Sixnet® Series

RAM®-6021 Router Software

Firmware Version 4.24

Software Manual | August 2016

Drawing No. LP0979-B

COPYRIGHT

©2015-2016 Red Lion Controls, Inc. All rights reserved. Red Lion, the Red Lion logo and Sixnet are registered trademarks of Red Lion Controls, Inc. All other company and product names are trademarks of their respective owners.

Red Lion Controls, Inc.

20 Willow Springs Circle

York, PA 17406

CONTACT INFORMATION:

AMERICAS

Inside US: +1 (877) 432-9908
Outside US: +1 (717) 767-6511
Hours: 8am-6pm Eastern Standard Time
(UTC/GMT -5 hours)

ASIA-PACIFIC

Shanghai, P.R. China: +86 21-6113-3688 x767
Hours: 9am-6pm China Standard Time
(UTC/GMT +8 hours)

EUROPE

Netherlands: +31 33-4723-225
France: +31 (0) 1 84 88 75 25
Germany: +49 (0) 1 89 5795-9421
UK: +44 (0) 20 3868 0909
Hours: 9am-5pm Central European Time
(UTC/GMT +1 hour)

Website: www.redlion.net

Email: support@redlion.net

Table of Contents

Disclaimer . . . iii
Purpose . . . iii
Audience . . . iii
Compliance Statements & User Information . . . iii
FCC Compliance Statement . . . iii
User Compliance Information . . . iv
Canadian Compliance Statement . . . iv
Trademark Acknowledgments . . . iv
Document History and Related Publications . . . iv
Publication History . . . v
Related Documents . . . v
Additional Product Information . . . v
Document Comments . . . v
Chapter 1 Accessing the Web User Interface . . . 1-1
1.1 Connect PC to Red Lion Router . . . 1-1
1.2 Setup PC IP Address . . . 1-2
1.2.1 Open the Control Panel . . . 1-2
1.2.2 Access Network and Settings . . . 1-3
1.2.3 Access Network Connection Settings . . . 1-4
1.2.4 Access Local Area Connection . . . 1-4
1.2.5 Open Properties . . . 1-5
1.2.6 Access Internet Protocol Properties . . . 1-5
1.3 Access Red Lion Web Server . . . 1-9
1.3.1 Red Lion Router Login Instructions . . . 1-9
Chapter 2 Web User Interface . . . 2-11
2.1 Web User Interface Introduction . . . 2-11
2.1.1 Organization . . . 2-11
2.2 Status Tab . . . 2-12
2.2.1 Summary . . . 2-12
2.2.2 EZ Config Wizard . . . 2-13
2.2.3 Network . . . 2-16
2.2.4 Diagnostics . . . 2-22
2.2.5 Syslog . . . 2-26
2.2.6 Gather Stats . . . 2-27
2.3 Admin Tab . . . 2-28
2.3.1 Access Settings . . . 2-28
2.3.2 System Time . . . 2-30
2.3.3 Certificate Manager . . . 2-31
2.3.4 Firmware Update . . . 2-33
2.3.5 Configuration Manager . . . 2-34
2.3.6 Package Installation . . . 2-37

2.3.7 Factory Defaults/Reboot . . . 2-38
2.3.8 Job Control . . . 2-39
2.4 Network Tab . . . 2-41
2.4.1 Interfaces . . . 2-41
2.4.2 Firewall . . . 2-48
2.4.3 Tunneling . . . 2-64
2.4.4 DNS Settings . . . 2-71
2.4.5 Static Routes . . . 2-73
2.4.6 TCP Global Settings . . . 2-75
2.5 Services Tab . . . 2-77
2.5.1 DHCP Server . . . 2-77
2.5.2 DHCP Relay . . . 2-80
2.5.3 Dynamic DNS . . . 2-83
2.5.4 SN Proxy Settings . . . 2-84
2.5.5 SixView Manager . . . 2-85
2.5.6 SSH/TELNET Server . . . 2-87
2.5.7 SSL Connections . . . 2-89
2.5.8 SNMP Agent . . . 2-94
2.5.9 Ping Alive . . . 2-95
2.5.10 Serial IP . . . 2-96
2.5.11 Email Client . . . 2-103
2.5.12 RAMQTT Client . . . 2-104
2.6 Automation Tab . . . 2-107
2.6.1 Local Station . . . 2-108
2.6.2 Serial Ports . . . 2-109
2.6.3 Tags . . . 2-111
2.6.4 Data Logger . . . 2-114
2.6.5 Modbus . . . 2-118
2.6.6 DNP3 . . . 2-126
2.6.7 I/O Settings . . . 2-148
2.7 Advanced Tab . . . 2-151
2.7.1 Out-of-Band Management . . . 2-151
2.7.2 VRRP (Virtual Redundancy Protocol) . . . 2-153
2.7.3 Expert Mode . . . 2-154
2.7.4 GWLNX . . . 2-157
2.7.5 Classic View . . . 2-167
2.8 Events . . . 2-169

