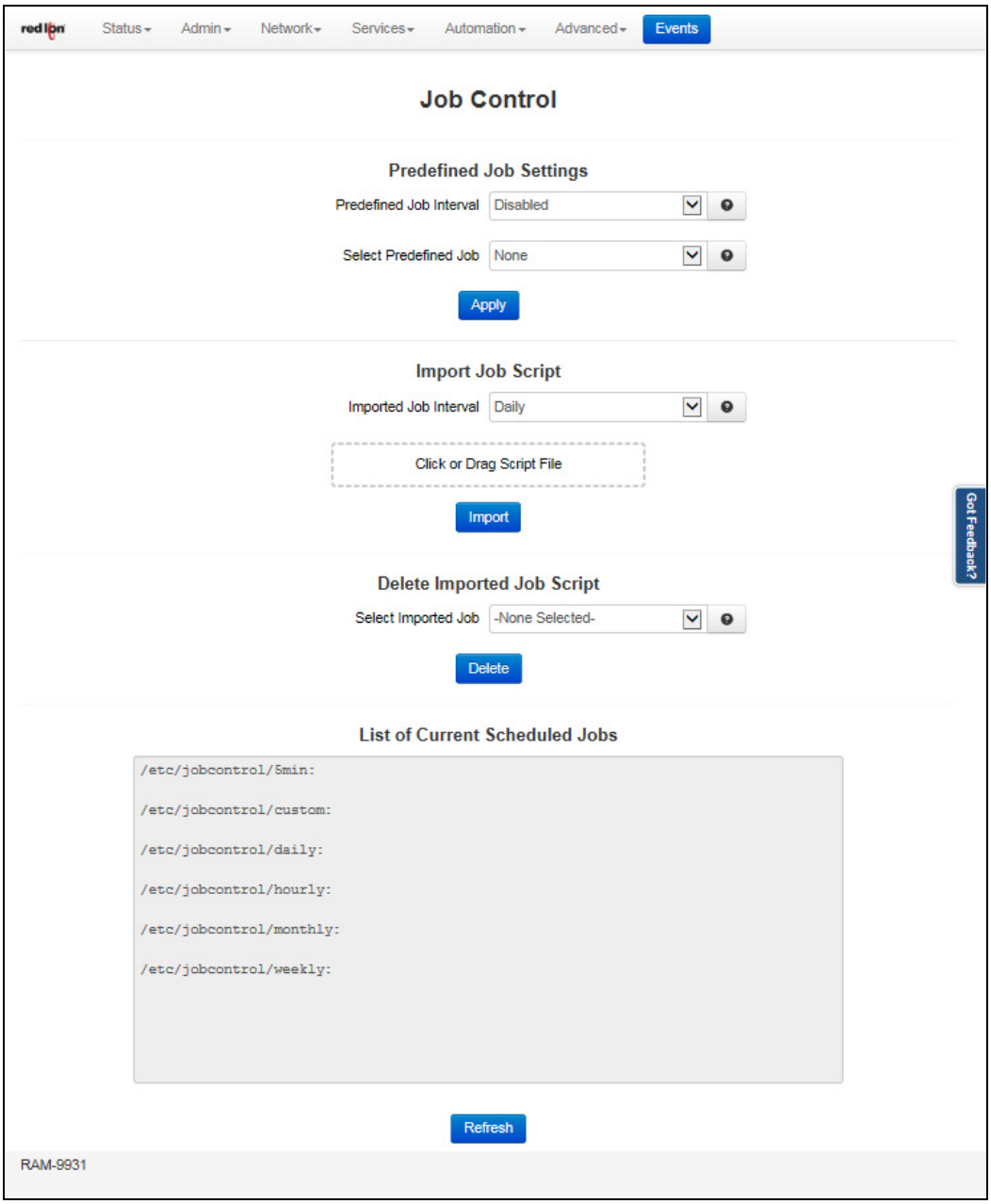


Restore Factory Default: Click on the *Restore* button to restore the factory default settings. A warning appears, read through the information and click OK. The restore may take 2-5 minutes.

Reboot System: Click on the *Reboot* button to reboot the device. A warning appears, read through the information and click OK. The reboot may take 2-5 minutes.

3.3.8 Job Control

The Job Control feature is used to create jobs that will be run at specified intervals.
Click on the *Job Control* menu item and the following dialog window appears:



Predefined Job Settings:

Predefined Job Interval: Select the appropriate periodic job interval from the drop-down list provided to run at the scheduled job interval. If the option ***Disabled*** is selected, all the jobs created for the selected job will be removed. The available predefined options are:

Daily: Will run at 4:02 am.

Weekly: Will run at 4:22 am, every Sunday.

Monthly: Will run at 4:42 am, on the first day of every month.

Select Predefined Job: Select the desired job to be scheduled for the selected job interval. The options are:

Reboot: Will reboot the unit at selected job interval.

Restart Serial IP: Will restart the GWLNX (Serial IP) application at selected job interval.

Click on the *Apply* button once the required changes have been made.

Import Job Script

Imported Job Interval: Select the appropriate job interval from the drop-down list to run at the scheduled job interval. The available options are:

5 minutes: Will run every 5 minutes.

Hourly: Will run every hour.

Daily: Will run at 4:02 am.

Weekly: Will run at 4:22 am, every Sunday.

Monthly: Will run at 4:42 am, on the first day of every month.

Upload Script File: Click on the Select File button to browse to the location where the job to be uploaded is stored.

Click on the *Import* button once the file is selected.

Delete Imported Job Script:

Select Imported Job: Select an imported job from the drop-down list to be deleted from any scheduled job interval.

Click on the *Delete* button once the job to be deleted has been selected.

List of Current Scheduled Jobs

This table displays the list of current scheduled jobs.

3.4 Network Tab

The Network Tab configures aspects of the Red Lion RTU or router affecting the networking functionality of the unit. From here you can configure the Cellular Connection, Ethernet Interfaces, Firewall, Tunneling, DNS Settings, Static Routes, DMNR/NEMO and TCP Global Settings.

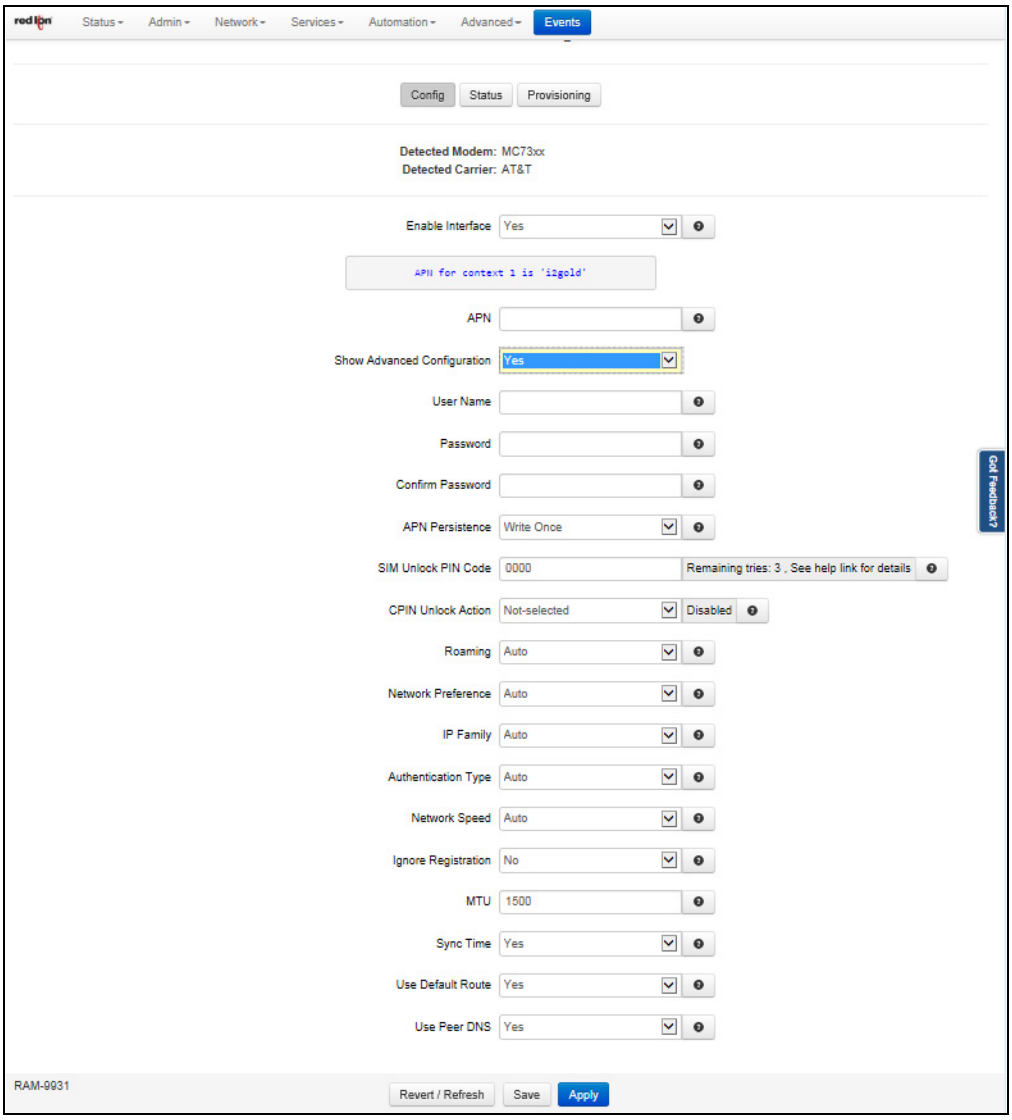
3.4.1 Cellular Connection

The Cellular Connection menu item is sub-sectioned into Configuration, Status and Provisioning. These options allow the user to configure/view the cellular information on unit.

Configuration

The Configuration menu item is used to make configuration changes to the cellular connection settings on the Red Lion unit.

Click on the *Configuration* menu item and the dialog window below appears (when Show Advanced Configuration is set to Yes):



The Config, Status and Provisioning buttons are a quick way to navigate to the three (3) sub-menus of the Cellular Connection menu.

Enable Interface: Select Yes to enable the interface to become active after the new settings are applied and upon subsequent system start-up. Select No to disable the cellular interface and prevent the cellular radio from attempting to establish a network connection.

APN: Enter the APN used to access your cellular wireless data service in this field.

Note 1: Maximum allowable characters for this field are 104 characters.

Note 2: Entering an APN value in this field will overwrite any APN stored in the modem for the selected context.

Show Advanced Configuration: Selecting Yes will enable the additional fields listed below.

User Name: Enter the user name assigned to you by your cellular wireless data plan provider which should have been given to you when you established your service.

Password: Enter the password assigned to you by your cellular wireless data plan provider which should have been given to you when you established your service.

Confirm Password: Enter the password you entered in the **Password** field, exactly as typed before. If the passwords do not match you will be prompted to re-enter it.

APN Persistence: Select the APN Persistence option.

Write Always: Will always overwrite the configuration used for connections

Write Once: Will update the APN once but not again in the future. This allows other processes to update the APN such as automatic tower APN updates. This is recommended for Verizon.

SIM Unlock PIN Code: Enter the 4 digit SIM Unlock PIN code here. Entering the wrong value multiple times may cause your SIM to become unusable and require service by your carrier. If you have previously entered this value, but it is now blank, the PIN was probably rejected by the SIM. Rejected PIN codes are cleared so that they are not attempted multiple times. Use this option with caution.

CPIN Unlock Action: Select the required CPIN action for SIM locking.

Enable: Lock SIM to require a SIM PIN password for use. This SIM PIN will be required every time the device is powered on. The current SIM PIN must be known in order to enable.

Disable: Unlock SIM to no longer require a SIM PIN password for use. The current SIM PIN must be known in order to disable.

Roaming: Set to allow cellular roaming.

Auto: Allow roaming (recommended).

Home Network Only: Attach to Home and Partner networks only.

Network Preference: Select the network preference.

Auto: Automatic registration.

Manual: Device only registers to specified network based on the entered Mobile Country Code (MCC) and Mobile Network Code (MNC). Will force device to not register with other networks.

Caution: This may affect connections to partner service providers and available roaming options. Use this option with caution.

IP Family: Select the IP Family required for your connection.The recommended setting for this field is Auto.

Auto: Default IPv4, IPv6 for Verizon firmware.

IPv4: Make IPv4 connection only.

IPv4v6: Make IPv4 and IPv6 connection.

Note: An IPv6 session is not guaranteed, and is not considered an error if an IPv4 session is successful. In order to route IPv6 traffic, Enable IPv6 under network settings. Not all carriers support IPv6.

Authentication Type: Select the authentication type for this APN profile. This is the encoding of the username/password.

Auto: Automatic authentication.

CHAP: Challenge-Handshake Authentication Protocol method of authenticating a user or device to an authenticating entity based on the challenge response.

PAP: Password Authentication Protocol method of authenticating a user or device to an authenticating entity based on the password.

Network Speed: Select the connection speed to be used for the cellular modem connection from the drop down list provided. Auto uses the widest available defaults, starting at the highest speed available (4G-LTE, if present). The recommended setting for this field is Auto or Default.

Possible values include:

- Default: Do not adjust the module settings.
- Auto
- LTE: 4G/LTE only
- 2G3G: 3G/2G only, no LTE
- 3G Only: 3G only service

Note: 3G limited models have an option to upgrade to an LTE modem by entering the unlock code provided by customer service. SN/RAM-6000 models with a -3G suffix are the only models available in this configuration.

- 2G Only: 2G only service

Ignore Registration: Attempt to make a cellular connection even when the modem is not registered on a network. The recommended setting for this field is NO.

MTU: Enter the MTU size you desire to use. In computer networking, the maximum transmission unit (MTU) of a communications protocol of a layer is the size (in bytes) of the largest protocol data unit that the layer can pass onwards. MTU parameters usually appear in association with a communications interface (NIC, serial port, etc.). Standards (Ethernet, for example) can fix the size of an MTU; or systems (such as point-to-point serial links) may decide MTU at connect time. A larger MTU brings greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU also means processing of fewer packets for the same amount of data. In some systems, per-packet-processing can be a critical performance limitation.

However, this gain is not without some downside. Large packets can occupy a slow link for some time, causing greater delays to following packets and increasing lag and minimum latency. For example, a 1500-byte packet, the largest allowed by Ethernet at the network layer (and hence over most of the Internet), ties up a 14.4k modem for about one second.

Recommended Setting: The recommended setting for this field is 1500.

Sync Time: This option will attempt to take the local time as reported by the cellular tower, and set the unit's system time to match. The recommended setting for this field is Yes, unless another method of time Sync, such as NTP is being used.

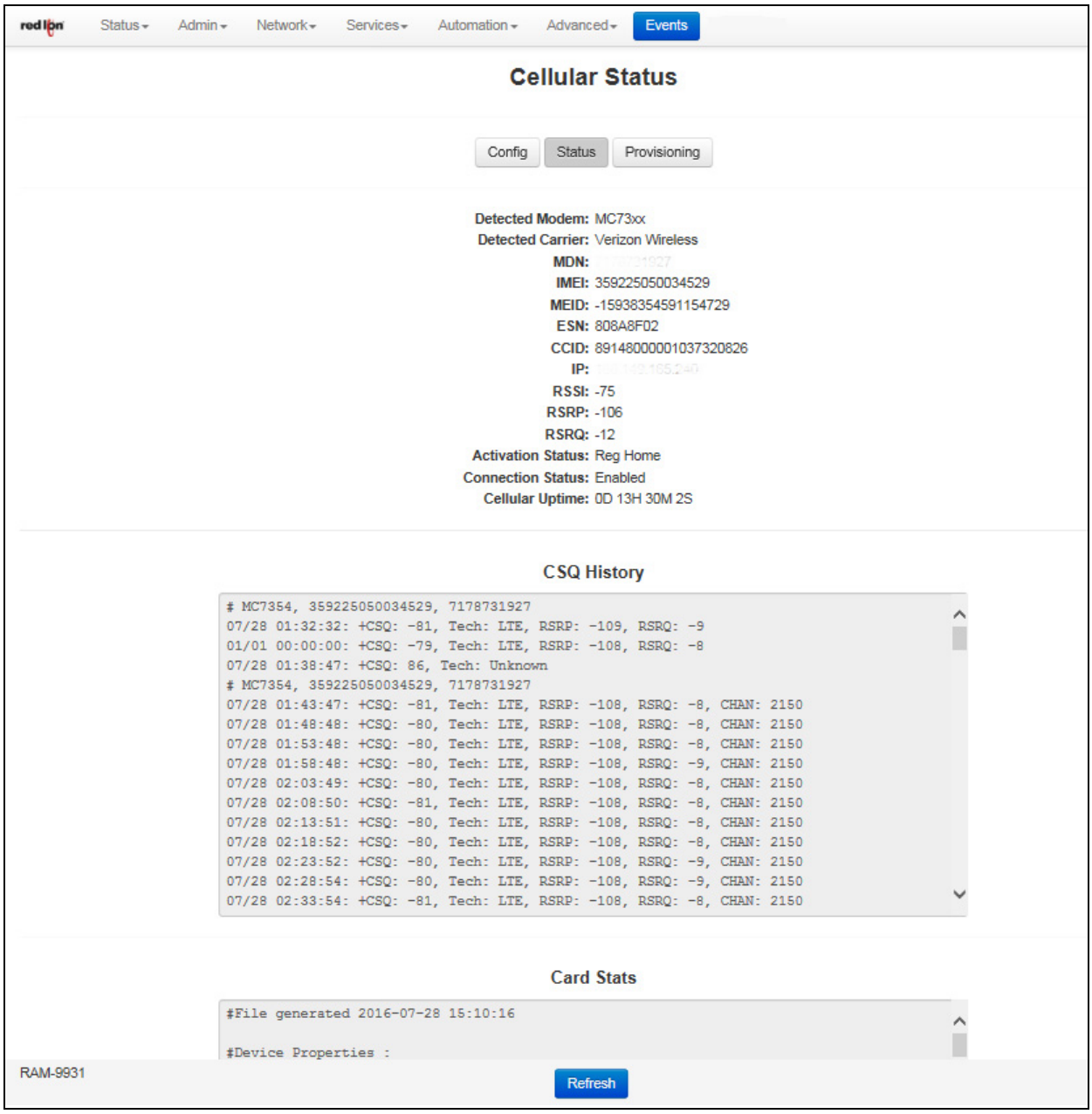
Use Default Route: This field allows you to choose to have the default route for the Red Lion RTU or router to be the cellular connection when it is connected, or to designate an Ethernet port as the default route. Select Yes to have the cellular connection use the default route once it is connected.

Use Peer DNS: Select Yes to have the cell connection accept DNS information from the peer device to which it is connected.

Click on the *Save* button for changes to be saved without activating the interface, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert/Refresh* button.

Status

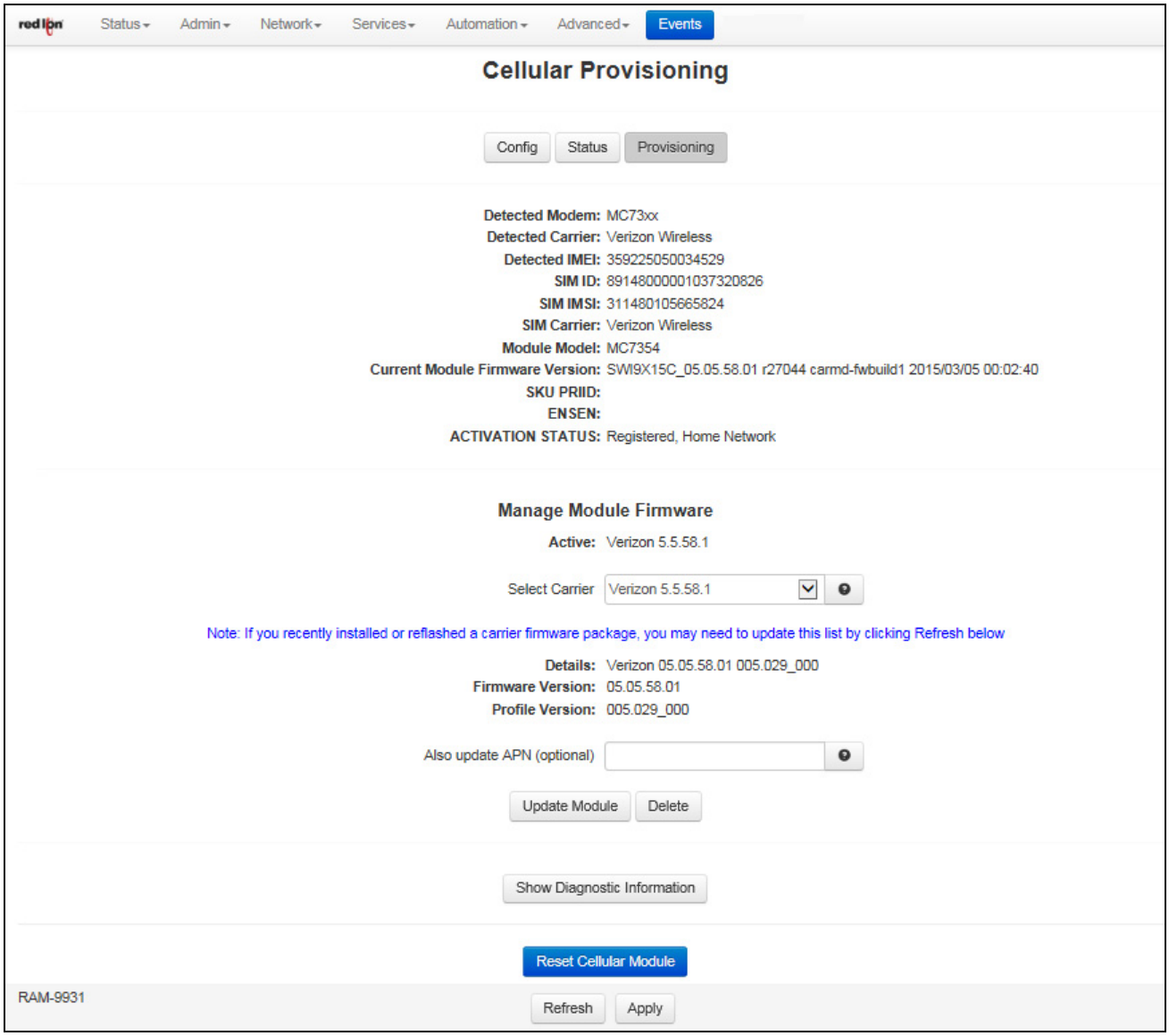
The Status menu item brings up a dialog window displaying the status of the cellular connection. From here, you can get information such as the type of modem, carrier, MDN, IMEI, MEID, ESN, CCID, IP, RSSI, RSRP, RSRQ, Activation Status, Connection Status, Cellular Uptime CSQ History and Card Stats.



Provisioning

The Provisioning menu displays carrier specific information that may be useful when initially provisioning your device with a new carrier.

Click on the *Provisioning* menu item. If a cellular connection is found, the following window appears with the information about the modem in the upper window:



Note: If the cellular SIM is not recognized, go to the Configuration dialog window and enter the required data (see Section 3.3.5).

Select Carrier: Select a carrier to view details on the cell module firmware and profile contained in the carrier package. With a carrier selected, you can click **Update Module** to flash the cell module with the displayed firmware and profile. To remove the carrier package from the device, click on the **Delete** button.

Note: **1:** To be available in this context, a carrier firmware package must be installed through the package installation screen.

Note: **2:** This feature is only available on the SN/RAM-69xx and RAM-99xx products.

Also update APN (optional): Enter the APN used to access your cellular wireless data service.

Note: If an APN is specified in this field, it will be automatically applied after the module is updated.

Note: The maximum amount of characters allowed in this field is 104 characters.

Note: Entering and APN value in this field will overwrite any APN stored in the modem for the selected context.

Click on the *Update Module* button for settings to be applied. This operation takes approximately 2 minutes to complete. The device will reboot following the Update Module process to re-initialize the modem with the newly uploaded carrier.

Click on the *Delete* button to remove the selected carrier from Select Carrier field. This will remove the stored carrier image from the device and it will no longer be selectable. This does not effect the active firmware currently loaded in the module.

Show Diagnostic Information

The information generated when the *Show Diagnostic Information* is clicked, is used for technical support purposes if the support engineer requests it.

Reset Cellular Module

The Reset Cellular Module button will reboot the cellular module only. It is recommended that you only do this if directed by a technical support representative. Rebooting the cellular module will disconnect the module from the network and re-establish a new connection once the module is powered back up.

3.4.2 Interfaces

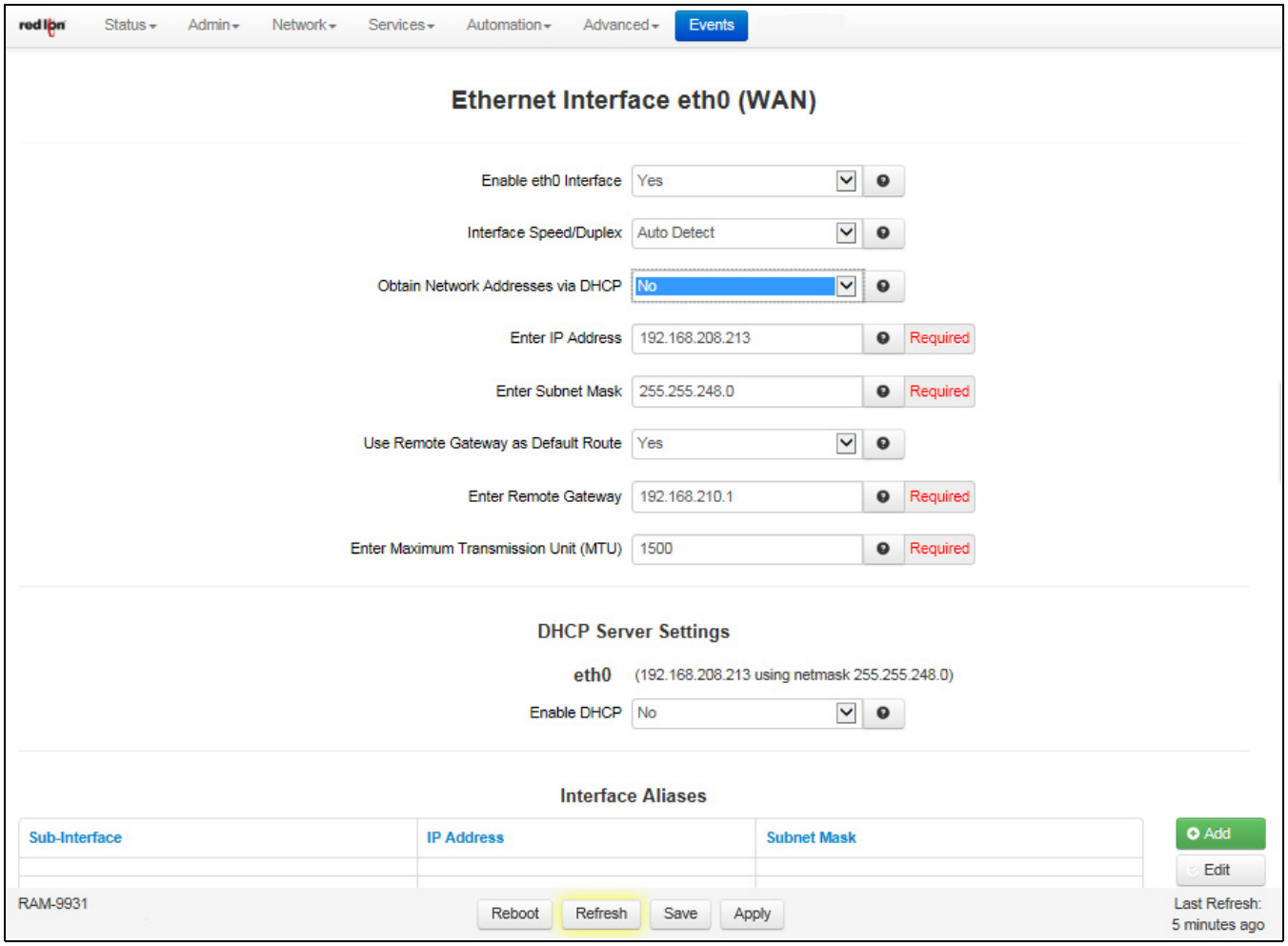
The Interfaces menu allows the administrator to configure the Ethernet ports of Red Lion RTU or routers to incorporate within their existing network topology.

Interfaces available may include eth0 (WAN), eth1 (LAN), Wifi, USB and IPv6. These will only be present if your hardware supports these interfaces. These ports are 'auto-sensing', allowing for greater flexibility.

eth0 (WAN) and eth1 (LAN) - (Network Interfaces)

The configuration procedure of the Ethernet ports is the same for eth0 and eth1, therefore this section will only reference the configuration of "WAN"/'eth0'. Please refer to this section when configuring "LAN"/'eth1'.

Click on the *eth0 (WAN)* menu item, select **Yes** and the following window appears:



Enable eth0 Interface: This field determines if the specified Ethernet port is enabled, allowing the administrator to disable the port if necessary.

Interface Speed/Duplex: Select the Speed and Duplex to be used for the physical interface. The recommended setting for this field is Auto-Detect.

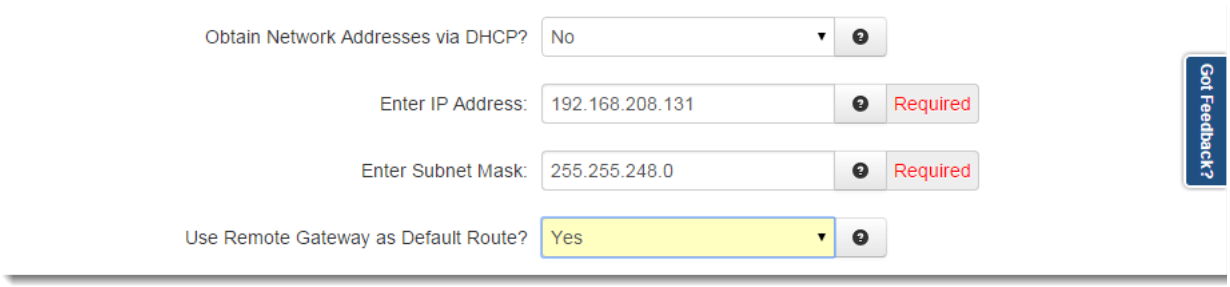
- Auto Detect: Use the 'best negotiated' speed and duplex. (default)
- 10 Mbps/Half: Force the interface to 10 Mbps and half-duplex.

- 100 Mbps/Half: Force the interface to 100 Mbps and half-duplex.
- 100 Mbps/Full: Force the interface to 100 Mbps and full-duplex.

Note: An incorrect 'forced' setting will result in communication failure for this interface.

Obtain Network Addresses via DHCP: Select ***Yes*** to allow the interface to obtain address information via a DHCP server. The device will obtain its IP address, netmask and remote gateway and optionally, use the remote gateway as the default route. It can also obtain DNS server address via DHCP.

Select ***No*** to prevent the interface from obtaining address information via a DHCP server. You will be required to enter an IP address, netmask and remote gateway addresses. DNS information can be provided by navigating to Network → DNS Settings.



Enter IP Address: This field appears when ***No*** is selected for "Obtain Network Addresses via DHCP". Specify the IP Address to be assigned to the Ethernet port when a 'Static' IP Address configuration is selected. This field will not be visible or accessible when a 'Dynamic' IP address configuration is selected, as the DHCP server will provide the Red Lion RTU or router with the IP address that it should use. This is a required field.

This address should have been provided by your Network Administrator. It must be an address valid for the network described by the value contained in the enter ***Subnet Mask*** field and must not conflict with any other device on the target network.

The IP address identifies a device on a TCP/IP network. Every device on a network must have a unique address. The range of valid addresses for a given network is determined by the value of the Netmask. Some addresses are reserved for special uses such as network and broadcast.

For example, if a netmask is 255.255.255.0 and the IP address assigned to the device is 192.168.1.3, then the range of valid addresses is 192.168.1.1 through 192.168.1.254 as 192.168.1.0 is the value reserved for the network and 192.168.1.255 is the value reserved for the broadcast address.

Enter Subnet Mask: Enter the desired Netmask for the interface in the field provided. This field is only available when "Obtain Network Addresses via DHCP" has been set to ***No***.

Your Network Administrator should be able to provide an appropriate value for this field. This value determines the valid range of IP addressed allowed in the ***Enter IP Address*** field.

Use Remote Gateway as Default Route: Select Yes to use this interface as the default route. If **Obtain Network Addresses via DHCP** is set to Yes, then the interface is configured to obtain its address information from a DHCP server, and uses the gateway address provided by the server as the default route. If **Obtain Network Addresses via DHCP** is set to NO, then the IP Address of the remote gateway will be required to be entered in the **Enter Remote Gateway** field.

Note: On devices with multiple interfaces, if may be possible for this setting to be made multiple times. When the Web UI is used to configure an interface, the last settings applied are the ones which take precedence. When a device reboots, the last interface to become active takes precedence. For devices with interfaces which activate/deactivate dynamically (cellular connections, fallback, etc.), the current interface activated takes precedence.

Enter Remote Gateway: Enter the IP Address for the gateway device in the field provided. This field is only available when **Obtain Network Addresses via DHCP** has been set to **NO**. This field is required if Use Remote Gateway as Default Route is set to Yes.

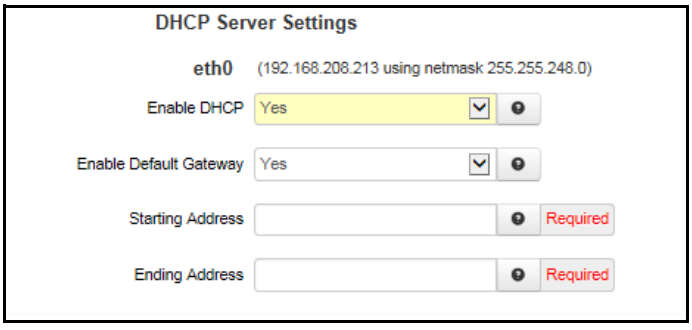
A gateway is a device (typically a RTU or router) used to gain access to another network. For example, if a device is attached to a LAN whose network address is 192.168.1.0 with a netmask of 255.255.255.0, then it can communicate directly with any other device on that network with a range of addresses of 192.168.1.1 through 192.168.1.254 (with 192.168.1.255 reserved for broadcast). An address outside of that range is on a different network which would need to be accessed indirectly through a RTU or router and that RTU or router would be the gateway to the network on which the remote target device resides, so to communicate with it would mean sending and receiving via the gateway device. This also requires either defining a static route (defined through the **Network →Static Routes** screen) via that gateway or making it the default route (by setting **Use Remote Gateway as Default Route** to Yes.

Your Network Administrator should be able to provide an appropriate value. The address must be one within the valid range for the network.

Enter Maximum Transmission Unit (MTU): Enter the desired MTU size. In computer networking, the **maximum transmission unit** (MTU) of a communications protocol of a layer is the size (in bytes) of the largest protocol data unit that the layer can pass onwards. MTU parameters usually appear in association with a communications interface (NIC, serial port, etc). Standards (Ethernet, for example) can fix the size of an MTU; or systems (such as point-to-point serial links) may decide the MTU at connect time. A larger MTU brings greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU also means processing of fewer packets for the same amount of data. In some systems, per-packet-processing can be a critical performance limitation. However, this gain is not without some downside. Large packets can occupy a slow link for some time, causing greater delays to following packets and layer (and hence over most of the Internet), ties up a 14.4k modem for about one second. The recommended setting is 1500.

DHCP Server Settings: Specify whether you want to enable a DHCP Server for the interface with your Yes/No selection for **Enable DHCP**.

> **Note:** If the interface is not enabled, or has been set to obtain its addressing parameters via DHCP, this option will be forced to **No**, and disabled until the interface is both enabled and set to use a static IP address.



Enable Default Gateway: Provide Default Gateway IP address to DHCP Client.

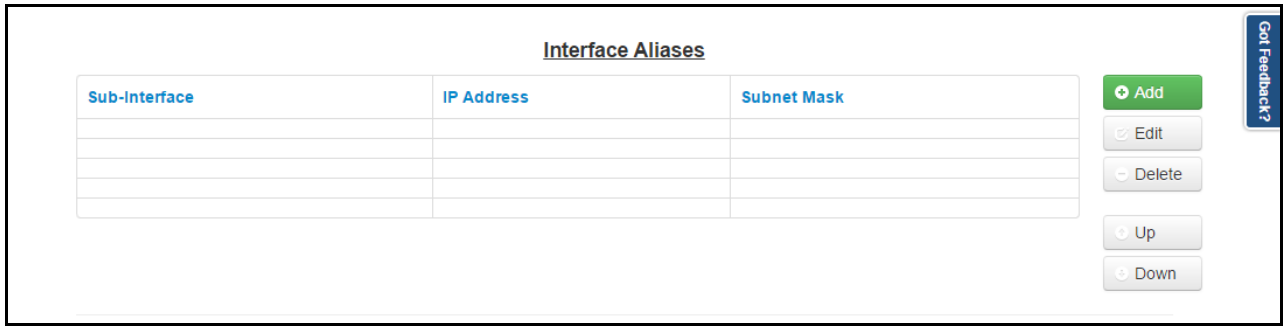
Set to **No** if you wish to only gain access to this device's web interface and have another connection from your PC out to the Internet.

Set to **Yes** if you wish to gain access to the Internet through this device.

Starting Address: Enter the starting IP address of a range you want the DHCP Server to provide for clients. The recommended setting is a valid address for the subnet for which the interface is configured. Use care to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

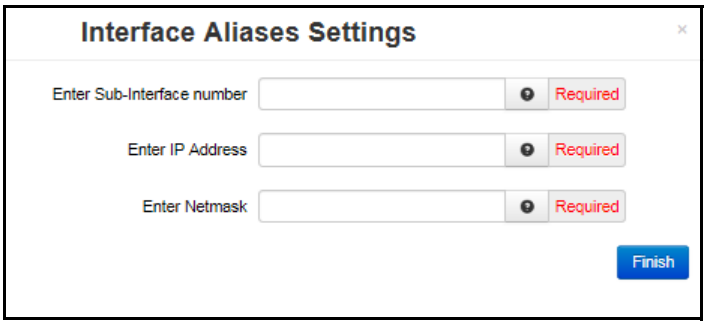
Ending Address: Enter the ending IP address of a range you want the DHCP Server to provide for clients. The recommended setting is a valid address for the subnet for which the interface is configured, beyond that chosen for the starting value of the range. Use care to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

Interface Aliases: Sub-interfacing is essentially the segmenting of a single wire, or Ethernet port, into multiple IP networks. Instead of subnetting and routing, you can create a sub-interface and then set it up as you would a standard Ethernet interface.



To configure a sub-interface:

Click on the *Add* button and the following pop-up window appears:

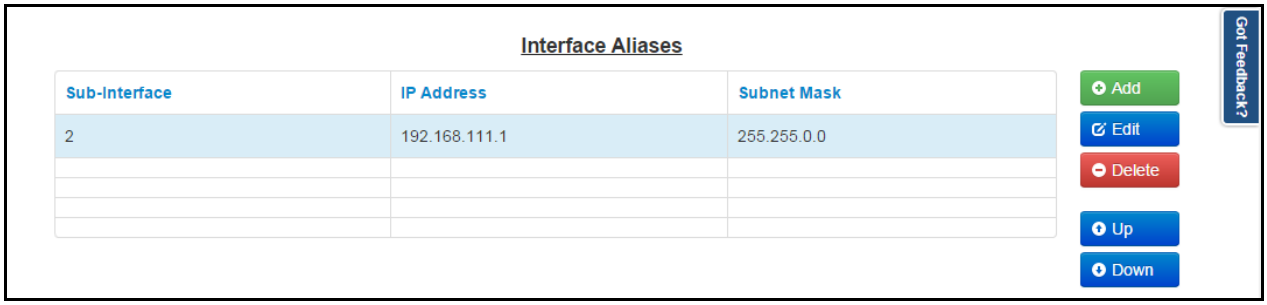


Enter Sub interface number (Required): This field is where you enter the sub interface number. The valid range is 0-99, and each aliased interface must be uniquely numbered. The final sub interface name will then be in the form **ethx:y** where **x** is the root interface number and **y** is the sub interface number. Your Network Administrator should provide guidance as to an appropriate value.

Enter IP Address (Required): This field specifies the IP Address of the sub interface. This address should be provided by your Network Administrator.

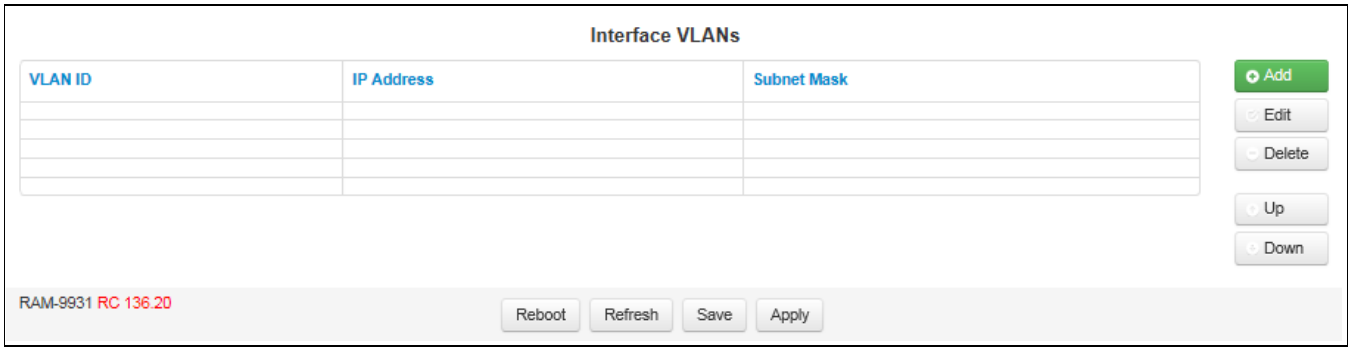
Enter Netmask (Required): This field specified the netmask to be assigned to the sub interface. Your Network Administrator should provide an appropriate value.

Click on the *Finish* button and you will be directed to the Ethernet Interface dialog window and the Interface Aliases table will be populated with the entered data.



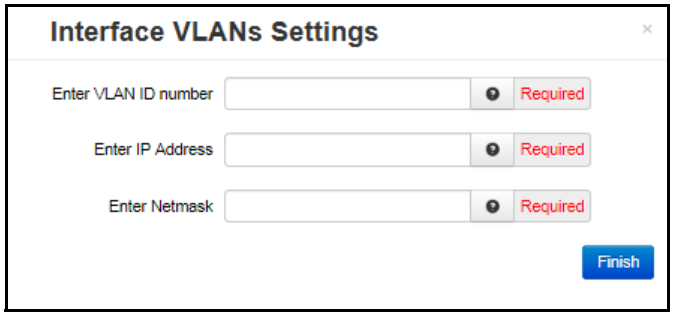
Interface VLANs: Sub-interfacing is essentially the segmenting of a single wire, or port, into multiple IP networks. Instead of subnetting and routing, you can create a sub-interface and then set it up as you would a standard Ethernet interface.

Note: VLAN's are available for any unit with Split LAN enabled under Switch Control.



To configure an Interface VLAN:

Click on the *Add* button and the following pop-up window appears:



Enter Sub-Interface number ID number (Required): Enter the desired Sub-Interface number in the field provided. The valid range is 0-99 and each interface must be uniquely numbered. The final Sub-Interface name will then be in the form ethx:y where x is the root interface number and y is the sub-interface number. Your Network Administrator should be able to provide guidance as to an appropriate value.

Enter IP Address (Required): Enter the desired interface IP Address into this field. This address should be provided by your Network Administrator.

Enter Netmask: Enter the desired Netmask for the sub interface in the field provided. Your Network Administrator should provide an appropriate number.

Click on the *Finish* button and you will be directed to the Ethernet Interface dialog window and the Interface Aliases table will be populated with the entered data.

Reboot: Will restart the system and apply all the settings upon reboot.

Revert: Will revert the settings in the dialog window back to the previous saved settings.

Save: The interface will not be activated or deactivated until the device is rebooted. This allows for other configuration changes to be made to the device which can be committed at a later time.

Apply: The current settings will be saved and the interface will either be activated or deactivated immediately. If the interface was already active, then it will be deactivate and reactivated using the configured settings just saved. If you were connected to the Web UI via this interface, an attempt will be made to re-connect to it using the new settings, when possible.

Applying new settings to the interface may result in disconnection, requiring reconnection using alternate methods.

Incomplete or incorrect network settings could render the device incommunicable and may require being able to connect either to the device directly or via the network to which it is attached.

Note: To configure the eth1 Interface, follow the steps documented for eth0.

Wi-Fi (WLAN) - (RAM-9631, RAM-9731 or RAM-9931 with factory option)

The Wi-Fi interface option is used to configure the parameters for Wi-Fi LAN Interface. From this option, the administrator may change wireless encryption settings as well as wireless network parameters.

Note: The Wi-Fi interface only supports Access Point Mode.

The RAM-9x31 unit's Wi-Fi capability is enabled by default. The factory default configuration will setup the following parameters:

SSID: Model Number - Last 6 digits of the Wi-Fi MAC address.

Channel: 7

Encryption: WPA PSK + WPA2 PSK

Passkey: (Serial Number after the dash)

For example, a unit identified as:

Model Number: RAM-9731

Wi-Fi MAC: 00:19:70:01:02:03

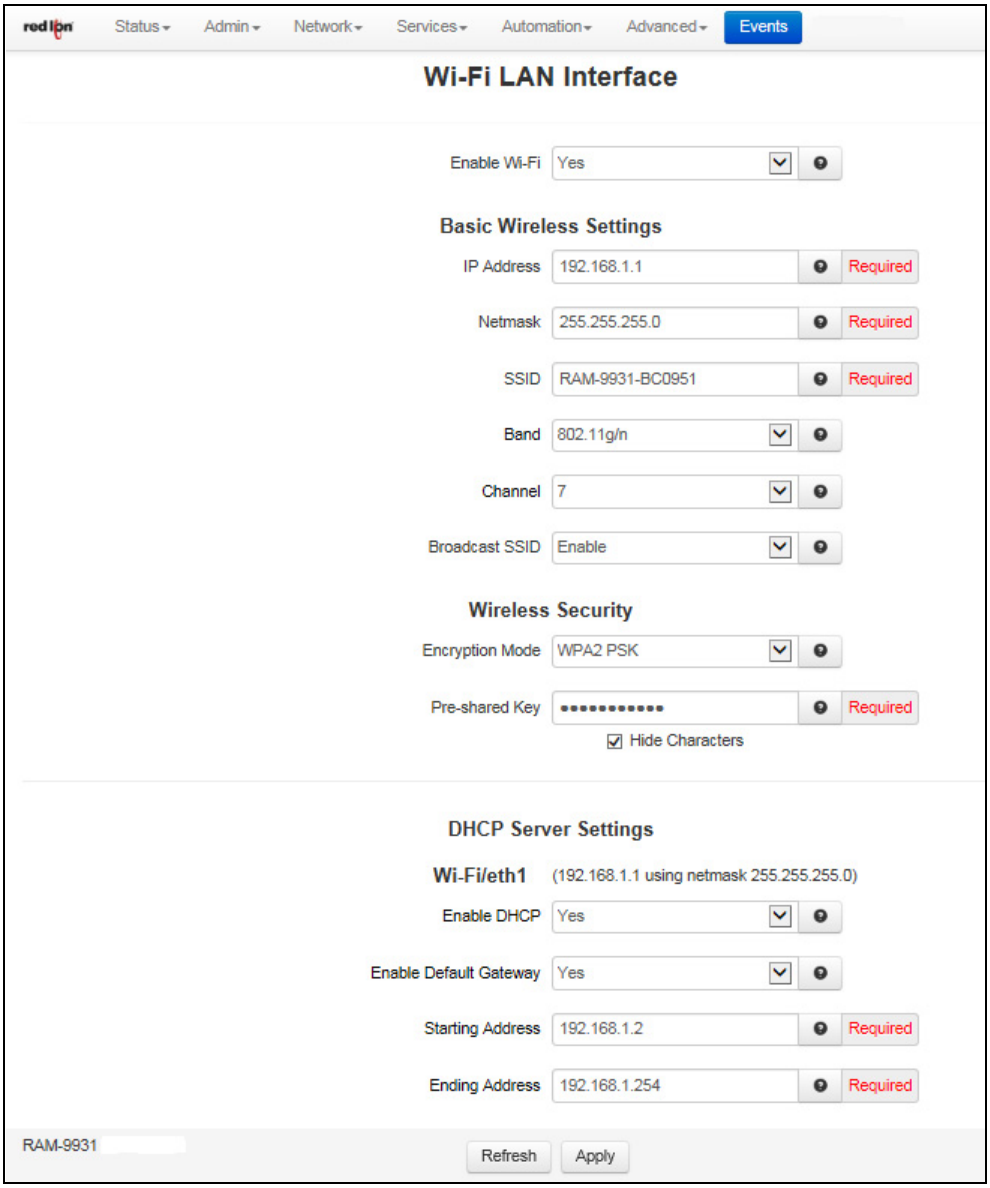
Serial Number: 973X-00000123456

Would have the values of:

SSID: RAM-9731-010203

Passkey: 00000123456

Wi-Fi LAN Interface



Enable WLAN Interface: Select ***YES*** to enable the Wi-Fi interface.

IP Address (Required): The wireless bridge IP Address is entered in this field. The IP Address identifies a device on the TCP/IP network. Every device on a network must have a unique address. The range of valid addresses for a given network and broadcast is determined by the value of the Netmask. Some addresses are reserved for special uses such as network and broadcast. Your Network Administrator should be able to provide an appropriate value. The default setting for this field is 192.168.1.1.

For example, if a netmask is 255.255.255.0 and the IP address assigned to the device is 192.168.1.3, then the range of valid addresses will be 192.168.1.1 through 192.168.1.254 as 192.168.1.0 is the value reserved for the network and 192.168.255 is the value reserved for the broadcast address.

Netmask (Required): Enter the desired Netmask for the wireless bridge interface. The default setting is 255.255.255.0. Your Network Administrator should be able to provide an appropriate value for this field.

SSID (Required): The SSID is a unique name for the wireless network. It is case sensitive and must not exceed 32 characters. All wireless devices in your network must use the same SSID. Verify that the correct SSID is being used and click the “Apply” button to set it.

Band: Select the wireless standard to use. Channel 14 is only permitted in 802.11b mode. If available in your region, use 802.11b to enable channel 14. Using 802.11g/n is recommended for best performance or use

802.11b/g for best compatibility with older clients.

Channel: Select the channel from the drop-down list that corresponds with your network settings. The available choices are between 1 and 11. All points in your wireless network must use the same channel in order to function correctly. The “Auto” option allows the chipset to select the channel on its own. Verify that the correct channel is selected and click the “Apply” button to set it.

Broadcast SSID: Allows the SSID to be broadcast on the network. Enabling this option makes it easier for clients to find the access point, but also allow attackers to know the name of your network. Select “Enable” to broadcast. Select “Disable” to increase network security and prevent the SSID from being seen on network PCs.

Encryption Mode: This option allows you to setup the wireless security using either WPA2 PSK, WPA2 PSK or WPA PSK and WPA2 PSK mode. If security is disabled, any client can connect to the Access Point. Turning on WPA requires clients to know an encryption key before connecting to the network.

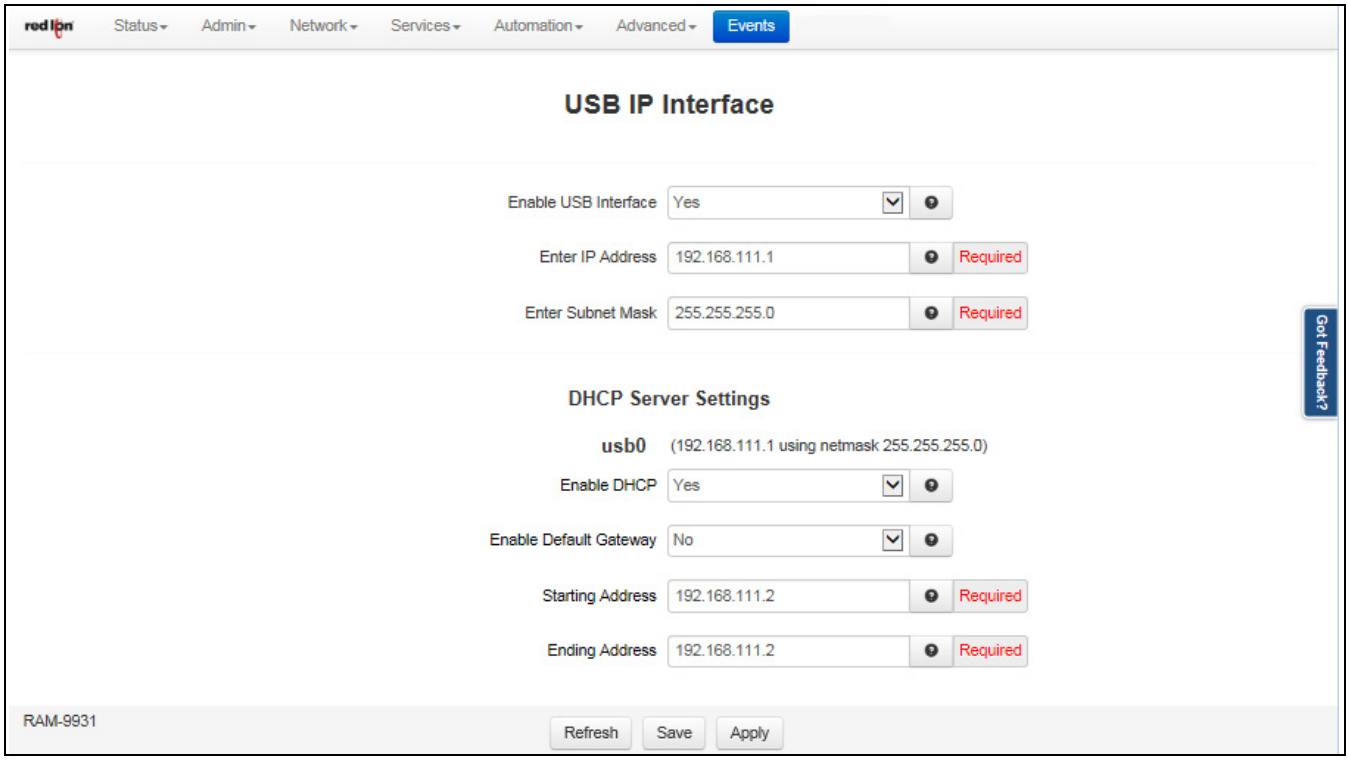
Pre-Shared Key (Required): This option is available when **WPA** types are selected as an option for **Encryption** and allow the user to specify the encryption key to be used. For WPA, this should be a passphrase of 8-63 printable ASCII characters. **WPA Pre-Shared Key:** This option allows the sender and recipient to share a secret key.

Click on the *Save* button for changes to be saved without activating the interface, the *Apply* button will save your settings and apply them immediately. To refresh the screen, click on the *Refresh* button.

USB

The USB interfaces menu item allows the administrator to configure the USB port of the Red Lion RTUs or routers to meet their needs. The default address is set for 192.168.111.1 with the subnet mask of 255.255.255.0

Click on the USB menu item and the USB IP Interface dialog window appears:



Enable USB Interface: Select ***YES*** to enable the USB interface. The recommended setting for this field is YES if using this interface.

Enter IP Address: Enter the desired interface IP address in this field. The IP Address identifies a device on a TCP/IP network. Every device on a network must have a unique address. The range of valid addresses for a given network is determined by the value of the Netmask. Some addresses are reserved for special uses such as network and broadcast.

For example, if a netmask is 255.255.255.0 and the IP address assigned to the device is 192.168.1.3, then the range of valid addresses is 192.168.1.1 through 192.168.1.254 as 192.168.1.0 is the value reserved for the network and 192.168.1.255 is the value reserved for the broadcast address.

The IP address should have been provided by your Network Administrator. It must be an address valid for the network described by the value contained in the **Enter Subnet Mask** field and must not conflict with any other device on the target network.

Enter Subnet Mask: Enter the desired Netmask for the interface in the field provided.

Your Network Administrator should be able to provide an appropriate value. This value determines the valid range of IP addresses allowed in the **Enter IP Address** field.

Click on the *Save* button for changes to be saved without activating the interface, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

IPv6

Enable IPv6: Selecting YES to this option will enable IPv6 routing for devices behind the RTU or router. RTU or Router Advertisement messages will be sent periodically to the specified LAN segment, and RTU or Router Solicitations will be responded to on that LAN segment only. A /64 real routable subclass will be available, based on the range provided by an upstream IPv6 RTU or Router on the WAN side. Each IPv6 device behind the RTU or router is responsible for its own IPv6 fire-walling.

This will not affect Neighbor Discovery nor Solicitation messages. Stateless Address Autoconfiguration (SLAAC) will also be unaffected. These local link addresses are always available.

WAN Interface: Specify the IPv6 upstream RTU or router path. If a unit has access to a real IPv6 RTU or router on multiple interfaces, you may specify it here. Cellular devices expect that the wwan0 interface will lead to the IPv6 RTUs or routers. Wired RTUs or Routers will expect that eth0 (default untrusted/external interface) may also lead to an upstream IPv6 RTU or router. The recommended setting for this option is *Auto*.

LAN Interface: The RTU or Router Advertisements are available for one /64 subclasses on one local LAN interface. You may choose a specific local interface if the default is not appropriate. You may not choose the same interface for the LAN that was setup for the WAN interface.

Click on the *Apply* button to save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

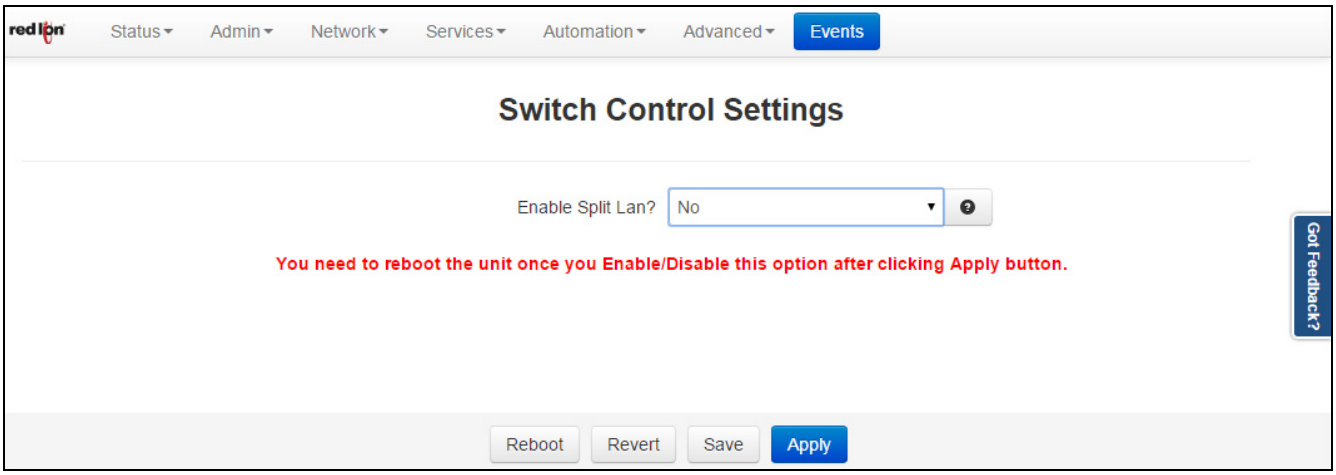
A reboot is required after changes to IPv6 routing configuration.

Switch Control

The purpose of the Switch Control function is to create a WAN/LAN separation This gives the user the ability to create a divided network with additional capabilities. This option only applies to units with the 5 port unmanaged switch (6x21).

Switch Control Settings

Enable Split Lan: This will alter the switch port allocations. When disabled, all switch ports 1-5 will be treated as a single LAN. This will be configurable as eth0 and will default to being a firewall trusted/internal interface.



When enabled, port 5 will be divided out as a WAN port, eth0 (firewalled as external/untrusted). Ports 1-4 will be an internally trusted LAN (eth1).

Warning: When switching modes, your firewall interface tables will be rebuilt and may need any custom changes reapplied. In addition, a USER INITIATED reboot is required to complete the mode switch.

Warning: When enabling switch mode, current Ethernet settings (eth0) will apply only to the single WAN port. On the front of the unit, this may be shown as <Port 5> under the power connector. The remaining four ports will be configured as a LAN (eth1). Custom VLANs will be unavailable for any Ethernet configuration while in Split LAN mode.

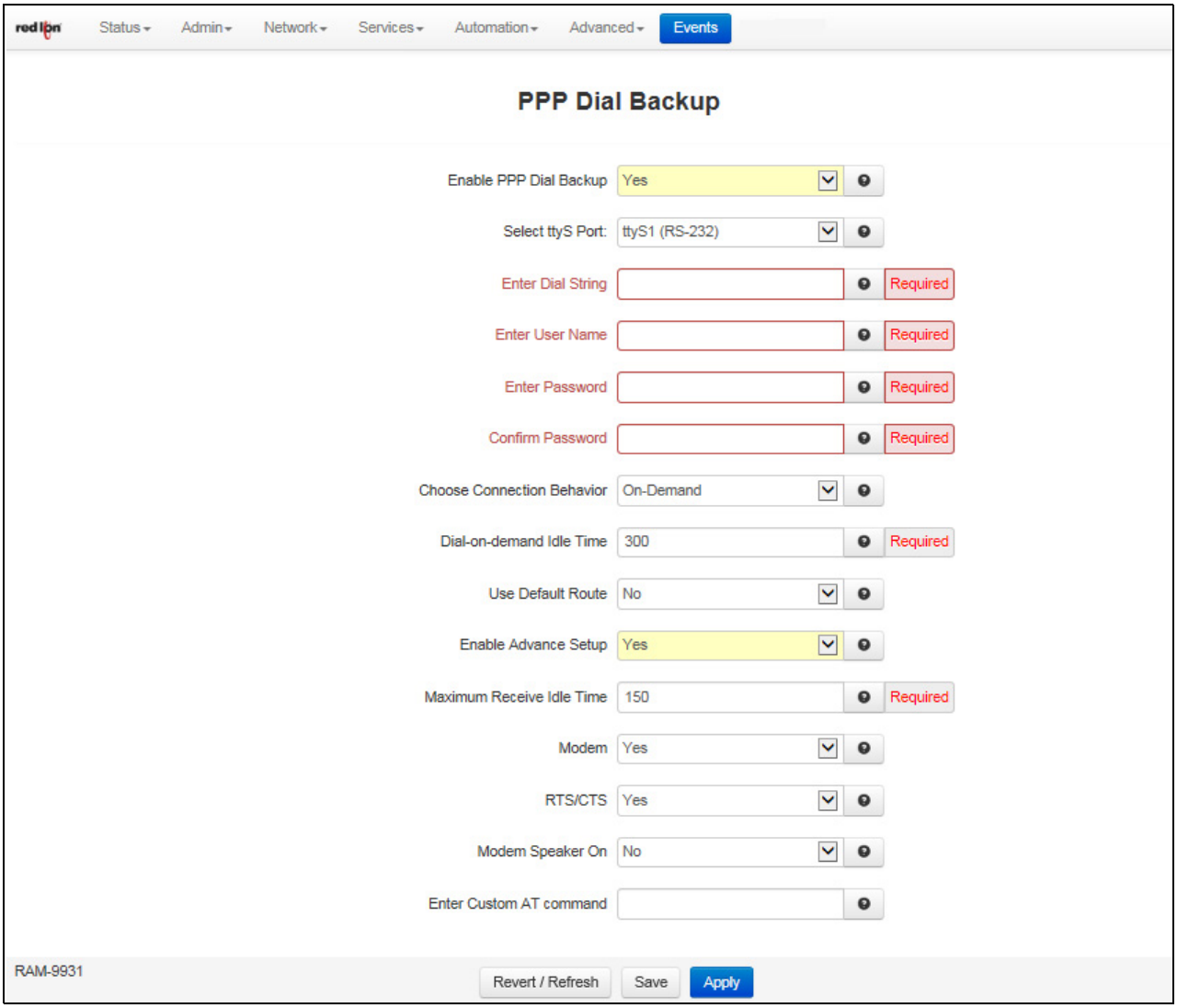
Please check your Ethernet connections to make sure that the new settings will not conflict with previous network configurations. You may need to revisit your Untrusted/Trusted interface lists in the **Firewall → General Settings**, as these will revert to new defaults (eth0 will be firewalled as Untrusted!). After Apply is clicked and you check firewall/ethernet configurations, a reboot is required to complete this process.

Click on the *Save* button for changes to be saved without activating the interface, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

PPP Dial Backup

The PPP Dial Backup menu item is used to configure the capability of an alternate connection by dialing into an ISDN should the primary RTU or router get interrupted.

Click on the *PPP Dial Backup* menu item and the PPP Dial Backup dialog window appears:



Enable PPP Dial Backup: Select ***YES*** to turn on the PPP Dial Backup and ***NO*** to turn off PPP Dial Backup.

Select ttyS Port: Select the ttyS port on which the modem is attached. For an external modem connected to a serial port, use the port name as labeled on the unit. For an internal modem, a common setting is ttyS3.

Enter Dial String (Required): Enter the phone number of the peer/ISP to dial.

Enter User Name (Required): Enter the name used for authenticating the local system to the peer. Please consult your ISP for these values.

Enter Password (Required): Enter the password to use for authenticating with the peer. Please consult your IPS for these values.

Confirm Password (Required): Re-type the password entered in the Enter Password field.

Choose Connection Behavior: In Persistent mode, the unit will always attempt to maintain a constant connection to the POTS network. In On-Demand mode, the connection to the POTS network will only be attempted when packets are destined to leave the modem's PPP interface. In addition, after a period of idle time, the connection will terminate.

Persistent: Select this option when the link is intended as a primary network connection.

On-Demand: Select this option when the link is intended as a fallback network connection.

Dial-on-demand Idle Time: is commonly chosen for an environment using an Ethernet connection as a primary interface, while IP Fallback is used to bring up this dial-up connection as a backup.

Use Default Route: Select *Yes* to use the peer as the default route. Select *Yes* when this link is intended as a primary network connection and *No* when this link is intended as a fallback network connection.

Enable Advance Setup: Select *Yes* to modify modem control, the modem speaker and enter modem initialization string. Select *No* to leave the advanced options as defaults.

Maximum Receive Idle Time (Required): Enter the number of seconds the connection may be allowed to remain "idle" or "unresponsive" (no data received) before closing the connection. If packets are leaving the interface, but no return packet is received for the specified time, then the connection is reset. This can be useful for detecting an unresponsive situation where the network is down, the modem is in an unknown state, or other low level error may have occurred.

Note: If the normal usage of the device regularly has packets leaving the unit with no expected response, then premature disconnections may result. Outgoing UDP packets with no expected response may be normal operation, yet will trigger this disconnection and reset.

Recommended Setting:

0 to turn off,
150 seconds (2.5 minutes) for normal operations (default)

Modem: Select *Yes* to use the modem control lines CD (Carrier Detect) and DTR (Data Terminal Ready). If you are having difficulty using your external modem, try alternating this value and re-testing.

RTS/CTS: Select *Yes* to set hardware flow control using RTS and CTS signals. If you are having difficulty using your external modem, try alternating this value and retesting.

Modem Speaker On: Select *Yes* to turn on the modem speaker for testing and proof of concept phase to audibly verify connection attempts. Select *No* for silent production mode.

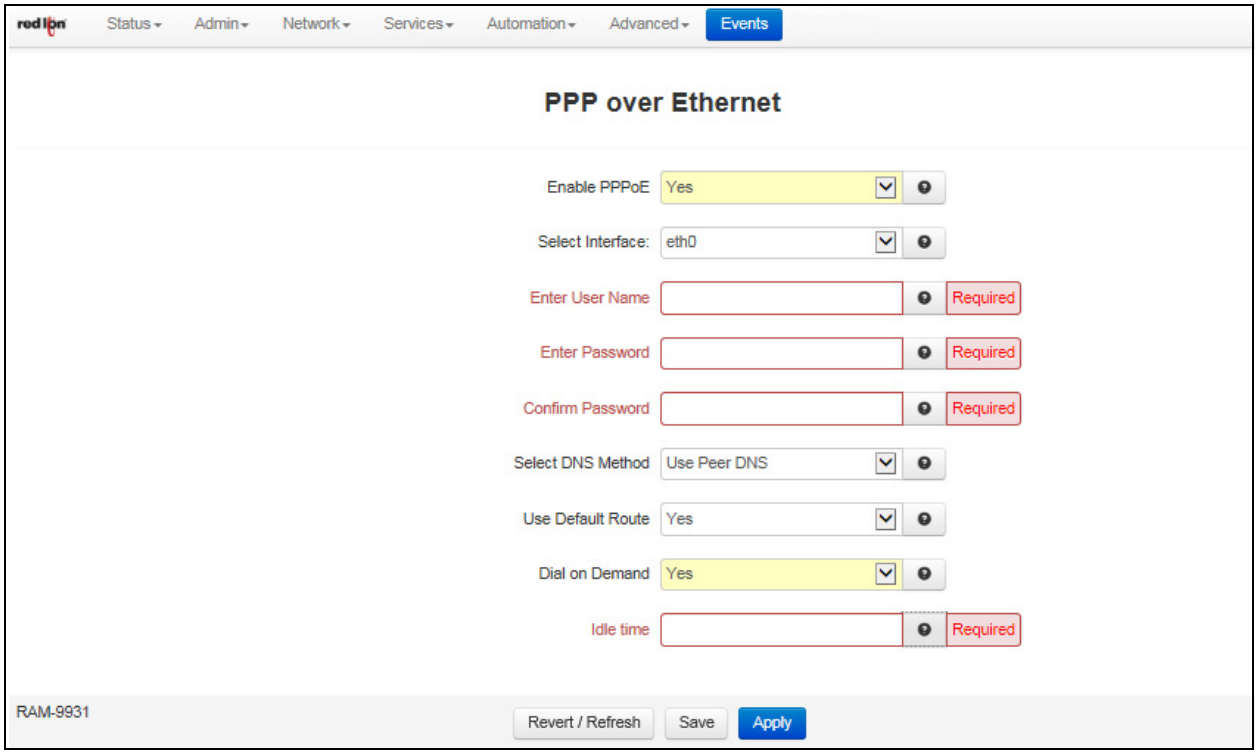
Enter Custom AT Command: Enter the modem initialization string. Please consult your modem AT Command documentation for unique initialization that may be required. Enter only a single initialization string.

Click on the *Save* button for changes to be saved without activating the interface, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

PPP over Ethernet

The PPP over Ethernet menu item is used to configure a connection by being able to connect a DSL or cable modem.

Click on the *PPP over Ethernet* menu item and the PPP over Ethernet dialog window appears:



Enable PPPoE: Select *Yes* to enable the PPP over Ethernet service on the specified interface when the Apply button is clicked. To disable the service, select *No* and click Apply.

Select Interface: Select the name of the Ethernet interface to which the PPP over Ethernet service should bind by choosing one of the options available in the provided drop-down list.

Enter User Name (Required): Enter the user name to be used with the PPPoE interface in the space provided. It is typically in the form *name@domain.com*.

Enter Password (Required): Enter the password to be used with the PPPoE interface in the space provided.

Confirm Password (Required): Re-input the password entered in the "Enter Password" field. This entry must match exactly the previously entered password.

Select DNS Method: Select the method by which DNS Server information should be obtained. The recommended setting for this field is "*Use Peer DNS*". Choices include:

> **Use Unit Default:** Do not obtain DNS information from PPPoE Server. Use settings from ***Network→DNS Settings*** instead.
>
> **Use Peer DNS:** DNS information should be obtained from the peer host once connected.
>
> **Use Custom DNS:** DNS information is entered manually in the fields which appear below.

Use Default Route: Select Yes to use this interface as the default route.

Dial on Demand: Select Yes to enable this feature. The recommended setting for this field is No.

Idle time: When Dial on Demand is enabled, an idle timeout (in seconds) may be entered in this field.

Click on the *Save* button for changes to be saved without activating the interface, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

3.4.3 Firewall

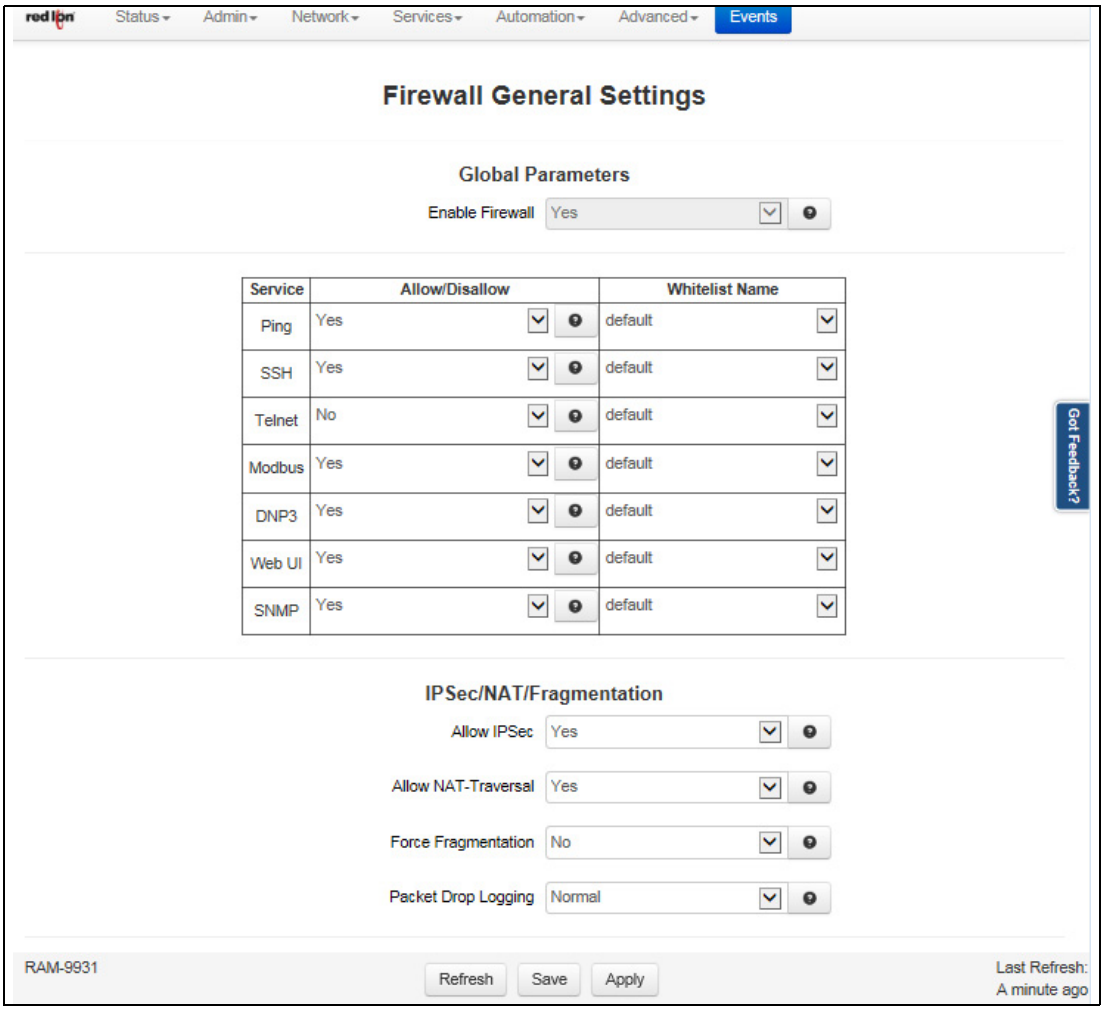
The Firewall menu item allows you to configure every aspect of the firewall on the Red Lion RTU or router.

The Firewall menu is organized in four (4) sub-sections: General Settings, ACL Rules, Masquerade/NAT/DMZ Rules, Port Allow/Forwarding Rules.

General Settings (Firewall)

The General Settings menu is used to configure common access services to the Red Lion RTU or router and configure how the interfaces are interpreted.

Click on the *General Settings* menu item.



Enable Firewall (Required): Specify whether to enable the firewall service on this device. The recommended setting for this field is *Yes*.

Note: Disabling the firewall will compromise security and routing functions of the unit.

Ping: To allow ICMP echo responses (*Ping*) from external devices through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this field is *Yes*.

To restrict access via a configured whitelist, select a whitelist name for the list of names available in the drop-down menu. **Note:** This setting will not override any firewall rules defined on other pages, such as service access or redirect rules.

Whitelist Name: Select the desired whitelist from the drop-down menu. Whitelists are created in the ***Network>Firewall>ACL Rules>Subnet>Whitelist Rules*** screen.

SSH: To allow external devices to connect to the SSH Server, via port 22, through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this field is *Yes*.

To restrict access via a configured Whitelist, click the check box marked **Use Whitelist** and then select a Whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined via the ***Network>Firewall>ACL Rules>Subnet Whitelist Rules*** screen.

Note: Setting this option to Yes does not enable the SSH server, it just allows it to be accessible via the firewall when it is enabled. The SSH Server may be enabled via the ***Services>SSH/TELNET Server*** screen.

If the SSH Server is configured to use a port other than 22, a rule specifically for the alternate port will need to be added via the Network>Firewall>Port Allow/Forwarding Rules>Service Access Rules screen.

Note: This setting will not override any firewall rules defined on other pages, such as service access or redirect rules.

SSH Whitelist Name: Select the desired whitelist for the drop-down menu. Whitelists are created in the **Network>Firewall>ACL Rules> Subnet Whitelist Rules** screen.

Telnet: To allow external devices to connect to the TELNET Server, via port 23, through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this field is *No*.

To restrict access via a configured whitelist, click the check box marked Use Whitelist and then select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined via the ***Network>Firewall>ACL Rules>Subnet Whitelist Rules*** screen.

Note: Setting this option to Yes does not enable the Telnet Server, it just allows it to be accessible via the firewall when it is enabled. The Telnet Server may be enabled via the Services>SSH/Telnet Server Screen.

Note: This setting will not override any firewall rules defined on other pages, such as service access or redirect rules.

Telnet Whitelist Name: Select the desired whitelist for the drop-down menu. Whitelists are created in the ***Network>Firewall>ACL Rules> Subnet Whitelist Rules*** screen.

Modbus: To allow external devices to connect to the local MODBUS Server through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this field is *No*. This defaults to port 502, but is controlled by the listening port chosen in the ***Automation>Modbus>Local Station*** screen.

To restrict access via a configured whitelist, click the check box marked **Use Whitelist** and then select a whitelist name for the list of names available in the drop-down list box provided. Whitelist may be viewed/defined via the ***Network>Firewall>ACL Rules>Subnet Whitelist Rules*** screen.

Note: Setting this option to Yes does not enable the MODBUS server, it just allows it to be accessible via the firewall when it is enabled. The MODBUS Server may be enabled via the A***utomation>ModBus>Forwarding*** screen.

Modbus Whitelist Name: Select the desired whitelist for the drop-down menu. Whitelists are created in the ***Network>Firewall>ACL Rules> Subnet Whitelist Rules*** screen.

DNP3: To allow external devices to connect to the DNP3 Server, via port 20,000, through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this field is *No*.

To restrict access via a configured whitelist, click the check box marked Use Whitelist and then select a whitelist name for the list of names available in the drop-down list box provided. Whitelists may be viewed/ defined via the ***Network>Firewall>ACL Rules>Subnet Whitelist Rules*** screen.

Note: Setting this option to Yes does not enable the DNP3 Server, it just allows it to be accessible via the firewall when it is enabled. Then DNP3 Server may be enabled via the ***Automation>DNP3>Physical Link Layer*** screen.

DNP3 Whitelist Name: Select the desired whitelist for the drop-down menu. Whitelists are created in the ***Network>Firewall>ACL Rules> Subnet Whitelist Rules*** screen.

Web UI: To allow external devices to connect to the Web Interface, through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this feature is *Yes*.

To restrict access via a configured whitelist, click the check box marked Use Whitelist and then select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/ defined via the ***Network>Firewall>ACL Rules>Subnet Whitelist Rules*** screen.

Note: This setting will not override any firewall rules defined on other pages, such as service access or redirect rules.

Web UI Whitelist Name: Select the desired whitelist for the drop-down menu. Whitelists are created in the ***Network>Firewall>ACL Rules> Subnet Whitelist Rules*** screen.

Allow SNMP Agent Access: To allow external devices to connect to the SNMP Agent, via port 161, through untrusted interfaces on this unit, select Yes; otherwise select No. The recommended setting for this feature is *Yes*.

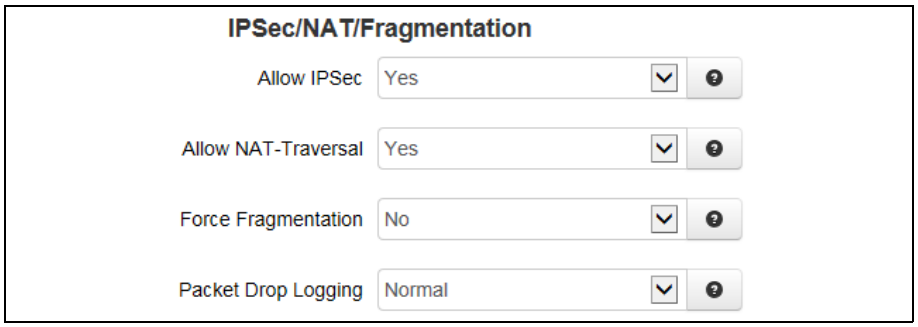
To restrict access via a configured whitelist, click the check box marked Use Whitelist and then select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/ defined via the ***Network>Firewall>ACL Rules>Subnet Whitelist Rules*** screen.

Note: Setting this option to Yes does not enable the SNMP Agent, it just allows it to be accessible via the firewall when it is enabled. The SNMP Agent may be enabled via the ***Services>SNMP Agent*** screen.

Note: This setting will not override any firewall rules defined on other pages, such as service access or redirect rules.

SNMP Whitelist Name: Select the desired whitelist for the drop-down menu. Whitelists are created in the ***Network>Firewall>ACL Rules> Subnet Whitelist Rules*** screen.

IPSec/NAT/Fragmentation



Allow IPSec: Specify whether to allow ESP data, as well as UDP port 500 to communicate with external devices through untrusted interfaces. The recommended setting for this field is *Yes*.

Note: This is necessary if you are planning to configure any IPSec tunnels originating from this device.

Allow NAT-Traversal (Required): Specify whether to allow data on UDP port 4500 on an untrusted interface. The recommended setting for this field is *Yes*.

Note: This is necessary if you are planning to run any IPSec tunnels through our device. This would support a unit behind a trusted interface to make an IPSec connection to a host beyond an untrusted interface.

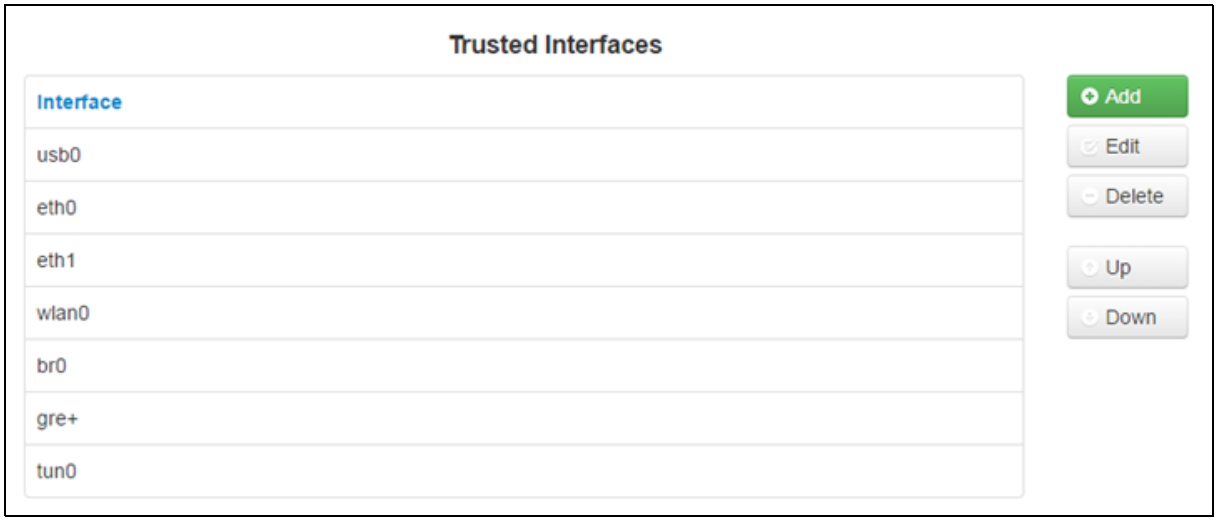
Force Fragmentation: When other hosts behind us send IP packets with the Don't Fragment (DF) bit set, enabling this option will clear the DF-bit before forwarding the packet. This allows upstream routers to fragment the packets if smaller MTUs are encountered along the way, but performance may be impacted for fragmentation and reassembly. If the DF-bit is set, then the packet will be dropped when smaller MTUs are encountered. This is useful if a mis-configured router is preventing PMTU discovery from operating properly. The recommended setting for this field is *No*.

Packet Drop Logging: This option controls the logging level of common packet drops. These messages normally appear in syslog. The three rate options are:

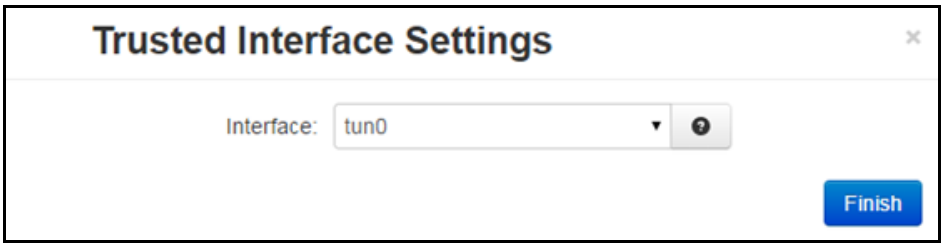
Normal: 2 messages per second max
Quieter: 10 messages per minute max
Silent: No messages are logged.

Trusted Interfaces

Identifies the trusted (internal) interface. Traffic from this interface will be permitted outbound. Default is “WAN/eth0”.



Click on the *Add* button for Trusted Interfaces and the following dialog window appears:



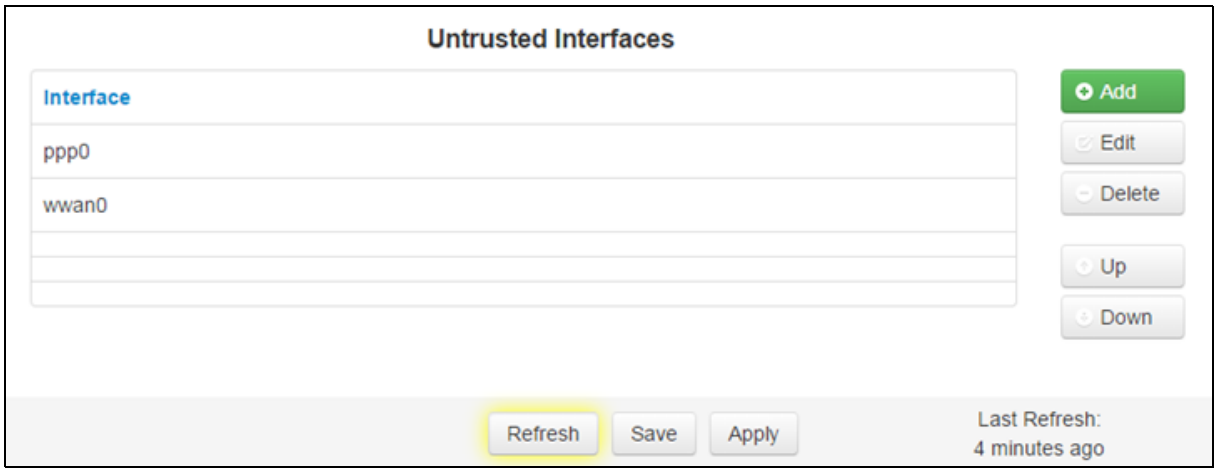
Interface: Choose an interface from the drop-down list provided. You may add as many interfaces as exist on the device. Each selection must be unique.

Trusted interfaces will not block traffic to/from devices connected to that interface. Filter Rules are the only rules that will control traffic on these interfaces.

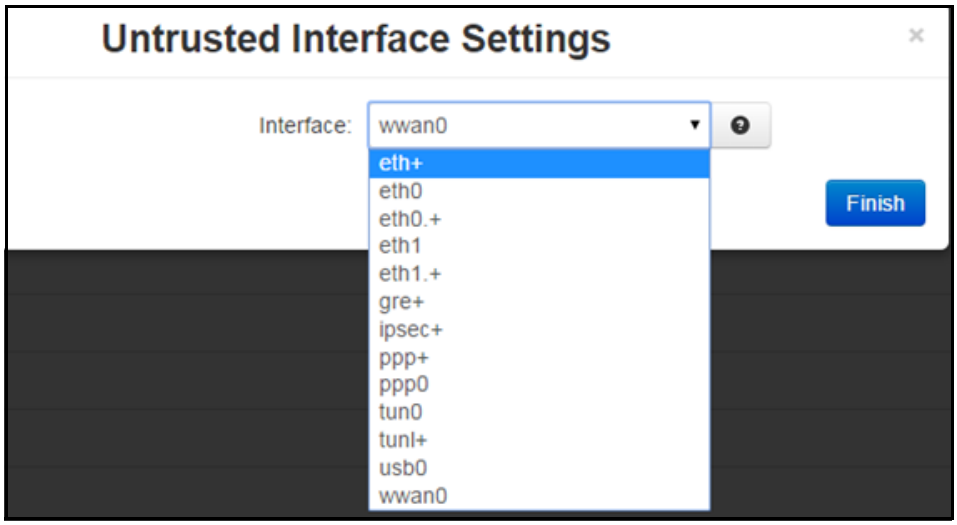
Click on the *Finish* button to populate the Trusted Interface screen.

Untrusted Interfaces

Identifies the Primary Untrusted (external) Interface and the following pop-up window appears:



Click on the *Add* button for Untrusted Interface and the following pop-up dialog window appears:



Interface: Choose an interface from the drop-down list provided. You may add any number of interfaces, up to as many exist on the device. Each selection must be unique.

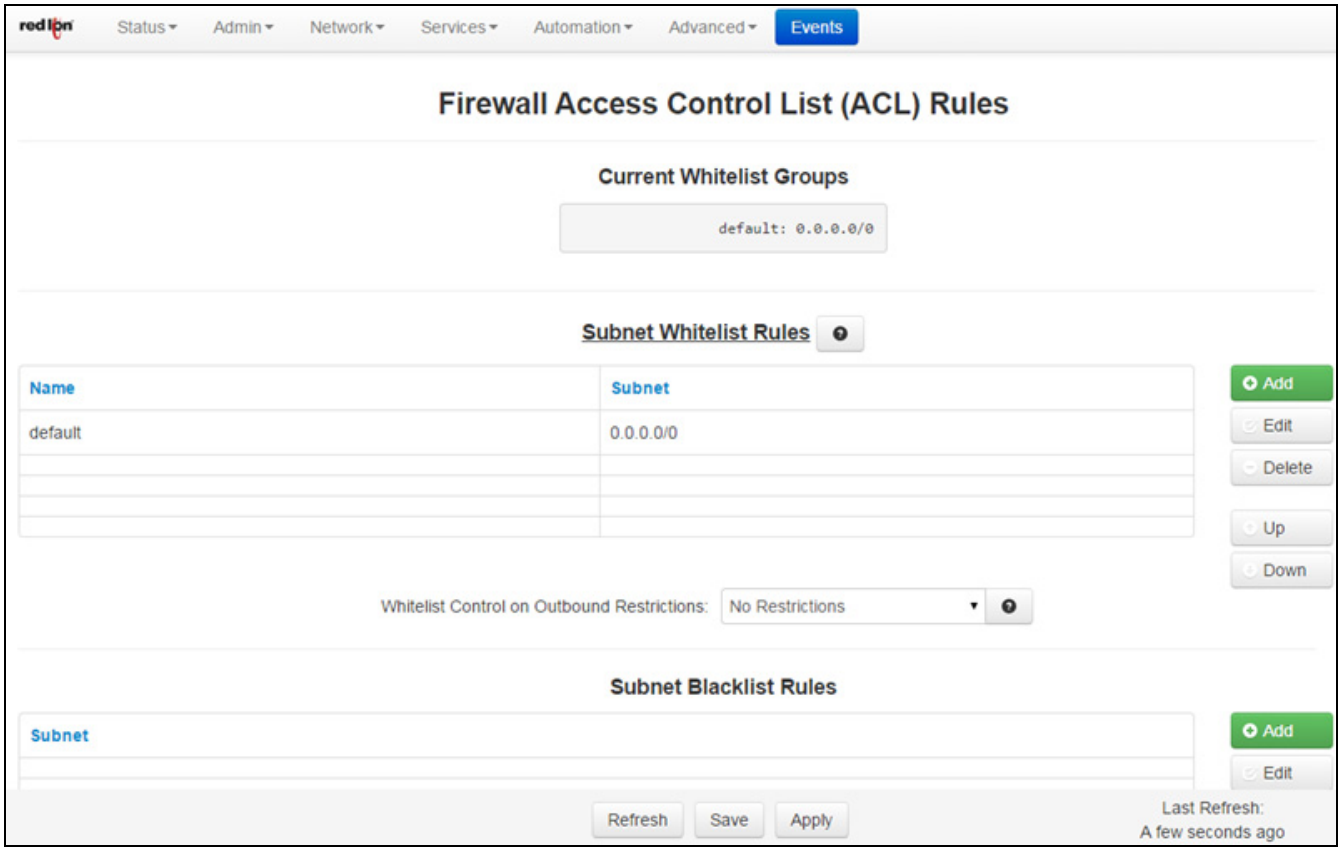
Untrusted interfaces will block all incoming traffic from devices/networks connected to this interface. Exceptions must be defined in firewall rules to allow traffic (General Settings, Allow/Redirect, etc.)

Click on the *Finish* button to populate the Untrusted Interface screen.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

ACL Rules - Firewall Access Control List Rules

From the ACL Rules dialog window, Whitelist and Blacklist rules are defined. Whitelist Rules are used to define a single IP Address or an entire network that would be allowed to access the network behind the Red Lion RTU or router. Blacklist Rules are used to define a single IP Address or an entire network that are *NOT* allowed to access the network behind the RTU or router.



Current Whitelist Groups: This field is populated by the information entered in the Subnet Whitelist Rules Section.

Subnet Whitelist Rules: Whitelist rules are available to define different populations of IP ranges, in order to give those IPs various permissions. Whitelist rules can be attached to many other rules in various sections to provide a targeted application of those rules to apply to only those subsets.

To create a whitelist with more than one IP range, enter multiple entries with the same whitelist name. Entries need not be contiguous. A compiled view of whitelists is available in this section.

You may not delete the "default" whitelist, but you may alter the entries for the "default" group by editing the existing entry and adding new entries for this list. 0.0.0.0/0 will match all IP ranges. Standard CIDR rules apply to specifying ranges.

Universally blocked ranges can be entered into the blacklist section and do not need to be attached to any specific rules.

Click on the *Add* button and the following dialog window appears:

Enter Whitelist Name (Required): Enter a name for the whitelist in the space provided. If the name of an existing whitelist is entered, then you are in effect adding another member to the list of subnets defined by that whitelist group.

After the Finish button is clicked, the entry will be added to the group in the (sorted) display area under the Current Whitelist Groups heading.