Service and Support Information . . . 3-181

Service Information . . . 3-181
Product Support . . . 3-181

Licensing & Warranty . . . 4-183

Appendix A . . . A-185

Appendix B . . . B-193

Preface

Disclaimer

Portions of this document are intended solely as an outline of methodologies to be followed during the maintenance and operation of the RAM-6021 Router 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 functions on the Red Lion Sixnet® Series RAM-6021 Routers.

Note: The RAM-6021 is a wired router. References to cellular connections throughout this manual do not apply to the RAM-6021.

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 router functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

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.

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/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
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
2016-04-04	April 2016	Supporting Firmware Version 3.23/4.23
2016-08-31	August 2016	Supporting Firmware Version 3.24/4.24

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 and in the Service and Support section.

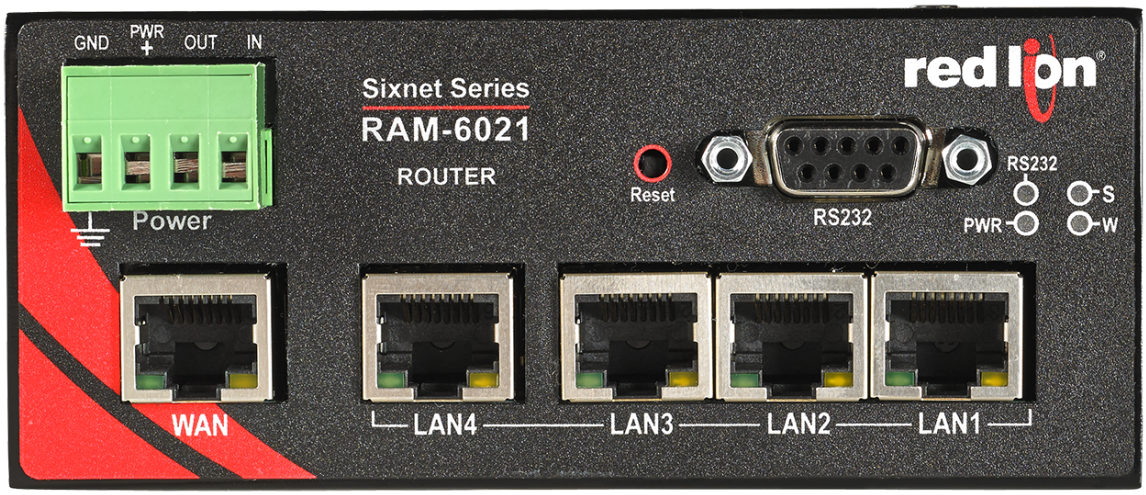
Document Comments

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

1.1 Connect PC to Red Lion Router

Connect a CAT-5 or CAT-6 Ethernet cable between the local PC and the Red Lion 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.

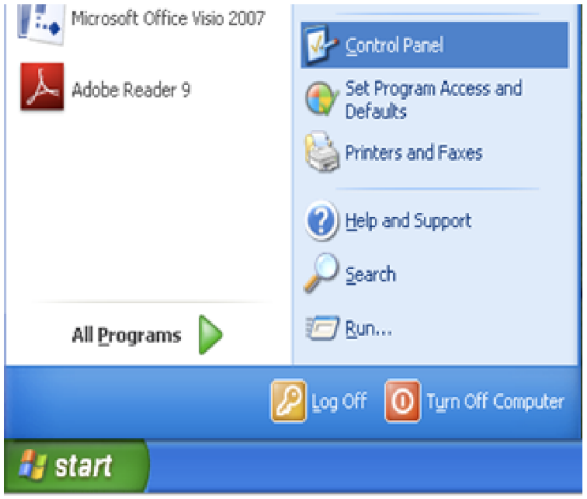
Note: The RAM-6021 is a wired router. References to cellular connections do not apply to the RAM-6021.