This whitelist name will become available for selection in the other Firewall Rules sections where a whitelist can be selected. ***Note:*** *The first whitelist entry, the 'default' entry may not be deleted or have its name changed, but its subnet value may be changed. Additional entries may be added, edited and deleted as needed.*

Enter Subnet (Required): Enter the network allowed to make connections to the above port(s), using IP/CIDR notation. To allow data from any source, enter 0.0.0.0/0. To specify a single host, use x.x.x.x/32, where x.x.x.x is the host's IP address.

Click on the *Finish* button. You will be returned to the Firewall Access Control List (ACL) Rules dialog window and the Subnet Whitelist Rules table will now be populated with the recently entered data.

To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

Whitelist Control on Outbound Restrictions: This setting controls whether or not the whitelist rules apply to packets originating from this device and being routed through the device. There are two (2) choices:

Only to Whitelist IPs from local: Packets that originate locally from the device that are destined for subnets outside those specified in any whitelist will be suppressed by the firewall.

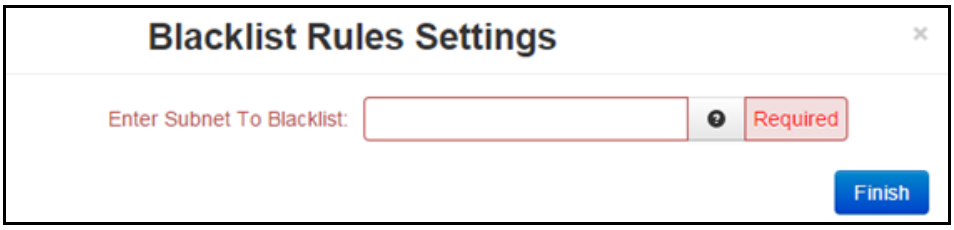
No Restrictions: The device may send a packet to any subnet and the whitelist rules apply only to packets received.

Note: ICMP traffic and UDP destination port 67 are omitted and will bypass whitelists. Failing to allow DNS IPs, will keep DNS from resolving addresses.

Whitelists may still be attached to specific rules in the firewall to further refine allowed networks.

Subnet Blacklist Rules: These rules are used to define a single IP Address or an entire network that are <u>*NOT*</u> allowed to access the network behind the Red Lion RTU or router.

Click on the *Add* button and the following window appears:



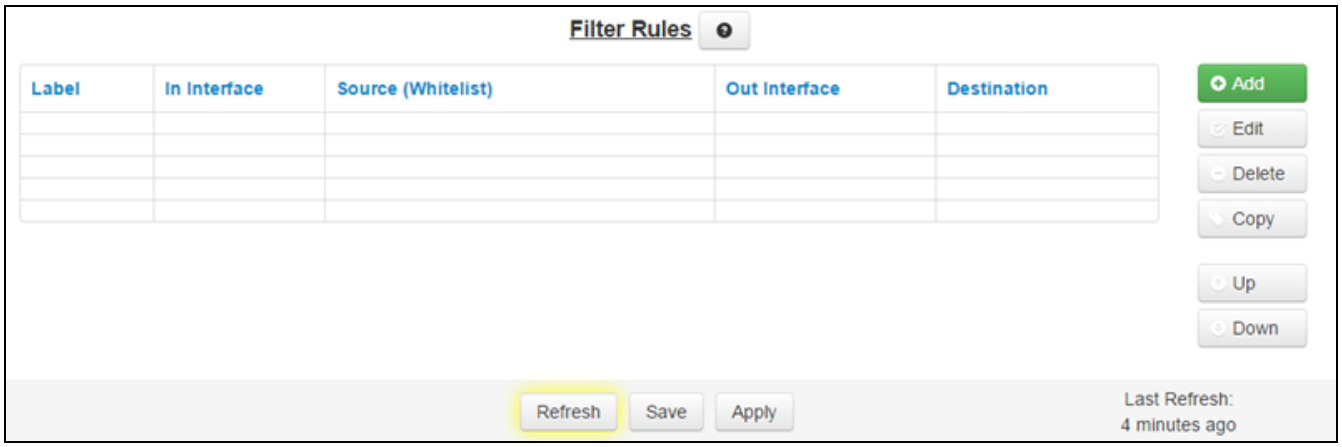
Enter Subnet To Blacklist (Required): Enter the network to be banned from making any incoming or outgoing connections, using IP/CIDR notation. To allow data from/to any source, enter 0.0.0.0/0. To specify a single host, use x.x.x.x/32, where x.x.x.x is the host's IP address. This will override any other sections rules (Allow/Redirect/DMZ/NAT/etc).

Click on the *Finish* button. You will be returned to the Firewall Access Control List (ACL) Rules dialog window and the Subnet Blacklist Rules table will now be populated with the recently entered data.

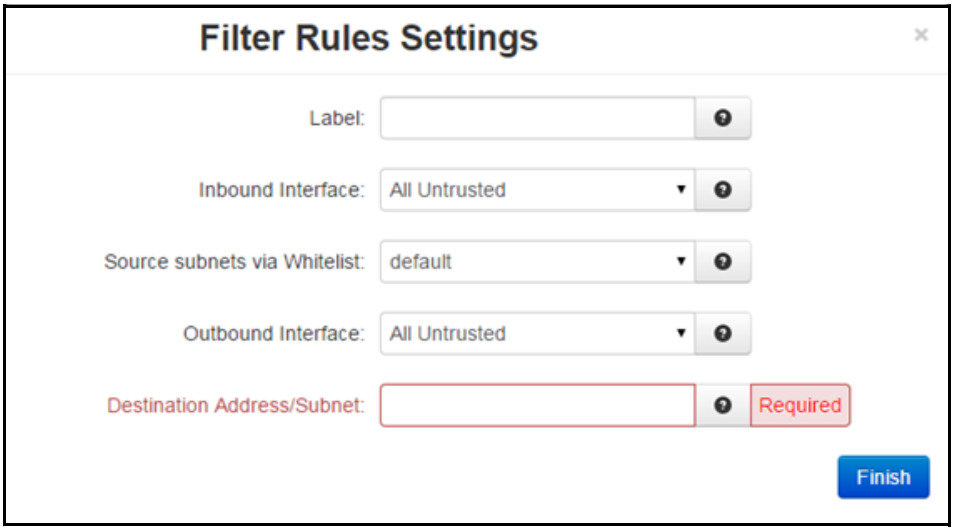
To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

Filter Rules: Trusted interfaces are by default trusted, and do not have restrictions. Filter rules allow setting up specific paths that are allowed to communicate, applying even to trusted interfaces. This allows restricting traffic between internal, trusted (LAN) interfaces and can also restrict general traffic to untrusted (LAN) interfaces.

Note: Once any filter is configured for restricting traffic, ALL traffic is then dropped that does not match the filter(s) for specified interfaces. IPSec traffic for VPN tunnels can also be filtered using these rules.



Click on the *Add* button and the following dialog window appears:



Inbound Interface: Select an interface associated with the Source Address/Subnet from the drop-down menu.

Source Subnets via Whitelist: Select a whitelist name for the list of names available in the drop-down menu. Whitelists are defined in the ***Network>Firewall>ALC Rules>Subnet Whitelist Rules*** screen.

Outbound Interface: Select the interface associated with the Destination Address/Subnet.

Destination Address/Subnet (Required): Enter the network to which the firewall allows access from the Outbound Interface.

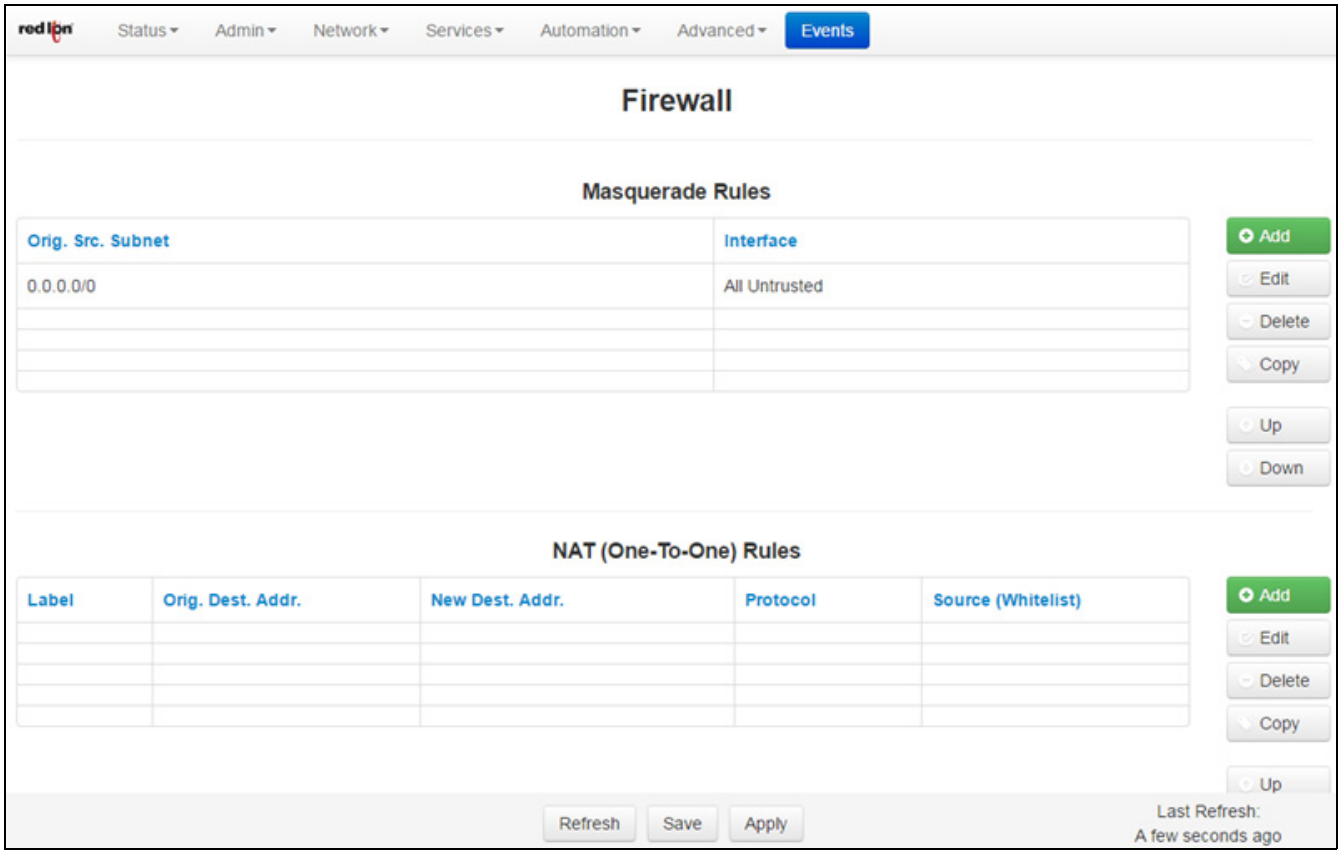
Click on the *Finish* button. You will be returned to the Firewall Access Control List (ACL) Rules dialog window and the Filter Rules table will now be populated with the recently entered data.

To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

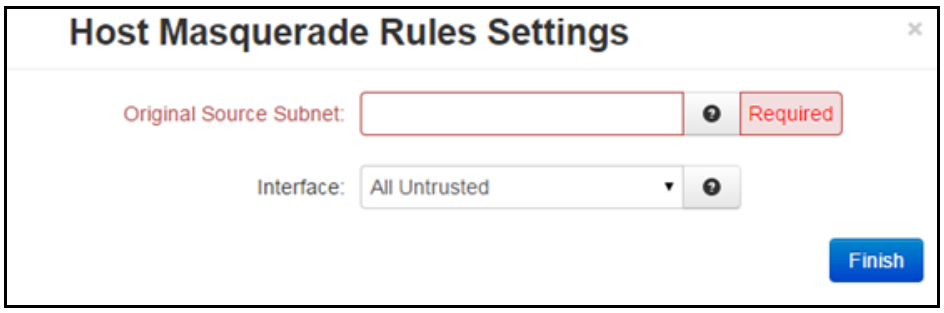
Masquerade/NAT/DMZ Rules

DMZ rules are used to configure rules to route through a Demilitarized Zone (DMZ), Masquerade rules are used to configure an interface to give all IP Addresses on a local network access to the Internet, while NAT(Network Address Translation) rules provide access to the Internet through a single machine that translates the IP addresses.



Masquerade Rules: The MASQ rules enable access to the Internet through a single unit/interface that translates the IP addresses. The unit itself has one or more IP addresses, but all the IP's behind the MASQ have 'private' Internet addresses.

Click on the *Add* button and the following dialog window appears:



Original Source Subnet (Required): Enter the subnet, using IP/CIDR notation that will be masqueraded out of a specific interface. All traffic that is sourced from this subnet and that is destined to go out the specified interface will be masqueraded with the source IP address of the interface specified.

Interface: Select the desired interface through which you wish to masquerade source addresses from the drop-down menu.

Click on the *Finish* button. You will be returned to the Masquerade/NAT/DMZ Rules dialog window and the Masquerade Rules table will now be populated with the recently entered data.

To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

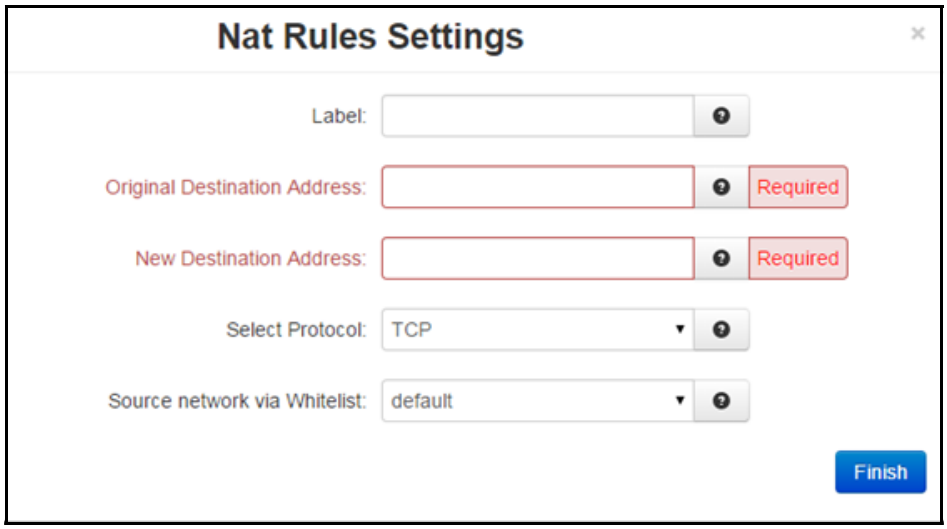
NAT (Network Address Translation) Rules: The NAT Rules enables access to the Internet through a single machine that translates the IP addresses. The NAT itself has one or more IP addresses, but all the machines behind the NAT have 'private' Internet addresses.

One-to-One NAT will perform a complete forwarding of app ports on the Original Destination IP to a new IP address entered in New Destination. Because the Original Destination need not be configured on this RTU or router, an interface is not required to setup.

One-to-One NAT Range will perform the same operation as a single One-to-One rule, but over a range of matched IP Addresses. The pool defined by the Original IP Start → End (the first Original IP will always translate to the first New IP, the second to the second, etc). The number of entries in each pool must match.

NAT (One-to-One) rule

Click on the *Add* button and the Nat Rules Settings following pop-up window appears:



Label: Enter a description to describe this NAT Rule. This field is not required for NAT Rules functionality and it is just for NAT Rule identification. Supported characters are alphanumeric plus the following special characters: _@-./',;:?~! #$%^&

Original Destination Address (Required): This field holds the address being transformed by NAT, the IP seen by a remote host. This address may be owned by an interface on this device or an unowned/fake range with a corresponding route (static or default). One-to-one NAT will perform a complete forwarding of all ports on the Original Destination IP to a new IP address entered in New Destination. Both fields can be any valid IP. Neither need to be already present/configured/owned on a local interface of this device. Ports 1-19 are excluded.

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.

New Destination Address (Required): This field holds the real LAN IP of the destination device behind this RTU or router. One-to-one NAT will perform a complete forwarding of all ports on the Original Destination IP to a new IP address entered in New Destination. Both fields can be any valid IP. Neither need to be already present/configured/owned on a local interface of this device. Ports 1-19 are excluded.

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.

Select Protocol: Choose the protocol type for this port's data. Options are TCP, UDP, All.

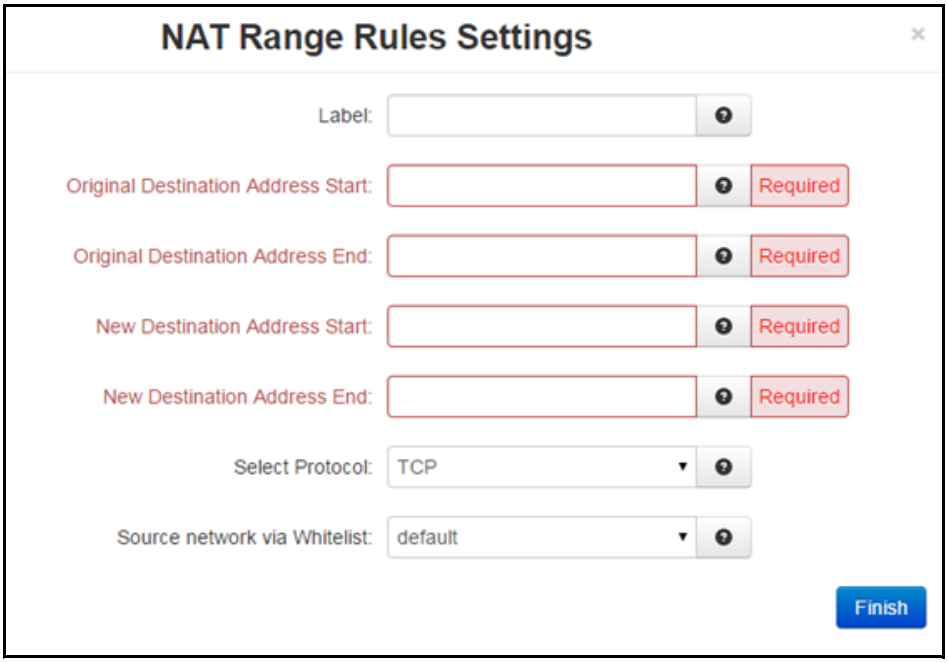
Source network via Whitelist: Select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined via the **Network/Firewall/ACL Rules** screen.

Click on the *Finish* button. You will be returned to the Masquerade/NAT/DMZ Rules dialog window and the NAT Rules table will now be populated with the recently entered data.

To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

NAT Range Rules

Click on the *Add* button and the following pop-up window appears:



Label: Enter a description to describe this NAT Range Rule. This field is not required for NAT Range Rules functionality and it is just for NAT Range Rule identification. Supported characters are alphanumeric plus the following special characters: _@-./',;:?~! #$%^&

Original Destination Address Start (Required): This field holds the starting address range being transformed by NAT, the IP's seen by a remote host.

This address may be owned by an interface on this device, oran unowned/fake range with a corresponding route (static or default). One-to-one NAT Range will perform a complete forwarding of all ports on the starting Original Destination IP to a starting new IP address entered in the New Destination Address Start field. Both fields can be any valid IP. Neither need to be already present/configured/owned on a local interface of this device. Ports 1-19 are excluded.

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.

Original Destination Address End (Required): This field holds the ending address range being transformed by NAT, the IP's seen by a remote host.

This address may be owned by an interface on this device, or an unowned/fake range with a corresponding route (static or default). One-to-one NAT Range will perform a complete forwarding of all ports for the range of starting/ending Original Destination IP's to a range of starting/ending New Destination IP addresses entered in New Destination Address Start and New Destination Address End fields. Both fields can be any valid IP. Neither need to be already present/configured/owned on a local interface of this device. Ports 1-19 are excluded.

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.

New Destination Address Start (Required): This field is used to hold the starting range of real LAN IP of the destination device behind this RTU or router.

One-to-One NAT Range will perform the same operation as a single One-to-One Rule, but over a range of matched IP Addresses. The pool defined by the Original IP Start→End, will be matched to the pool defined by New IP Start→ End (the first Original IP will always translate to the first New IP, the second to the second, etc.). The number of entries in each pool must match. Both fields can be any valid IP. Neither need to be already present/configured/owned on a local interface of this device. Ports 1-19 are excluded.

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.

New Destination Address End (Required): This field is used to hold the ending range of real LAN IP of the destination device behind this RTU or router.

One-to-One NAT Range will perform the same operation as a single One-to-One rule, but over a range of matched IP Addresses. The pool defined by the Original IP Start→End, will be matched to the pool defined by New IP Start→End (the first Original IP will always translate to the first New IP, the second to the second, etc.). The number of entries in each pool must match. Both fields can be any valid IP. Neither need to be already present/configured/owned on a local interface of this device. Ports 1-19 are excluded.

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.

Select Protocol: Choose the protocol type for this port's data. Options are TCP, UDP, All.

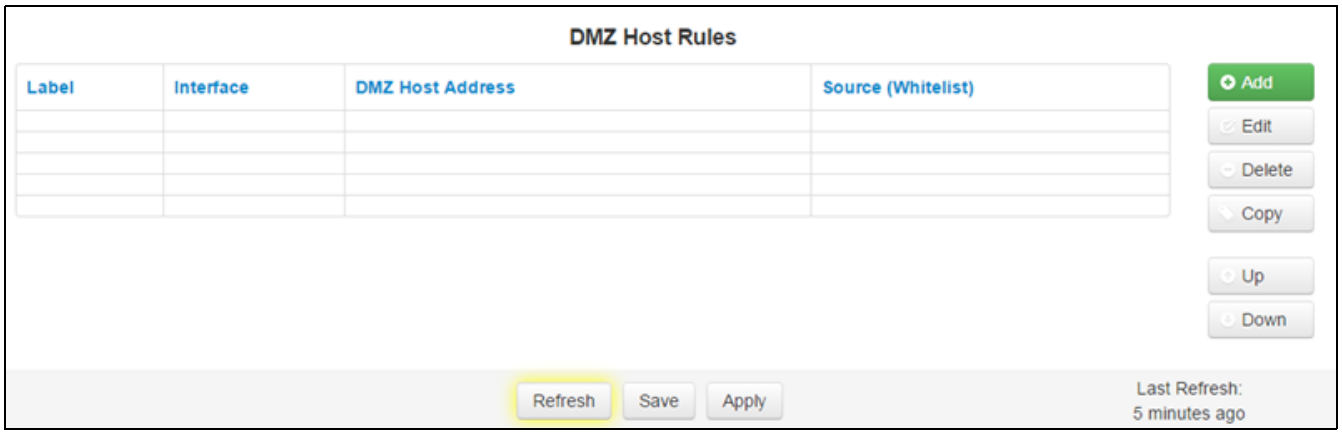
Source Network via Whitelist: Select a whitelist name for the list of names available in the drop-down list. Whitelists may be viewed/defined via the **Network/Firewall/ACL Rules** screen.

Click on the *Finish* button. You will be returned to the Masquerade/NAT/DMZ Rules dialog window and the NAT Rules table will now be populated with the recently entered data.

To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

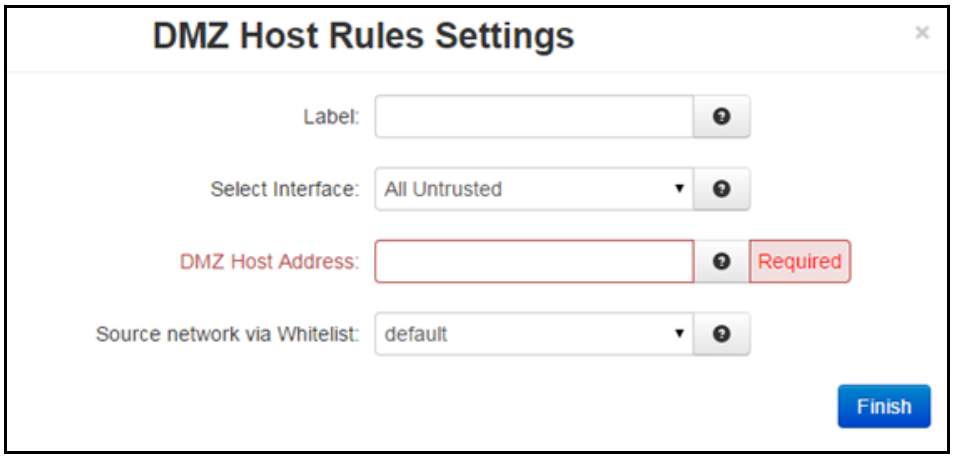
DMZ Rules

DMZ rules are used to configure routes through a Demilitarized Zone (DMZ).



To add a DMZ host rule

Click on the *Add* button and the following dialog window appears:



Label: Enter a description to describe this DMZ Rule. This field is not required for DMZ Rules functionality and it is just for DMZ Rule identification. Note: Supported characters are alphanumeric plus the following special characters: _@-./',;:?~! #$%^&

Select Interface: Click on the pull down-down menu to choose an interface that will be forwarded to a DMZ Host. All incoming packets (TCP/UDP/ICMP/etc) will be forwarded to the DMZ Host specified.

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the DMZ Host.

DMZ Host Address (Required): Enter the IP address of the DMZ Host. This IP address will receive all packets destined for the interface specified. ***Note:*** *Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the DMZ Host.*

Note: Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the DMZ Host.

Source subnets via Whitelist: Select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined via the **Network/Firewall/ACL Rules** screen.

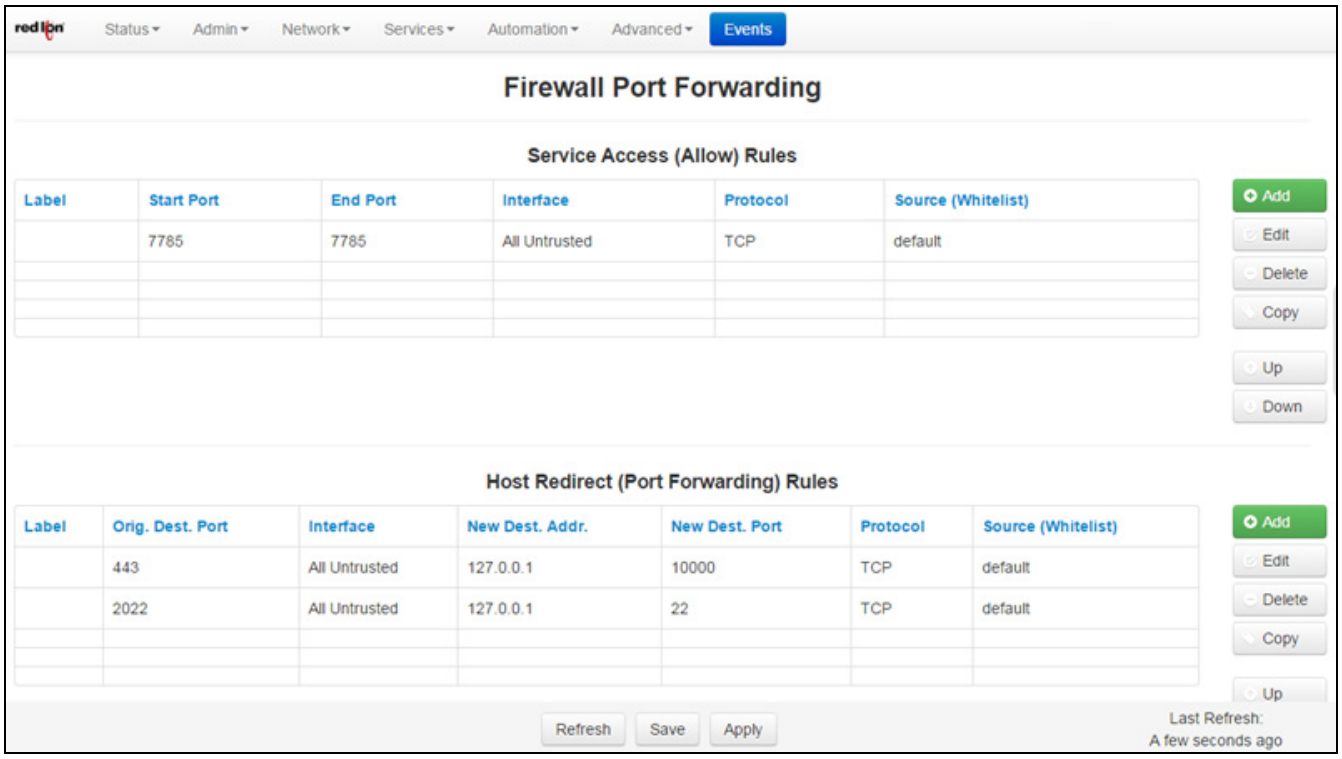
Click on the *Finish* button. You will be returned to the Masquerade/NAT/DMZ Rules dialog window and the NAT Rules table will now be populated with the recently entered data.

To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

Port Allow/Forwarding Rules

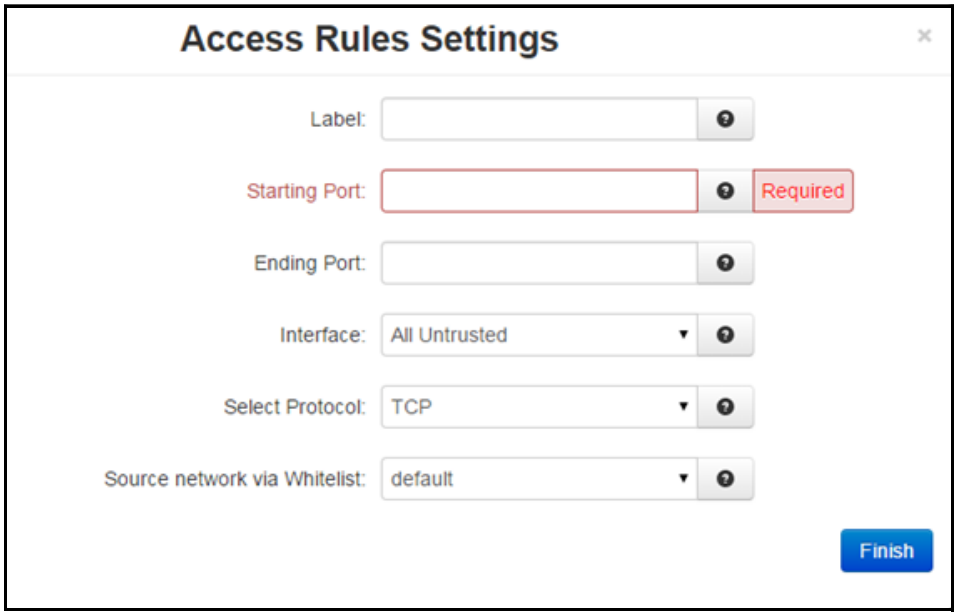
The Firewall Port Forwarding is used to configure routes from a small range of IP Addresses or all IP Addresses through one or more interfaces to a designated IP Address located behind the Red Lion RTU or router.



Service Access (Allow) Rules: The Service Access Rules option is used to define what ports, either as a single port or a range of ports, are authorized access through the firewall on the Red Lion RTU or router.

To add a new Service Access Rule.

Click on the Add button and the following dialog window:



Label: Enter a description to describe this Allow Rule. This field is not required for Allow Rules functionality and it is just for Allow Rule identification. Supported characters are alphanumeric plus the following special characters: _@-./',;:?~! #$%^&

Starting Port (Required): Enter the starting TCP or UDP port number for this rule.

Note: If adding only one port, enter it here.

Ending Port (Required): Enter the ending TCP or UDP port number for this rule.

Note: If adding only one port, please omit this entry.

Interface: Select the interface on which this port will be opened. Incoming connections to this interface will be allowed into the device. ***Note:*** *For connections destined to a device beyond this unit, use Host Redirect, NAT or DMZ rules instead.*

Select Protocol: Choose the protocol for the type of data you want to allow.

Source Network via Whitelist: Select a whitelist name from the list of names available in the drop-down list. Whitelists may be viewed/defined in the via the **Network/Firewall/ACL Rules** screen.

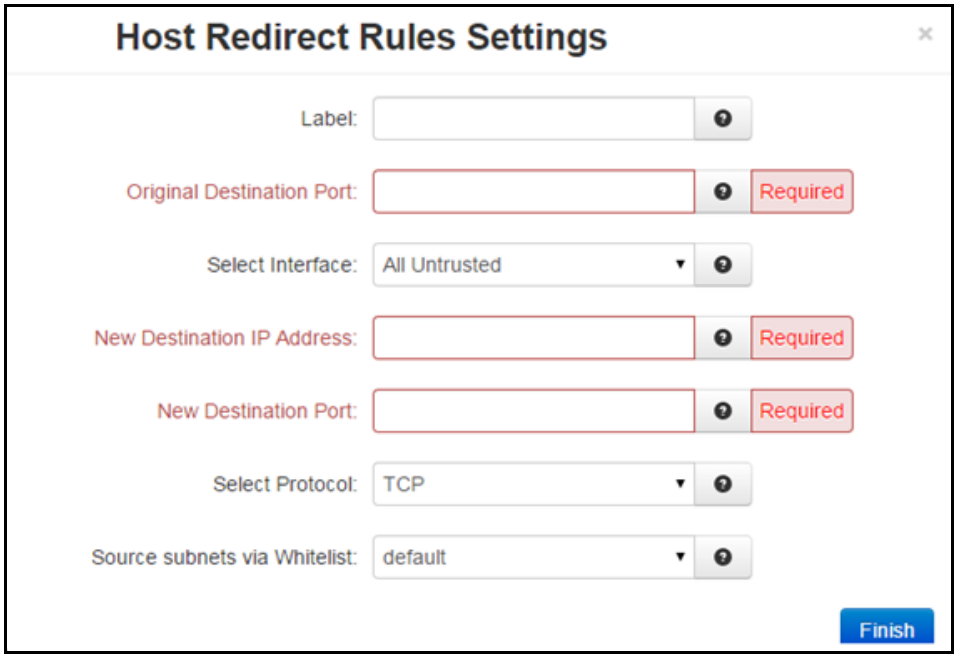
Click on the *Finish* button. You will be returned to the Firewall Port Forwarding dialog window and the Service Access (Allow) Rules table will now be populated with the recently entered data.

To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

Host Redirect (Port Forwarding) Rules: The Host Redirect Rules option is used to configure port forwarding rules that permit ports on external, untrusted interfaces to be passed to ports on internal hosts on the same or different ports.

Click on the *Add* button on the following dialog window appears:



Label: Enter a description to describe this Redirect Rule. This field is not required for Redirect Rules functionality and it is just for Redirect Rule identification. Supported characters are alphanumeric plus the following special characters: _@-./',;:?~! #$%^&

Original Destination Port (Required): Enter the port that an external device will try to connect to. This is the port that will be open on the specified interface.

Select Interface: Select the interface on which to open the specified port. Incoming connections will be allowed.

New Destination IP Address (Required): Enter the IP Address that the incoming connection will be redirected to. This can be an IP Address within or beyond this device.

New Destination Port (Required): Enter the port that the incoming connection will be redirected to. This may be the same number as the Original Destination Port.

Select Protocol: Choose the protocol type for this port's data. Options are TCP and UDP.

Source Subnets via Whitelist: Select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined in the via the **Network/Firewall/ACL Rules** screen.

Click on the *Finish* button. You will be returned to the Firewall Port Forwarding dialog window and the Host Redirect (Port Forwarding) Rules table will now be populated with the recently entered data.

To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

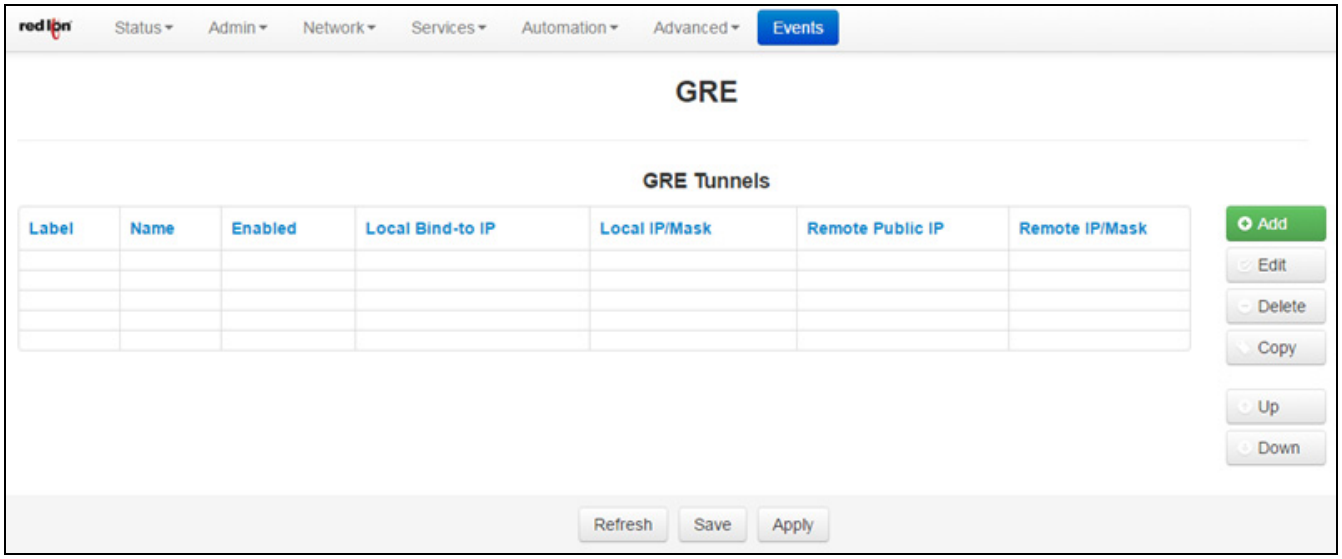
3.4.4 Tunneling

The Tunneling menu is divided into two (3) sub-sections: GRE Tunnels, IP in IP Tunnels and IPSec.

GRE Tunnels (Generic Routing Encapsulation)

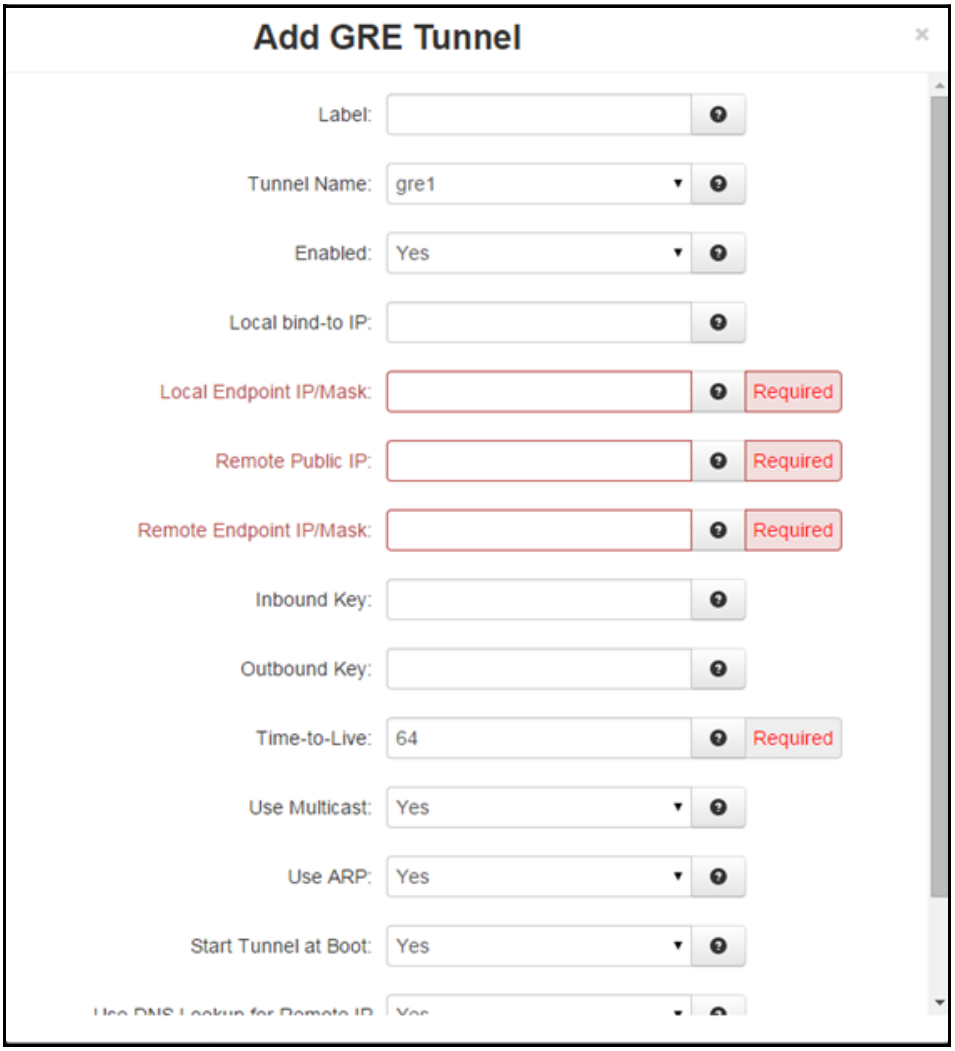
The GRE Tunnels menu item is used to configure a GRE Tunnel. GRE is a tunneling protocol that was originally developed by Cisco. It can do a few more things than IP-in-IP tunnelling. For example, you can also transport multicast traffic and IPv6 through a GRE tunnel.

Click on the *GRE Tunnels* menu item and the GRE dialog window appears:



To add a GRE Tunnel:

Click on the *Add* button and the Add GRE Tunnel pop-up window appears:



Label: Enter a description to describe this tunnel. This field is not required for GRE tunnel functionality and it is just for tunnel identification. Supported characters are alphanumeric plus the following special characters: _@-./',;:?~! #$%^&

Tunnel Name: Select the name of the GRE name by choosing one of the options available in the provided drop-down list.

Enabled: Select Yes to enable the tunnel.

Local bind-to IP: Set the local bind IP address for tunneled packets. This field is optional.

> **Note:** If supplied, the Local IP Address must be an address on another interface of this host. If not supplied, tunneled packets can be received from any interface.

Local Endpoint IP/Mask (Required): Set the local GRE IP Endpoint IP/mask.

Remote Public IP (Required): Set the Remote Public IP for this GRE connection.

Remote Endpoint IP/Mask (Required): Set the Remote GRE IP Endpoint IP/mask.

Inbound Key: Specify a key for use with keyed GRE. Key is either a number or an IP address. The Inbound Key is used for input only. This is an optional field.

Outbound Key: Specify a key for use with keyed GRE. Key is either a number or an IP address. The Outbound Key is used for output only. This is an optional field.

Time-to-Live (Required): Set a fixed Time-to-Live for tunneled packets. The recommended setting for this field is 64. Values over 64 may cause connection failures.

Use Multicast: Select Yes to enable Multicast for the tunnel.

Use ARP: Select Yes to enable ARP for the tunnel.

Start Tunnel at Boot: Select Yes to allow the interface to become active at system start.

Use DNS Lookup for RemoteIP: Select Yes to use DNS Lookup for the Remote IP. Every 5 minutes this will be resolved against the servers found in Network >DNS Settings. If the resolved IP changes, the tunnel will be restarted with the new Remote IP.

Use this option to allow units with dynamic IPs to maintain a GRE tunnel. This requires the use of DynDNS, or other dynamic DNS updating protocols to populate the dynamic IP changes.

Click on the *Finish* button. You will be returned to the GRE Tunnels dialog window and the Configuration Table will now be populated with the recently entered data.

To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

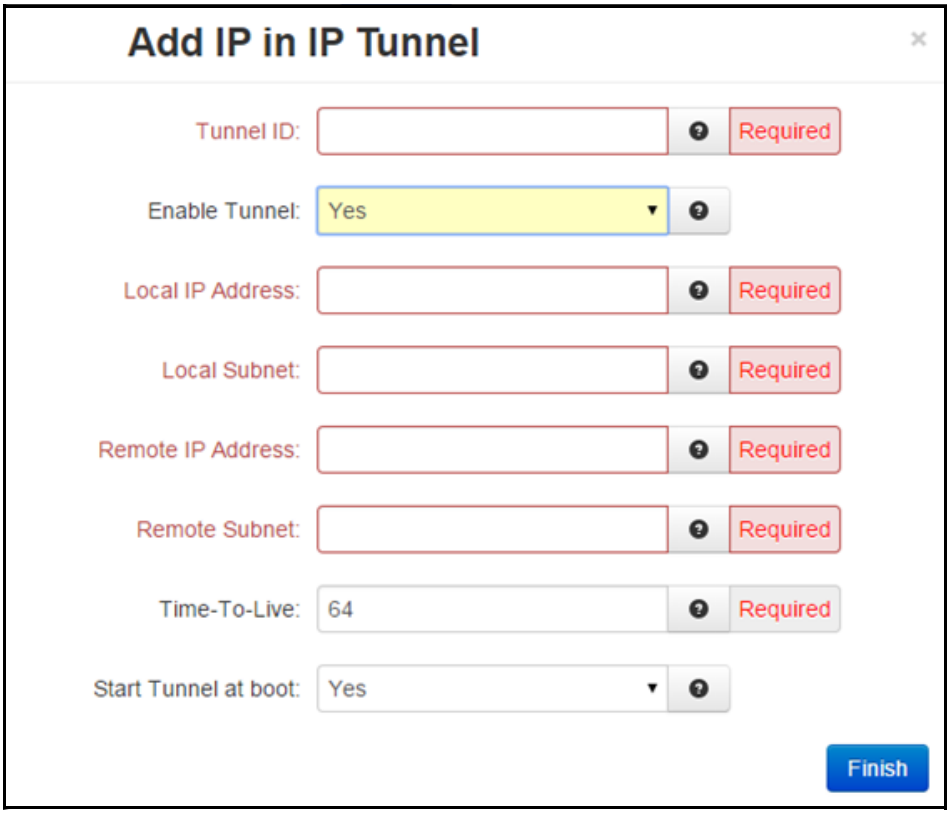
IP in IP Tunnels

The IP in IP Tunnels menu items is used to configure a simple IP Tunnel. IP in IP Tunnel essentially encapsulates an IP packet into another packet with the same protocol as the transport protocol.

Click on the *IP in IP Tunnels* menu item and the following window appears:

To add an IP in IP Tunnel:

Click on the *Add* button and the following window appears:



Tunnel ID (Required): Enter a unique numerical identifier in this field. It will be used for naming the tunnel interface which appears in the interface list as tunl1, tunl2, etc. depending on the IDs provided.

Enable Tunnel: Select Yes to enable the tunnel.

Local IP Address (Required): Set the fixed local address for tunneled packets. Note: If supplied, the Local IP Address must be an address on another interface of this host. If not supplied, tunneled packets can be received from any interface.

Local Subnet (Required): Set the local, private IPP network/mask.

Remote IP Address (Required): Set the IP Address of the remote endpoint for this tunnel.

Remote Subnet (Required): Set the remote, private IP network/mask.

Time-To-Live (Required): Set a fixed Time-To-Live for tunneled packets. Note: Values over 64 cause connection failures.

Start Tunnel at boot: Select Yes to allow the interface to become active at system start.

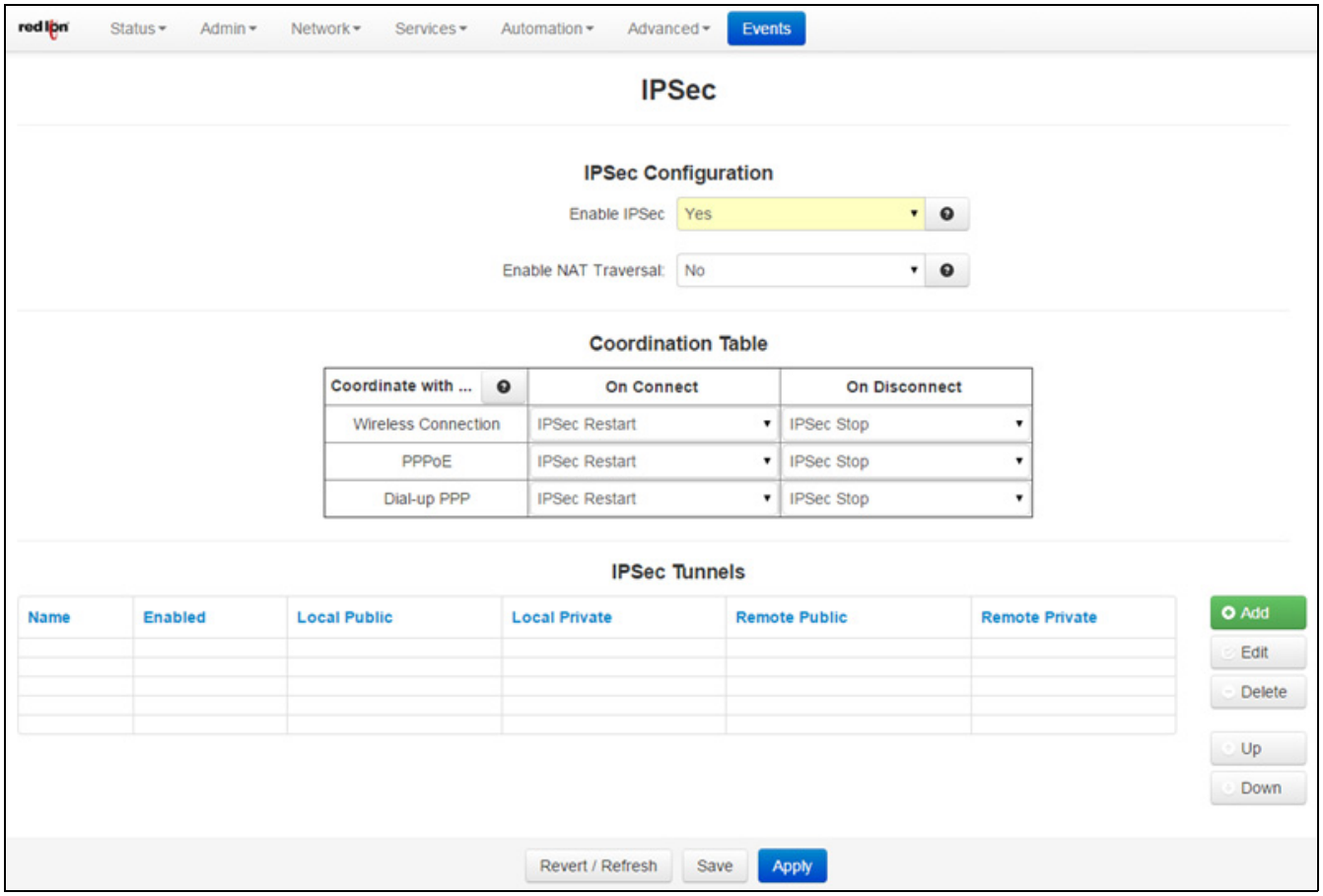
Click on the *Finish* button. You will be returned to the IP in IP dialog window and the IP in IP Tunnels Table will now be populated with the recently entered data.

To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

IPSec

The IPSec dialog window is split into two sections. The top section pertains to the IPSec configuration and the bottom portion is where IPSec tunnels are created and edited.



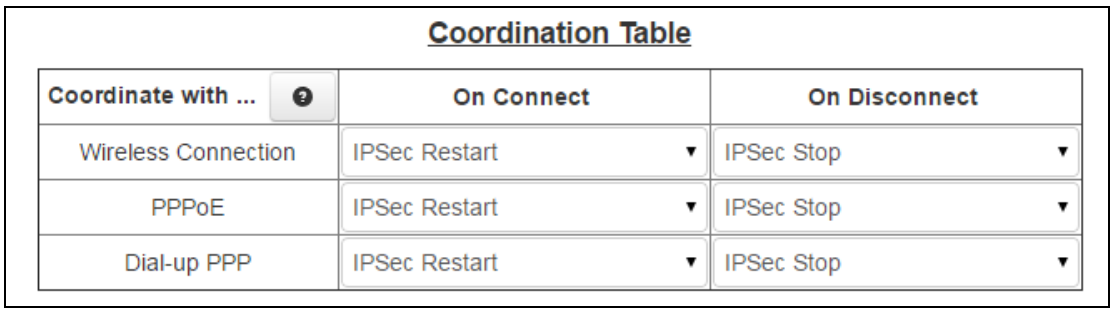
IPSec Configuration

Enable IPSec: Specify whether you want to enable the IPSec service. If you select No, all tunnels will be disabled.

Enable NAT Traversal: Specify whether all tunnels use NAT Traversal.

Coordination Table

You may select specific actions to be performed either upon PPP connect, PPP disconnect or both.



Coordinate with...: The available actions include Wireless Connection, PPPoE and Dial-Up PPP.

On Connect: The available options are:

Do Nothing: Perform no action

IPSec Restart: IPSec is restarted

IPSec Stop: IPSec is stopped

On Disconnect: The available options are:

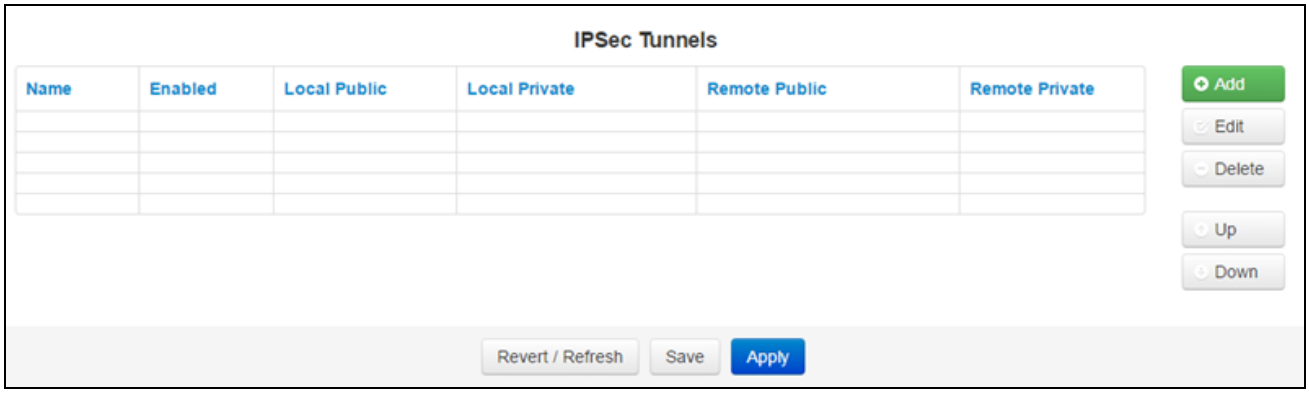
Do Nothing: Perform no action

IPSec Restart: IPSec is restarted

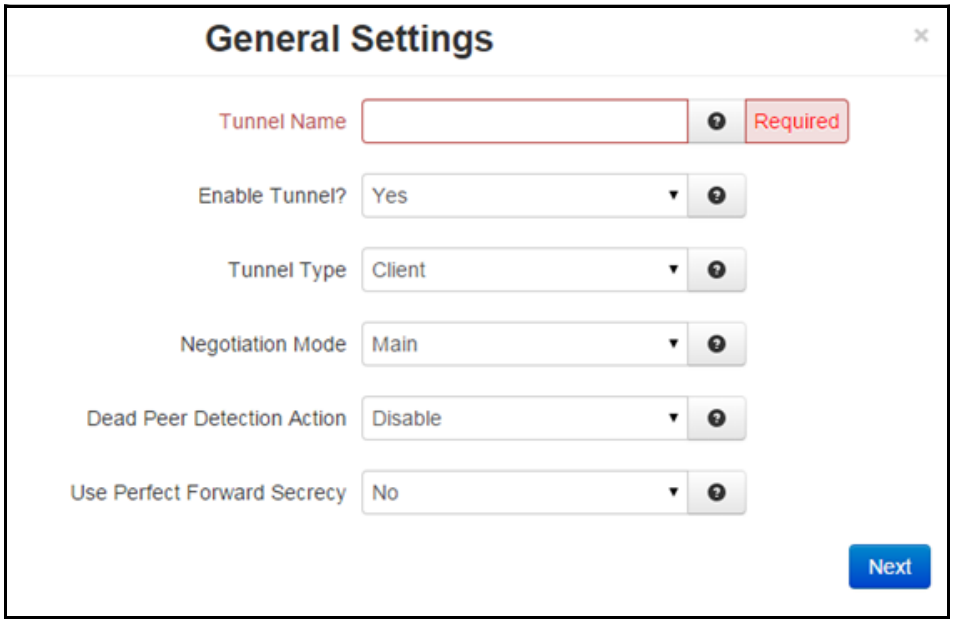
IPSec Stop: IPSec is stopped

With these combinations, the connection management may be fine-tuned so that the tunnel(s) may be able to restart faster, rather than having to rely on Dead Peer detection or other time out mechanisms alone.

IPSec Tunnels



Click on the *Add* button and the following **General Settings** dialog window appears:



Tunnel Name (Required): Enter a descriptive name for the tunnel in this field. The name must not contain spaces.

Enable Tunnel: Specify whether this tunnel should connect to its remote peer now, and after any reboot.

Tunnel Type: Controls the initial mode of the tunnel at startup. The options given to IPsec are:

Client: auto=start

Server: auto=add

Dynamic: auto=route

For more information, please consult an IPsec user guide on aspects of these specific modes.

Negotiation Mode: As a default, this field is set to Main mode ISAKMP Negotiation. When using dynamic, or DHCP issued IP addresses (for example with cellular cards), some remote devices may require the use of Aggressive Mode ISAKMP Negotiation. Should you encounter this situation, you can perform aggressive mode ISAKMP negotiation by changing this parameter from “Main” to “Aggressive ISAKMP”.

To use Aggressive ISAKMP Negotiations, select Yes from the list provided or No to prevent it’s use.

Dead Peer Detection Action (DPD Action): This feature can help detect when a remote end-point is no longer communicating properly.

Disable: Select disable if you are not using this option.

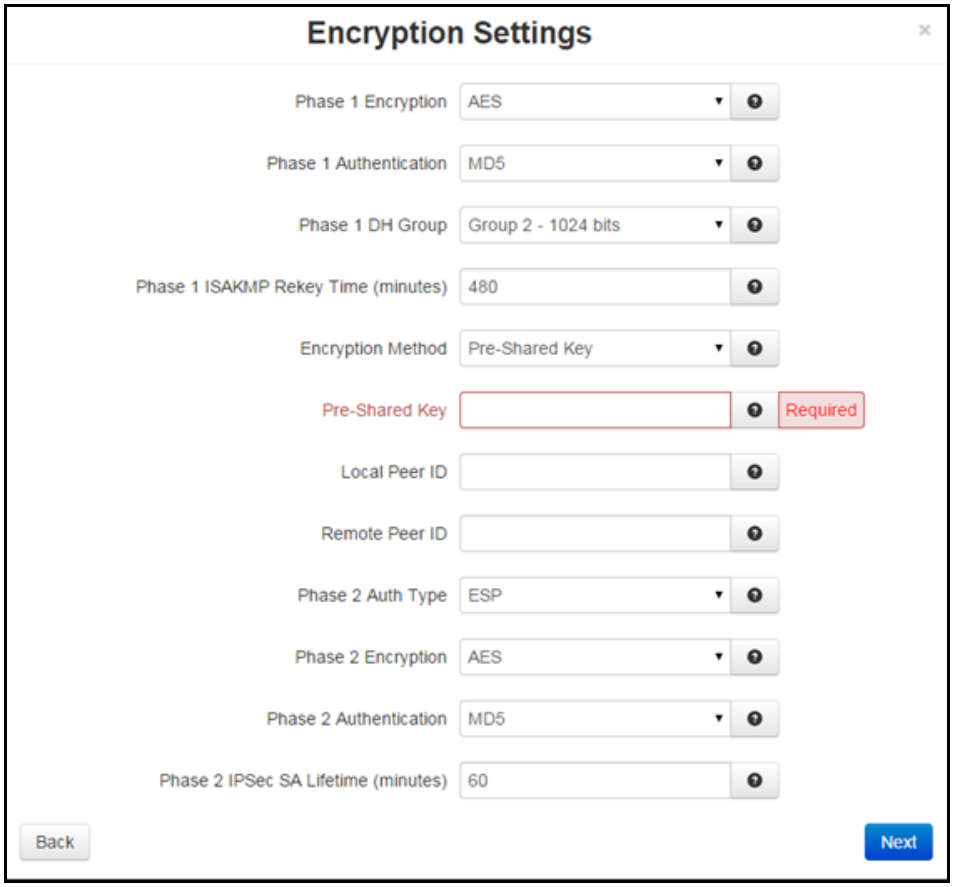
Hold: Once an error is detected, the hold state will only renegotiate the tunnel after new traffic destined for the tunnel is detected.

Restart: The restart state will attempt to immediately re-establish the connection to the concentrator. For this reason, restart may use more bandwidth and may not be the ideal choice for a limited data plan. However, if a host at the central site needs to initiate connections down to a local device through the tunnel, restart may be necessary so that the tunnel is always up and waiting for new data from the concentrator.

Use Perfect Forward Secrecy: This option specifies whether or not the tunnel uses Perfect Forward Secrecy when negotiation cryptography parameters with the remote device.

Note: This parameter must be set the same on the devices on both sides of the tunnel in order for a Security Association (SA) to be established. This is one of the first things that should be checked when tunnel negotiation difficulties are encountered.

Click on the *Next* button and the following **Encryption Settings** dialog window appears:



Phase 1 Encryption: Select the type of encryption needed for phase 1 (IKE). The options are AES, AES128, AES256, 3DES.

Phase 1 Authentication: Select the type of authentication needed for phase 1 (IKE). The options are MD5 and SHA1.

Phase 1 DH Group: Select the DH Group needed for phase 1 (IKE) by choosing one of the values from the drop-down list provided. This option selects the encryption level of the Diffie-Hellman keys and these are:

None: A value of none means that no DH Group will be selected for this end of the tunnel and it will adopt the settings of its peer during connection initiation.

Group 1: 768 bits

Group 2: 1024 bits

Group 5: 1536 bits

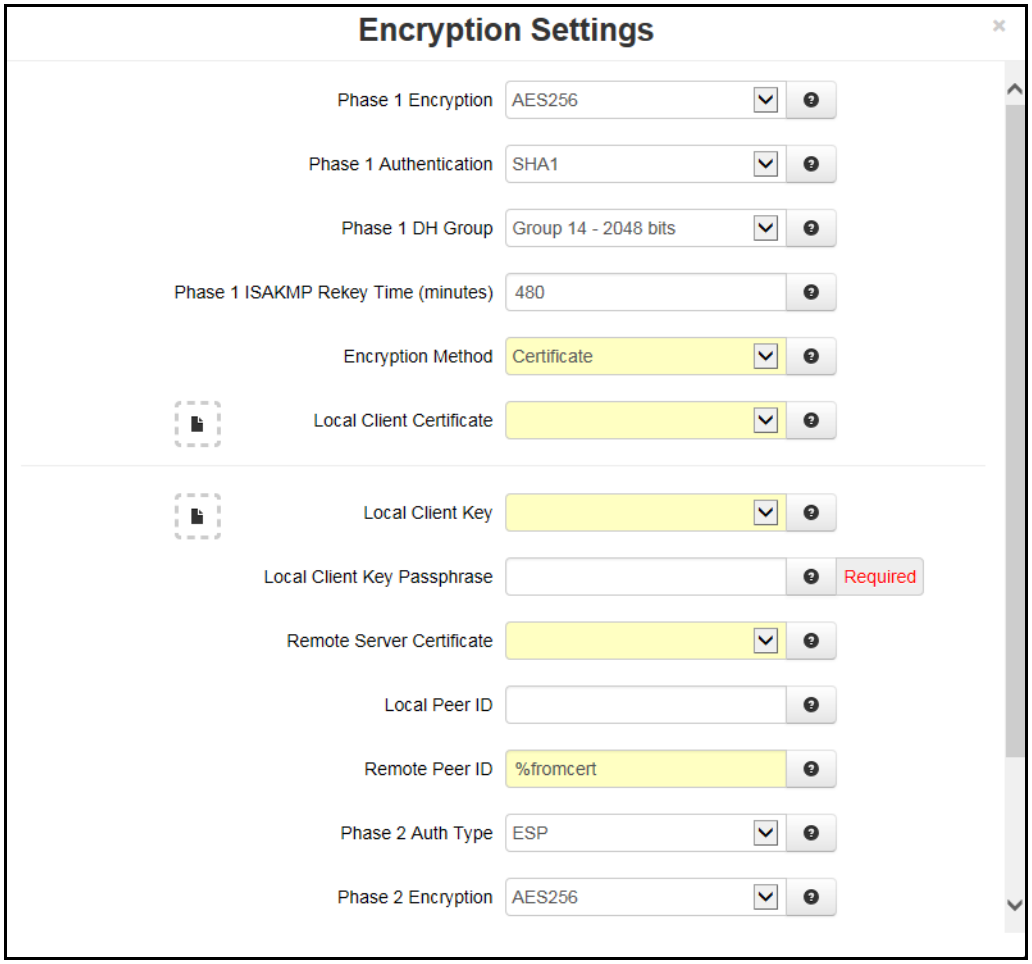
Group 14: 2048 bits

Longer keys imply better security but at a cost of longer negotiation/set-up time during the initial connection establishment. These settings must match on both ends of the connection.

Phase 1 ISAKMP ReKey Time (minutes): Select how long, in minutes, the keying channel of a connection (ISAKMP SA) should last before being renegotiated. We recommend that the Phase 2 IPSec SA Lifetime be less than the Phase 1 ISAKMP Rekey timer.

Encryption Method: Specify how the two end-points for this tunnel should authenticate with each other. Current options are **Pre-Shared Key** and **X.509 Certificates**. You may select certificates only after they are loaded in the **Admin > Certificate Manager**. The default setting is *Pre-Shared Key. Certificate* is an available option.

Certificate: Selecting Certificate changes the fields displayed on the Encryption Settings screen. Four additional fields appear.



Local Client Certificate (Required): Select the certificate file name you want to associate with this tunnel. Drag and drop the Local Client certificate into the box adjacent to the Local Client Certificate field. Or, click on the file icon to browse to the certificate for use. Select the desired certificate file and click Open to upload the file. Certificates may also be added under the **Admin → Certificate Manager** section of web UI.

Local Client Key (Required): Select the key file name you want to associate with this tunnel. Drag and drop the Local Client Key into the box adjacent to the Local Client Key field. Or, Click on the file icon to browse to the certificate for use. Select the desired certificate file and click Open to upload the file. Keys may also be added under the **Admin → Certificate Manager** section of web UI.

Remote Server Certificate (Required): Select the certificate file name you want to associate with this tunnel. Drag and drop the Remote Server Cert into the box adjacent to the Local Client Certificate field. Certificates may also be added under the **Admin → Certificate Manager** section of web UI.

Remote Peer ID (Required): Automatically populates with %fromcert when the Certificate Encryption Method option is selected.

Pre-Shared Key (Required): Specify the key to be exchanged for encryption negotiation during phase (IKE). The key must not contain a double-quote character. **Note:** The Pre-Shared Key must match on both ends of the tunnel in order to work.

Local Peer ID: Specify how the left participant should be identified for authentication. This can be an IP address of a fully qualified domain name preceded by @ (which is used as a literal string and not resolved).

Remote Peer ID: Specify how the right participant should be identified for authentication. This can be an IP address of a fully qualified domain name preceded by @ (which is used as a literal string and not resolved).

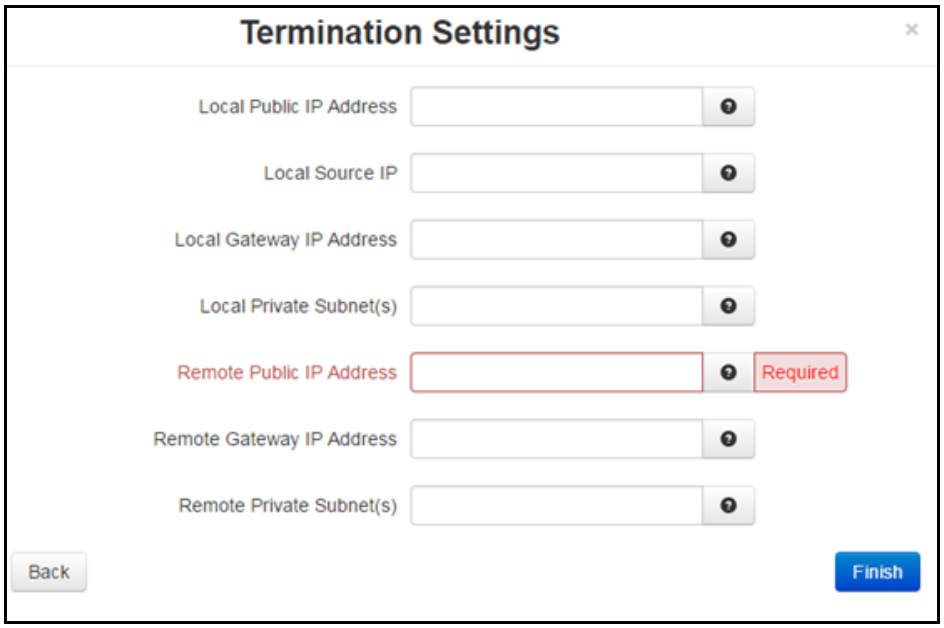
Phase 2 Auth Type: Defines whether authentication should be done as part of ESP encryption, or separately using the AH protocol.

Phase 2 Encryption: Select the ESP encryption algorithm to be used for the connection.

Phase 2 Authentication: Select the ESP authentication algorithm to be used for the connection.

Phase 2 ISAKMP Time (minutes): Select how long, in minutes, a particular instance of a connection (a set of encryption/authentication keys for user packets) should last, from successful negotiation to expiration.

Click on the *Next* button and the Termination Settings dialog window appears:



Local Public IP Address: This parameter typically only needs to be specified when the Red Lion RTU or router is configured to use more than one external, untrusted interface. Specify the IP Address of the left participant's public network interface.

For example, if the Red Lion RTU or router has an external cellular interface (ppp0) and an external Ethernet interface that is connected to a cable or DLS modem, and you need to bind the tunnel's crypto endpoint to the Ethernet interface, you would specify the IP address of the appropriate Ethernet interface here.

Note: If this value is omitted, it will be filled in automatically with the local address of the default route interface (as determined at IPSec startup time).

Local Source IP: Specify the Local IP Address to source when transmitting. The IP Address for this host to use when transmitting a packet to the other side of this link. Relevant only locally, the other end need not agree. This option is used to make the gateway itself use its internal IP, which is part of the left or right subnet . Otherwise, it uses its nearest IP Address, which is its public IP Address.

This option is primarily used when defining subnet-subnet connections, so that the gateways can talk to each other and the subnet at the other end, without the need to build additional host-subnet, subnet-host and host-host tunnels.

Local Gateway IP Address: Specify the next-hop gateway, IP address for the left participant's connection to the public network. **Note:** If no value is provided, the tunnel uses the right participant as its next hop.

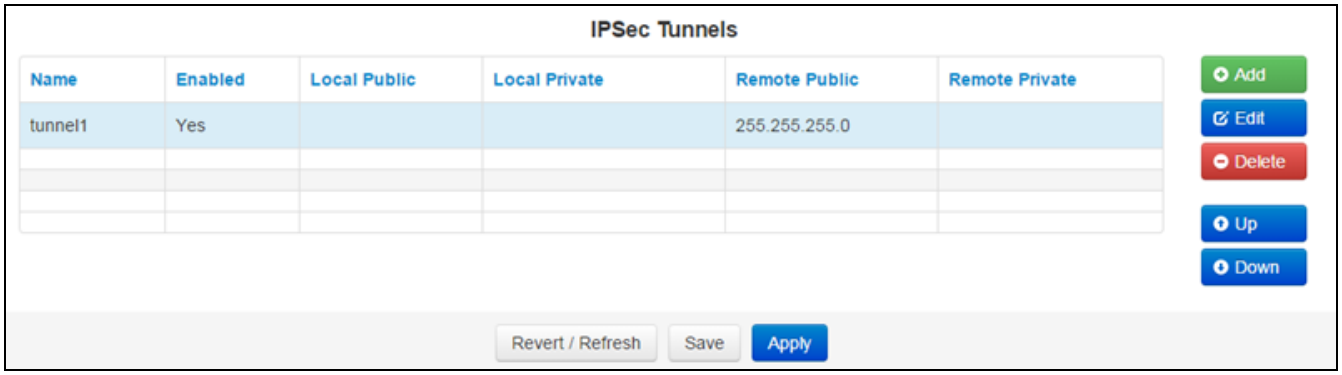
Local Private Subnet(s): Specify the private subnet(s) behind the left participant, expressed in CIDR format (xxx.xxx.xxx.xxx/nn) as network/netmask. More than one subnet can be specified by using a semi-colon to separate each entry.

Remote Public IP Address: Specify the IP address of Host name of the right participant's public-network interface. This field is required if Client is selected as Tunnel Type. If "Server" or "Dynamic" is selected as Tunnel Type, and this field is blank, then the value of **%any** will be used in the configuration file.

Remote Gateway IP Address: Specify the next hop gateway IP Address for the right participant's connection to the public network. **Note:** If no value is provided., the tunnel uses the left participant as it's next hop.

Remote Private Subnet(s): Specify the private subnet(s) behind the right participant, expressed in CIDR format (xx.xxx.xxx.xxx/nn) as network/netmask. More than one subnet can be specified by using a semi-colon to separate each entry.

Click on the *Finish* button. You will be returned to the IPSec dialog window and the IPSec Tunnels table will now be populated with the recently entered data.



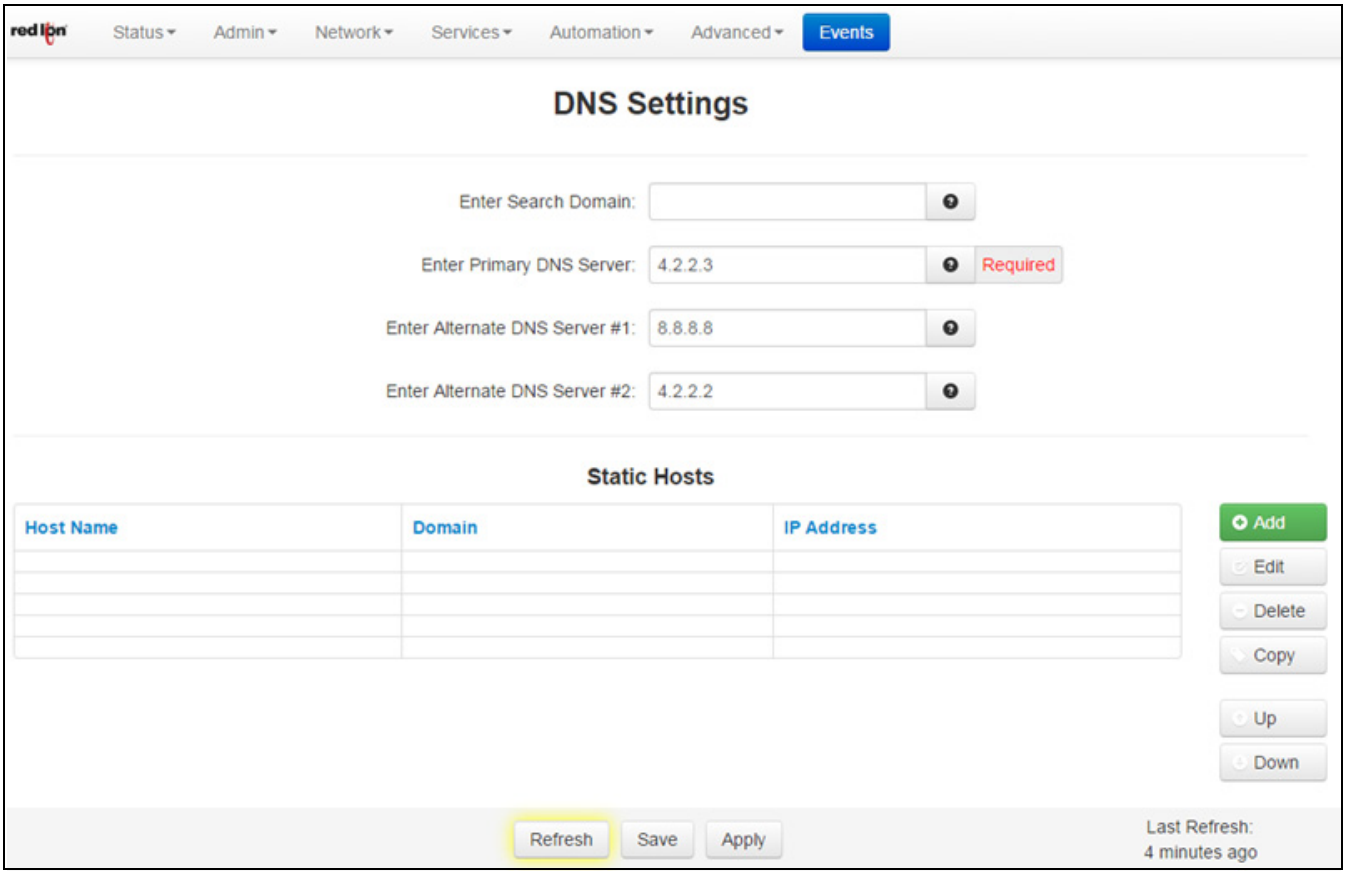
To delete an existing tunnel, select it in the table and click on the *Delete* button. To edit an existing tunnel, select it in the table and click on the *Edit* button.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

3.4.5 DNS Settings

The Domain Name Server (DNS) Settings dialog window is split into two sections. The top section pertains to the DNS settings and the bottom section is where static hosts are added and edited.

Click on the *DNS Settings* menu item and the following dialog window appears:



Enter Search Domain: Enter the local domain name(s) to be searched, separated by spaces. These domains are used as the default local domains when performing DNS queries. **Example:** local.net domain.com

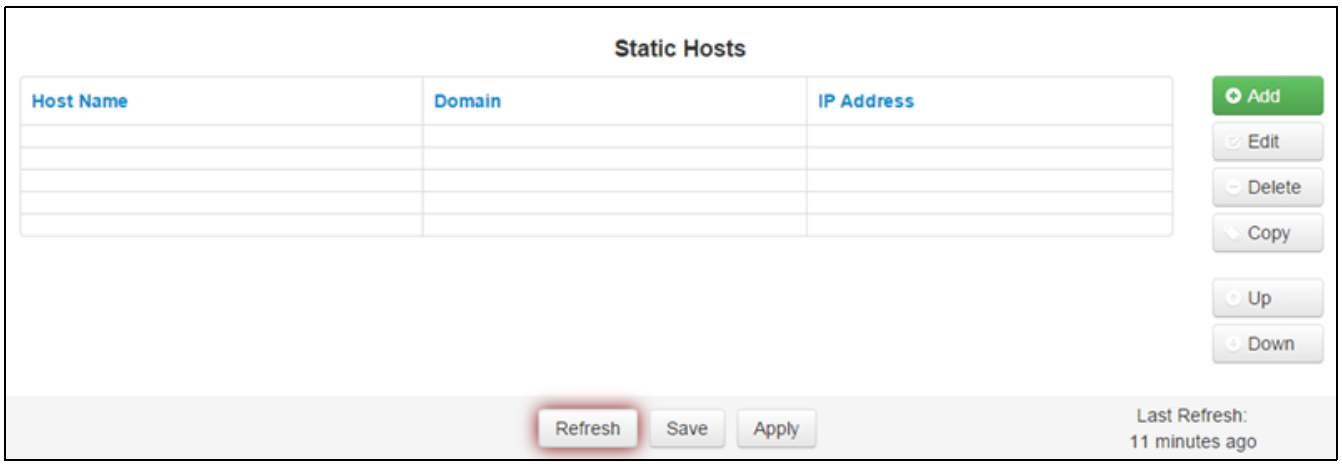
Enter Primary DNS Server (Required): *This field is already filled in; it is showing the current server in use by the Red Lion server.* Enter the IP Address of the Primary DNS Server you want to use. **Note:** This setting may be overridden if a network interface is set to obtain its configuration information from its peer (either via PPP or DHCP).

Enter Alternate DNS Server #1: *This field is already filled in; it is showing the current server in use by the Red Lion server.* Enter the IP Address of a Backup DNS Server you want to use, if the Primary DNS Server is unable to perform a DNS lookup. **Note:** This setting may be overridden if a network interface is set to obtain its configuration information from its peer (either via PPP or DHCP).

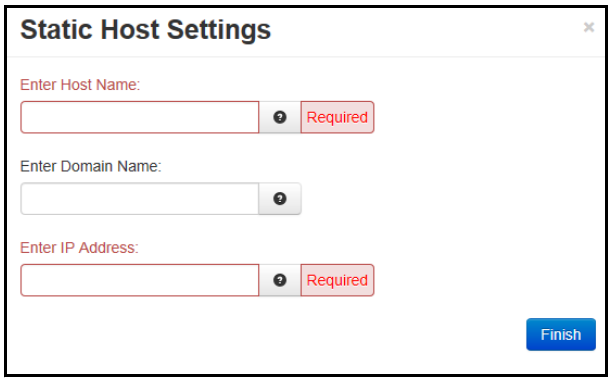
Enter Alternate DNS Server #2: *This field is already filled in; it is showing the current server in use by the Red Lion server.* Enter the IP Address of a Backup DNS Server you want to use, if the Primary DNS Server is unable to perform a DNS lookup. **Note:** This setting may be overridden if a network interface is set to obtain its configuration information from its peer (either via PPP or DHCP).

Static Hosts

Static Host entries may be added for local hosts, allowing the Red Lion RTU or router to resolve local host names to IP addresses.



Click on the *Add* button on the following dialog window appears:



Enter Host Name (Required): Enter the desired Host Name.

Enter Domain Name: Enter the desired Domain Name.

Enter IP Address (Required): Enter the host IP Address.

Click on the *Finish* button. You will return to the DNS Settings dialog window and the Static Hosts table will now be populated with the recently entered data.

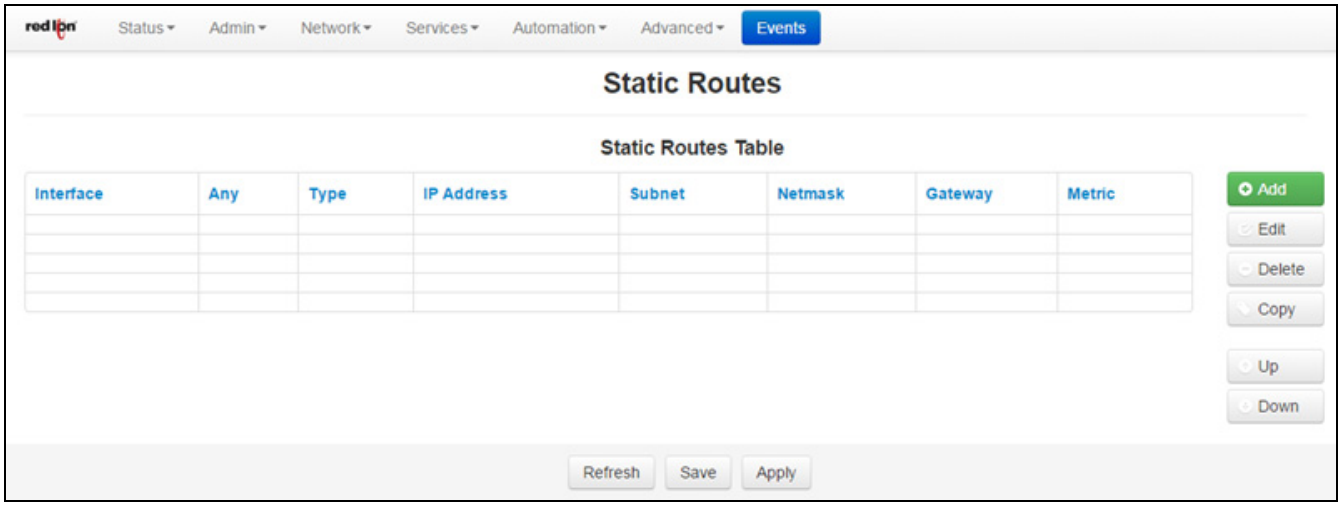
To delete an existing host, select it in the table and click on the *Delete* button. To edit an existing host, select it in the table and click on the *Edit* button.

Click on the *Save* button for changes to be saved without activating them until you reboot the unit. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

3.4.6 Static Routes

The Static Routes menu allows you to configure a route to a network through an interface manually.

Click on the *Static Routes* menu item and the Static Routes dialog window will open:



To add a Static Route on the Red Lion RTU or router:

Click on the *Add* button and the dialog window below appears:

Interface: Select the interface to which the route should be applied by selecting one of the available options from the drop-down list. The available interfaces varies depending on the particular model of device, as well as the current configuration, and may include those created as aliases, VPN tunnels.

Use as "Any" Route?: Select whether or not this route should be used as an "any" route by selecting Yes or No from the provided drop-down list.

When set to **Yes**, the route will take effect when a network change event (up/down) occurs on any interface. For example, if the configured interface is set to eth0, and the ppp0 interface becomes active, then the route will be reapplied to eth0.

When set to **No**, the route will take effect only when a network change occurs on the configured interface. For example, if the configured interface is eth1, then the route will be assigned only when eth1 has a network change to an active state.

Select Route Type: Select the type of route to be created by choosing one of the available options from the provided drop-down list. The choices are Host or Network.

Select **Host** to create a route to a specific device. This will require setting the T**arget IP Address** and **Gateway** parameters.

Select **Network** to create a route to a remote network. This will require setting the **Network IP Address**, **Netmask** and **Gateway** parameters.

Enter Target IP Address (Required): Enter the IP Address of the destination host to which the route should be created.

Enter Gateway (Required): Enter the IP Address of the gateway for the specified host or network. A gateway is a device (typically a RTU or router) used to gain access to another network.

For example, if a device is attached to a LAN whose a network address is 192.168.1.0 with a netmask of 255.255.255.0, than it can communicate directly with any other device on that network with a range of addresses of 192.168.1.1 through 192.168.1.254 (with 192.168.1.255 reserved for a broadcast). An address outside of that range is on a different network which would need to be accessed indirectly through a RTU or router and that RTU or router would be the gateway to the network on which the remote target device resides. In order to communicate with it, it would mean sending and receiving via the gateway device. The address must be one within the valid range for the network on which the designated interface resides.

Enter Metric: Enter a value for the route metric in this field. Recommended value is 0.

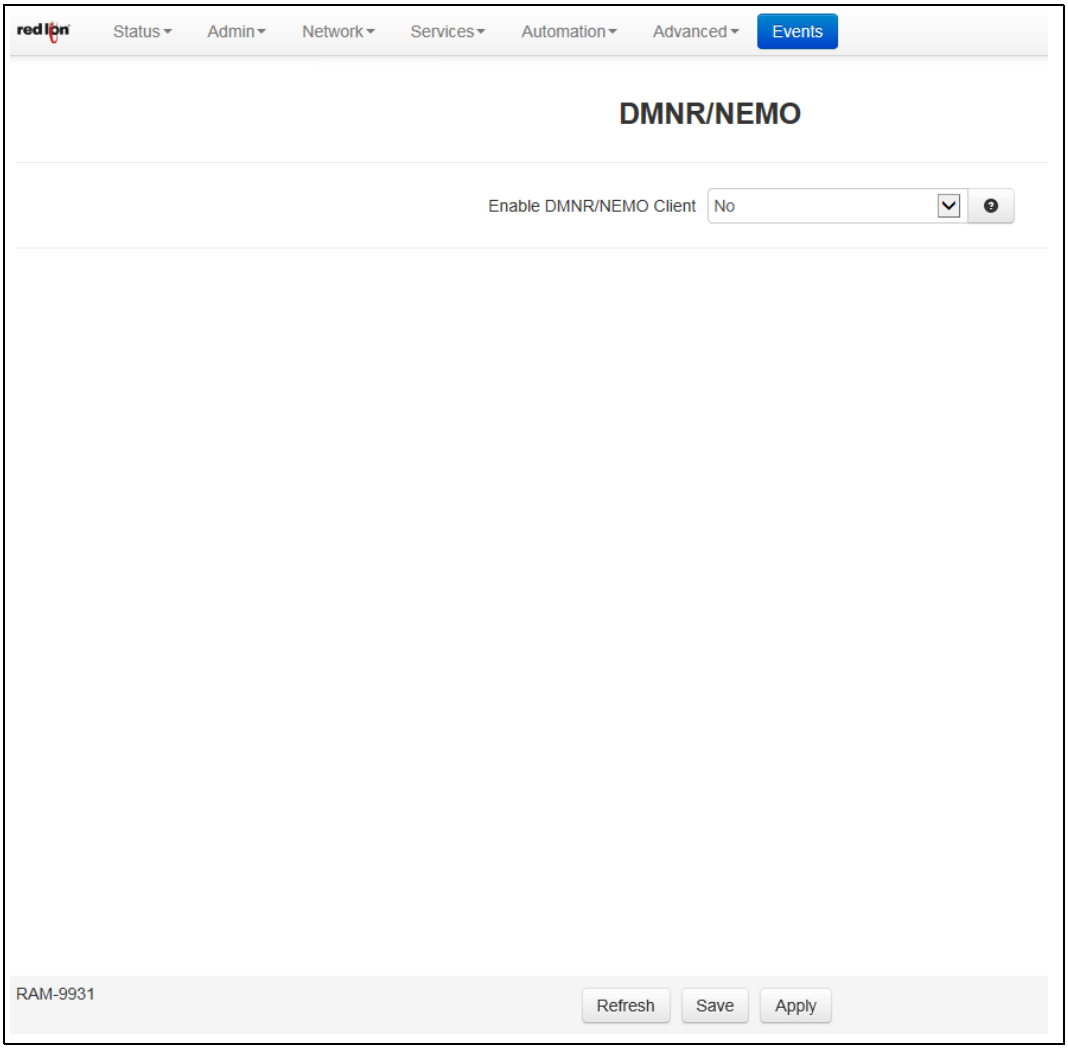
Click on the *Finish* button. You will return to the Static Routes dialog window and the Static Routes table will now be populated with the recently entered data.

To delete a static route, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

3.4.7 DMNR/NEMO Settings

Click on the *DMNR/NEMO* menu item the following dialog window appears:



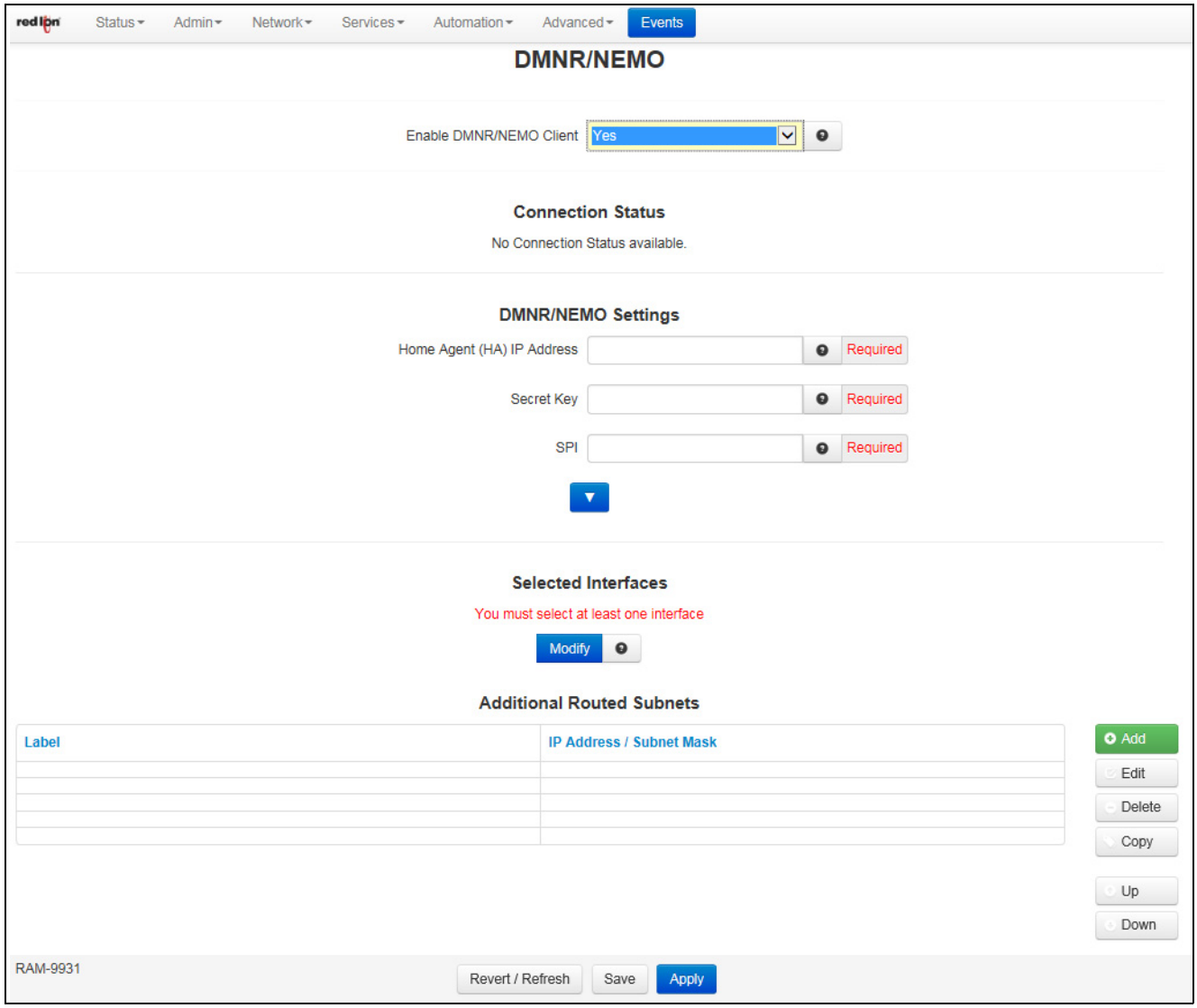
Enable DMNR/NEMO Client: Yes/No options to enable a DMNR/NEMO client (Dynamic Mobile Network Routing / Network Mobility).

Selecting *Yes* will invoke the DMNR/NEMO Settings screen.

2.4.7.1 DMNR/NEMO Client

The DMNR/NEMO Client menu item is used to Specify whether to enable the DMNR/NEMO Client on this device.

Select the *DMNR/NEMO* menu item, select *yes* to enable and the following window appears:



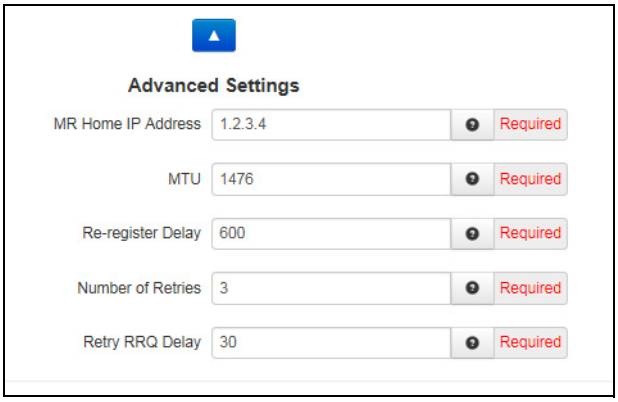
Home Agent (HA) IP Address: Enter the NEMO server address for the client to connect (provided by Verizon) (Required field).

Secret Key: N-MHAE-KEY, paired with the SPI for authentication. This field minimum length is 6 and the maximum length is 64 and any character is supported. This must match remote server end for authentication. (Required field) (provided by Verizon)

SPI: N-MHAE-SPI, paired with the Secret Key for authentication. This value must match remote server end. The valid values are 1 - 65534. (Required field).

Advanced Settings

Clicking on the down arrow below the DMNR/NEMO Settings will display the Advanced Settings fields on the screen. Modify the field contents as necessary.



MR Home IP Address: Enter the MR Home IP address - a /32 IPv4 address programmed into the MR configuration and used by the MR as a source of all NEMO signaling. This will be the IP of the MR GRE endpoint and does not need to be different on every device.

Recommended Setting 1.2.3.4 (Required field)

MTU: Enter maximum transmission unit (MTU). The valid values are 800 - 1476.

Recommended Setting 1476 (Required field)

Re-register Delay: Enter the interval to send re-register (RRQ) packets as long as the HA is responding. If the LIFETIME number received from the HA is less, then that value will be used instead (minus about 30 seconds). The valid values are 60 - 65534.

Recommended Setting 600 (Required field)

Number of Retries: Enter the number of retries the client will attempt to register between failures, when the HA is not responding. After maximum retries are exhausted, device will enter a 5 minutes hold-off period before the connection will start over.
The valid values are 0 - 255. A value of 0 is forever.

Recommended Setting 3 (Required field)

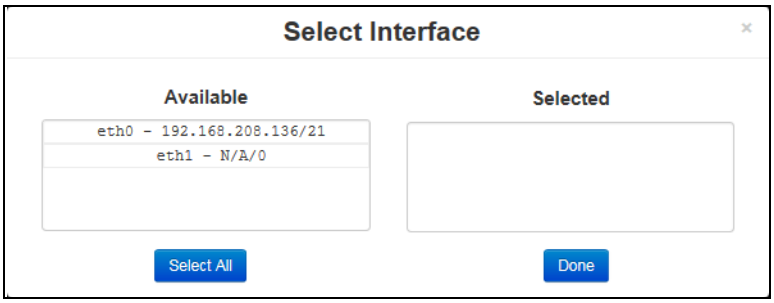
Retry RRQ Delay: Enter delay in seconds between retransmitting RRQ packets. If the LIFETIME number last received from the HA is less than the delay number entered, then the LIFETIME number will be used (minus about 30 seconds). The valid values are 5 - 65534.

Recommended Setting 30 Seconds (Required field)

Selected Interfaces

Mandatory Option: You must list at least one interface. Interface could be virtual, so if it is not there at config read time, the client will keep looking for it. The interface subnet will be an advertised route. Maximum number of total routes is limited to 16.

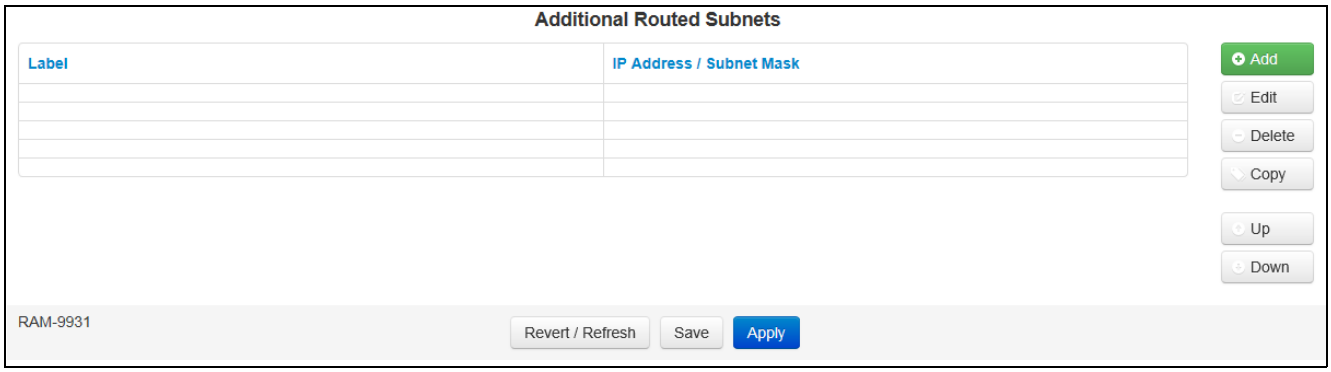
Clicking on the *Modify* button below the DMNR/NEMO Advanced Settings will display the Select Interface pop up window on the screen.



Select the desired interface by clicking the name of the available interface (or select all available interfaces using the *Select All* option) from the Available list on the left side of the screen. Verify your selection(s) move to the Selected side of the screen and click *Done* when finished or click *Clear* to revert your selection.

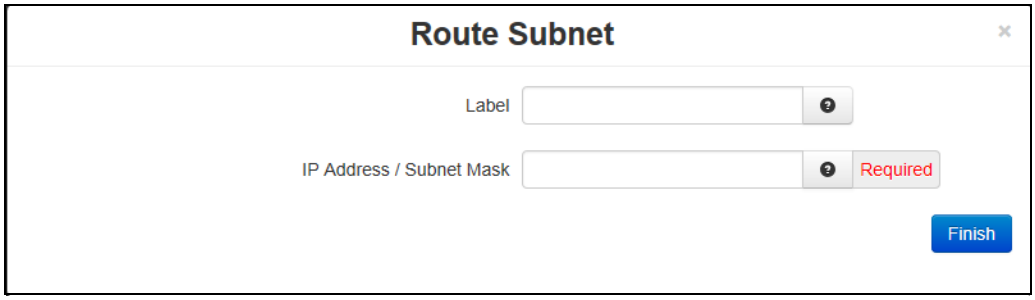
Additional Routed Subnets

This function is used to Add, Edit, Delete, Copy or Move routed subnets. Current and added routed subnets are visible and selectable in the primary display area. Each is displayed by Label and IP Address / Subnet Mask.



Add

This button is used to add a routed subnet. Clicking on the *Add* button to the right of the Additional Routed Subnets area displays the Route Subnet pop up window on the screen.



Enter a name (label) into the Label field for the Subnet you are adding. This is not required but can be helpful in identifying the purpose of the subnet within the network.

Enter the IP address and subnet mask using IP/CIDR notation into the IP Address / Subnet Mask field. The allowed CIDR values are 8 - 32. This subnet will be an advertised route. The maximum number of total interface/subnet routes is limited to 16.

Click *Finish*.

Verify the added subnet appears in the primary display area.

Edit

Use this button to edit an existing routed subnet. Select the routed subnet and click on the Edit button to the right of the Additional Routed Subnets area to display the Route Subnet pop up window on the screen.

Modify the name (label) as required in the Label field for the Subnet you want to edit.

Modify the IP address and Subnet mask as required for the Subnet into the IP Address / Subnet Mask field you are editing and click Finish.

Verify the edited subnet information appears in the primary display area.

Delete

Use this button to delete an existing routed subnet. Select the routed subnet and click on the Delete button to the right of the Additional Routed Subnets area.

Confirm the deletion request on the confirmation pop up.

Verify the deleted routed subnet no longer appears in the primary display area.

Copy

Use this button to copy an existing routed subnet. Verify the subnet copy information appears in the primary display area.

After the copy is made you can select the copy of the routed subnet in the primary display area and click on the Edit button to the right of the Additional Routed Subnets area to modify the configuration data as required.

Up / Down

Use these buttons to move an existing routed subnet up or down in the Additional Routed Subnets display.

Verify the subnet information appears in the primary display area as intended.

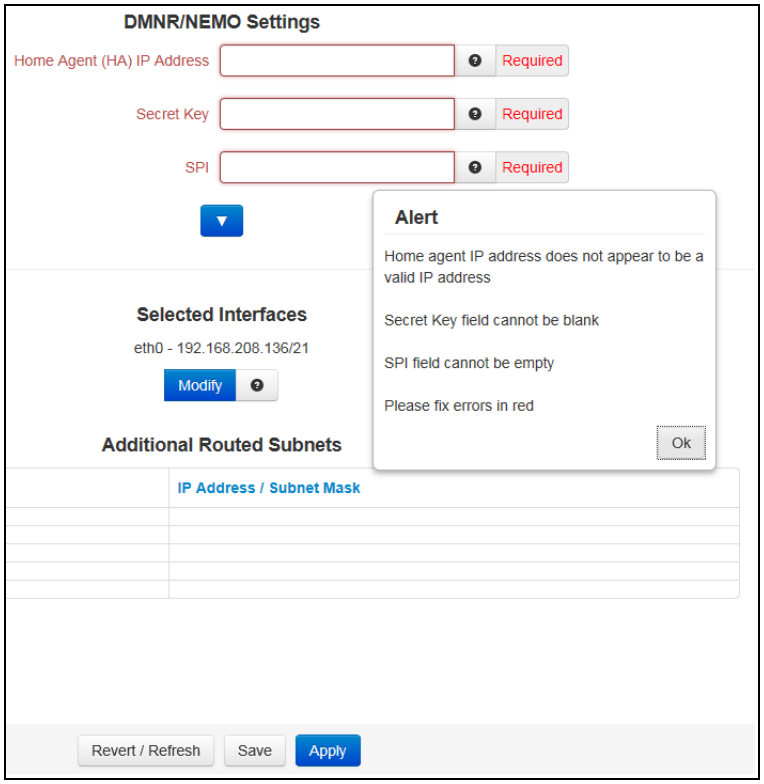
Revert / Refresh

Click the *Revert / Refresh* button to revert to the previous defaults.

Save / Apply

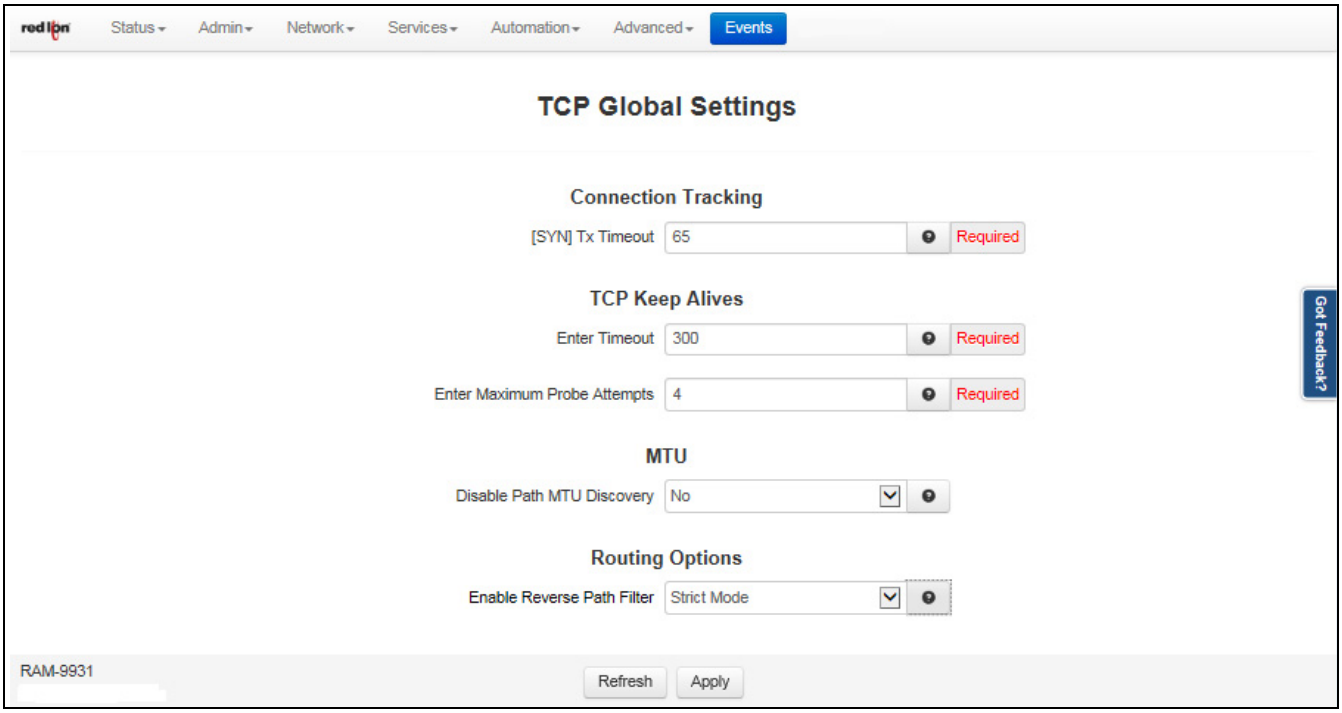
Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately.

Note: An Alert pop-up appears advising if any configuration data is out of specification. Note the corrections required, click *OK*, fix errors and click *Save* or *Apply* again.



3.4.8 TCP Global Settings

Click on the *TCP Global Settings* menu item the following dialog window appears:



[SYN] Tx Timeout (Required): Specifies the timeout value, in seconds, for SYN packets for connection tracking. 65 is generally recommended default, which differs from the system default of 120. The recommended tuning range is 30-120.

Enter Timeout (Required): Specifies the amount of time, in seconds, that a TCP connection can remain in an idle state before sending Keep-Alive Probes to verify that the remote end of the socket is still available. The recommended setting for this field is:

10 - 30 for Ethernet connections where data usage is not an issue.

60 - 300 for cellular connections where total data usage must be considered.

Enter Maximum Probe Attempts (Required): Specifies the acceptable number of failed probes that will be sent to the remote end of a TCP socket before determining the connection to be failed and disconnecting. The recommended values are 3-6.

Disable Path MTU Discovery: Enable/Disable Path MTU Discovery. This might be useful if a private cellular network is restricting MTU sizes along the network path and causing packet drops. The recommended value for this field is No (off).

Enable Reverse Path Filter: Select the desired Reverse Path Filter (rp_filter) from the drop down options. Reverse path filtering is a mechanism adopted by the Linux kernel, as well as most of the available networking devices to check whether a receiving packet source address is routable. When a device with reverse path filtering enabled receives a packet, the device will first check whether the source of the received packet is reachable through the interface it came in on.

- If the received packet's source address is routable through any of the interfaces on the device, the device will accept the packet.
- If the received packet's source address is not routable through any of the interfaces on the device, the device will drop that packet.

There are three available options:

- **No Source validation**
- **Strict Mode**: As defined in RFC3704 Strict Reverse Path, each incoming packet is tested against the FIB and if the interface is not he best reverse path then the packet check will fail. By default failed packets are discarded.
- Loose Mode: As defined in RFC3704 Loose Reverse Path, each incoming packet's source is also tested against the FIB and if the source address is not reachable via any interface then the packet check will fail.

Current recommended practice in RFC3704 is to enable strict mode to prevent IP spoofing from DDos attacks. If using asymmetric routing or other complicated routing, then loose mode is recommended.

Click on the *Apply* button to save the newly entered values. To revert to the previous defaults, click on the *Revert* button.

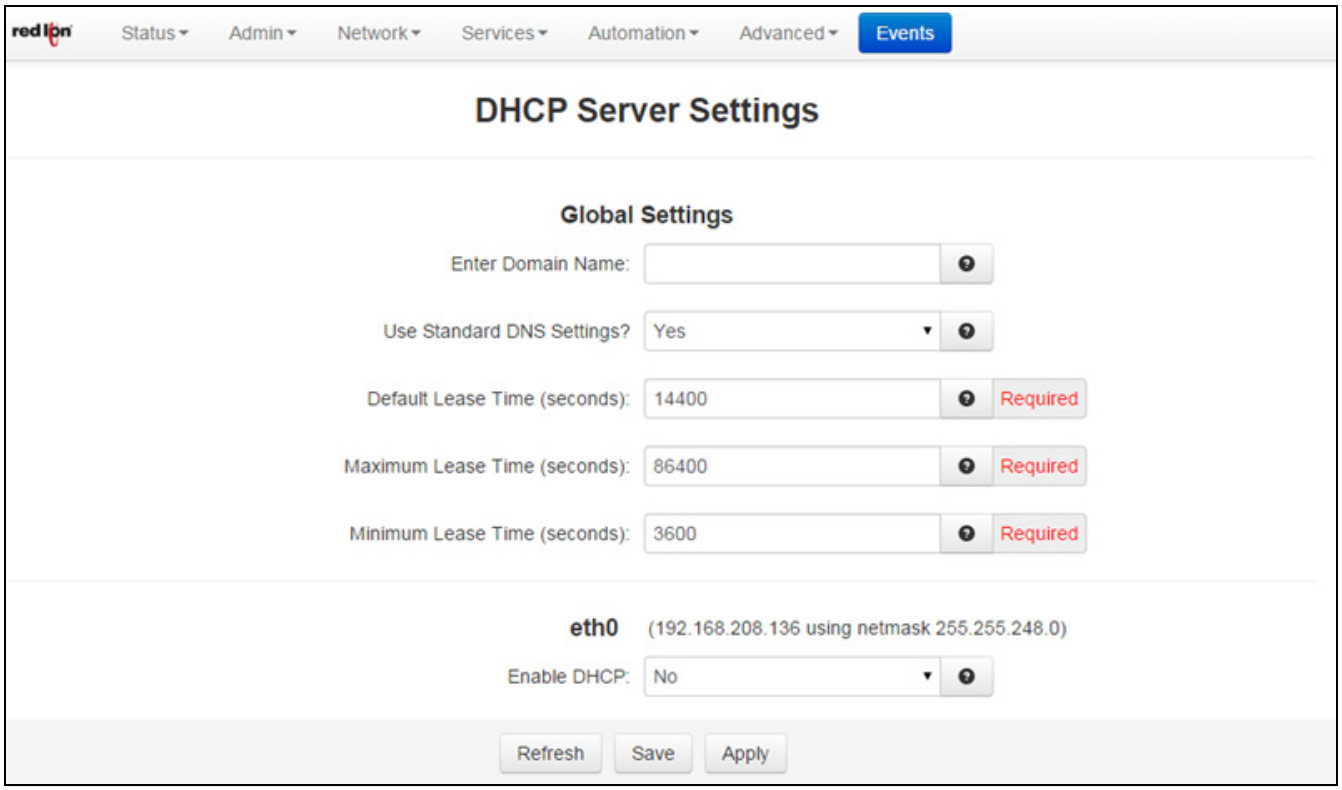
3.5 Services Tab

The Services Tab is where you can configure the various service offerings of the Red Lion RTU or router. These services include DHCP Server, DHCP Relay, Dynamic DNS, SN Proxy Settings, SixView Manager, GPS Settings, SSH/TELNET Server, SSL Connections, SNMP Agent, Ping Alive, Serial IP, RAMQTT and SMS Handling.

3.5.1 DHCP Server

Used to configure one of the internal Ethernet interfaces to be a DHCP server and hand out IP Addresses to systems connected to the Red Lion RTU or router.

Click on the *DHCP Server* menu item and the following dialog window appears:



Global Settings

Enter Domain Name: Enter the domain name that will be passed to DHCP Clients.

Use Standard DNS Settings:

- Choosing “Yes” will automatically use the DNS Servers obtained by this unit’s internet connection and/or entries specified in Networking→DNS Settings. This is the preferred method of operation.
- Choosing “No” allows you to issue custom DNS servers to connected DHCP Clients. This will not affect any DNS Servers used by this unit for local domain resolution.

Default Lease Time (seconds): Specify the amount of time, in seconds, that the DHCP Server allows clients to maintain their leases. Default value is “**14400**” (4 hours).

Maximum Lease Time (seconds): Specify the amount of time, in seconds, that the DHCP Server allows clients to maintain their leases. Default “**86400**”(24 hours).

Minimum Lease Time (seconds): Specify the amount of time, in seconds, that the DHCP Server allows clients to maintain their leases. Default "**3600**"(1 hour).

eth0:

Enable DHCP: Specify whether you want to enable a DHCP Server for the interface.

Note: If the interface is not enabled, or has been set to obtain its addressing parameters via DHCP, this option will be forced to NO, and disabled until the interface is both enabled and set to use a static IP address.

Enable Default Gateway: Provide Default Gateway IP Address to DHCP Client. Select No if you wish to only gain access to this device's web interface and have another connection from your PC out to the Internet. Select Yes if you wish to gain access to the Internet through this device.

Starting Address (Required): Enter the Starting IP Address of a range you want the DHCP Serer to provide for clients.

Recommended Setting: An address valid for the subnet for which the interface is configured. Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

Ending Address (Required): Enter the Ending IP Address of a range you want the DHCP Server to provide for clients.

Recommended Setting: An address valid for the subnet for which the interface is configured, beyond that chosen for the starting value of the range. Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

Wi-Fi/eth1:

Enable DHCP: Specify whether you want to enable a DHCP Server for the interface.

Note: If the interface is not enabled, or has been set to obtain its addressing parameters via DHCP, this option will be forced to NO, and disabled until the interface is both enabled and set to use a static IP address.

Enable Default Gateway: Provide Default Gateway IP Address to DHCP Client. Select No if you wish to only gain access to this device's web interface and have another connection from your PC out to the Internet. Select Yes if you wish to gain access to the Internet through this device.

Starting Address (Required): Enter the Starting IP Address of a range you want the DHCP Serer to provide for clients.

Recommended Setting: An address valid for the subnet for which the interface is configured. Care should be used to endure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

Ending Address (Required): Enter the Ending IP Address of a range you want the DHCP Server to provide for clients.

Recommended Setting: An address valid for the subnet for which the interface is configured, beyond that chosen for the starting value of the range. Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

usb0:

Enable DHCP: Specify whether you want to enable a DHCP Server for the interface.

Note: If the interface is not enabled, or has been set to *obtain* its addressing parameters via DHCP, this option will be forced to "NO", and disabled until the interface is both enabled and set to use a static IP Address.

Enable Default Gateway: Provide Default Gateway IP Address to DHCP Client. Select NO if you wish to only gain access to this device's web interface and have another connection from your PC out to the Internet. Select YES if you wish to gain access to the Internet through this device.

Starting Address (Required Field): Enter the Starting IP Address of a range you want the DHCP Server to provide for clients.

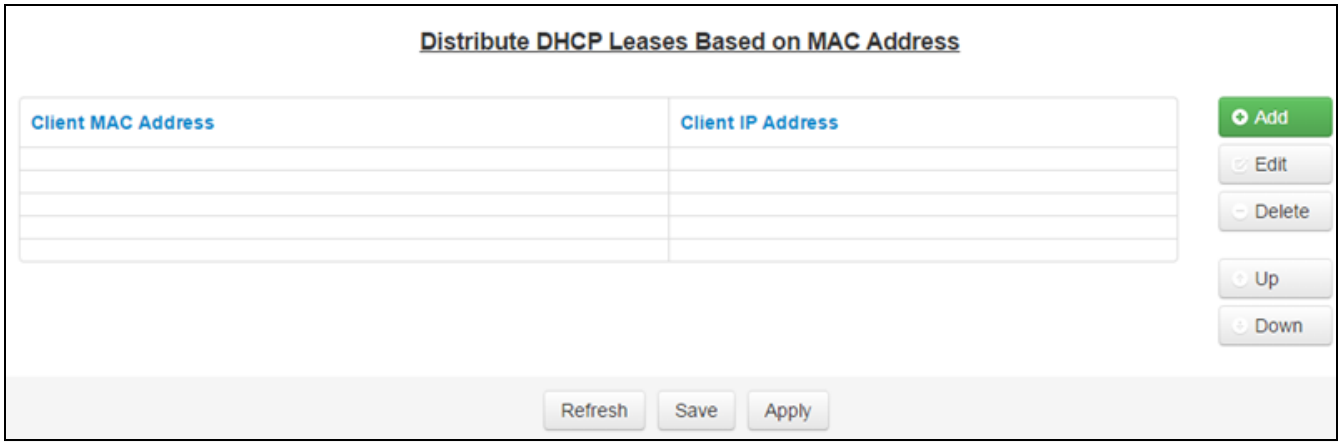
Recommended Setting: An address valid for the subnet for which the interface is configured. Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

Ending Address (Required Field): Enter the Ending IP Address of a range you want the DHCP Server to provide for clients.

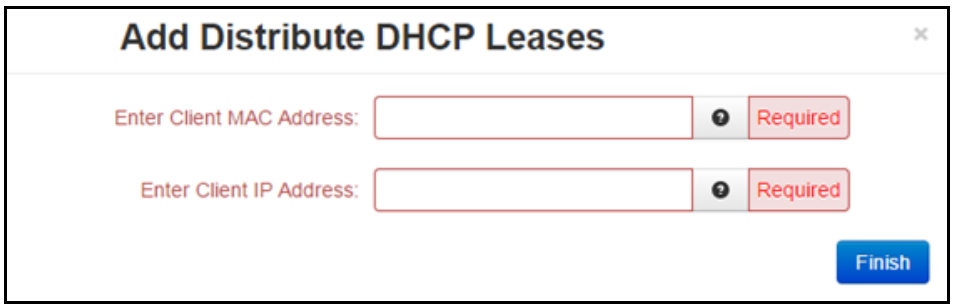
Recommended Setting: An address valid for the subnet for which the interface is configured, beyond that chosen for the starting value of the range. Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

Show DHCP Leases: Click on the *Show DHCP* button to display the current DHCP leases logged on to the unit.

Distribute DHCP Leases Based on MAC Address:



Click on the *Add* button to assign an IP Address to a device based on a MAC address, so that device obtains the same IP each time it requests a new IP from the DHCP server. The following window appears:



Enter Client MAC Address (Required): This is the field where you enter the Client's computer or device MAC (Media Access Control) address.

The MAC address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable hardware identifier for the network.

When entering the MAC address information, type the 12-digit MAC address in the following format: xx:xx:xx:xx:xx:xx including the colons.

Enter Client IP Address (Required): Enter the IP address for which you wish to assign to a client's computer or device MAC address.

The IP address can be any valid address for the subnet for which the interface is configured. Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to sue statically assigned IP addresses.

This address should be provided by your Network Administrator.

Click on the *Finish* button. You will return to the DHCP Server Settings dialog window and the entered data will be visible on the table at the bottom of the window.

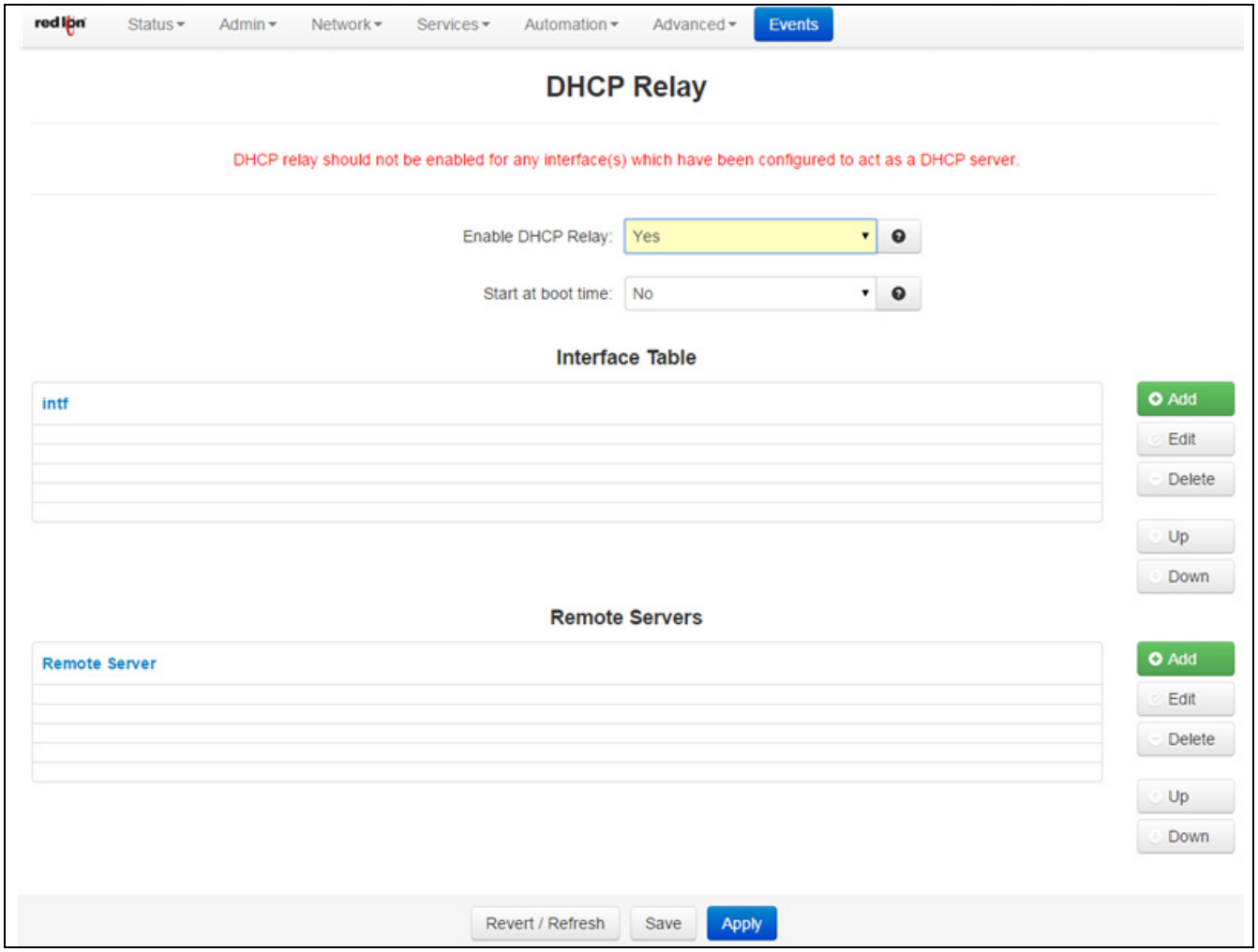
To delete an address, select it in the table and click on the *Delete* button. To edit an existing address, select it in the table and click on the *Edit* button.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

3.5.2 DHCP Relay

This feature will enable a DHCP Relay service, which will connect a local interface with a remote DHCP Server. DHCP Relay should not be enabled for any interface(s) which have been configured to act as a DHCP server.

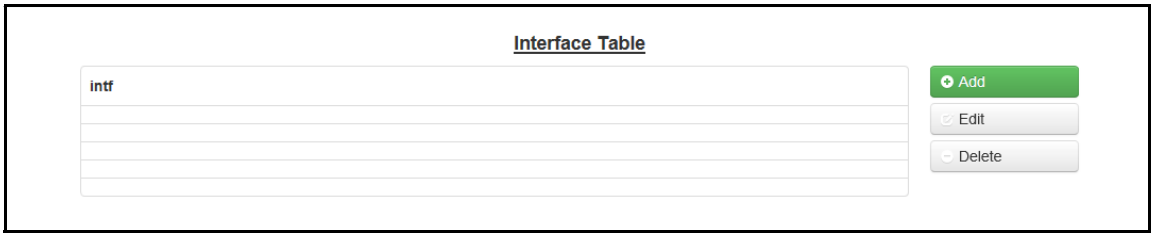
Click on *DHCP Relay* and the following dialog window appears:



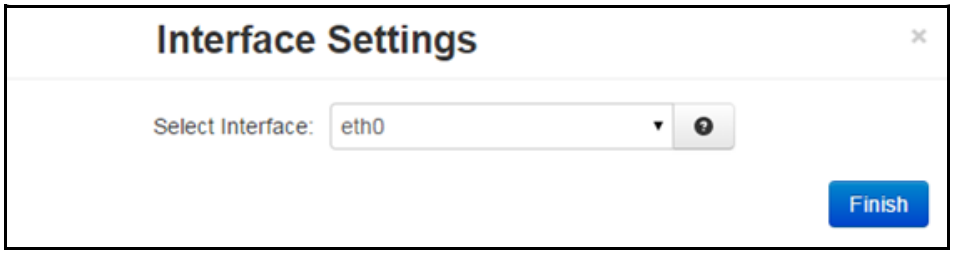
Enable DHCP Relay: Select YES to enable the DHCP Relay, or NO to disable it. The service will start once the Apply button is clicked. If the Save button is clicked, the service will not be started until the device is rebooted and then **only** if the *Start at boot time* option has also been set to YES.

Start at boot time: Select YES to enable the DHCP Relay at boot time, or NO for manual control. If the DHCP Relay service is required to be operational at all times, then set to YES. If another process, such as VRRP, is going to dynamically enable/disable DHCP Relay service as needed, then set to NO.

Interface Table:

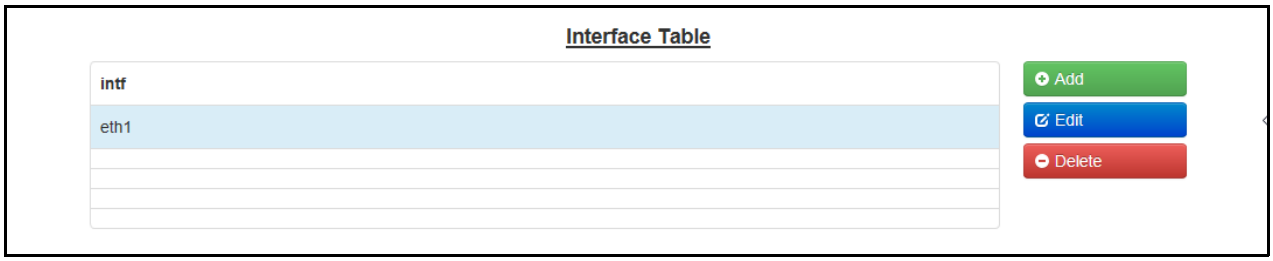


Click on the *Add* button and the following dialog window appears:



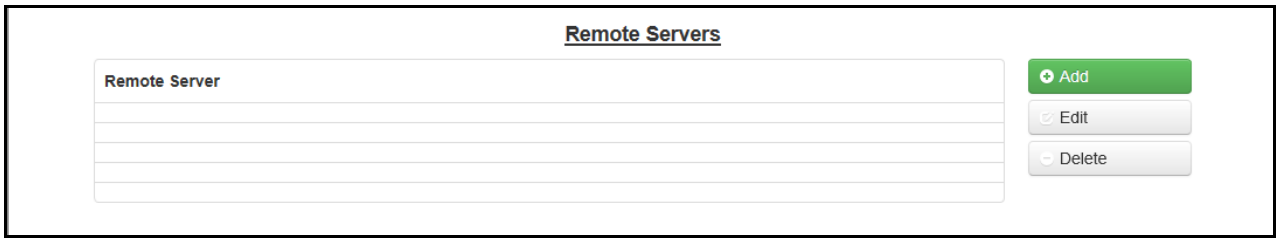
Select Interface: Select the interface to receive its IP from the remote DHCP server from the drop down menu.

Click on the *Finish* button. You will be returned to the DHCP Relay dialog window and the Interface Table will be populated with the entered data.

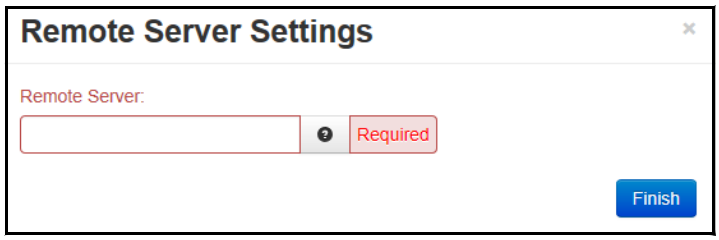


To delete an existing interface, select it in the table and click on the *Delete* button. To edit an existing interface, select it in the table and click on the *Edit* button.

Remote Servers:

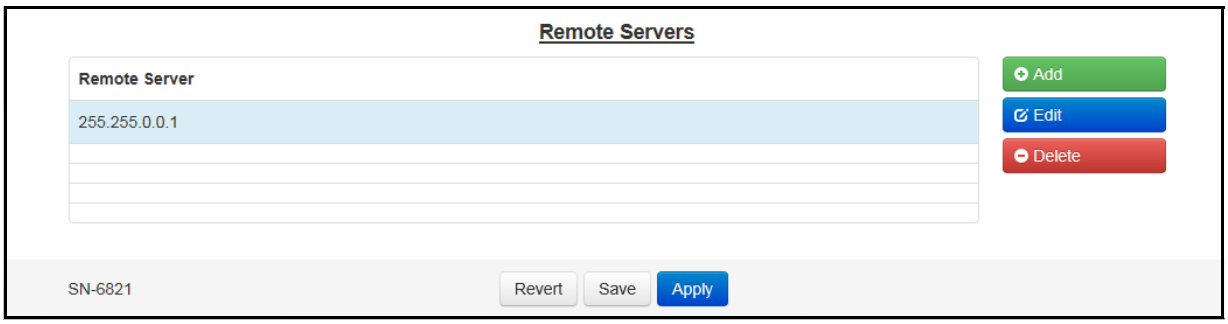


Click on the *Add* button and the following dialog window appears:



Remote Server: Enter the IP Address or fully qualified domain name of all remote DHCP Servers available. It is the responsibility of the remote DHCP Server to coordinate the issuing DHCP addresses.

Click on the *Finish* button. You will be returned to the DHCP Relay dialog window and the Remote Servers table will be populated with the entered data.



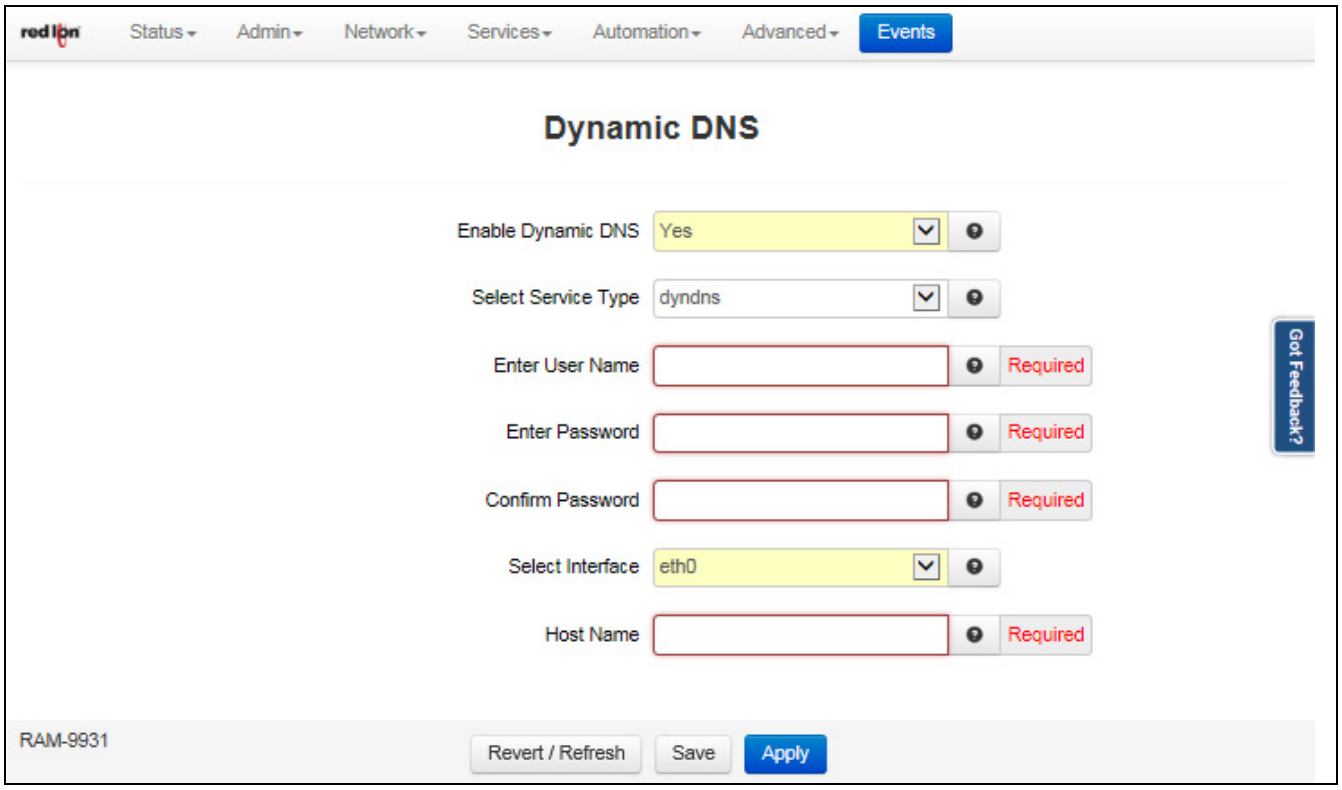
To delete an existing server, select it in the table and click on the *Delete* button. To edit an existing server, select it in the table and click on the *Edit* button.

Click on the *Save* button for changes to be saved without activating the interface/server until you reboot the unit. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

3.5.3 Dynamic DNS

The Dynamic DNS menu item is used to configure a dynamic DNS name for the Red Lion RTU or router that does not have a static public IP Address. A subscription to a service providing Dynamic DNS, such as DYNDNS.ORG, is required.

Click on the *Dynamic DNS* menu item and the following dialog window appears:



Enable Dynamic DNS: Select Yes to enable the Dynamic DNS Service.

Select Service Type: Select the desired Dynamic DNS Service from the list provided. Duck DNS service added in release 3.23/4.23.

Enter User Name (Required): Enter the User Name used to access your Dynamic DNS Service in this field.

Enter Password (Required): Enter the password used to access your Dynamic DNS Service in this field.

Confirm Password (Required): Re-enter the password entered in the field above. The password must match exactly.

Select Interface: Specify the interface you want to access via Dynamic DNS. Changes made to the interface configuration after enabling Dynamic DNS will result in updates being sent to your Dynamic DNS service provider.

Host Name (Required): Enter the host name and domain you which to be assigned by the Dynamic DNS Service.

Server Name/Address (Required): Enter the host name or IP Address (along with port number, if needed) for user to access the Dynamic DNS Server. ***Example:*** *members. dyndns.com:80*

The recommended setting for this field is automatically displayed when you select a Service Provider. If you require a value other than the recommended value, your Network Administrator or Dynamic DNS Service Provider should be able to provide the appropriate value, which can be entered manually.

Server Request Path (Required): Enter the Request URL required to connect to the Dynamic DNS Service in this field.

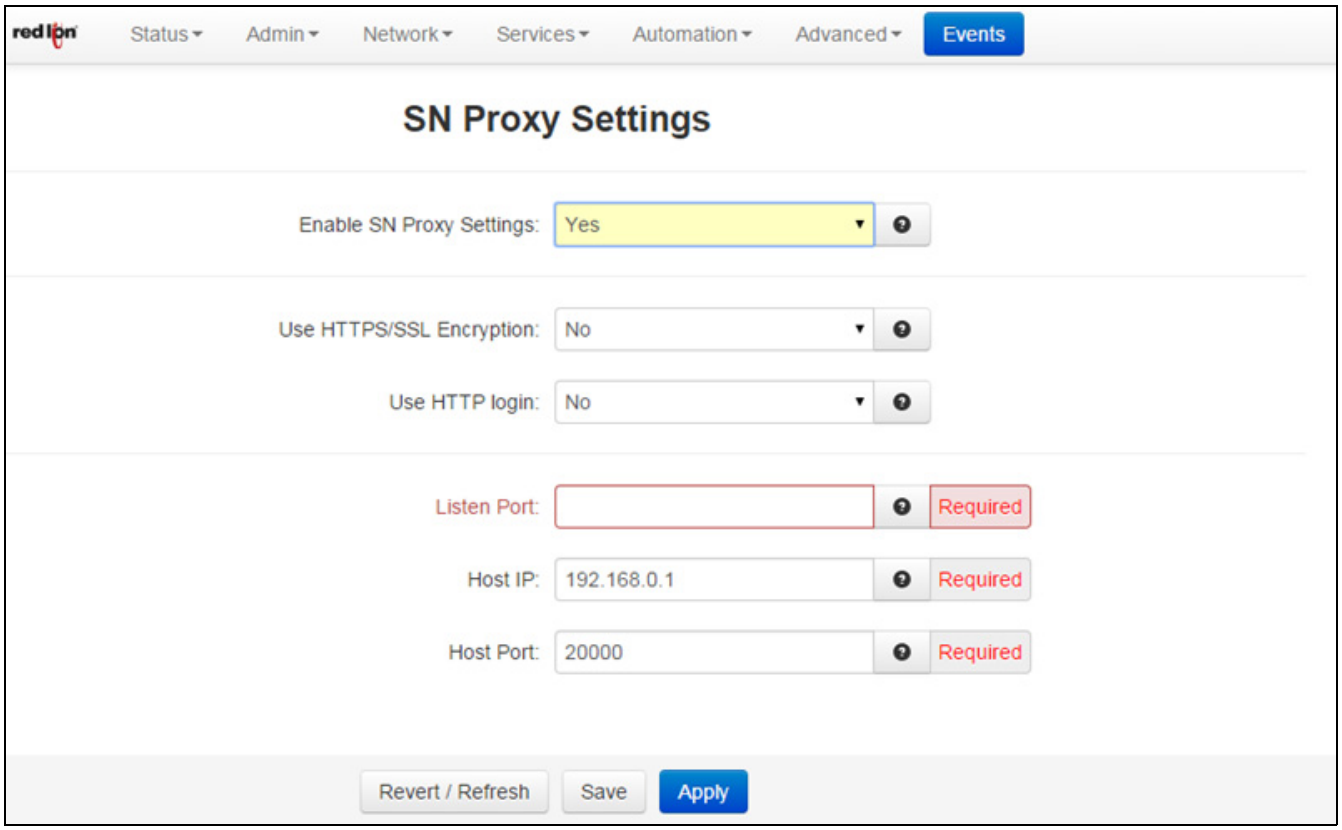
The recommended setting for this field is automatically provided when a Service type is selected. If you require a value other than the recommended value, your Network Administrator or Dynamic DNS Service Provider should be able to provide the appropriate value, which can be entered manually.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

3.5.4 SN Proxy Settings

SN Proxy is a web relay proxy service used to gain access to devices that are behind our Red Lion RTU or router providing additional security and access control to devices that may not offer such functionality. A proxy based service provides a more robust connection than just using a port forward rule, including the ability to add an additional user login for authentication, encryption via SSL as well as isolation via Access Control Lists.

Click on the SN Proxy Settings menu item and the SN Proxy Settings dialog window will open.



Enable SN Proxy Settings: Enables or disables the SN Proxy feature. If NO is selected, all other fields in the dialog window will be hidden.

Use HTTPS/SSL Encryption: Specify whether you want to enable the SSL engine for a more secure connection.

Use HTTP login: Specify whether you want to enable HTTP login. ***Note:*** *If you enable the HTTP login, you will be required to enter the username and password.*

Listen Port (Required): Enter the port number the SN Proxy listens for requests on.

Host IP (Required): Enter the proxy server host IP address that will be accepting this connection request.

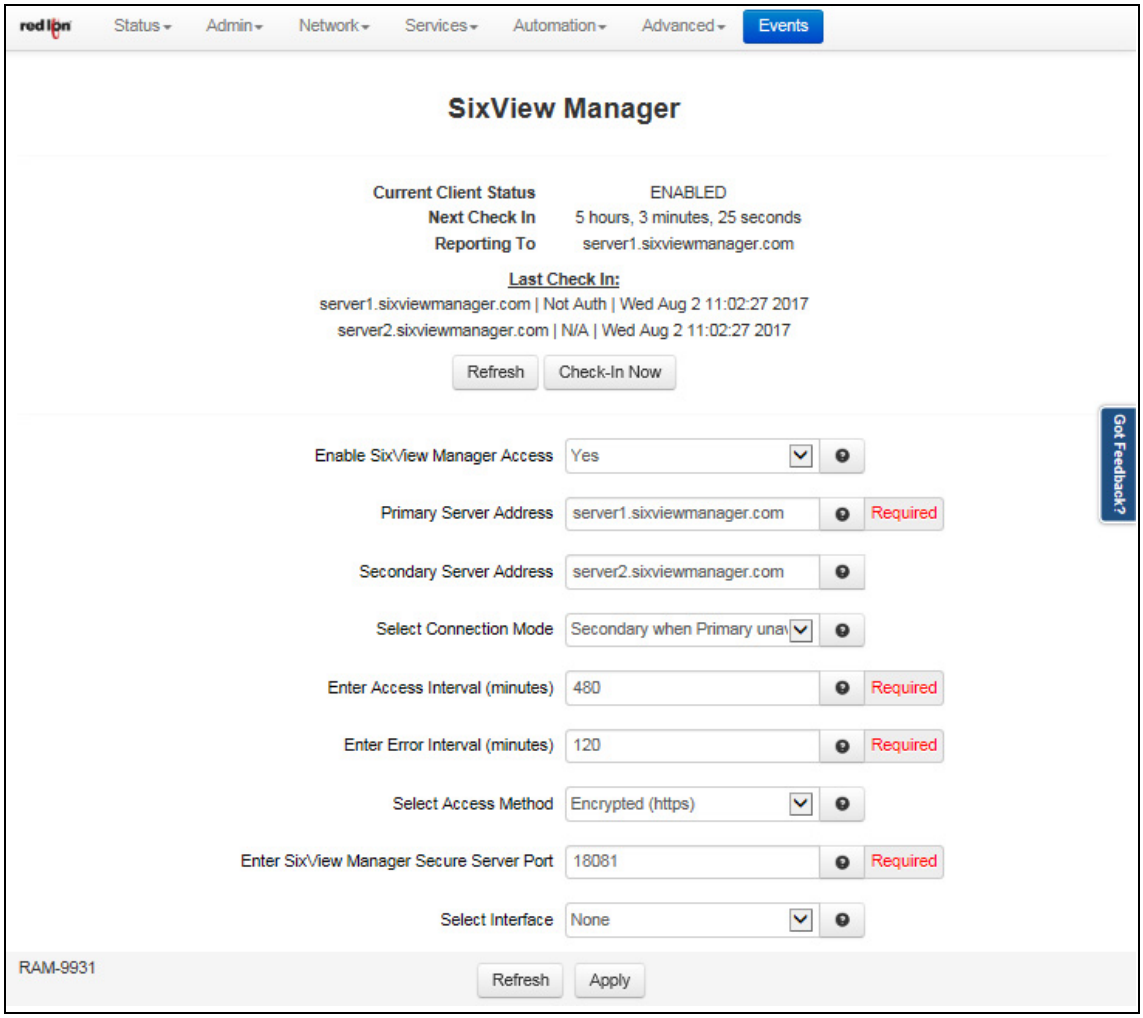
Host Port (Required): Enter the proxy server host port number.

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert*, will reset all fields to factory defaults.

3.5.5 SixView Manager

The SixView Manager menu item allows you to configure various aspects of the SixView Manager Client to communicate with a SixView Manager hosted at Red Lion or at your location.

Click on the *SixView Manager* menu item and the following window appears:



Enable SixView Manager Access: Select *Yes* to enable the SixView Manager Client, which will enable the device to communicate with the SixView Manager Server identified by the Host Address entered in the field below. To disable the SixView Manager Client, select *No* in the "Enable SixView Manager Access" pull down menu. All fields in the dialog window will disappear. The recommended setting for this field is *Yes*.

Note: A device managed by the SixView Manager Server may have its configuration altered at any time, without warning, so it is important to be aware of the actions the selected SixView Manager Server is configured to perform upon receiving a check-in from a new device before enabling this option. The recommended setting for this field is YES.

Primary Server Address (Required): Enter the IP Address or host name of your SixView Manager primary server.

When changing the Primary Address to your own private SixView Manager server, you may want to consider setting the Secondary Address to the Red Lion SixView Manager test server (server1.sixviewmanager.com) for trial and initial production rollouts This will enable Red Lion support staff to monitor the progress and better assist in diagnosing potential problems.

Secondary Server Address: Enter the IP Address or host name of your SixView Manager secondary server.

When changing the Primary Address to your own private SixView Manager server, you may want to consider setting the Secondary Address to the Red Lion SixView Manager test server (server2.sixviewmanager.com) for trial and initial production rollouts. This will enable Red Lion support staff to monitor the progress and better assist in diagnosing potential problems.

Select Connection Mode: Select the desired Connection Mode from the drop-down menu.

- **Primary Only:** The SixView Manager client only connects to the Primary Server.
- **Secondary Only:** The SixView Manager client only connects to the Secondary Server.
- **Both:** The SixView Manager client connects to the Primary and Secondary Servers.
- **Secondary when Primary unavailable:** The SixView Manager client preferentially connects to the Primary, using the Secondary as a backup.

The recommended setting is “Secondary when Primary unavailable” or “Both” are the preferred methods in configurations supporting redundant SixView Manager servers.

Enter Access Interval (minutes) (Required): Enter the number of minutes the SixView Manager Client process should wait before connecting to the SixView Manager server. A value of 220 is suggested for Cellular carriers that use an inactivity time out of four hours.

Note: While lower values can result in more timely status reports with the SixView Manager Server, it comes at an expense of increased data traffic, which may be an issue when the connection utilizes a cellular modem with a service plan where cost is based on bandwidth usage. A value of 220 is suggested for Cellular carriers that use an inactivity timeout of four hours.

Enter Error Interval (minutes) (Required): Enter the number of minutes the SixView Manager client should wait before re-attempting a previously failed check-in attempt. The recommended setting for this field is 30.

Select Access Method: Select the desired Access Method from the provided drop-down. There are two (2) access methods:

- **Unencrypted (http):** Faster, but less secure.
- **Encrypted (https):** Slower, but more secure.

Note that the encrypted method adds significant overhead which may be a consideration when using a cellular modem connection. For example, if an ipsec_restart is an option, then when selected, will be run whenever the fallback logic selects and activates this interface.

Enter SixView Manager Server Port # (Required): If the SixView Manager Server has been configured to accept connections on a port other than its standard default, that custom port number should be entered in this field. The administrator of the SixView Manager Server will be able to provide you with the necessary information to properly set this parameter. The recommended setting for this field is 18081.

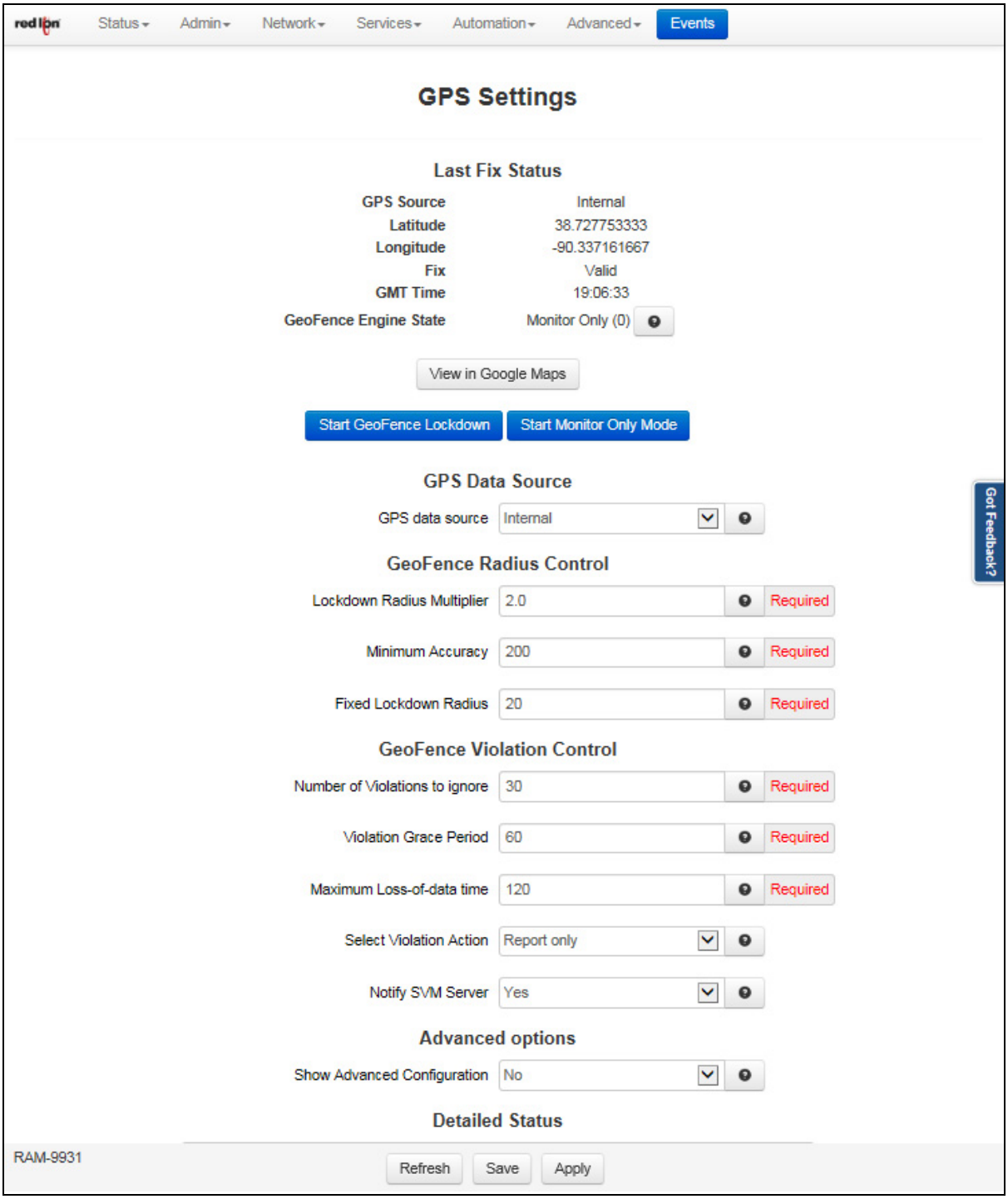
Select Interface: Select the name of the interface to which the SixView Manager Client will bind for communications with the SixView Manager Server. The recommended setting for this field is *None*.

Note: This option will only be necessary if the SixView Manager Client is required to communicate through a configured IPSec, GRE or IPIP tunnel.

Click *Apply* for the settings to take effect immediately. Selecting *Revert*, will reset all fields to factory defaults.

3.5.6 GPS Settings

Click on the GPS Settings menu item and the following dialog window appears:



GeoFence Engine State: Options and descriptions are listed in this field. Eventable register state is listed in parenthesis next to the label.

Monitor Only (0): Reporting GPS location only. No GeoFence Lockdown.

Lockdown - Waiting for Data (1): Waiting on GPS data to compute lockdown fence.

Lockdown - Wait for Entries (2): Have data, but waiting on more entries to compute fence.

Lockdown - Wait on Satellites (3): Have entries, but waiting on better satellites to compute fence.

Lockdown - Failed (4): Lockdown failed to build GeoFence (same behavior as Monitor Only).

Lockdown - Good (5): Successful lockdown. Fence built, and we are inside the GeoFence.

Lockdown - Unstable (6): ALERT. We are ok, but stray data points keep going outside fence, but are within satellite.

Lockdown - Violation Alert (7): ALERT. We are out of lockdown GeoFence. No Action Taken Yet.

Lockdown - Violation Outside (8): ERROR. We are out of lockdown GeoFence. Violation Action Taken.

Lockdown - Violation no Data (9): ERROR. We lost GPS data for enough time, that we don't know where we are. Violation Action Taken.

Lockdown - Unknown State: Undefined action type.

View in Google© Maps: Click on the button to view the physical location of the unit on Google maps.

Start GeoFence Lockdown: Click on this button to lock the device into a specific area. If the device moves from this location, the Select Violation Action selected in the GeoFence Violation Control section will come into effect. To disable the GeoFence Lockdown, start Monitor Only Mode.

Start Monitor Only Mode: Click on this button to log a violation. A violation will be logged but the option selected in the Select Violation Action field will not be performed.

GPS Data Source

Select GPS data source: Select where the data source data is gathered from. The available choices are:

Internal: If this option is selected and GPSd is available on the system, the data will be gathered from the GPSd process. This process will automatically poll GPS data from supported devices as they are attached. This includes onboard GPS chipset, and cellular GPS from some series (RAM-6900).

External: If this option is selected, data is gathered from an attached external GPS device. Specify the tty port that the device will be attached to, as well as the serial data rate (defaulted to 4800, found in Advanced).

Fixed: If Fixed is selected, GPS data will not be collected from any real source, but will be emulated as always being the fixed values entered by the user. Any Lat/Long point may be specified, in decimal format, with negative meaning S or W.

GeoFence Radius Control

Lockdown Radius Multiple (Required): Enter the value of the Lockdown Radius Multiplier in this field. The recommended setting for this field is 2.

When the Geofence engine begins to build a fence, it will create a Calculated Minimum Radius allowed using an accuracy figure based on the acquisition 200 GPS location points obtained over an initial settling interval of about 15-20 minutes. This value is then multiplied by the Lockdown Radius Multiplier to obtain the Modified Minimum Radius.

The Modified Minimum Radius will not be allowed to become less than the Minimum Accuracy, and will be adjusted to the Minimum Accuracy as prevailing conditions require. The allowable range is 1.0 - 5.0.

Minimum Accuracy (Required): Enter the value of the Minimum Accuracy in this field. The recommended setting for this field is 50-200.

When the GeoFence engine begins to build a fence, it will calculate an allowed Minimum Radius using an accuracy figure based on an average of 200 location points acquired over an interval of 15-20 minutes. This value is then multiplied by the Lockdown Radius Multiplier to obtain the Modified Minimum Radius.

The Modified Minimum Radius will not be allowed to be less than the Minimum Accuracy, and will be increased to the Minimum Accuracy as needed. The Minimum Accuracy will also provide a lower limit for the Fixed Lockdown Radius. The allowable range is 0-2000.

Fixed Lockdown Radius (Required): The value of the Fixed Lockdown Radius may be entered in this field. The recommended setting for this option is 0 (off).

GeoFence behavior can be described in the following ways:

- **Flexible radius**: To select this option, the Fixed Lockdown Radius must be set to **0**.
- **Flexible radius with additional fixed buffer:** To select this option, enter a value, preceded with '**+**'.
- **Fixed radius:** To select this option, enter any non-zero value.

During the establishment of a GeoFence, a set of 200 location points are obtained over a period of 15-20 minutes to determine an initial 'minimum radius' possible for the device. The Flexible radius behavior uses the *Calculated Minimum Radius* and the configured *Lockdown Radius Multiplier* values to set the GeoFence boundary. Setting the *Fixed Lockdown Radius* to a positive offset (+20, for example) has the effect of adding a fixed amount of buffer space to the *Calculated Minimum Radius*, and the *Lockdown Radius Multiplier* has no effect.

For Fixed Radius behavior, the configured value for the *Fixed Lockdown Radius* is used to set an absolute minimum radius for the GeoFence, subject to increase by the configured *Minimum Accuracy* or *Calculated Minimum Radius* values as needed.

Note that since the calculated minimum radius may change over time depending on acquired GPS location data, the value will never be allowed to become less than the *Minimum Accuracy* nor the *Calculated Minimum Accuracy*.

GeoFence Violation Control

Number of Violations to ignore (Required): Enter the number of violations to ignore in this field. The recommended value for this field is 10-30 points (approximately 20-60 seconds).

To limit false alarms from occasional drifting GPS points, this value will ignore a certain number of anomalous points before alerting a SixView Manager server. This prevents an inaccurate site from constantly updating the SixView Manager with dubious information. New points are received about every 2 seconds. The allowable range is 0-300.

Violation Grace Period (Required): The value of the Grace Period may be entered in this field. The recommended setting for this field is 60.

Once we have ignored the first few anomalous location fixes, points outside the GeoFence are considered a violation. This timer specified (in seconds) how long to tolerate points outside the GeoFence boundary, before declaring a full "Violation Outside" and enacting the "Violation Action". The allowable range is 30-600.

Maximum Loss-of-data time (Required): The maximum number of seconds for which no GPS data is received may be entered in this field. The recommended setting for this field is 120.

Ordinarily, a GPS device generates location information updates on a continuous regular periodic basis. A loss of these updates may be due to a temporary or intermittent reception issue, or due to the device having been moved to an area devoid of GPS reception or disconnection or an external GPS receiver, either deliberately or accidentally by persons authorized to do so or not.

This parameter sets the period of GPS data loss beyond which the device may be considered having been tampered with and subject to securing actions. The allowable range is 30-1200.

Select Violation Action: Select the action to be taken when a protected perimeter violation occurs using the drop-down list provided. The available options are:

- Report Only: The device reports violation events to a SixView Manager server.
- **Block Network:** All network traffic, except to a SixView Manager server, will be blocked.
- **Block All:** In addition to the actions taken in Block Network, all access to the device including via physical ports (console, etc.) is blocked.
- **Custom:** Configured special actions are applied.

Notify SVM Server: Control whether GeoFence status changes are reported to the SVM Servers configured in Services→SixView Manager.

Advanced options

Show Advanced Configuration: Select Yes to configure advanced GPS parameters.

Valid Points (Required): The maximum number of valid GPS location entries required for GeoFence boundary establishment may be entered in this field. The recommended setting for this field is 200.

This configures the number of GPS Data points to collect before building the GeoFence boundary. These points are collected when instructed to go into initial Lockdown mode. Larger values require more time to build the initial fence, yet may yield a more accurate Calculated Minimum Radius. The allowable range is 100-1000.

Distance Reporting Threshold (Required): The value for the Distance Reporting Threshold may be entered in this field.

When not in GeoFence Lockdown, a Distance Threshold exceeded message will be sent to a SixView Manager server every time the unit is moved more than the configured amount (in feet) from its previously recorded location. This is typically only useful in a mobile application. The allowable range is 200-1000000 (feet).

Require User Cleared Violations: Select whether the user is required to clear perimeter violations using the drop-down list provided. The recommended setting for this field is 0. Available values are:

- No
- Yes

Whenever a full violation state has been reached (Violation Outside or Violation No Data), the next good GPS data point received will automatically clear the violation and return the unit to “Lockdown Good”. When this option is set to Yes, then the Violation will NOT be cleared until a SixView Manager server or user sends down a command to re-initiate Lockdown. This will build a new GeoFence boundary based on current location and radius parameters.

Maximum log entries (Required): The value for Maximum log size may be entered in this field. The recommended value for this field is 600.

Number of log entries to keep in a GPS raw log in NMEA format. Raw GPS Log access is available upon request. A new log entry will be generated according to the setting in Raw Log Interval. A maximum of 50k is saved. The allowable range is 100-1000.

Discardable # outlier points (Required): The value of the # Outlier Points to Ignore may be entered in this field. The recommended setting for this field is 5.

When a GeoFence is being established, the GPS engine ignores a certain number of the first few anomalous location fixes before points outside the GeoFence are subject to **violation** actions. After that initial ‘settling period’, each new GPS point must be examined in relation to the established boundary. Even under ideal conditions, intermittent signal reception and/or multipath interferences issues can result in points being erroneously reported beyond the GeoFence boundary. This parameter can be used to tune the filtering of this ‘jitter’ to reduce the likelihood of a false positive GeoFence violation. The allowable range is 0-50.

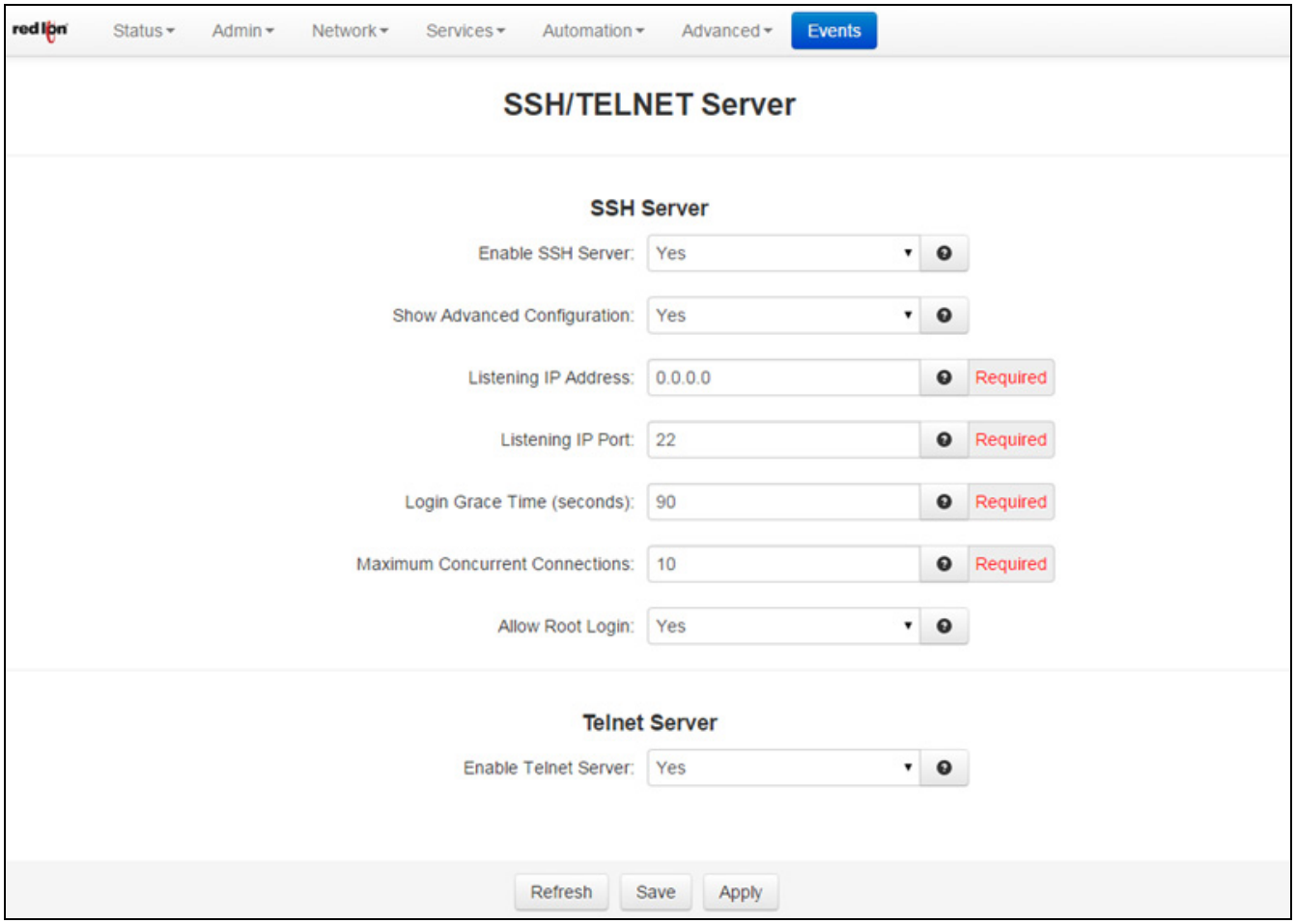
Log Update Interval (seconds): This parameter determines how often (in seconds) the current GPS data point will be saved in NMEA format in a Raw GPS logfile. The allowable range is 5-10000.

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert*, will reset all fields to factory defaults.

3.5.7 SSH/TELNET Server

The SSH/TELNET Server menu allows you to configure whether the Red Lion RTU or router will communicate with the network via Secure Shell (SSH) and to enable or disable TELNET on the Red Lion RTU or router.

Click on the SSH/TELNET menu item and the following dialog window appears:



SSH Server

Enable SSH Server: Select YES to enable the SSH server. *Note:* Enabling the SSH Server does not, by default, allow SSH data through the firewall. If you have connection problems, please check your firewall settings.

Configure Advanced Parameters: Select YES to configure advanced options for the SSH Server (Optional). The recommended setting for this field is NO.

Listening IP Address: Specifies the local IP Address on which the SSH server will accept connections. *Note:* Specifying a value of 0.0.0.0 allows the SSH server to accept connections on any interface. Firewall rules must be present to allow SSH connection on untrusted interfaces. The recommended setting for this field is 0.0.0.0.

Listening IP Port: Specifies the local IP port on which the SSH server will accept connections. *Note:* Specifying a value other than 22 will require proper firewall rules in order to allow connections to the given port. The recommended setting for this field is 22.

Login Grace Time (seconds): Specifies the amount of time, in seconds, after which the SSH server will disconnect, if the user has not successfully logged in. The recommended setting for this field is 30.

Maximum Concurrent Connections: Specifies the maximum number of concurrent unauthenticated connections to the SHH server. Additional connections will be dropped until authentication succeeds, or the Login Grace Time expires for a connection. The recommended setting for this field is 10.

Allow Root Login: Specifies whether root can log in directly to the SSH server. The recommended setting for this field is *No*.

Telnet Server

Enable Telnet Server: Select YES to enable the Telnet Server. *Note:* Enabling the Telnet Server does not, by default, allow Telnet data through the firewall. If you have connection problems, please check your firewall settings.

The recommended setting for this field is NO.

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert*, will reset all fields to previously saved defaults.

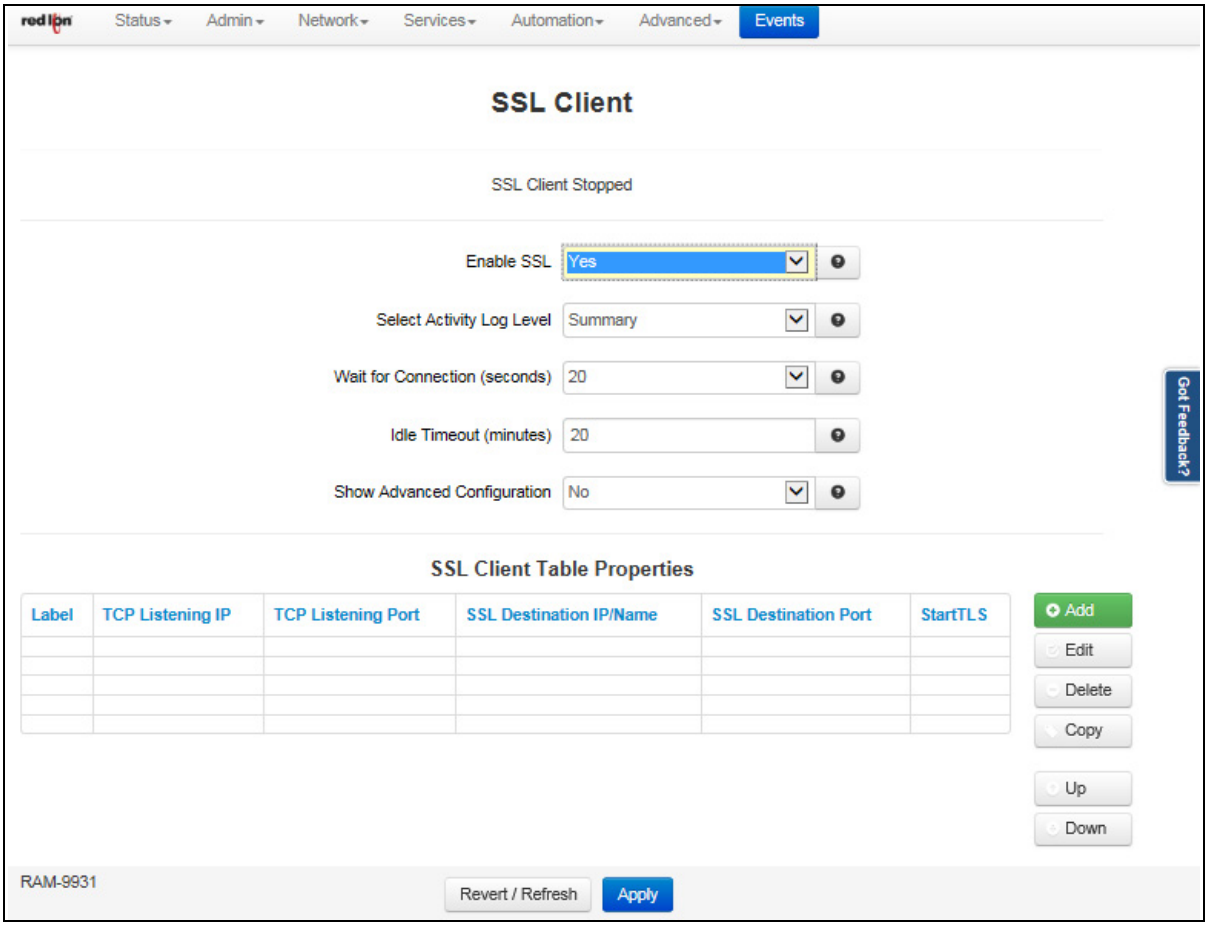
3.5.8 SSL Connections

The SSL Connections menu item is used to configure the Red Lion RTU or router to either act as a Secure Socket Layer (SSL) Client to receive certificates or as an SSL Server to issue certificates. The SSL Connections tab is sub-sectioned into the SSL Client and the SSL Server.

SSL Client

The SSL Client menu item is used to configure the Red Lion RTU or router to be a SSL client and receive a certificate of authorization from an SSL server to authenticate connections for secure communications.

Click on the *SSL Client* menu item and the following dialog window appears:



Enable SSL: Select Yes to configure SSL client/server. Select No and then the Apply button to disable SSL.

Select Activity Log Level: This option controls the logging level for SSL Connection activity. The recommended setting for a production environment is: Summary. For a test environment: Full.

Wait for Connection (sec.): Time (in seconds) allowed after sending SYN packets, to wait for SYN-ACK. The recommended setting for this field is 20 seconds.

Idle Timeout (min): Time (in minutes) allowed for no traffic over an SSL connection, before closing down the link. The recommended setting for this field is 720 (minutes).

Enable Advance Setup: Select Yes to modify advanced SSL options.

Bind Interface for accepting TCP Connections: This will restrict the unencrypted listening socket to allow connections coming into the specified interface only. The recommended setting for this field is *Any*.

Bind Interface for outgoing SSL Connections: This will restrict the encrypted socket to initiate connections out the specified interface only. Specifying an interface here may conflict with policy routing, however it may be required in a GRE/VPN or other tunneled environment. Please consult with a network architect for additional assistance. The recommended setting for this field is *Any*.

Ciphers: This field is a list of supported openssl ciphers. Please consult support staff before attempting to change these values. Reference Google: "openssl cipher list" for more information.

Select Certificate: Specifying a certificate in client mode uses this certificate chain as a client side certificate chain. Using client side certs is optional. The certificates must be in PEM format, with an unencrypted key (not password protected when generated). Use Admin→Certificate Manager to install/update certs.

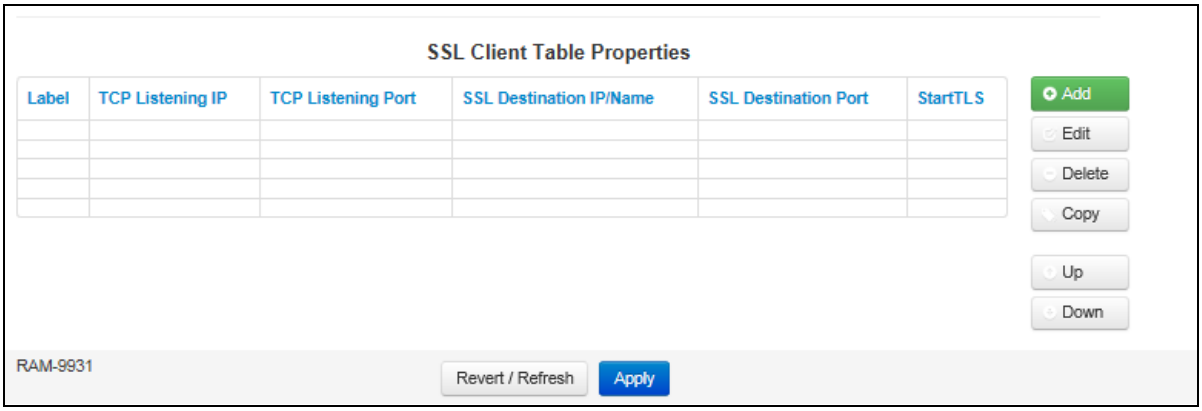
Select Keep-Alive behavior: This option enables TCP Keep-alives on the underlying sockets. The following options are supported:

- **None:** Keep-alives not used.
- **All:** Keep-alives enabled for all sockets.
- **Accept:** Keep-alives enabled for listening server socket side connections only. This applies to the clear text server for Client mode sockets, or the SSL Encrypted server for Server mode sockets.
- **Remote:** Keep-alives enabled for client initiated sockets.
- **Local:** Keep-alives enabled for Client connections bound to a local IP address.

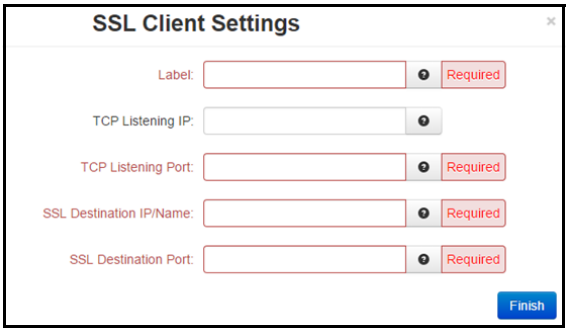
You may need to adjust the master Keep-alive timer via Network→TCP Global Settings→TCP Keep Alives.

Note: Enabling TCP keep-alives may dramatically increase the total amount of traffic for the affected socket(s) depending on the master interval, probe and timeout settings, which should be considered for connections using a wireless (cellular) connection with respect to total data usage for the subscripted plan.

SSL Client Table Properties:



Click on the *Add* button and the following dialog window appears:



Label (Required): Enter a unique name to describe this connection.

TCP Listening IP: Enter the IP to listen on for incoming connections. If not using static IP addresses, it is recommended to use the Advanced Setup option “Bind Interface for accepting TCP Connections” instead. The recommended settings for this field are:

- Leave Blank (0.0.0.0) to allow connections from any interface.
- Use 127.0.0.1 for internal connection use only (gwlnx Protocol Converter).

TCP Listening Port (Required): Enter the listening port for this connection. Please note that this port must be allowed in the Firewall access rules for any external/untrusted interface. It may be useful to review the results of ***Status→Network→Socket Statuses→TCP Only*** to confirm that your choice of listening port is not already in use. (Ports under “Local Address” with a state of “Listen” are in use.)

SSL Destination IP (Required): Enter the IP or Domain Name of the SSL server to which you would like to connect.

SSL Destination Port (Required): Enter the Port number of the SSL server to which you would like to connect.

Click on the *Finish* button. You will be returned to the DHCP Relay dialog window and the Remote Servers table will be populated with the entered data.

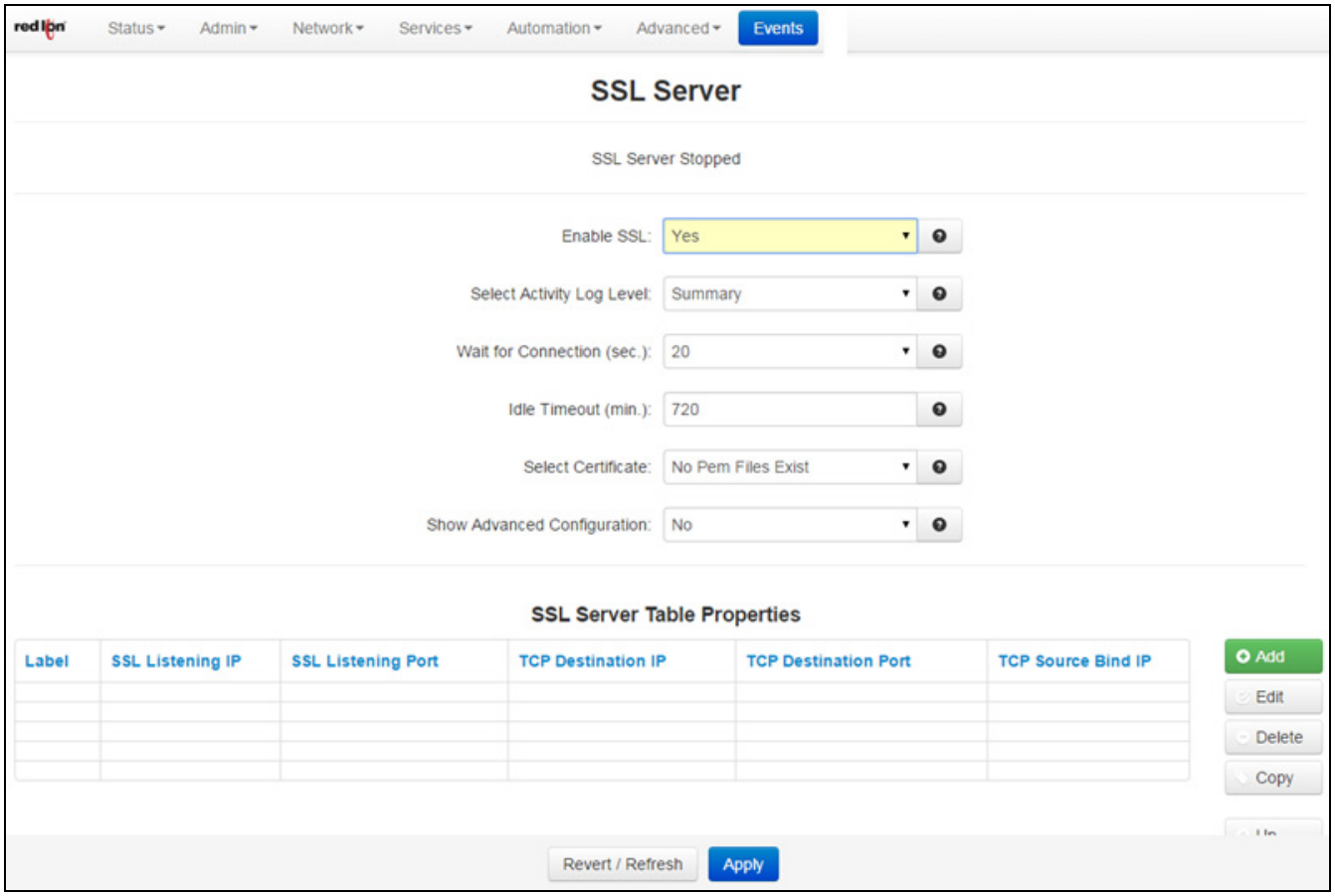
To delete an existing SSL Client, select it in the table and click on the *Delete* button. To edit an SSL Client, select it in the table and click on the *Edit* button.

Click *Save* to store the settings for the next reboot, or click APPLY for the settings to take effect immediately. Selecting Revert, will reset all fields to previously saved defaults.

SSL Server

The SSL Server menu item is used to configure the Red Lion RTU or router to issue SSL certificates to requesting SSL clients.

Click on the *SSL Server* menu item and the following dialog window appears:



Enable SSL: Select Yes to configure SSL client/server. Select No and click the Apply button to disable SSL.

Select Activity Log Level: This controls the logging level for SSL Connection activity. The recommended setting for a production environment is *Summary*. The recommended setting for a test environment is *Full*.

Wait for Connection (sec.): Time (in seconds) allowed after sending SYN packets, to wait for SYN-ACK. The recommended setting for this field is 20 seconds.

Idle Timeout (min.): Time (in minutes) allowed for no traffic over an SSL connection, before closing down the link. The recommended setting is 720 minutes.

Select Certificate: A server certificate must be provided. This will be used to encrypt communication with all clients. The certificates must be in PEM format, with an unencrypted key (not password protected when generated). Self signed certificates are highly recommended. Use Admin→Certificate Manager to install/ update certs.

Enable Advanced Setup: Select Yes to modify advanced SSL options.

Bind Interface for accepting SSL Connections: This will restrict the encrypted listening socket to allow connections coming into the specified interface only. The recommended setting for this field is *Any*.

Bind Interface for outgoing TCP Connections: This will restrict the unencrypted socket to initiate connections out the specified interface only. Specifying an interface here may conflict with policy routing,

however it may be required in a GRE/VPN or other tunneled environment. Please consult with a network architect for additional assistance. The recommended setting for this field is *Any*.

Ciphers: This field is a list of openssl ciphers supported. Please consult support staff before attempting to change. Reference Google:"open ssl cipher list" for more information. The recommended settings for this field are: RC4-MD5:RC4-SHA:SSLv3.

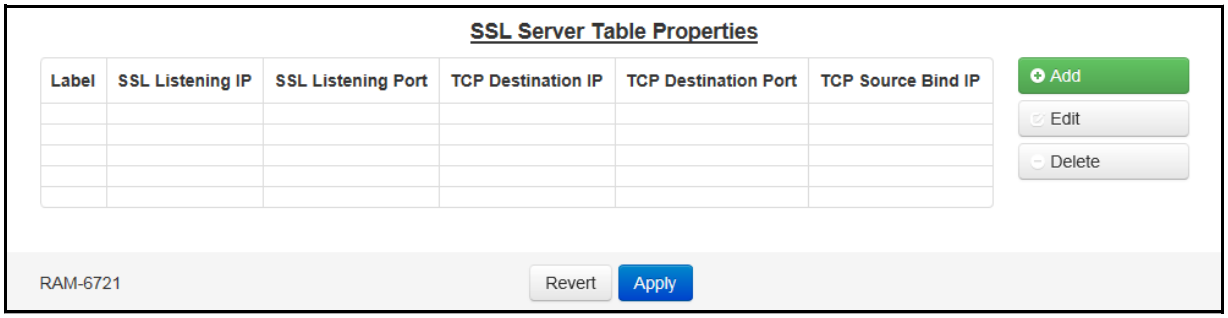
Select Keep-Alive behavior: This option enables TCP Keep-alives on the underlying sockets. The following options are supported:

- **None:** Keep-alives not used.
- **All:** Keep-alives enabled for all sockets.
- **Accept:** Keep-alives enabled for listening server socket side connections only. This applies to the clear text server for Client mode sockets, or the SSL Encrypted server for Server mode sockets.
- **Remote:** Keep-alives enabled for client initiated sockets.
- **Local:** Keep-alives enabled for Client connections bound to a local IP address.

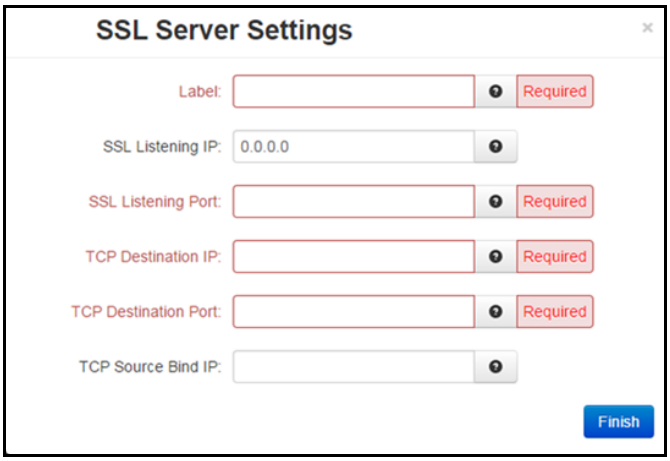
You may need to adjust the master Keep-alive timer via Network→TCP Global Settings→TCP Keep Alives.

Note: Enabling TCP keep-alives may dramatically increase the total amount of traffic for the affected socket(s) depending on the master interval, probe and timeout settings, which should be considered for connections using a wireless (cellular) connection with respect to total data usage for the subscripted plan.

SSL Server Table Properties



Click on the *Add* button and the following dialog window appears:



Label (Required): Enter a unique name to describe this connection.

SSL Listening IP: Enter the IP to listen on for incoming SSL connections. If not using static IP addresses, it is recommended to use the Advanced Setup option "Bind Interface for accepting TCP Connections" instead. The recommended setting for this field is to leave it blank (0.0.0.0) to allow connections from any interface.

SSL Listening Port (Required): Enter the listening port for SSL connections. Please note that this port must be allowed in the Firewall access rules for any external/untrusted interface. It may be helpful to review the results of Status→Network→Socket Statuses→TCP Only to confirm that your choice of listening port is not already in use. (Ports under “Local Address” with a stat of “LISTEN” are in use.)

TCP Destination IP (Required): Enter the IP or Domain Name of the standard TCP server to which you would like to connect. Use 127.0.0.1 for internal connection use only (gwlnx Protocol Converter, or OOB Encryption Setup).

TCP Destination Port (Required): Enter the Port number of the standard TCP server to which you would like to connect.

TCP Source Bind IP: Enter the IP to bind for outgoing TCP connections. If not using static IP addresses, it is recommended to use the Advanced option “Bind Interface for outgoing TCP Connections”. The recommended setting for this field is to leave it blank for normal operation (no binding).

Click on the *Finish* button. You will be returned to the DHCP Relay dialog window and the Remote Servers table will be populated with the entered data.

To delete an SSL Server, select it in the table and click on the *Delete* button. To edit an existing SSL Server, select it in the table and click on the *Edit* button.

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert*, will reset all fields to previously saved defaults.

3.5.9 SNMP Agent

SNMP (Simple Network Management Protocol) is an industry standard way of querying networking devices to obtain statuses, updates, alerts and behaviors.

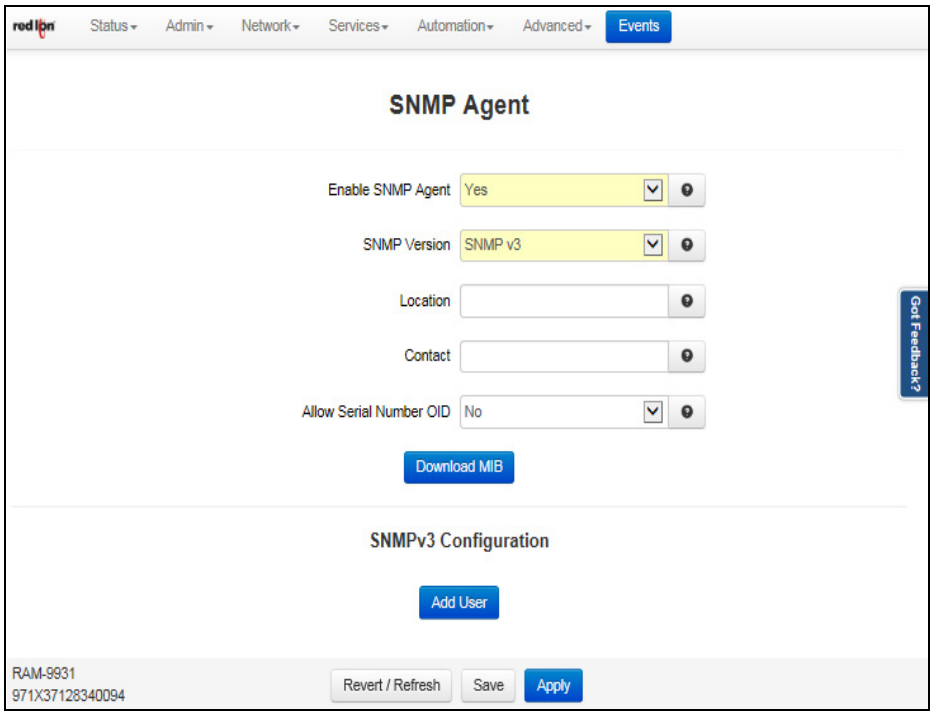
To retrieve SNMP data from the Red Lion device you must have an SNMP manager or Server at the head end. The Red Lion RTU or router will only act as an SNMP client, providing data it is polled for. It will not act as a manager to poll other devices.

The SNMP Agent allows you to query the unit for information via SNMP using what is called a MIB (Management Information Base). Standard MIB-II queries are supported, as well as a custom RED-LION-RAM.MIB. A great deal of useful information about the unit interface, including cellular signal strength, interface status, and more can be queried. When configuring firewalls to allow SNMP traffic, be sure to allow access to port 161 so that the device may return its results. This is the industry standard port number for SNMP traffic.

A complete listing of the OIDs found in the RED-LION-RAM.MIB can be found in the Appendix at the end of this manual.

* The community string is “public” (do not enter the quotes).

Click on the *SNMP Agent* menu item and the SNMP Agent dialog window appears:



Enable SNMP Agent: Select YES to enable the SNMP Agent. Note: Enabling the SNMP Agent does not, by default, allow SNMP data through the firewall. If you have connection problems, please check your firewall settings.

SNMP Version: Select the SNMP version to use for the device SNMP agent.

SNMP v1/v2c: Provides a community string sent in plaintext with no authentication or privacy.

SNMP v3: Provides both authentication and privacy, which can be used separately or together.

Community String for SNMP Agent Access (Required for SNMP v1/v2c): Specify the community string to use for authentication between the SNMP Agent and Manager. Alpha-numeric strings are supported. **Note:** The community string must match on both ends of the connection in order to work.

The default community string for the RED-LION-RAM.MIB is “public”.

Location: Enter the physical location where the unit is stored. This field is useful in determining where a device is located. The maximum amount of characters that can be used in this field is 250 ASCII characters.

Contact: Enter the name of the contact person for this managed device. This field is useful in determining who to contact in the event of an issue. The maximum amount of characters that can be used in this field is 250 characters.

Allow Serial Number OID: Select YES to allow users and management systems to retrieve the unit serial number from the SNMP Agent. If NO is selected, a query of the serial number OID will return “UNKNOWN”.

Download MIB: Click on this button to download the MIB file.

Add User (Used with v3): Click on this button to enter the user settings in the SNMPv3 User Settings pop-up.

User Name (Required): Enter the User Name. The user name can contain up to 32 characters and include any combination of alphanumeric characters. Spaces are not allowed.