1.2 Setup PC IP Address

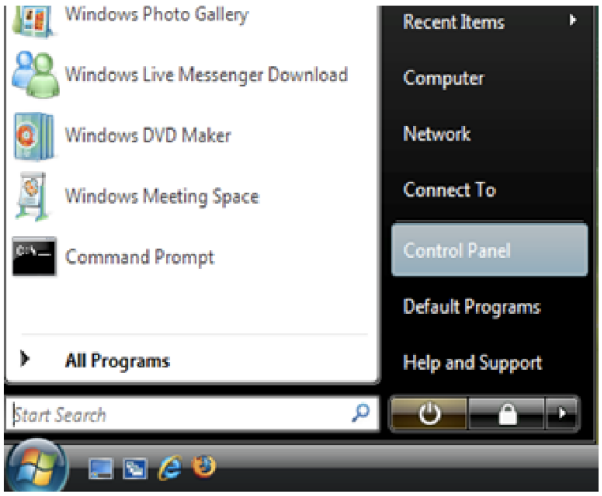
1.2.1 Open the Control Panel

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

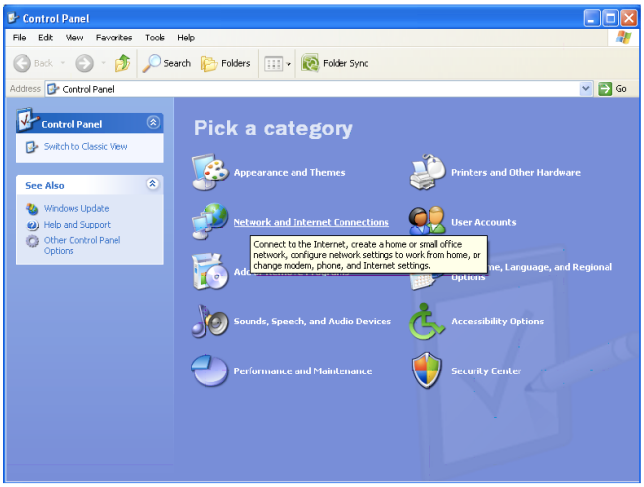
XP



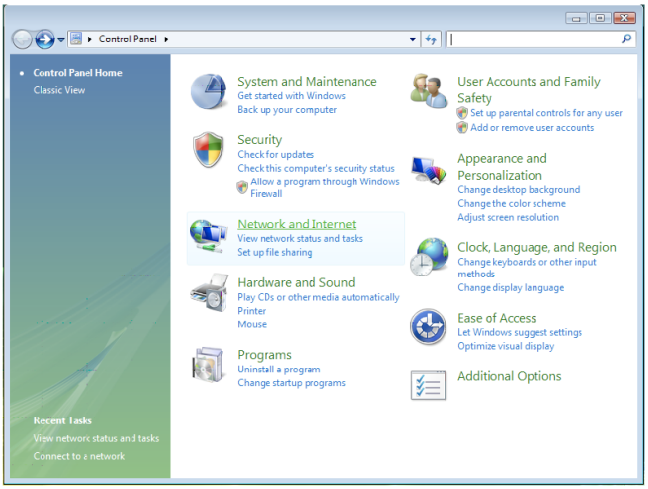
Vista/Windows 7



XP



VISTA/WINDOWS 7



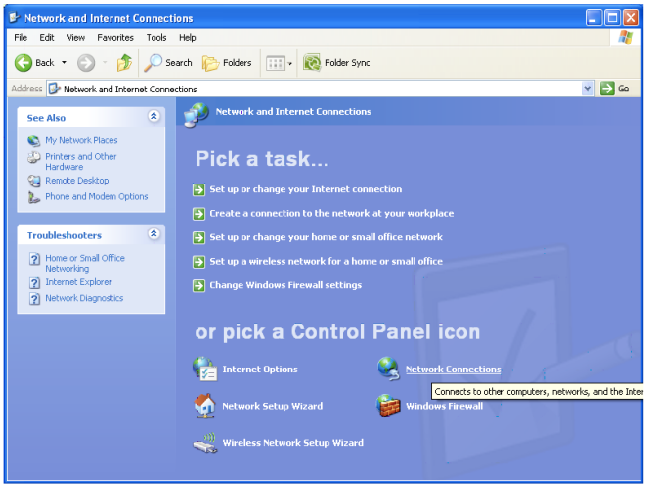
1.2.2 Access Network and Settings