Authentication Type: Select the desired Authentication Type for the configured SNMPv3 user. This option is required for SNMPv3 functionality.

None: No authorization and no privacy, basically no security.

MD5: Insecure Message Digest algorithm.

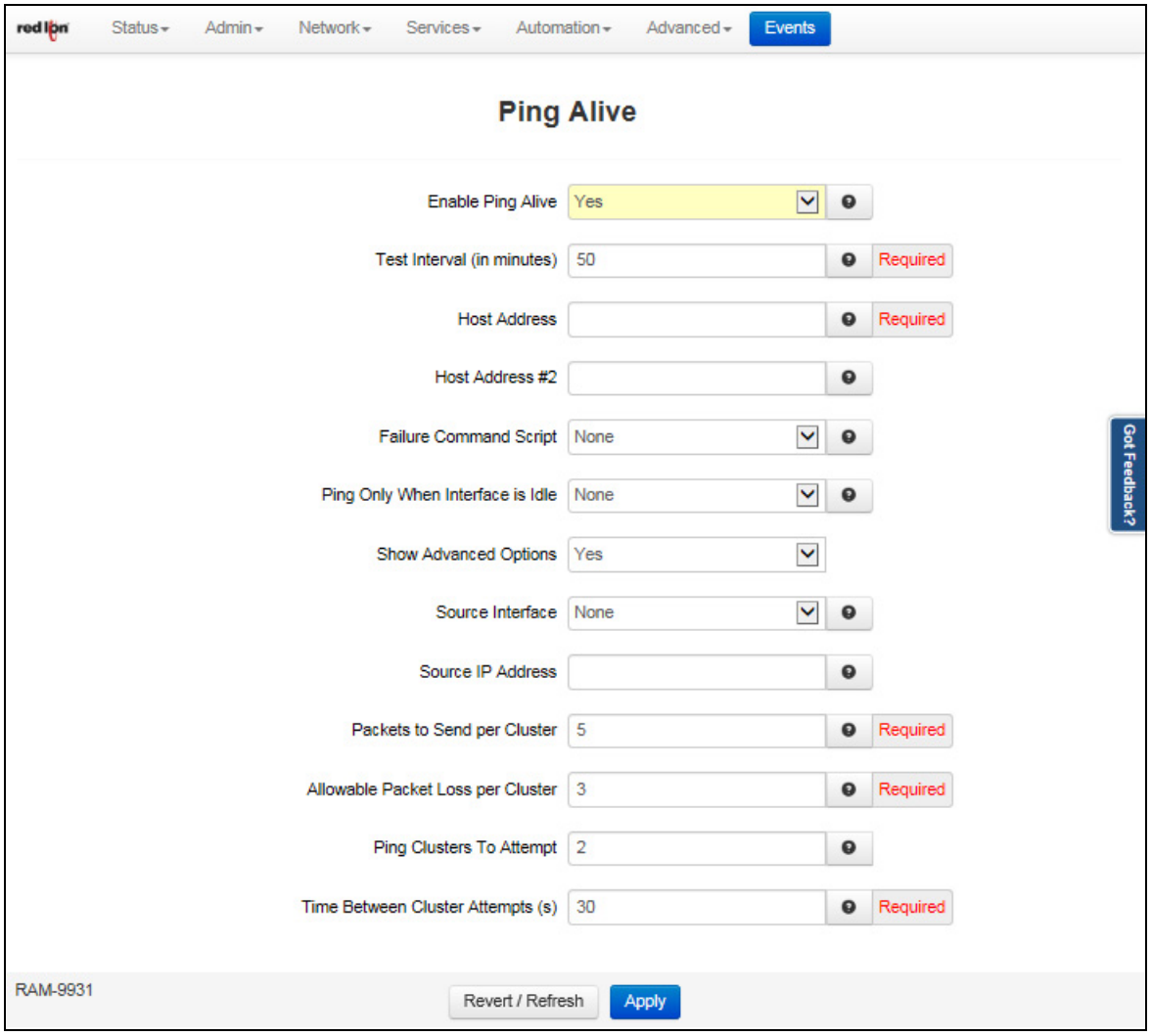
SHA: secure Hash Algorithm.

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert*, will reset all fields to previously saved defaults.

3.5.10 Ping Alive

Ping is a diagnostic tool used for verifying connectivity between two hosts on a network. It sends ICMP (Internet Control Message Protocol) echo request packets to a remote IP address and watches for ICMP responses.

Select the *Ping Alive* tab menu and the following dialog window appears:



Enable Ping Alive: Select YES to enable the Ping Alive Service. The recommended setting for this option is NO. Ping Alive will send the specified number of packets in Test Packets to Send, every interval defined in Test Interval. Should the ping fail to the first host, a second host may also be defined. Host Fail Type will control how many hosts must fail before a failure is declared and Failure Command Script will execute the failure action specified at that time. This can be used to force interface traffic, or to probe connectivity to an end point.

Test Interval (in minutes)(Required): Enter the time interval (in minutes) to which the ping packets would be sent. The recommended setting for this option is 50.

Host Address (Required): Enter the IP Address of the destination host to which the ping packet would be sent. Default setting is “127.0.0.1”.

Host Address #2: Enter the IP Address of the second destination host to which the ping packet would be sent. This second host is tested only when the first one fails. There is no default setting for this option.

Failure Command Script: Choose the name of the command script to be executed when the PING test fails. For example, if “Restart Wireless” is an option, then when selected, the wireless interface will be restarted.

Note: Recommended setting is “*None*” for standard operation with no special behaviors. “*RestartWireless*” is useful when using a wireless (cellular) interface. “*Reboot*” will restart the entire device.

Ping Only When Interface is Idle: Select the name of the interface which the ping alive service will monitor for activity. This service will send a ping ONLY when the connection for the selected interface is idle or reset. Recommended setting is "*None*".

Note: If **None** is selected, this functionality is disabled.

Show Advanced Options: Displays the following fields when selected.

Source Interface: Select the name of the interface to which the service will bind for communications tests. When set to *None*, the system will choose automatically. The recommended setting for this option is None.

Source IP Address: Enter the IP address to use as a source for communications tests. Note: This will be the source IP address of the PING packets, but does not necessarily reflect the interface from which packet will traverse the unit.

Packets to Send per Cluster (Required): Specify the number the ping packets to send out to test connectivity. The minimum is 1 and the maximum is 10. The recommended setting for this field is 5 - 10.

Allowable Packet Loss per Cluster (Required): Specify the number of lost packets that are acceptable before the link is considered unavailable.

Note: The value must be less that the number of test packets set via Test Packets to Send.

Example: If Test Packets to Send is set to 5 and Allowable Packet Loss is set to 3, then 2 pings of the 5 sent out must have replies for connectivity to be declared successful. If only 1 ping reply is received, then a failure to that host will be declared.

Ping Cluster to Attempt: Enter the number of cluster ping attempts to retry before determining a failure. If one set of pings succeeds to pass, the next test will be performed on the next interval. If all attempts fail, then the configured action(s) are performed. The valid cluster ping attempts range is 1 -5.

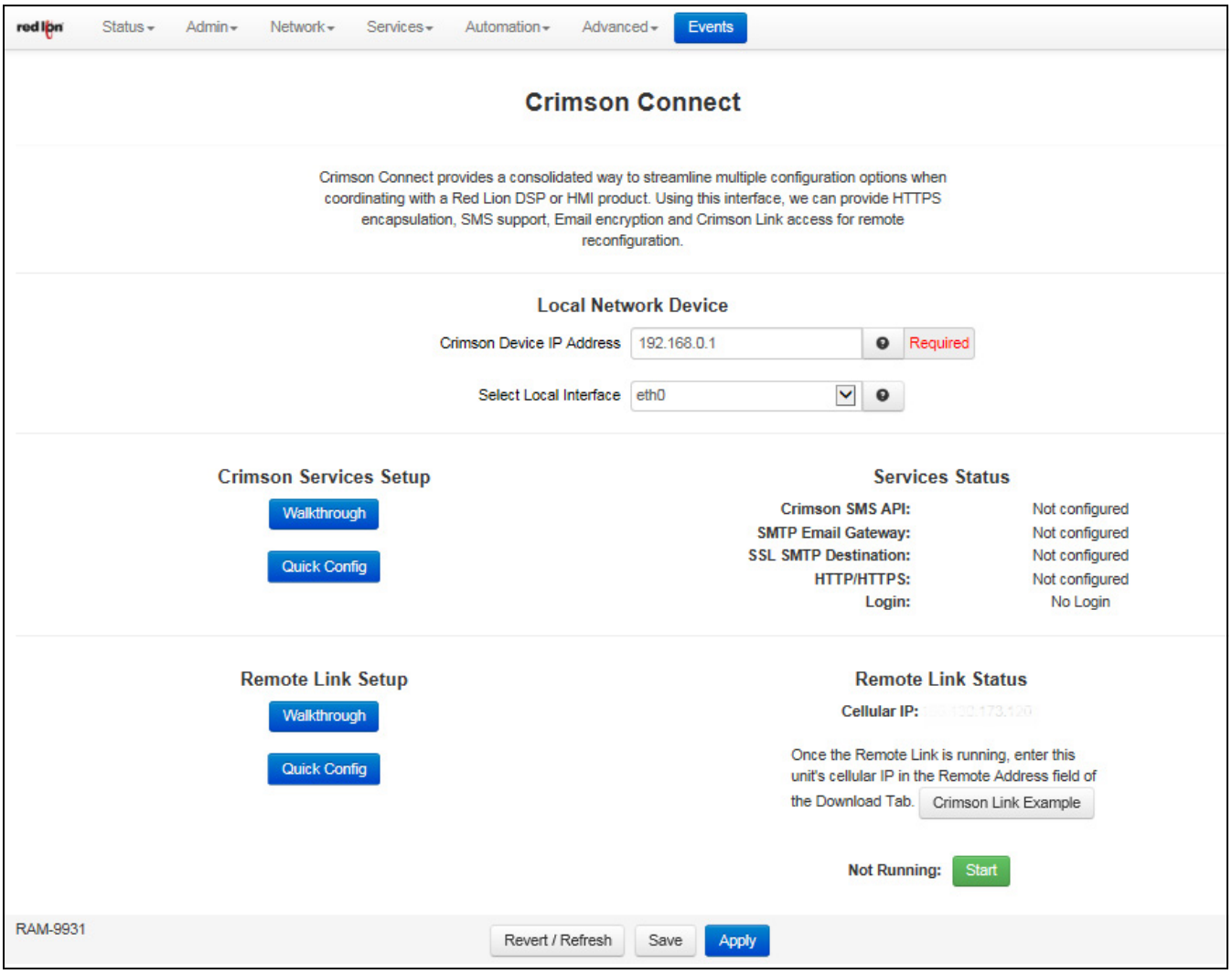
Time Between Cluster Attempts: Enter the number of seconds to wait between Cluster Ping Attempts. The valid grace period wait range is 15 - 300.

Click on the *Apply* button for the changes to take effect. Selecting Revert / Refresh, will reset all fields to previously saved defaults.

3.5.11 Crimson Connect

Crimson Connect provides a consolidated way to streamline multiple configuration options when coordinating with a Red Lion DSP or HMI product. Using this interface provides HTTPS encapsulation, SMS support, Email encryption and Crimson Link access for remote reconfiguration.

Settings for this feature work in conjunction with settings from the Crimson software. Please consult your Crimson manual for setup information as indicated in sections below.



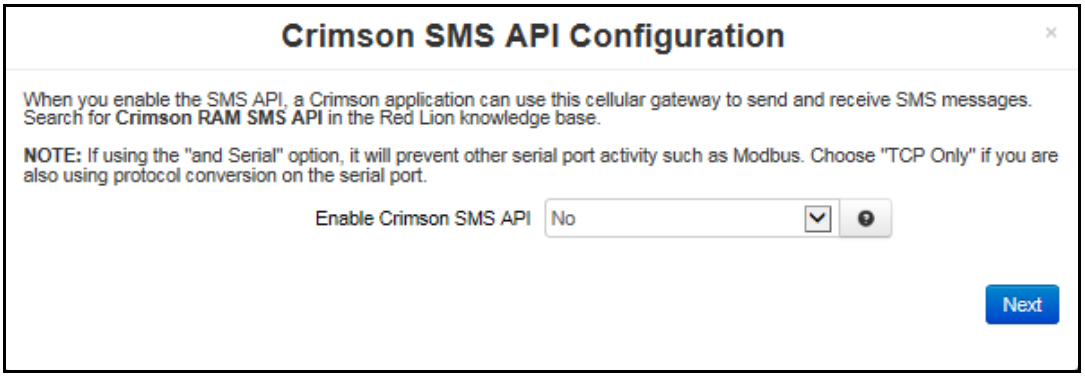
Crimson Device IP Address: Enter the IP address of your local Crimson device. Use Status→Diagnostics→Ping to test connectivity to your device.

Select Local Interface: Select the local interface used to connect to the Crimson device (eth0 or eth1).

Crimson Services Setup

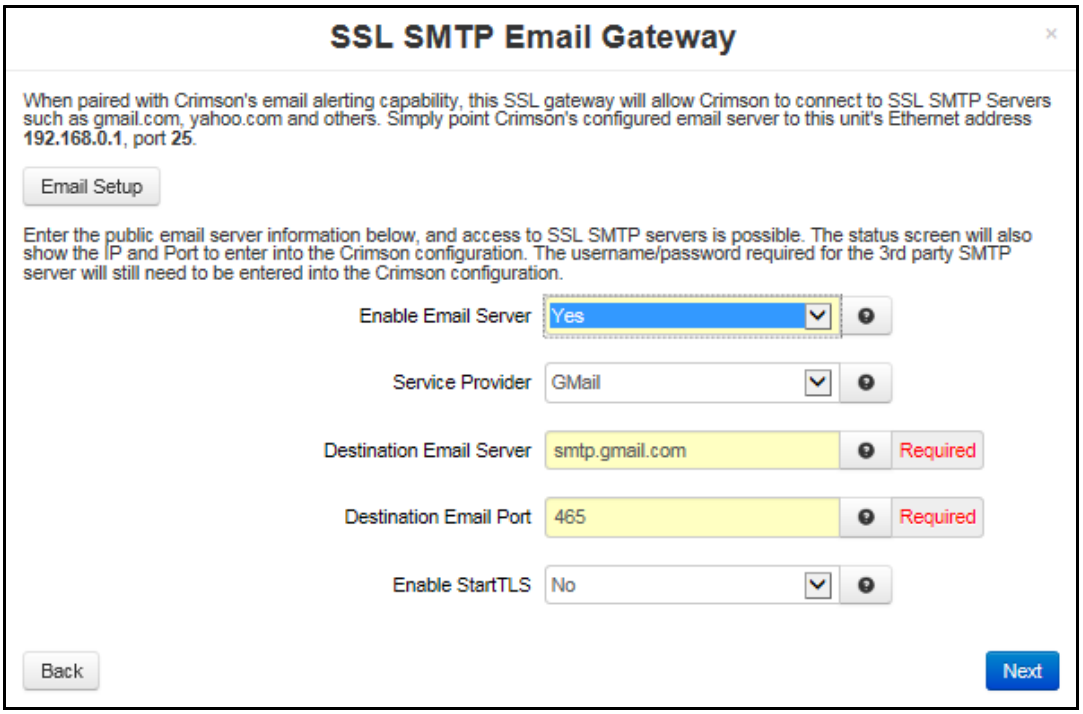
Walkthrough: This option provides step-by-step instructions for Crimson Services setup.

Click on the Walkthrough button to begin the Crimson Services setup. The Crimson SMS API Configuration window will pop-up.



Enable Crimson SMS API: Enable the Crimson SMS API interface on port 1000. See Crimson HOWTO guide for more information and instructions on how to configure your Crimson application to connect to these SMS services.

Click on the Next button.



Email Setup: When paired with Crimson's email alerting capability, this SSL gateway allows Crimson to connect to SSL SMTP Servers such as gmail.com, yahoo.com and others. Simply point Crimson's configured email server to this unit's Ethernet address **192.168.208.136** and Server Port **25**. Please view the Crimson Manual for instructions on how to setup Mail Manager.

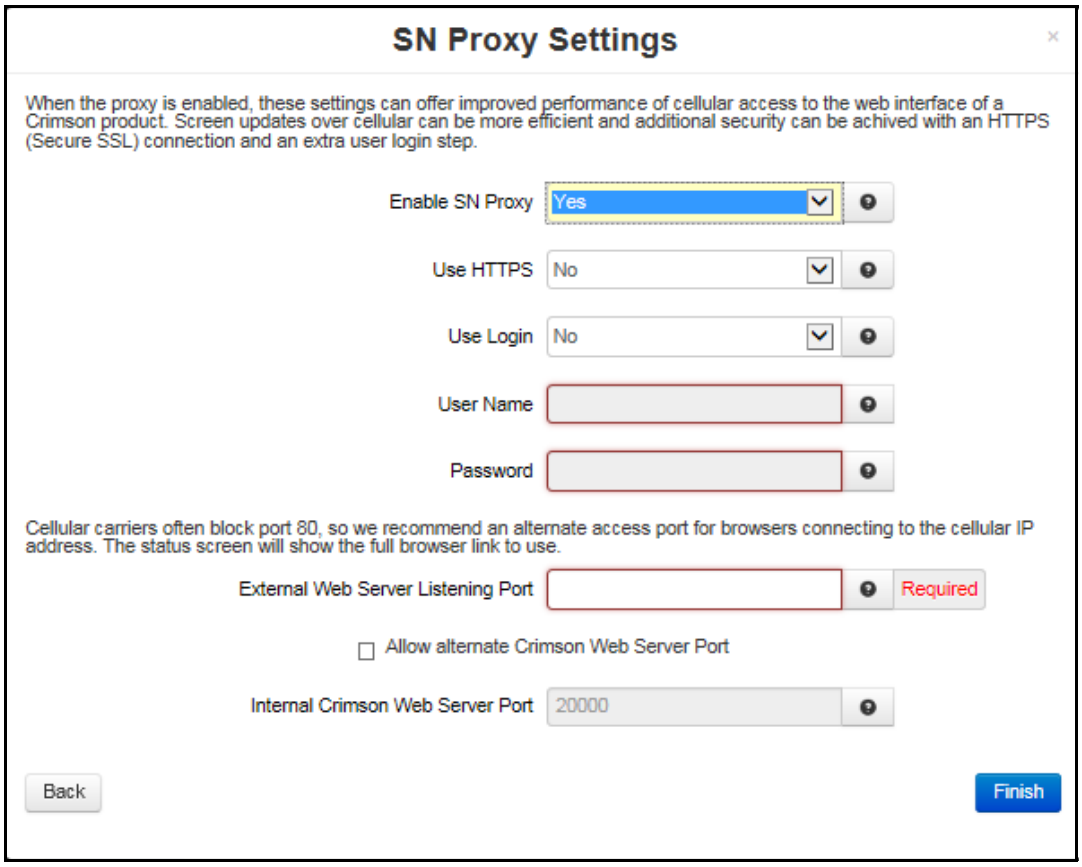
Next, enter the public email server information below, and access to SSL SMTP servers is possible. The status screen will also show the IP and Port to enter into the Crimson configuration. The username/password required for the 3rd party SMTP server will still need to be entered into the Crimson configuration.

Service Provider: Select the Domain Name of the remote SSL email server.

Destination Email Server (Required): Enter the IP or Domain Name of the remote SSL email server. Example: smtp.gmail.com

Destination Email Port (Required): Enter the Port number of the remote SSL email server. Common Secure SMTP ports are 25, 465, and 587. Example: smtp.gmail.com requires port 465

Click on the *Next* button.



These proxy settings can offer improved performance of cellular access to the web interface of a Crimson product. Screen updates over cellular can be more efficient and additional security can be achieved with an HTTPS (Secure SSL) connection and an extra user login step.

Use HTTPS: Specify whether access to the Crimson Web server will be encapsulated in HTTPS encryption.

Use Login: Use HTTP login: Specify whether you want to enable additional user login requirements. This HTTP login will occur prior to accessing the Crimson Web interface, which may require additional login steps.

> **Note:** If you enable this login, you are also required to enter the username and password. This is separate and distinct from access to this router's GUI interface.

User Name: Enter username required to connect to proxy server.

Password: Enter password required to connect through this proxy server.

Cellular carriers often block port 80, so we recommend an alternate access port for browsers connecting to the cellular IP address. The status screen will show the full browser link to use.

External Web Server Listening Port (Required): Enter the port number that will be available for external access to your Crimson device. This port will be open on all untrusted interfaces (as defined in the firewall).

External browsers that connect to this port and complete authentication will then be allowed to connect to the Crimson device on the local network.

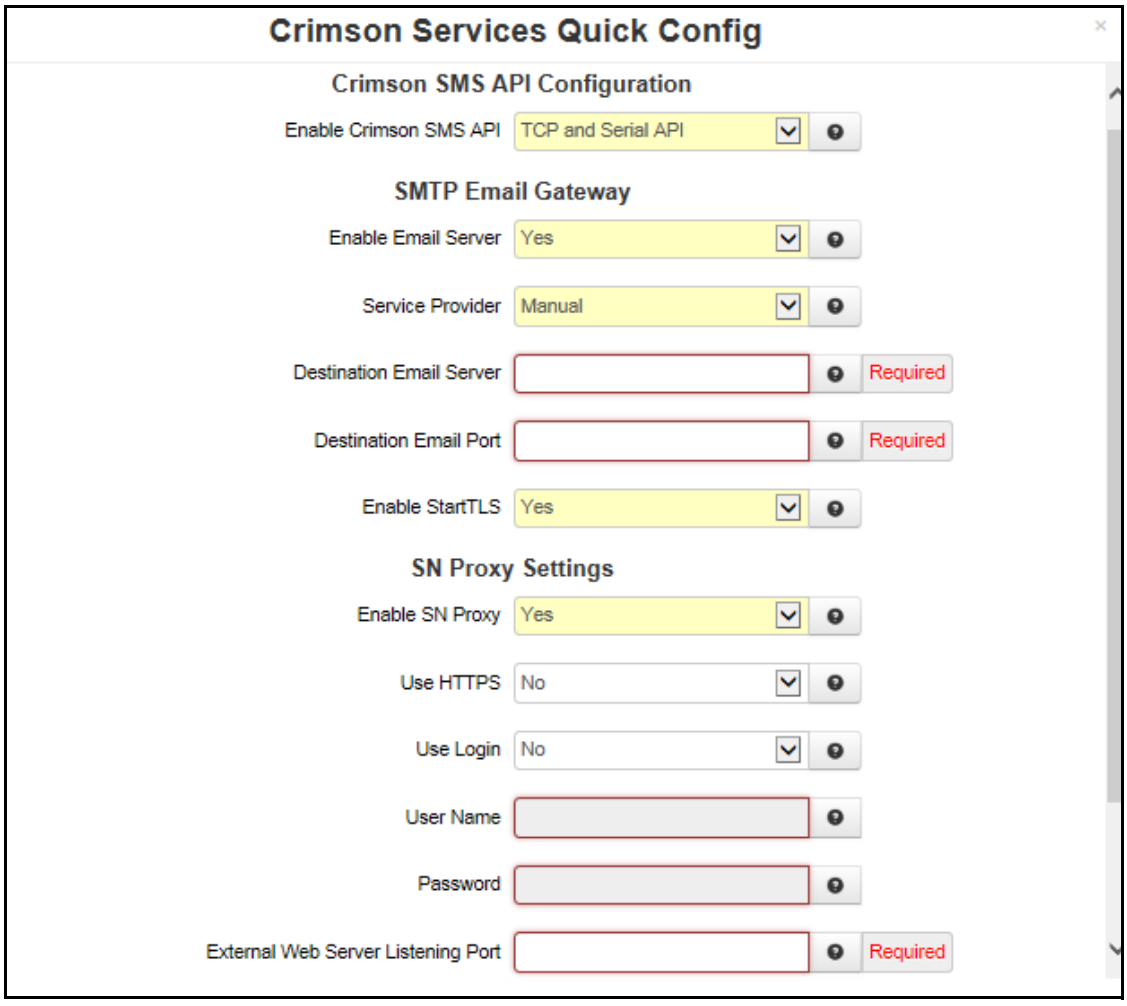
Some cellular carriers block certain incoming ports (like 80). You may need to experiment with different values here. The recommended setting for this field is 8080.

Allow alternate Crimson Web Server Port:

Internal Crimson Web Server Port: The common listening web server port on Crimson devices is port 80. If you are using a non-standard port on your Crimson device, enter it here.

Click on the *Finish* button.

Quick Config: This option has the same fields as the Walkthrough setup, but can be configured in one dialog window.



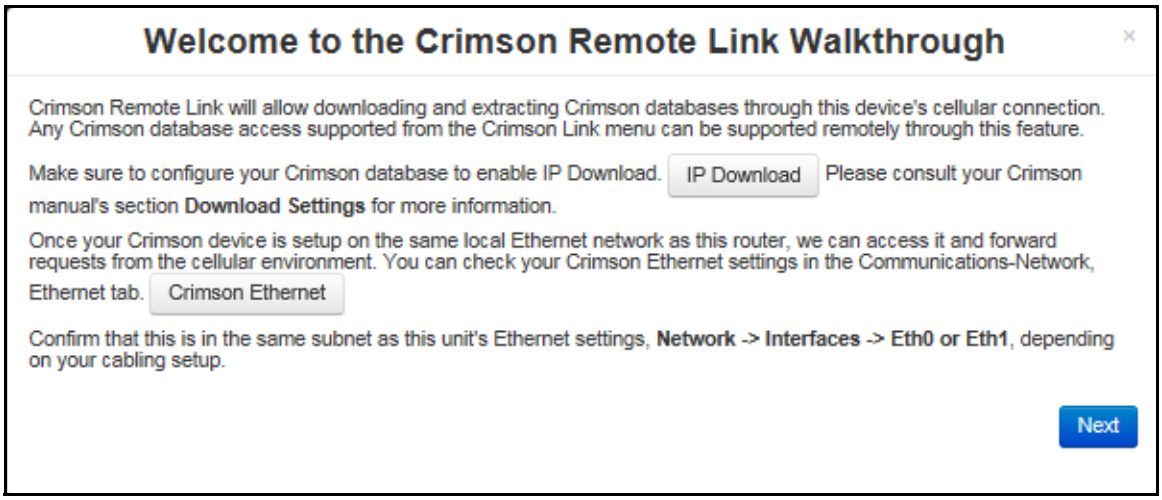
Services Status

The status of the Crimson Services will show in this section of the Crimson Connect section.

Remote Link Setup

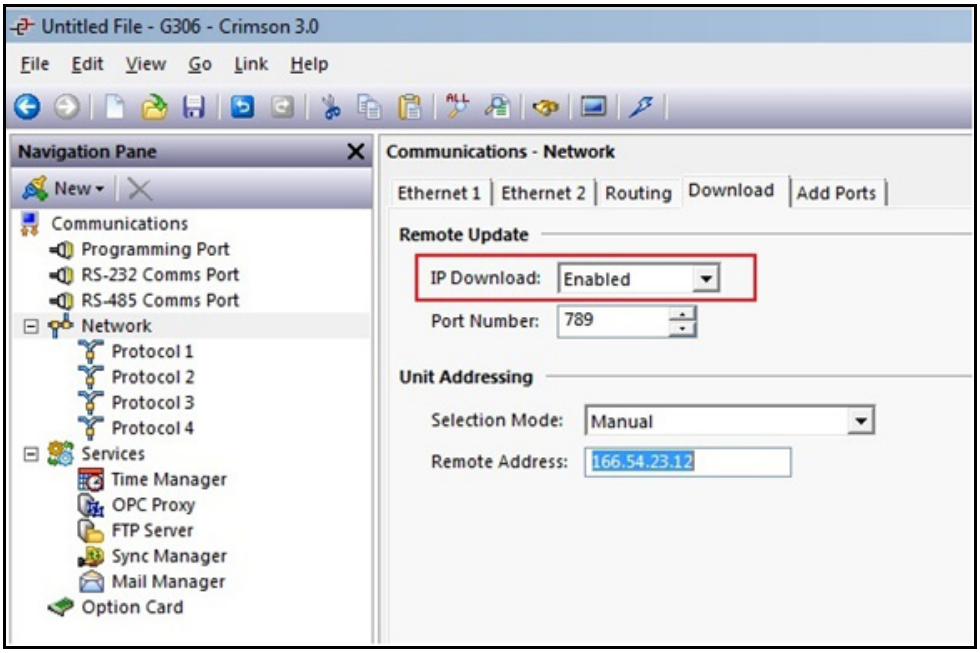
Walkthrough: This option provides step-by-step instructions for Crimson Services setup.

Click on the Walkthrough button to begin the Crimson Remote Link setup. The Crimson Remote Link Walkthrough window will pop-up.

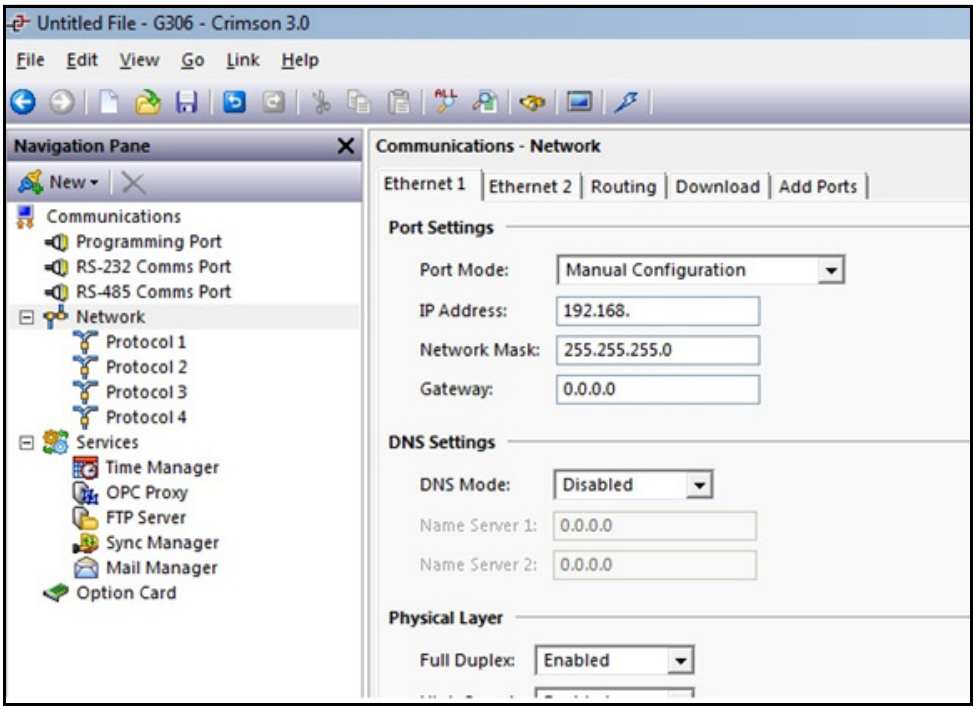


Crimson Remote Link allows downloading and extracting Crimson databases through this device's cellular connection. Any Crimson database access supported from the Crimson Link menu can be supported remotely through this feature. **Please consult your Crimson manual's section "Download Settings" for more information.**

Make sure to configure your Crimson database to enable IP Download.

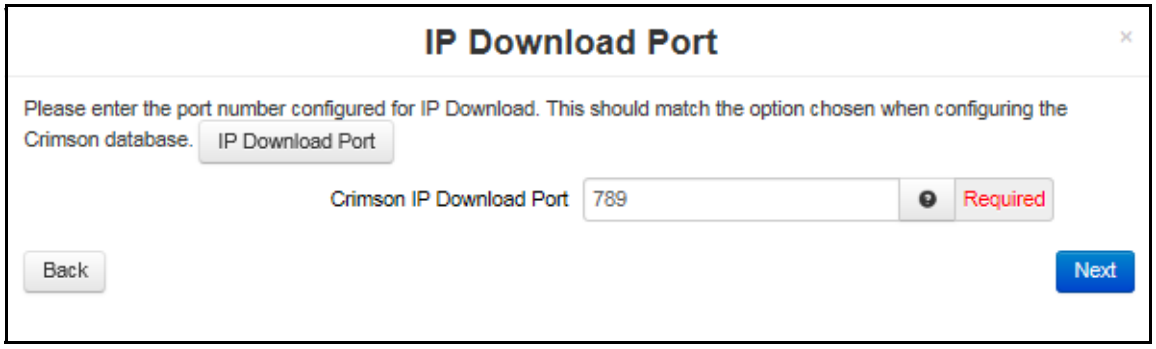


Once your Crimson device is setup on the same local Ethernet network as this router, we can access it and forward requests from the cellular environment. You can check your Crimson Ethernet settings in the Communications-Network, Ethernet tab.

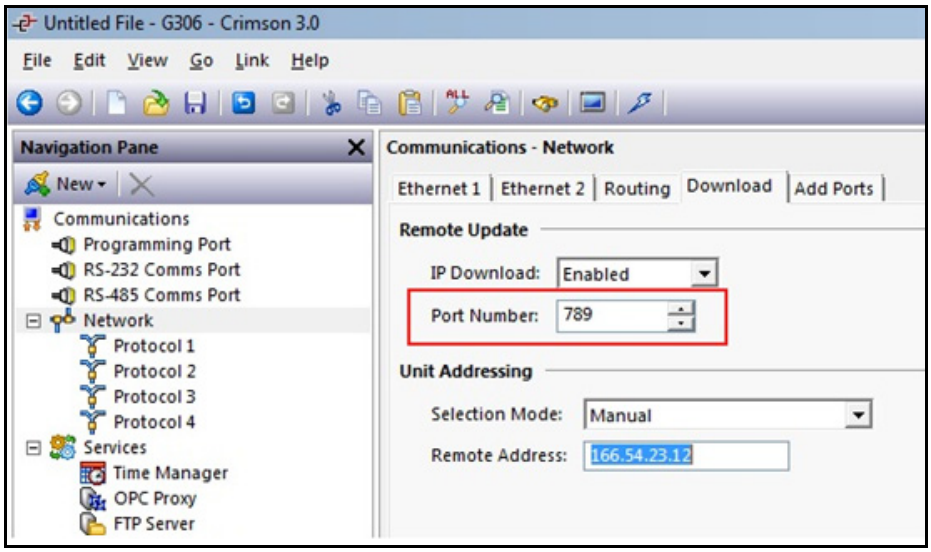


Confirm that this is in the same subnet as this unit's Ethernet settings, Network → Interfaces → Eth0 or Eth1, depending on your cabling setup.

Click on the *Next* button.



Crimson IP Download Port (Required): The port number is found in the **Communications→Network** settings in Crimson.



Click on the *Next* button.

Time to allow access to Crimson Link (in minutes): Enter time to allow access to Crimson Link (in minutes). Once the Crimson Remote Link is Started, it will only allow the initial connection within the number of minutes specified here. New attempts after this timeout will be rejected, but current connections will not be prematurely terminated.

Note: Minimum time to allow access to Crimson Link is 5 minutes and the maximum is 240 minutes (4 hours).

Security Filtering: Connections from the IP (or IP range) listed here will be allowed to connect to the Crimson Link enabled device.

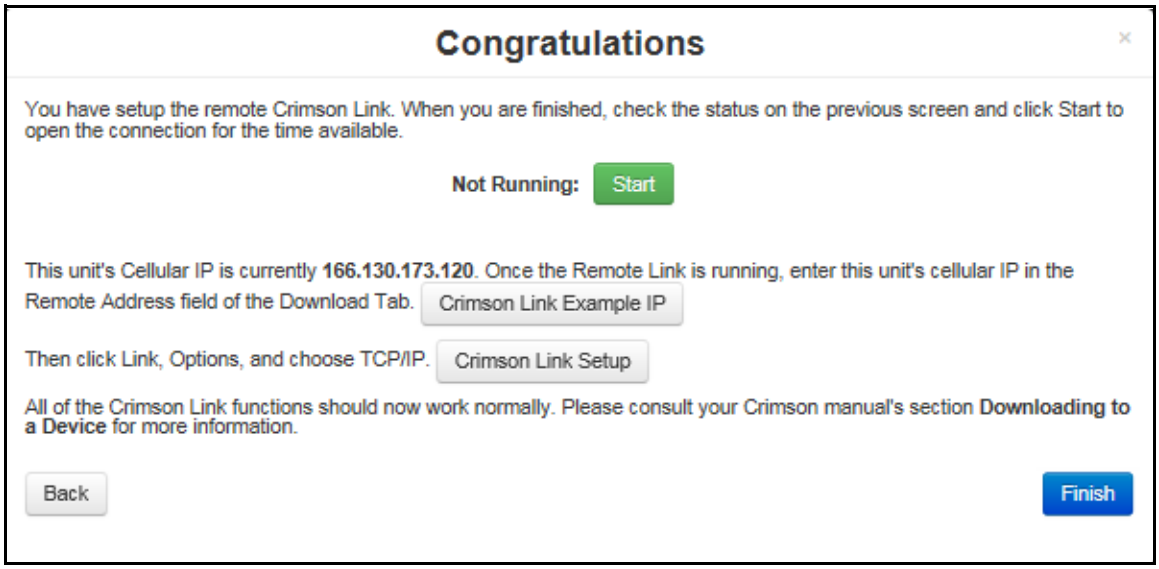
None - Allow World: This allows connections from any remote IP Address. Choose this if you are unsure what IP to enter, or if multiple people may access this link.

Allow Currently Connected IP Only: This will auto detect the IP in use from this current browser session. If you are running Crimson on the same PC that is accessing this page in a browser, try this option first.

Allow Specific IP: Enter a specific IP in the Filter From field. Only this IP will be allowed to connect to the Crimson Link. If your endpoints are connecting through a firewall, a computer's assigned IP might not be the same IP used when connecting to this remote unit.

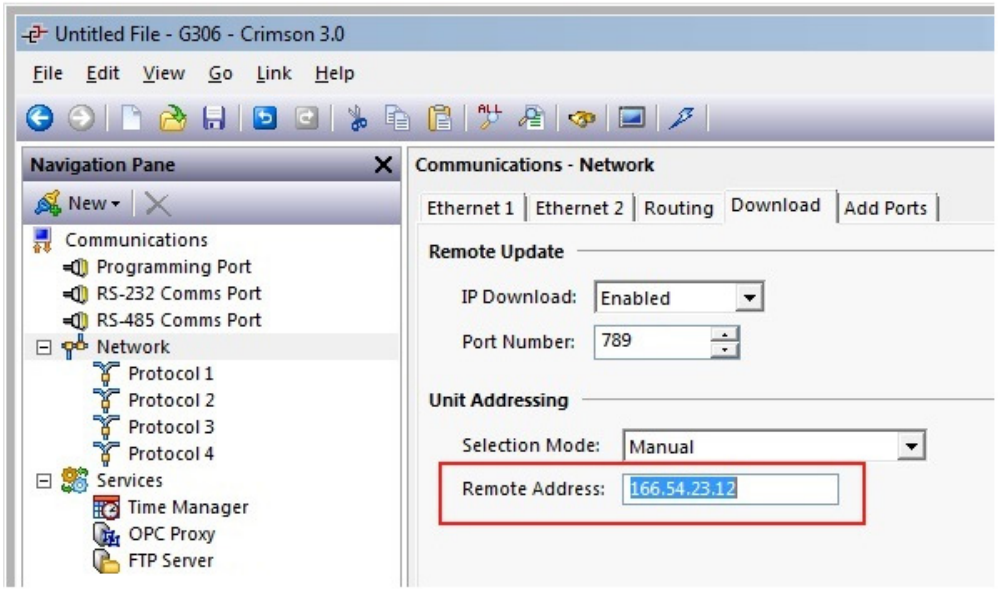
Filter From: Enter specific IP address here. This field is enabled when Allow Specific option is selected

Click on the Next button.

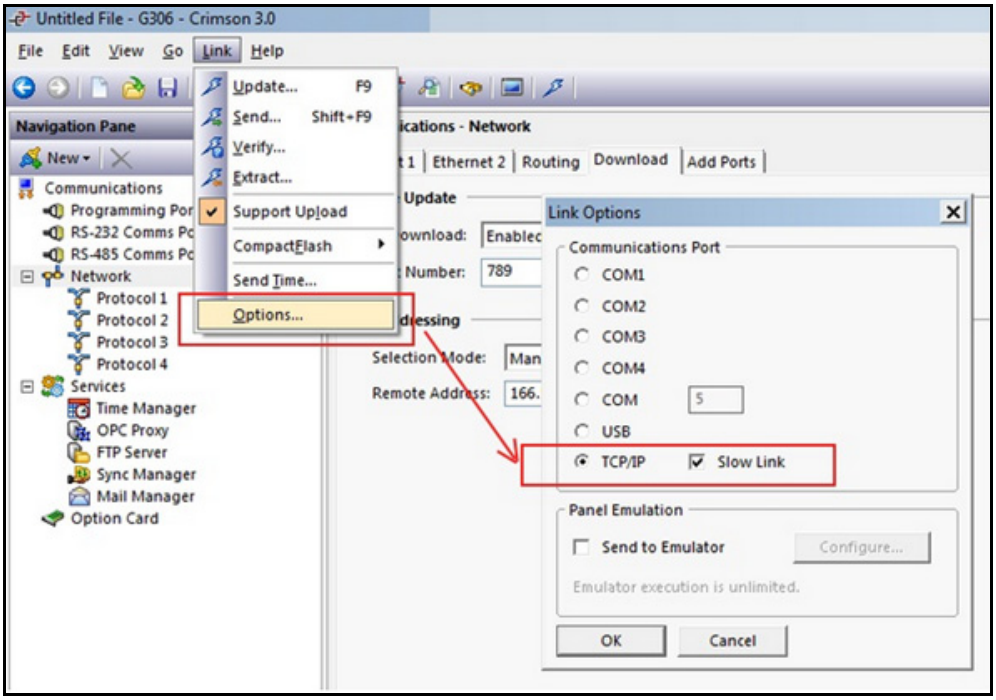


Now that the remote Crimson Link has been setup, click the status on the Crimson Connect main dialog window and click *START* to open the connection for the time available.

Once the Remote Link is running, enter this unit's cellular IP in the Remote Address field of the Download Tab. **Please consult the Crimson manual for more detailed information.**



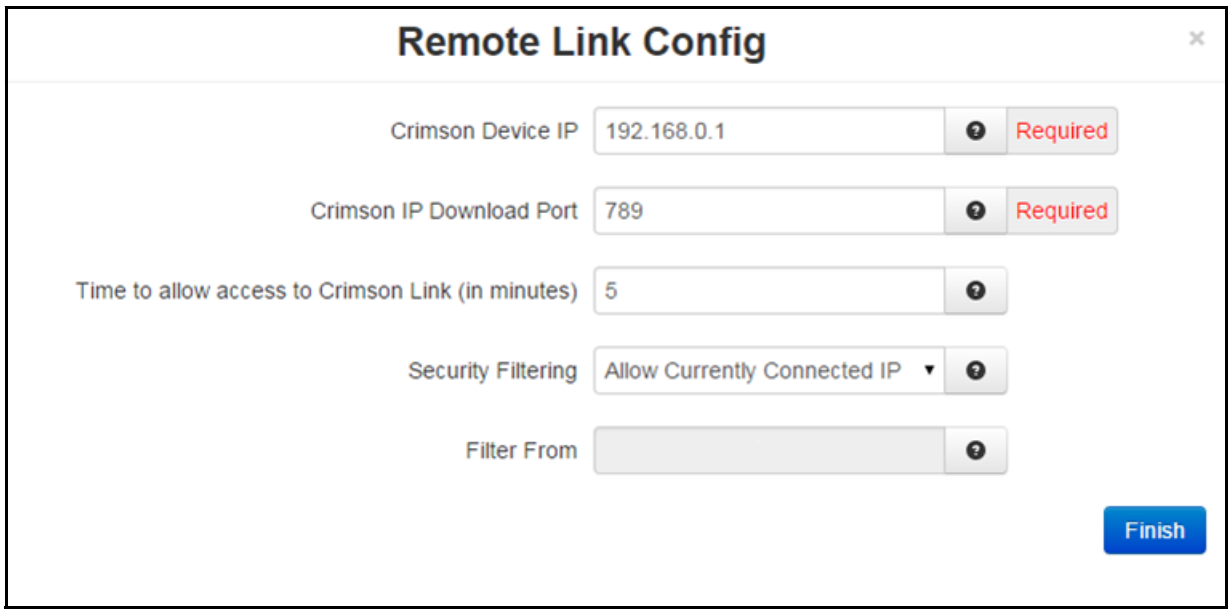
Then click *Link*, *Options*, and choose *TCP/IP*.



All of the Crimson Link functions should now work normally. Please consult your Crimson manual's section "**Downloading to a Device**" for more information.

Click on the *Finish* button.

Quick Config: This option has the same fields as the Walkthrough setup, but can be configured in one dialog window



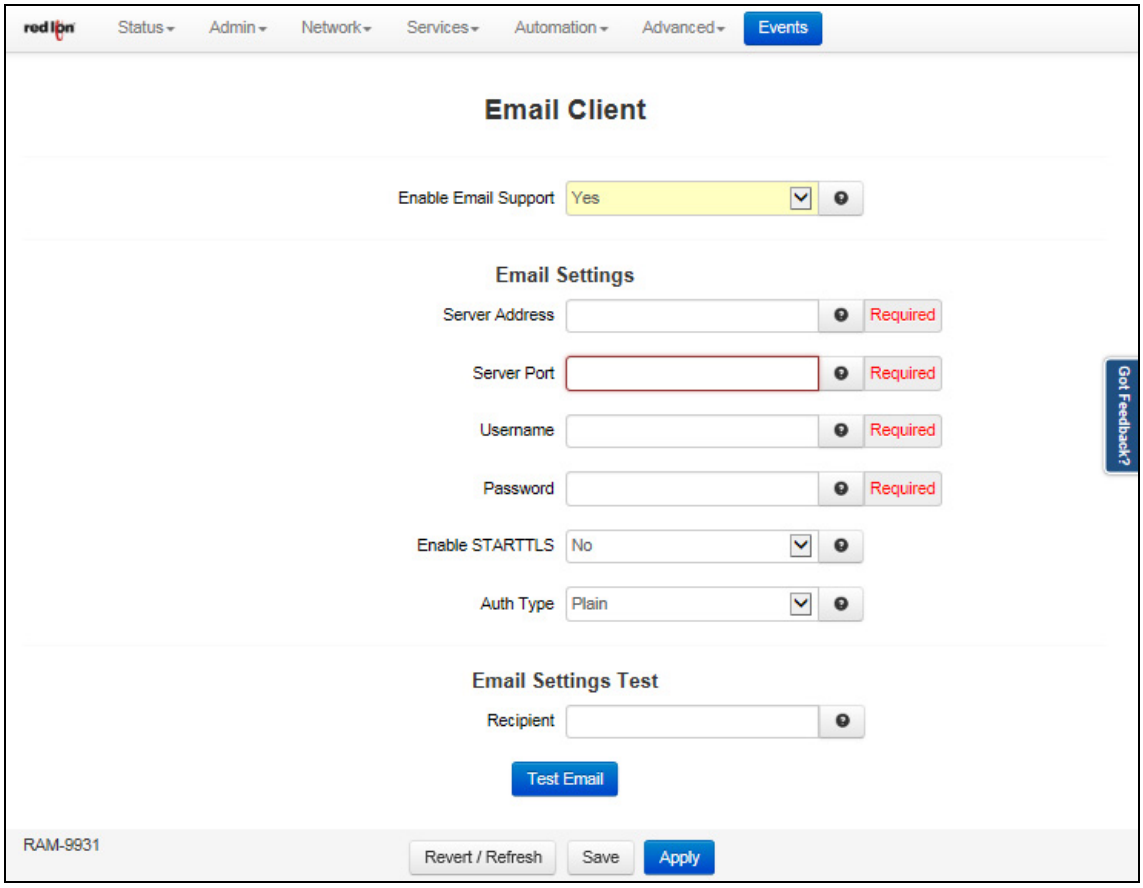
Remote Link Status

Once the remote link is running, enter the unit's cellular IP in the Remote Address field of the download tab.

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately.

3.5.12 Email Client

Specify whether to enable the SMTP email client support on this device. If this option is disabled, your email action routines will be unable to send.



Enable Email Support: Specify whether to enable the SMTP email client support on this device. If this option is disabled, your email action routines will be unable to send. Consult your email service provider or system administrator for your server settings.

Server Address (Required): Enter your SMTP server address. Gmail accounts require allowing less secure apps to access your account. You can sign-in to your account and follow the instruction below.

Access your account:

- Go to Allow less secure apps and choose Allow to let less secure apps access your Google account.
- Common SMTP Server Settings

Server Port (Required): Enter your SMTP server port.

Username (Required): Enter the username used to connect to your SMTP server account.

Password (Required): Enter the password used to connect to your SMTP server account.

Enable STARTTLS: Specify whether to enable the STARTTLS option for your email server.

Note: STARTTLS is an extension to plain text communication protocols, which offers a way to upgrade a plain text connection to an encrypted (TLS or SSL) connection instead of using a separate port for encrypted communication.

Auth Type: Select the authorization type for email client that may log in using an authentication mechanism chosen among those supported by the email server.

Any: Any authorization method supported.

Plain: Force server to use plain mode (for compatibility).

Email Settings Test: Enter an email address for the email message destination.

Recipient: Multiple email addresses can be entered by separating them with a comma.

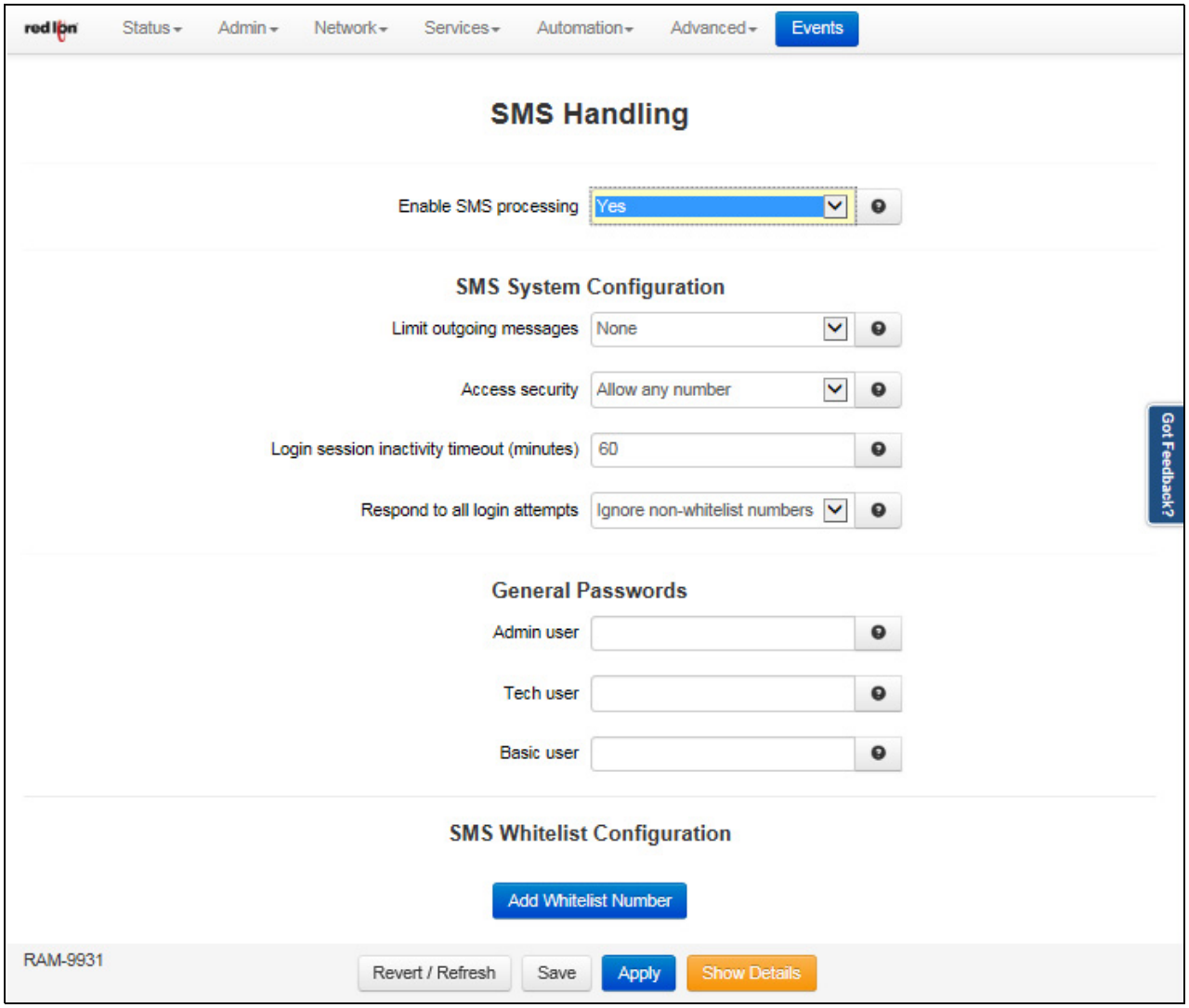
Note: The email will come from the address configured in *Sender* field or *Username* field if the Sender field is blank. Examples; username@email.com or username@email.com,usergroup@email.com

Test Email: Click on this button to execute the Email Settings Test. An email will be sent to the recipient using the Email Client server settings and an Email Debug window will display the log of the email sending process for diagnostics.

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert/Refresh*, will reset all fields to previously saved defaults.

3.5.13 SMS Handling

Specify whether to enable the SMS Command Handling Engine. If this option is disabled, all incoming SMS messages will be ignored unless SDK applications are processing them.



Enable SMS Processing: Specify whether to enable the SMS processing support on this device. If this option is disabled, your SMS action routines will be unable to send. Consult your SMS service provider or system administrator for your account settings.

SMS System Configuration

Limit outgoing messages: Select the desired Limit Period for operational permission. This is the time period for which you want to restrict the amount of messages that are sent by the device. There are three available options.

None: No time bound restrictions on sent messages.

Hourly: Messages will be restricted by the number of messages per hour.

Daily: Messages will be restricted by the number of messages sent per day.

Access security: Select the Access security profile for who will be allowed access to the device. There are three available options.

Allow any number: Any number can access features for all user types. Login is still required.

Allow any number, Admin must be on whitelist: Any number can access Basic/Tech functions, but only whitelist users can access Admin functions. Login is still required.

Allow only Whitelist numbers: Only Whitelist users can login. All users will need to login to have the functions of their access level. Non-whitelist users' requests will be ignored.

Login session inactivity timeout (minutes): Set the amount of inactivity time, in minutes, the system will keep an incoming number logged in and accepting commands before timing out and requiring a new log in. The available range is 1 - 1440 minutes.

Respond to all login attempts: This option determines when the device will respond to invalid login attempts. The available options are:

Yes: Respond to all invalid login attempts.

Ignore non-whitelist numbers: Respond only to numbers that are on the whitelist and ignore all others.

General Passwords

Note: The password may be alphanumeric with a minimum 4 and a maximum 20 alphanumeric characters. The following special characters may be used **`~!@#$%^&*()_-=+[]{}\|\\:;,<.>/?**.

Admin user: Set the password to be used by the Admin users for unlimited Read / Write access.

Tech user: Set the password to be used by Tech users for Basic level Read Only access for IODB values and Write permissions for Event alarm clearance only.

Basic user: Set the password to be used by the Basic users for Read Only access.

SMS Whitelist Configuration

To control access via a whitelist by incoming number, select the Add Whitelist Number button and complete the SMS Whitelist Settings screen to add members to the whitelist and set permission levels.

Incoming number: Enter the incoming number (phone number without parenthesis) to allow this number to access the SMS command handler. Incoming number must be numeric digits with or without - (hyphen) character(s).

Note: All - (hyphen) characters are being stripped from the phone number. The total number of digits must be at least 4, but cannot exceed 20 digits.

Reply-To number: Enter the Reply-To number (phone number without parenthesis) to allow this number to use the SMS command handler. Reply-To number must be numeric digits with or without - (hyphen) character(s). This is useful if an international number code is required by the active cellular plan to reach this recipient.

Note: All - (hyphen) characters are being stripped from the phone number. The total number of digits must be at least 4, but cannot exceed 20 digits.

Password: Enter the password required for the selected incoming number to access the SMS handler system.

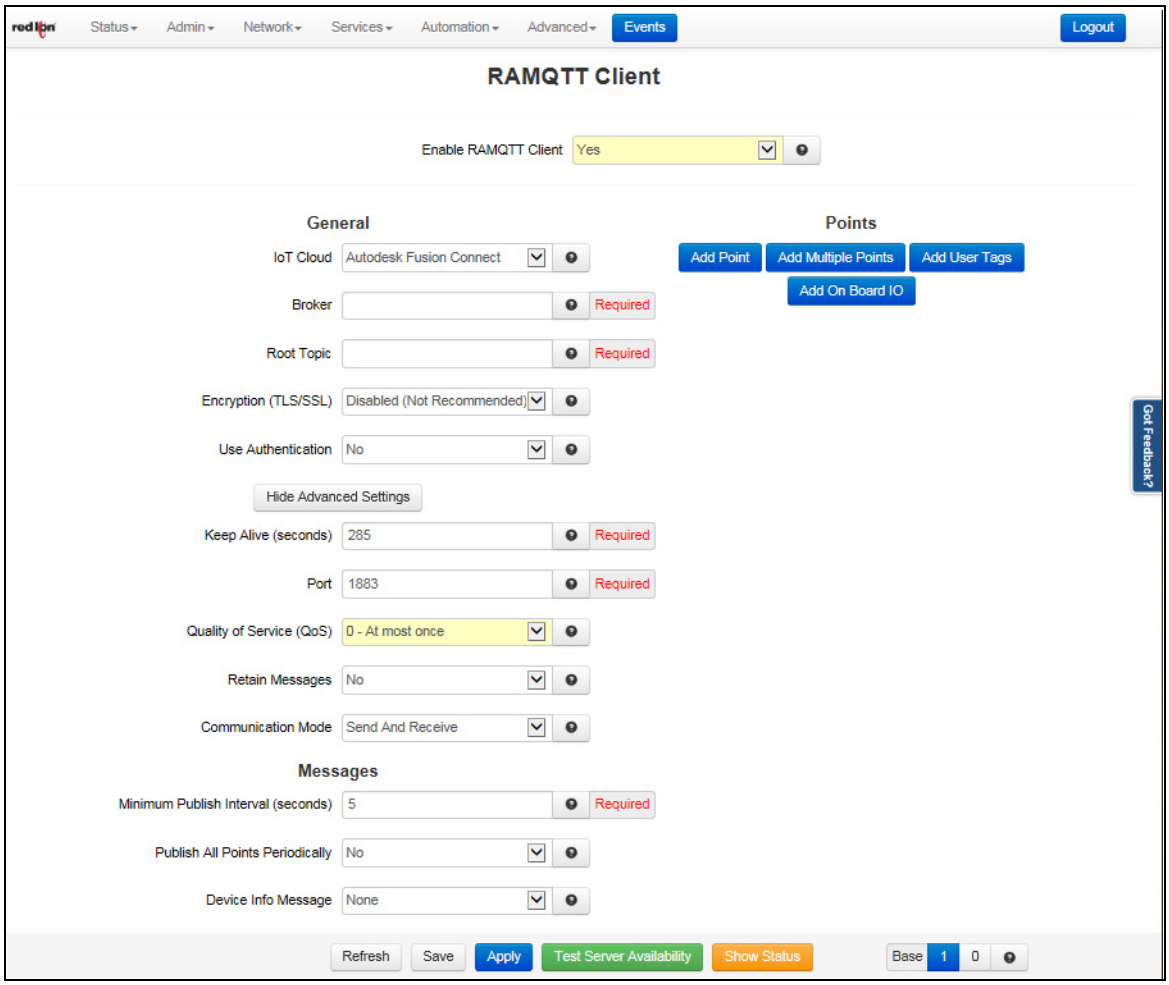
Note: The password may be alphanumeric with a minimum 4 and a maximum 20 alphanumeric characters. The following special characters may be used **`~!@#$%^&*()_-=+[]{}\|\\:;,<.>/?**.

Permission level: Select the permission level for this incoming number. The available options are Admin user, Tech user and Basic user as defined earlier in this section.

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert/Refresh*, will reset all fields to previously saved defaults. Select Show Details to view current status, send a test message or to Rotate the SMS log.

3.5.14 RAMQTT Client

Specify whether to enable the RAMQTT client support on this device.



3.5.14.1 Amazon® AWS™ IoT

General

IoT Cloud: Select the name of the Cloud Service Provider, from the drop down list, that will be receiving messages from this device.

- Amazon AWS IoT

Broker: Enter the Broker IP address or Domain Name provided by the Cloud Service Provider.

Messages

See Messages on page -171

Device Certificates

Device Cert: Device Certificate is required for connecting to AWS. This can be user generated or generated by AWS.

Device Cert Key: Device Certificate Key is required for connecting to AWS. This can be user generated or generated by AWS.

Device Root CA: Root Certificate Authority is required for connecting to AWS. This must be the Root Certificate Authority provided by AWS.

Note: You can also click on the file icon to browse to the certificate for use.

Advanced Settings

Port: Enter the port number associated with the Broker IP address or Domain Name.

The standard ports for MQTT are:

- Unencrypted: 1883
- Encrypted: 8883

Keep Alive (seconds): The Keep Alive value is the maximum time in seconds an idle connection will be allowed. If no data needs to be transmitted for this period, then an empty Keep Alive packet will be transmitted to maintain the connection as active with the server. If the Keep Alive is set to 0, it will be disabled. The acceptable value range is from 1 to 65535.

Caution: Low values may generate large amounts of unnecessary data.

- Recommended Setting: The optimal setting is unique to Cloud Service Provider.
  Generic: 2 Hours (7200 seconds)
  Fusion Connect: Less than 5 Minutes (285 seconds)

Track Server Responses: If this option is enabled, RAMQTT will receive a response message from the Broker explaining the status of the message for each message sent. This allows RAMQTT to get more detailed information on errors that the Broker might report.

Note: Since each message sent to the Broker will trigger a received message from the Broker, this will create additional overhead and increase overall data usage.

Communication Mode: Determines if RAMQTT will receive data in addition to sending data.

Send an Receive: RAMQTT will both publish data and subscribe to topics to receive data. The subscription topics enable RAMQTT to receive special commands, such as installing packages and updating configurations. Choose this option if RAMQTT should support Broker to Device communication and commands in addition to publishing data.

Send Only: RAMQTT will not subscribe to any topics and therefore will not receive any messages from the Broker. This prevents any unwanted communication to the device if RAMQTT should only publish data. However, RAMQTT will no longer be able to support commands without the ability to receive messages. Choose this option if RAMQTT should only publish data.

3.5.14.2 AT&T® M2X

General

IoT Cloud: Select the name of the Cloud Service Provider, from the drop down list, that will be receiving messages from this device.

- AT&T M2X

Broker: Enter the Broker IP address or Domain Name provided by the Cloud Service Provider.

Encryption (TLS/SSL): Select whether the connection will be encrypted.

Registration: Select whether Auto Registration will be used or if the device is Already Registered.

If Auto Registration is selected enter:

- **Master API Key:** The Master API Key is used to automatically register a device to the cloud. After device registration is complete, the Device API Key and Device ID will be added to the RAMQTT configuration and the Master API Key will be removed.
- **Distribution ID:** The Distribution ID is used to tell the cloud that this device is to be auto registered as part of a Distribution. The Distribution is defined by the user through the cloud side interface.

  Note: If the Distribution ID is provided then the Master API Key must be provided as well.

If Already Registered is selected enter:

- **Device API Key:** The Device API Key is used to allow the device to publish to topics on the cloud.

  Note: This will be auto generated if the device auto-registers using the Master API Key.

- **Device ID:** The Device ID is used to identify which device on the cloud will receive messages from this device.

  Note: This will be auto generated if the device auto-registers using the Master API Key.

Messages

See Messages on page -171

Advanced Settings

Port: Enter the port number associated with the Broker IP address or Domain Name.

The standard ports for MQTT are:

- Unencrypted: 1883
- Encrypted: 8883

Keep Alive (seconds): The Keep Alive value is the maximum time in seconds an idle connection will be allowed. If no data needs to be transmitted for this period, then an empty Keep Alive packet will be transmitted to maintain the connection as active with the server. If the Keep Alive is set to 0, it will be disabled. The acceptable value range is from 1 to 65535.

Caution: Low values may generate large amounts of unnecessary data.

- Recommended Setting: The optimal setting is unique to Cloud Service Provider.
  Generic: 2 Hours (7200 seconds)
  Fusion Connect: Less than 5 Minutes (285 seconds)

Retain Messages: The Retain Messages option determines whether the latest message sent will be saved by the Broker.

Yes: This sets the retain flag so that the latest message sent by RAMQTT will be saved by the Broker. Any new subscribers will receive this message upon subscribing. This enables newly connected subscribers to receive the latest data immediately without having to wait for RAMQTT to publish the next message. This is particularly useful if RAMQTT has a very long publish interval and subscribers need to know the latest data as soon as possible.

No: The latest message sent by RAMQTT will not be saved by the Broker.

Track Server Responses: If this option is enabled, RAMQTT will receive a response message from the Broker explaining the status of the message for each message sent. This allows RAMQTT to get more detailed information on errors that the Broker might report.

Note: Since each message sent to the Broker will trigger a received message from the Broker, this will create additional overhead and increase overall data usage.

Recording Method: Determines how changes in data are recorded and published.

Latest Changes Only: RAMQTT will only record the latest changes and publish them at the publish interval.

All Changes: RAMQTT will record changes in data in between publish intervals and store them until RAMQTT is ready o publish changes. This allows messages to contain a history of changes instead of only the latest values. This option gives greater detail to moving data trends by recording more data points, but will create larger messages for data that changes rapidly, resulting in increased data usage.

3.5.14.3 Autodesk® Fusion Connect

General

IoT Cloud: Select the name of the Cloud Service Provider, from the drop down list, that will be receiving messages from this device.

- Autodesk Fusion Connect

Root Topic: The text in this field will act as the root topic for MQTT messages being sent to the Broker.

For example, if the root topic is “redlion”, then all topics published by this device will be like the following:

- Go"<root topic>/<device serialnumber>/<sub topic>""redlion/9721X12345678912/pressure"

Broker: Enter the Broker IP address or Domain Name provided by the Cloud Service Provider.

Encryption (TLS/SSL): Select whether the connection will be encrypted.

Use Authentication: Select whether authentication will be used.

Messages

See Messages on page -171

Advanced Settings

Port: Enter the port number associated with the Broker IP address or Domain Name.

The standard ports for MQTT are:

- Unencrypted: 1883
- Encrypted: 8883

Keep Alive (seconds): The Keep Alive value is the maximum time in seconds an idle connection will be allowed. If no data needs to be transmitted for this period, then an empty Keep Alive packet will be transmitted to maintain the connection as active with the server. If the Keep Alive is set to 0, it will be disabled. The acceptable value range is from 1 to 65535.

Caution: Low values may generate large amounts of unnecessary data.

- Recommended Setting: The optimal setting is unique to Cloud Service Provider.
  Generic: 2 Hours (7200 seconds)
  Fusion Connect: Less than 5 Minutes (285 seconds)

Retain Messages: The Retain Messages option determines whether the latest message sent will be saved by the Broker.

Yes: This sets the retain flag so that the latest message sent by RAMQTT will be saved by the Broker. Any new subscribers will receive this message upon subscribing. This enables newly connected subscribers to receive the latest data immediately without having to wait for RAMQTT to publish the next message. This is particularly useful if RAMQTT has a very long publish interval and subscribers need to know the latest data as soon as possible.

No: The latest message sent by RAMQTT will not be saved by the Broker.

Communication Mode: Determines if RAMQTT will receive data in addition to sending data.

Send an Receive: RAMQTT will both publish data and subscribe to topics to receive data. The subscription topics enable RAMQTT to receive special commands, such as installing packages and updating configurations. Choose this option if RAMQTT should support Broker to Device communication and commands in addition to publishing data.

Send Only: RAMQTT will not subscribe to any topics and therefore will not receive any messages from the Broker. This prevents any unwanted communication to the device if RAMQTT should only publish data. However, RAMQTT will no longer be able to support commands without the ability to receive messages. Choose this option if RAMQTT should only publish data.

3.5.14.4 Cumulocity

General

IoT Cloud: Select the name of the Cloud Service Provider, from the drop down list, that will be receiving messages from this device.

- Cumulocity

Broker: Enter the Broker IP address or Domain Name provided by the Cloud Service Provider.

User Name: Enter the user name required to connect to the MQTT Broker.

Password: Enter the password required to connect to the MQTT Broker.

Messages

See Messages on page -171

Device Certificates

Device Root CA: Root Certificate Authority is required for connecting to AWS. This must be the Root Certificate Authority provided by AWS.

Note: You can also click on the file icon to browse to the certificate for use.

Advanced Settings

Port: Enter the port number associated with the Broker IP address or Domain Name.

The standard ports for MQTT are:

- Unencrypted: 1883
- Encrypted: 8883

Keep Alive (seconds): The Keep Alive value is the maximum time in seconds an idle connection will be allowed. If no data needs to be transmitted for this period, then an empty Keep Alive packet will be transmitted to maintain the connection as active with the server. If the Keep Alive is set to 0, it will be disabled. The acceptable value range is from 1 to 65535.

Caution: Low values may generate large amounts of unnecessary data.

- Recommended Setting: The optimal setting is unique to Cloud Service Provider.
  Generic: 2 Hours (7200 seconds)
  Fusion Connect: Less than 5 Minutes (285 seconds)

Track Alarms:

Recording Method: Determines how changes in data are recorded and published.

Latest Changes Only: RAMQTT will only record the latest changes and publish them at the publish interval.

All Changes: RAMQTT will record changes in data in between publish intervals and store them until RAMQTT is ready o publish changes. This allows messages to contain a history of changes instead of only the latest values. This option gives greater detail to moving data trends by recording more data points, but will create larger messages for data that changes rapidly, resulting in increased data usage.

3.5.14.5 Ignition

General

IoT Cloud: Select the name of the Cloud Service Provider, from the drop down list, that will be receiving messages from this device.

- Ignition

Broker: Enter the MQTT Broker IP address or Domain Name provided by the Cloud Service Provider.

Add Redundancy Broker: Enter the IP address or Domain Name of an additional MQTT Broker provided by the Cloud Service Provider. Use the *Remove* button to delete a Redundancy Broker.

Primary Host ID: Enter the MSQTT Broker IP address or Domain Name provided by the Cloud Service Provider.

Encryption (TLS/SSL): Select whether the connection will be encrypted.

User Name: Enter the user name required to connect to the MQTT Broker.

Password: Enter the password required to connect to the MQTT Broker.

Group Name: Enter the name of the group this device will be registered to.

Messages

See Messages on page -171

Device Certificates

Device Root CA: Root Certificate Authority is required for connecting to AWS. This must be the Root Certificate Authority provided by AWS.

Note: You can also click on the file icon to browse to the certificate for use.

Advanced Settings

Port: Enter the port number associated with the Broker IP address or Domain Name.

The standard ports for MQTT are:

- Unencrypted: 1883
- Encrypted: 8883

Keep Alive (seconds): The Keep Alive value is the maximum time in seconds an idle connection will be allowed. If no data needs to be transmitted for this period, then an empty Keep Alive packet will be transmitted to maintain the connection as active with the server. If the Keep Alive is set to 0, it will be disabled. The acceptable value range is from 1 to 65535.

Caution: Low values may generate large amounts of unnecessary data.

- Recommended Setting: The optimal setting is unique to Cloud Service Provider.
  Generic: 2 Hours (7200 seconds)
  Fusion Connect: Less than 5 Minutes (285 seconds)

Communication Mode: Determines if RAMQTT will receive data in addition to sending data.

Send an Receive: RAMQTT will both publish data and subscribe to topics to receive data. The subscription topics enable RAMQTT to receive special commands, such as installing packages and updating configurations. Choose this option if RAMQTT should support Broker to Device communication and commands in addition to publishing data.

Send Only: RAMQTT will not subscribe to any topics and therefore will not receive any messages from the Broker. This prevents any unwanted communication to the device if RAMQTT should only publish data. However, RAMQTT will no longer be able to support commands without the ability to receive messages. Choose this option if RAMQTT should only publish data.

Recording Method: Determines how changes in data are recorded and published.

Latest Changes Only: RAMQTT will only record the latest changes and publish them at the publish interval.

All Changes: RAMQTT will record changes in data in between publish intervals and store them until RAMQTT is ready o publish changes. This allows messages to contain a history of changes instead of only the latest values. This option gives greater detail to moving data trends by recording more data points, but will create larger messages for data that changes rapidly, resulting in increased data usage.

3.5.14.6 Microsoft® Azure® IoT Hub

General

IoT Cloud: Select the name of the Cloud Service Provider, from the drop down list, that will be receiving messages from this device.

- Microsoft Azure IoT Hub

Authentication Type: The Authentication Type determines how RAMQTT will authenticate with the Azure IoT Hub.

SAS Token: RAMQTT will use an already existing/generated SAS Token to authenticate with the Azure IoT Hub.

Self Signed Certificates: RAMQTT will use the selected Device Certificate file, Device Certificate Key file, and a Root Certificate Authority file to authenticate the Broker.

Device Connection String: RAMQTT will use a Device Connection String to generate a SAS Token to authenticate with the Azure IoT Hub. Each time the SAS Token expires, RAMQTT will use the Device Connection String to generate a new SAS Token.

The Device Connection String is the Connection String for the Azure IoT Device. It is used to generated SAS Tokens which allow RAMQTT to authenticate with the Azure IoT Hub. RAMQTT will generate an initial SAS Token using the Device Connection String and will continue to generate new SAS Tokens as old ones expire.

If new Device Connection Strings are generated for the Azure IoT Device, RAMQTT will not be able to generate a valid SAS Token using the old Device Connection String.

Messages

See Messages on page -171

Device Certificates

Device Cert: Device Certificate is required for connecting to some cloud service providers. This can be user generated or uploaded from another source. If applicable a certificate fingerprint/thumbprint will be generated on executing a Save/Apply and will appear below.

Device Cert Key: Device Certificate Key is required for connecting to AWS. This can be user generated or generated by AWS.

Device Root CA: Root Certificate Authority is required for connecting to AWS. This must be the Root Certificate Authority provided by AWS.

Note: You can also click on the file icon to browse to the certificate for use.

Advanced Settings

Port: Enter the port number associated with the Broker IP address or Domain Name.

The standard ports for MQTT are:

- Unencrypted: 1883
- Encrypted: 8883

Keep Alive (seconds): The Keep Alive value is the maximum time in seconds an idle connection will be allowed. If no data needs to be transmitted for this period, then an empty Keep Alive packet will be transmitted to maintain the connection as active with the server. If the Keep Alive is set to 0, it will be disabled. The acceptable value range is from 1 to 65535.

Caution: Low values may generate large amounts of unnecessary data.

- Recommended Setting: The optimal setting is unique to Cloud Service Provider.
  Generic: 2 Hours (7200 seconds)
  Fusion Connect: Less than 5 Minutes (285 seconds)

Communication Mode: Determines if RAMQTT will receive data in addition to sending data.

Send an Receive: RAMQTT will both publish data and subscribe to topics to receive data. The subscription topics enable RAMQTT to receive special commands, such as installing packages and updating configurations. Choose this option if RAMQTT should support Broker to Device communication and commands in addition to publishing data.

Send Only: RAMQTT will not subscribe to any topics and therefore will not receive any messages from the Broker. This prevents any unwanted communication to the device if RAMQTT should only publish data. However, RAMQTT will no longer be able to support commands without the ability to receive messages. Choose this option if RAMQTT should only publish data.

3.5.14.7 Nokia IMPACT

General

IoT Cloud: Select the name of the Cloud Service Provider, from the drop down list, that will be receiving messages from this device.

- Nokia Impact

Broker: Enter the Broker IP address or Domain Name provided by the Cloud Service Provider.

Encryption (TLS/SSL): Select whether the connection will be encrypted.

Credentials: This option determines whether RAMQTT will attempt to generate token credentials for this device or use existing token credentials.

Generate Token Credentials: RAMQTT will attempt to generate token credentials for this device using the account user name and password and the name of the group to register the token credentials to.

Using Existing Token Credentials: RAMQTT will use existing token credentials.

Account User Name: Enter the user name required to connect to the MQTT Broker.

Account Password: Enter the password required to connect to the MQTT Broker.

Group Name: Enter the name of the group this device will be registered to.

Messages

See Messages on page -171

Device Certificates

Device Root CA: Root Certificate Authority is required for connecting to AWS. This must be the Root Certificate Authority provided by AWS.

Note: You can also click on the file icon to browse to the certificate for use.

Advanced Settings

Port: Enter the port number associated with the Broker IP address or Domain Name.

The standard ports for MQTT are:

- Unencrypted: 1883
- Encrypted: 8883

Keep Alive (seconds): The Keep Alive value is the maximum time in seconds an idle connection will be allowed. If no data needs to be transmitted for this period, then an empty Keep Alive packet will be transmitted to maintain the connection as active with the server. If the Keep Alive is set to 0, it will be disabled. The acceptable value range is from 1 to 65535.

Caution: Low values may generate large amounts of unnecessary data.

- Recommended Setting: The optimal setting is unique to Cloud Service Provider.
  Generic: 2 Hours (7200 seconds)
  Fusion Connect: Less than 5 Minutes (285 seconds)

Communication Mode: Determines if RAMQTT will receive data in addition to sending data.

Send an Receive: RAMQTT will both publish data and subscribe to topics to receive data. The subscription topics enable RAMQTT to receive special commands, such as installing packages and updating configurations. Choose this option if RAMQTT should support Broker to Device communication and commands in addition to publishing data.

Send Only: RAMQTT will not subscribe to any topics and therefore will not receive any messages from the Broker. This prevents any unwanted communication to the device if RAMQTT should only publish data. However, RAMQTT will no longer be able to support commands without the ability to receive messages. Choose this option if RAMQTT should only publish data.

3.5.14.8 Telenor Cloud Connect

General

IoT Cloud: Select the name of the Cloud Service Provider, from the drop down list, that will be receiving messages from this device.

- Telenor Cloud Connect

Broker: Enter the Broker IP address or Domain Name provided by the Cloud Service Provider.

Device Name: Enter the device name provided by the cloud server provider.

Messages

See Messages on page -171

Device Certificates

Device Cert: Device Certificate is required for connecting to AWS. This can be user generated or generated by AWS.

Device Cert Key: Device Certificate Key is required for connecting to AWS. This can be user generated or generated by AWS.

Device Root CA: Root Certificate Authority is required for connecting to AWS. This must be the Root Certificate Authority provided by AWS.

Note: You can also click on the file icon to browse to the certificate for use.

Advanced Settings

Port: Enter the port number associated with the Broker IP address or Domain Name.

The standard ports for MQTT are:

- Unencrypted: 1883
- Encrypted: 8883

Keep Alive (seconds): The Keep Alive value is the maximum time in seconds an idle connection will be allowed. If no data needs to be transmitted for this period, then an empty Keep Alive packet will be transmitted to maintain the connection as active with the server. If the Keep Alive is set to 0, it will be disabled. The acceptable value range is from 1 to 65535.

Caution: Low values may generate large amounts of unnecessary data.

- Recommended Setting: The optimal setting is unique to Cloud Service Provider.
  Generic: 2 Hours (7200 seconds)
  Fusion Connect: Less than 5 Minutes (285 seconds)

Communication Mode: Determines if RAMQTT will receive data in addition to sending data.

Send an Receive: RAMQTT will both publish data and subscribe to topics to receive data. The subscription topics enable RAMQTT to receive special commands, such as installing packages and updating configurations. Choose this option if RAMQTT should support Broker to Device communication and commands in addition to publishing data.

Send Only: RAMQTT will not subscribe to any topics and therefore will not receive any messages from the Broker. This prevents any unwanted communication to the device if RAMQTT should only publish data. However, RAMQTT will no longer be able to support commands without the ability to receive messages. Choose this option if RAMQTT should only publish data.

3.5.14.9 User Configurable

General

IoT Cloud: Select the name of the Cloud Service Provider, from the drop down list, that will be receiving messages from this device.

- **User Configurable:** Select this Generic Mode MQTT Client to fully customize the client to connect into your own MQTT Broker instance

Broker: Enter the Broker IP address or Domain Name provided by the Cloud Service Provider.

Port: Enter the port number associated with the Broker IP address or Domain Name.

The standard ports for MQTT are:

- Unencrypted: 1883
- Encrypted: 8883

Client ID: The Client ID is the client identification for the MQTT connection. This ID allows the Broker to identify and evaluate the state of the connection. This ID must be unique and therefore it is best practice to use the serial number of the device as the Client ID.

User Name: Enter the user name required to connect to the MQTT Broker.

Password: Enter the password required to connect to the MQTT Broker.

Encryption (TLS/SSL): Determines if the data sent to the broker will be encrypted.

Enabled: If the option is set to 'Enabled' then the information sent to the broker will be encrypted, securing any sensitive data that might be contained in the messages. If unsure which option to use, choose this option.

Disabled (Not Recommended): If the option is set to 'Disabled (Not Recommended)' then the information sent to the broker will not be encrypted. This option is not recommended as it is not secure. Information will be sent in plain text which means anyone will be able to read the information. Avoid this option if the data being sent is private, or if unsure which option to choose.

Authentication Type: The Authentication Type determines how RAMQTT will authenticate with the server.

CA Signed Server Certificate: RAMQTT will automatically trust the Broker and will not authenticate the Broker's Root Certificate. This option is not recommended as it does not actually authenticate the Broker to verify it is the Broker RAMQTT should be connected to.

CA Certificate File: RAMQTT will use the selected Root Certificate Authority file to authenticate the Broker. This Root Certificate file is usually provided by the solution provider.

Self Signed Certificates: RAMQTT will use the selected Device Certificate file, Device Certificate Key file, and a Root Certificate Authority file to authenticate the Broker.

This option is only visible when Encryption is set to Enabled.

Advanced Settings

Keep Alive (seconds): The Keep Alive value is the maximum time in seconds an idle connection will be allowed. If no data needs to be transmitted for this period, then an empty Keep Alive packet will be transmitted to maintain the connection as active with the server. If the Keep Alive is set to 0, it will be disabled. The acceptable value range is from 1 to 65535.

Caution: Low values may generate large amounts of unnecessary data.

- Recommended Setting: The optimal setting is unique to Cloud Service Provider.
  Generic: 2 Hours (7200 seconds)
  Fusion Connect: Less than 5 Minutes (285 seconds)

Quality of Service (QOS): Quality of Service (QoS) levels determine how the MQTT protocol will handle communication of data between RAMQTT and the Broker. Each QoS level will take different measures to ensure the data gets to the Broker.

Note: Please note that not all Cloud Providers support QoS 2.

QoS 0 - At most once: Messages won't be acknowledged by the Broker or stored and redelivered by RAMQTT. This is the "Fire and Forget" mode and relies on the underlying TCP protocol for retransmissions.

This option is best used when RAMQTT will send data frequently.

QoS 1 - At least once: Messages will be sent at least once by RAMQTT to the Broker. RAMQTT will store the message until the Broker sends an acknowledgment back. RAMQTT will resend the message if the Broker does not respond within a certain amount of time.

This option is best used when the network connection is not always reliable.

QoS 2 - Exactly once: Messages will be sent exactly once by RAMQTT to the Broker. The message will be stored by both RAMQTT and the Broker. RAMQTT and the Broker will exchange special acknowledgments until both sides confirm the message was sent and received. This QoS is the slowest but surest way to ensure data is published by RAMQTT and recieved by the Broker.

This option is best used for when the network connection is unreliable and conserving data usage is important. It is also beneficial when large infrequent messages are published by RAMQTT.

Retain Messages: The Retain Messages option determines whether the latest message sent will be saved by the Broker.

Yes - This sets the retain flag so that the latest message sent by RAMQTT will be saved by the Broker. Any new subscribers will receive this message upon subscribing. This enables newly connected subscribers to receive the latest data immediately without having to wait for RAMQTT to publish the next message. This is particularly useful if RAMQTT has a very long publish interval and subscribers need to know the latest data as soon as possible.

No - The latest message sent by RAMQTT will not be saved by the Broker.

Communication Mode: Determines if RAMQTT will receive data in addition to sending data.

Send an Receive: RAMQTT will both publish data and subscribe to topics to receive data. The subscription topics enable RAMQTT to receive special commands, such as installing packages and updating configurations. Choose this option if RAMQTT should support Broker to Device communication and commands in addition to publishing data.

Send Only: RAMQTT will not subscribe to any topics and therefore will not receive any messages from the Broker. This prevents any unwanted communication to the device if RAMQTT should only publish data. However, RAMQTT will no longer be able to support commands without the ability to receive messages. Choose this option if RAMQTT should only publish data.

Topics

IODB Points: All Tags selected in the Points section will be publish to the IODB Points topic.

Topic Macros: Topics support macros that can reference unique information about the device to be used within the topic itself.
%c or %C - The value of Client ID field
%m or %M - MAC Address for the eth0 network interface (alphanumeric, no special characters)
%i or %I - IMEI
%s or %S - The device's serial number
%j or %J - ICCID
%p or %P - IP address for the eth0 network interface (includes the '.' characters)

Examples:
test/topic/%s
test/topic/971X12345678912
company/%i/%c
company/123456789123456/test_client

Device Info: Information about the device will be published to the Device Info topic. The amount of information is based on the Device Info Message setting.

Topic Macros: Topics support macros that can reference unique information about the device to be used within the topic itself.
%c or %C - The value of Client ID field
%m or %M - MAC Address for the eth0 network interface (alphanumeric, no special characters)
%i or %I - IMEI
%s or %S - The device's serial number
%j or %J - ICCID
%p or %P - IP address for the eth0 network interface (includes the '.' characters)

Examples:
test/topic/%s
test/topic/971X12345678912
company/%i/%c
company/123456789123456/test_client

Location: Information about the device's location will be published to the Location topic.

Topic Macros: Topics support macros that can reference unique information about the device to be used within the topic itself.
%c or %C - The value of Client ID field
%m or %M - MAC Address for the eth0 network interface (alphanumeric, no special characters)
%i or %I - IMEI
%s or %S - The device's serial number
%j or %J - ICCID
%p or %P - IP address for the eth0 network interface (includes the '.' characters)

Examples:
test/topic/%s
test/topic/971X12345678912
company/%i/%c
company/123456789123456/test_client

Last Will And Testament: The device's Last Will and Testament message will be published to the Last Will and Testament topic.

Topic Macros: Topics support macros that can reference unique information about the device to be used within the topic itself.
%c or %C - The value of Client ID field
%m or %M - MAC Address for the eth0 network interface (alphanumeric, no special characters)
%i or %I - IMEI
%s or %S - The device's serial number
%j or %J - ICCID
%p or %P - IP address for the eth0 network interface (includes the '.' characters)

Examples:
test/topic/%s
test/topic/971X12345678912
company/%i/%c
company/123456789123456/test_client

Command Response: Responses to received command messages will be published to the Command Response topic.

Command: RAMQTT will subscribe to the Command topic to receive command messages.

Topic Macros: Topics support macros that can reference unique information about the device to be used within the topic itself.
%c or %C - The value of Client ID field
%m or %M - MAC Address for the eth0 network interface (alphanumeric, no special characters)
%i or %I - IMEI
%s or %S - The device's serial number
%j or %J - ICCID
%p or %P - IP address for the eth0 network interface (includes the '.' characters)

Examples:
test/topic/%s
test/topic/971X12345678912
company/%i/%c
company/123456789123456/test_client

Messages

See Messages on page -171

Device Certificates

Device Cert: Device Certificate is required for connecting to AWS. This can be user generated or generated by AWS.

Device Cert Key: Device Certificate Key is required for connecting to AWS. This can be user generated or generated by AWS.

Device Root CA: Root Certificate Authority is required for connecting to AWS. This must be the Root Certificate Authority provided by AWS.

Note: You can also click on the file icon to browse to the certificate for use.

3.5.14.10 All IoT Cloud Service Providers

Publish All Points Periodically: When set to Yes a configurable time interval is visible (minutes).

Points: Add (single) Point, or Add Multiple Points by entering the Tag Name, selecting the Type from the drop down (when adding one point at a time) or pop up list (when adding multiple points). Points can also be removed after identifying them and clicking on the Remove button.

Refresh, Save, Apply, Test Server Availability, Show Status: Use these buttons to refresh the screen, save changes, apply the changes, test the connection or display status of the RAMQTT Client.

Base 1 0: This toggles the system-wide register display format, which can be represented in two schemes: Zero-based or One-based. Zero-Based is also called Native format, and all register ranges would begin counting at 0. One-Based addressing starts all ranges with 1, and is the system commonly used with Modbus.

Each register label consists of the Tag name, followed by the address in two parts: type and address. Type and address will change to match the Zero (Native) and One (Modbus) formatting conventions. An untagged register will show an implied tag in <angle brackets>.

Messages

Minimum Publish Interval (seconds): Minimum time in seconds between published I/O data point messages. Messages are published as soon as any value changes, but subsequent changes will be separated by this amount of time to prevent flooding. Increase this value to reduce data usage from high-frequency changes. The acceptable value range is from 1 to 65535.

Publish All Points Periodically: Determines whether RAMQTT will publish all of the Points values at a set interval.

Publish All Points Interval: How often RAMQTT will publish all point's values, regardless of changes.

If set to 0, this option will be disabled.

This option is not recommended where data usage is limited. Publishing point values that have not changed can lead to extra stale data, increasing the message size, and over all amount of data.

Device Info Message: Choose the type of Device Info message to be sent. This is in addition to the I/O data point update messages.

The standard message options are:

MESSAGE OPTION	MESSAGE DESCRIPTION	MESSAGE CONTENT
None	Sends no message	None

MESSAGE OPTION	MESSAGE DESCRIPTION	MESSAGE CONTENT
Basic	Sends a basic/small, predefined list of device information values to the cloud	• Unit name • Serial Number • Cell IP • Up Time • Version • Model
Full	Sends a full, predefined list of device information values to the cloud	• Version long (ex: 4.24.99.0) • Host Name • Unit Temp • Cell modem firmware version • PWR1 Volt • Cell Module Temp • All active interface IPs • Cell Service Type • MDN • Cell Carrier PLMN • Cell Current Channel • ECIO • RSRP • RSRQ • Cell PRL Version • Sim ID • Sim IMSI • Wireless UpTime • IMEI • Wireless Signal • RSSI • Current APN • GPS Altitude • GPS Time • GPS Number of Satellites • GPS Feet From Centerpoint • GPS Speed

Note: GPS Latitude and Longitude are included in a separate section of the Basic and Full Device Info Messages. While the Latitude and Longitude values are included in the same message, they might not be displayed on the cloud side visualization in the same area as the other device info values.

Device Info Publish Interval (minutes): How often in minutes to publish the device info message. This information is not likely to change often in most installations. A high value is recommended.

Default is 480 Minutes (8 hours). Valid range is between 5 and 65535.

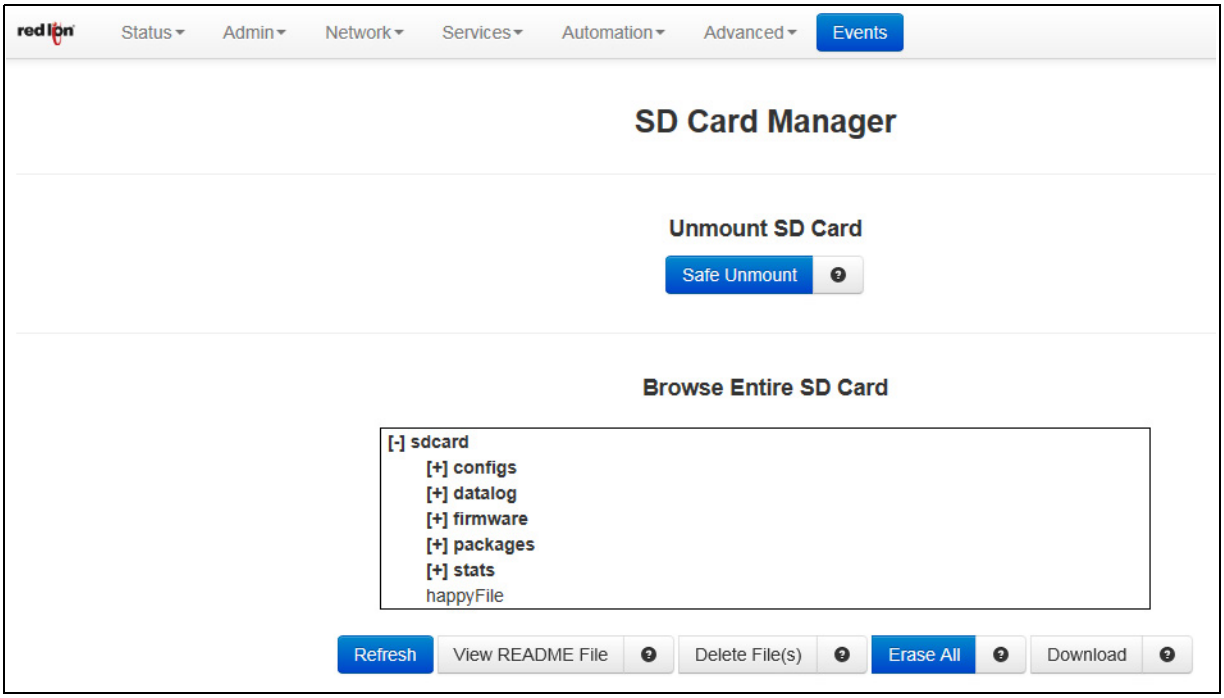
3.5.15 SD Card Manager

The SD Card Manager menu item is used to safely unmount the SD Card. Options are also available to view, download, or delete files on the SD Card while it is mounted into the device.

This feature is only available on the RAM-9000 series (RAM 6000 does not have an SD Card).

Te RAM-9000 supports SD cards in the following file formats: FAT32, VFAT, ext3, ext4, and NTFS.

Select the SD Card Manager menu item and the following dialog window appears:



Unmount SD Card / Safe Unmount: Clicking this button will safely unmount the SD card. It is required to eject the SD card and reinsert it or reboot the unit before attempting to access the SD card again.

Browse Entire SD Card: Select any directory on the SD Card to view the files contained. Selected files appear in the Selected Files box.

View README File: Select the file you would like to view in the file menu above and then click View README File.

Delete File(s): Remove the selected file(s) from the SD card. You can select multiple files to be deleted from SD card at once.

Erase All: There are two functions for this button depending on the current contents of the SD Card.This button is visible when there are files and directories on the SD card. Clicking this button will remove **ALL files and directories** from the SD card, then create the standard directory structure described below and add a README file describing the purpose of each.

Apply Directory Structure: This button is visible when the SD card is inserted and there are no files found on the SD card. Click this button to create the required directories on the SD Card for use by the system. This MUST be done before the SD Card will be available for use by the system.

configs - This directory is where the user will find any export of system configuration, gather configs as well as where the user should store a config.xml that is intended to be imported from the SD Card.

datalog - This is where the datalog files will be stored if SD Card is selected as the "Save Destination".

firmware - This is where the user would put any firmware update files they intend to reflash form the SD Card.

packages - This is where the user should store any package installation files that will be installed from the SD Card.

stats - This is where any exported gatherstats files will be copied when Save Stats to SD Card is set to Yes.

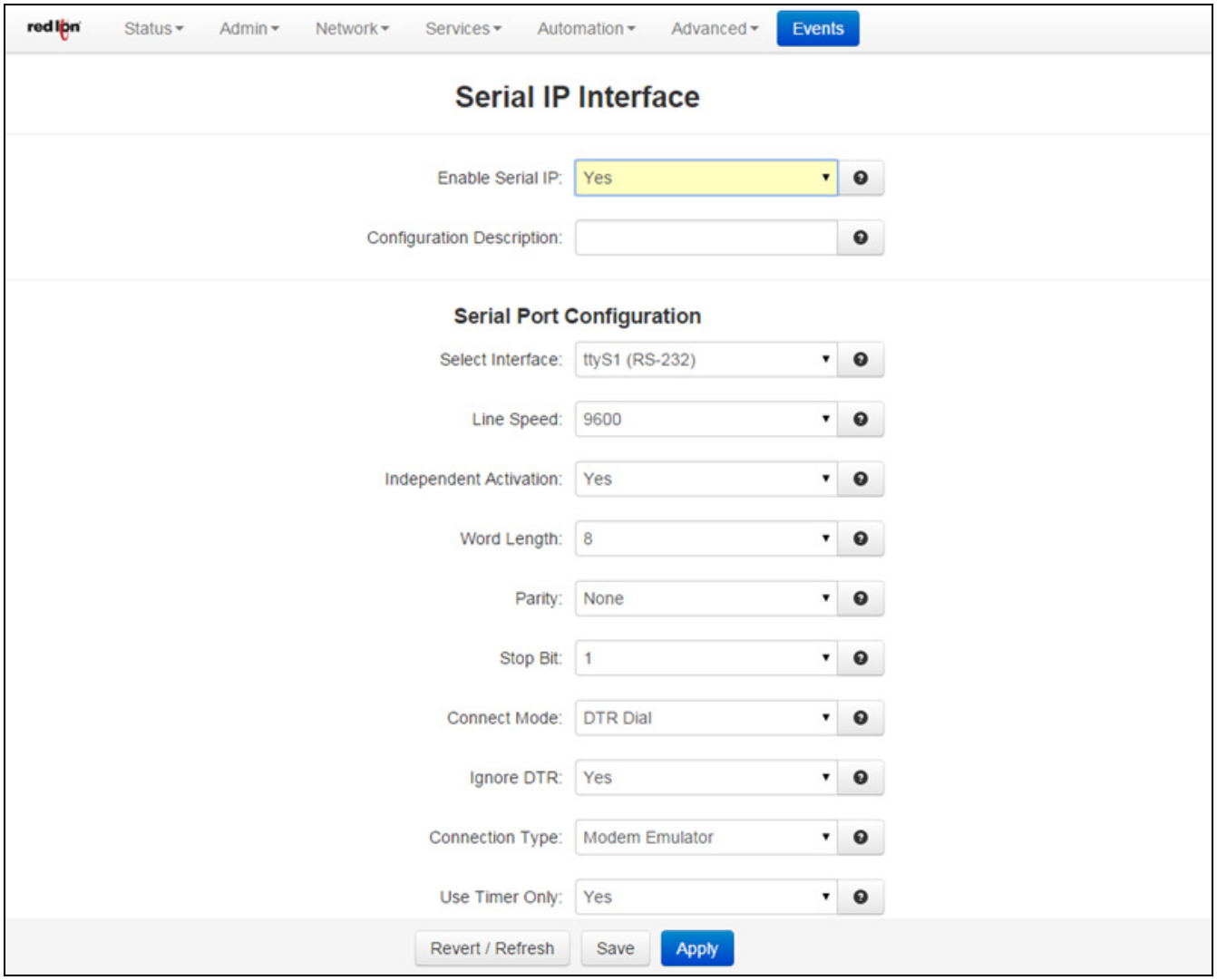
It is best practice to insert the SD Card into the Red Lion device, Apply Directory Structure then move the SD Card to your other environments to copy the applicable files.

Download: Download the selected file to your computer.

3.5.16 Serial IP

The Serial IP menu item is used to configure serial communication such as POS device, serial data logging or serial transmitter via serial cable on the Red Lion RTU or router and third party UDP or TCP/IP Client/Server application.

Select the Serial IP menu item and the following dialog window appears:



Enable Serial IP: Select Yes to enable the Serial IP interface.

Configuration Description: Enter a description to describe the intent of this communication. Character limit is 128.

Select Interface: Select the interface to be used by clicking on the drop-down menu. The available options are: ttyS1 (RS-232), ttyS5 (RS-485) and ttyAUX0.

Line Speed: Select the desired interface speed to be used via the provided drop-down. Consult the configuration of the remote device being attached, this setting must be compatible.

Independent Activation: This option determines if the Serial Port of the device will accept data before the remote side is active. At least one of the two sides in the configuration must be set for Independent Activation.

If neither side is set, then the device will not accept date. This function provides integrity for the device by preventing data from being accepted until it can be delivered successfully.

Select *Yes* for standard usage. Select *No* for serial to TCP Server configuration to insure there is a TCP Server socket available before marking the serial port active. Select *Negotiate* only if directed by Red Lion Technical Support.

Word Length: Select the word length (bits per character) to be used via the provided drop-down. Consult the configuration of the remote device being attached, this setting must be compatible.

Parity: Select the parity to be used via the provided drop-down. Consult the configuration of the remote device being attached, this setting must be compatible.

Stop Bit: Select the number of stop bits to be used via the provided drop-down. Consult the configuration of the remote device being attached, this setting must be compatible.

Connect Mode: If this option is set to No, the device will expect to receive AT Commands in order to go to active state. Some DTE (Data Terminal Equipment) devices required to go active if they provide DTR (Data Terminal Ready) signal. The recommended setting for this field is *Yes*, if DTR is the connect signal.

Ignore DTR: This option needs to be set to Yes, if the serial port is connected to a DTE device that only provides 3 wires (Transmit, Receive and Ground) for communication or the DTE device could drop DTR signal while sending AT commands. The recommended setting for this field is *YES* if 3 wires connection is expected.

Connection Type: Select the connection type you desire from the drop-down list. The recommended setting for this field is Modem Emulator for direct connection.

Modem Emulator: Provided direct connection between the device serial port and the DTE terminal via straight RS232 cable.

Via Modem: This option is only used if the device provides TELCO/BPX or RJ11 To Terminal port for communication.

Use Timer Only: This option provides two different methods of detecting the end of message indicator on received serial port data.

Select *Yes* in order to use the Inter Character Timeout value configured on this device as the end of message indicator.

Select *No* in order to define the end of message character(s) string indicator.

If this option is set to *Yes* the Define End of Message and Strip End of Message indicators options are displayed.

Define End of Message Indicator (hexadecimal): The end of message character(s) are used to determine when the end of the message is received by the device serial port. Any hexadecimal character(s) 0-9, a-f or A-F can be configured as end of message indicator.

Strip End of Message Indicator: Used to select whether or not to strip the end of message character(s) before forwarding the message to the remote network.

Inter Character Timeout (ms): When the timer expires on the serial port, the device will forward the message received to the remote device. This option is used when there is no consistent character to signal the end of a received message. This timer will be reset to the configured value on each received character. The recommended value for this field is 5 milliseconds at 9600 baud.

Maximum Buffer Size: Set the maximum buffer size to be used for receiving serial data before forwarding to the remote device. A value of 0 will allocate 8192 bytes of buffer by default and the data could be sent to the remote application based on TCP stack window size. The recommended setting for this field is 292 for DNP3 type connections and 0 for all other connections.

Enable Hardware Flow Control: Select Yes to set hardware flow control using RTS and CTS signals. The recommended settings for this field are: *No* if dealing with 3 wires port (Transmit, Receive and Ground pins), *Yes* if dealing with the port that have all their signal pins present.

Number of Missed Polls Allowed: Set the maximum number of missed RTU polls before re-initializing all the internal memory and buffer conditions. If a packet is transmitted out the serial port and no response packet is received, this is counted as a missed poll and data content is not evaluated.

Recommended Setting:

0 - To disable this action.

Any other value greater or equal to 5 is dependent upon your environment requirements.

Show Advanced Configuration: Select *Yes* to configure advanced Serial IP options.

Enable DNIS Table Routing: Select whether or not to Enable the DNIS Table Routing for this communication. If this option is selected as *Yes*, the device will use the connect table entries to configure the device for serial and TCP/IP communication. This option will force the device to read multiple entries based on *LABEL* (phone number) and connect to appropriate TCP/IP server destination. You can access the connect Table configuration via GUI by clicking:
Advanced → GWLNX → Connect Table Configuration

Recommended Setting:

No - For standard usage

Yes - For routing an ATD (phone number) command to a specific remote destination.

TCP/UDP Port Configuration

Socket Type: Select the Socket Type you desire to have for Serial IP communication from the drop-down list.

UDP: If this option is selected, the device will act as a UDP (Connectionless) and listening on the configured Listening IP Port for connection from the client.

Peer IP Address (Required): Enter the peer IP Address into this field. This is required for UDP communication. This specifies the Peer IP address and if set to 0.0.0.0 any remote IP can send UDP packets to our peer port, and return packets will be sent back to the IP of the last host that sent a message. Packets cannot be sent until one is received first (to learn the remote peer's IP). If set to a specific IP, then packets will be sent to this IP only. The recommended setting for this field is "0.0.0.0" to allow any IP to send packets to the peer import number. You also have the option to set a second, third, fourth and fifth address in respective fields further below on the dialog window.

Peer IP Port (Required): Enter the peer Port number into the field. This is required for UDP communication. Consult your network administrator for UDP applicaton destination port number. You also have the option to set a second, third, fourth and fifth address in respective fields further below on the dialog window. You also have the option to set a second, third, fourth and fifth port in respective fields further below on the dialog window.

Client IP Port (Required): Enter the client IP port number into this field. This is required if the peer IP Address is set to a specific IP, then packets will be sent to specific IP at this client IP port number only. Consult your network administrator for UDP application destination port number. Set to 0 if the Peer IP

is set to “0.0.0.0”. You also have the option to set a second, third, fourth and fifth port in respective fields further below on the dialog window.

Source Interface: Select a source interface to bind to. The recommended setting is None, if you are not using any tunnels.

Note: This option could be very crucial if your connection is going through some GRE or IPSec tunnels.

TCP Client: If this option is selected, the device will act as a TCP Client and connects to the host processor once the serial port becomes active.

Enable IP Destination Config File: Enabling this option allow you to configure the host destination IP/Port address or DNS Name/Port number via **Advanced → GWLNX → IP Destination** option. The advantage of this option is to change the host destination without changing any settings in Serial IP configuration screen. The recommended setting is *Yes*, if configuring the IP destination via **Advanced → GWLNX → IP Destination**.

TCP/UDP Independent Activation: This option determines if the TCP/IP port of the device will accept data before the remote side (Serial Port) is active. At least one of the two sides in the configuration must be set for Independent Activation. If neither side is set, then the device will not accept data. This function provided integrity for the device by preventing data from being accepted until it can be delivered successfully. A TCP Server set to Yes, will listen even if the serial side is not considered connected, If set to *No*, it will not listen for a connection until the serial side is considered connected. A TCP Client set to *Yes* will always attempt to connect to the configured destination IP, even if the serial side is not connected or active. If set to *No*, it will attempt a connection only when the serial side is first considered connected. The recommended setting is *Yes* for Servers and *No* for clients.

TCP Headers: Select the TCP/IP Header Type (Message Length Field) required for TCP/IP communication from the drop-down list. The available options for this field as shown below.

None: If this option is selected, the device will not add or remove any bytes as the length field from the data packets received or transmitted.

Standard: If this option is selected, the device will add 2 bytes of binary exclusive network order to all transmitted TCP packets, and will remove the 2 bytes from the received TCP packets.

Extended: If this option is selected, the device will add 4 bytes of binary exclusive network order to all transmitted TCP packets, and will remove the 4 bytes from the received TCP packets. Extended header normally is used as an indicator First, Mid and Last when dealing with the large TCP messages and possibility of TXP/IP packet fragmentation.

Host IP Address (Required): Enter the host destination IP Address into this field. This is required if the device is acting as a TCP/IP Client.

Host IP Port (Required): Enter the host destination Port Address in this field. This field is required if the device is acting as a TCP/IP Client.

Client Source Port: Enter the Source Port Address into this field This is required if the device is acting as a TCP/IP client and using specific source port for TCP socket connection.

TCP Server: If this option is selected, the device will act as TCP Server and listen on the configured Listening IP Port for connection from the client.

TCP/UDP Independent Activation: This option determines if the TCP/IP port of the device will accept data before the remote side (Serial Port) is active. At least one of the two sides in the configuration must be set for Independent Activation. If neither side is set, then the device will not accept data. This function provided integrity for the device by preventing data from being accepted until it can be delivered successfully. A TCP Server set to Yes, will listen even if the serial side is not considered connected, If set to *No*, it will not listen for a connection until the serial side is considered connected. A

TCP Client set to *Yes* will always attempt to connect to the configured destination IP, even if the serial side is not connected or active. If set to *No*, it will attempt a connection only when the serial side is first considered connected. The recommended setting is *Yes* for Servers and *No* for clients.

TCP Headers: Select the TCP/IP Header Type (Message Length Field) required for TCP/IP communication from the drop-down list. The available options for this field as shown below.

None: If this option is selected, the device will not add or remove any bytes as the length field from the data packets received or transmitted.

Standard: If this option is selected, the device will add 2 bytes of binary exclusive network order to all transmitted TCP packets, and will remove the 2 bytes from the received TCP packets.

Extended: If this option is selected, the device will add 4 bytes of binary exclusive network order to all transmitted TCP packets, and will remove the 4 bytes from the received TCP packets. Extended header normally is used as an indicator First, Mid and Last when dealing with the large TCP messages and possibility of TXP/IP packet fragmentation.

Allow peer to Re-attach While Connected: Select whether or not to allow TCP peer to re-attach to our server while the socket is connected. If enabled, a new connection attempt from the same peer will be accepted, and the previous TCP connection will be closed. This can be useful to re-establish a connection if the link is not closed gracefully.

Listening IP Address (Required): Enter the listening IP Address into this field. This is required if the device is acting as a TCP/IP Server. If set to 0.0.0.0 any remote client can connect to our listening port, and if set to a specific IP, only client with configured IP can connect to our listening port.

Listening IP Port (Required): Enter the listening Port number into this field. This is required if the device is acting as a TCP/IP Server.

TCP Client/Server 2 Way: If this option its selected, the device will listen on configured Listening IP Port for client connection to communicate with serial device and once the client is disconnected, and the serial device connected to the ttyS1 port needs to report it's status, the device will connect to the host destination to report the device's status.

Enable IP Destination Config File: Enabling this option allows the user to configure the host destination IP/Port address via the IP Destination option in the Advanced menu. The recommended setting for this field is *YES*, if configuring the IP destination via ***Advanced → GWLNX → IP Destination***.

TCP Headers: Select the TCP/IP Header Type (Message Length Field) required for TCP/IP communication from the drop-down list. The available options for this field as shown below.

None: If this option is selected, the device will not add or remove any bytes as the length field from the data packets received or transmitted.

Standard: If this option is selected, the device will add 2 bytes of binary exclusive network order to all transmitted TCP packets, and will remove the 2 bytes from the received TCP packets.

Extended: If this option is selected, the device will add 4 bytes of binary exclusive network order to all transmitted TCP packets, and will remove the 4 bytes from the received TCP packets.

Extended header normally is used as an indicator First, Mid and Last when dealing with the large TCP messages and possibility of TXP/IP packet fragmentation.

Host IP Address (Required): Enter the host destination IP Address into this field. This is required if the device is acting as a TCP/IP Client.

Host IP Port (Required): Enter the host destination Port Address in this field. This field is required if the device is acting as a TCP/IP Client.

Client Source Port: Enter the Source Port Address into this field This is required if the device is acting as a TCP/IP client and using specific source port for TCP socket connection.

Allow Peer to Re-attach While Connected: Select whether or not to allow TCP peer to re-attach to our server while the socket is connected. If enabled, a new connection attempt from the same peer will be accepted, and the previous TCP connection will be closed. This can be useful to re-establish a connection if the link is not closed gracefully.

Listening IP Address (Required): Enter the listening IP Address into this field. This is required if the device is acting as a TCP/IP Server. If set to 0.0.0.0 any remote client can connect to our listening port, and if set to a specific IP, only client with configured IP can connect to our listening port.

Listening IP Port (Required): Enter the listening Port number into this field. This is required if the device is acting as a TCP/IP Server.

UDP Broadcaster: If this option is selected, the device will support multiple UDP broadcast addresses. Click on **Add UDP Broadcast Port** to configure the port through the **UDP Broadcast Port Settings** window.

Peer IP Address (Required): Enter the peer IP Address into this field. This is required for UDP communication. This specifies the Peer IP address and if set to 0.0.0.0 any remote IP can send UDP packets to our peer port, and return packets will be sent back to the IP of the last host that sent a message. Packets cannot be sent until one is received first (to learn the remote peer's IP). If set to a specific IP, then packets will be sent to this IP only. The recommended setting for this field is "0.0.0.0" to allow any IP to send packets to the peer import number. You also have the option to set a second, third, fourth and fifth address in respective fields further below on the dialog window.

Peer IP Port (Required): Enter the peer Port number into the field. This is required for UDP communication. Consult your network administrator for UDP applicaton destination port number. You also have the option to set a second, third, fourth and fifth address in respective fields further below on the dialog window. You also have the option to set a second, third, fourth and fifth port in respective fields further below on the dialog window.

Client IP Port (Required): Enter the client IP port number into this field. This is required if the peer IP Address is set to a specific IP, then packets will be sent to specific IP at this client IP port number only. Consult your network administrator for UDP application destination port number. Set to 0 if the Peer IP is set to "0.0.0.0". You also have the option to set a second, third, fourth and fifth port in respective fields further below on the dialog window.

Second/Third/Fourth/Fifth Peer IP Address: In the respective fields, enter the second, third, fourth or fifth peer IP Address. This is the second, third, fourth or fifth broadcast destination IP address for

UDP communication. The recommended setting for this field is *<0.0.0.0>* if the additional peer IP address option is not used.

Second/Third/Fourth/Fifth Peer IP Port: Enter the second, third, fourth or fifth port number in the respective fields.

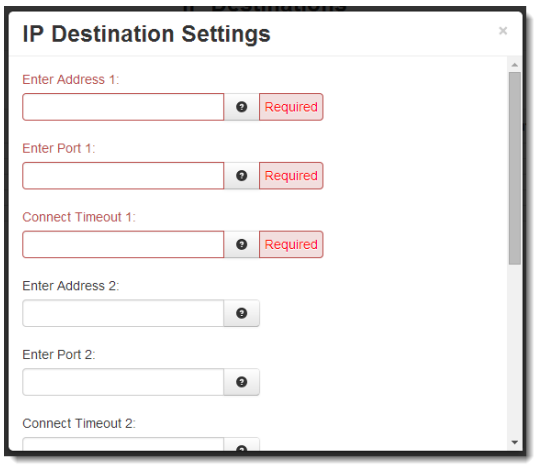
Second/Third/Fourth/Fifth Client IP Port: Enter the second, third, fourth or fifth client IP port number into the respective fields. This is Required if the second, third, fourth or fifth is set to a specific IP, then packets will be sent to specific IP at this client IP port number only.

TCP Client BroadCaster: If this option is selected, the device will support up to 20 TCP Client broadcast sockets using Configure IP Destinations for connectivity. These sockets are persistent connections when the serial port becomes active. Click on the Configure IP Destinations button to enter port information into the IP Destinations Table. See ***Configure IP Destinations*** explanation below for a description of available options.

TCP Client BroadCaster Traffic Activator: If this option is selected, the device will support up to 20 TCP Client broadcast sockets using Configure IP Destinations for connectivity and would connect only if the serial data is available to broadcast. Click on the Configure IP Destinations button to enter port information into the IP Destinations Table. See ***Configure IP Destinations*** explanation below for a description of available options.

Configure IP Destinations: Used when TCP Client BroadCaster or TCP Client BroadCaster Traffic Activator Socket Type options are selected.

Click on *Add* button to define the required IP Destination Settings.



Enter Address 1 (Required): This field indicates the Client Primary IP Address that the GWLNX uses to connect to the Host Server.

Enter Port 1 (Required): This field indicates the Client Primary Port Address that the GWLNX uses to connect to the Host Server Port.

Connect Timeout 1 (Required): This field is used to specify the time (in seconds) to attempt a connection to this TCP Destination, before declaring it unreachable. After the specified time, the next destination will be attempted. The valid range is 2 - 250 seconds. The recommended setting for this field is 10 seconds. A value of less than 10 seconds is not recommended for wireless environment.

Enter Address 2/3: This is a Client First Alternative IP address that GWLNX uses to connect to the Host Server.

Enter Port 2/3: This is a Client First Alternative Port address that GWLNX uses to connect to the Host Server Port.

Connect Timeout 2/3: Specify the time in seconds to attempt a connection to this TCP Destination, before declaring it unreachable. After the specified time, the next destination will be attempted. The valid range is 2 - 250 seconds. The recommended setting for this field is 10 seconds. A value less that 10 seconds is not recommended for a wireless environment.

Header Type: This field indicates a Header Length used in TCP/IP packet that contains the message length being Send or Receive. Available options in this field are: Default, None and JBM Standard. The recommended setting is *Default*.

Click on the *Finish* button when the required information has been entered. You will be returned to the IP Destinations dialog window and the IP Destinations Table Properties table will be populated with the entered data.

To delete an existing IP Destination, select it in the table and click on the *Delete* button. To edit an existing IP Destination, select it in the table and click on the *Edit* button.

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert*, will reset all fields to previously saved defaults.

3.6 Automation Tab

The Automation menu contains all aspects of managing your Modbus and DNP3 based I/O transfers or messages.

This option is only supported in the RAM 6000 and the RAM 9000 series. The RAM 6000 or RAM 9000 acts as a MODBUS Master and as an I/O concentrator for MODBUS/DNP3 devices. I/O for these devices can be read or written using MODBUS/DNP3 I/O transfers with the RAM 6000 or RAM 9000 acting as a MODBUS/DNP3 master. I/O data is stored in a local I/O database.

The RAM 6000 and RAM 9000 series will support:

- I/O transfers using MODBUS/DNP3
- Slave Station Status
- Forwarding of MODBUS/DNP3 messages
- Developing of third party applications using our SDK based on ELDK4.2 and the SIXNET IODB API.

Additionally, the RAM 6000 and RAM 9000 series will act as a MODBUS slave. This allows MODBUS masters to request or update I/O points in the I/O database.

Modbus Configuration

User interfaces will be provided to configure I/O transfers, the MODBUS forwarding table and serial interfaces. MODBUS configuration data will be stored in an XML based file named modbus.xml. This file will contain the following sections:

- **serials:** xml section to define the parameters used for serial ports for both MODBUS and DNP3.
- **localStation:** xml section to define the local station number and name for both MODBUS and DNP3.
- **remoteStations:** defines remote stations and the I/O transfers associated with them.
- **regAllocation:** defines the number of registers for each I/O type.
- **forwards:** defines the list of remote stations to forward MODBUS requests.

There are two (2) methods to configure these sections.

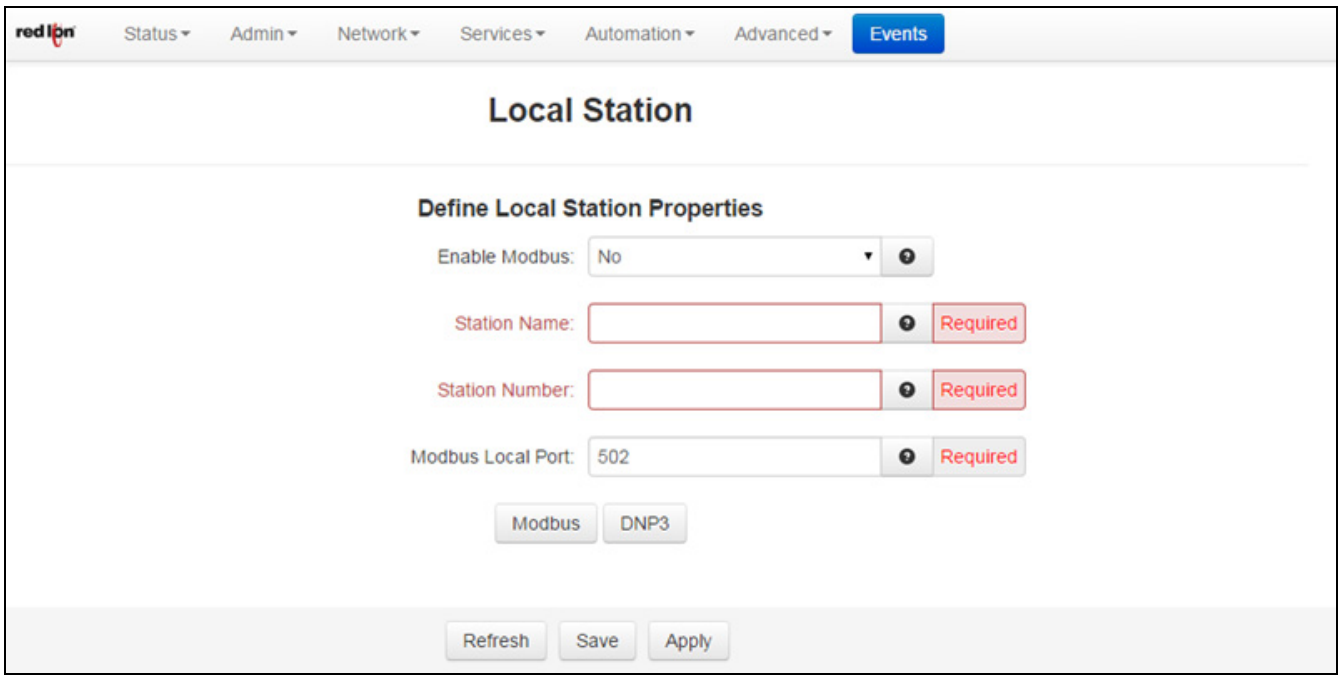
- **CLI:** The command line interface for the cellular RTUs and routers provides a Cisco-style telnet command line interface. It writes an XML configuration file, which is used to drive the backend daemons.
- **Web UI:** This method is a WEB based interface which is the focus of this documentation.

The user interfaces will have the ability to:

- Configure/Display local station information such as station name and station number.
- Configure/Display serial ports
- Configure/Display remote stations
- Configure/Display I/O transfers
- Configure/Display MODBUS forward stations
- Configure/Display MODBUS registers allocation

3.6.1 Local Station

Click on the Local Station sub menu item and the following menu appears:



Enable Modbus: Select Yes to enable the Modbus option.

Station Name (Required): Enter the name of the local station. The station name must be less than or equal to 32 characters.

Sation Number (Required): Enter the local station number. The station number must be in a range of 1 - 247. The values may be duplicated for other station as long as the station as long as the station can be uniquely addressed by an IP address or is connected on a serial port. **Note:** 0 is a broadcast address. 248-255 are reserved addresses.

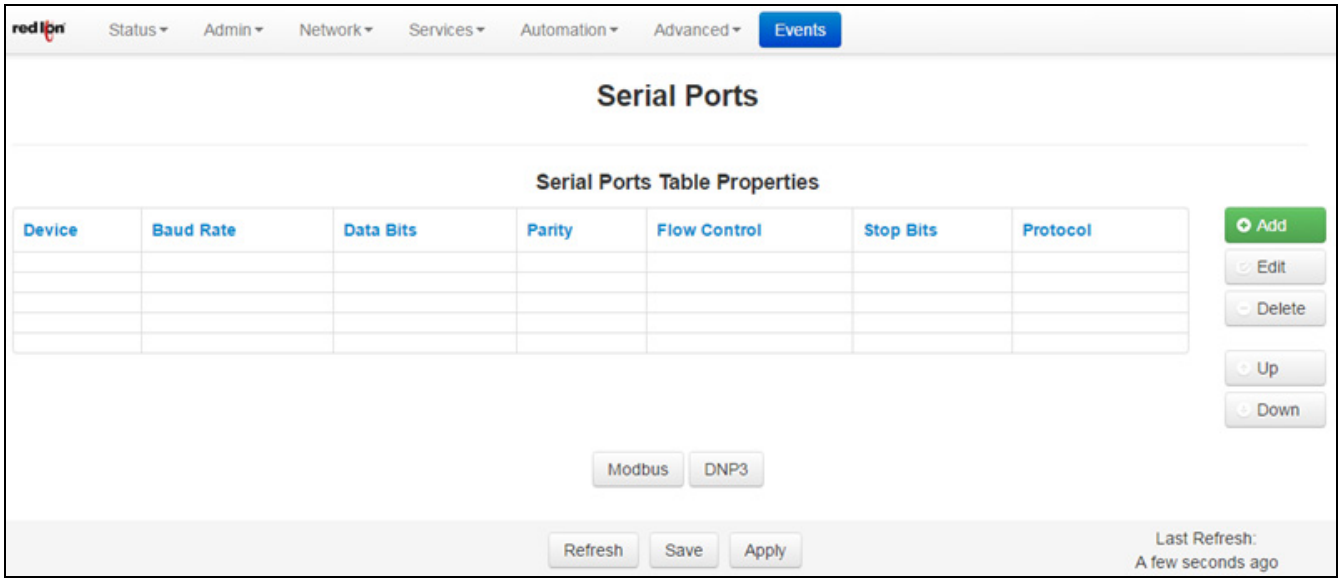
Modbus Local Port (Required): Enter a valid port number. The port must be within the range of 1 - 65535 and the recommended default port is set to 502. Take care to choose a port number not already used by other system services. Consult Status→Network →Socket Statuses →TCP Only for a list of ports currently in use. Please note that a Firewall Allow rule will need to be added for remote access.

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately.

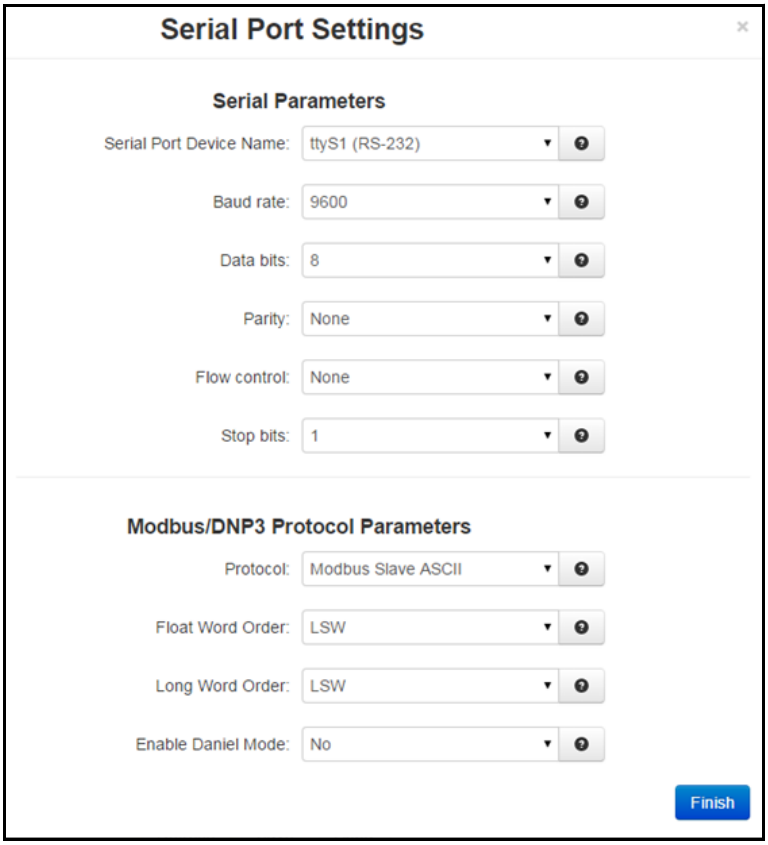
3.6.2 Serial Ports

This section is used to configure the RS-232 port that is facing the front of the Red Lion device as well as the RS-485 terminal (only available on the RAM 9000 Series) to integrate into your Modbus/DNP3 schema.

Click on the *Serial Port* menu item and the following window appears:



Click on the *Add* button and the following pop-up window appears:



Serial Port Device Name: Name of the serial device. Valid values: ttys1 (RS232), ttys5 (RS485)

Baud Rate: Baud rate for the serial device. Supported baud rates are: ***300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 and 115200.***

Data Bits: Number of data bits. Supported data bits are ***7*** and ***8***.

Parity: Parity for serial device. Supported parities are: ***none, even, odd, mark*** and ***space***.

Flow Control: Flow control for serial device. Supported flow controls are: ***none, hardware, xon/xoff, half duplex, full duplex.***

Stop Bits: Stop bits for serial device. Supported stop bits are ***1*** and ***2***.

Protocol: Protocol being used on serial device. Supported protocols are: ***DNP3, Modbus Master ASCII, Modbus Master RTU, Modbus Slave ASCII, Modbus Slave RTU, Modbus Master RTU Fwd*** and ***Modbus ASCII Fwd.***

Float Word Order: Controls the swapping of words within floats. Ignored if using Daniel mode. This is needed for configuring the serial slave application. Supported orders are ***LSW*** and ***MSW.***

Long Word Order: Controls the swapping of words within longs. Ignored if using Daniel mode. This is needed for configuring the serial slave application. Supported orders are ***LSW*** and ***MSW***.

Enable Daniel Mode: Use Daniel mode extensions when dealing with longs and floats. This is needed for configuring the serial slave application.

Click on the *Finish* button to populate the Serial Ports Table Properties.

To delete a serial port, select it in the table and click on the *Delete* button. To edit a serial port, select it in the table and click on the *Edit* button.

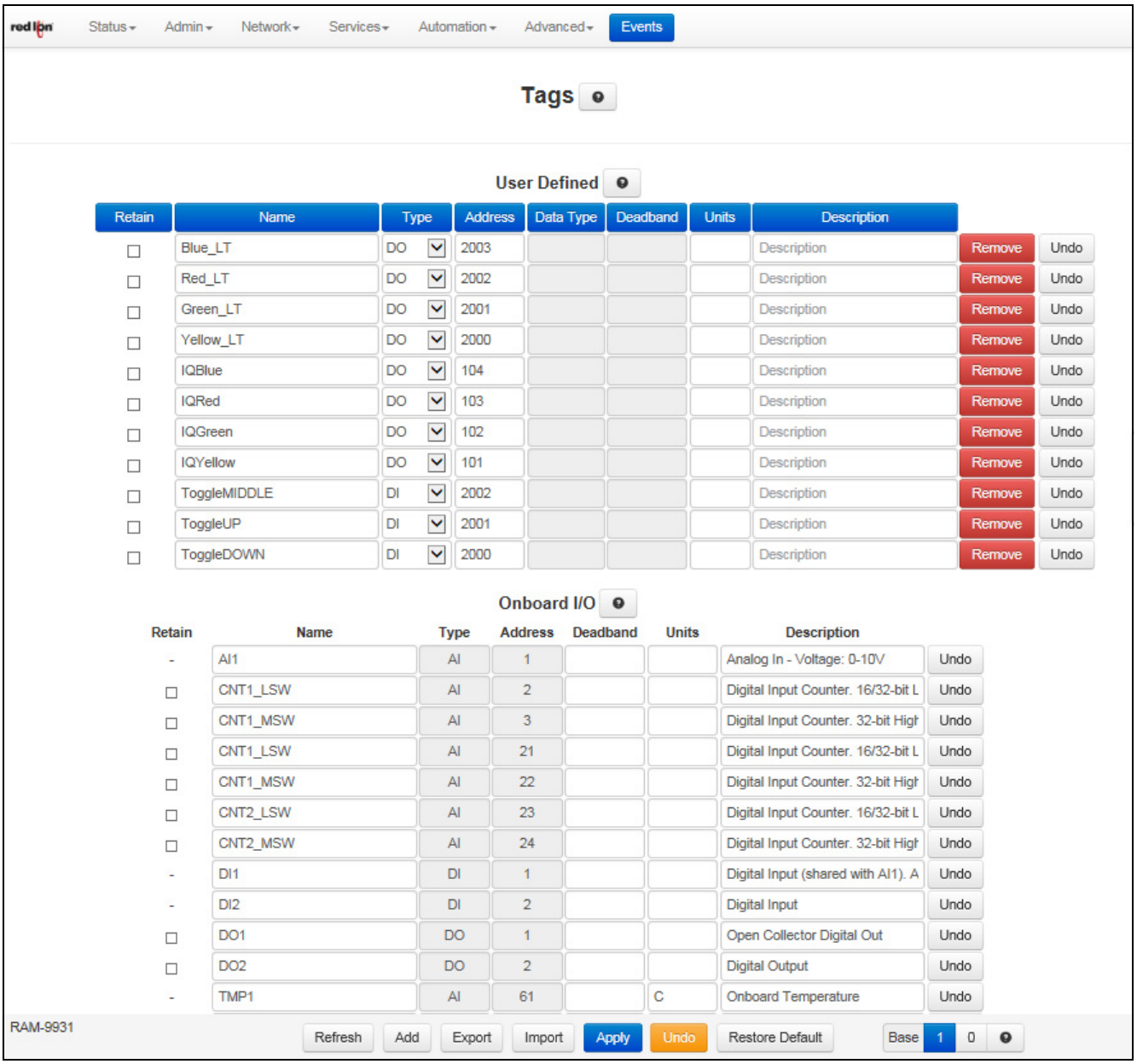
Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

3.6.3 Tags

Tagging is a method used to attach a human readable and yet logical name to an IODB register. These tags provide an easier method of organizing and identifying internal registers when designing and monitoring the data in a Modbus environment.

Tags are used for local reference only and do not get transferred between master and slave devices when performing IO transfers.

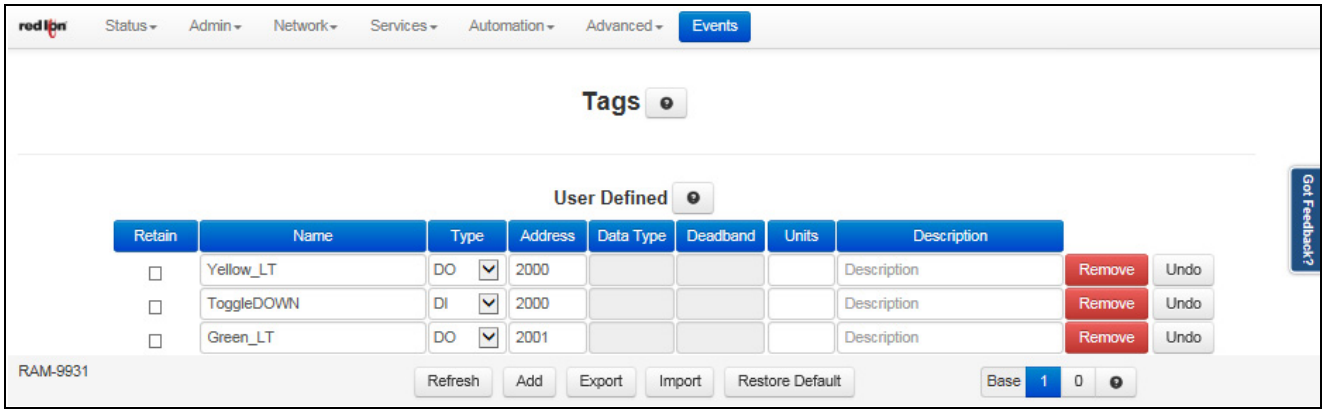
Base 1 0: This toggles the system-wide register display format, which can be represented in two schemes: Zero-based or One-based. Zero-Based is also called Native format, and all register ranges would begin counting at 0. One-Based addressing starts all ranges with 1, and is the system commonly used with Modbus.



User Defined

Create custom tags for your I/O here. These tags will be listed in drop-down forms throughout this user interface. Tag names must be unique and may not copy the names of Onboard or Status tags.

To add a new tag, click on the *Add* button located at the bottom of the dialog window. A new blank line appears.



Retain: Checking this box allows the register value associated with the tag to be retained in battery-backed SRAM across a device power cycle. **This feature is only available on the RAM 9000 models.**

Name: Enter a unique name for the tag. The tag name may contain upper and lower case alpha numerical characters. The only special characters allowed are the period (.) and the underscore (_).

Type: Select the desired output type from the drop down list. Available choices are: AI, AO, DI, DO, LI, LO, FI, FO.

Address: Enter the desired tag address. There are 65536 registers of each data type available.

Data Type: Click to select options for interpretation of this tag's value. Clicking this button brings up another pop up dialog window allowing the user to set the Data Type elements for the tag.

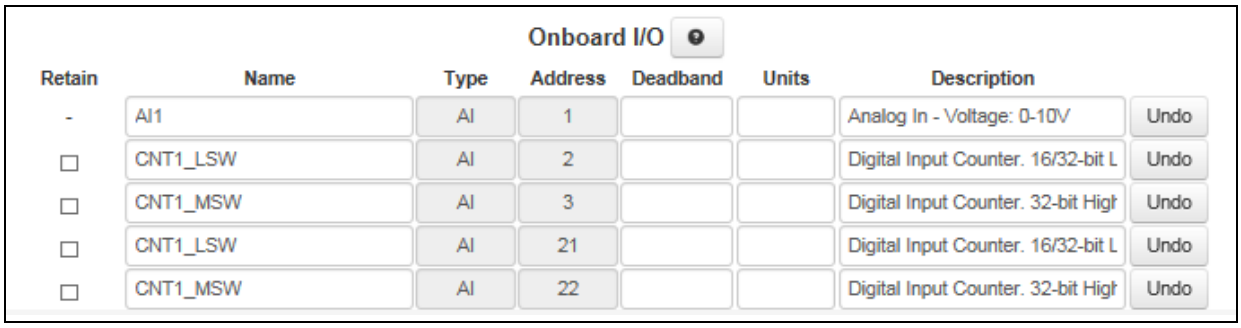
Deadband: The amount of +/- fluctuation of the data value before triggering a change notification for RAMQTT, Events, Data Logger, or other services.

Units: Enter the desired tag unit of measure as applicable.

Description: Enter a description of what the tag represents.

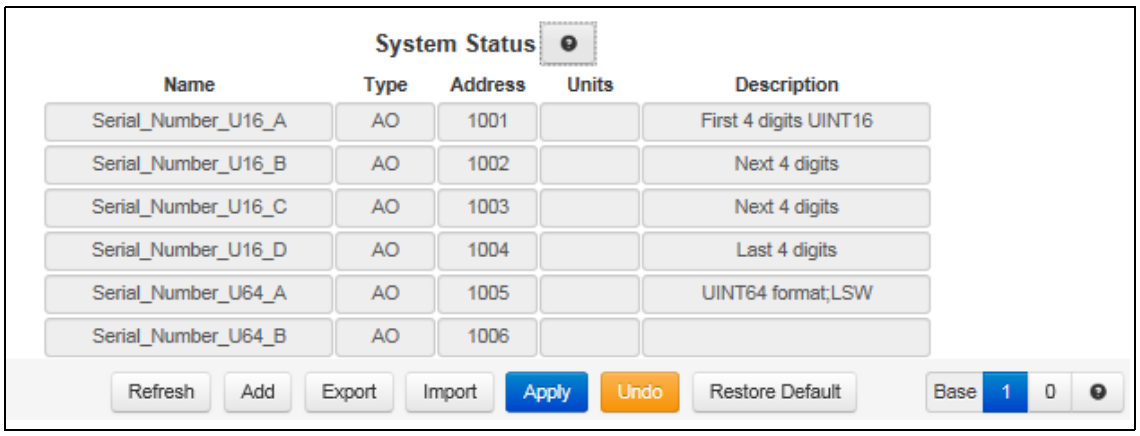
Onboard I/O

These tags are linked to physical I/O on the device. The type or address cannot be changed, but you may rename them according to function or connected hardware.



System Status

These tags are linked to status metrics internal to the device. They cannot be renamed or otherwise modified. See Appendix B in the user guide for more information.

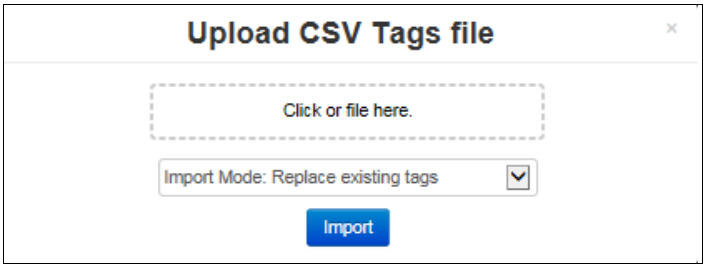


Click on the *Refresh* button to refresh screen after new entries have been entered.

To delete an existing tag, click on the *Remove* button next to the tag to be deleted.

To export the list of tags, click on the *Export* button and a *tags.csv* file will be created and can be found in the PC's downloads folder.

To import a list of tags, click on the *Import* button and the Upload CSV Tags file dialog window appears.

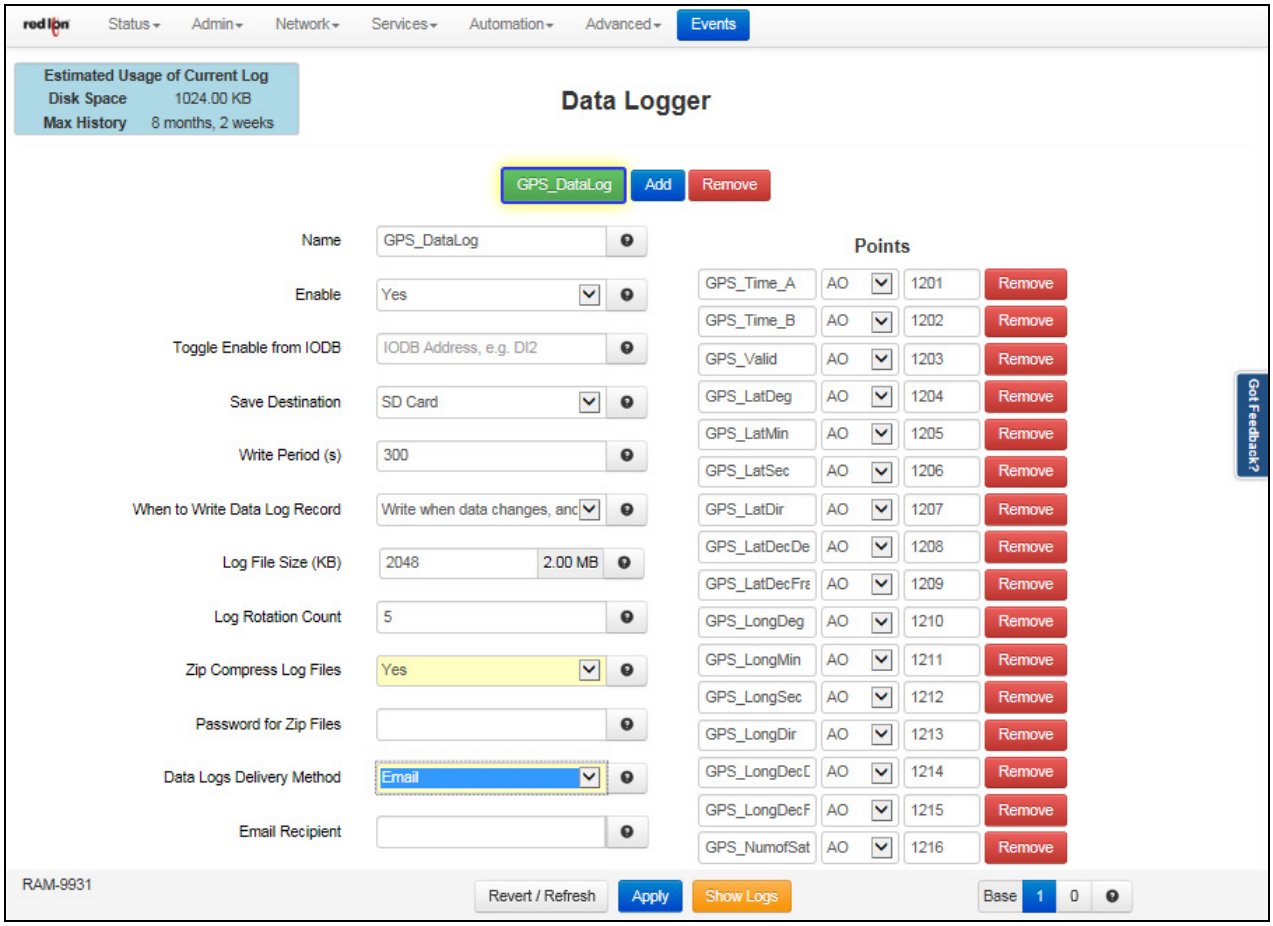


Click on the dashed button and browse to the location where the.*csv* file is located, select the Import Mode, then press the *Import* button. You may also drag the.csv file from a window and drop into the file upload dialog box.

To restore the system default Tags, click on the *Restore Defaults* button. All user defined tags will be removed from the list.

3.6.4 Data Logger

Click on the *Automation* menu item, select Data Logger from the drop-down menu and the following Data Logger configuration screen appears:



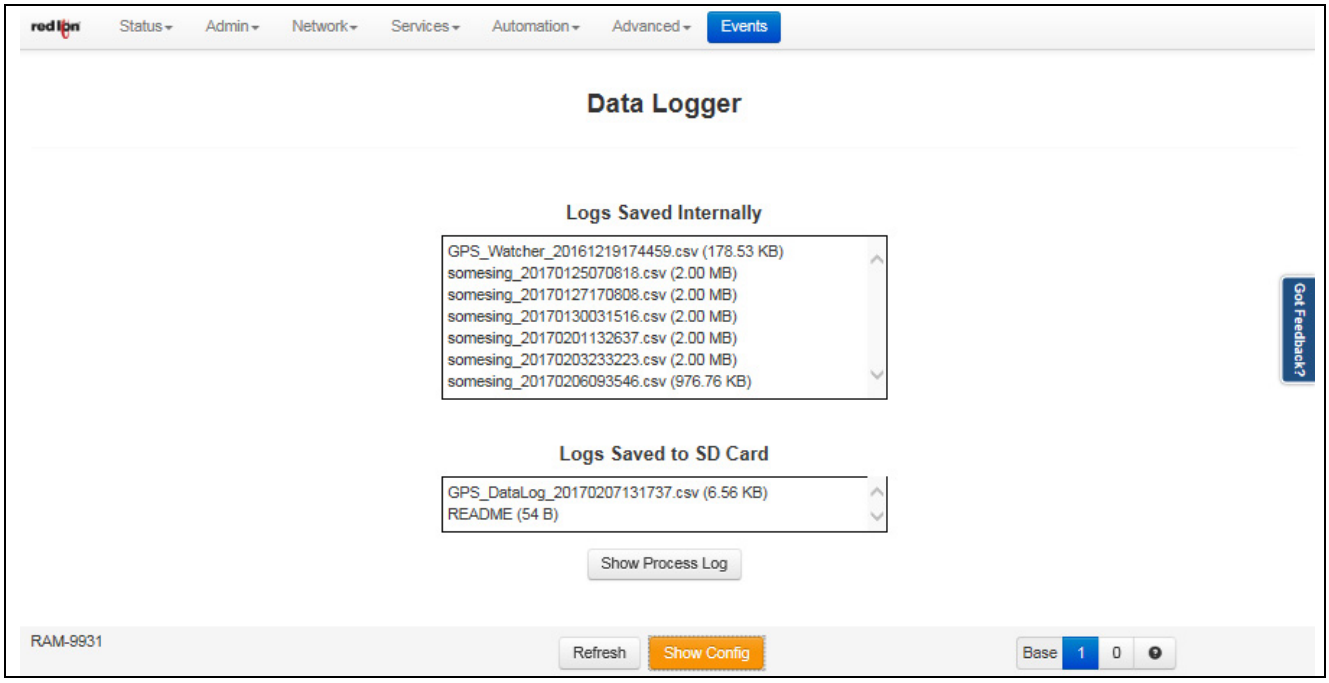
Data Logger allows for the collection of data from defined points and save them as a log file to an internal destination or to an SD card (only available on RAM 9xxx).

Note: The Data Logger feature is available on all models using release 3.23 / 4.23 or newer.

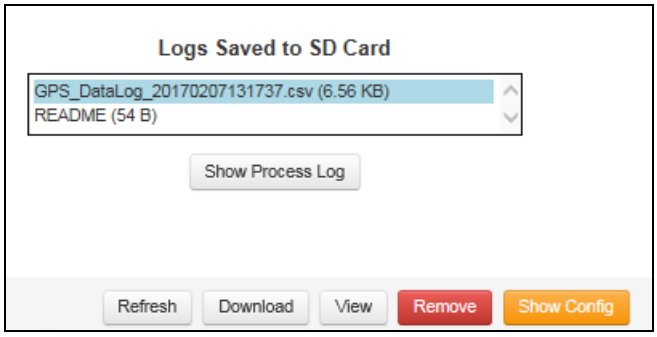
Navigation

Click on the green named log file button to display the data log configuration associated with the displayed log file name ([GPS_DataLog] in this example). Then click on Show Logs to display the list of datalog files.

Click on the *Add* button to create a new file and configure the data log file parameters.



Click on any file to select the log file to Download, View, Remove or show the Process log associated with the log file.



Click on the *Download* button to copy the selected Data Logger file to your PC for evaluation.

Click on the *View* button to load a snapshot of the beginning and end of the highlighted file, but does not display the entire file.

Click on the *Remove* button to remove the currently selected datalog config.

Click on the *Show Config* button to return to the Data Logger configuration screen.

Configure a Data Log File

Click the blue *Add* button to display a new data log file associated with the displayed log file name [No Name].

Configure the data log file by populating the screen fields.

Name: The name of your log. This will also be a prefix for the log files.

Allowed Characters: A-Z a-z 0-9 - . _

Enable: Enable this log. Points will be periodically recorded in a log file prefixed with the specified name.

Options - Yes/No

Toggle Enable from IODB: Toggle logging based on IODB register (optional field).

For example: if set to DI42, Points will only be recorded if register DI42 is high.

Save Destination: Destination for the log files. The available options are Internal or SD Card.

Internal will configure your logs to be stored internally on the device. These can be downloaded through the Web UI or with gatherstats

SD Card (if applicable) will configure your logs to be stored on the SD Card (if present)

Logs will be created in this folder: sdcard/datalogs/

Note: Estimated disk usage may change based on anticipated file system compression. This is in addition to any zip compression.

Write Period(s): How often a data log record will be created (in seconds)

Recommended: Relative to the rate of change you expect from the logged points

When to Write Data Log Record: There are two options that are paired with the write period. This setting will control what conditions create a data log record.

Write a record every period: If the Write Period is 60 seconds, this will create a new data log record every 60 seconds consistently.

Write when data changes, and periodically: The IODB list is sampled every second, and if changes are detected a record is created. In addition, a record will also be created every Write Period of time (60 seconds in this example).

Recommended: Relative to the rate of change you expect from the logged points

Log File Size (KB): Log file size (per file) in Kilobytes

Max: 10240 KB (10MB)
Min: 1 KB
Recommended: 2048

Log Rotation Count: The number of logs that will be kept in rotation

E.g., when the current log fills up, the oldest is removed, and a new log is started. If the number of logs in rotation exceeds this value, the oldest is removed

Recommended: 5

Zip-compress Log Files: Compress log files using zip

This will reduce storage space by 80%-90%

Password for Zip Files: Encrypt zip-compressed log files using this password.

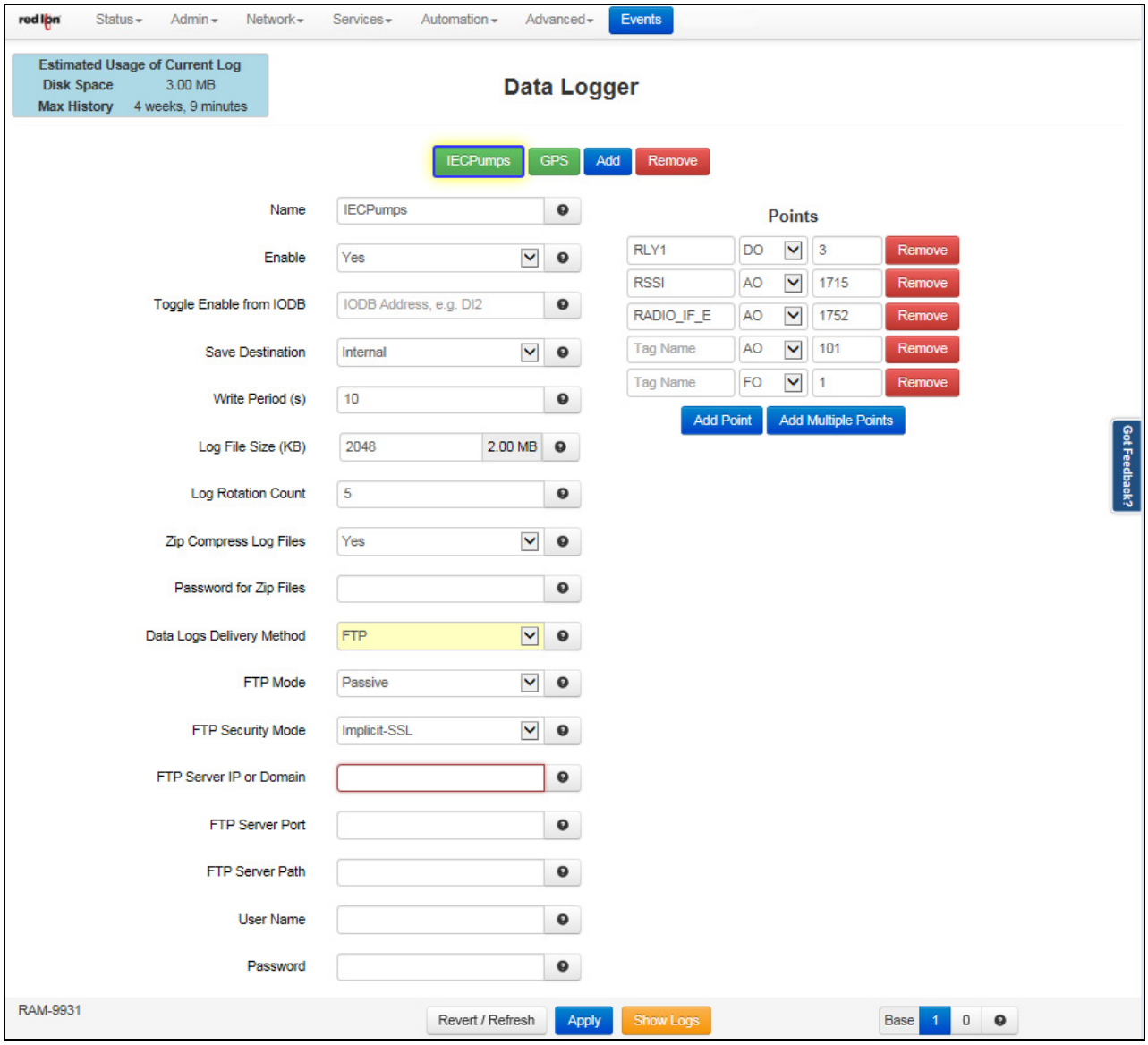
Data Logs Delivery Method: Select the delivery method for generated data logs; None, Email, FTP or Both.

Email Recipient: When selected enter an email address destination for the logs. Multiple email addresses may be entered by separating them with a **comma**.

Note: No spaces are allowed in this field.

Note: The Email Client service must be configured independent from the Datalog before emails can be sent successfully.

FTP: When selected enter the FTP configuration data for delivery of the data log by FTP.



FTP Mode

Passive: In passive mode FTP the client initiates both connections to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server. When opening an FTP connection, the client opens two random unprivileged ports locally (N > 1023 and N+1). The first port contacts the server on port 21, but instead of then issuing a PORT command and allowing the server to connect back to its data port, the client will issue the PASV command. The result of this is that the server then opens a random unprivileged port (P > 1023) and sends P back to the client in response to the PASV command. The client then initiates the connection from port (N+1) to port P on the server to transfer data.

Active: In active mode FTP the client connects from a random unprivileged port (N > 1023) to the FTP server's command port, port 21. Then, the client starts listening to port (N+1) and sends the

FTP command PORT (N+1) to the FTP server. The server will then connect back to the client's specified data port from its local data port, which is port 20.

FTP Security Mode

Implicit: Negotiation is not supported with implicit FTPS configurations. A client is immediately expected to challenge the FTPS server with a TLS **ClientHello** message. If such a message is not received by the FTPS server, the server should drop the connection.
In order to maintain compatibility with existing non-FTPS-aware clients, implicit FTPS was expected to listen on the IANA well known port 990/TCP for the FTPS control channel, and port 989/TCP for the FTPS data channel. This allowed administrators to retain legacy-compatible services on the original 21/TCP FTP control channel.

Explicit: In explicit mode (also known as FTPES), an FTPS client must **explicitly request** security from an FTPS server and then step up to a mutually agreed encryption method. If a client does not request security, the FTPS server can either allow the client to continue in insecure mode or refuse the connection.

specified data port from its local data port, which is port 20.

FTP Server IP or Domain: Enter the FTP server IP address or domain name.

FTP Server Port: Enter the port number associated with the IP address or domain name.

FTP Server Path: Enter the FTP server directory path. The directory path has to start and end with a / character.

User Name: Enter the user name required to connect to the FTP server.

Password: Enter the password required to connect to the FTP server.

Both Email and FTP: When selected enter an email address destination for the logs. Multiple email addresses may be entered by separating them with a **comma**, and complete all field entries for FTP delivery method.

Points: Configure fields to create data points

Tag Name: Enter the name

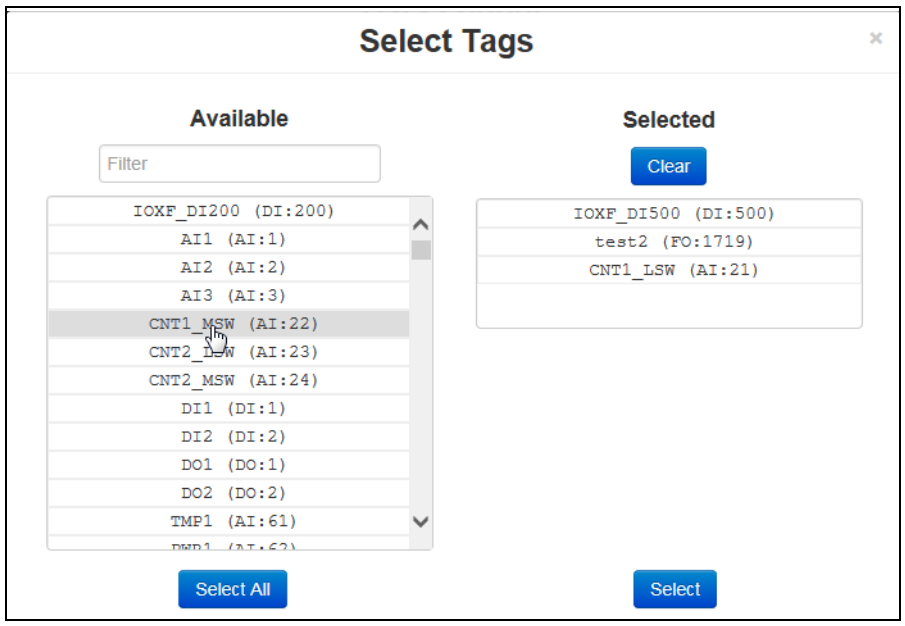
Type: Select from the drop-down menu options

Address: Enter the point address

ADD Point: Click to add the point just configured

Remove: Click to remove a data point

Add Multiple Points: Click to invoke a pop-up screen to select multiple points individually or all at once.



Selected Tags move from Available Selected list. Click *Select* button when finished making selections.

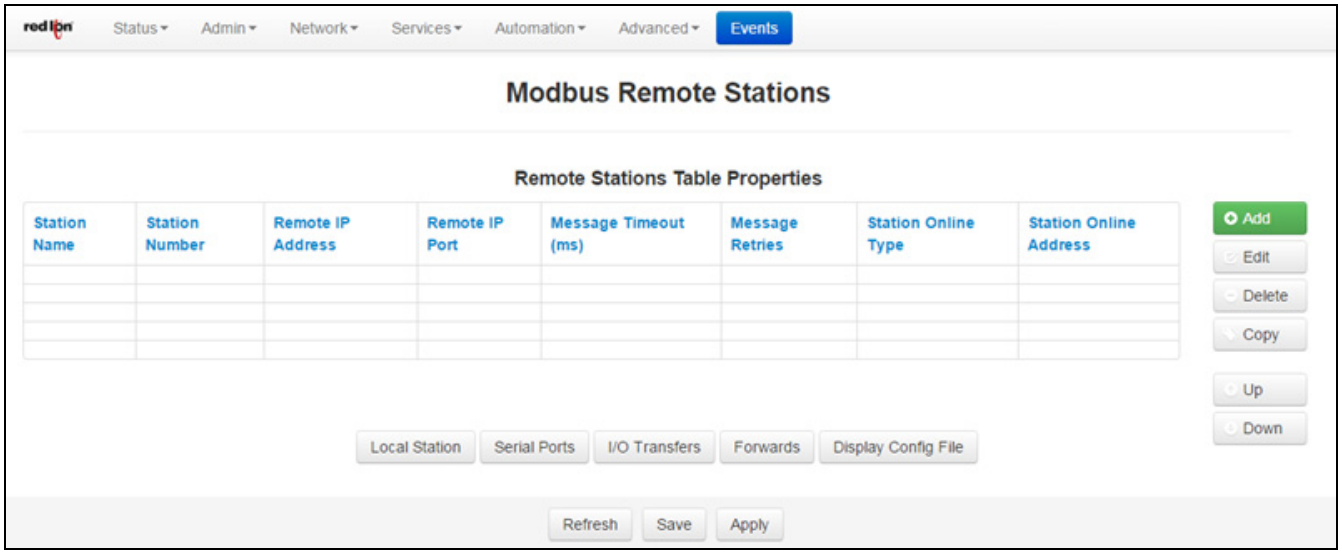
Base 1 0: Display toggle buttons located in the footer bar and will toggle the display of registers visible on the page from 0 based to 1 based.

Click the *Apply* button to save and apply the new data log configuration.

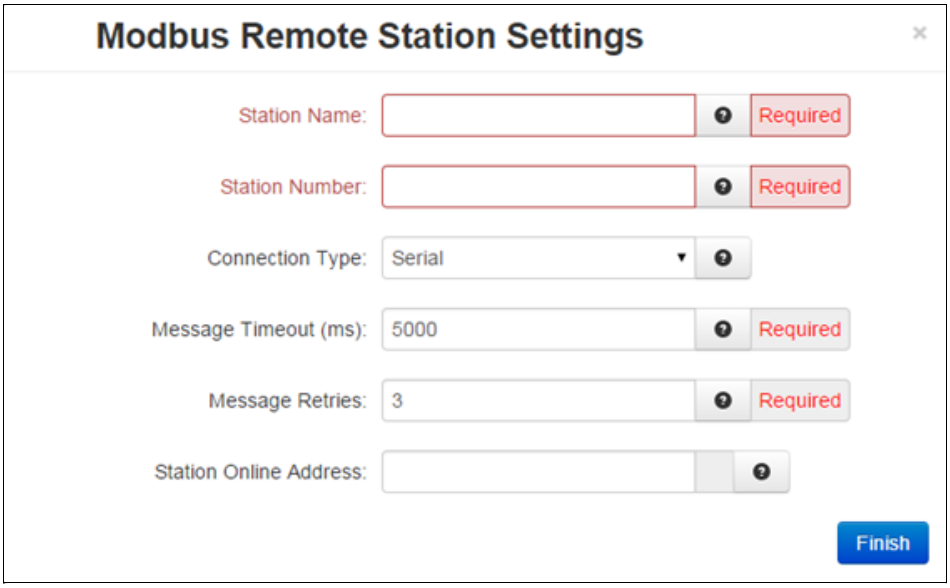
3.6.5 Modbus

Remote Station

Click on the *Remote Station* menu item and the following dialog window appears:



Click on the *Add* button to configure the remote station parameters and the following pop-up window appears:



Station Name (Required): Enter the name of the remote station. The remote station name must be less than or equal to 32 characters. All the defined remote station names will be populated in the I/O Transfer screens as a selection for assigning I/O transfer for selected remote station name.

Station Number (Required): Enter the remote station number. The station number must be in range of 1-247. Values may be duplicated for other station as long as the station can be uniquely addressed by an IP address or is connected on a serial port**. Note:** 0 is a broadcast address. 248-255 are reserved addresses.

Connection Type: Select the remote connection via the drop down. Available options are IP and Serial.

Remote IP Address (Required): Enter the remote station IP address in a valid IPv4 unicast address format, or it may be blank if I/O transfers to this remote station only use the serial port.

Remote IP Port (Required): Enter a valid IP port number (1-65535) that the remote station listens on for MODBUS requests.

Take care to choose a port number not already used by other system services. View *Status→Network→Socket Statuses→TCP* Only for a list of ports currently in use. Please note that a Firewall Allow rule will need to be added for remote access (*Network→Firewall→Port Allow/Forwarding Rules→Service Access Rules*).

Message Timeout (ms) (Required): Enter the Timeout period, in milliseconds, to wait for an I/O transfer to complete. The valid range is 10ms-60000ms.

Message Retries (Required): Enter the number of times to retry an I/O transfer before giving up. If a station status bit is provided, it would be marked off line when this occurs. The recommended value is 3.

Station Online Address: Discrete input address is used as a station status indicator. If provided, it is set to True when any I/O transfers to a remote station complete successfully, and false otherwise. Enter the Address of a local discrete input or blank if not used.

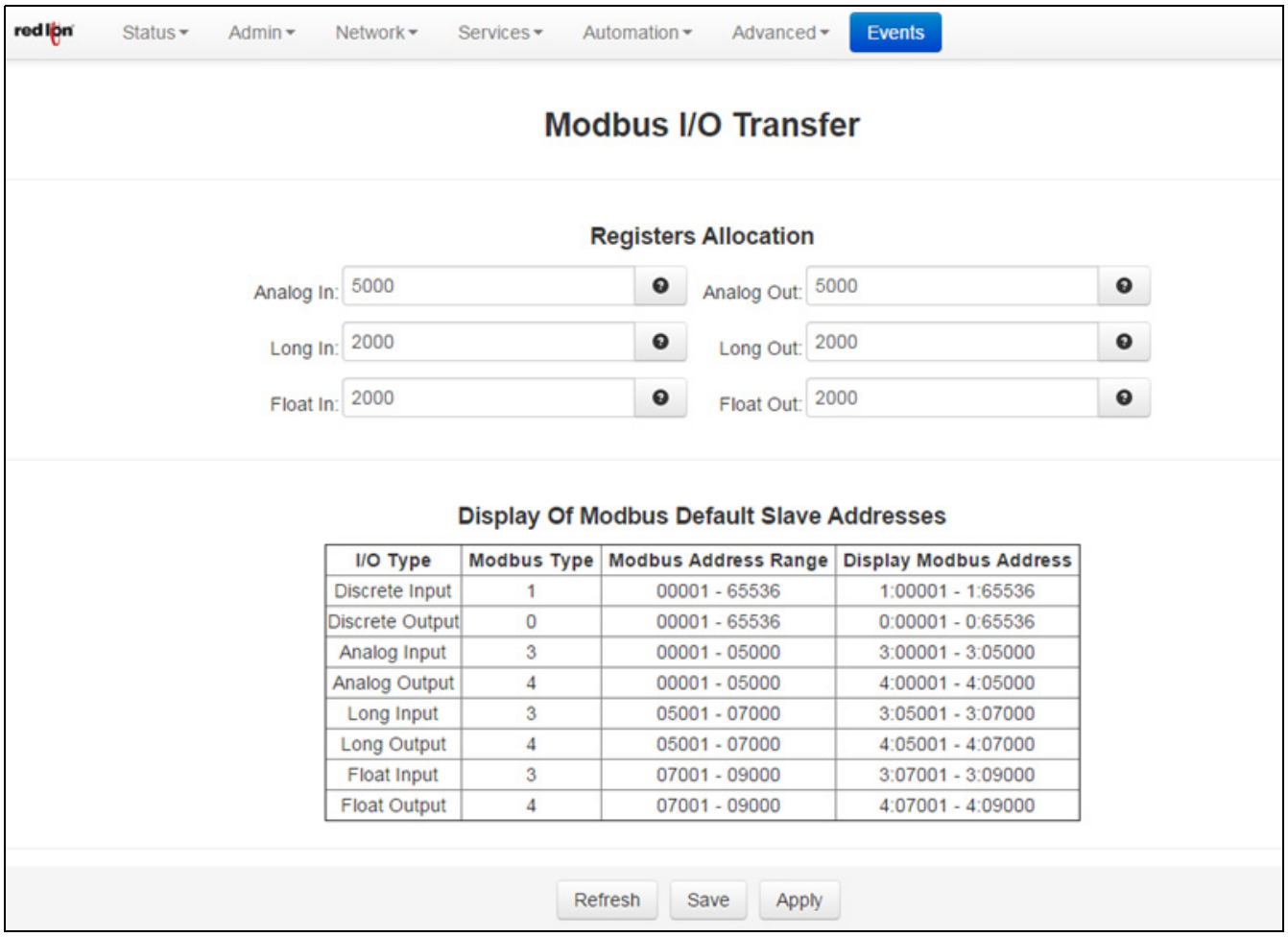
Click on the *Finish* button to populate the Modbus Remote Station Table. If more stations are needed, click on the *Add* button and enter the required field for each station.

To edit a *Remote* Station, select the station in the table and click on the edit button. To delete an existing station, select the station in the table and click on the *Delete* button.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

I/O Transfer

Click on the I/O Transfer menu item and the following window appears:



Register Allocation: This section is displaying the default values for the following:

Analog In: By default we support 5000 Analog Input registers, but the range is 1 - 10000.

Analog Out: By default we support 5000 Analog Output registers, but the range is 1 - 10000.

Long In: By default we support 2000 Long Input registers, but the range is 1 - 10000.

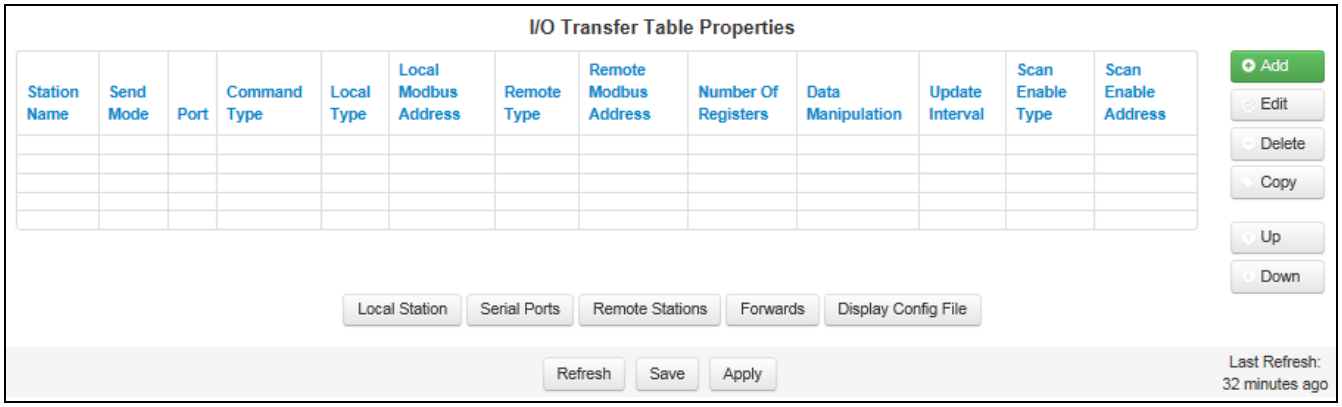
Long Out: By default we support 2000 Long Output registers, but the range is 1 - 10000.

Float In: By default we support 2000 Float Input registers, but the range is 1 - 10000.

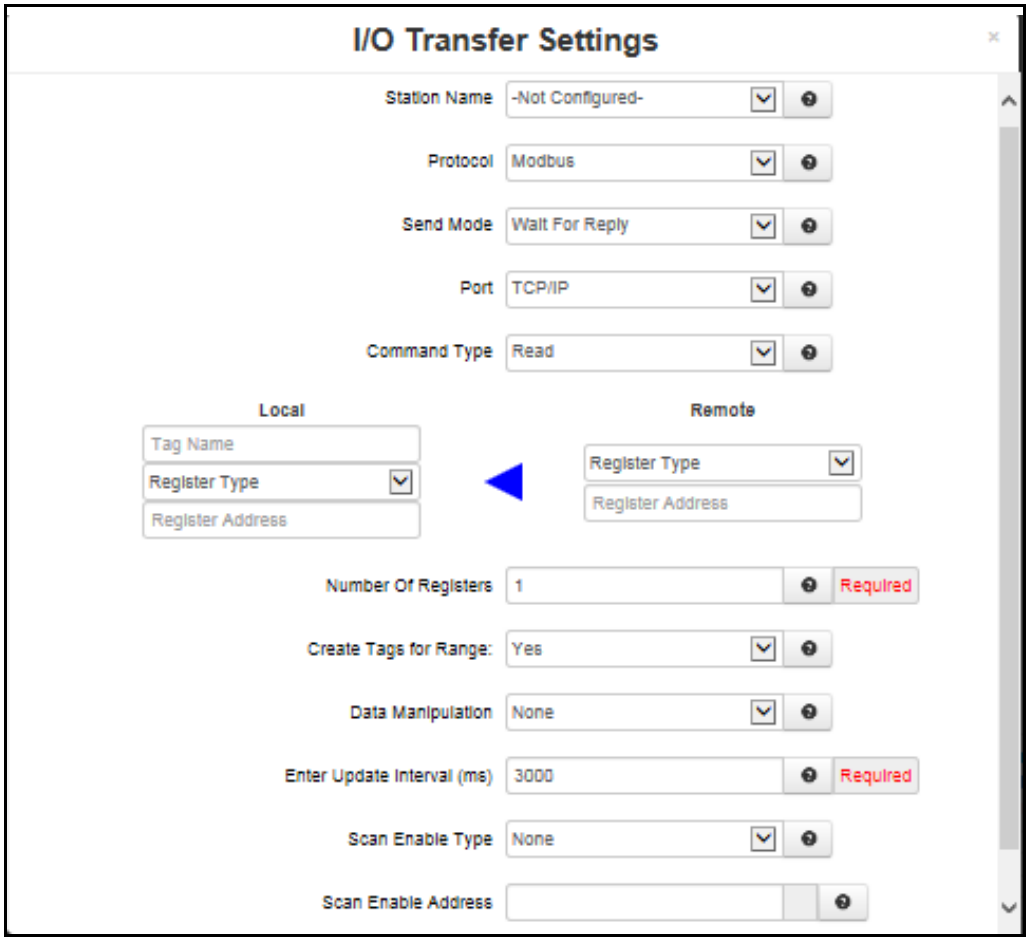
Float Out: By default we support 2000 Float Output registers, but the range is 1 - 10000.

The range of Modbus slave addresses are displayed based on default register allocation. You can change the registers allocation values to your required register values and the range of Modbus slave addresses will be changed based on the new values.

I/O Transfer Table Properties



Click on the *Add* button to configure the I/O Transfer for the remote station and the IO Transfer Settings pop-up window will open



Station Name: Name of the remote station for this I/O transfer. This option lists the name of all the remote stations that you have already defined and configured in remote station table entry. Select the remote station name that you want for this I/O transfer.

Protocol: Protocol used for the I/O transfer. Modbus is currently the only supported protocol used for I/O transfers.

Send Mode: Mode used to send an I/O transfer. Available options are:

waitForReply: The Modbus master must wait for an I/O request that it has sent to complete before sending another request to the remote station.

rapidFire: The Modbus master may send many I/O requests to a remote station before waiting for responses from the remote station.

Valid Values: Wait for Reply or Rapid Fire

Port: The port that the I/O request is being sent across. The supported ports are: RS232 Port, UDP and TCP. If UDP or TCP port are selected, the remote station selected for this I/O transfer should have its IP address defined.

Command Type: The commands used for I/O transfers are:

Read: Used for reading MODBUS registers from the remote station.

Write: Used for writing MODBUS registers to the remote station.

Write Single: Used for writing a single MODBUS register to the remote station.

Note: Only an option when writing a singe discrete output or single analog output.

Read/Write: Used for reading a single MODBUS register from the remote station, unless a local IODB change to the same register has been detected. In that case, the local IODB change takes priority and is written to the remote station.

Local Type: Local Station I/O type. See Table2 - I/O Types and Limits.

Local Relative Address (Required): First address of the local I/O used for the I/O transfer. Valid values are 1 through a value of defined registers configured for specified I/O type. The address ranges are displayed on I/O Transfer screen under 'Display of Modbus Default Slave Addresses' based on configured local register allocation for specified I/O type.

Remote Type: I/O type on the remote station. See Table2, 3, 4 - I/O Types and Limits.

Note: If modbus WRITE operation is selected, this field should be limited to output register types.

Remote Address: First register address for the remote I/O used for the I/O transfer. Valid values are 1 - 65536.

Number of Registers (Required): Number of registers requested in the I/O transfer. This must be 1, if the WRITE_SINGLE command is selected. See Table 2, 3, 4 - I/O Types and Limits.

Note: Number of Registers must be 1, if WRITE_SINGLE command is selected.

Create Tags for Range: Create a tag for each local IODB register with custom prefix: IOXF_[Type][Address]

Warning: Tags will OVERWRITE any existing tags applied to these registers.

Enter Update Interval (ms) (Required): Time interval, in milliseconds, for the I/O transfer. The recommended value for this field is 500ms or higher.

Scan Enable Type: I/O Type used for controlling and I/O transfer using either a discrete input or discrete output register. Valid options are **DI** or **DO** or **Blank** if not used.

Scan Enable Address: The address of the discrete register used to control an I/O transfer. Valid values are 0 through number of registers configured for specified I/O type. **Blank** if not used.

Data Manipulation: Used to make register level conversions to the order of the byte, word or endian orientation:

None: No manipulation will occur to the data being transfered.

Reverse Bytes: Individual bytes in each register will be swapped from MSB to LSB. Only available for 16-bit registers and higher.

Example BA -> AB, DCBA -> ABCD

Reverse Words: Individual Words in each register will be swapped from MSB to LSW. Only available for 32-bit registers.

Example DCBA -> BADC

Endian Swap: The entire register range contents as a whole will be reordered from Most Significant to Least Significant.

Example DCBA -> CDAB

Click on the *Finish* button to populate the I/O Transfer Table Properties. If more stations are needed, click on the *Add* button and enter the required field for each station.

To edit a *Remote* Station, select the station in the table and click on the edit button. To delete an existing station, select the station in the table and click on the *Delete* button.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

Table 1: I/O Types and Limits for Read Commands

I/O Type		Number of regs supported in I/O transfer
Discrete Input	DI	2000
Discrete Output	DO	2000
Analog Input	AI	125
Analog Output	AO	125
Float Input	FI	62
Float Output	FO	62
Long Input	LI	62
Long Output	LO	62

Table 2: I/O Types and Limits for Write Commands

I/O Type		Number of regs supported in I/O transfer
Discrete Input	DI	1968
Discrete Output	DO	1968
Analog Input	AI	123
Analog Output	AO	123
Float Input	FI	61
Float Output	FO	61
Long Input	LI	61
Long Output	LO	61

Table 3: Valid Type Combinations for READ I/O Xfers

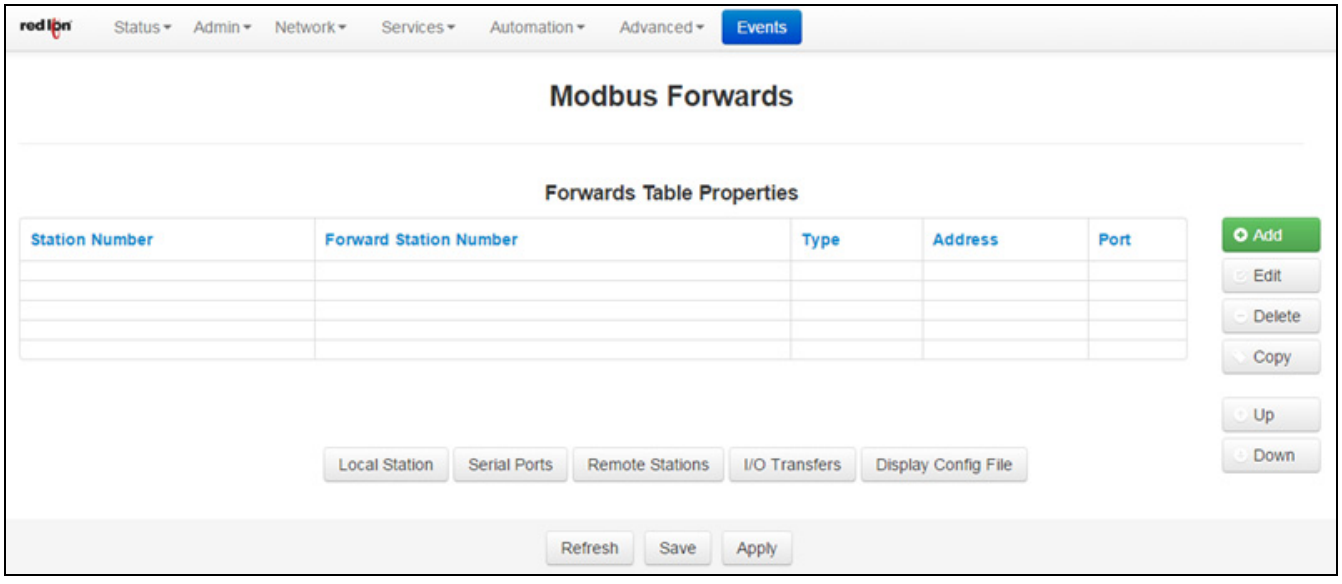
Local Type	Valid Remote Type
DI	DI | DO
DO	DI | DO
AI	AI | AO
AO	AI | AO
FI	FI | FO
FO	FI | FO
LI	LI | LO
LO	LI | LO

Table 4: Valid Type Combinations for WRITE I/O Xfers

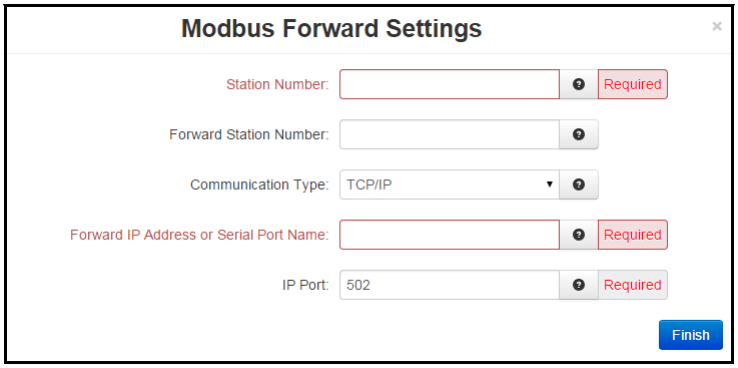
Local Type	Valid Remote Type
DI	DO
DO	DO
AI	AO
AO	AO
FI	FO
FI	FO
LI	LO
LO	LO

Forwards

Click on the *Forwarding* menu item and the following dialog window appears:



Click on the *Add* button to configure the Forwarding and the following pop-up window appears:



Station Number (Required): Station number to be forwarded. Valid values are 1 - 247.

Forward Station Number: If supplied, replaces the station number in the request with this value. Valid values are 1 - 247.

Communication Type: Select the forwarding method. Valid options are **TCP/IP**, **UDP/IP** or **Serial** (Serial type can be set in next dialog).

Forward IP Address or Serial Port Name (Required): The address to forward the modbus request if forwarding on with IP, or the serial device name if forwarding the request on the serial port.

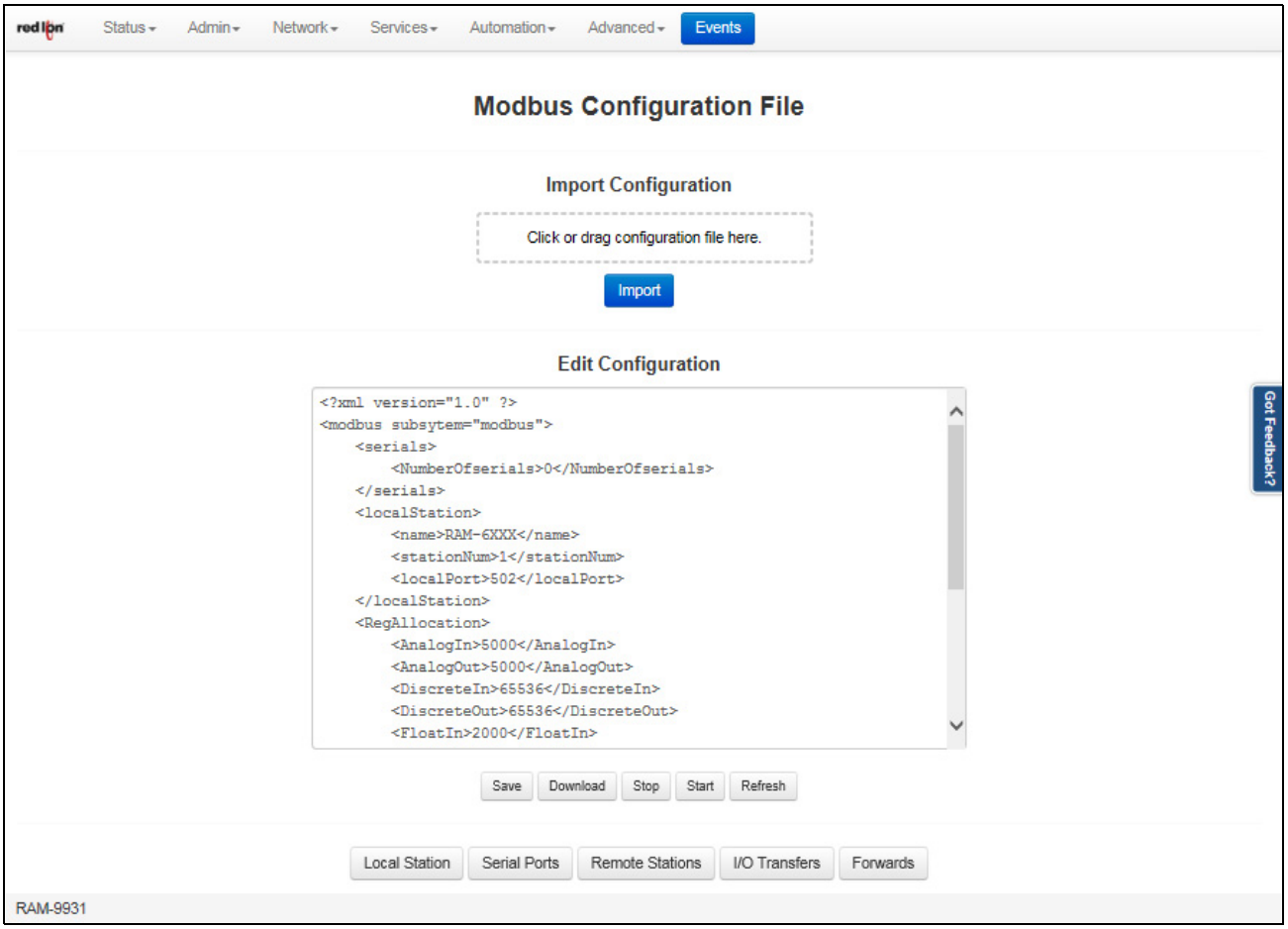
IP Port (Required): Enter a valid port number (1-65535) to be used to forward the request to on the remote station. It is recommended that a port number not already used by other system services is chosen. Consult **Status→ Network→Socket Statuses→TCP Only** for a list of ports currently in use. Please note that a Firewall Allow rule will need to be added for remote access. (**Network→Firewall→Port Allow/Forwarding Rules→Service Access Rules**).

Click on the *Finish* button to populate the Forwarding Table screen. If more than one forward is needed, click and repeat the *Add* button.

Click on the *Save* button to save the Forwarding configuration in the modbus.xml file. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

Display Config File

Click on the *Display Config File* menu item and the Modbus Configuration File dialog window appears.



Import Configuration: This option allows you to import a configuration file to replace your existing Modbus configuration file. Click to browse for your configuration file or drag and drop into the dashed upload box to select your Modbus.xml configuration file on your PC, then click on the Upload button and once the upload is successful, click on the Import button to replace your existing Modbus.xml configuration file.

Configure Modbus Configuration File: This option will load the Modbus configuration file into the text box for editing. The available controls (buttons) are as follows:

Save - Save the contents of the text box in to the Modbus configuration file.

Stop - Stop the Modbus service, if it is currently running.

Start - Stop the Modbus service, if it is currently running and start them back up.

Refresh - Reload the Modbus configuration file into the text box.

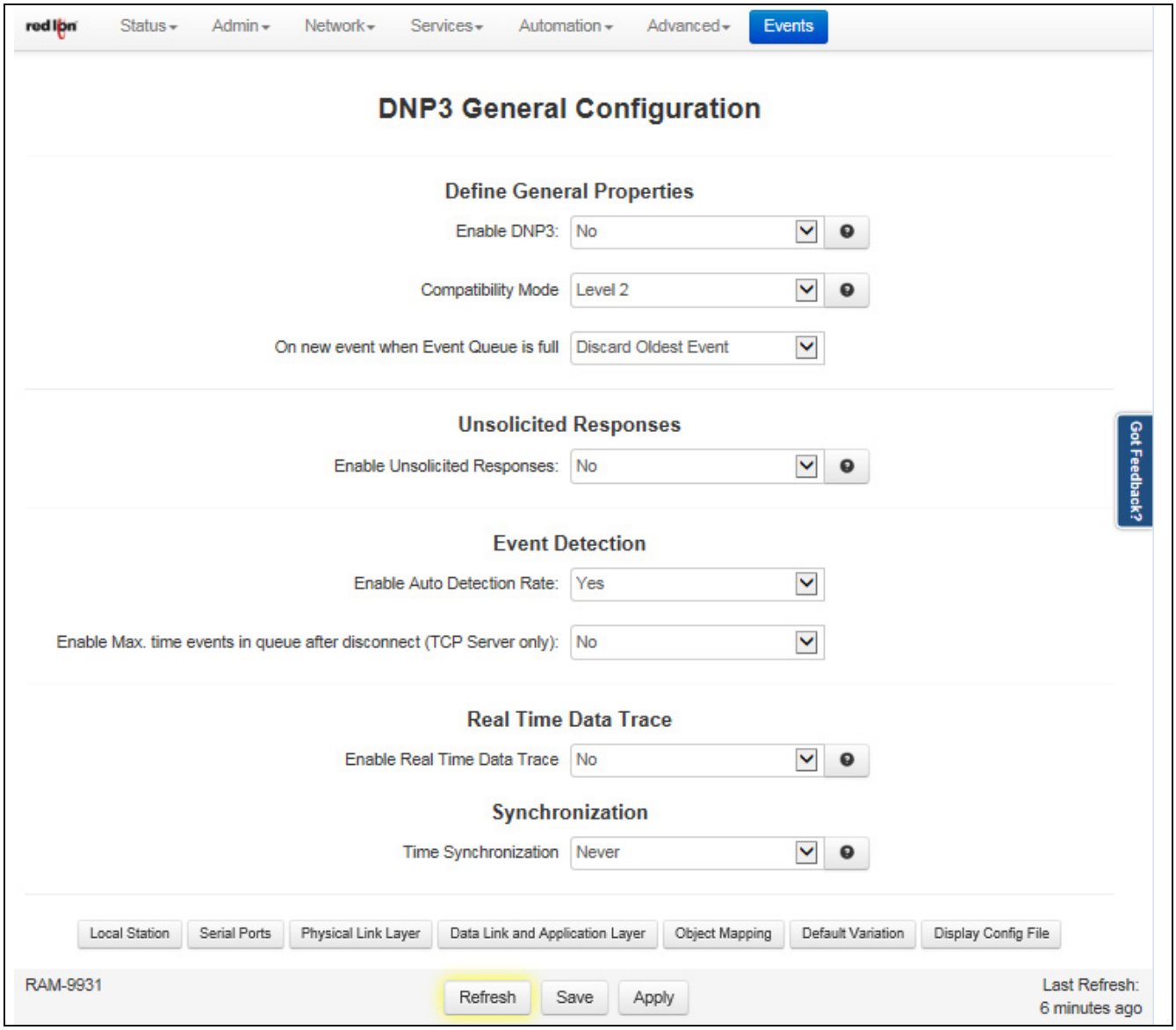
Download - Download the current Modbus configuration file to your PC as **"**modbus.xml.txt**"**.

3.6.6 DNP3

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies. Usage in other industries is not common. It was developed for communications between various types of data acquisition and control equipment.

General

Click on the DNP3→General menu option and the following screen appears:



Define General Properties

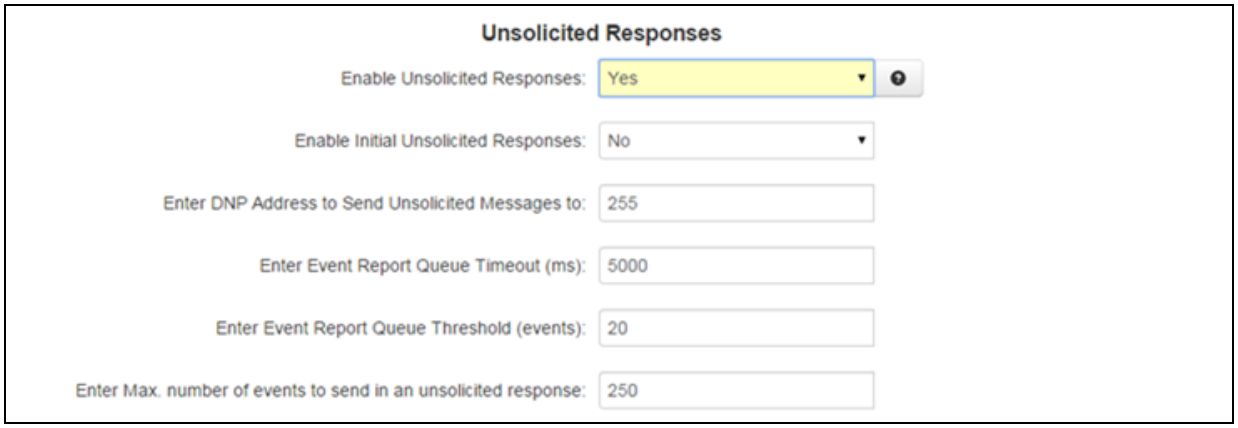
Enable DNP3: Select Yes to enable DNP3.

Compatibility Mode: The DNP3 Slave driver can work under two(2) modes: Level 2 or Level 2+.

On new event when Event Queue is full: Select whether to discard the oldest or newest message when log is full.

Unsolicited Responses

Enable Unsolicited Responses: Select if the DNP3 Slave should send unsolicited messages to the DNP3 Master. If this selection is checked, then the user should also configure the following:



Enter DNP3 Address to Send Unsolicited Messages to: The address of the station to which DNP3 Slave will send unsolicited messages in the DNP3 Address to Send Unsolicited Messages field.

Enable Initial Unsolicited Responses: Enter Yes to enable.

Enter Event Report Queue Timeout (ms): The amount of time in milliseconds any event will be allowed to remain in the event queue before being reported in the Event Report Queue Timeout field. Minimum value: 1,000 ms (1 second), maximum value: 3,600,000 ms (1 hour).

Enter Event Report Queue Threshold (events): The minimum number of events in the event queue required to trigger the generation of an unsolicited even report message in the Event Report Queue Threshold field.

Enter Max. number of events to send in an unsolicited response: The maximum number of events to send in every unsolicited message.

Note: When planning on using unsolicited responses, there must be at least one DNP3 object configured to generate events on any of the three DNP3 event classes, or else, no events will be generated and thus no unsolicited responses at all will be generated by the station.

Event Detection / Real Time Data Trace / Synchronization

Enable Auto Detection Rate: Check this box to automatically set the detection rate.

Enable Max. time events in queue after disconnect (TCP Server only): Click to enable.

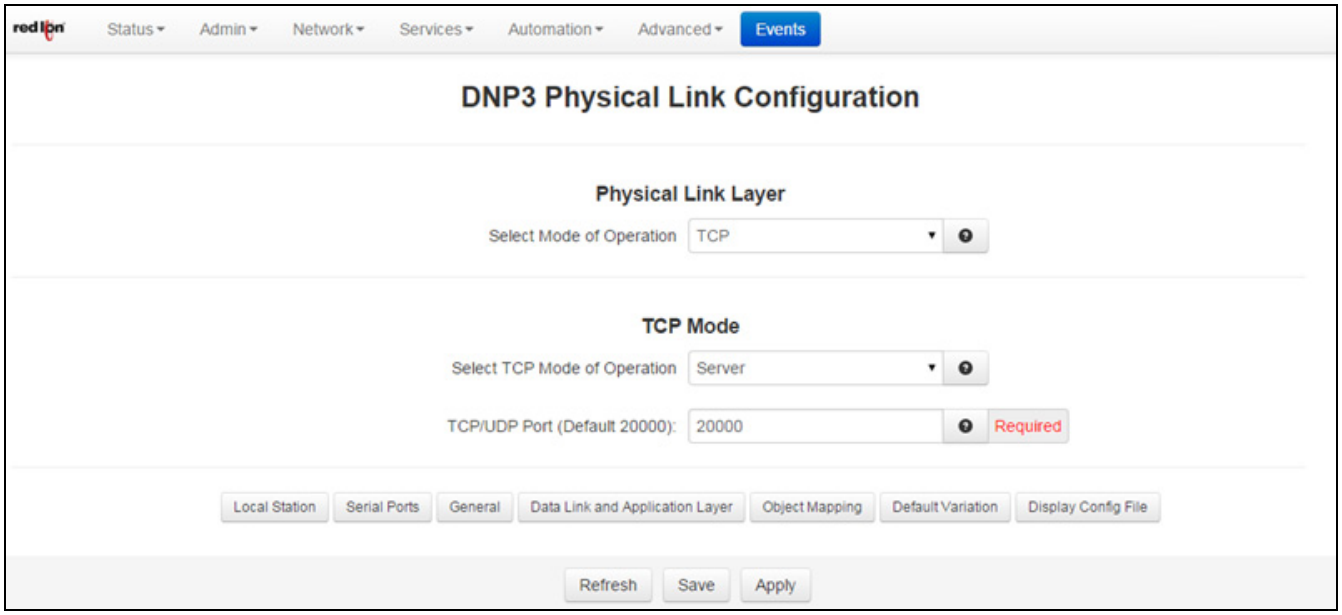
Enable Real Time Data Trace: The DNP3 Slave Driver can be configured to generate real time traces of every Master-Slave DNP3 transaction for diagnosis and debugging purposes. The real time communication data traces can be enabled/disabled at any time. The output will be directed to a text file within the file system for later upload. When your trace scenario is complete, simply run a gatherstats to automatically include this DNP3 trace. Then contact Support with your results.

Time Synchronization: The station can be configured to request Time Synchronization from the DNP3 Master. Requests can be configured to be made at intervals of once per minute, once per hour, once per day or never.

Click on the *Save* button to save your configuration. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

(Navigation buttons across the bottom of the DNP3 screen match the selections made from the drop down tab menu.)

Physical Link Layer



Select Mode of Operation: The DNP3 Slave Driver implementation supports RS-232 and RS-485 (two and four wires) over serial port communications as well as TCP/IP and UDP/IP over LAN/WAN communications. When the user selects the Serial Mode, the TCP/UDP section is disabled. The same happens to the Serial section if the Mode of Operation selected is TCP or UDP.

Serial: This section groups all the parameters needed to establish serial communication. When you select this option, the following options appear in the dialog window:

Serial Port: Select serial port device name from provided drop-down list for serial connection. Options are: ttyS1(RS232) and ttyS5 (RS485).

Enable Collision Avoidance: The DNP3 Slave Driver can be configured to enable or disable collision avoidance. The collision avoidance method implemented is Detection of Transmitted Data with a random pre-transmission back-off time, as recommended by the DNP3 Technical Bulletin 9804-007.

TCP: This section is enabled when the Mode of Operation selected is TCP. The parameters to be configured are:

Select TCP Mode of Operation: DNP3 slave driver can operate as Server or Client Mode. In Client Mode the user has to set TCP Host field, it is used to enter the name of the Host IP Address.

TCP/UDP Port: Enter the port number where the communication will be established. By default this value is 20,000. This parameter is used in both TCP and UDP protocol.

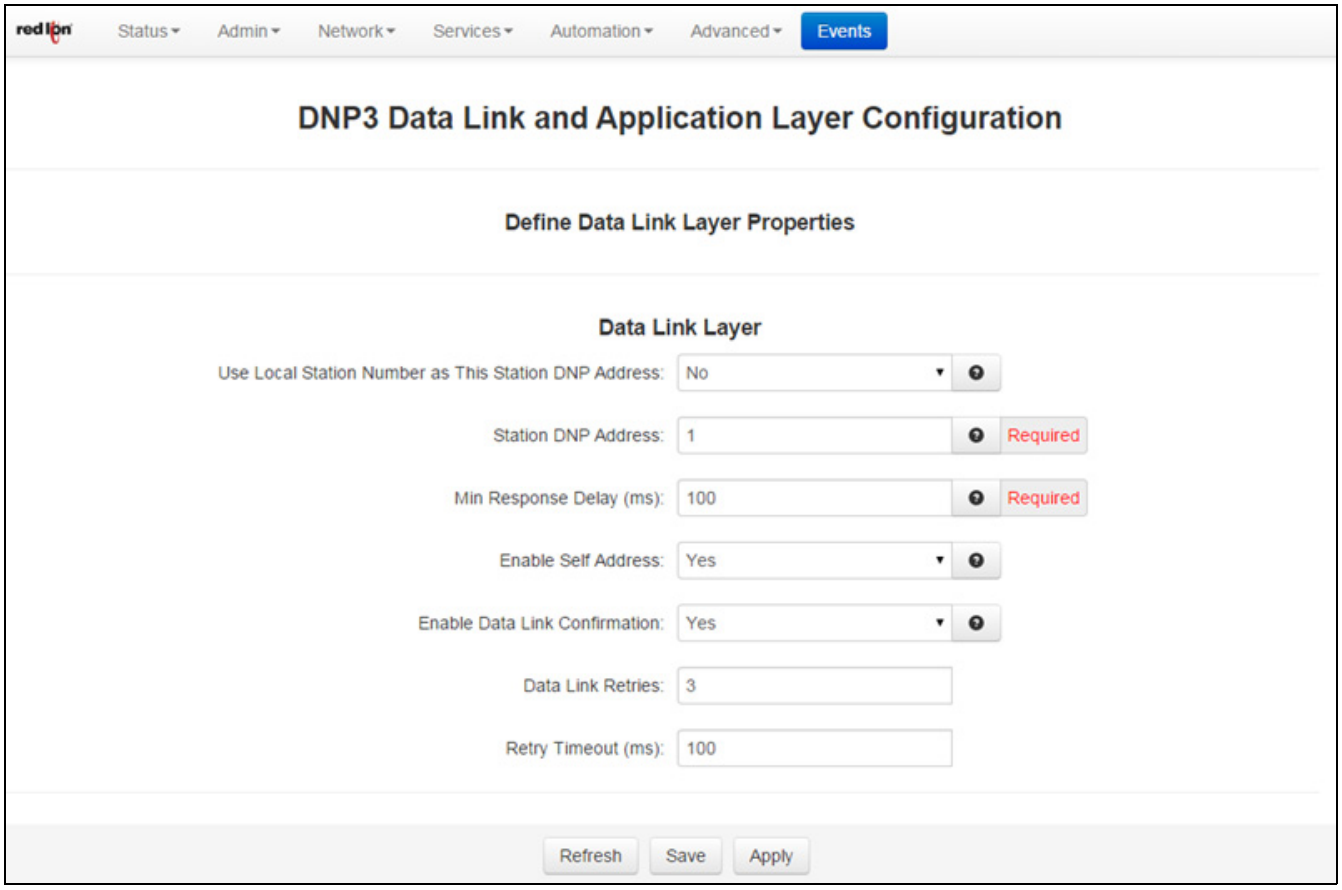
UDP: This section is enabled when the Mode of Operation is set to UDP. The parameters to be configured are:

TCP/UDP Port: Enter the port number where the communication will be established. By default this value is 20,000. This parameter is used in both TCP and UDP protocol.

UDP Host Destination Address to Send Unsolicited Messages: Host Address to which unsolicited messages will be sent when working in UDP mode.

Click on the *Save* button to save your configuration. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

Data Link and Application Layer



Use Local Station Number as This Station DNP3 Address: DNP3 address for the slave. This value can be set by the user or automatically assigned by the Add-On. If the check box Same As station Number is selected, then the DNP3 Address will be equal to the Station Number.

Data Link Layer

Enter Station DNP3 Address (Required): Enter the address for this Station if not being automatically assigned.

Min Response Delay (ms) (Required): This is the time delay in milliseconds (from 0 to 65535 msec) before sending the response from the slave.

Enable Self Address: The DNP3 Slave Driver can be configured to send its own DNP3 Address when a DNP3 Master asks for it. When this box is checked, if a message is sent with the Self Address (65532) in the destination address field, the will respond with its unique individual address. This feature simplifies the commissioning, troubleshooting and maintenance of devices with an unknown address. If this feature is not enabled, the station will ignore the messages sent to the Self Address.

Enable Data Link Confirmation: The DNP3 Slave Driver can be configured to retry unconfirmed data link primary frames. The number of retries the driver sends and the retry timeout are configurable.

This service is disabled unless Data Link Confirmation option is set to Yes.

Data Link Retries: The number of Retries is configurable between 0 (Data Link Retries disabled) and 255.

Retry Timeout (ms): The Retry Timeout is configurable between 0 (Data Link Retries disabled) and 5000ms

Note: The Driver's Data Link Layer will attempt to retry (will resend) an unconfirmed data link primary frame when the confirmation has not been received within the configured timeout. If the confirmation fails to arrive after the configured number of retries, the communications link is considered failed and a reset sequence is required before a new primary frame could be sent.

Application Layer

Enable Application Layer Confirmation: The DNP3 Slave Driver can be configured to retry unconfirmed application link primary frames. The number of retries the driver sends and the retry timeout are configurable. This service is disabled unless Application Link Confirmations check box is selected.

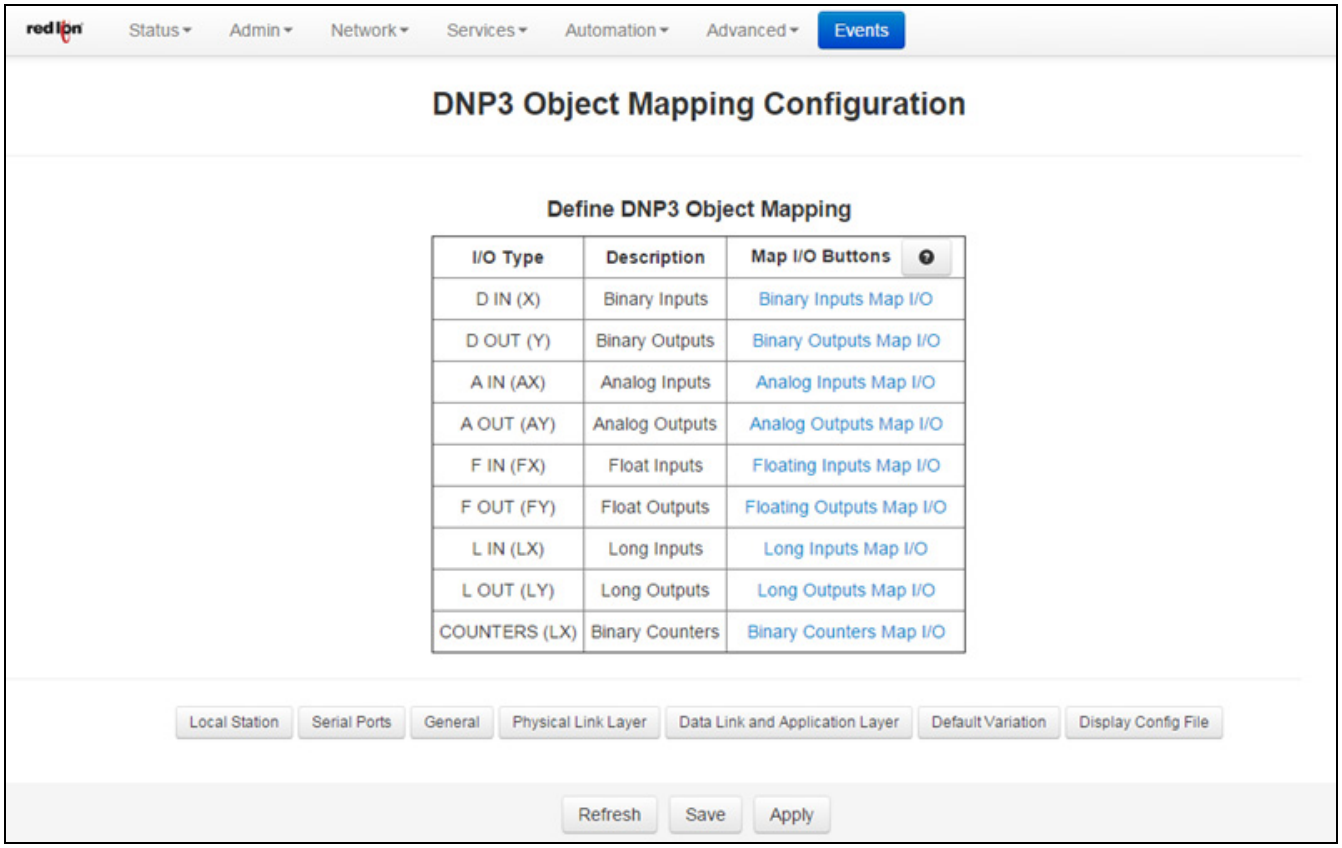
Application Layer Retries: The number of Retries is configurable between 0 (Application Link Retries disabled) and 255.

Application Layer Timeout (ms): The Retry Timeout is configurable between 0 (Application Link Retries disabled) and 5,000ms

Use different SEQ numbers for CONFIRM and RESPONSE: Check to enable.

Click on the *Save* button to save your configuration. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

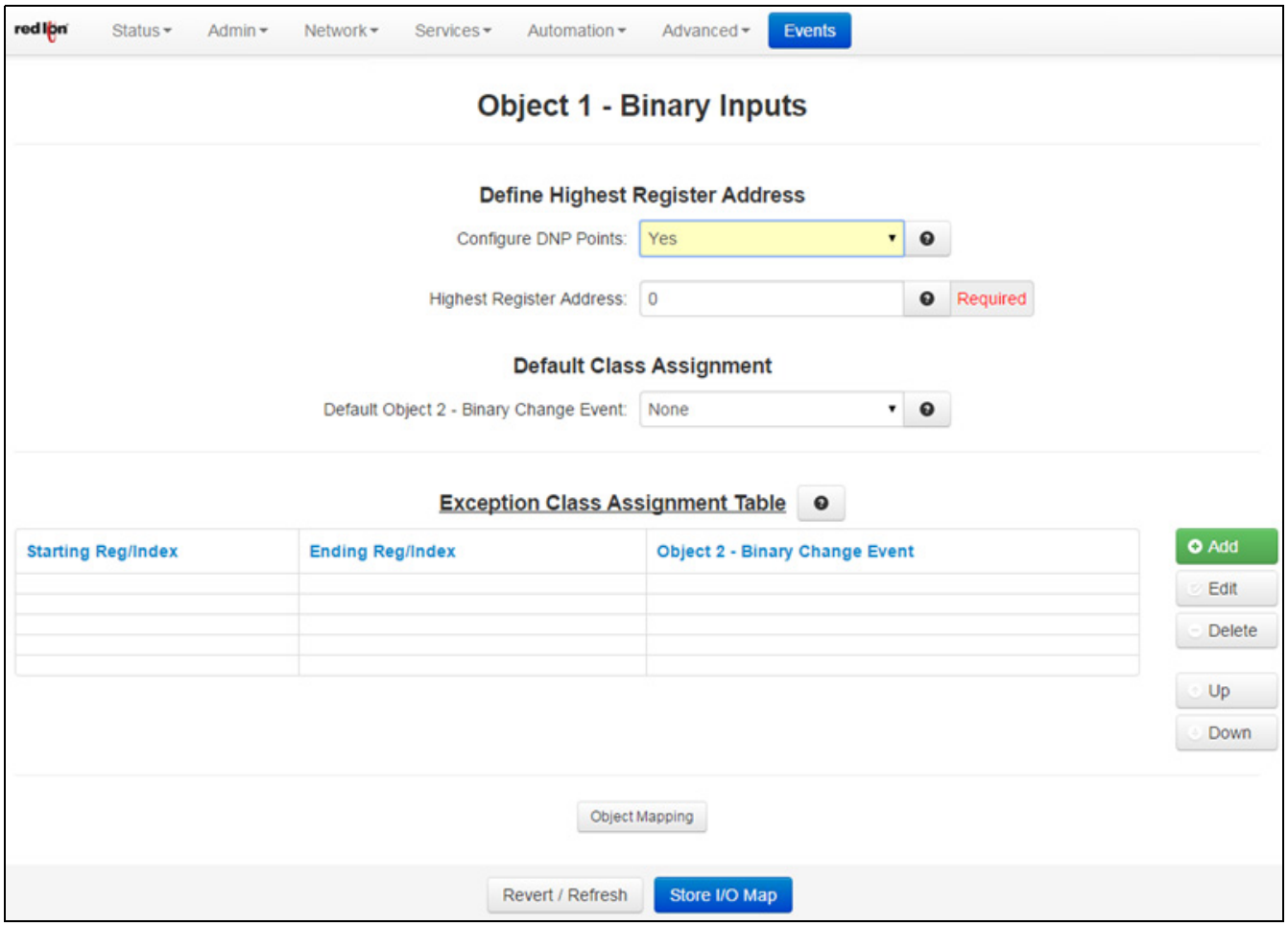
Object Mapping



Object Mapping: When clicking on each link a dialog window appears. The dialog window is used to configure and map every DNP3 point to a specific I/O. ***Note:*** *Each type of I/O must have its corresponding Object Mapping Window opened at least once, or else the I/O won't be mapped.*

Binary Inputs Map I/O: This section provides configuration of Mapping Binary Input I/O's Reg/Index to DNP3 points for generating events based on configured Class Assignments when the status of any Binary Input I/O's changes.

Default Class Assignments are applied to all the Reg/Index defined by Highest Register Address except Reg/Index entries that are defined in Exception Class Assignments Table.



Configure DNP3 Points: If option is No, then no Binary Inputs is mapped as DNP3 points.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP3 points. If Configure DNP3 Points option is set to Yes, the Highest Register Address field is displayed to enter a Highest Register Address value.

Default Object 2 - Binary Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, 2 or 3), otherwise it should be associated to None. By default all DNP3 points do not generate events, this feature should be modified by the user.

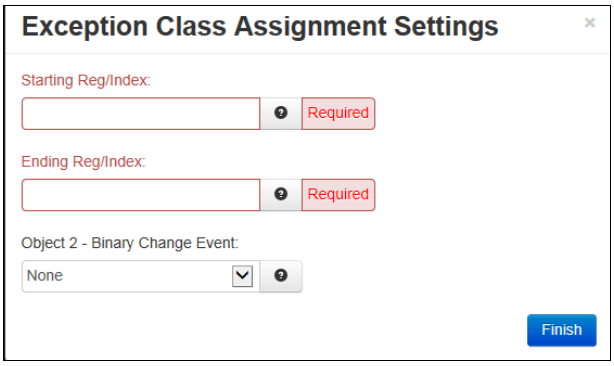
Exception Class Assignment Table: The Exception table provides you with the ability to define Reg/Index ranges that are needed to be configured differently than Default Class Assignments.

Example: If the Highest Register Address is set to 10 and Reg/Index 2, 4, 6-7 are needed to be set for different class assignments than default, then the final result for all 10 registers would be as follows:

- Reg/Index 0-1, 3, 5 and 8-10 will be set to Default Class Assignments.
- Reg/Index 2, 4 and 6-7 will be set to Exception Class Assignments.

Note: The order of table entry ranges must be entered from lowest Reg/Index to highest Reg/Index, otherwise the Web UI will alert the end user for incorrect range entries. The starting Reg/Index and Ending Reg/Index of Exception table entries for a single Reg/Index such as Reg/Index 2 and 4 in above example has to be the same address. The maximum suggested entries for the exception table are 10-15 entries.

Click the *Add* button to define an Exclusion range.



Starting Reg/Index (Required): Enter the Starting Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be less than or equal to Ending Register.

Ending Register (Required): Enter the Ending Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be greater than or equal to Starting Register.

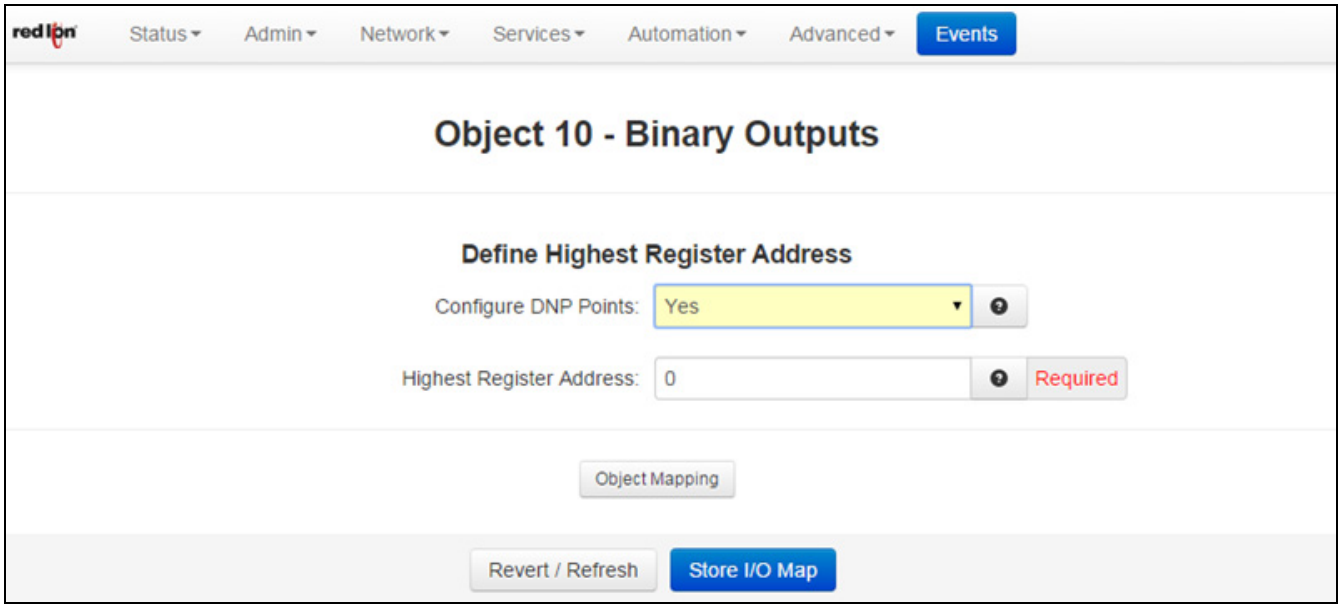
Object 2 - Binary Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't generate events, this feature should be modified by the user.

Click *Finish* to enter your exclusion into the table.

To edit an entry, select the station in the table and click on the *Edit* button. To delete an existing entry, select the station in the table and click on the *Delete* button.

Click on *Store I/O Mapping* to save your configuration before moving to the next project. Click on the *Object Mapping* button to return to the DNP3 Object Mapping Configuration dialog window.

Binary Outputs Map I/O



Configure DNP3 Points: If option is No, then no Binary Outputs are mapped as DNP3 points.

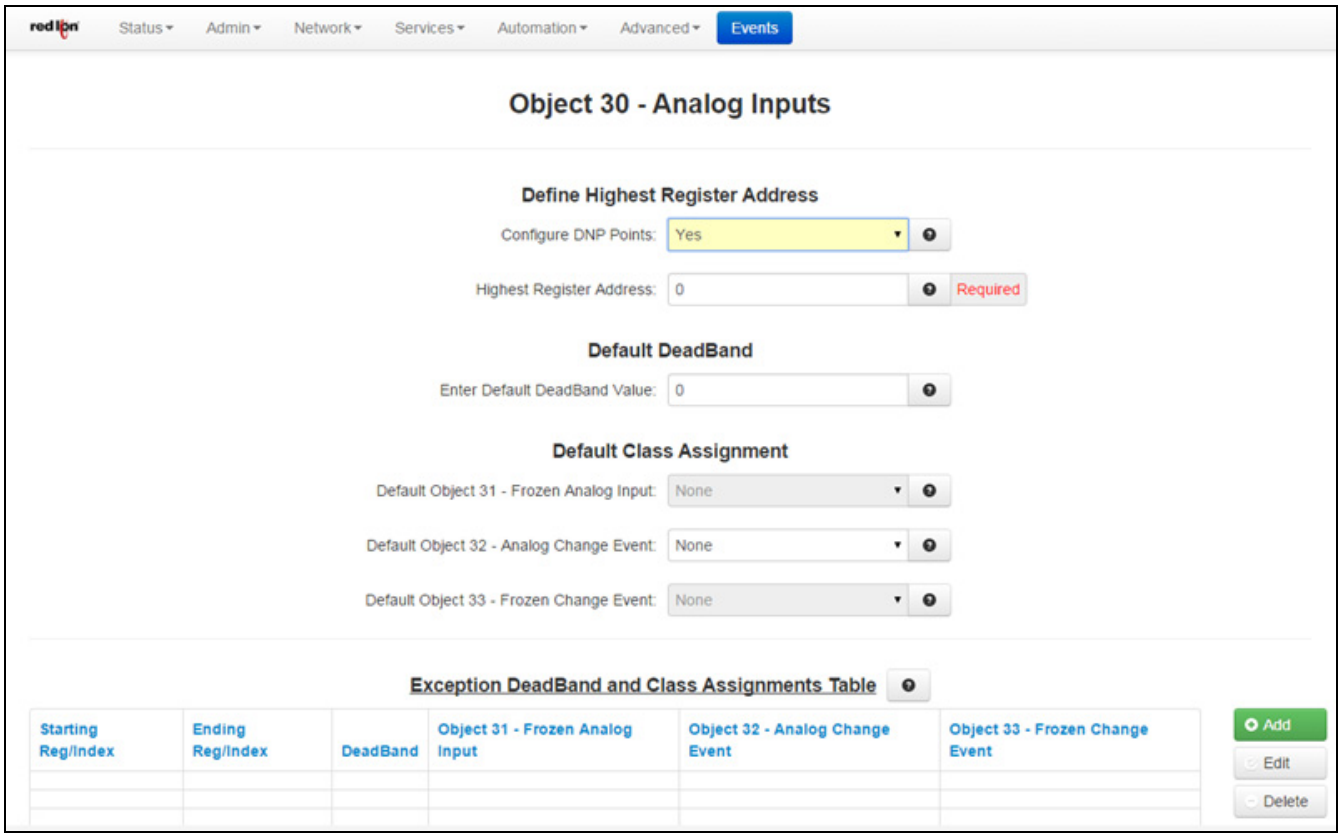
Highest Register Address (Required): This field is used to show or set the highest register address to map DNP3 points. If Configure DNP3 Points option is set to Yes, the Highest Register Address field is shown to enter a Highest Register Address value.

Click on *Store I/O Mapping* to save your configuration before moving to the next project. Click on the *Object Mapping* button to return to the DNP3 Object Mapping Configuration dialog window.

Analog Inputs Map I/O

This section provides configuration of Mapping Analog Input I/O's Reg/Index to DNP3 points for generating events based on configured DeadBand and Class Assignments when the status of any Analog Input I/O's changes.

Default DeadBand and Class Assignments are applied to all the Reg/Index defined by Highest Register Address except Reg/Index entries that are defined in Exception DeadBand and Class Assignments Table.



Define Highest Register Address

Configure DNP3 Points: If option is set to No, then no Analog Inputs are mapped as DNP3 points. If set to Yes, the Highest Register Address field is shown to enter a Highest Register Address value.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP3 points.

Default Deadband

Enter Default Deadband Value: Values outside this deadband generate events. The deadband parameter sets how even data is generated by your module as a DNP3 slave device.

For example, the Analog Input deadband being set to a value of 1000 will report all of the points as being class 3 data (as set by the “Analog Input Class” parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input deadband can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

Default Class Assignment

Default Object 31 - Frozen Analog Input: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don’t generate events, this feature should be modified by the user.

Default Object 32 - Analog Change Event: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object2 Binary

Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't generate events, this feature should be modified by the user.

Default Object 33 - Frozen Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't generate events, this feature should be modified by the user.

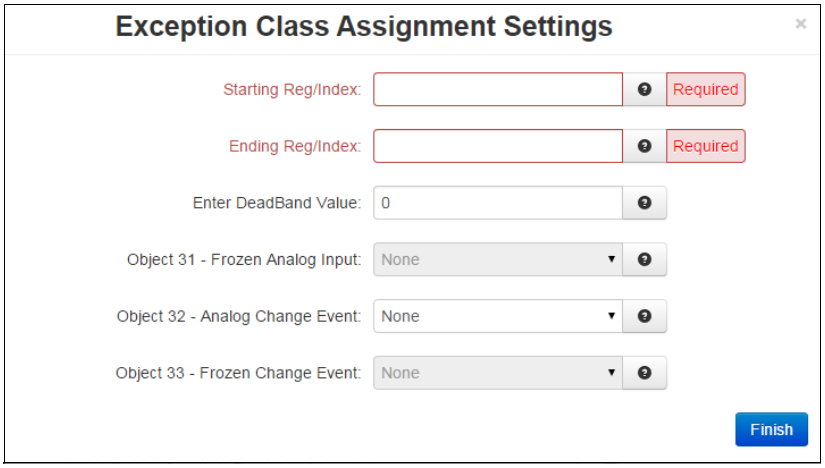
Exception DeadBand and Class Assignments Table: The Exception table provides the ability to define Reg/Index ranges that are needed to be configured differently than Default DeadBand and Class Assignments.

Example: If the Highest Register Address is set to 10 and Reg/Index 2, 4 6-7 are needed to be set for different DeadBand and Class Assignments than Default, then the final result for all 10 registers would be as follows:

- Reg/Index 0-1, 3, 5 and 8-10 will be set to Default DeadBand and Class Assignments.
- Reg/Index 2, 4 and 6-7 will be set to Exception DeadBand and Class Assignments.

Note: The Starting Reg/Index and Ending Reg/Index of Exception table entries for a single Reg/Index such as Reg/Index 2 and 4 in above example has to be the same address.

Click the *Add* button and the following dialog window appears:



Starting Reg/Index (Required): Enter the Starting Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be less than or equal to Ending Register.

Ending Reg/Index (Required): Enter the Ending Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be greater than or equal to Starting Registers.

Enter DeadBand Value (Required): Values outside this deadband generate events. The deadband parameter sets how event data is generated by your modules as a DNP3 slave device.

For example: The Analog Input deadband being set to a value of 1000 will report all of the points as being class 3 data (as set by the "Analog Input class" parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input deadband can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

Object 31 - Frozen Analog Input: This field is activated on both levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't generate events, this feature should be modified by the user.

Object 32 - Analog Change Event: This field is activated on both levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't generate events, this feature should be modified by the user.

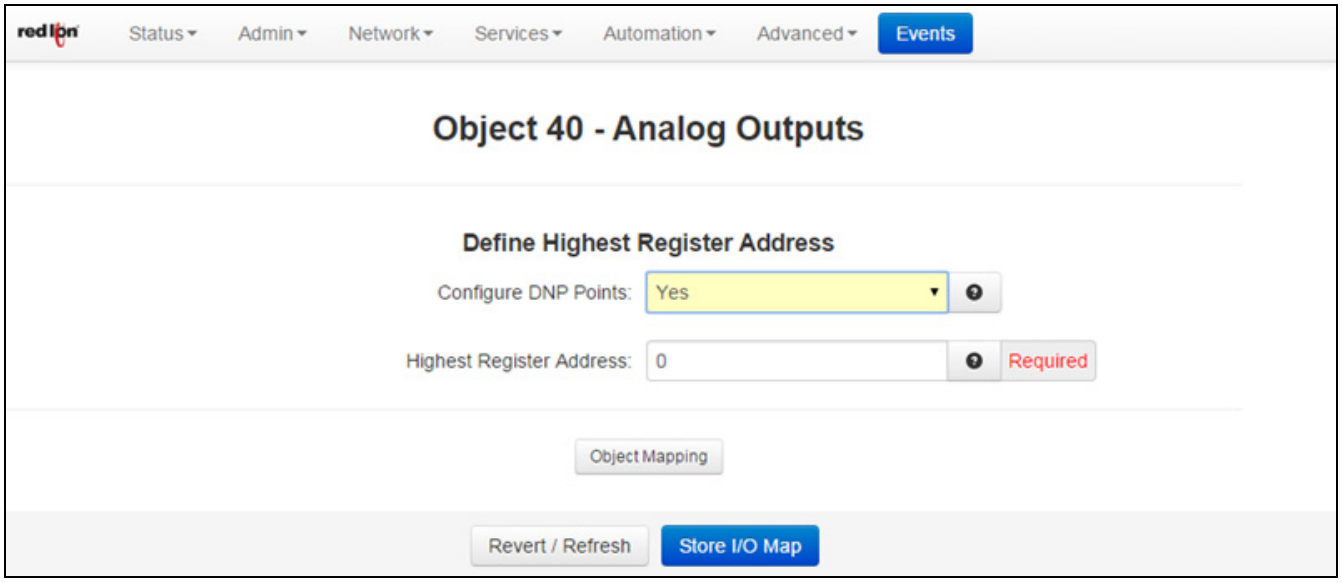
Object 33 - Frozen Change Event: This field is activated on both levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't generate events, this feature should be modified by the user.

Click *Finish* to enter your exception into the table.

To edit an entry, select the station in the table and click on the *Edit* button. To delete an existing entry, select the station in the table and click on the *Delete* button.

Click on *Store I/O Mapping* to save your configuration before moving to the next project. Click on the *Object Mapping* button to return to the DNP3 Object Mapping Configuration dialog window.

Analog Outputs Map I/O



Configure DNP3 Points: If No is selected, then no Analog Outputs are mapped as DNP3 points. If set to Yes, the Highest Register Address field is displayed.

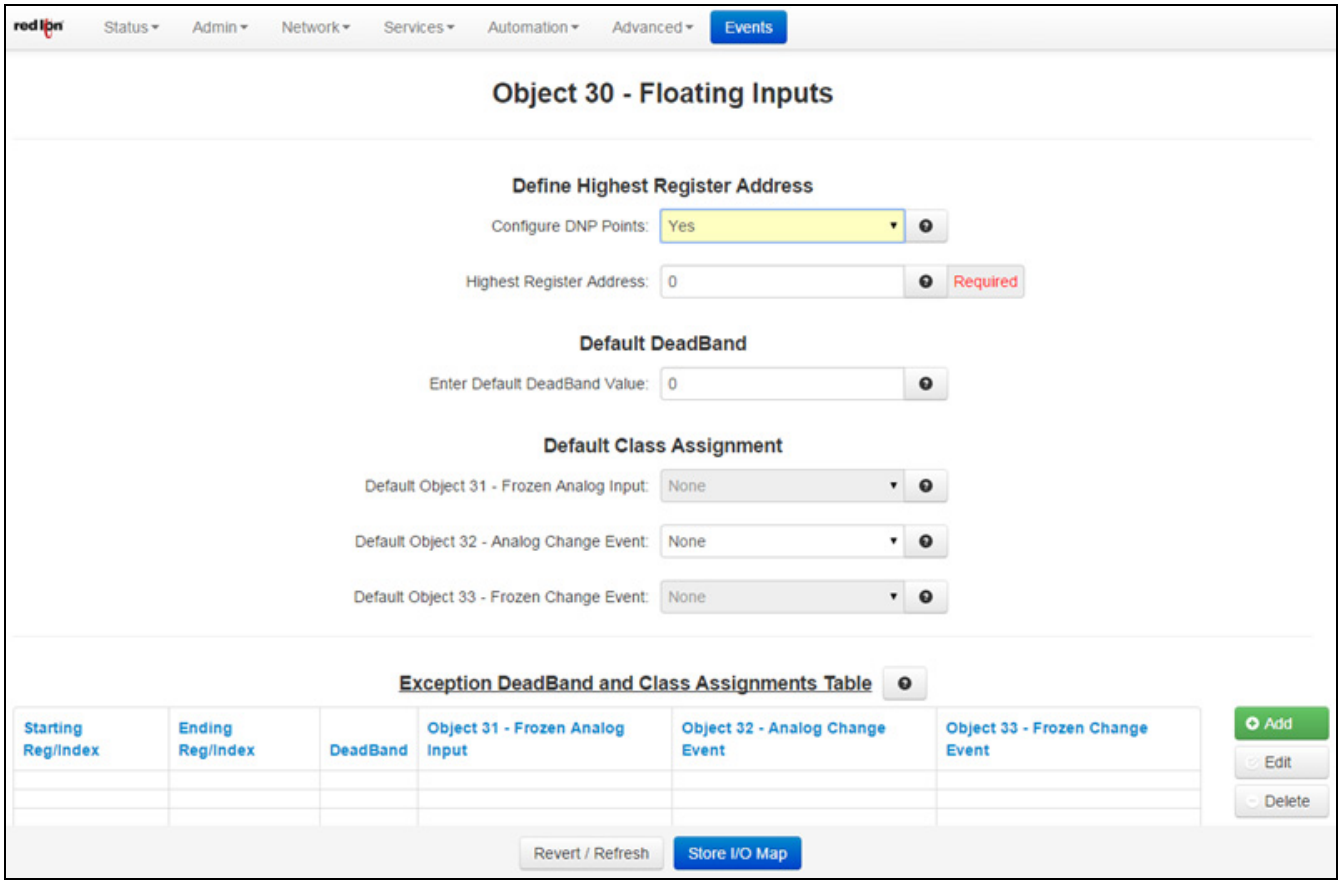
Highest Register Address (Required): This field is used to show or set the highest register address to map DNP3 points.

Click on Store I/O Mapping to save your configuration before moving to the next project. Click on the Object Mapping button to return to the DNP3 Object Mapping Configuration dialog window.

Floating Inputs Map I/O

This option provides configuration of Mapping Float Input I/O's Reg/Index to DNP3 points for generating events based on configured DeadBand and Class Assignments when the status of any Float Input I/O's changes.

Default DeadBand and Class Assignments are applied to all the Reg/Index defined by Highest Register Address except Reg/Index entries that are defined in Exception DeadBand and Class Assignments Table.



Define Highest Register Address

Configure DNP3 Points: If option is set to No, then no Floating Inputs are mapped as DNP3 points. If set to Yes, the Highest Register Address field is shown to enter a Highest Register Address value.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP3 points.

Default Deadband

Enter Default DeadBand Value: Values outside this deadband generate events. The deadband parameter sets how event data is generated by your module as a DNP3 slave device.

For example: The Analog Input deadband being set to a value of 1000 will report all of the points as being class 3 data (as set by the “Analog Input class” parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input deadband can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

Default Class Assignment

Default Object 31 - Frozen Analog Input: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don’t generate events, this feature should be modified by the user.

Default Object 32 - Analog Change Event: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be

associated to None. By default all DNP3 Points don't generate events, this feature should be modified by the user.

Default Object 33 - Frozen Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't generate events, this feature should be modified by the user.

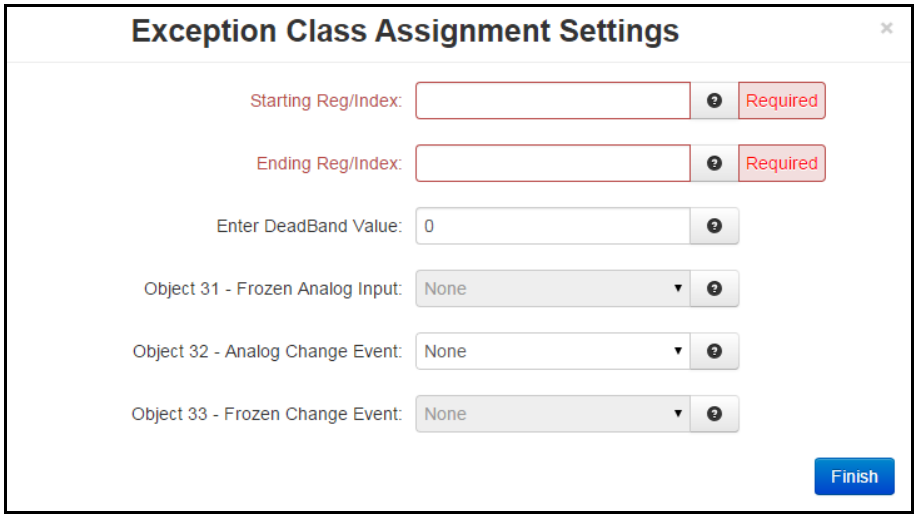
Exception DeadBand and Class Assignment Table: The Exception table provides you with the ability to define Reg/Index ranges that are needed to be configured different than Default DeadBand and Class Assignments.

Example: If the Highest Register Address is set to 10 and Reg/Index 2, 4, 6-7 are needed to be set for different DeadBand and Class Assignments than Default, then the final result for all 10 registers would be as follows:

- Reg/Index 0-1, 3, 5 and 8-10 will be set to Default DeadBand and Class Assignments.
- Reg/Index 2, 4 and 6-7 will be set to Exception DeadBand and Class Assignments.

Note: The Starting Reg/Index and Ending Reg/Index of Exception table entries for a single Reg/Index such as Reg/Index 2 and 4 in above example has to be the same address.

Click the *Add* button and the following dialog window appears:



Starting Reg/Index (Required): Enter the Starting Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be less than or equal to Ending Register.

Ending Reg/Index (Required): Enter the Ending Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be less than or equal to Starting Register.

Enter DeadBand Value (Required): Values outside this DeadBand generate events.

For example: The Analog Input DeadBand being set to a value of 1000 will report all of the points as being class 3 data (as set by the "Analog Input class" parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input deadband can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

Object 31 - Frozen Analog Input: This field is activate by both Levels 2 and 2+. It's used to determine if a DNP3 point will generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't generate events, this feature should be modified by the user.

Object 32 - Analog Change Event: This field is activate by both Levels 2 and 2+. It's used to determine if a DNP3 point will generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't generate events, this feature should be modified by the user.

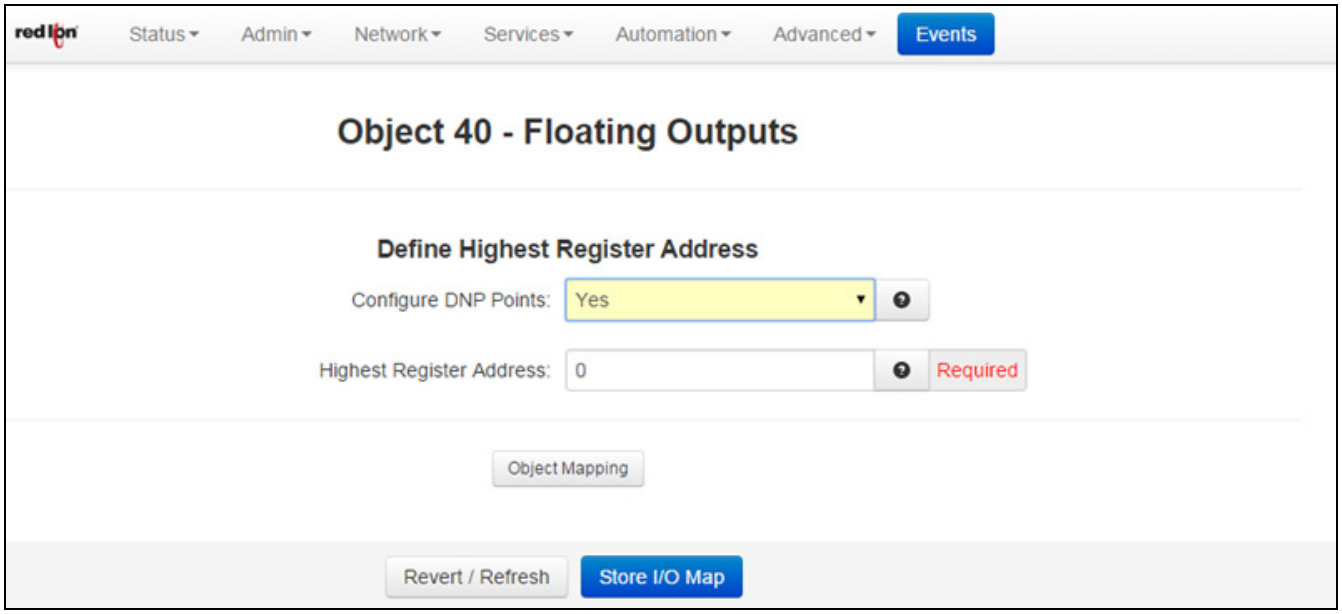
Object 33 - Frozen Change Event: This field is activate by both Levels 2 and 2+. It's used to determine if a DNP3 point will generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't generate events, this feature should be modified by the user.

Click *Finish* to enter your exception into the table.

To edit an entry, select the station in the table and click on the *Edit* button. To delete an existing entry, select the station in the table and click on the *Delete* button.

Click on *Store I/O Mapping* to save your configuration before moving to the next project. Click on the *Object Mapping* button to return to the DNP3 Object Mapping Configuration dialog window.

Floating Outputs Map I/O



Configure DNP3 Points: If No is selected, then no Analog Outputs are mapped as DNP3 points. If set to Yes, the Highest Register Address field is activated.

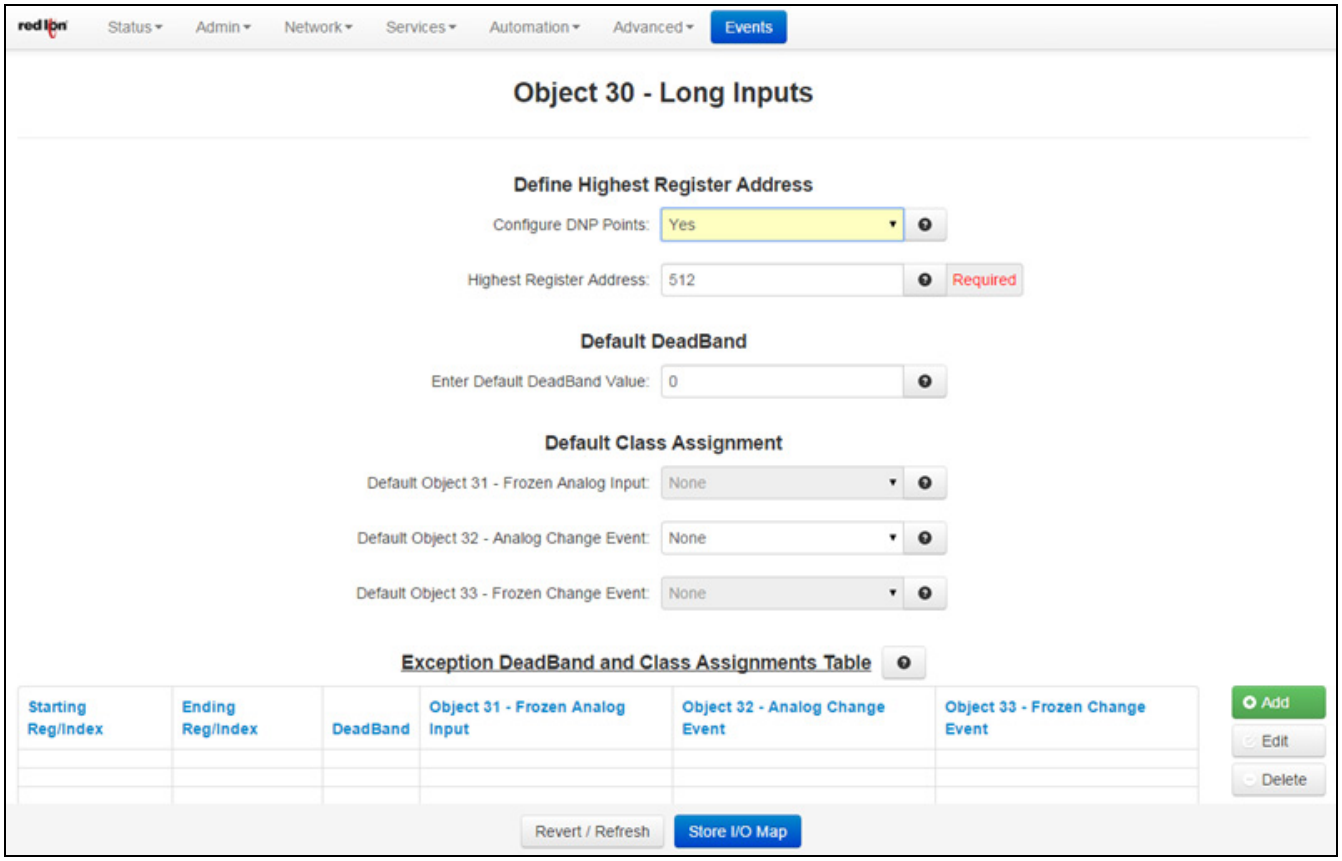
Highest Register Address (Required): This field is used to show or set the highest register address to map DNP3 points.

Click on *Store I/O Mapping* to save your configuration before moving to the next project. Click on the *Object Mapping* button to return to the DNP3 Object Mapping Configuration dialog window.

Long Inputs Map I/O

This option provides configuration of Mapping Long Input I/O's Reg/Index to DNP3 points for generating events based on configured DeadBand and Class Assignments when the status of any Long Input I/O's changes.

Default DeadBand and Class Assignments are applied to all the Reg/Index defined by Highest Register Address except Reg/Index entries that are defined in Exception DeadBand and Class Assignments Table.



Define Highest Register Address

Configure DNP Points: If set to No, then no Binary Inputs are mapped as DNP3 points. If set to Yes, the Highest Register Address field is shown to enter a Highest Register Address value.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP3 points.

Default Deadband

Enter Default DeadBand Value: Values outside this DeadBand generate events. The DeadBand parameter sets how event data is generated by your module as a DNP3 slave device.

For example: The Analog Input DeadBand being set to a value of 1000 will report all of the points as being class 3 data (as set by the “Analog Input class” parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input deadband can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

Default Class assignment

Default Object 31 - Frozen Analog Input: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don’t generate events, this feature should be modified by the user.

Default Object 32 - Analog Change Event: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be

associated to None. By default all DNP3 Points don't generate events, this feature should be modified by the user.

Default Object 33 - Frozen Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP Points don't generate events, this feature should be modified by the user.

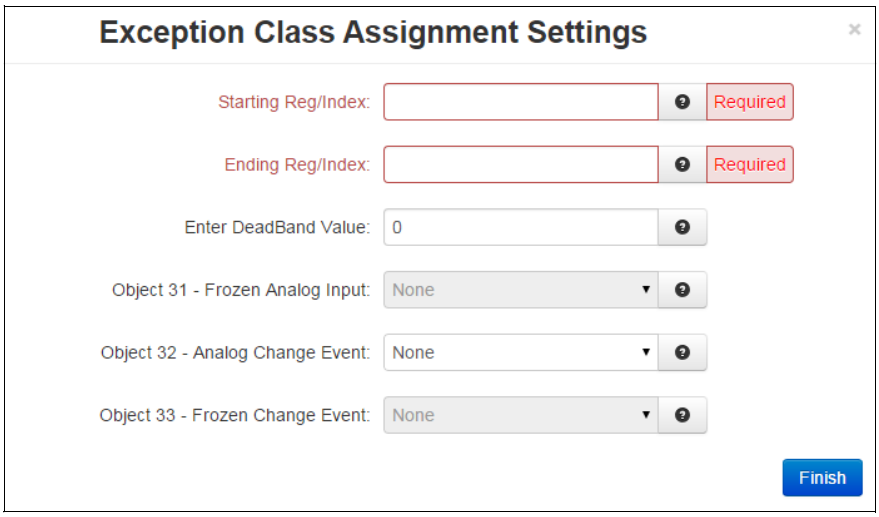
Exception DeadBand and Class Assignments Table: The Exception table provides the ability to define Reg/Index ranges that are needed to be configured differently than default DeadBand and Class Assignments.

Example: The Stating Reg/Index for Long Input is 512 and if the Highest Register Address is set to 522 and the Reg/Index 514, 516, 518-519 are needed to be set for different DeadBand and Class Assignments than default, then the final result for all 10 registers would be as follows:

- Reg/Index 512-513, 515, 517 and 520-522 will be set to Default DeadBand and Class Assignments.
- Reg/Index 514, 516 and 518-519 will be set to Exception DeadBand and Class Assignments.

Note: The Starting Reg/Index and Ending Reg/Index of Exception table entries for a single Reg/Index such as Reg/Index 514 and 516 in above example has to be the same address.

Click the *Add* button and the following dialog window appears:



Starting Reg/Index (Required): Enter the Starting Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be less than or equal to Ending Register.

Ending Reg/Index (Required): Enter the Ending Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be greater than or equal to Starting Register.

Enter DeadBand Value (Required): Values outside this DeadBand generate events. The DeadBand parameter sets how event data is generated by your module as a DNP3 slave device.

For example: The Analog Input DeadBand being set to a value of 1000 will report all of the points as being class 3 data (as set by the "Analog Input class" parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input DeadBand can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

Object 31 - Frozen Analog Input: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events)

then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't' generate events, this feature should be modified by the user.

Object 32 - Analog Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't' generate events, this feature should be modified by the user.

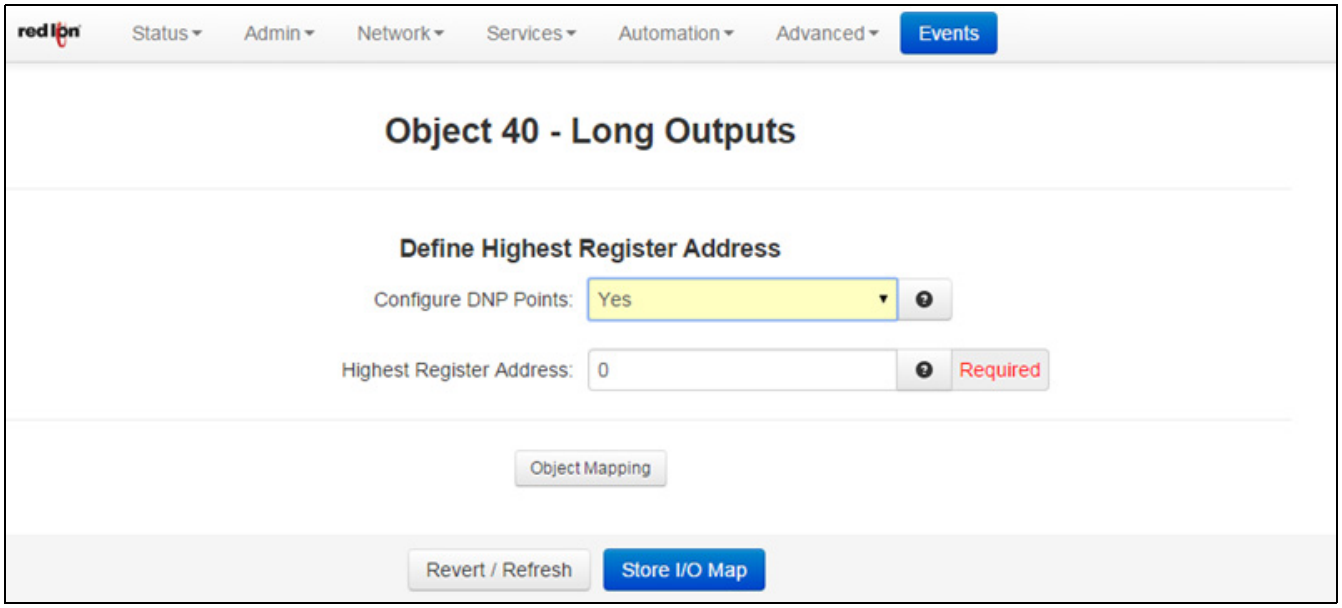
Object 33 - Frozen Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't' generate events, this feature should be modified by the user.

Click *Finish* to enter your exception into the table.

To edit an entry, select the station in the table and click on the *Edit* button. To delete an existing entry, select the station in the table and click on the *Delete* button.

Click on *Store I/O Mapping* to save your configuration before moving to the next project. Click on the *Object Mapping* button to return to the DNP3 Object Mapping Configuration dialog window.

Long Outputs Map I/O



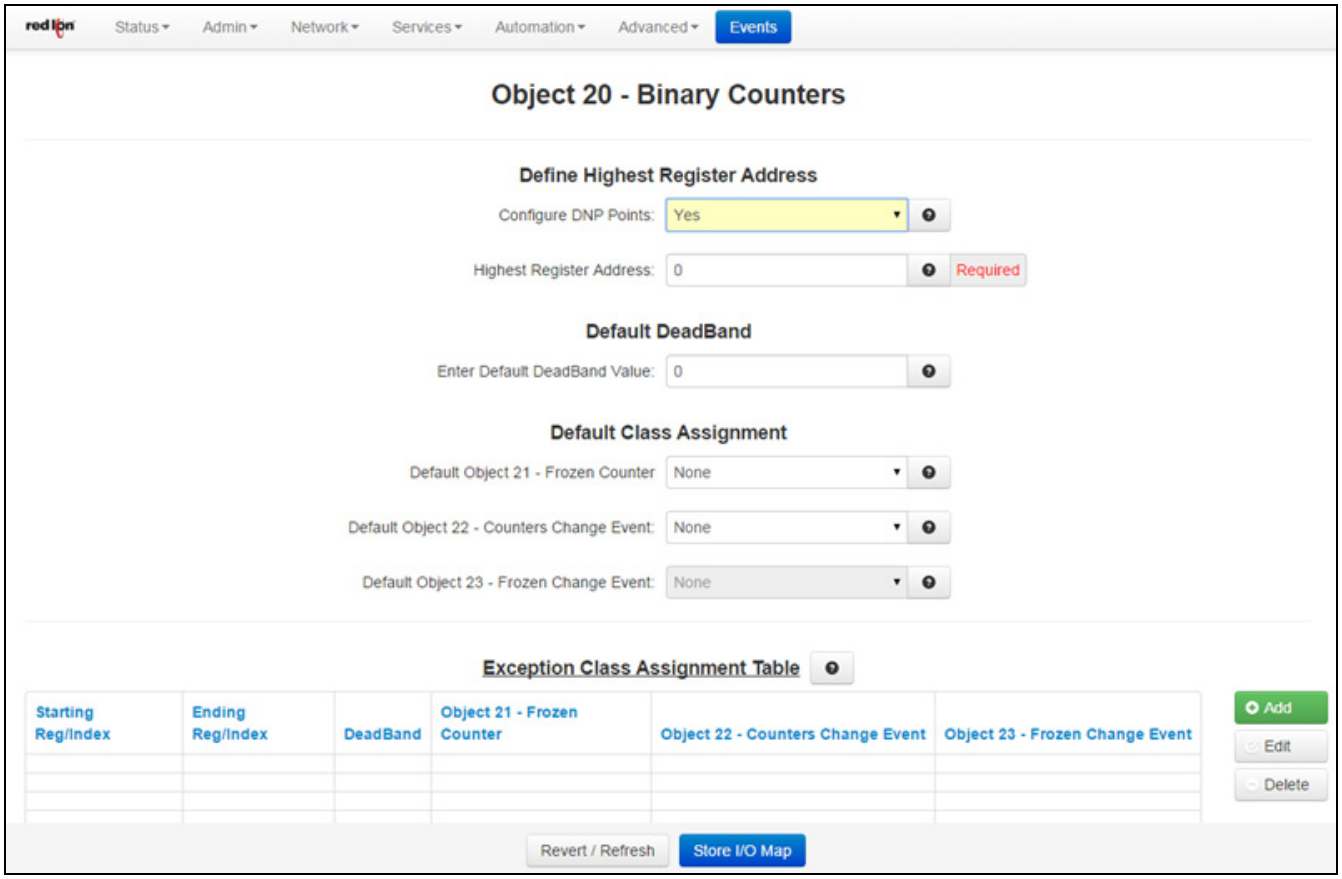
Configure DNP3 Points: If option is set to No, then no Long Outputs are mapped as DNP3 points. If set to Yes, the Highest Register Address field is shown to enter a Highest register Address value.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP3 points.

Click on *Store I/O Mapping* to save your configuration before moving to the next project. Click on the *Object Mapping* button to return to the DNP3 Object Mapping Configuration dialog window.

Binary Counters Map I/O

This option provides configuration of Mapping Binary Counters I/O's Reg/Index to DNP3 points for generating events based on configured DeadBand and Class Assignments when the status of any Binary Counter I/O's changes. DeadBand and Class Assignments are applied to all the Reg/Index defined by Highest Register Address except Reg/Index entries that are defined in Exception DeadBand and Class Assignments Table.



Define Highest Register Address

Configure DNP3 Points: If option is set to No, then no Binary Counters are mapped as DNP3 points. If set to Yes, the Highest Register Address field is shown to enter a Highest Register Address value.

Highest Register Address (Required): This field is used to show or set the highest register address to map DNP3 points.

Default Deadband

Enter Default DeadBand Value: Values outside this DeadBand generate events. The DeadBand parameter sets how event data is generated by your module as a DNP3 slave device.

For example: The Analog Input DeadBand being set to a value of 1000 will report all of the points as being class 3 data (as set by the “Analog Input Class” parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input deadband can be set to any value between 0 to 32767 (generate an event when the value changes to 32767).

Default Class Assignment

Default Object 21 - Frozen Counter: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don’t generate events, this feature should be modified by the user.

Default Object 22 - Counters Change Event: This field is activated on both Levels 2 and 2+. It’s used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don’t generate events, this feature should be modified by the user.

Default Object 23 - Frozen Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all DNP3 Points don't generate events, this feature should be modified by the user.

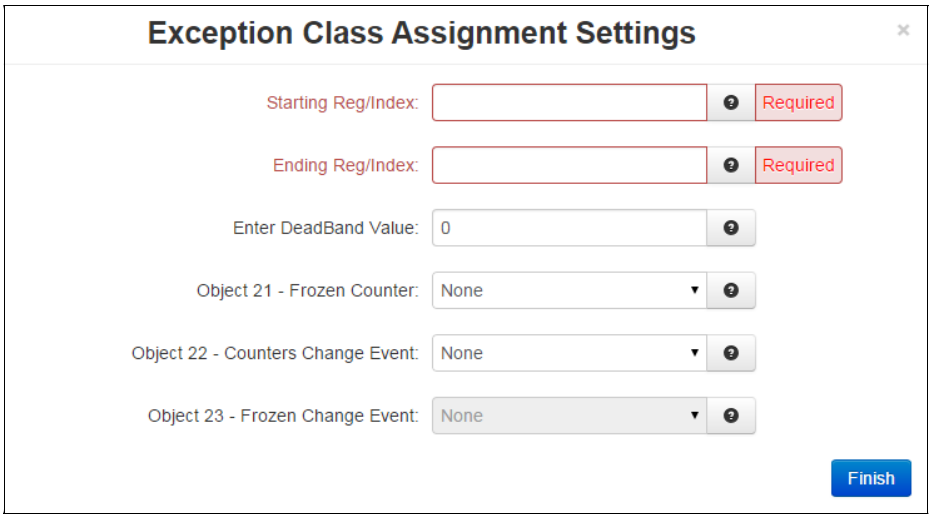
Exception Class Assignment Table: The Exception table provides you with the ability to define Reg/Index ranges that are needed to be configured different than Default DeadBand and Class Assignments.

Example: If the Highest Register Address is set to 10 and Reg/Index 2, 4, 6-7 are needed to be set for different DeadBand and Class Assignments than Default, then the final result for all 10 registers would be as follows:

- Reg/Index 0-1, 3, 5 and 8-10 will be set to Default DeadBand and Class Assignments.
- Reg/Index 2, 4 and 6-7 will be set to Exception DeadBand and Class Assignments.

Note: The Starting Reg/Index and Ending Reg/Index of Exception table entries for a single Reg/Index such as Reg/Index 2 and 4 in above example has to be the same address.

Click the *Add* button and the following dialog window appears:



Starting Reg/Index (Required): Enter the Starting Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be less than or equal to Ending Register.

Ending Reg/Index (Required): Enter the Ending Register for exception class assignments. The valid ranges are 0 to your configured highest register, and must be greater than or equal to Starting Register.

Enter DeadBand Value: Values outside this DeadBand generate events. The DeadBand parameter sets how event data is generated by your module as a DNP3 slave device.

For example: The Analog Input DeadBand being set to a value of 1000 will report all of the points as being Class 3 data (as set by the "Analog Input Class" parameter being set to 3) and it will generate an event every time an analog input changes by a value of 1000 or more. This Analog Input DeadBand can be set to any value between 0 to 32767 (generate an event when the value changes by 32767).

Object 21 - Frozen Counter: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a Class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default, all DNP3 Points don't generate events, this feature should be modified by the user.

Object 22 - Counters Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events)

then it should be associated to a Class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default, all DNP3 Points don't generate events, this feature should be modified by the user.

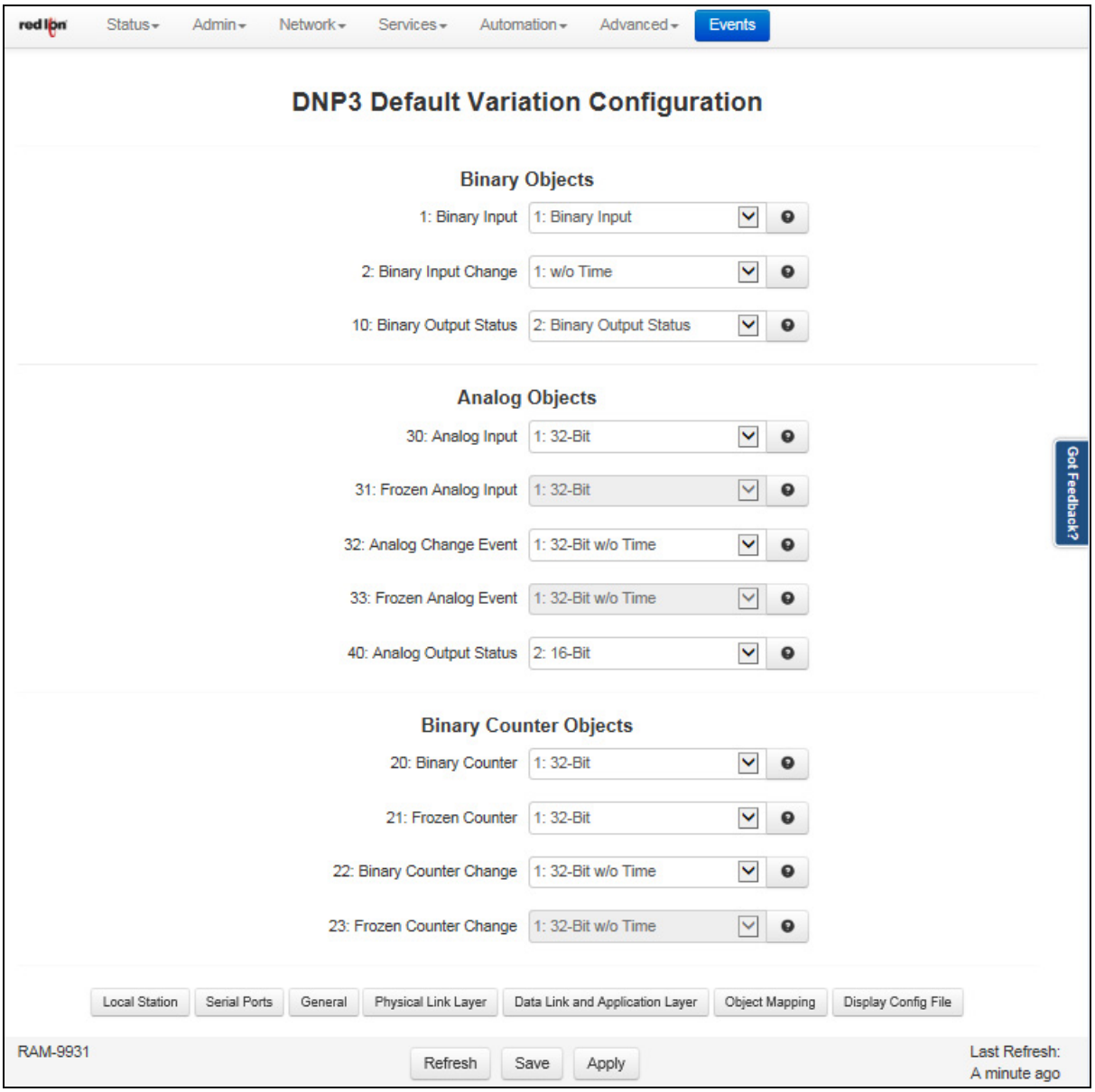
Object 23 - Frozen Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a Class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default, all DNP3 Points don't generate events, this feature should be modified by the user.

Click *Finish* to enter your exception into the table.

To edit an entry, select the station in the table and click on the *Edit* button. To delete an existing entry, select the station in the table and click on the *Delete* button.

Click on *Store I/O Mapping* to save your configuration before moving to the next project. Click on the *Object Mapping* button to return to the DNP3 Object Mapping Configuration dialog window.

Default Variation



Binary Objects

1: Binary Input: Combo Box that shows the different choices for Object 1 (Binary Input) that the user can select as a default variation.

2: Binary Input Change: Combo Box that shows the different choices for Object 2 (Binary Input Change Events) that the user can select as a default variation.

10: Binary Output Status: Combo Box that shows the different choices for Object 10 (Binary Output) that the user can select as a default variation.

Analog Objects

30: Analog Input: Combo Box that shows the different choices for Object 30 (Analog Input) that the user can select as a default variation.

31: Frozen Analog Input: Combo Box that shows the different choices for Object 31 (Frozen Analog Input) that the user can select as a default variation (only on Level 2+).

32: Analog Change Event: Combo Box that shows the different choices for Object 32 (Analog Input Change Events) that the user can select as a default variation.

33: Frozen Analog Event: Combo Box that shows the different choices for Object 33 (Frozen Analog Input Change Event) that the user can select as a default variation (only on Level 2+).

40: Analog Output Status: Combo Box that shows the different choices for Object 40 (Analog Output) that the user can select as a default variation.

Binary Counter Objects

20: Binary Counter: Combo Box that shows the different choices for Object 20 (Binary Counters) that the user can select as a default variation.

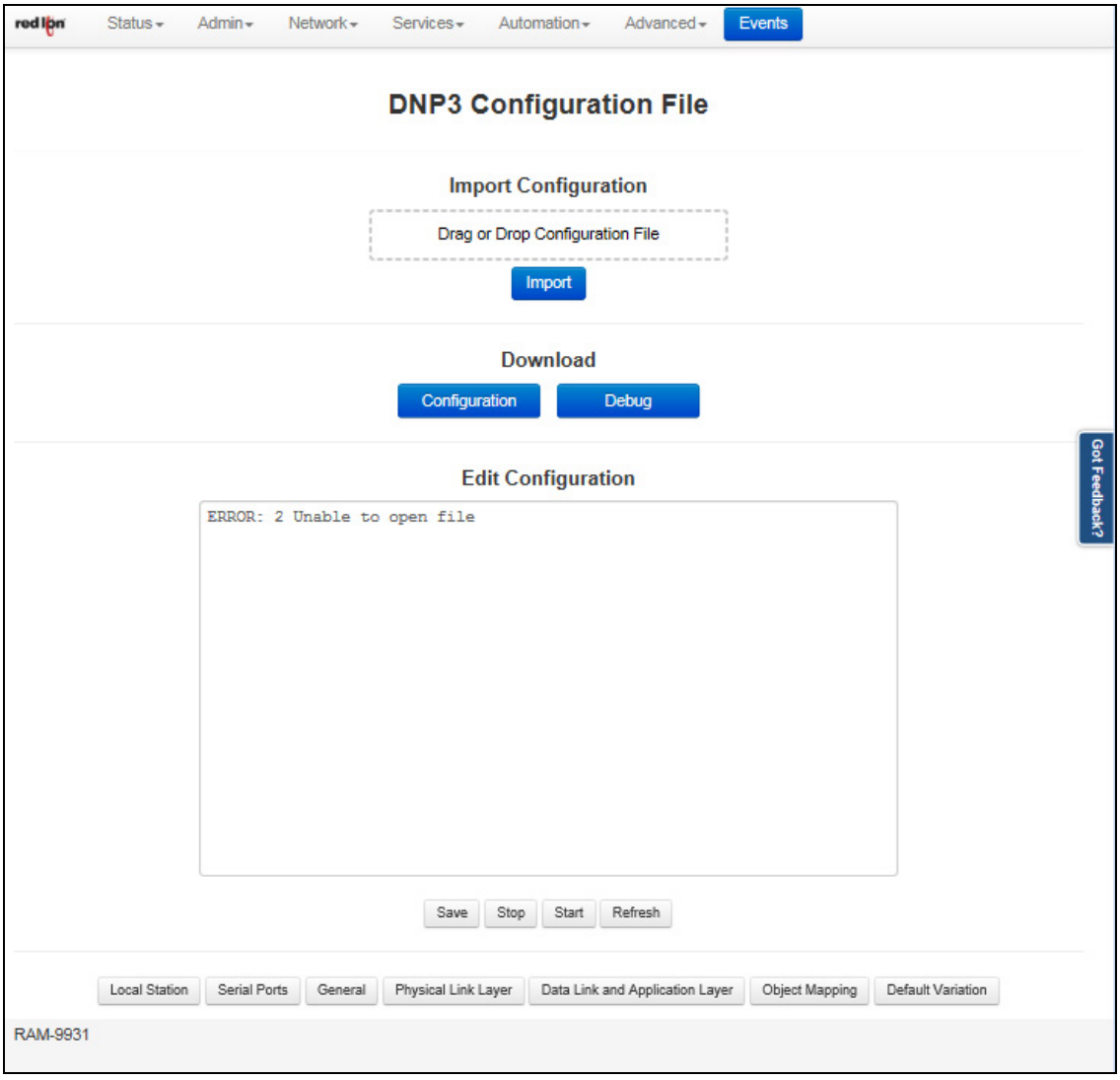
21: Frozen Counter: Combo Box that shows the different choices for Object 21 (Frozen Binary Counters) that the user can select as a default variation.

22: Binary Counter Change: Combo Box that shows the different choices for Object 22 (Binary Counters Change Events) that the user can select as a default variation.

23: Frozen Counter Change: Combo Box that shows the different choices for Object 23 (Frozen Binary Counters Change Event) that the user can select as a default variation (only on Level 2+).

Click on the *Save* button to save the Forwarding configuration in the modbus.xml file. The *Apply* button will save your settings and apply them immediately.

Display Config File



From this screen you are able to import, export and manually edit the DNP3 configuration file.

Import Configuration: This option allows you to import a configuration file to replace your existing DNP3 configuration file. Simply click on the Drag and Drop dialog box to select your DNP3 configuration file on your PC or you may drag and drop the configuration file onto the upload box. Click on the Import button to replace your existing DNP3 configuration file.

Download: You may use this feature to download the DNP3 configuration file (sxdnpdrv.ini) or DNP3 debug file (dnp3debug.log) to your local drive for review analysis.

Edit Configuration: This option will display the DNP3 configuration file in the text box for manual editing.

The following controls (buttons) are available:

Save: Save the contents of the text box into the DNP3 configuration file.

Stop: Stop the DNP3 services, if it is currently running.

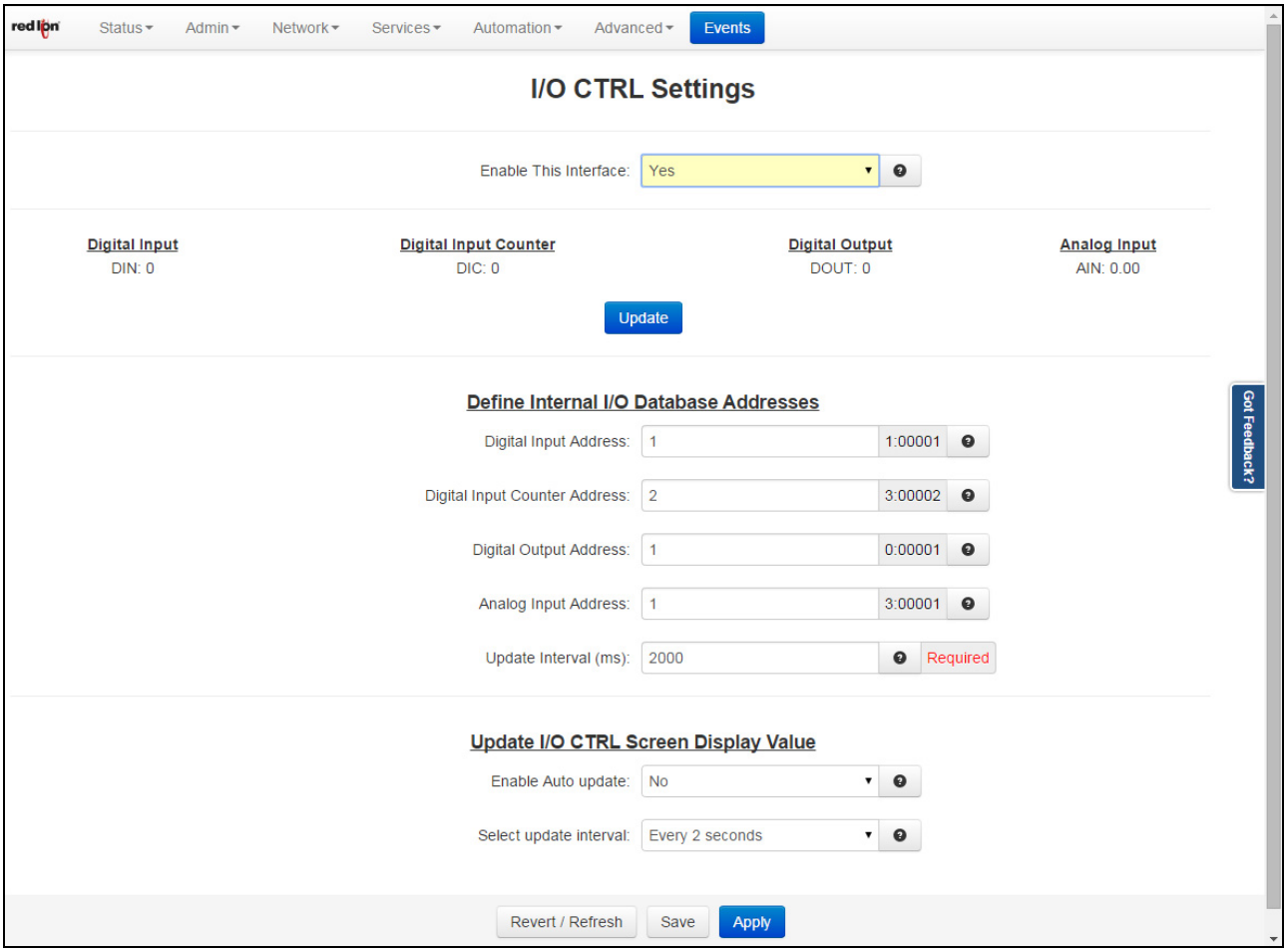
Start: Start the DNP3 services, or it will restart the DNP3 services if they are already running.

Refresh: Reload the DNP3 configuration file into the text box.

3.6.7 I/O Settings (RAM 6000 Models)

I/O Control

Click on the *I/O Control* menu item and the following window appears:



Enable this interface: Select Yes to enable the I/O CTRL Interface.

Digital Input Address: Enter the address of internal IODB database for Digital Input I/O control. Valid values for this field are 1 through 65535 as defined for specified I/O type.

Digital Input Counter Address: Enter the address of internal IODB database for Digital Input Counter. The valid values for this field are 1 through a value of defined register allocation configured for Analog Input I/O type. The address ranges are displayed on I/O Transfer screen under 'Display of Modbus Default Slave Addresses' based on configured local register allocation for specified I/O type.

Note: This address cannot be the same address as Analog Input Address. Take care to select a unique address to be used in Analog Input IODB for Digital Input Corner.

Digital Output Address: Enter the address of internal IODB database for Digital Output I/O control. Valid values for this field are 1 through 65535 as defined for specified I/O type.

Analog Input Address: Enter the address of internal IODB database for Analog Input I/O control. Valid values for this field are 1 through value defined registers configured for specified I/O type. The address ranges are

displayed on I/O Transfer screen under 'Display Of Modbus Default Slave Addresses' based on configured local register allocation for specified I/O type.

Update Interval (ms) (Required): Enter update interval, in milliseconds, for updating the internal IODB database with value of supported I/O CTRL. The recommended value for this field is 500ms or higher.

Enable Auto update?: Select Yes to enable automatic updating of the I/O ports value. Manual updating is disable while auto update is in effect. The recommended setting for this field is Yes.

Select update interval: Select the update interval to be used when auto update is enabled from one of the choices in the drop-down list provided. Choices (in seconds) include: 3, 5, 10 or 15.

Be advised that when connected via Cellular interface, the data collected will count towards your total data plan usage.

Click on the *Save* button to save the Forwarding configuration in the modbus.xml file. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

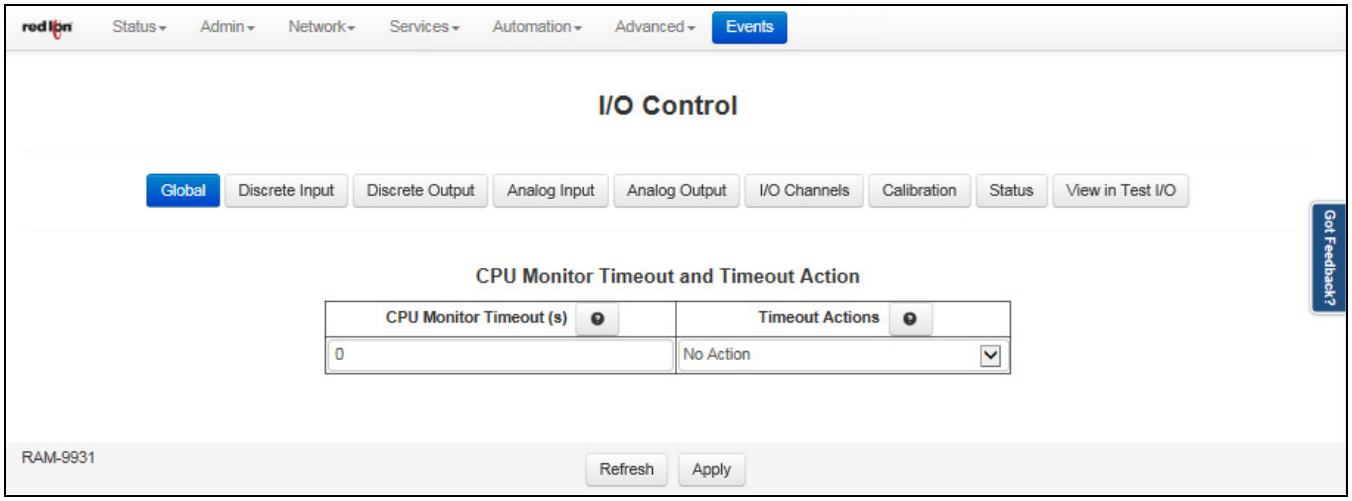
Test I/O

Test I/O is used to verify the functionality of I/O states in gateways, RTUs and I/O modules, refer to Test I/O on page 238 for detailed information

3.6.8 I/O Settings (RAM-9000 Models)

I/O Control

Click on the *I/O Control* menu item and the following window appears:



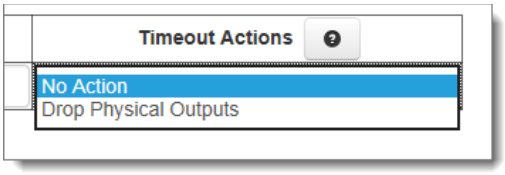
Global: Clicking on the Global button will return the user to the main I/O Control dialog window.

CPU Monitor Timeout (ms): This option is used to make the I/O fail safe if the main CPU stops working. The main CPU controls communication, IODB and code written in C. If the main CPU stops working, the I/O processor will detect that in the time defined in this field. Suggested timeouts are 1000ms to 10000ms. Timeouts faster then 100ms are not recommended. The maximum allowed timeout value is 0xFFFF(65535ms).

Setting this value to 0 will disable the feature. The default value for this field is 0 (Timeout Disabled).

Select the “Timeout Actions” field to define what the I/O should do when a CPU timeout occurs.

Timeout Actions: When a timeout to the CPU occurs, the selected “Timeout Action” will take effect.



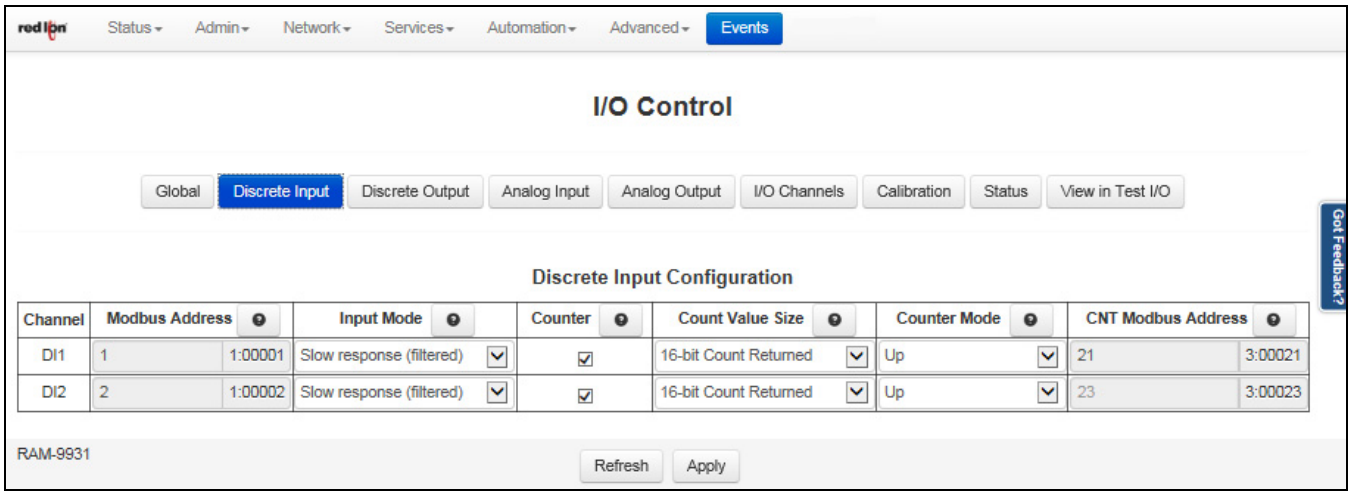
When “Drop Physical Outputs” is selected, all outputs are dropped to and OFF stated.

When “No Action” is selected, outputs will hold their last known value.

In a discrete output module, the OFF state is simply turning the outputs off, in an analog output module, OFF means to set all outputs to a nominal calibrated zero output. TPO Outputs will be set to output 0, but may require the normal TPO interval to elapse before the output will go off.

Discrete Input

Click on the *Discrete Input* button and the following dialog window appears:



Channel: A channel is a physical IO point that can be either analog or digital.

Modbus Address: Configuration must be sequential. Addresses are fixed sequentially from the base address.

Input Mode: This field defines the filtering mode of the Discrete Input channel. Select an option from the drop down list.

Disabled: Selecting this option will completely disable the channel and a zero (0) will be reported.

Slow Response (filtered): When this option is selected, the Discrete Input will have software filtering applied to the input. Software filtering is suitable when the input is connected to a mechanical switch or relay because it will eliminate contact bounce. In this mode, counting is limited to a maximum of 10 Hz.

Fast Response (no filtering): When this option is selected, the discrete input will have no filtering applied to the input. This option is suitable for solid state switches where no contact bounce is present.

Counter: This option will be available when Input Mode supports counters. When the checkbox is checked, the counter mode is enabled. The Count Value Size, Counter Mode and CNT Starting Address become available and must be configured as well. The counter value is stored in the CNT IODB address.

Count Value Size: This is a plain counter mode that is either 16 or 32-bits in size, which counts on positive edge or negative edge depending on the polarity bit.

16-bit Count Returned: When this option is selected, the count will increment in a single register from 0 to 65535, then roll over to 1 and continue to count upward again.

32-bit Count Returned: Select this option to use two (2) consecutive 16-bit registers as one 32-bit register. When the first register rolls over to 1, the second register begins counting at 65536 (second register is most significant) and continues counting upward in 32-bit mode.

Note: Two (2) consecutive registers are always allocated in the “CNT IODB/Modbus Address” column whether set for 16-bit or 32-bit mode. Therefore, when using 16-bit Count Returned option, the second register should be ignored.

Counter Mode: When this option is selected, the counter mode must also be selected. If the 16-bit Counter Returned is selected, the analog input register increases from 0 to 32767, then -32768 to 0. If the 32-bit Count Returned is selected, the long integer input register increases from 0 to 4.2949673E9, then -4.2949673E9 and back to 0. The menu selections for this options are listed below:

Note: When the Input Mode is set to Slow Response (filtered) some of the Counter Mode options are not particularly suited since the maximum count is 10Hz. For example, Frequency Rate 0.1s would only be capable of measuring one count.

Up: Upward accumulator of input pulses

Run time sec: This is the on-time timer feature that counts the time the associated input is in the ON state. The output for this option is in seconds.

Run time min: This is the on-time timer feature that counts the time the associated input is in the ON state. The output of this option is minutes.

Freq. Rate: Depending on the frequency rate selected, the pulses are accumulated for 100ms, 200ms, 500ms, 1 second, 2 seconds, 5 seconds, 10 seconds, 30 seconds, 60 seconds or 60 minutes.

ON Pulse Width: Width time is ms between consecutive leading (OFF to ON) and trailing (ON to OFF) edges.

OFF Pulse Width: Width time is ms between consecutive leading (ON to OFF) and trailing (OFF to ON) edges.

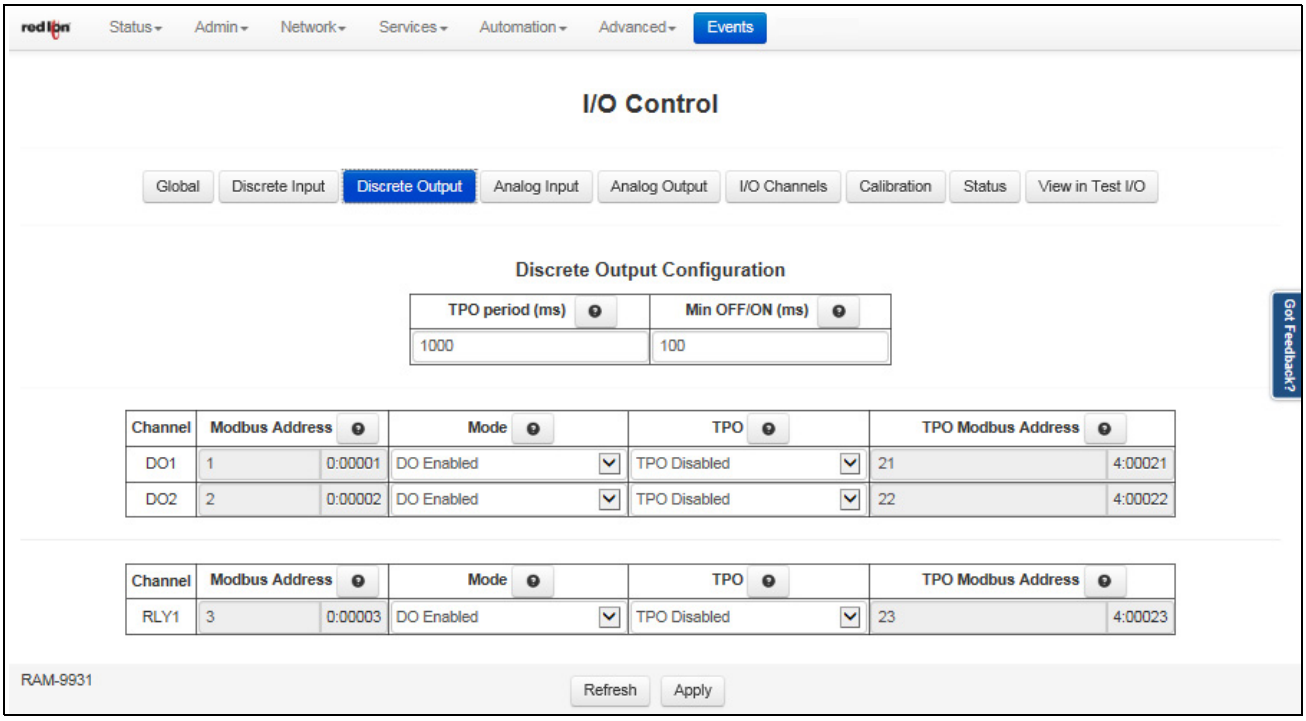
- Pulses longer than the maximum size allowed by the register will result in an overflow condition (full scale 16-bit value equal to 65535)
- Pulses shorter than 1ms will not be accurately detected resulting in erroneous values.
- If no edge is ever detected by an input, the result will read as $0000. Timing only begins when an edge is detected.

Note: Counters are volatile (they will forget their counts if power is lost). Typically, retention of the values and resetting the counts is accomplished in software at the host computer that polls these inputs.

CNT Modbus Address: Configuration must be sequential, CNT addresses are sequential by two registers from the base address.

Discrete Output

Click on the *Discrete Output* button and the following dialog window appears:



TPO period (ms): Time Proportioned Outputs (TPO) are outputs that turn on and off in proportion to an analog value. Typically, the output will turn on and off once during the specified TPO period (cycle time).

Specify a cycle time for all enabled TPO outputs in the module. The range of the cycle time is 20ms to 10 minutes (600,000ms). Each TPO will pulse ON and OFF once during each cycle period, unless a minimum OFF/ON time is specified. The default TPO period value is 1000ms.

Min OFF/ON (ms): Specify a minimum OFF/ON time (shortest allowable ON or OFF pulse) if the output devices are not capable of changing stat within 1/32767 of the desired time. (Mechanical relays are an example of such a device).

The range for the minimum OFF/ON time is 10ms to 10 minutes. All settings will maintain the time proportion by waiting multiple cycle times, if needed, to turn an output ON or OFF. The default value for this field is 100ms.

Channel: A channel is a physical I/O point that can be either analog or digital.

Modbus Address: Configuration must be sequential. Addresses are fixed sequentially from the base address.

Mode: This option will enable/disable the discrete output channel.

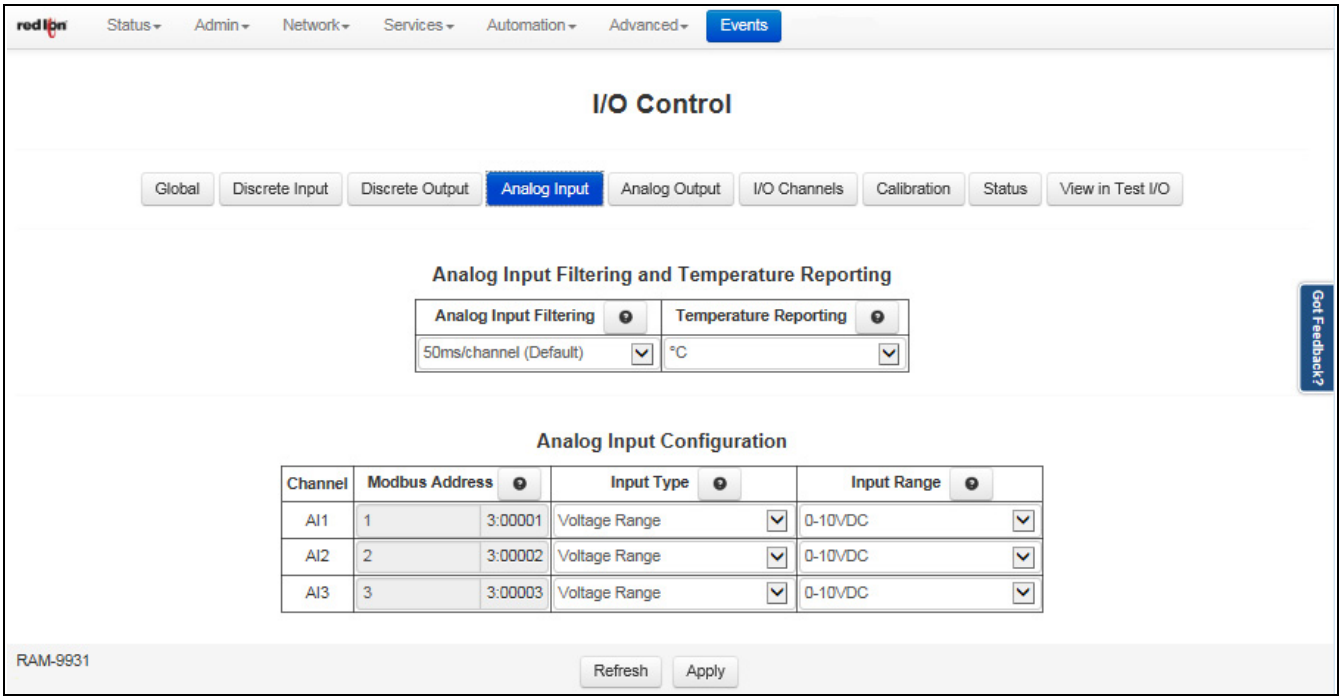
TPO: Select the Enable Time Proportioned Outputs (TPO Disabled/Enabled) in the drop down list, if it is desirable to have any discrete outputs in this module function as time proportioned outputs. All discrete outputs support this TPO capability. Each channel can function as a TPO output or a discrete output, but not both. If TPO is enabled, the TPO period, Min. OFF/ON and TPO IODB/Modbus address must be configured as well.

The analog value associated with each channel will control how long the TPO will be ON or OFF (16-bit value from 0-32767). For example, an analog value of zero will tell the output to be OFF. A value of 3276 (10% of 32767) will turn the output on for 10%of the “TPO Period” value. 32767 (full scale) will control the output to be ON at all times except for Min OFF/ON time.

TPO Modbus Address: This field indicates the register addresses of the analog outputs that control the TPO’s when enabled. Configuration must be sequential. Addresses are fixed sequentially from the base address.

Analog Input

Click on the *Analog Input* button and the following dialog window appears:



Analog Input Filtering: The table below explains the filtering (integration) options on the analog inputs. The faster the integration time, the quicker the channels will be sampled. However, quicker samples will render less accurate readings. For most accurate readings, select the slower sample/filtering settings.

Integration Time	Samples/Second (1 Channel)	Notes
3ms/channel	320	Best for high speed reporting and lower accuracy
6ms/channel	160	
12.5ms/channel	80	
25ms/channel	40	
50ms/channel (default)	20	Best for 50/60Hz noise rejection and higher accuracy.
100ms/channel	10	
200ms/channel	5	

Temperature Reporting: Choose from 1°C, 0.1°C, 1°F and 0.1°F. When set for 1°C or F, the temperature is reported as whole degrees and if set for 0.1°C or F, the reported value is the temperature multiplied by 10 and reported as an integer.

Channel: A channel is a physical I/O point that can be either analog or digital.

Modbus Address: This field indicate the register addresses for each channel. Configuration must be sequential. Addresses are fixed sequentially from the base address.

Input Type: Select the type of signal that will be connected to the input.

Disabled: This option will completely disable the channel so the channel will always report a zero. The Input Range is configuration will be disabled as well.

Voltage Range: When this option is selected, the analog input will be configured to take a DC voltage range. The Input Range must also be configured.

Current Range: With this option selected, the analog input will be configured to take current instrumentation input (0-40mA or 4-20mA). The Input Range must also be configured.

Input Range: Select the range that will be connected to the input channel.

0-5 VDC and 0-10 VDC: This option will be available when the Voltage Range option is selected. In these modes, the value will be scaled from the selected range (0-5 VDC and 0-10 VDC) to 0-32767 (decimal).

0-20 mA Positive Results Only and 4-20 mA Positive Results Only: These options will be available when the Current Range option is selected In these modes, the value will be scaled from the selected range (0-20mA and 4-20mA) to 0-32767 (decimal). No negative results will be displayed. If no signal is connected, the analog input value reported will be 0 (decimal).

4-20 mA Negative below 4mA: When this option is selected, the 4-20 mA range will be scaled from 0-32767 (decimal). A negative value will be displayed when nothing is connected to the input or the instrument is no longer supplying a current. This setting can be used to detect a failed or disconnected instrument.

Note: Negative numbers are determined by using the most significant bit in the 16-bit decimal value as a signed bit. When the most significant bit is 0, the value is positive. When the most significant bit is 1, the value is negative. Therefore, the value read from the channel may be displayed differently depending on the device that is reading that value. For example, negative values may also be read as any decimal value above 32767.

Analog Output

Click on the *Analog Output* button and the following dialog window appears if analog output is supported for the model in use:

Channel: A channel is a physical I/O point that can be either analog or digital.

Modbus Address: This field indicate the register addresses for each channel. Configuration must be sequential. Addresses are fixed sequentially from the base address.

Output Range: Select the type of signal to be supplied by the output channels.

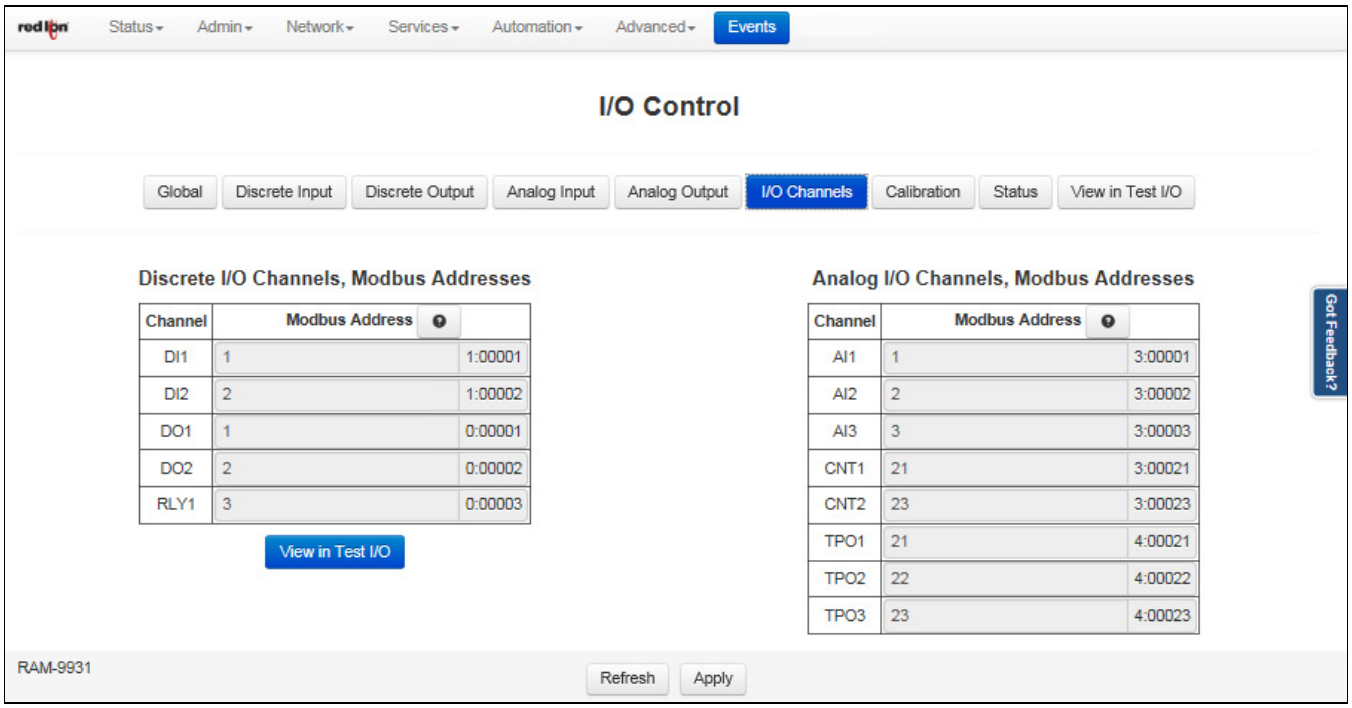
Disabled: This option will completely disable the output channel.

0-5 VDC: When selected, the analog output will be configured to supply a DC voltage from 0-5 VDC. The output voltage will be scaled to 0-32767 (decimal value in the IODB/Modbus Address field).

0-20 mA: When selected, the analog output will be configured to supply a current from 4-20 mA. The output voltage will be scaled to 0-32767 (decimal value in the IODB/Modbus Address field).

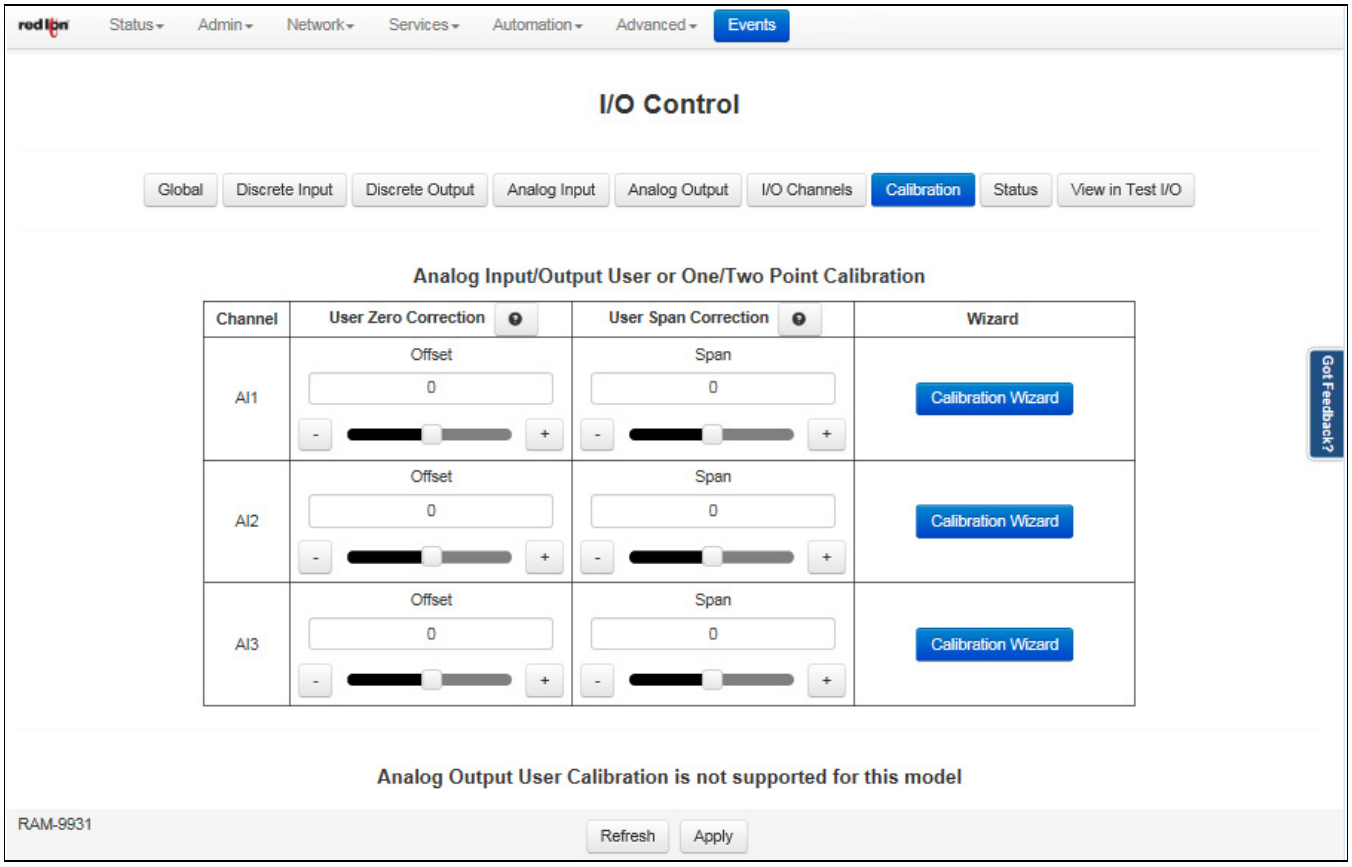
I/O Channels

Click on the *I/O Channels* button and the dialog window below appears. The I/O Channels dialog window will provide a list of all the channels with their associated IODB/Modbus Address.



Calibration

Click on the *Calibration* button and the following dialog window appears:



Channel: A channel is a physical I/O point that can be either analog or digital.

User Zero Correction: Manually adjust the user offset calibration for analog inputs/outputs. Every analog/ input is calibrated at the factory according to the specified accuracy. The user calibration is supplied to account to adjust the reported values to account for wiring or instrumentation errors. For this reason, most inputs/ outputs will NOT need to be calibrated.

Zero or Offset calibrations are used to adjust the reported value from 5 to 15% full scale. The calibration can be adjusted coarsely by moving the slide bar from left to right with a mouse. For fine adjustments, use the -/+ buttons on either side of the slide bar. The corresponding adjustment will be displayed in the calibration configuration. The calibration will not take effect until the apply button is clicked.

A negative adjustment (negative calibration value) will cause the reported channel value to go down. A positive adjustment (positive calibration value) will cause the reported channel value to go up. The larger the calibration value the greater the difference will be between the reported channel value and the actual measured value.

Instructions on adding user calibrations:

Use this method to calibrate a channel using the manual slide bar user calibration.

1. Set your analog signal device for a near minimum (5 to 15% full scale) output. Measure the device's output at the module's screw terminals with a precision meter or external standard monitor.
2. Apply the small signal to the analog input channel. Compare the value currently being reported with the value on your meter. If they are not equal, adjust the Offset value by the using the slide bar and arrows

in the Offset display box. Click the Apply button and observe the effect of the new offset factor. Repeat this step until a satisfactory reading is obtained.

3. Set your analog device for a near full scale (85 to 95% full scale) output. Compare the value currently being reported with the value on your meter. If they are not equal, adjust the span value by using the slide bar and arrows in the span display box. Click the Apply button and observe the effect of the new span factor. Repeat this step unit a satisfactory reading is obtained.
4. The channel is now calibrated.

User Span Correction: Manually adjust the user span calibration for analog inputs/outputs. Every analog input/output is calibrated at the factory according to specified accuracy. The user calibration is supplied to account to adjust the reported values to account for wiring or instrumentation errors. For this reason, most inputs/outputs will NOT need to be calibrated. Span calibration are used to adjust the reported value from 85 to 95% of full-scale.

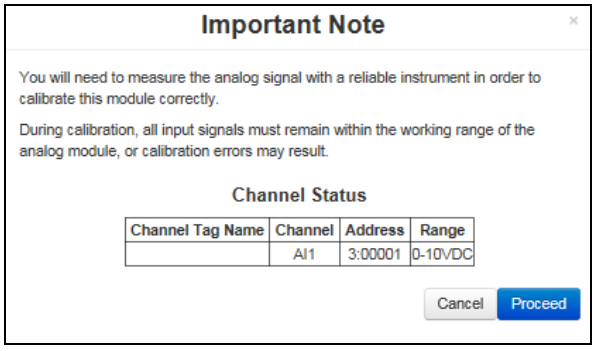
The calibration can be adjusted coarsely by moving the slide bar to the left or right with a mouse. For fine adjustments, use the -/+ buttons on either side of the slide bar. The corresponding adjustment will be displayed in the calibration configuration. The calibration will not take effect until the apply button is clicked. A negative adjustment (negative calibration value) will cause the reported channel value to go down. A positive adjustment (positive calibration value) will cause the reported channel value to go up. The larger the calibration value, the greater the difference will be between the reported channel value and the actual measured value.

Instructions on adding user calibration:

Use this method to calibrate a channel using the manual slide bar user calibration:

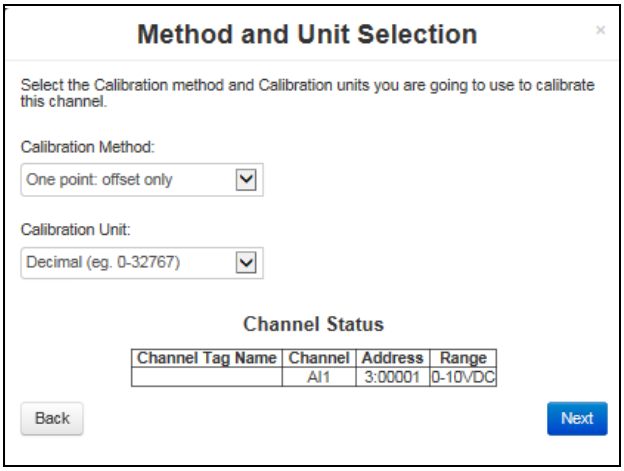
1. Set your analog signal device for a near minimum (5 to 15% full scale) output. Measure the device's output at the module's screw terminals with a precision meter or external standard monitor.
2. Apply the small signal to the analog input channel. Compare the value currently being reported with the value on your meter. If they are not equal, adjust the Offset value by using the slide bar and arrows in the Offset display box. Click the Apply button and observe the effect of the new offset factor. Repeat this step until a satisfactory reading is obtained.
3. Set your analog signal device for a near full scale (85 to 95% full scale) output. Compare the value currently being reported with the value on your meter. If they are not equal, adjust the Span value by using the slide bar and arrows in the Span display box. Click the Apply button and observe the effect of the new span factor. Repeat this step until a satisfactory reading is displayed.
4. The channel is now calibrated.

Calibration Wizard: You will need to measure the analog signal with a reliable instrument in order to calibrate the module correctly using the calibration wizard. Click on the Calibration Wizard button adjacent to the channel to start the wizard:

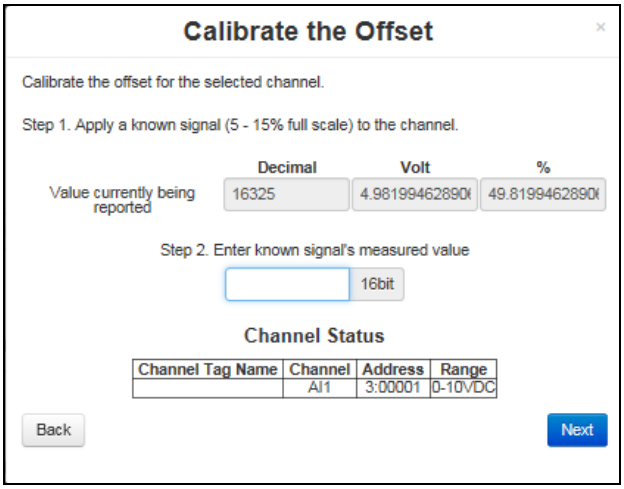


1. Click the Proceed button.

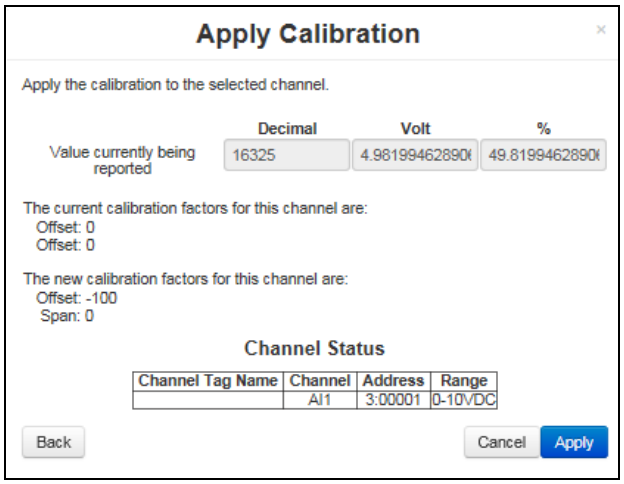
2. Select the calibration method and calibration units to use in the calibration.



3. Calibrate the offset for the selected channel by entering known signal's measured value.



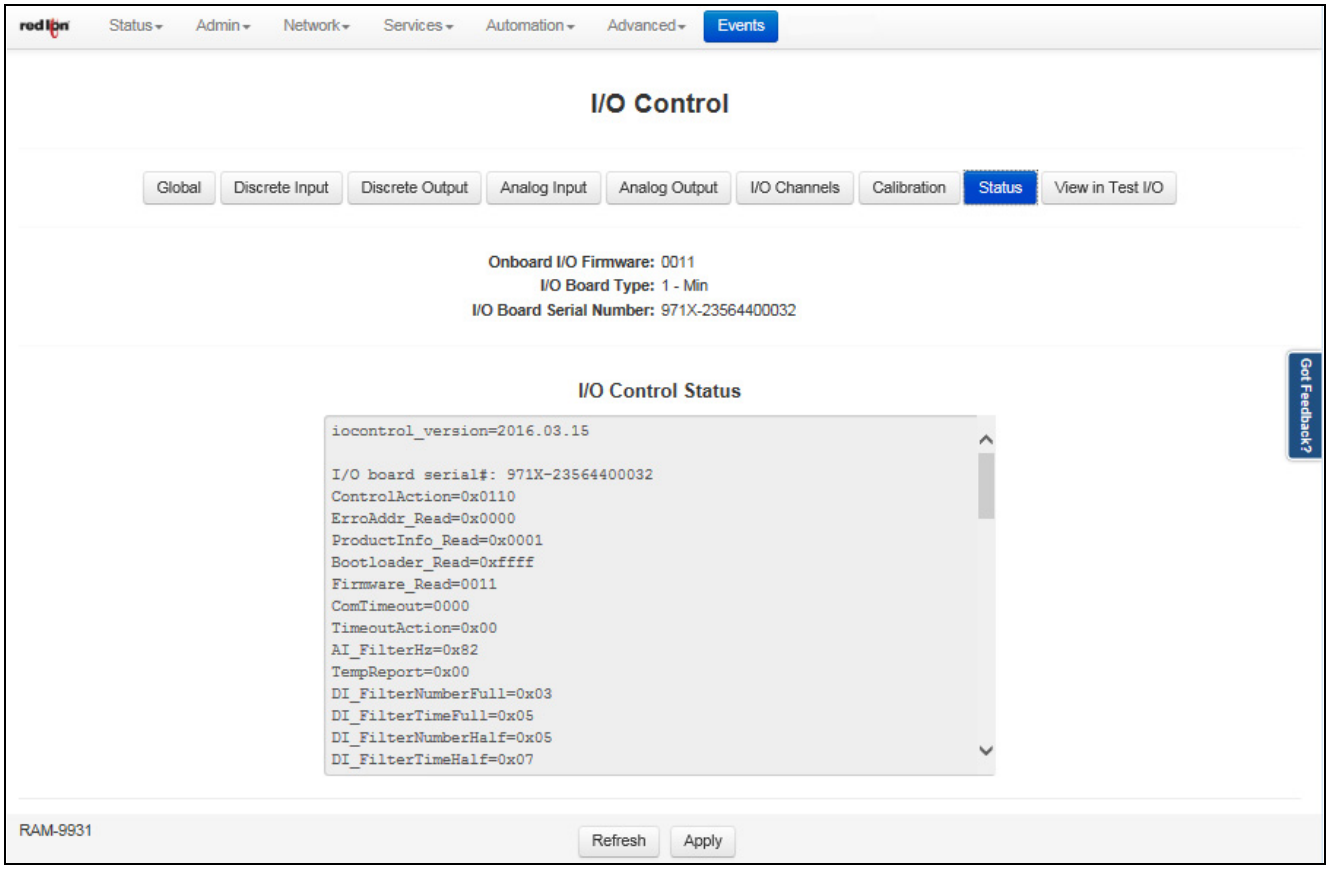
4. Apply the new calibration factors for the channel by clicking Apply button on the Apply Calibration screen.



5. Or cancel the calibration wizard by clicking Cancel button on the Apply Calibration screen.

Status

Click on the *Status* button and the dialog window below will provide you with your system's I/O Control Status and I/O Control Config Status.



View in Test I/O:

Click on the *Test I/O* button to be directed to the Test I/O Access dialog window. See section 3.6.5 for more information on this feature.

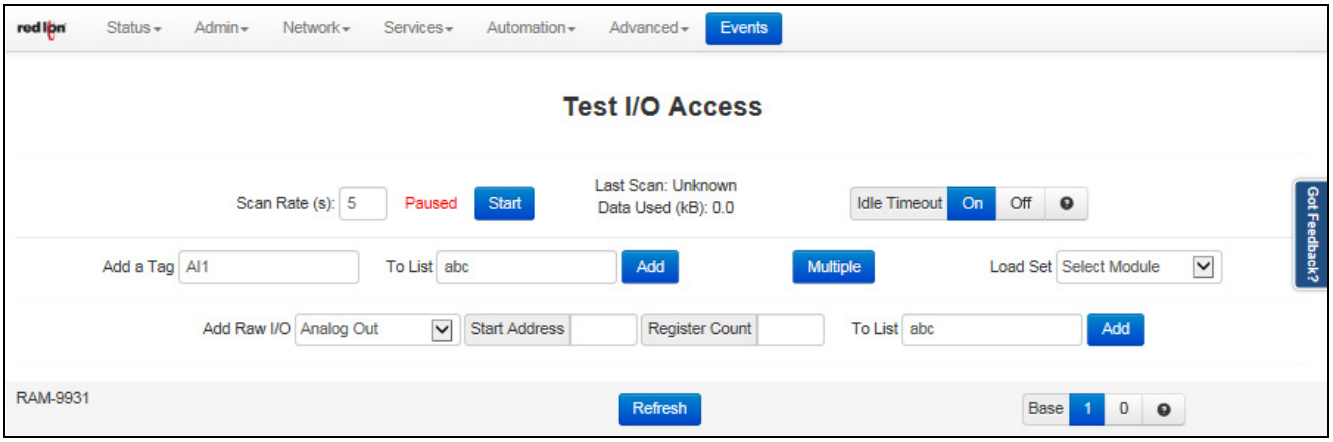
3.6.9 Test I/O

Test I/O is used to verify the functionality of I/O states in gateways, RTUs and I/O modules.

When a RAM-9000 model reboots for a power cycle, at the startup the I/O data turns out to no longer represent the previous real world situations if the tags do not have the Retain option checkbox selected. Since I/O data is critical for the device use we offer the I/O Retain feature to store the configured I/O data for as long as the on-board battery can supply the SRAM. The Test I/O Access screen offers the means of testing an I/O after startup to verify critical I/O data is retained by reading the outputs and sending corresponding physical signals to devices.

Note: The Retain option is only available on specific tags for the RAM-9000 models.

The Test I/O Access screen offers the means of testing an I/O after startup to verify critical I/O data is present by reading the outputs and sending corresponding physical signals to devices.



The Test I/O interface has been kept simple to make managing the test I/O process easier and keep the screen less cluttered, easier to look at and quickly locate your test values.

Scan Rate: This is the time in which the screen will automatically refresh values from the internal IODB.

Idle Timeout: When this option is enabled (ON button selected), the browser will stop scanning after two minutes of inactivity.

Add a Tag: Start typing the tag name you would like to add and a pop up appears that lists all tags that match the pattern you entered. Click the Tag name to select it from the pop up list

To List: Select the list to add the selected tag to or create a list by entering its name here and clicking on Add. Lists are used to group I/O points together for more organized viewing.

Multiple: Select multiple tags to add to the indicated list from the Add to set pop up screen and clicking on Select to add the selected tags to the list.

Load Set Select Module: Select the desired IODB Status Module from the drop down list. Valid IODB Modules are:

System Status	GPS	Cellular	RAMQTT Points	User List
Traffic	Network	RAMQTT Status	On-board IO	

Add Raw I/O: From the drop down list, select the type of I/O you would like to test. Valid I/O types are:

Analog In	Discrete In	Long In	Float In
Analog Out	Discrete Out	Long Out	Float Out

Start Address: Once the I/O type has been selected, enter the Start Address.

Register Count: Enter the Register Count for the number of registers you would like to display.

To List: Select the list to add the selected tag or create a list by entering its name here and clicking on Add. Lists are used to group I/O points together for more organized viewing.

Click on the *Add* button to test the I/O.

The messages logs show the range entered and each register that can be edited and monitored for the analog Inputs.

Base 1 0: This toggles the system-wide register display format, which can be represented in two schemes: Zero-based or One-based. Zero-Based is also called Native format, and all register ranges would begin counting at 0. One-Based addressing starts all ranges with 1 and is the system commonly used with Modbus.

Each register label consists of the Tag name, followed by the address in two parts: type and address. Type and address will change to match the Zero (Native) and One (Modbus) formatting conventions. An untagged register will show an implied tag in <angle brackets>.

You may enter values here and observe your IODB data from another device / location to see those values get updated or you may initiate a change from another device/input and observe the changes presented here on your Test I/O interface.

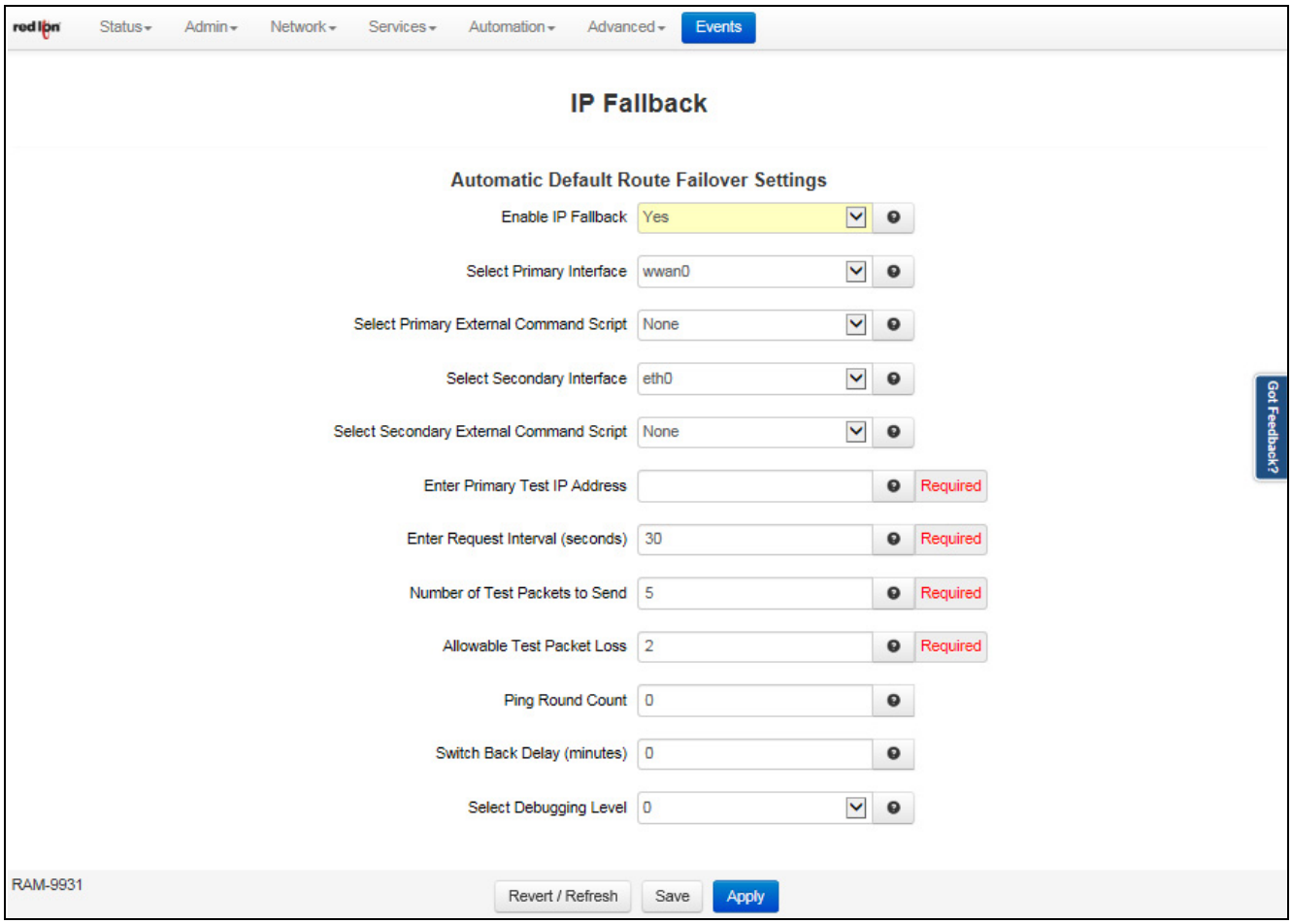
3.7 Advanced Tab

The Advanced tab provides user access to advanced configuration features available for the Red Lion RTU or router, including IP Fallback, IP Transparency, Out-of-Band Management, VRRP, Expert Mode and GWLNX.

3.7.1 IP Fallback

The IP Fallback option is used to configure the Red Lion RTU or router to failover between two interfaces, e.g. Primary route on T1/ DSL/Cable on eth0, and secondary on Cellular if the primary loses Internet connection.

Click on the *IP Fallback* menu item and the following dialog window appears:



Enable IP Fallback: Select *YES* to enable the IP Fallback. Enable this option if you have two paths (interfaces) configured with WAN (Internet) support. An example would be primary Ethernet (eth0) and secondary cellular (ppp0).

Note: When using an Ethernet port setup as DHCP Client, choose: **Use Remote Gateway as Default Route: NO** in the Ethernet port setup screen. Default route control will be managed by the IP Fallback instead.

Select Primary Interface: Specify your desired primary interface for IP Fallback behavior.

Select Primary External Command Script: Choose the name of the command script to be executed when the associated interface becomes active. For example, if a *Restart IPSec* is an option, then when selected, it will be run whenever the fallback logic selects and activates this interface.

The recommended setting for this field is *None* for standard operation with no special behaviors. *Restart IPSec* is useful when using an IPSec VPN tunnel.

Select Secondary Interface: Select the secondary interface to be used for IP Fallback. Selecting vrrp will coordinate with the VRRP process, so that when the primary interface is determined to be unavailable, VRRP will stop broadcasting availability.

Select Secondary External Command Script: Choose the name of the command script to be executed when the associated interface becomes active. For example, if a *Restart IPSec* is an option, then when selected, it will run whenever the fallback logic selects and activates this interface.

The recommended setting for this field is *None* for standard operation with no special behaviors. *Restart IPSec* is useful when using an IPSec VPN tunnel.

Enter Primary Test IP Address (Required): Specify the IP address of a host with which the IP Fallback service will communicate to test connectivity. Value must be a pingable address, and not a domain name. The best choice would be an address that represents end-to-end connectivity.

Enter Request Interval (in seconds) (Required): Specify the time, in seconds, to wait between connectivity tests. The minimum is 10, maximum is 600. **Note:** This value should be 30 or higher for cellular connections.

Number of Test Packets to Send (Required): Specify the number of 0 byte ping packets to send out to test connectivity. The minimum is 2, maximum is 30. The recommended setting for this field is 5 - 10.

Allowable Test Packet Loss (Required): Specify the number of lost packets that are acceptable before the IP Fallback service will consider the link unavailable, and switch to its secondary. Note: the value must be less than the number of test packets set via Test Packets to Send.

Ping Round Count: This is the number of **ping rounds** that must be successful in a row to switch back from the secondary interface to the primary. The purpose is to delay switching back to the primary until it has proven stable to multiple tests.

Example: Setting this value to 3 means 3 complete ping set rounds must be successful based on the configuration prior to switching back to the primary interface.

Default: 0 (disabled)

Switch Back Delay (minutes): The minimum number of minutes to wait prior to switching from the secondary interface back to the primary interface. The purpose is to prevent rapid flipping in an unstable environment. A larger value will force the secondary link to be used for a longer period of time, even if the primary becomes available.

Example: Setting this value to 5 will set a minimum delay of 300 seconds (5 minutes). If the process switches to the secondary interface due to a failure, and after 2 minutes the primary interface is determined to be good (based on the configuration), there will still be an extra 3 minute delay prior to switching back to the primary interface.

Default: 0 (disabled)

Select Debugging Level: Specify a debug level for logging purpose. This is recommended only when existing configurations do not function as expected, and when directed to change by Red Lion Technical Support.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit.

Click the *Apply* button will save your settings and apply them immediately.

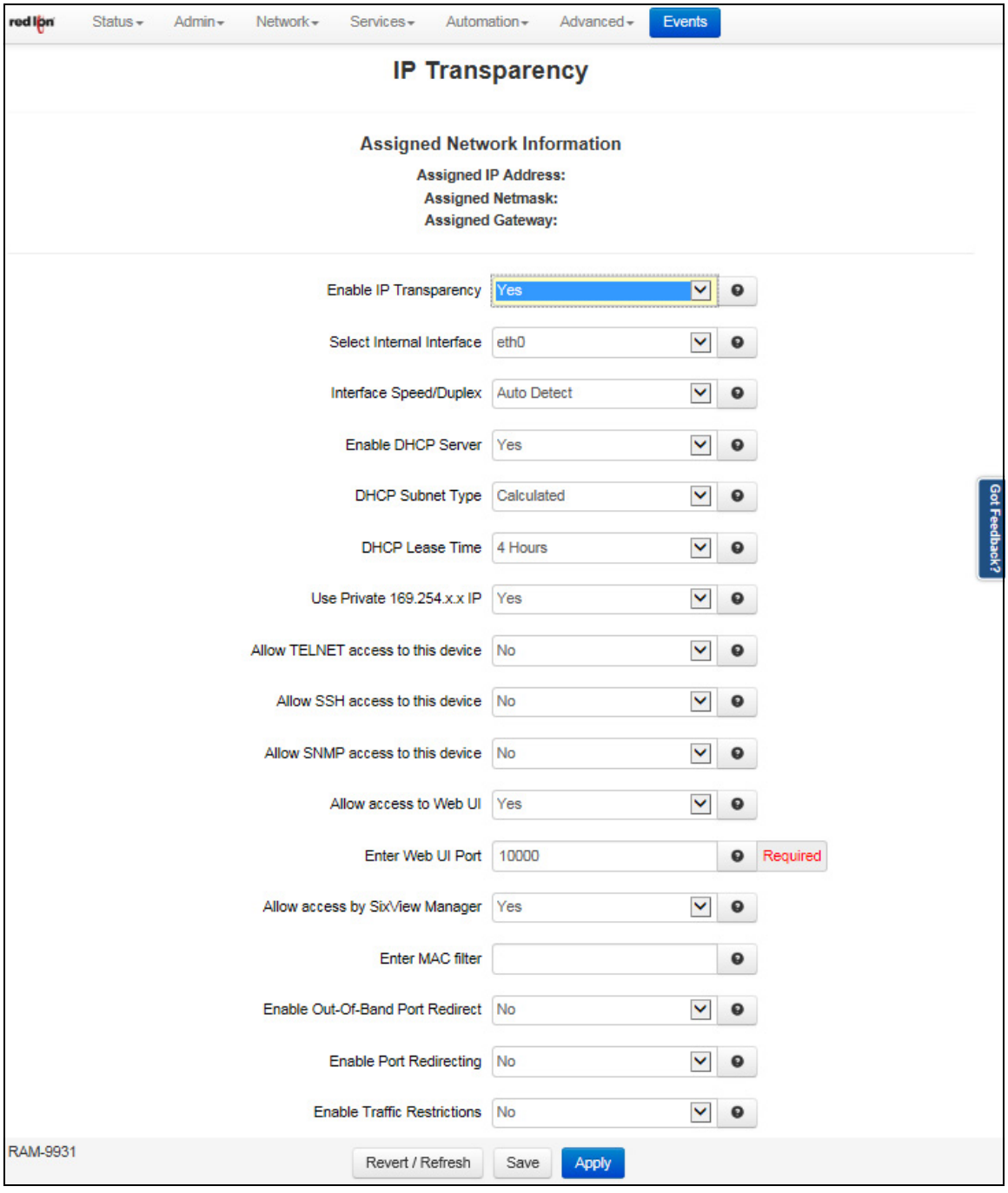
To revert to the previous defaults, click on the *Revert* button.

3.7.2 IP Transparency

IP Transparency is supported on Red Lion RTUs or routers. The IP Transparency menu item is used to configure the transparent bridging capability of the Red Lion RTU or router.

IP Transparency is a special use capability. IP Transparency will take all inbound traffic to the Red Lion RTU or router and pass it transparently through to the interface specified. This is useful when it is desired to pass traffic to a legacy firewall, or VPN concentrator located behind the Red Lion RTU or router and not to use the firewall or VPN capabilities of the Red Lion RTU or router itself.

Click on the *IP Transparency* menu item and the IP Transparency dialog window appears:



Enable IP Transparency: Select Yes to enable the IP Transparency feature. Settings will take effect immediately when the Apply button is clicked or after a reboot when Save is clicked. Note: Enabling IP Transparency will negate all configured firewall rules. The firewall and DMZ Host services will be disabled prior to using IP Transparency.

Select Internal Interface: Select the interface to be designated the “internal” interface by making the appropriate choice from the provided list. The wireless IP will be issued out of this interface.

Interface Speed/Duplex: Select the Speed and Duplex to be used for the physical interface. The recommended setting for this field is *Auto-Detect*. The following options are available:

- **Auto Detect:** Use the ‘best negotiated’ speed and duplex (default)
- **10 Mbps/Half:** Force the interface to 10 Mbps and half-duplex
- **100 Mbps/Half:** Force the interface to 100 Mbps and half-duplex
- **100 Mbps/Full:** Force the interface to 100 Mbps and full-duplex

Note: An incorrect ‘forced’ setting will result in communication failure for this interface.

Enable DHCP Server: Select Yes to allow the DHCP Server(s) to be enabled while IP Transparency is in effect.

DHCP Subnet Type: A calculated subnet will be based on the actual IP Address received from the wireless network. This option is more compatible with a wide variety of RTUs or routers, but will mask out nearby IP addresses. This may make other IP’s within the host network unreachable. Point-to-Point uses a /32 subnet, but is not compatible with some RTUs or routers. The recommended setting for this field is *Calculated*.

DHCP Lease Time: Choose the time for DHCP Leases when issuing the Transparent IP. The recommended setting for this field is 4 hours.

Use Private 169.254.x.x IP: Select whether the internal IP Transparency interface will host a “dummy” gateway IP simulator to the IP Transparency IP, or if it uses a calculated 169.254.x.x IP Address. Some Cisco routers might not ARP properly when this option is turned on.

Pros: Option turned Off may allow some Cisco routers to ARP better.

Cons: With the option turned Off, the unit will black hole some IPs, and they will not be reachable from the device behind. Example: IP from ISP is 1.2.3.3. Calculated Mask is 1.2.3.2/30. Now IPs 1.2.3.0, 1.2.3.1 and 1.2.3.2 become unroutable beyond the device.

Allow TELNET access to this device: Select Yes to allow TELNET access to this device. Incoming connections on the specified port will be directed internally to port 23, instead of to the device behind the specified Internal Interface. *Note: For this option to function properly, the TELNET Server must be enabled on port 23 via the Services tab.*

Allow SSH access to this device: Select Yes to allow SSH access to this device. Incoming connections on the specified port will be directed internally to port 22, instead of to the device behind the specified Internal Interface. *Note: For this option to function properly, the SSH Server must be enabled on port 22 via the Services tab.*

Allow SNMP access to this device: Select Yes to allow SNMP access to this device. Incoming connections on UDP port 161 will be directed internally to port 161 instead of to the device behind the specified Internal Interface. *Note: For this option to function properly, the SNMP Agent must be enabled via the Services tab.*

Allow access to Web UI: Select Yes to allow access (for incoming TCP Port 10000 connections) to the Web UI on this device. Selecting No allows the connection through to the device behind the selected interface. The recommended setting for this field is *Yes*.

Enter Web UI Port (Required): Enter the TCP Port number to be used for Web UI access when Web UI access has been enabled. The port chosen will be redirected locally (to internal 10000). Connections on this port number will not reach the device behind the specified Internal Interface. The recommended setting for this

field is 10000. All Web UI traffic will be redirected locally to port 10000 automatically. This behavior is built-in and not configurable.

Allow access by SixView Manager: Select *Yes* to allow access (for incoming TCP Port 7785 connections) to trigger this device for remote check-in by the SixView Manager server. Selecting No allows the connection through to the device behind the selected interface. The recommended setting for this field is *Yes*.

Enter MAC filter: Enter a valid MAC address using the following format: *nn:nn:nn:nn:nn:nn*, where *nn* is a number in hexadecimal form (0-9, a-f, A-F) to enable a MAC filter for use with IP Transparency. A MAC filter allows only packets whose MAC address matches the filter value to be passed thru this device. Leaving this field empty effectively disables MAC filtering.

Enable Out-of-Band Port Redirect: Select *Yes* to allow any Out-of-Band ports to be redirected locally to this device. When enabled, the OOB Ports specified in the Advanced→Out-of-Band Mgt section will be automatically allowed. The recommended setting for this field is *Yes*, when also configuring Out-of-Band Mgt on this unit.

Enable Port Redirecting: Select *Yes* to allow redirecting of ports to a device beyond this device (the one being configured). Example: A device beyond the IPT device is running a WEB server on port 80, but an upstream RTU or router is blocking Port 80. Redirecting traffic to another port, say 8080, allows communication with the server. This would be setup as our External port 8080 redirected to an Internal Port 80, Protocol TCP.

When this feature is enabled, a new field appears containing a table into which multiple entries can be entered. Each entry will include the External and Internal Port numbers and a traffic type (TCP or UDP).

Enable Traffic Restrictions: Select *Yes* to restrict traffic to a device beyond this device (the one being configured). When this feature is enabled, a Traffic Restrictions table appears to allow selection of the restriction mode and a table into which multiple entries can be entered. Each entry will specify the network IP address range to which the restrictions will be applied.

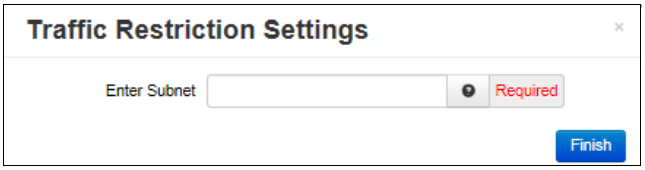
Enable Traffic Restrictions: This field is enabled when “Enable Traffic Restrictions” has been set to Yes. Select the restriction mode from the list provided.

None: No filtering is performed.

Only: Allow connections to/from the associated subnet list only. (Inbound and Outbound Restrictions)

In: Allow new incoming connections from the associated subnet list only, but allow any originating outbound connections from the host behind the Red Lion RTU or router. (Inbound Restriction)

Click on the *Add* button and the following window appears:



Enter Subnet (Required): Enter subnet range for which to restrict traffic in the CIDR form *nnn.nnn.nnn.nnn/xx*, where *nnn* is the IP Address and *xx* is the subnet in Network Bits format.

Click on the *Finish* button to populate the Table Restrictions screen.

To delete an existing item, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

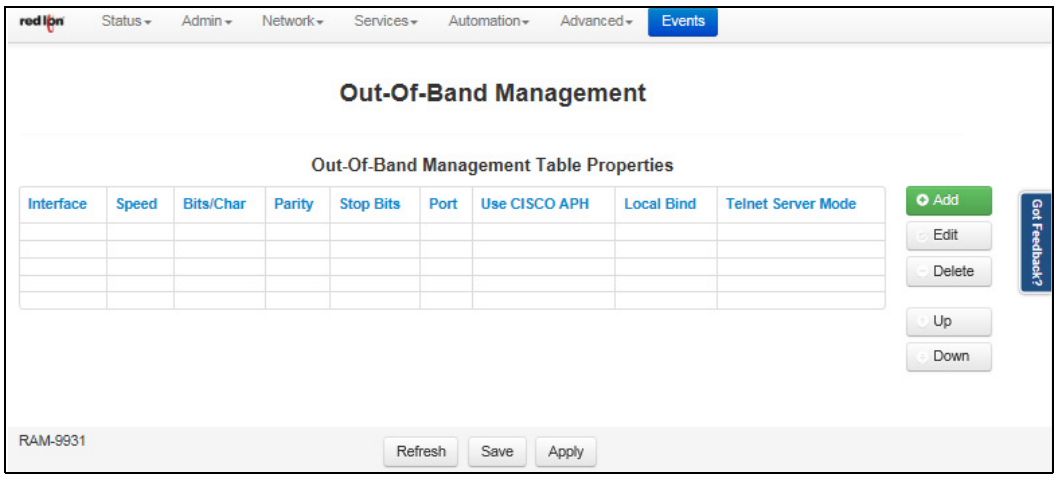
Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

3.7.3 Out-of-Band Management

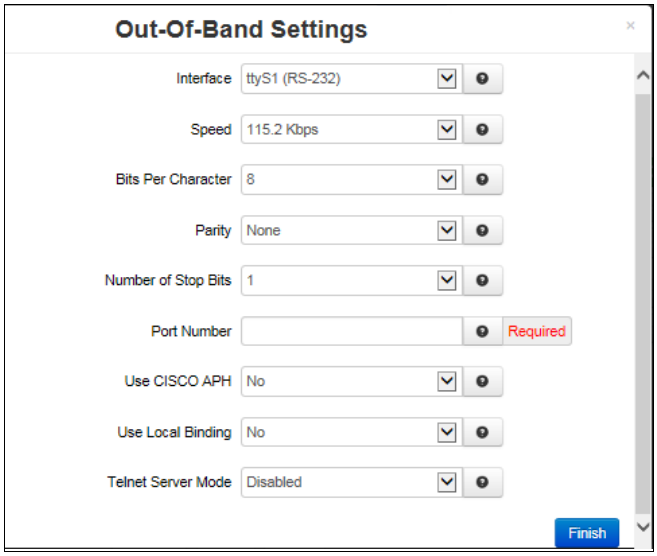
The Out-of-Band (OOB) Management menu item is used to configure the capability of remotely administrating a third-party device connected via a serial cable on the Red Lion RTU or router.

Note: Please refer to the third-party device user manual and/or technical support to determine what type of connection is required to connect with the Red Lion RTU or router from the RS-232 serial port.

Click on the *Out-of-Band Mgt* menu item and the following dialog window appears:



Click on the *Add* button to add an instance for OOB Management and the following window appears:



Interface: Select the interface to used.

Note: For Speed, Bits, Parity and Stop Bits, consult the configuration of the remote device being attached; this setting must be compatible.

Speed: Select the desired interface speed to be used.

Bits per Character: Select the word length (bits per character) to be used.

Parity: Select the parity to be used. Consult the configuration of the remote device being attached, this setting must be compatible.

Number of Stop Bits: Select the number of stop bits to be used. Consult the configuration of the remote device being attached, this setting must be compatible.

Port Number (Required): Enter a valid port number (1-65535) to be used for the connection.

Take care to choose a port number not already used by other system services. Consult the **Status→Network→Socket Statuses→TCP Only** menu for a list of ports currently in use. Please note that a Firewall Allow rule will need to be added for remote access in Network→Firewall→Port Allow/Forwarding Rules→Service Access Rules.

Use CISCO APH: Select *Yes* to enable the CISCO APH or *No* to prevent it's use. The recommended setting for this field is Yes when connecting to a Cisco console port.

Use Local Binding: Select *Yes* to enable Local Binding. Local Binding will prevent remote access to this port. You will be required to Telnet/SSH to the unit's command line, and then Telnet to the OOB port locally (telnet localhost<OOB Port>).

Telnet Server Mode: This option controls how some options negotiations will be performed with a TELNET client. Recommended setting is "Basic + drop LF & NUL" is a commonly utilized setting. The following options are available:

Disabled: No TELNET options negotiation is performed.

Basic: Common TELNET options negotiation is performed.

Basic + drop LF: Line feed characters (x'0A) are dropped.

Basic + drop LF & NUL (Cisco Preferred): LF and NUL (x'00) characters are dropped.

Basic + drop LF & NUL/HIGH: LF, NUL and any characters > x'7F are dropped.

Basic + drop CR: Carriage return characters (x'0D) are dropped.

Basic + drop CR & NUL: CR and NUL (x'00) characters are dropped.

Basic + drop CR & NUL/HIGH: CR, NUL (x'00) and any characters > x'7F are dropped.

Note: Selecting the right value for your particular situation may require some experimentation.

The Basic Telnet Server will enable some telnet negotiation options with common Telnet Clients, which may provide a better user experience. If you are having problems with odd echoed characters, or other interactive problems, please enable this option.

If you are having problems with login not accepting your password, or pressing "Enter" seems to behave as if two Enter keys have been pressed, try one of the "Drop" options.

Click on the *Finish* button to populate the Out-of-Band Management screen.

To delete an existing item, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

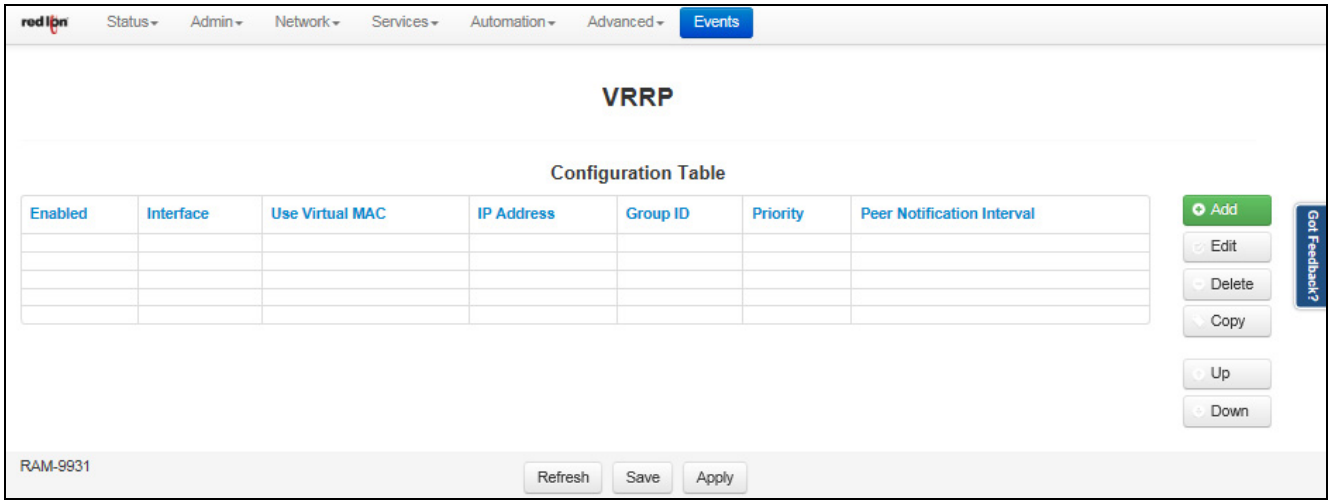
Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

3.7.4 VRRP (Virtual Router Redundancy Protocol)

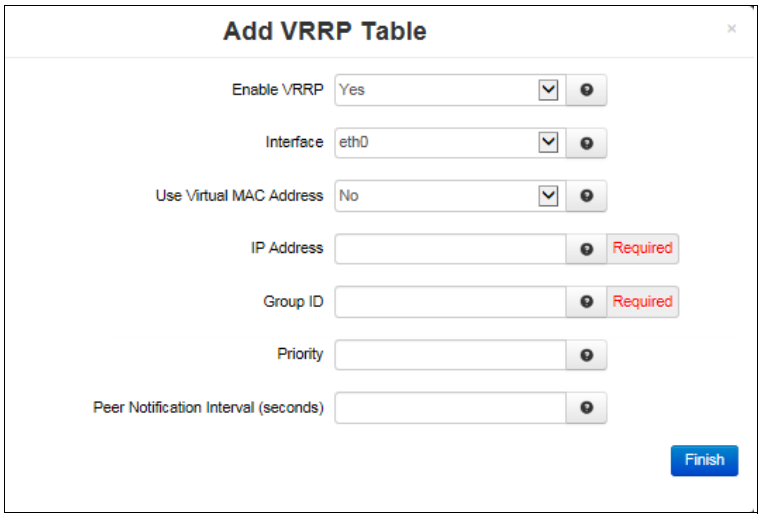
To configure VRRP, select the option from the Advanced menu.

The VRRP menu item allows you to configure the capability of providing redundancy capabilities to each other as well as other third party devices.

Click on the *VRRP* menu item and the following dialog window appears:



Click on the *Add* button and the following dialog window appears:



Enable VRRP: Specify whether you want to enable the VRRP service on this device. The service will be started after clicking the Apply, and on each subsequent boot. VRRP is designed to work with multiple systems. Enable only if you intend to setup other VRRP partners.

Interface: Specify the interface the VRRP service should use for communication.

Use Virtual MAC Address: Specify whether you want to allow the VRRP service to use virtual MAC addresses with the shared IP. If set to No, the actual interface MAC will be used.

Recommended Setting

No – If you are using managed switches between the devices, the virtual MAC will confuse the loop detection. Many VRRP control packets will be dropped and status will bounce.

Yes – If you are not using managed switches, this mode will allow remote devices to reconnect faster to the backup unit in the event of an outage. This is because local ARP tables will not need to expire and reacquire different MAC addresses for the shared IP.

IP Address (Required): Specify the IP address of the virtual server. This value must not be currently assigned to any other network interface on the subnet. Furthermore, this value must match in any VRRP partner's configuration for redundancy to operate correctly.

Group ID (Required): Specify the ID number of the virtual server. This value must match in any VRRP partner's configuration for redundancy to operate correctly. Multiple VRRP Virtual interfaces can operate on the same subnet, as long as each set of redundant partners uses a different ID.

Priority (Required): Specify the priority to use in VRRP negotiations. Valid values are 1-255.

Note: If this is the "Master" device, the priority should be sent higher than the "Backup" device (255 is highest priority).

Peer Notification Interval (seconds): Specify the amount of time, in seconds, between VRRP broadcast packets.

Once you have entered the desired default settings for the VRRP, click on the *Finish* button and you will return to the VRRP dialog window. The Configuration Table will be populated with the information entered.

To modify settings, select the line to be edited and click the *Edit* button. To remove settings from the table, select the desired line and click on the *Delete* button.

Click *Save* to store the settings for the next reboot, or click APPLY for the settings to take effect immediately. Selecting *Revert*, will reset all fields to previously saved defaults.

3.7.5 Expert Mode

The Expert Mode menu allows you to edit the configuration fields of Red Lion SN/RAM 6000 and RAM 9000 RTU or router directly. This option provides the ability to perform advanced configuration capabilities for complex organizations.

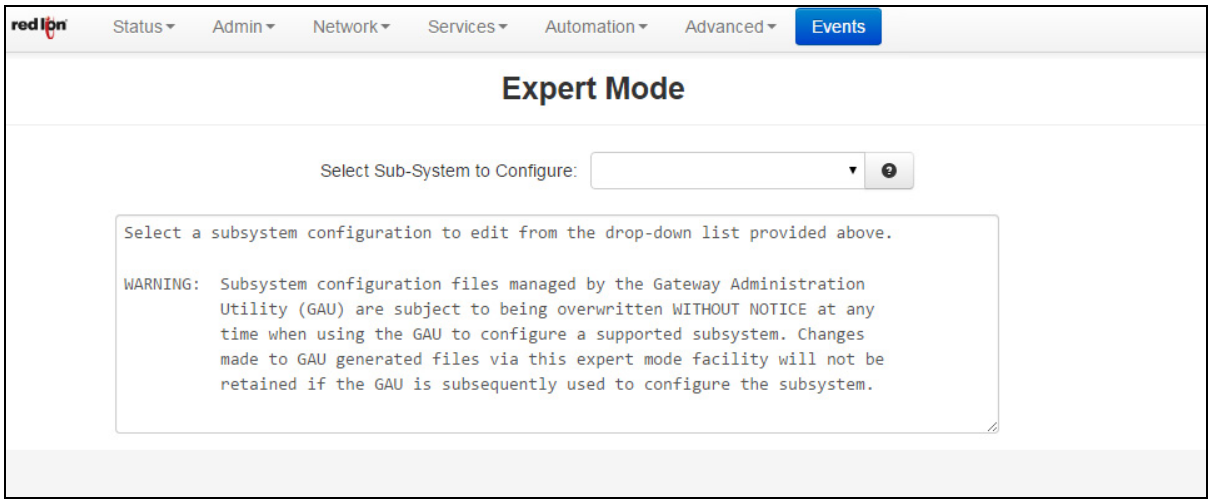
Note: Expert Mode is not recommended unless directed by Red Lion Technical Support.

Warning: Should you choose to edit the configuration files directly, we encourage you to contact Red Lion Technical Support. Once you have manually edited a configuration file without the use of the Web UI, you should refrain from any further configurations to that subsystem through the Web UI, as it will overwrite any changes you may have made.

Configure Sub-Systems

The “Configure Sub-Systems” menu item allows you to edit the main configuration files of the Red Lion RTU or router. It is not recommended that you perform configuration activities using this facility unless instructed to do so by Red Lion Technical Support.

Click on the *Configure Sub-System* menu item and the following window appears:



Select Sub-System To Configure: Select a component sub-system from the list as directed by Technical Support. Your choice will load the given sub-system’s configuration file into the text box for editing. The following controls (buttons) are available:

Cancel: Reload the file in the text box, removing all unsaved changes.

Default: Load a default file in to the text box for editing. All changes to the defaults file will be reflected in the “real” (rather than the default) configuration file.

Save: Save the contents of the text box in to the “real” sub-system configuration file.

Stop: Stop the component sub-system service if it is currently running.

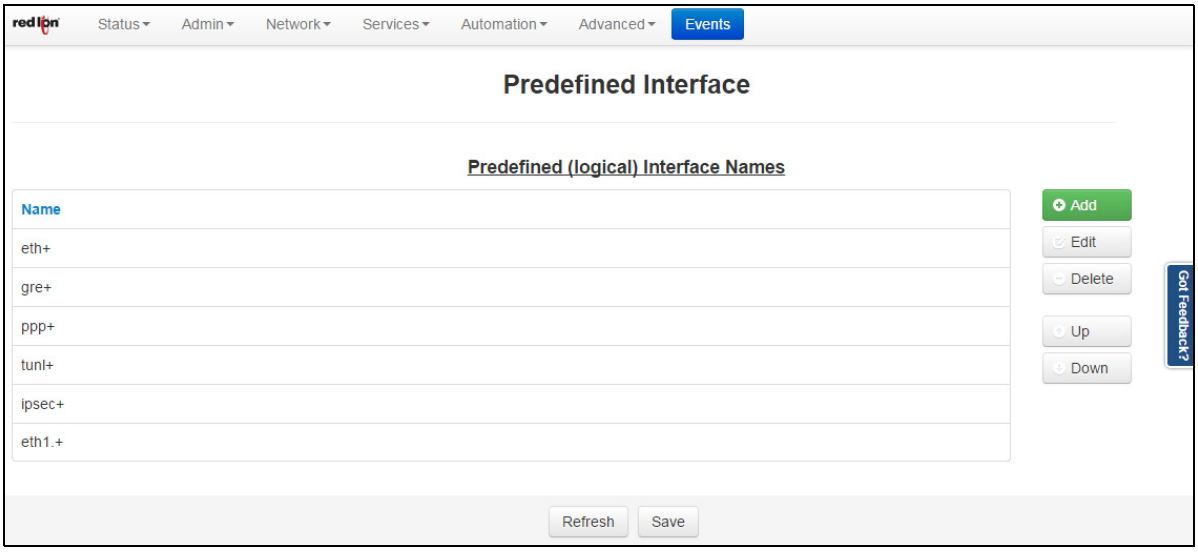
Start: Start the component sub-system service, or re-start it if it is currently running. Some may need a Stop first.

Predefined Interface

The Predefined Interface Names menu item allows you to create a named interface for use in applications such as OpenVPN that require a logical interface, i.e. tun0 that the Red Lion does not know about. Using the Predefined

Interface Name will place the name of the interface into the pull-down menus of interface selections to be used by the system.

Click on the *Predefined Interface Names* menu item and the following dialog window appears:



Click on the *Add* button to add a named interface and the following pop-up window appears:

Enter (logical) Interface Name (Required): Enter the name of the interface to be used for the logical interface. For example: tun0, gre4, ppp100, etc.

Click on the *Finish* button to populate the Predefined Interface Names screen.

Click *Save* to store the settings for the next reboot. Selecting *Revert*, will reset all fields to the previously saved defaults.

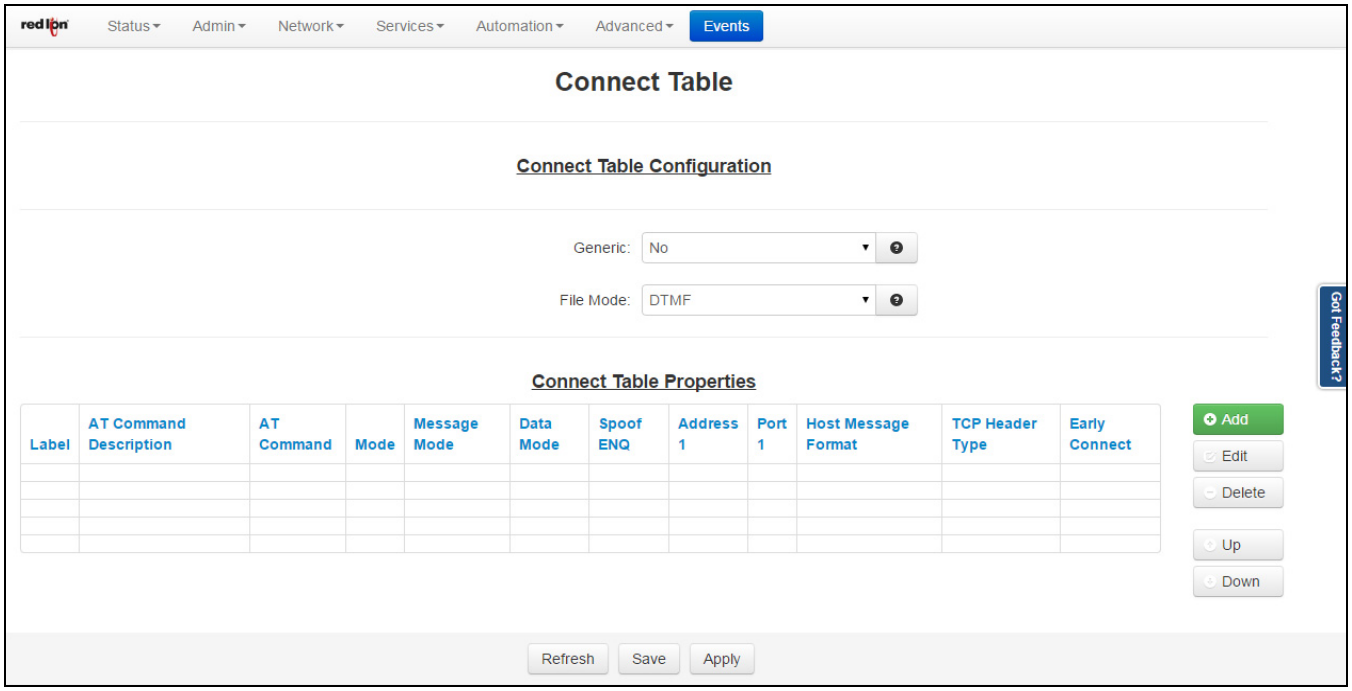
3.7.6 GWLNX

The GWLNX menu item is used to define the following sub-menus: Connect Table Configuration, Install Configuration, Install Application, IP Destinations, CLI Status, GWLNX Status and GWLNX Log.

Connect Table Configuration

The Connect Table Configuration menu item is used to configure the communication ports behavior via Serial or Modem using Dialed Number Identification Service (DNIS) method.

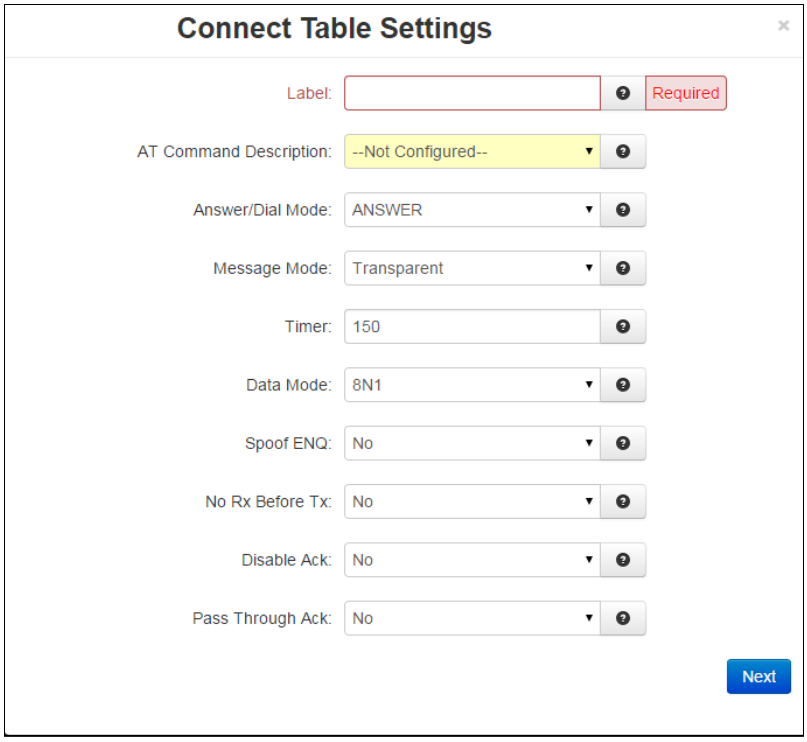
Click on the *Connect Table Configuration* menu item and the following dialog window appears:



Generic: Please use the recommended setting unless directed to change by Red Lion Technical Support. The recommended setting for this field is No.

File Mode: Please use the recommended setting unless directed to change by Red Lion Technical Support. The recommended setting for this field is DTMF.

Connect Table Properties: To create a table setting, click on the *Add* button and the following dialog window appears:



Label (Required): Enter the Lookup Key associated with this entry. This is commonly a phone number, or a portion of a phone number for partial matches of incoming calls. (i.e. “18” will match 1-800-xxx-xxx, 1-888, 1-866 and similar numbers.) The recommended setting for this field is 1001.

A value of “default” will designate this entry as the option to use if no other entry matches. If no “default” label exists, the first entry in the list will be the default and match any incoming number received.

For a Dial/Ring-Out Mode, this field should match the phone number entered in the Com Port Manager configuration for GWLNX TCP Server port number, if using a dynamic TCP Listening Port.

AT Command Description: The best choice is often determined by previous testing with a particular model/ brand of connecting device. The first three “Direct” options are the most commonly used. The recommended setting for this field is Direct 1200 Bell212 = At&Q6+MS=B212

If choosing a User Defined option, enter the full AT command. Below is a list of AT Commands:

- Direct 1200 Bell212 = AT&Q6+MS=B212
- Direct 1200 V22 = AT&Q6+MS=V22
- Direct 2400 V22bis = AT&Q6+MS=V22B
- Direct2 1200 Bell212 = AT\NO+MS=B212
- Direct2 1200 V22 = AT\NO+MS=V22
- Direct2 2400 V22bis = AT\NO+MS=V22B
- ErrorC 1200 Bell212 = AT\N3+MS=B212
- ErrorC 1200 V22 = AT\N3+MS=V22
- ErrorC 2400 V22bis = AT\N3+MS=V22B

Answer/Dial Mode: For incoming calls, choose “ANSWER_2WAY_RAW”. For outbound (Ring Out/Ring Down) mode, choose “DIAL”. The other options should only be used if instructed to do so by Red Lion Technical Support. The recommended setting for this field is ANSWER_2WAY_RAW.

Message Mode: This will choose between enabling the local VIsa protocol engine or allowing Passthru/ Transparent mode. The recommended setting for this field is Transparent.

Transparent: Allow raw communication between the Dial port and the TCP Connection.

Visa: Enable local Visa I engine. This will process one transaction, and issue an EOT after the transaction response has been sent to the dial device.

Visa2: Enable local Visa II engine. After a transaction is complete and ENQ will be issued to query the next transaction in sequence. If there is no response to the ENQ, then an EOT is issued.

Timer: Transparent Mode is the inter-character delay (in milliseconds) used on the serial side to determine when a remote device is finished transmitting. A low value may generate a faster response, but can send many TCP packets and 'fragment' the serial data packets. A higher value will collect a larger amount of data into a single TCP packet, and will generally keep packet boundaries more intact. Visa mode is unused. The recommended setting for this field is 150 for Transactions and 10 for some Streaming Protocols (ATM Management Protocols).

Data Mode: The following data mode is supported:

8N1: Data will be treated as full 8 bits valid. If the serial device is transmitting 7E1, then 7E1 formatted data will be transmitted to the TCP side.

7E1: Process data as if in 7E1 format. If the serial device is transmitting 7E1, then appropriate parity will be stripped/added so that communication on the TCP side will be in 8N1.

The recommended setting for Transparent mode: As needed for various serial devices and TCP hosts.

The recommended setting for Visa mode: Leave this setting at 8N1. Automatic 7E1 detection is used.

Spoof ENQ: The recommended setting for this field is *No*.

Transparent Mode: This will enable an ENQ packet to be sent to the serial device to initiate a transaction. Up to 5 ENQ's will be sent while waiting.

Visa Mode: Unused. The Visa engine will automatically issue ENQ's as needed, according to the GWLNX config file.

No Rx Before Tx: Discarding data before transmitting in supported Message Mode. The recommended setting for this field is *No*.

Transparent Mode: This will discard any data received from the serial side, prior to transmitting some data to the remote serial device. This can be useful to discard initial line noise remnants from modem connections before an ENQ is issued (or other start-data message types from a TCP host).

Visa Mode: Unused. This is automatically enabled in the Visa engine, as it awaits a STX.

Disable Ack: Acknowledgement behavior in supported Message Mode. The recommended setting for this field is No.

Transparent Mode: Unused.

Visa Mode: Once a message is received from the serial device (ATM/POS) and the LRC is valid, this will disable sending an ACK. Certain ATP/POS devices will fail if sent an ACK, and rather use the response message from the TCP host as an implied ACK. Certain ATM/POS devices require an ACK before receiving the response message from the TCP host.

Pass Through Ack: Passing Acknowledgment in supported Message Mode. The recommended setting for this field is No, unless using a SmartConnect device at the host processing side.

Transparent Mode: Unused.

Visa Mode: When an ACK is received from an ATM/POS device, pass that up to the host processor.

Enter IP Address 1 (Required): For coordination with SSL Connections, use 127.0.0.1. When using ANSWER mode, this is a Client Primary IP address that GWLNX uses to connect to the Host server. When using DIAL mode, this field is not used.

Enter Port 1 (Required): This is a Client Primary Port address that GWLNX uses to connect to the Host Server Port. For coordination with SSL Connections, this field should match the "TCP Listening Port" configured in Services→SSL Connections→SSL Client, to reach the specified remote SSL Host Server.

When using DIAL mode, and GWLNX is configured for Dynamic TCP Server Listener Port, this field will specify the TCP Port to listen on.

The recommended setting for this field is 1000.

Enter IP Address 2: This is a Client First Alternative IP Address that GWLNX uses to connect to the Host Server.

Enter Port 2: This is a Client First Alternative Port Address that GWLNX uses to connect to the Host Server Port.

Enter IP Address 3: This is a Client Second Alternative IP Address that GWLNX uses to connect to the Host Server.

Enter Port 3: This is a Client Second Alternative Port Address that GWLNX uses to connect to the Host Server Port.

Host Message Format: Following are the host message formats in supported Message Mode. The recommended setting for this field is Default.

Transparent Mode: Unused.

Visa Mode: This describes the format expected by the TCP host processor of Visa transactions. Visa Messages from the AMT/POS device will conform to: STX - PAYLOAD - ETX - LRC

Default: Use the current settings in the GWLNX configuration.

Payload Only: Strip Visa header/trailers. Send only the Payload.

Payload - ETX: Strip the Visa header and LRC block check.

STX - Payload - ETX - LRC: Strip only the LRC block check.

STX - Payload - ETX - LRC: Send the fully formatted Visa message.

Header Type: The TCP connection to a host may required length headers. This will optionally be prepended to the data received from the serial side, for either transparent or Visa Mode. The recommended setting for this field is *Default*.

Default: Use current GWLNX configuration.

None: Use no headers.

JBM Standard: Use JBM Standard Headers. This will prepend a Two Byte Length (2BL) Header to the data, indicating the number of bytes in the message, not including the header bytes. Messages from the host must also have the 2BL header to be received properly.

Example: With the Host Message Format set to STX-Payload-ETX, and just JBMSTD Headers used, the TCP message sent to the Host will be: XX XX STX Payload ETX. Where XX XX would be the length of the payload data, plus 2 (STX and ETX bytes). If Payload was 296 bytes, then the 2BL would be 01 2A (in Hex).

Allow Early Connect: Only adjust this option if directed by Red Lion Technical Support. The recommended setting for this field is *Yes*.

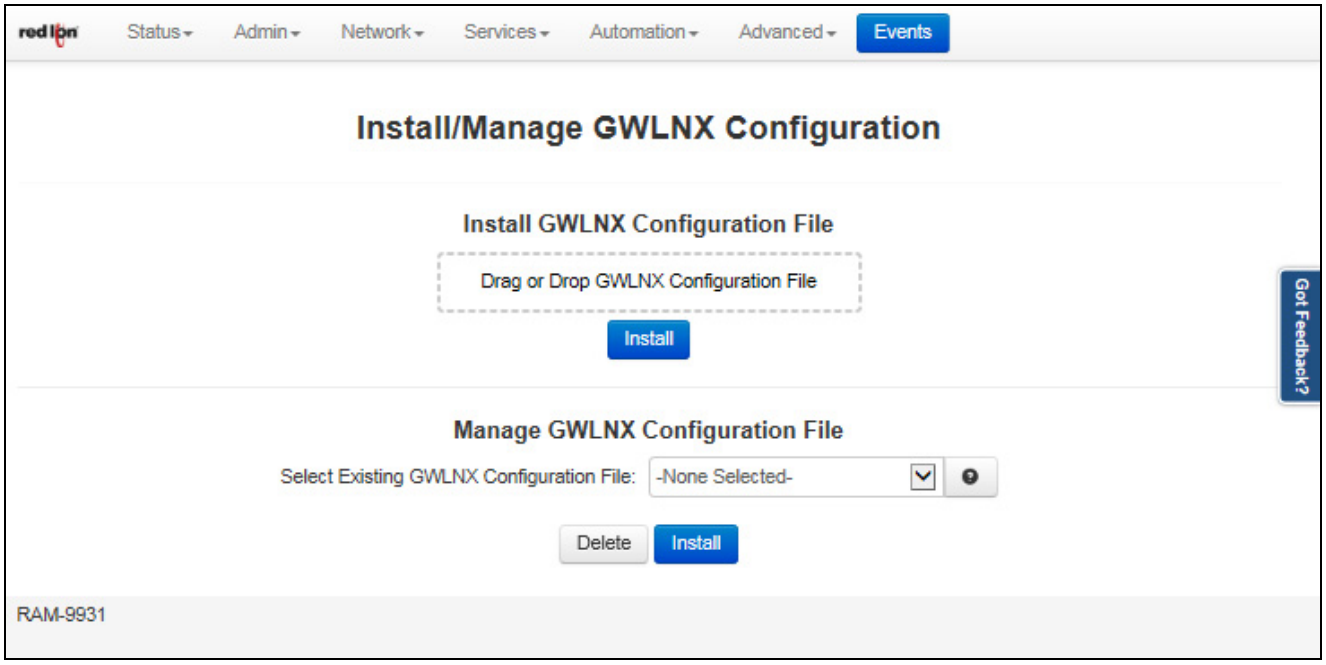
Click on the *Finish* button and you will be directed to the Connect Table dialog window and the Connect Table Properties table will be populated with the entered data.

Click on the *Save* button for changes to be saved without activating the interface, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

Install Configuration

The Install Configuration menu item is used to install the new GWLNX configuration on Red Lion RTU or router devices. The Manage Configuration section is used to install or delete GWLNX configuration files that already reside on Red Lion RTU or router devices.

Click on the *Install Configuration* menu item and the following dialog window appears:



Install GWLNX Configuration File:

Select GWLNX Configuration File: Click the 'Drag or Drop GWLNX' box to select a GWLNX configuration file to upload from your local system. You can also drag and drop a file into this box for uploading. It is recommended that you do not upload new files unless directed by Red Lion Technical Support.

Manage GWLNX Configuration File:

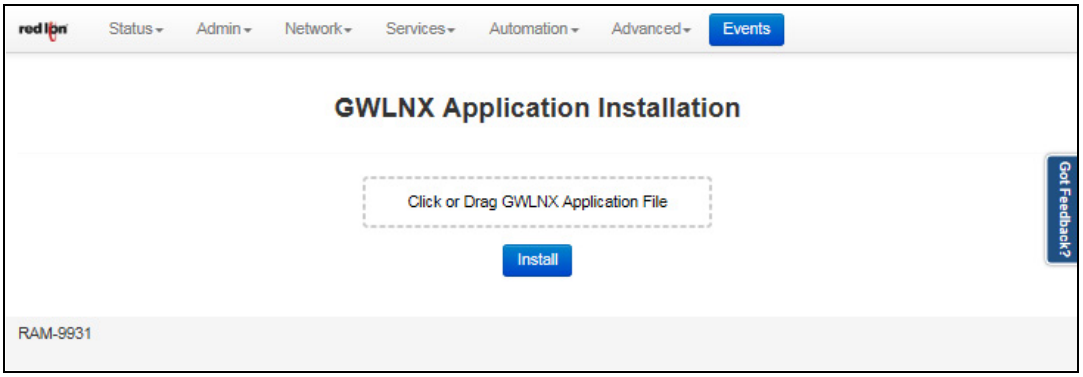
Select GWLNX Configuration File: Select a GWLNX configuration file on the remote unit to install or to delete. It is recommended that you do not install or delete files unless directed by Red Lion Technical Support.

Warning: Deleting the 'unit.cfg' file may result in the 'gwlnx' application from not running on the next restart.

Install Application

The Install Application menu item is used to install a new GWLNX application on Red Lion RTU or router devices.

Click on the *Install Application* menu item and the following dialog window appears:

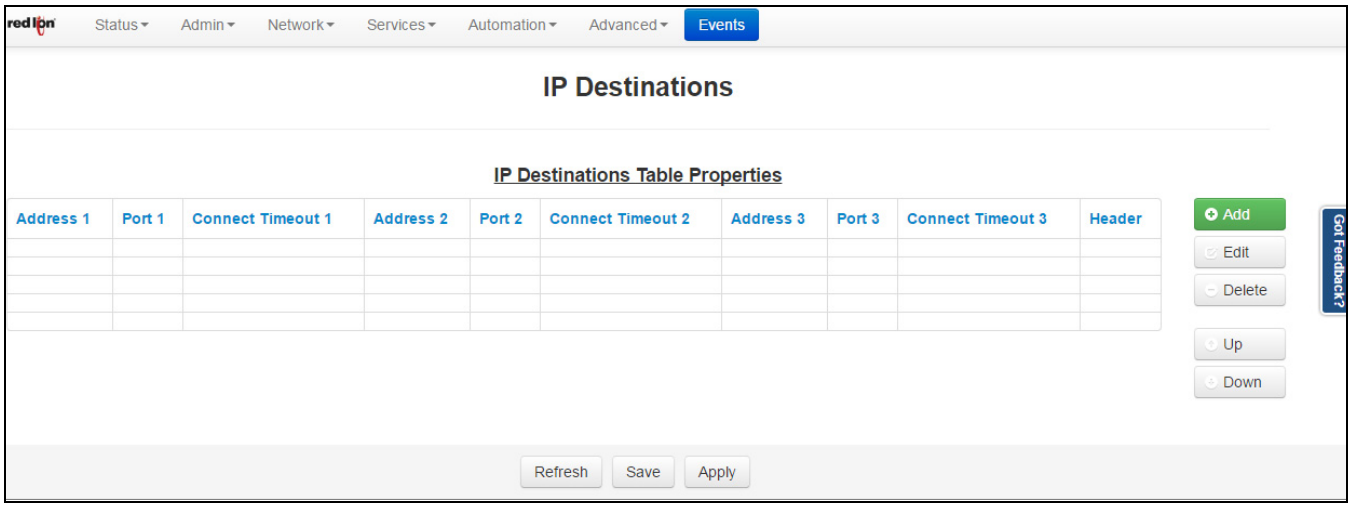


Click on the upload box or drag and drop your GWLNX installation file on the file upload box to select a GWLNX zip file to upload from your local system. It is recommended that you do not upload files unless directed to do so by Red Lion Technical Support.

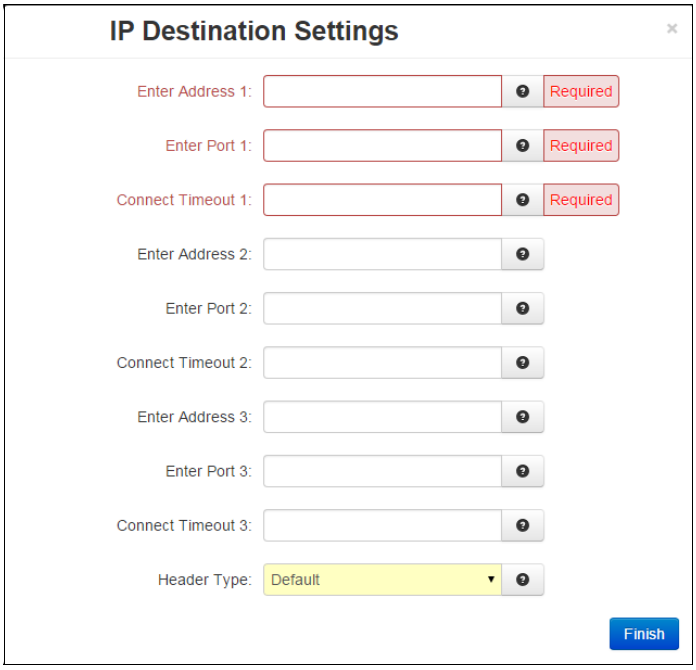
IP Destinations

The IP Destinations menu item is used to configure the host processor (Server) IP/Port Addresses that GWLNX application uses for TCP/IP communication protocol.

Click on the *IP Destinations* menu item and the following dialog window appears:



Click on the *Add* button to define IP Destination Settings.



Enter Address 1 (Required): This is a Client Primary IP Address that GWLNX uses to connect to the Host Server.

Enter Port 1 (Required): This is a Client Primary Port Address that GWLNX uses to connect to the Host Server Port.

Connect Timeout 1 (Required): Specify the time in seconds to attempt a connection to this TCP Destination, before declaring it unreachable. After the specified time, the next destination will be attempted. Valid range is 2 -250 seconds. The recommended setting for this field is 10 seconds. A value less than 10 seconds is not recommended for a wireless environment

Enter Address 2: This is a Client First Alternative IP Address that GWLNX uses to connect to the Host Server.

Enter Port 2: This is a Client First Alternative Port Address that GWLNX uses to connect to the Host Server Port.

Connect Timeout 2: Specify the time in seconds to attempt a connection to this TCP Destination, before declaring it unreachable. After the specified time, the next destination will be attempted. Valid range is 2 - 250 seconds. The recommended setting for this field is 10 seconds. A value less than 10 seconds is not recommended for a wireless environment.

Enter Address 3: This is a Client Second Alternative IP Address that GWLNX uses to connect to the Host Server.

Enter Port 3: This is a Client Second Alternative Port Address that GWLNX uses to connect to the Host Server Port.

Connect Timeout 3: Specify the time in seconds to attempt a connection to this TCP Destination, before declaring it unreachable. After the specified time, the next destination will be attempted. Valid range is 2 - 250 seconds. The recommended setting for this field is 10 seconds. A value less than 10 seconds is not recommended for a wireless environment.

Header Type: This is a Header Length used in TCPIP packet that contains the Message Length being Send or Receive. The recommended setting for this field is Default.

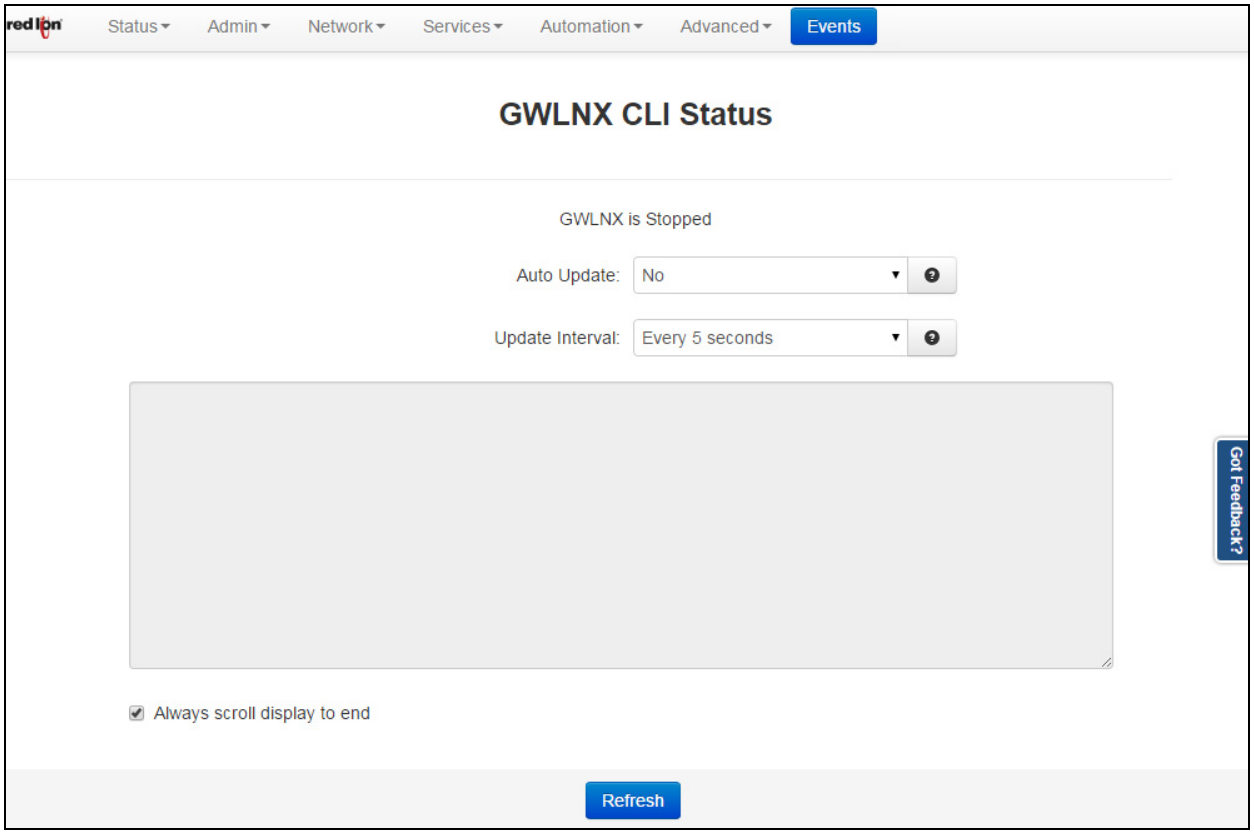
Click on the *Finish* button and you will be directed to the IP Destinations dialog window and the IP Destinations Table Properties will be populated with the entered data.

Click on the *Save* button for changes to be saved without activating the interface, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

CLI Status

The CLI Status menu item is used to view the status of the ports defined in the GWLNX configuration file if the GWLNX application is running.

Click on the *CLI Status* menu item and the following dialog window appears:



Auto Update: Select Yes to enable automatic updating of the log file display, the update interval can be selected using the Select Update Interval provided immediately below this control. Manual updating is disabled while auto-update is in effect. The current filter and maximum lines to be displayed will be used.

Be advised that when connected via a Cellular interface, the log file data collected will count towards your total data plan usage.

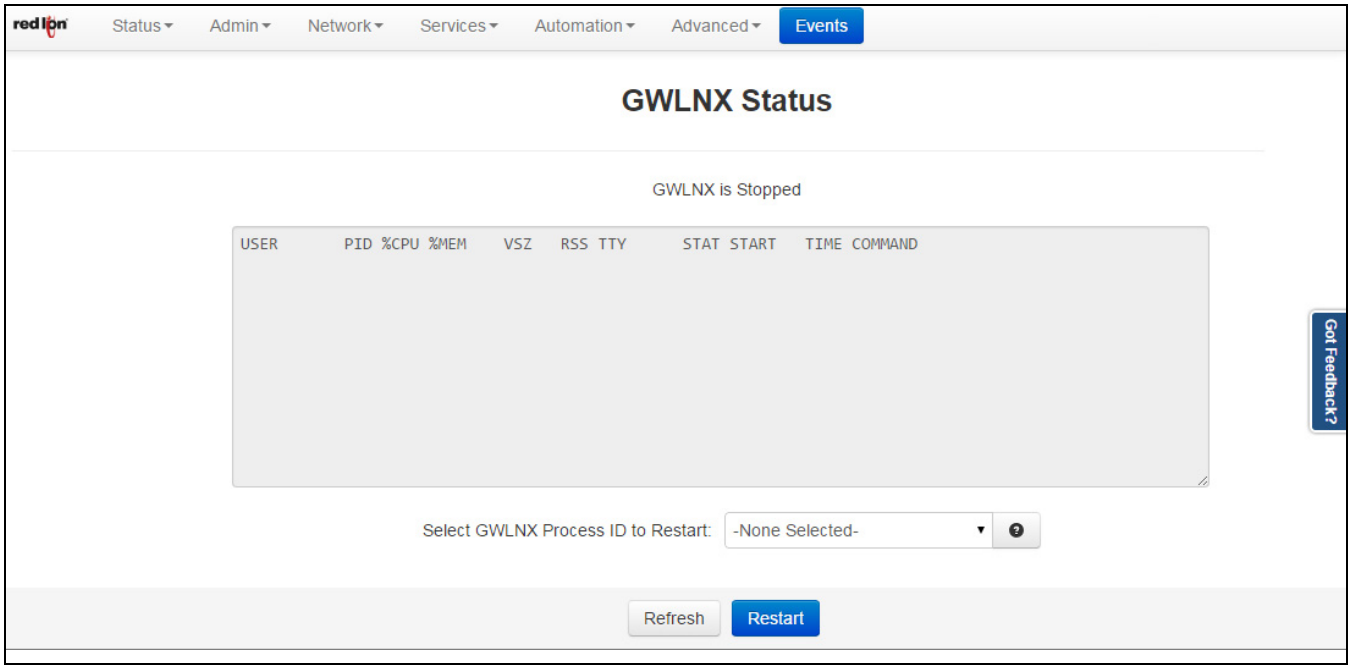
Update Interval: Select the update interval to be used when auto-update is enabled from one of the choices in the drop-down list provided. Choices (in seconds) include: 5, 15, 30 & 60.

Be advised that when connected via a Cellular interface, the log file data collected will count towards your total data plan usage.

GWLNX Status

The GWLNX Status menu item is used to view the GWLNX process ID and has the ability to restart the application by selecting the process ID from the provided drop-down list. The Refresh button will refresh the process ID, if the Gwnlx application has been restarted.

Click on the *GWLNX Status* menu item and the following dialog window appears:



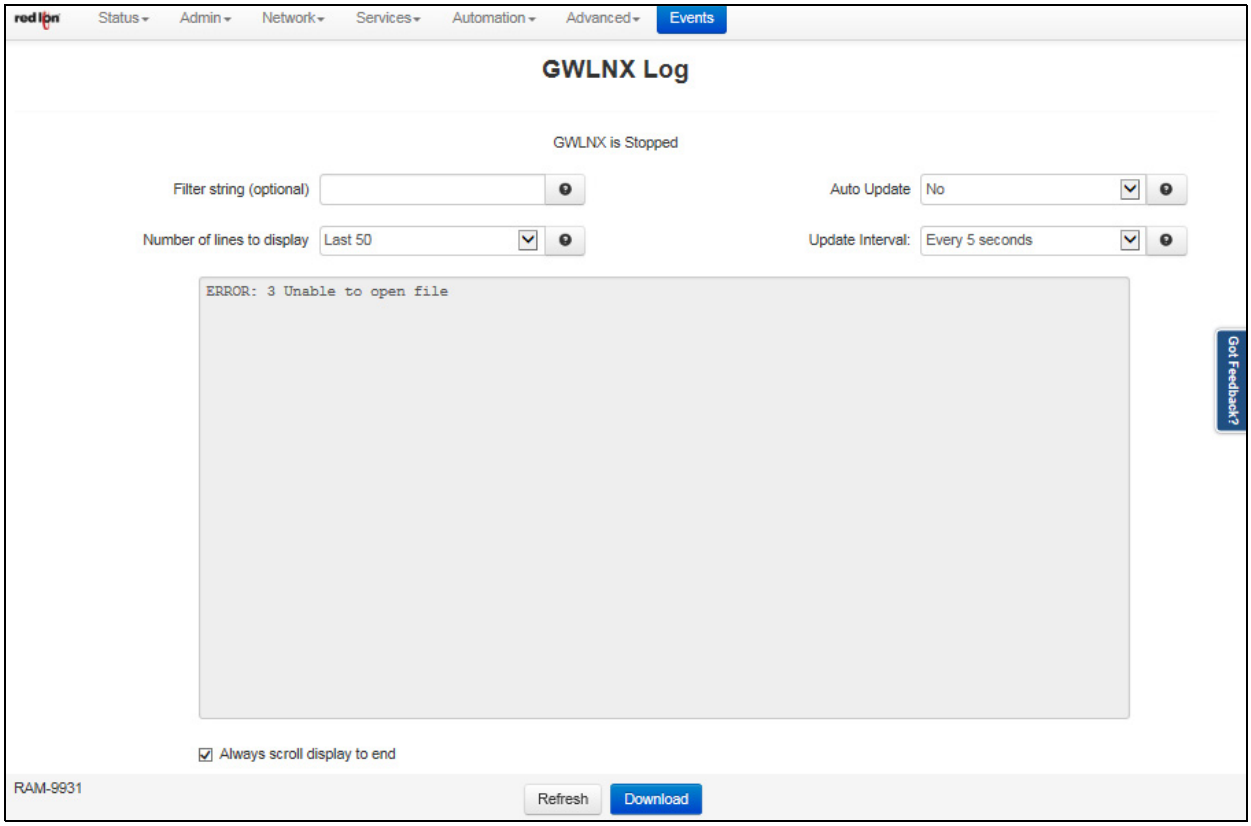
Select GWLNX Process ID to Restart: Select the GWLNX Process ID (PID) that you would like to restart.

Click on the *Restart* Button. This will restart the unit.

Gwnlx Log

The GWLNX Log menu item is used to view the logfile generated by GWLNX at startup, which provides the state of each port controller defined in the GWLNX configuration file and logs the Send/Receive traffics for each configured port controller.

Click on the *GWLNX Log* menu item.



Filter string (optional): Enter a filter string in the space provided, only lines containing the filter value(s) will be displayed via a 'grep' style filter mechanism. Note that the filter is case sensitive.

Number of lines to display: Select the number of lines to be displayed from one of the choices in the drop-down list provided. Choices include: 50, 100, 250, 500, 1000 & 2000.

> **Note:** Be advised that when connected via a Cellular interface, the log file data collected will count towards your total data plan usage.

Auto Update: Select Yes to enable automatic updating of the log file display, the update interval can be selected using the Select Update Interval provided immediately below this control. Manual updating is disabled while auto update is in effect. The current filter and maximum lines to be displayed will be used.

> **Note:** Be advised that when connected via a Cellular interface, the log file data collected will count towards your total data plan usage.

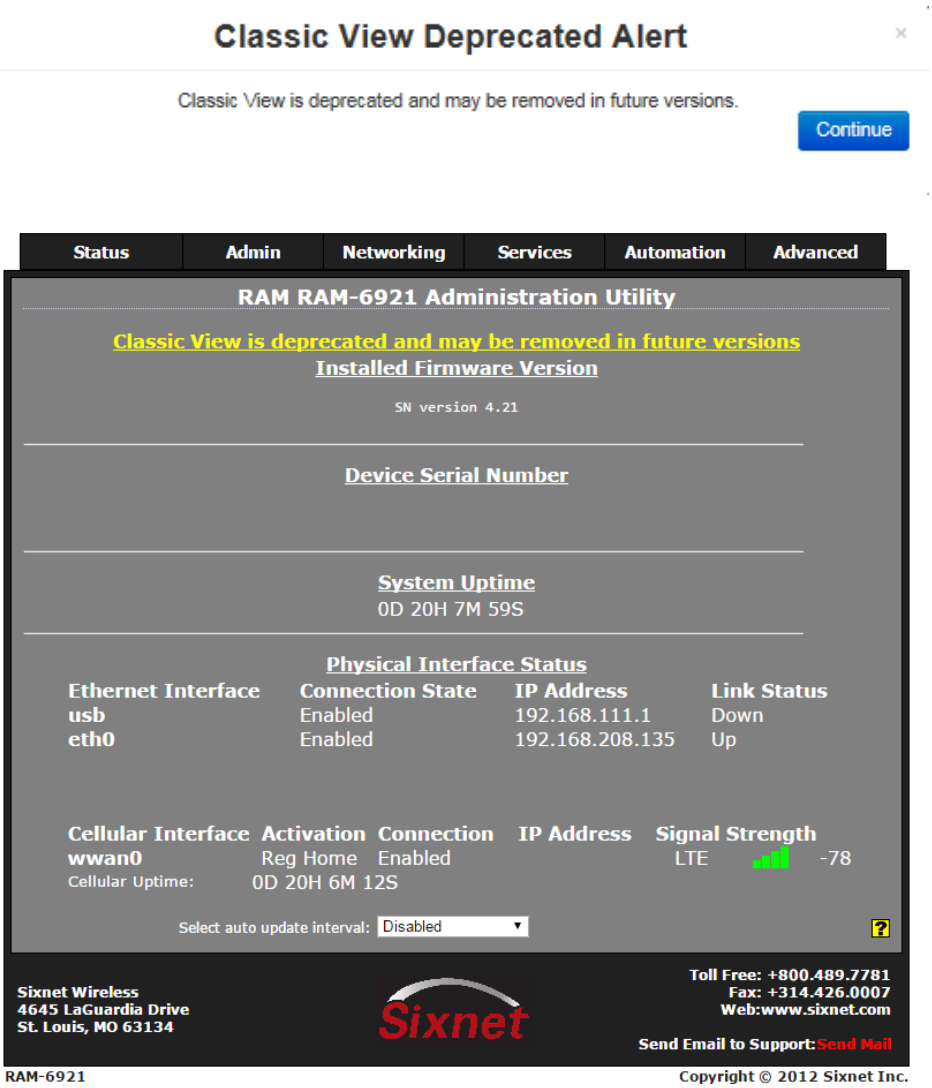
Update Interval: Select the update interval to be used when auto update is enabled from one of the choices in the drop-down list provided. Choices (in seconds) include: 5, 15, 30 & 60.

> **Note:** Be advised that when connected via a Cellular interface, the log file data collected will count towards your total data plan usage.

Click on the *Download* button to send the entire GWLNX logfile "logfile.txt" to your PC download directory. Click on the *Refresh* button to view the latest items being logged.

3.7.7 Classic View

Classic View is no longer actively supported or maintained as of Version 4.16. Not all features are available in Classic View that are present in the standard interface.



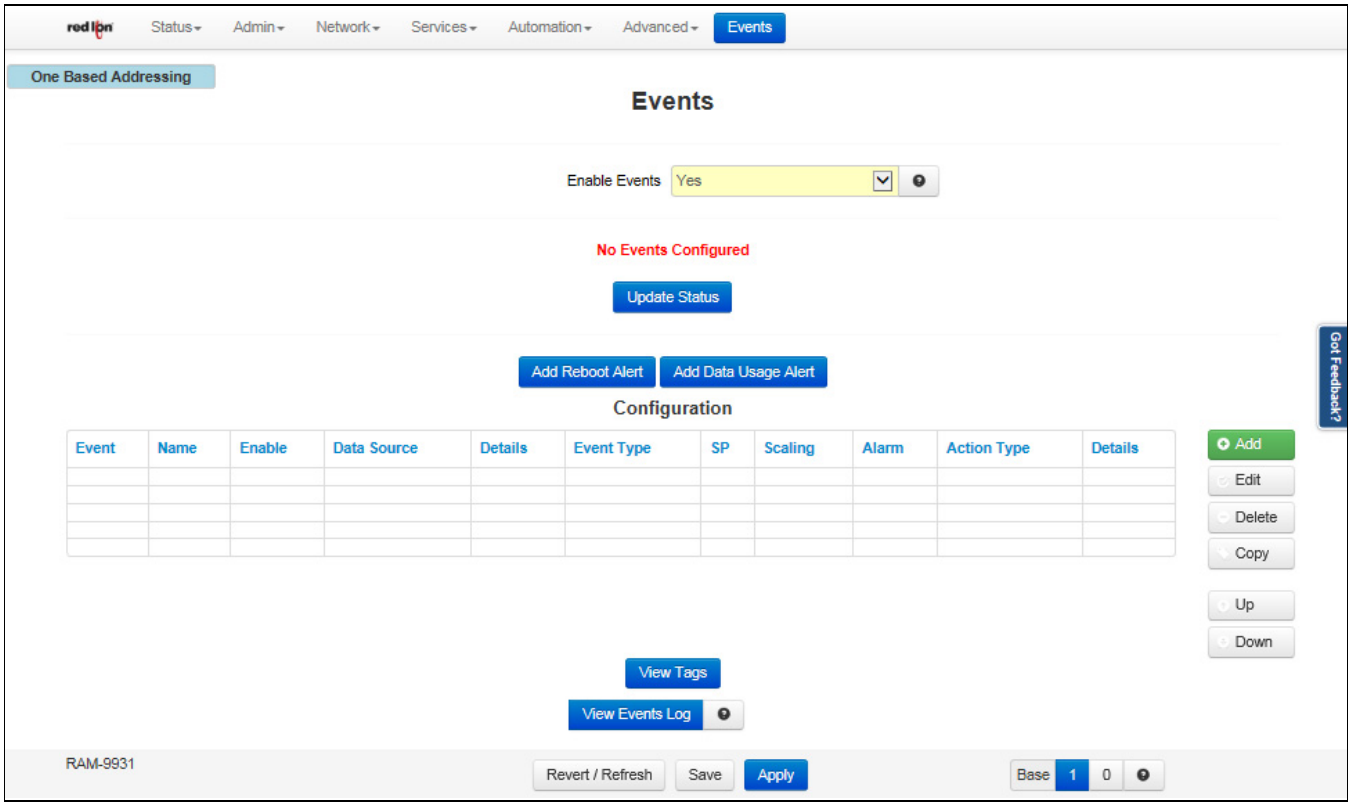
3.8 Events

Events are used to apply a series of logic checks to a register(s) that allows the user to program an action based on the content of a specific register. Properly configured events can identify when a tank level is too high or if the RSSI signal strength has deviated outside an expected range, then react by writing to a known output and/or status register.

Multiple events can be used to create more advanced logic or to create multiple stages of severity for alarms.

See Appendix B for a list of system status variables that are already established in the IODB. For example, events can be configured to watch these values and trigger actions based on when a reboot occurs (system uptime < 2 minutes), when a cellular link is down (wwan0 connected = 0), or when data traffic measured over a month exceeds a user's threshold.

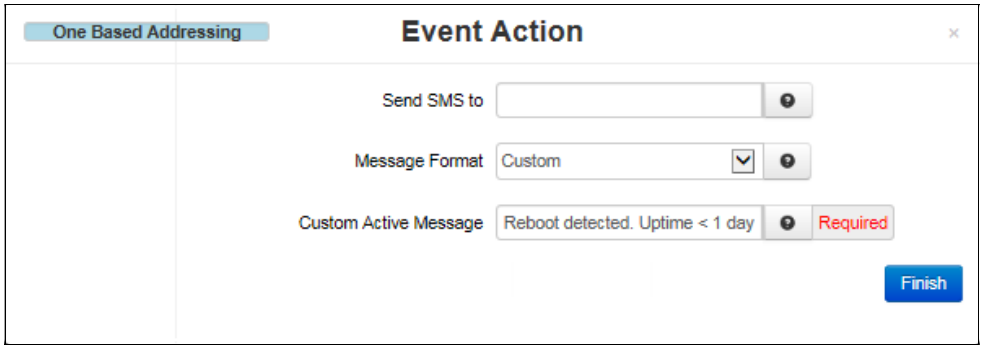
Note: Not all models have the same Events capabilities. Please call Red Lion Technical Support or your local representative for more details.



Enable Events: Select *YES* to enable the Events Control service. If *NO* is selected, all events will be disabled.

Update Status: Click the *Update Status* button to get a current event status.

Add Reboot Alert: Click on the *Add Reboot Alert* button to define parameters for reboot alerts.



Send SMS to (Required):

SMS Message: Enter a single phone number for the text message destination. Leading access numbers and area codes may be required based on the carrier, location, account type, and roaming status. Example: 1-555-555-1212, 0114185551212

Email Message: Enter an email address for the email message destination. Multiple email addresses may be entered by separating them with a comma. The email will come from the address configured in Services→Email Client. Example: username@email.com OR username@email.com,usergroup@email.com

Message Format: Define what type of content the Event alert message contains.

Standard: Send only the standard informational message.

Custom: Send only the custom message as specified. Tag values may be inserted as a variable by declaring the Tag Name framed in $. ie: $TAGNAME$.

Standard + Custom: Append up to a 60 character custom message to the standard message.

The Standard message will be constructed as follows:

EVT<Num>:<Name> <Cond> <Custom> Duration:<Time> DS:<DSValue> <Clear Condition>

Where

<Num> is the event number.

<Name> is the event name.

<Cond> is the current event condition or status, ACTIVE or INACTIVE.

<Custom> is the optional custom message specified by the user.

<Time> is the amount of time that the event has been active.

<DSValue> is the value of the Data Source that caused the event to activate or deactivate.

<Clear Condition> will indicate if the event "Will Auto Clear" on its own or if a "Manual Clear Required".

Note: Manual Clearing can be accomplished by clicking the Clear button on the Event Status page, or by writing a "1" into the Clear Condition register defined in IODB. See Appendix B.

The Data Source value will change depending on the type of Data Source configured for each event. When an Event Expression is used, a series of bits will indicated the True/False status of terms in the Event Expression. For example, if you had an expression like:

Evt1 | Evt2 | (Evt3 & Evt4)

You could get a message that would trigger with:

1000000000000

0100000000000

0011000000000

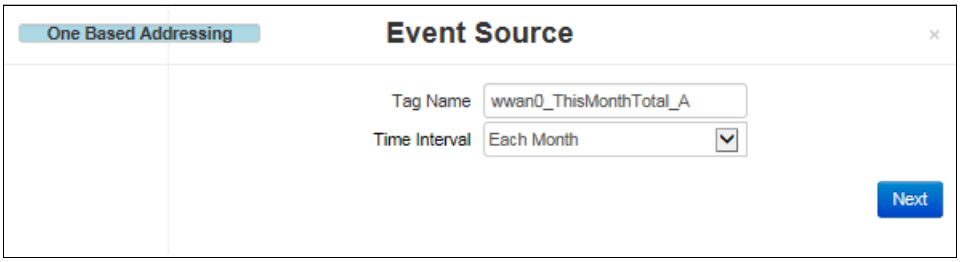
First Bit = the first event name in the expression, and so on.

Custom Active Message (Required): Enter a custom message when event goes active to be sent to the recipient. If appended to a standard message, the length is limited to 60 characters.

Click on the *Finish* button. You will return to the *Events* dialog window.

Add Data Usage Alert

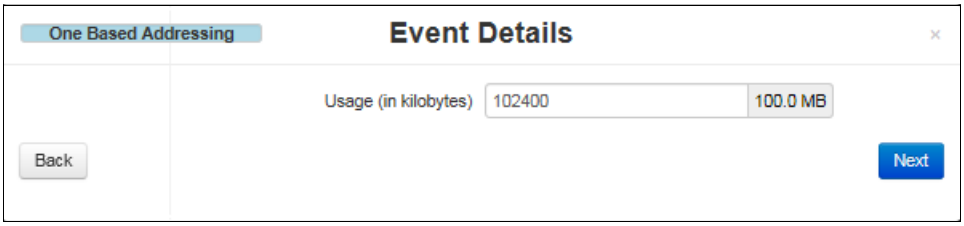
Click on the *Add Data Usage Alert* button to define parameters for data usage alerts.



Tag Name: Enter the tag name this Data Usage alert will be applied to.

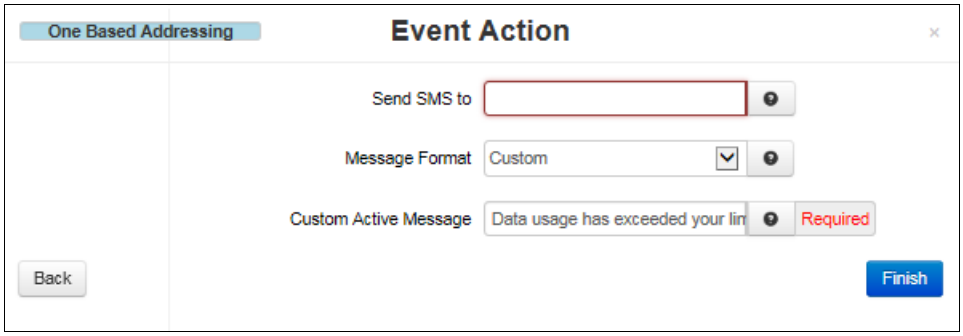
Time Interval: Select how often an alert is desired. The options are each month or each day.

Click on the *Next* button.



Usage (in kilobytes): Define what type of content the event alert will contain.

Click on the *Next* button.



Send SMS to (Required):

SMS Message: Enter a single phone number for the text message destination. Leading access numbers and area codes may be required based on your carrier, location, account type, and roaming status. Example: 1-555-555-1212 and 0114185551212.

Email Message: Enter an email address for the email message destination. Multiple email addresses may be entered by separating them with a comma. The email will come from the address configured in Services→Email Client. Example: username@email.com OR username@email.com,usergroup@email.com

Message Format: Define what type of content the Event alert message will contain.

Standard: Send only the standard informational message.

Custom: Send only the custom message as specified. Tag values may be inserted as a variable by declaring the Tag Name framed in $. ie: $TAGNAME$.

Standard + Custom: Append up to a 60 character custom message to the standard message.

The Standard message will be constructed as follows:

EVT<Num>:<Name> <Cond> <Custom> Duration:<Time> DS:<DSValue> <Clear Condition>

Where

<Num> is the event number.

<Name> is the event name.

<Cond> is the current event condition or status, ACTIVE or INACTIVE.

<Custom> is the optional custom message specified by the user.

<Time> is the amount of time that the event has been active.

<DSValue> is the value of the Data Source that caused the event to activate or deactivate.

<Clear Condition> will indicate if the event "Will Auto Clear" on its own or if a "Manual Clear Required".

Note: Manual Clearing can be accomplished by clicking the Clear button on the Event Status page, or by writing a "1" into the Clear Condition register defined in IODB. See Appendix B.

The Data Source value will change depending on the type of Data Source configured for each event. When an Event Expression is used, a series of bits will indicated the True/False status of terms in the Event Expression. For example, if you had an expression like:

Evt1 | Evt2 | (Evt3 & Evt4)

You could get a message that would trigger with:

1000000000000

0100000000000

0011000000000

First Bit = the first event name in the expression, and so on.

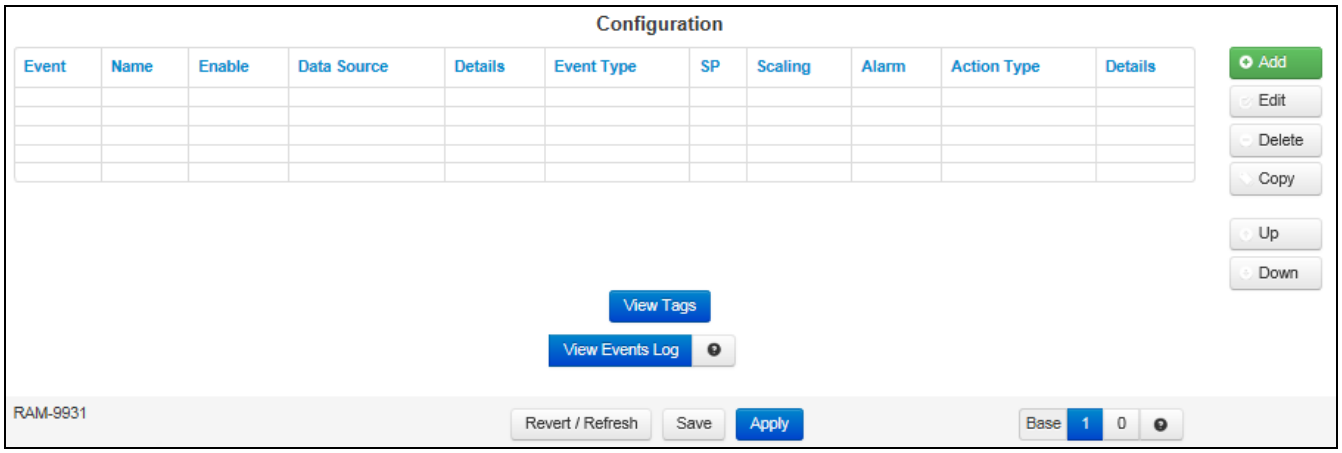
Custom Active Message (Required):

SMS Message: Enter a custom message when an event goes active to be sent to the recipient(s). If appended to a standard message, the length is limited to 60 characters.

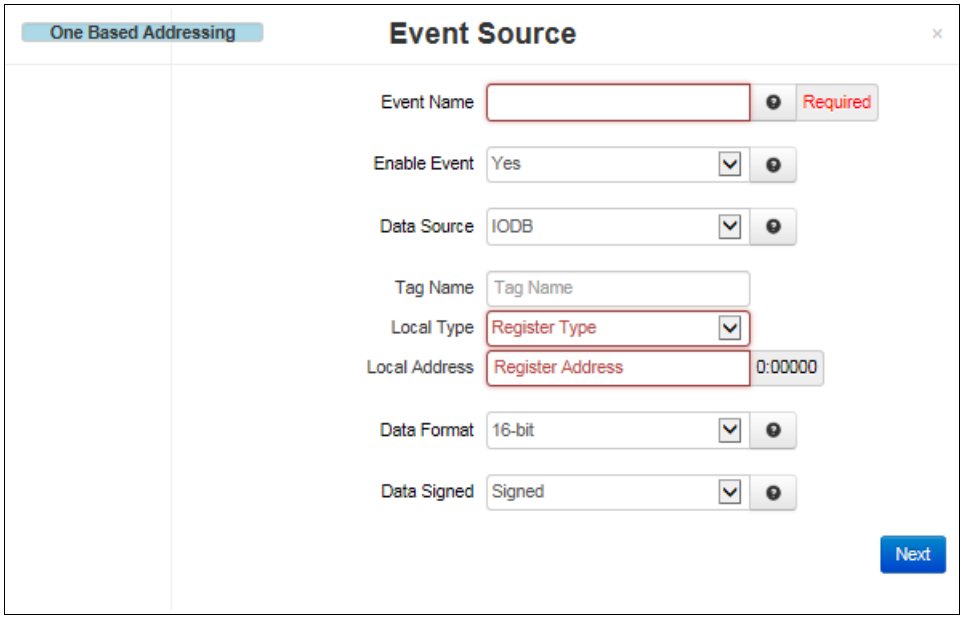
Email Message: Enter a custom message body that will be sent to the Recipient(s) when the event goes active.

Click on the *Finish* button. You will be returned to the *Events* dialog window.

Configuration



Click on the *Add* button and the Event Configuration dialog window appears:



Event Name (Required): Enter a unique name to describe this event. The value must be alphanumeric with at least one letter, and may not contain spaces or special characters.

This field will be used as an operand when building logical Event Expressions.

Enable Event: This controls whether the event will be evaluated at runtime or not. An event can be disabled without deleting it. Disabled events will always report their status as 0 or False and no action will be taken.

Data Source: Choose which data source to use for this event.

> **IODB:** Monitor a specific IODB register value to trigger the event. Any register that does not map to physical I/O is treated as a virtual register, simply stored in memory.
>
> **Event Condition:** This allows a logical Event Expression to be built from other events conditions. As other events change their status/condition between true and false, this information can be combined into a equation form. By combining multiple events, you can create complex actions based on multiple independent conditions.

Tag Name: This field will auto-populate when the user starts to type a tag name. Tag names are managed in Automation → Tags.

Local Type: The Local Type will auto-populate based on the Tag Name entered. These settings are pulled from the Tags dialog window located in Automation → Tags.

It may also be entered manually if no Tag has been defined for this type: Address.

Local Address: The Local Address will auto-populate based on the Tag Name entered. These settings are pulled from the Tags dialog window located in Automation → Tags.

The Local Address may also be entered manually if no Tag has been defined for this Type: Address.

Data Format: Choose how to treat the data stored in the location specified. Choosing a 32-bit or 64-bit data type will cause the following sequential registers to be appended. Big Endian is MSB first (also called Network Order), and Little Endian is LSB first.

Data Signed: Select whether to treat the data as an unsigned integer or two's compliment signed value.

Event Expression: If Event Condition is selected in the Data Source field, the Event Expression field appears.

The Event Expression is a logical equation built to combine the condition/status of multiple events into a single action. Other events will be referenced by their Event Name. These operands will evaluate those event's condition/status to be a 0 (false/inactive) or 1 (true/active).

There are 4 logical test operations that can be performed on the operands: Once the desired information has been selected, click on the NEXT button and the next dialog window appears:

NOT: Represented by the exclamation symbol (!)

AND: Represented by the ampersand symbol (&)

OR: Represented by the pipe symbol (|)

EQU: Represented by the equals symbol (=)

Examples:

EVT1 & EVT2 | EVT3 & !EVT4

!EVT1 & !(EVT2 || (EVT3 & EVT4)) | EVT5

$TAG1$ & $TAG2$ | $TAG3$ & !$TAG4$

!$TAG1$ & !($TAG2$ || ($TAG3$ & $TAG4$)) | $TAG5$

EVT1 & MyEvent | $TAGNAME$

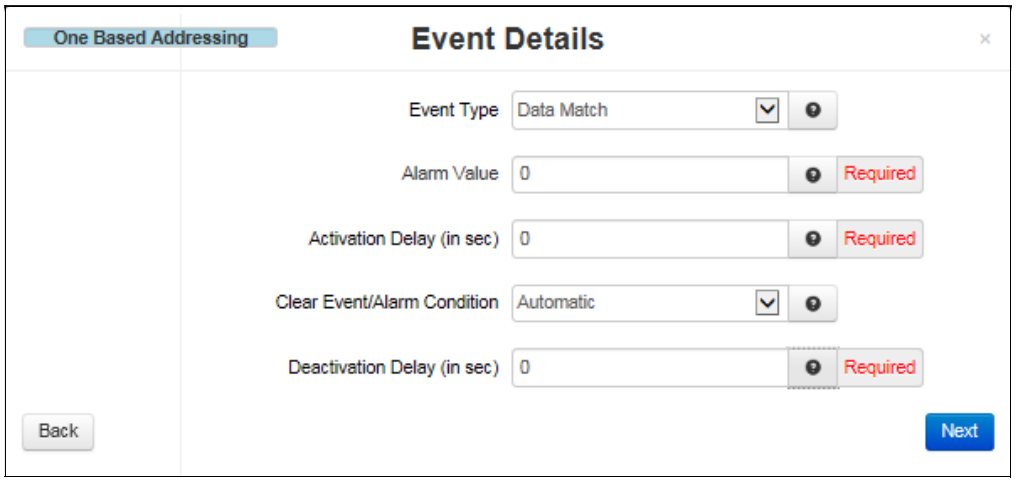
$TAG1$ & $TAG2$ | $TAG3$ & !$TAG4$

where EVT1, EVT2, EVT3, EVT4, EVT5 and MyEvent represents the event name and $TAG1$, $TAG2$, $TAG3$, $TAG4$, $TAG5$ and $TAGNAME$ represents the I/O type register address.

Rules:

- "!" only takes effect for the operand or the total result of the pair of parenthesis at its right hand side
- “=” shall be between only two operands. Another “=” following is not allowed
- EVT1 == EVT2 == EVT3, shall be written as EVT1 = EVT2 & (EVT2 = EVT3)
- Operations are evaluated from left to right, unless parenthesis takes higher priority
- Maximum level of cascaded parenthesis is 3
- Maximum named event operands is 16
- “!=” is not allowed. Instead, use EVT1 = !EVT2 or !EVT1 = EVT2

Click on the *Next* button.



Event Type: An event is TRUE when:

Data Match: The value of the register is equal to the alarm value.

Data Mismatch: The value of the register is not equal to the alarm value.

Absolute High: The value of the register exceeds the alarms value.

Absolute Low: The value of the register falls below the alarms value.

Deviation High: The value of the register exceeds the setpoint by an amount equal to or greater than the alarms value.

Deviation Low: The value of the register falls below the setpoint by an amount equal to or greater than the alarms value.

Out of Band: The value of the register moves outside a band, equal in width to twice the alarms value and centered on the setpoint.

In Band: The value of the register moves inside a band, equal in width to twice the alarms value and centered on the setpoint.

Rate of Change: The value of the register changes within given Time Window by the specified amount of Change Limit.

Scaling: Transform an input register from one range of values to another range.

Bit Operations: Transform a set of DI/DO values between bit locations of an AI/AO register. There are two options under Transform Type: Bit Unpacking and Bit Packing.

Bit Unpacking: Using the Analog register specified, write out bit values from least significant bit to the most significant bit. This will write into 16 Digital register locations, beginning at the register specified on the next page **Event Action**.

Bit Packing: Starting with the Digital register specified, assemble 16 digital registers into a single Analog value. This will be written into the location specified on the next page **Event Action**.

Note: The first digital register specified is the least significant bit, and the last is the most significant bit.

Bit Unpacking Example: For Analog value **21845** and Write Action Address of DO:1, digital outputs DO:1-DO:16 will be populated as follows, with **DO:1** being the **least** significant bit:

Digital Type	Digital Value
DO1	1
DO2	0
DO3	1
DO4	0
...	...
DO13	1
DO14	0
DO15	1
DO16	0

Bit Packing Example: For Bit Packing, the inverse is true: DO:1-DO:16 will be assembled into specified analog register, with **DO:1** being the **least** significant bit.

Calculations: Perform basic math functions between registers.

Alarm Value (Required): Value at which the alarm will trigger.

If the Event Type is a Data Match or Data Mismatch type, the alarm will trigger on this exact value. In all other cases, the data source must exceed this value (above or below depending)

This must be within the limits of the data source.

For IODB, these limits are:

	Min Unsigned	Max Unsigned	Min Signed	Max Signed
Digital	0	1	0	1
16 Bit	0	65535	-32768	32768
32 Bit	0	232 -1	-231	231-1
64 Bit	0	264-1	-263	263-1

Activation Delay (in sec) (Required): The Activation Delay is used to indicate how long (in seconds) the alarm condition must exist and be true before the alarm will become active.

For example, if the alarm is configured to go active when an input register is an Absolute High exceeding 1000, then the register value must stay above 1000 for the activation delay period, or else it will be ignored.

Clear Event/Alarm Condition: Select the desired option to clear an event condition.

Automatic: Allows an event condition to clear to an inactive state when the input meets configured conditions.

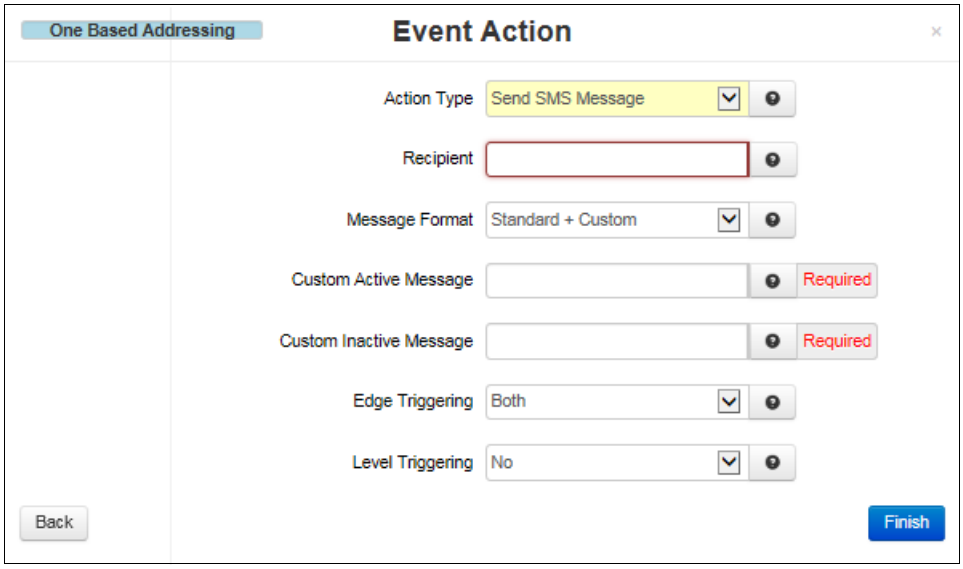
Manual: Requires a user to login and clear the event. An event that is not cleared will continue to generate actions if it is level triggered. If the action is edge triggered, and this event is not cleared, then no new event action will result.

Deactivation Delay (in sec) (Required): Used to prevent an event from oscillating between the on and off states when the process is near the alarm value. Default value: 0 to disable.

Once an event is active and the input condition then falls to an inactive condition, it must remain in the inactive state for this delay period (in seconds) before the alarm will actually be considered inactive.

If configured, this delay and hysteresis must both be satisfied for the alarm to be cleared.

To move on to the next screen, click on the *NEXT* button.



Action Type: Select the desired Action Type for the event.

None: No action, log the event only.

Send SMS Message: Send an SMS message to a single recipient. Use multiple Events to notify more than one contact.

Write IODB Value: Write to a known IODB register.

Run Command: Run a Command Script that performs an Action.

SVM Alert Message: Send an alert message to the SVM server that appears in unit history.

Send SMS/Email (Action Type)

Recipient (Required):

SMS Message: Enter a single phone number for the text message destination. Leading access numbers and area codes may be required based on your carrier, location, account type, and roaming status. Dashes and periods will be ignored. Example: 1-202-555-1212 OR 0114185551212

Email Message: Enter an email address for the email message destination. Multiple email addresses may be entered by separating them with a comma. The email will come From the address configured in Services→Email Client. Example: username@email.com OR username@email.com,usergroup@email.com

Message Format: Define what type of content the Event alert message will contain.

Standard: Send only the standard informational message.

Custom: Send only the custom message as specified. Tag values may be inserted as a variable by declaring the Tag Name framed in $. ie: $TAGNAME$.

Standard + Custom: Append up to a 60 character Custom message to the standard message.

The Standard Message will be constructed as follows:

EVT<Num>:<Name> <Cond> <Custom> Duration:<Time> DS:<DSValue> <Clear Condition>

Where

<Num> is the event number.

<Name> is the event name.

<Cond> is the current event condition or status, ACTIVE or INACTIVE.

<Custom> is the optional custom message specified by the user.

<Time> is the amount of time that the event has been active.

<DSValue> is the value of the Data Source that caused the event to activate or deactivate.

<Clear Condition> will indicate if the event "Will Auto Clear" on its own or if a "Manual Clear Required".

Note: Manual Clearing can be accomplished by clicking the Clear button on the Event Status page, or by writing a "1" into the Clear Condition register defined in IODB. See Appendix B.

The Data Source value will change depending on the type of Data Source configured for each event. When an Event Expression is used, a series of bits will indicated the True/False status of terms in the Event Expression. For example, if you had an expression like:

Evt1 | Evt2 | (Evt3 & Evt4)

You could get a message that would trigger with:

1000000000000

0100000000000

0011000000000

First Bit = the first event name in the expression, and so on.

Custom Active Message (Required):

SMS Message: Enter a custom message to be sent to the recipient(s) when the event goes active. If appended to a standard message, the length is limited to 60 characters.

Email Message: Enter a custom message body that will be sent to the Recipient(s) when the event goes active.

Custom Inactive Message (Required):

SMS Message: Enter a custom message to be sent to the recipient(s) when the event goes active. If appended to a standard message, the length is limited to 60 characters.

Email Message: Enter a custom message body that will be sent to the Recipient(s) when the event goes active.

Edge Triggering: Select the desired setting for this field.

Neither: Executes the action based on any edge triggering options.

Rising Only: Executes the action only on transition of the event becoming true (active).

Falling Only: Executes the action only on transition of the event becoming false (inactive).

Both: Executes the action on any transition between true and false.

Level Triggering: Selecting Yes the action to execute as often as specified in the periodic action while the event remains true. Choosing NO indicates level will not be considered when evaluating the Event condition.

Write IODB (Action Type)

Periodic Action (in sec): Specifying a non-zero number will cause the action to repeat every period of the number of seconds.

Tag Name: This field will auto-populate when the user starts to type a tag name. Tag names are managed in Automation → Tags.

Write Type: The WriteType will auto-populate based on the Tag Name entered. These settings are pulled from the Tags dialog window located in Automation → Tags. The Write Type may also be entered manually if no Tag has been defined for this Type: Address.

Write Address: The Local Address will auto-populate based on the Tag Name entered. These settings are pulled from the Tags dialog window located in Automation → Tags. The Write Address may also be entered manually if no Tag has been defined for this Type: Address.

Value to Write: Choose what to write into the IODB register.

Data Source: Writes the input of the event.

Event Condition: Writes a 1 = TRUE or 0 = FALSE for this event condition.

Fixed Value: Writes a constant fixed number to that entry, when true.

Counter: Increments the value in the IODB location by one.

Run Command Script: Choose the name of the command script to be executed when the Event is True.

None: Standard operation with no special behaviors.

Rotate Data Logs: Rotate running data logs.

Create Data Log Entry: Create new data log entry

Restart IPSec: Restart the IPSec service. i.e. Bring the IPSec tunnel down, then reestablish the tunnel.

Stop IPSec: Stop the IPSec service.and do not reestablish the tunnel.

Restart Modbus: Restart Modbus services.

Reboot: Reboot the entire device.

Restart Serial IP: Restart the serial IP service.

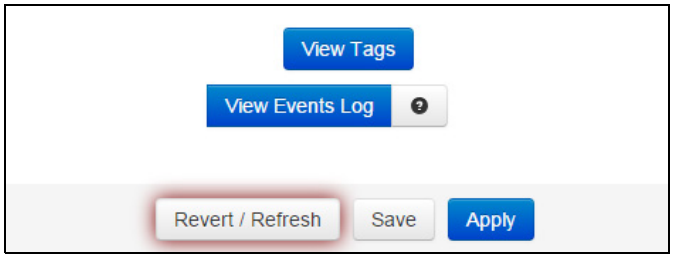
Reset Wireless: Restart the Cellular Module.

SVM Alert Message (Action Type)

Alert Level: Select an Alert Level for the message that appears in SixView Manager. These correspond to Syslog levels, where 0 is most critical and 7 is informational.

Click on the *Finish* button. You will be returned to the Events dialog window and the Configuration table will be populated with the entered data.

To delete an existing event, select it in the table and click on the *Delete* button. To edit an existing event, select it in the table and click on the *Edit* button. To move events in the table, use the Up and Down buttons. You can also duplicate an existing Event by clicking on the Copy button.



To view existing Tags, click on the *View Tags* button. This will bring you to the Tags dialog window found in the Automation menu. From this screen, you can add, edit or delete tags. See section 3.6.3 for more information.

Click on the *View Events Log* button to view the status of each event configured on your device. Each line consists of 7 fields that are comma separated.

Each line of events include:

- Date/Time
- Event Number
- Event Name (“N/A” if no name)
- Event Condition/Status (1/0)
- Event Condition/Status (Active/Inactive)
- Event Data Source Value (0 at initial time)
- Description (optional)

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert/Refresh*, will reset or refresh all fields to previously saved defaults.

Service and Support Information

Service Information

We sincerely hope that you never experience a problem with any of our products. If you do need support, call Red Lion at 1-877-432-9908 for Technical Support. A trained specialist will help you determine the source of the problem. Many problems are easily resolved with a single phone call. If it is necessary to return a unit to us, an SO (Service Order) can be obtained on the Red Lion website.

Red Lion tracks the flow of returned material with our SO system to ensure speedy service. You must include this SO number on the outside of the box so that your return can be processed immediately.

Be sure to have your original purchase order number and date purchased available.

We suggest that you give us a repair purchase order number in case the repair is not covered under our warranty. You will not be billed if the repair is covered under warranty.

Please supply us with as many details about the problem as you can. The information you supply will be written on the SO form and supplied to the repair department before your unit arrives. This helps us to provide you with the best service, in the fastest manner. Repairs are completed as soon as possible. If you need a quicker turnaround, ship the unit to us by air freight. We give priority service to equipment that arrives by overnight delivery.

We apologize for any inconvenience that the need for repair may cause you. We hope that our rapid service meets your needs. If you have any suggestions to help us improve our service, please give us a call. We appreciate your ideas and will respond to them.

For Your Convenience:

Please fill in the following and keep this manual with your Red Lion system for future reference:

P.O. #:_____ Date Purchased: _____

Purchased From:_____

Serial Number: _____

Product Support

Technical Support:
Inside US: +1 877 432-9908
Outside US: +1 717 767-6511
E-mail: support@redlion.net

Customer Service:
Inside US: +1 877 432-9908
Outside US: +1 717 767-6511
E-mail: customer.service@redlion.net

Licensing & Warranty

Software License

Software supplied with each Red Lion product remains the exclusive property of Red Lion. Red Lion grants with each unit a perpetual license to use this software with the express limitations that the software may not be copied or used in any other product for any purpose. It may not be reverse engineered, or used for any other purpose other than in and with the computer hardware sold by Red Lion.

Statement of Limited Warranty

(a) Red Lion Controls Inc., (the "Company") warrants that all Products shall be free from defects in material and workmanship under normal use for the period of time provided in "Statement of Warranty Periods" (available at www.redlion.net) current at the time of shipment of the Products (the "Warranty Period"). **EXCEPT FOR THE ABOVE-STATED WARRANTY, COMPANY MAKES NO WARRANTY WHATSOEVER WITH RESPECT TO THE PRODUCTS, INCLUDING ANY (A) WARRANTY OF MERCHANTABILITY; (B) WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE; OR (C) WARRANTY AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY; WHETHER EXPRESS OR IMPLIED BY LAW, COURSE OF DEALING, COURSE OF PERFORMANCE, USAGE OF TRADE OR OTHERWISE.** Customer shall be responsible for determining that a Product is suitable for Customer's use and that such use complies with any applicable local, state or federal law.

(b) The Company shall not be liable for a breach of the warranty set forth in paragraph (a) if (i) the defect is a result of Customer's failure to store, install, commission or maintain the Product according to specifications; (ii) Customer alters or repairs such Product without the prior written consent of Company.

(c) Subject to paragraph (b), with respect to any such Product during the Warranty Period, Company shall, in its sole discretion, either (i) repair or replace the Product; or (ii) credit or refund the price of Product provided that, if Company so requests, Customer shall, at Company's expense, return such Product to Company.

(d) **THE REMEDIES SET FORTH IN PARAGRAPH (c) SHALL BE THE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY AND COMPANY'S ENTIRE LIABILITY FOR ANY BREACH OF THE LIMITED WARRANTY SET FORTH IN PARAGRAPH (a)**.

Appendix A

RED-LION-RAM.MIB Contents

Refers to: 3.5.10 SNMP Agent: RED-LION-RAM.MIB Contents

Note: The RAM-6021 Wired Router will not return any values for Wireless specific fields.

The following MIBs are cellular specific. It is to be noted that all of the following can be retrieved on the SN firmware version of Red Lion's RTUs or routers, the A, M, and R Series RTUs or routers are dependent on the cellular module/aircard installed/inserted into the RTU or router. Some manufacturers allow for more information to be retrieved from the module/aircard than others.		
unitDescription	DISPLAYSTRING	RTU or Router Model Name (e.g. RAM-9931).
unitSerialNumber	DISPLAYSTRING	Serial Number (e.g. 123456789012).
unitFirmwareVersion	DISPLAYSTRING	Firmware Version Number (e.g. 4.25.84.47).
unitName	DISPLAYSTRING	Unit Name (e.g. RAM-0647e3 or User Preferred Name via GUI Access Settings)
Cellular		
mdn	DISPLAYSTRING	Mobile Directory Number, the actual phone of the device. Cellular Mobile Directory Number (e.g. (xxx)xxx-xxxx).
minIMEI	DISPLAYSTRING	Mobile Identification Number, the number given to a service plan provided by the carrier. International Mobile Equipment Ind entity, number used by the GSM network to identify valid devices. Cellular Intl Mobile Equipment Identifier
nai	DISPLAYSTRING	Network Access Identifier, a standard way of identifying users who request access to a network. Cellular Network Access Identifier.
sipUser	INTEGER	Session Initiation Protocol, used to establish sessions between multiple parties in a location-independent manner. Typically voice sessions. Cellular Session Initiation Protocol User.
sid	INTEGER	System ID, a unique 5-digit number assigned to each carrier by the FCC. Cellular System ID.
nid	INTEGER	Network ID, used to divide SIDs into smaller areas. Cellular Network Identifier.

prl	INTEGER	Preferred Roaming List, a list of information that resides in the memory of the module/aircard. It lists the radio frequencies the module/aircard can use in various geographic areas. The part of the list for each area is ordered by the bands the module/aircard should try to use first. Therefore it's a kind of priority list for which towers the module/aircard should use. The PRL helps determine which home-network towers to use, and also which towers belonging to other networks to use in roaming situations (areas where the home network has no coverage.) When roaming, the PRL may instruct the module/aircard to use the network with the best roaming rate for the carrier, rather than the one with the strongest signal at the moment. Since a PRL tells the module/aircard “where” to search for a signal, as carrier networks change over time, an updated PRL may be required for a module/aircard to “see” all of the coverage that it should, both with the home network and for roaming. Cellular Preferred Roaming List.
activated	INTEGER	Determines if the module/aircard is authorized onto the carrier’s network. Values are Unknown (-1), No(0), Yes (1). Cellular module activation status.
omaSupported	INTEGER	Open Mobile Alliance for Device Management (OMA DM), designed for management of small mobile devices such as mobile phones, PDAs and palm top computers. The device management is intended to support the following typical uses: **Provisioning -** Configuration of the device (including first time use), enabling and disabling features **Configuration of Device -** Allow changes to settings and parameters of the device **Software Upgrades -** Provide for new software and/or bug fixes to be loaded on the device, including applications and system software. **Fault Management -** Report errors from the device, query about status of device. Values are Unknown(-1), No(0), Yes (1) Cellular OMA Supported status.
currentMipProfile	INTEGER	Cellular Mobile IP Profile.
esn	DISPLAYSTRING	Electronic Serial Number, is a permanent identification number used to recognize mobile devices accessing particular telecommunications networks. The ESN is assigned and embedded into a wireless communications device by the device's manufacturer. Cellular Module Electronic Serial Number.
pesn	DISPLAYSTRING	Pseudo ESN, a reversed ESN manufacturer code 128, which allow legacy equipment to recognize MEIDs. Cellular Module Pseudo ESN.
meid	DISPLAYSTRING	Mobile Equipment Identifier, 56 bits long, and like ESN’s, identify the manufacturer of a mobile device as well as the serial number assigned to the device by that manufacturer. Cellular Mobile Equipment Identifier.
vendor	DISPLAYSTRING	Manufacturer of the module/aircard. Cellular Module manufacturer.

modelName	DISPLAYSTRING	The vendor-provided model name of the modem/card/module (e.g. sierra598U).
fwVersion	DISPLAYSTRING	Firmware version of the module/aircard. Cellular Module Firmware version #.
hwVersion	DISPLAYSTRING	Hardware version of the module/aircard. Cellular Module hardware version #.
carrier	DISPLAYSTRING	Service provider for cellular network. Cellular Service Provider.
lowRssi	INTEGER	Low Speed Received Signal Strength Indication. Cellular High Speed received signal strength indication.
lowEcio	INTEGER	Ec/Io is a ratio of good to bad energy, representing the cell towers “cleanness” in its signal to you. In other words - signal to noise ratio. Cellular Low Speed EC/IO.
highRssi	INTEGER	High Speed Received Signal Strength Indication. Cellular High Speed received signal strength indication.
highEcio	INTEGER	Ec/Io is a ratio of good to bad energy, representing the cell towers “cleanness” in its signal to you. In other words - signal to noise ratio. Cellular High Speed EC/IO.
currentRssi	INTEGER	Current Received Signal Strength Indication. Cellular Current Received Signal Strength Indication.
currentEcio	INTEGER	Ec/Io is a ratio of good to bad energy, representing the cell towers “cleanness” in its signal to you. In other words - signal to noise ratio. Cellular Current EC/IO.
svcType	DISPLAYSTRING	GSM, which stands for Global System for Mobile communications, reigns as the world's most widely used cell phone technology. CDMA, or Code Division Multiple Access, uses a “spread-spectrum” technique whereby electromagnetic energy is spread to allow for a signal with a wider bandwidth. This allows multiple people on multiple cell phones to be “multiplexed” over the same channel to share a bandwidth of frequencies. Cellular Service Type.
currentChannel	INTEGER	Channels are used to different frequency range network to operate on the same frequency in the same area that do not interfere with each other. Cellular Channel.
cdmaType	DISPLAYSTRING	None, Analog, Digital - High Data Rate type normally digital. Cellular CDMA Type (e.g. None, Analog, Digital).
hdrType	DISPLAYSTRING	Unknown, None, Rev0, RevA - The CDMA/EV-DO sub type. Cellular HDR (e.g. Unknown, None, Rev0, RevA).
cdmaRoaming	DISPLAYSTRING	Home, Roaming, Roaming - unknown. Roaming type indicator inside or outside the providers home network. Cellular Roaming indicator - CDMA.

hdrRoaming	DISPLAYSTRING	None, Roaming - SIDS Guaranteed, Roaming - SIDS Not Guaranteed. EVDO Roaming state. Cellular Roaming indicator - EVDO.
roaming	INTEGER	0 or 1. 0 = currently not roaming, 1 = currently roaming. Cellular current roaming status.
currentState	INTEGER	Connecting, Dormant, Connected, Disconnected, Error, CallIncoming. Current Modem State. Cellular state (e.g. connecting, dormant, connected, disconnected, error, call incoming).
speedPref	DISPLAYSTRING	Automatic, CDMAonly, EVDOonly. What speed preference the modem is currently set to lock to. Cellular Module speed pref.
roamPref	DISPLAYSTRING	HomeOnly, HomePreferred - AUTO, RoamOnly, Aonly, Bonly, AutoA, AutoB, unknown. The current setting for the modem's network roaming preference. Cellular Module roaming pref.
devName	DISPLAYSTRING	The device name as presented by the operating system (e.g. /dev/ttyUSB0).
ifName	DISPLAYSTRING	The cellular interface name, if known, as presented by the operating system (e.g. ppp0).
txCount	INTEGER	Current Wireless PPP RX byte count since connection has been up, updated every 30 minutes. Cellular Module TX Byte Count, updated every 30 mins.
rxCount	INTEGER	Current Wireless PPP RX byte count since connection has been up, updated every 30 minutes. Cellular Module RX Byte Count, updated every 30 mins.
gprsState	DISPLAYSTRING	The “state” of the GSM connection: idle, ready, standby. Cellular GPRS State.
rxLevel	DISPLAYSTRING	The signal level seen at the receiver measured in -dBm. Cellular RX Level.
servingCell	DISPLAYSTRING	The Current Cell on which the device is camped. Cellular Serving Cell.
rccState	DISPLAYSTRING	Radio Resources Control State (also called Packet Data Transfer state): idle, CELL_DCH, CELL_FACH, CELL_PCH, and URA_PCH Cellular RCC State.
gsmChannel	DISPLAYSTRING	Indicates which GSM channel or band of frequencies the device is currently connected to. Cellular GSM Channel.
psState	DISPLAYSTRING	Pulls CELLMODEM_PS_STATE from /var/log/wireless.cardstats Cellular PS State.
mode	DISPLAYSTRING	Pulls CELLMODEM_MODE from /var/log/wireless.cardstats Cellular Mode.

temperature	DISPLAYSTRING	Pulls CELLMODEM_TEMPERATURE from /var/log/wireless.cardstats Cellular Module Temp (not available on all modules).
simContextApn0	DISPLAYSTRING	Pulls CELLMODEM_SIM_CONT_APN0 from /var/log/wireless.cardstats Cellular SIM APN 0.
simContextApn1	DISPLAYSTRING	Pulls CELLMODEM_SIM_CONT_APN1 from /var/log/wireless.cardstats Cellular SIM APN 1.
simStatus	DISPLAYSTRING	Pulls CELLMODEM_SIM_STATUS from /var/log/wireless.cardstats Cellular SIM Status.
serviceDomain	DISPLAYSTRING	Pulls CELLMODEM_SERVICE_DOMAIN from /var/log/wireless.cardstats Cellular Service Domain.
availServiceType	DISPLAYSTRING	Pulls CELLMODEM_AVAIL_SERVICE_TYPE from /var/log/wireless.cardstats Cellular Available Service Type.
wCdmaL1State	DISPLAYSTRING	Pulls CELLMODEM_WCDMA_L1_STATE from /var/log/wireless.cardstats Cellular WCDMA L1 State.
mmcsState	DISPLAYSTRING	Pulls CELLMODEM_MM_CS_STATE from /var/log/wireless.cardstats Cellular MM CS State.
gmmPsState	DISPLAYSTRING	Pulls CELLMODEM_GMM_PS_STATE from /var/log/wireless.cardstats Cellular GMM PS State.
wCdmaChannel	DISPLAYSTRING	Pulls CELLMODEM_WCDMA_CHANNEL from /var/log/wireless.cardstats Cellular WCDMA Channel.
wCdmaBand	DISPLAYSTRING	Pulls CELLMODEM_WCDMA_BAND from /var/log/wireless.cardstats Cellular WCDMA Band.
systemMode	DISPLAYSTRING	Pulls CELLMODEM_SYSTEM_MODE from /var/log/wireless.cardstats Cellular System Mode.
powerOnTime	DISPLAYSTRING	Pulls CELLMODEM_POWERON_TIME from /var/log/wireless.cardstats Cellular Power On Time.
lowSpeedCsq	DISPLAYSTRING	Pulls CELLMODEM_LOWSPEED_CSQ from /var/log/wireless.cardstats Cellular Low Speed CSQ.
highSpeedCsq	DISPLAYSTRING	Pulls CELLMODEM_HIGHSPEED_CSQ from /var/log/wireless.cardstats Cellular High Speed CSQ.
band	DISPLAYSTRING	Pulls CELLMODEM_BAND from /var/log/wireless.cardstats Cellular Band.
imei	DISPLAYSTRING	Pulls CELLMODEM_IMEI from /var/log/wireless.cardstats Cellular IMEI.
simId	DISPLAYSTRING	Pulls CELLMODEM_SIM_ID from /var/log/wireless.cardstats Cellular SIM ID.
carrPLMN	DISPLAYSTRING	Carrier PLMN
rxLevelC0	DISPLAYSTRING	Receive Level C0
rxLevelC1	DISPLAYSTRING	Receive Level C1
locAreaCode	DISPLAYSTRING	Location Area Code

lteBand	DISPLAYSTRING	LTE Band
lteRxChan	DISPLAYSTRING	LTE Receive Channel
lteTxChan	DISPLAYSTRING	LTE Transmit Channel
lteBW	DISPLAYSTRING	LTE Bandwidth
lteRSRPint	DISPLAYSTRING	LTE Reference Signal Received Power
lteRSRQint	DISPLAYSTRING	LTE Reference Signal Received Quality
lteTracAreaCode	DISPLAYSTRING	LTE Trac Area Code
creg	DISPLAYSTRING	Cellmodem CREG Not registered, Searching
cellularUpTime	DISPLAYSTRING	Cellular Up Time in Seconds
lteRSRP	INTEGER	LTE Reference Signal Received Power in Integer
lteRSRQ	INTEGER	LTE Reference Signal Received Quality in Integer
lteSINRint	INTEGER	LTE Signal to Interference Plus Noise Ratio in Integer
trafficppp0		
todayRxPpp0	DISPLAYSTRING	Vnstat Today RX for PPP0 Interface
todayTxPpp0	DISPLAYSTRING	Vnstat Today Tx for PPP0 Interface
todayTotalPpp0	DISPLAYSTRING	Vnstat Today Total Rx/Tx for PPP0 Interface
yesterdayRxPpp0	DISPLAYSTRING	Vnstat Yesterday Rx for PPP0 Interface
yesterdayTxPpp0	DISPLAYSTRING	Vnstat Yesterday Tx for PPP0 Interface
yesterdayTotalPpp0	DISPLAYSTRING	Vnstat Yesterday Total Rx/Tx for PPP0 Interface
CurrMonthRxPpp0	DISPLAYSTRING	Vnstat Current Month Rx for PPP0 Interface
CurrMonthTxPpp0	DISPLAYSTRING	Vnstat Current Month Tx for PPP0 Interface
CurrMonthTotalPpp0	DISPLAYSTRING	Vnstat Current Month Total Rx/Tx for PPP0 Interface
PreMonthRxPpp0	DISPLAYSTRING	Vnstat Previous Month Rx for PPP0 Interface
PreMonthTxPpp0	DISPLAYSTRING	Vnstat Previous Month Tx for PPP0 Interface
PreMonthTotalPpp0	DISPLAYSTRING	Vnstat Previous Month Total Rx/Tx for PPP0 Interface
todayRxPpp0Kib	INTEGER	Vnstat Today Rx for PPP0 Interface in Kib
todayTxPpp0Kib	INTEGER	Vnstat Today Tx for PPP0 Interface in Kib
todayTotalPpp0Kib	INTEGER	Vnstat Today Total Rx/Tx for PPP0 Interface in Kib
yesterdayRxPpp0Kib	INTEGER	Vnstat Yesterday Rx for PPP0 Interface in Kib
yesterdayTxPpp0Kib	INTEGER	Vnstat Yesterday Tx for PPP0 Interface in Kib
yesterdayTotalPpp0Kib	INTEGER	Vnstat Yesterday Total Rx/Tx for PPP0 Interface in Kib
CurrMonthRxPpp0Kib	INTEGER	Vnstat Current Month Rx for PPP0 Interface in Kib
CurrMonthTxPpp0Kib	INTEGER	Vnstat Current Month Tx for PPP0 Interface in Kib
CurrMonthTotalPpp0Kib	INTEGER	Vnstat Current Month Total Rx/Tx for PPP0 Interface in Kib
PreMonthRxPpp0Kib	INTEGER	Vnstat Previous Month Rx for PPP0 Interface in Kib
PreMonthTxPpp0Kib	INTEGER	Vnstat Previous Month Tx for PPP0 Interface in Kib
PreMonthTotalPpp0Kib	INTEGER	Vnstat Previous Month Total Rx/Tx for PPP0 Interface in Kib
trafficwwan0		
todayRxWwan0	DISPLAYSTRING	Vnstat Today Rx for WWAN0 Interface
todayTxWwan0	DISPLAYSTRING	Vnstat Today Tx for WWAN0 Interface
todayTotalWwan0	DISPLAYSTRING	Vnstat Today Total Rx/Tx for WWAN0 Interface
yesterdayRxWwan0	DISPLAYSTRING	Vnstat Yesterday Rx for WWAN0 Interface
yesterdayTxWwan0	DISPLAYSTRING	Vnstat Yesterday Tx for WWAN0 Interface
yesterdayTotalWwan0	DISPLAYSTRING	Vnstat Yesterday Total Rx/Tx for WWAN0 Interface
CurrMonthRxWwan0	DISPLAYSTRING	Vnstat Current Month Rx for WWAN0 Interface

CurrMonthTxWwan0	DISPLAYSTRING	Vnstat Current Month Tx for WWAN0 Interface
CurrMonthTotalWwan0	DISPLAYSTRING	Vnstat Current Month Total Rx/Tx for WWAN0 Interface
PreMonthRxWwan0	DISPLAYSTRING	Vnstat Previous Month Rx for WWAN0 Interface
PreMonthTxWwan0	DISPLAYSTRING	Vnstat Previous Month Tx for WWAN0 Interface
PreMonthTotalWwan0	DISPLAYSTRING	Vnstat Previous Month Total Rx/Tx for WWAN0 Interface
todayRxWwan0Kib	INTEGER	Vnstat Today Rx for WWAN0 Interface in Kib
todayTxWwan0Kib	INTEGER	Vnstat Today Tx for WWAN0 Interface in Kib
todayTotalWwan0Kib	INTEGER	Vnstat Today Total Rx/Tx for WWAN0 Interface in Kib
yesterdayRxWwan0Kib	INTEGER	Vnstat Yesterday Rx for WWAN0 Interface in Kib
yesterdayTxWwan0Kib	INTEGER	Vnstat Yesterday Tx for WWAN0 Interface in Kib
yesterdayTotalWwan0Kib	INTEGER	Vnstat Yesterday Total Rx/Tx for WWAN0 Interface in Kib
CurrMonthRxWwan0Kib	INTEGER	Vnstat Current Month Rx for WWAN0 Interface in Kib
CurrMonthTxWwan0Kib	INTEGER	Vnstat Current Month Tx for WWAN0 Interface in Kib
CurrMonthTotalWwan0Kib	INTEGER	Vnstat Current Month Total Rx/Tx for WWAN0 Interface in Kib
PreMonthRxWwan0Kib	INTEGER	Vnstat Previous Month Rx for WWAN0 Interface in Kib
PreMonthTxWwan0Kib	INTEGER	Vnstat Previous Month Tx for WWAN0 Interface in Kib
PreMonthTotalWwan0Kib	INTEGER	Vnstat Previous Month Total Rx/Tx for WWAN0 Interface in Kib
trafficeth0		
todayRxEth0	DISPLAYSTRING	Vnstat Today Rx for Eth0 Interface
todayTxEth0	DISPLAYSTRING	Vnstat Today Tx for Eth0 Interface
todayTotalEth0	DISPLAYSTRING	Vnstat Today Total Rx/Tx for Eth0 Interface
yesterdayRxEth0	DISPLAYSTRING	Vnstat Yesterday Rx for Eth0 Interface
yesterdayTxEth0	DISPLAYSTRING	Vnstat Yesterday Tx for Eth0 Interface
yesterdayTotalEth0	DISPLAYSTRING	Vnstat Yesterday Total Rx/Tx for Eth0 Interface
CurrMonthRxEth0	DISPLAYSTRING	Vnstat Current Month Rx for Eth0 Interface
CurrMonthTxEth0	DISPLAYSTRING	Vnstat Current Month Tx for Eth0 Interface
CurrMonthTotalEth0	DISPLAYSTRING	Vnstat Current Month Total Rx/Tx for Eth0 Interface
PreMonthRxEth0	DISPLAYSTRING	Vnstat Previous Month Rx for Eth0 Interface
PreMonthTxEth0	DISPLAYSTRING	Vnstat Previous Month Tx for Eth0 Interface
PreMonthTotalEth0	DISPLAYSTRING	Vnstat Previous Month Total Rx/Tx for Eth0 Interface
todayRxEth0Kib	INTEGER	Vnstat Today Rx for ETH0 Interface in Kib
todayTxEth0Kib	INTEGER	Vnstat Today Tx for ETH0 Interface in Kib
todayTotalEth0Kib	INTEGER	Vnstat Today Total Rx/Tx for ETH0 Interface in Kib
yesterdayRxEth0Kib	INTEGER	Vnstat Yesterday Rx for ETH0 Interface in Kib
yesterdayTxEth0Kib	INTEGER	Vnstat Yesterday Tx for ETH0 Interface in Kib
yesterdayTotalEth0Kib	INTEGER	Vnstat Yesterday Total Rx/Tx for ETH0 Interface in Kib
CurrMonthRxEth0Kib	INTEGER	Vnstat Current Month Rx for ETH0 Interface in Kib
CurrMonthTxEth0Kib	INTEGER	Vnstat Current Month Tx for ETH0 Interface in Kib
CurrMonthTotalEth0Kib	INTEGER	Vnstat Current Month Total Rx/Tx for ETH0 Interface in Kib
PreMonthRxEth0Kib	INTEGER	Vnstat Previous Month Rx for ETH0 Interface in Kib
PreMonthTxEth0Kib	INTEGER	Vnstat Previous Month Tx for ETH0 Interface in Kib
PreMonthTotalEth0Kib	INTEGER	Vnstat Previous Month Total Rx/Tx for ETH0 Interface in Kib
trafficeth1		
todayRxEth1	DISPLAYSTRING	Vnstat Today Rx for Eth1 Interface

todayTxEth1	DISPLAYSTRING	Vnstat Today Tx for Eth1 Interface
todayTotalEth1	DISPLAYSTRING	Vnstat Today Total Rx/Tx for Eth1 Interface
yesterdayRxEth1	DISPLAYSTRING	Vnstat Yesterday Rx for Eth1 Interface
yesterdayTxEth1	DISPLAYSTRING	Vnstat Yesterday Tx for Eth1 Interface
yesterdayTotalEth1	DISPLAYSTRING	Vnstat Yesterday Total Rx/Tx for Eth1 Interface
CurrMonthRxEth1	DISPLAYSTRING	Vnstat Current Month Rx for Eth1 Interface
CurrMonthTxEth1	DISPLAYSTRING	Vnstat Current Month Tx for Eth1 Interface
CurrMonthTotalEth1	DISPLAYSTRING	Vnstat Current Month Total Rx/Tx for Eth1 Interface
PreMonthRxEth1	DISPLAYSTRING	Vnstat Previous Month Rx for Eth1 Interface
PreMonthTxEth1	DISPLAYSTRING	Vnstat Previous Month Tx for Eth1 Interface
PreMonthTotalEth1	DISPLAYSTRING	Vnstat Previous Month Total Rx/Tx for Eth1 Interface
todayRxEth1Kib	INTEGER	Vnstat Today Rx for ETH1 Interface in Kib
todayTxEth1Kib	INTEGER	Vnstat Today Tx for ETH1 Interface in Kib
todayTotalEth1Kib	INTEGER	Vnstat Today Total Rx/Tx for ETH1 Interface in Kib
yesterdayRxEth1Kib	INTEGER	Vnstat Yesterday Rx for ETH1 Interface in Kib
yesterdayTxEth1Kib	INTEGER	Vnstat Yesterday Tx for ETH1 Interface in Kib
yesterdayTotalEth1Kib	INTEGER	Vnstat Yesterday Total Rx/Tx for ETH1 Interface in Kib
CurrMonthRxEth1Kib	INTEGER	Vnstat Current Month Rx for ETH1 Interface in Kib
CurrMonthTxEth1Kib	INTEGER	Vnstat Current Month Tx for ETH1 Interface in Kib
CurrMonthTotalEth1Kib	INTEGER	Vnstat Current Month Total Rx/Tx for ETH1 Interface in Kib
PreMonthRxEth1Kib	INTEGER	Vnstat Previous Month Rx for ETH1 Interface in Kib
PreMonthTxEth1Kib	INTEGER	Vnstat Previous Month Tx for ETH1 Interface in Kib
PreMonthTotalEth1Kib	INTEGER	Vnstat Previous Month Total Rx/Tx for ETH1 Interface in Kib
gpscurrent		
CurrentGpsValid	DISPLAYSTRING	GPS Current Valid Fixed Quality (0 = Invalid, 1 = Valid)
CurrentGpsLat	DISPLAYSTRING	GPS Current Latitude Degrees
CurrentGpsLong	DISPLAYSTRING	GPS Current Longitude Degrees
CurrentGpsAlt	DISPLAYSTRING	GPS Current Altitude Tenths of Meter (280.2 = 2802)
CurrentGpsTimeStamp	DISPLAYSTRING	GPS Current Time Stamp
CurrentGpsNumSat	DISPLAYSTRING	GPS Current Number of Satellites
CurrentGpsFtfromcp	DISPLAYSTRING	GPS Current Feet From Lockdown Center Point
CurrentGpsSpeed	DISPLAYSTRING	GPS Current Speed, SOG tenths of knots (50.1 = 501)
CurrentGpsCourse	DISPLAYSTRING	GPS Current Course, Heading in tenths of degree (280.3 = 2803)
GpsSource	DISPLAYSTRING	GPS Source of Data (1=Internal;3=Fixed)
GpsLockdownState	DISPLAYSTRING	GPS Current Lockdown State (0 = Monitor;5 = Lockdown;7-9 = Violation)
GpsLockdownRadius	DISPLAYSTRING	GPS Current Lockdown Radius (ft), Units in Feet as calculated from centerpoint

Appendix B

IODB Status Module

The IODB status module is a set of IODB registers that are reserved for system use to collect device based information and make that information available to be polled by any head end or SCADA server appliances via Modbus based I/O transfers.

These registers are created as Analog OUT registers as not to interfere with any on board I/O or other commonly used register types.

Frequency Legend: Rare = 30 minutes, Sometimes = 5 minutes, Often = 30 seconds, Quickly = 5 seconds, Rapidly = 1 second

Register type is Analog Out and the initial register offset is 1000.

System Status				
Index	Name	Description	Frequency	Notes
1001	Serial_Number_UINT16_A	First 4 digits, UINT16	Rare	16 digit field saved as 4, 4-digit numbers
1002	Serial_Number_UINT16_B	Next 4 digits	Rare	
1003	Serial_Number_UINT16_C	Next 4 digits	Rare	
1004	Serial_Number_UNIT16_D	Last 4 digits	Rare	
1005	Serial_Number_UINT64_A	UINT64 format; LSW	Rare	16 digit field saved as a single UNT64, Little Endian, LSB First.
1006	Serial_Number_UINT64_B		Rare	Serial Number = (Reg1005 + (Reg1006 * 2^16) + (Reg1007 * 2^32) + (Reg1008 * 2^48)
1007	Serial_Number_UINT64_C		Rare	
1008	Serial_Number_UINT64_D		Rare	
1009	Model_Number	4 digit model number	Rare	No prefixes or suffixes
1010	Firmware_Version	3 digit number	Rare	425=4.25, 325=3.25
1011	Date_Year	Year, 4 digit number	Rapidly	
1012	Date_Month	Month, 1-12	Rapidly	
1013	Date_Day	Day, 1-31	Rapidly	
1014	Date_DayOfWeek	Day, 1-7	Rapidly	Sunday=0
1015	Date_DayOfYear	DOY, 1-365	Rapidly	
1016	Time_Hour	Hour, 0-23	Rapidly	Current Time
1017	Time_Min	Minute, 0-59	Rapidly	
1018	Time_Second	Second, 0-59	Rapidly	
1019	Uptime_Days	Days, 0-9999	Rapidly	Time since last reboot
1020	Uptime_Hours	Hours, 0-23	Rapidly	
1021	Uptime_Minutes	Minutes, 0-59	Rapidly	
1022	Uptime_Seconds	Seconds, 0-59	Rapidly	
1023	CPU Load	% CPU Load	Quickly	
1061	Onboard_Temp	Onboard-Temp, in C	Often	Units are in Celsius, 3 digits displayed, insert a decimal after the first 2 digits. i.e. 273 is 27.3

1062	Onboard_VIN1	Input Voltage 1, in mV	Often	
1063	Onboard_VIN2	Input Voltage 2, in mV	Often	
1064	Onboard_VBATT	Battery voltage, in mV	Often	
1068	AI_Calibration	Reserved; non-zero during calibration	N/A	A non-zero value indicates user calibration is in progress
1069	AO_Calibration	Reserved; non-zero during calibration	N/A	A non-zero value indicates user calibration is in progress

Traffic - VNStat entries are in KiB (Kilobytes)				
Index	Name	Description	Frequency	Notes
1071	ppp0_TodayRX_A	UINT32; LSW	Sometimes	All UINT32 values should be handled as Unsigned, 32-bit Integers, Little Endian, LSB First.
1072	ppp0_TodayRX_B	UINT32; MSW	Sometimes	Crimson settings would be a Holding Register, Data Type: Word as Long, Manipulation: Reversed, Treat As: Unsigned.
1073	ppp0_TodayTX_A	UINT32; LSW	Sometimes	
1074	ppp0_TodayTX_B	UINT32; MSW	Sometimes	
1075	ppp0_TodayTotal_A	UINT32; LSW	Sometimes	
1076	ppp0_TodayTotal_B	UINT32; MSW	Sometimes	
1077	ppp0_YesterdayRX_A	UINT32; LSW	Sometimes	
1078	ppp0_YesterdayRX_B	UINT32; MSW	Sometimes	
1079	ppp0_YesterdayTX_A	UINT32; LSW	Sometimes	
1080	ppp0_YesterdayTX_B	UINT32; MSW	Sometimes	
1081	ppp0_YesterdayTotal_A	UINT32; LSW	Sometimes	
1082	ppp0_YesterdayTotal_B	UINT32; MSW	Sometimes	
1083	ppp0_ThisMonthRX_A	UINT32; LSW	Sometimes	
1084	ppp0_ThisMonthRX_B	UINT32; MSW	Sometimes	
1085	ppp0_ThisMonthTX_A	UINT32; LSW	Sometimes	
1086	ppp0_ThisMonthTX_B	UINT32; MSW	Sometimes	
1087	ppp0_ThisMonthTotal_A	UINT32; LSW	Sometimes	
1088	ppp0_ThisMonthTotal_B	UINT32; MSW	Sometimes	
1089	ppp0_LastMonthRX_A	UINT32; LSW	Sometimes	
1090	ppp0_LastMonthRX_B	UINT32; MSW	Sometimes	
1091	ppp0_LastMonthTX_A	UINT32; LSW	Sometimes	
1092	ppp0_LastMonthTX_B	UINT32; MSW	Sometimes	
1093	ppp0_LastMonthTotal_A	UINT32; LSW	Sometimes	
1094	ppp0_LastMonthTotal_B	UINT32; MSW	Sometimes	
1095	wwan0_TodayRX_A	UINT32; LSW	Sometimes	
1096	wwan0_TodayRX_B	UINT32; MSW	Sometimes	
1097	wwan0_TodayTX_A	UINT32; LSW	Sometimes	
1098	wwan0_TodayTX_B	UINT32; MSW	Sometimes	
1099	wwan0_TodayTotal_A	UINT32; LSW	Sometimes	
1100	wwan0_TodayTotal_B	UINT32; MSW	Sometimes	
1101	wwan0_YesterdayRX_A	UINT32; LSW	Sometimes	
1102	wwan0_YesterdayRX_B	UINT32; MSW	Sometimes	

1103	wwan0_YesterdayTX_A	UINT32; LSW	Sometimes	
1104	wwan0_YesterdayTX_B	UINT32; MSW	Sometimes	
1105	wwan0_YesterdayTotal_A	UINT32; LSW	Sometimes	
1106	wwan0_YesterdayTotal_B	UINT32; MSW	Sometimes	
1107	wwan0_ThisMonthRX_A	UINT32; LSW	Sometimes	
1108	wwan0_ThisMonthRX_B	UINT32; MSW	Sometimes	
1109	wwan0_ThisMonthTX_A	UINT32; LSW	Sometimes	
1110	wwan0_ThisMonthTX_B	UINT32; MSW	Sometimes	
1111	wwan0_ThisMonthTotal_A	UINT32; LSW	Sometimes	
1112	wwan0_ThisMonthTotal_B	UINT32; MSW	Sometimes	
1113	wwan0_LastMonthRX_A	UINT32; LSW	Sometimes	
1114	wwan0_LastMonthRX_B	UINT32; MSW	Sometimes	
1115	wwan0_LastMonthTX_A	UINT32; LSW	Sometimes	
1116	wwan0_LastMonthTX_B	UINT32; MSW	Sometimes	
1117	wwan0_LastMonthTotal_A	UINT32; LSW	Sometimes	
1118	wwan0_LastMonthTotal_B	UINT32; MSW	Sometimes	

GPS				
Index	Name	Description	Frequency	Notes
1201	GPS_TimeA	UINT32; LSW	Quickly	All UINT32 values should be handled as Unsigned, 32-bit Integers, Little Endian, LSB First.
1202	GPS_TimeB	UINT32	Quickly	http://www.geomidpoint.com/latlon.html
1203	GPS_Valid	Fix Quality	Quickly	0=Invalid (V), 1=Valid (A)
1204	GPS_LatDeg	Latitude, Degrees	Quickly	Absolute
1205	GPS_LatMin	Latitude, Minutes	Quickly	
1206	GPS_LatSec	Latitude, Seconds	Quickly	
1207	GPS_LatDir	Latitude, Direction	Quickly	0=N, 1=S
1208	GPS_LatDecDeg	Latitude, Signed Hours	Quickly	N is positive, S is negative, (Signed Degrees Format)
1209	GPS_LatDecFrac	Latitude, Decimal part	Quickly	
1210	GPS_LongDeg	Longitude, Degrees	Quickly	Absolute
1211	GPS_LongMin	Longitude, Minutes	Quickly	
1212	GPS_LongSec	Longitude, Seconds	Quickly	
1213	GPS_LongDir	Longitude, Direction	Quickly	0=E, 1=W
1214	GPS_LongDecDeg	Longitude, Signed Hours	Quickly	E is positive, W is negative (Signed Degrees Format)
1215	GPS_LongDecFrac	Longitude, Decimal part	Quickly	
1216	GPS_NumofSat	Number of Satellites	Quickly	
1217	GPS_Altitude	Altitude, tenths of meter	Quickly	280.2 = 2802
1218	GPS_Speed	SOG, tenths of knots	Quickly	50.1 = 501
1219	GPS_Course	Heading, in tenths of deg	Quickly	280.3 = 2803
1220	GPS_Lockdown_State	Current State	Quickly	0=Monitoring; 5=Good; 7-9=Violation of Lockdown
1221	GPS_Lockdown_Radius	Radius (ft)	Quickly	Units in Feet as calculated from centerpoint

1222	GPS_Source	Source of data	Quickly	0=unknown; 1=internal; 3=user fixed
1223	GPS_Time_HH	GPS Time Hours	Quickly	
1224	GPS_Time_MM	GPS Time Minutes	Quickly	
1225	GPS_Time_SS	GPS Time Seconds	Quickly	

Network Identifiers				
Index	Name	Description	Frequency	Notes
1301	Eth0_IP_a	First Octet	Quickly	
1302	Eth0_IP_b	Second Octet	Quickly	
1303	Eth0_IP_c	Third Octet	Quickly	
1304	Eth0_IP_d	Fourth Octet	Quickly	
1305	Eth0_Subnet_a	First Octet	Quickly	
1306	Eth0_Subnet_b	Second Octet	Quickly	
1307	Eth0_Subnet_c	Third Octet	Quickly	
1308	Eth0_Subnet_d	Fourth Octet	Quickly	
1309	Eth0_DHCP	DHCP Client Enabled?	Often	0=Static IP, 1=DHCP Assigned IP
1310	Eth0_Link	Link Status	Often	0 = No Link, 1 = Link detected
1311	Eth1_IP_a	First Octet	Quickly	
1312	Eth1_IP_b	Second Octet	Quickly	
1313	Eth1_IP_c	Third Octet	Quickly	
1314	Eth1_IP_d	Fourth Octet	Quickly	
1315	Eth1_Subnet_a	First Octet	Quickly	
1316	Eth1_Subnet_b	Second Octet	Quickly	
1317	Eth1_Subnet_c	Third Octet	Quickly	
1318	Eth1_Subnet_d	Fourth Octet	Quickly	
1319	Eth1_DHCP	DHCP Client Enabled?	Often	0 = Static IP, 1 = DHCP Assigned IP
1320	Eth1_Link	Link Status	Often	0 = No Link, 1 = Link detected
1321	ppp0_IP_a	First Octet	Quickly	
1322	ppp0_IP_b	Second Octet	Quickly	
1323	ppp0_IP_c	Third Octet	Quickly	
1324	ppp0_IP_d	Fourth Octet	Quickly	
1325	ppp0_Subnet_a	First Octet	Quickly	
1326	ppp0_Subnet_b	Second Octet	Quickly	
1327	ppp0_Subnet_c	Third Octet	Quickly	
1328	ppp0_Subnet_d	Fourth Octet	Quickly	
1329	ppp0_DHCP	NA	Often	NA, always 0
1330	ppp0_Link	Link Status	Quickly	0 = No Link, 1 = Link detected
1331	wwan0_IP_a	First Octet	Quickly	
1332	wwan0_IP_b	Second Octet	Quickly	
1333	wwan0_IP_c	Third Octet	Quickly	
1334	wwan0_IP_d	Fourth Octet	Quickly	
1335	wwan0_Subnet_a	First Octet	Quickly	
1336	wwan0_Subnet_b	Second Octet	Quickly	
1337	wwan0_Subnet_c	Third Octet	Quickly	
1338	wwan0_Subnet_d	Fourth Octet	Quickly	

1339	wwan0_DHCP	NA	Often	0 = Static IP, 1 = DHCP Assigned IP
1340	wwan0_Link	Link Status	Quickly	0 = No Link, 1 = Link detected
1341	br0_IP_a	First Octet	Quickly	
1342	br0_IP_b	Second Octet	Quickly	
1343	br0_IP_c	Third Octet	Quickly	
1344	br0_IP_d	Fourth Octet	Quickly	
1345	br0_Subnet_a	First Octet	Quickly	
1346	br0_Subnet_b	Second Octet	Quickly	
1347	br0_Subnet_c	Third Octet	Quickly	
1348	br0_Subnet_d	Fourth Octet	Quickly	

RAMQTT - Service Status				
Index	Name	Description	Frequency	Notes
1401	RAMQTT_Connection	RAMQTT Connection	Rapidly	1 - Connected, else 0
1402	RAMQTT_Connect_Time_A	UINT32;LSW	Rapidly	
1403	RAMQTT_Connect_Time_B	UINT32	Rapidly	
1404	RAMQTT_Connect_Time_DD	Connected time Days	Rapidly	
1405	RAMQTT_Connect_Time_HH	Connected time Hours	Rapidly	
1406	RAMQTT_Connect_Time_MM	Connected time Minutes	Rapidly	
1407	RAMQTT_Connect_Time_SS	Connected time Seconds	Rapidly	
1408	RAMQTT_Error_Code_M2X	API Error Codes from M2X	Often	400 - Bad Request, 401 - Unauthorized, 403 - Forbidden, 404 - Not Found, 429 - Too Many Requests, 500 through 504 - Server Error
1409	RAMQTT_Error_Code_AWS	API Error Codes from AWS	Often	400 - Bad Request (Invalid JSON), 401 - Unauthorized, 403 - Forbidden, 404 - Not Found (Thing not Found), 409 - Version Conflict, 413 - Payload Too Large, 415 - Unsupported Media Type (Non UTF-8 Encoding), 429 - Too Many Requests, 500 - Internal Server Error
1410	RAMQTT_Error_Code_FC	API Error Codes from Fusion Connect	Often	

Events - Event Status and Clearing				
Index	Name	Description	Frequency	Notes
1501	Event1_Status	0 = False; 1 = True; 2 = Error	Quickly	Status of the event as currently True or False
1601	Event1_Clear_Condition	Write a 1 to clear an event condition	Quickly	Write a 1 here to clear a manual event. Once cleared, this value will change back to 0.
1502	Event2_Status		Quickly	
1602	Event2_Clear_Condition		Quickly	
...				

1599	Event99_Status		Quickly	
1699	Event99_Clear_Condition		Quickly	

Cellular - All cellular points are from cardstats file				
Index	Name	Description	Frequency	Notes
1701	IMEI_a	First 4 digits, UINT16	Often	
1702	IMEI_b	Next 4 digits	Often	
1703	IMEI_c	Next 4 digits	Often	
1704	IMEI_d	Last 4 digits	Often	
1705	ESN_a	UINT 64 - LIttle Endian; LSW	Often	3G-ESN should be found by viewing the number in Hex.
1706	ESN_b		Often	3G-ESN = Reg1705 + (2^16 * Reg1706)
1707	ESN_c		Often	
1708	ESN_d		Often	
1709	MDN_a	First 4 digits, UINT16	Often	MDN is the Machine Device number (phone number) assigned to the SIM or CDMA module if no SIM
1710	MDN_b	Next 4 digits	Often	
1711	MDN_c	Next 4 digits	Often	
1712	MDN_d	Last 4 digits	Often	
1713	SIMSTATUS		Often	1 = Available, 0 = otherwise
1714	MODEL		Often	3 or 4 digit chipset model
1715	RSSI	units are -dBm	Often	Absolute value shown
1716	ECIO	units are dB	Often	Absolute value shown
1717	RSRP	units are -dBm	Often	Absolute value shown
1718	RSRQ	units are -dBm	Often	Absolute value shown
1719	CURRENTCHAN		Often	
1720	CellUpTime_Days	Days 0 - 9999	Often	Time in current cellular connection
1721	CellUpTime_Hours	Hours 0 - 23	Often	
1722	CellUpTime_Minutes	Minutes 0 - 59	Often	
1723	CellUpTime_Seconds	Seconds 0 - 59	Often	
1724	CellUpTime_TotalSecondsA	UINT32	Often	Time in current cellular connection as a total of seconds
1725	CellUpTime_TotalSecondsB	UINT32	Often	
1726	IMEI_A	UINT 64 - Little Endian; LSW	Often	IMEI = (Reg1726 + (Reg1727 * 2^16) + (Reg1728 * 2^32) + (Reg1729 * 2^48))
1727	IMEI_B		Often	
1728	IMEI_C		Often	
1729	IMEI_D		Often	
1730	MDN_A	UINT 64 - Little Endian; LSW	Often	MDN = (Reg1730 + (Reg1731 * 2^16) + (Reg1732 * 2^32) + (Reg1733 * 2^48))
1731	MDN_B		Often	
1732	MDN_C		Often	
1733	MDN_D		Often	
1734	MEID_A	UINT 64 - Little Endian; LSW	Often	MEID = (Reg1734 + (Reg1735 * 2^16) + (Reg1736 * 2^32) + (Reg1737 * 2^48))

1735	MEID_B		Often	MEID should be found by viewing the number in Hex.
1736	MEID_C		Often	
1737	MEID_D		Often	
1738	SIM_ID_A	UINT 64 - Little Endian; LSW	Often	SIM_ID = (Reg1738 + (Reg1739 * 2^16) + (Reg1740 * 2^32) + (Reg1741 * 2^48))
1739	SIM_ID_B		Often	
1740	SIM_ID_C		Often	
1741	SIM_ID_D		Often	
1742	SIM_IMSI_A	UINT 64 - Little Endian; LSW	Often	SIM_IMSI = (Reg1742 + (Reg1743 * 2^16) + (Reg1744 * 2^32) + (Reg1745 * 2^48))
1743	SIM_IMSI_B		Often	
1744	SIM_IMSI_C		Often	
1745	SIM_IMSI_D		Often	
1746	SIM_CARRIER_NUMBER_A	UINT32; LSW	Often	SIM_CARRIER_NUMBER = Reg1746 + (Reg1747 * 2^16)
1747	SIM_CARRIER_NUMBER_b	UINT32; MSW	Often	
1748	CARRIER_PLMN_A	UINT32; LSW	Often	CARRIER_PLMN = Reg1748 + (Reg1749 * 2^16)
1749	CARRIER_PLMN_B	UINT32; MSW	Often	
1750	SERVICE_TYPE_E	0=No Service; See Appx.B Notes	Often	0=NO SERVICE; 1=CDMA 1xRTT; 2=CDMA 1xEVDO; 3=AMPS (unsupported); 4=GSM; 5=UMTS; 6=WLAN; 7=GPS; 8=LTE; Others=Unknown;
1751	DATA_BEARER_E	0 or 255 = Unknown; See Appx.B Notes	Often	0=Unknown; 1=CDMA 1xRTT; 2=CDMA 1xEV-DO Rev 0; 3=GPRS; 4=WCDMA; 5=CDMA 1xEV-DO Rev A; 6=EDGE; 7=HSDPA DL, WCDMA UL; 8=WCDMA DL, HSUPA UL; 9=HSDPA DL, HSUPA UL; 10=LTE; 11=CDMA EV-DO Rev A EHRPD; 12=HSDPA+ and WCDMA; 13=HSDPA+ and HSUPA; 14=DC_HSDPA+ and WCDMA; 15=DC_HSDAP+ and HSUPA; 16=NULL Bearer;
1752	RADIO_IF_E	0=No Service; See Appx.B Notes	Often	0=NO SERVICE; 1=CDMA 1xRTT; 2=CDMA 1xEVDO; 3=AMPS (unsupported); 4=GSM; 6=UMTS; 6=WLAN; 7=GPS; 8=LTE; Others=Unknown;
1753	SYS_MODE_E	0=No Service; See Appx.B Notes	Often	0=No Service; 1=AMPS; 2=CDMA; 3=GSM; 4=HDR; 5=WCDMA; 6=GPS; 7=WLAN; 8=LTE; Others=Unknown;
1754	SESSION_STATE	0=Disconnected; 1=Otherwise	Often	0=Home; 1=Roaming; 2=Roaming, Partner; >2=Unknown;
1755	SESSION_IPV4_STATE	0=Disconnected; 1=Otherwise	Often	
1756	SESSION_IPV6_STATE	0=Disconnected; 1=Otherwise	Often	
1757	LAST_SESSION_END_EREASON	See Appx.B Notes	Often	
1758	ROAMING	1=Roaming; 0=Not Roaming	Often	0=Home; 1=Roaming; 2=Roaming, Partner; >2=Unknown;

1759	SERVSYS_MCC	Mobile Country Code	Often	
1760	SERVSYS_MNC	Mobile Network Code	Often	
1761	SERVSYS_SYSTEM_ID	Serving System ID	Often	
1762	SERVSYS_SYSTEM_ID	Serving System ID	Often	
1763	SERVSYS_BS_ID	Base Station ID	Often	
1764	SERVSYS_LAC	Location Area Code	Often	
1765	SERVSYS_CELL_ID_A	System Cell ID - UINT32; LSW	Often	SERVSYS_CELL_ID = Reg1765 + (Reg1766 * 2^16)
1766	SERVSYS_CELL_ID_B	UINT32; MSW	Often	
1767	SMS_SENT	Number of Send SMS	Often	
1768	SMS_SENT_FAIL	Number of Failed Send SMS	Often	
1769	SMS_RECV	Number of received SMS	Often	
1770	SINR	Signal Interference + Noise Ratio	Often	
1771	RSSI_ABS	absolute; units are -dBm	Often	
1772	ECIO_ABS	absolute; units are -dB	Often	
1773	RSRP_ABS	absolute; units are -dBm	Often	
1774	RSRQ_ABS	absolute; units are -dBm	Often	
1775	SIM_ID_A	First 3 or 4 digits UINT16	Often	
1776	SIM_ID_B	Next 4 digits	Often	
1777	SIM_ID_C	Next 4 digits	Often	
1778	SIM_ID_D	Next 4 digits	Often	
1779	SIM_ID_E	Last 4 digits	Often	
1780	SIM_ID_LUHN_CHECKSUM	Last digit of SIM ID as LUHN checksum	Often	

Appendix C

SMS Handler Commands

This appendix contains a table of all currently available commands for the SMS handler. The commands are separated into three parts: command, target, and action. Not all commands will use all three. Most commands will have an abbreviated option shown after the forward slash (/).:

Command	Target	Action
Login / log	<password>	
Quit / qui exit / exi		
get / g	gps wwanip / wwa ethip / eth celldata / cel ipsec / ips openvpn / ope ssh ramqtt / ram device / dev cmd event / eve	status / sta lat long locate / loc status / sta active / act all <event name> <event #>
read / r	Tag name IO Notation (1 - based)	Value value
write / w	Tag name IO Notation (1 - based)	value value
do /d	celldata / cel ipsec /ips openvpn / ope ssh modbus / mod SVM datalog / dat cmd event / eve	on,off, or reset on,off, or restart on,off, or restart on,off, or restart on,off, or restart trigger / tri ratate / rot newline / new <filename> <event_#> clear / cle <event_name> clear / cle all clear / cle
help / ?	<command>	