Click on the link to access network and Internet settings

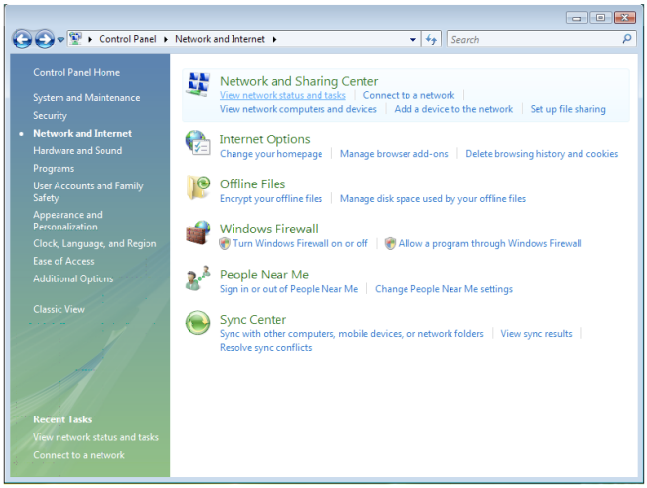
- XP - “Network and Internet Connections”
- Vista/Windows 7 “Network and Internet”

The displays should be similar to the following:

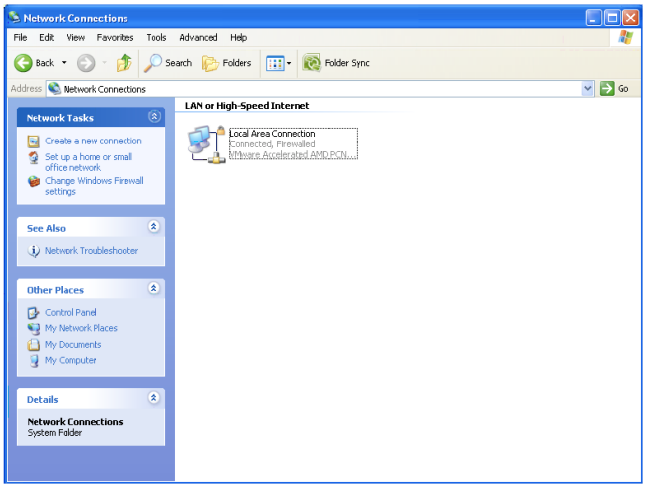
XP



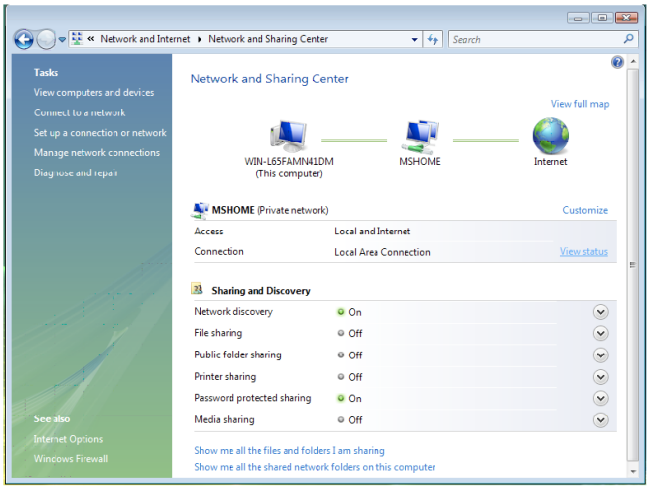
VISTA/WINDOWS 7



XP



Vista/Windows 7



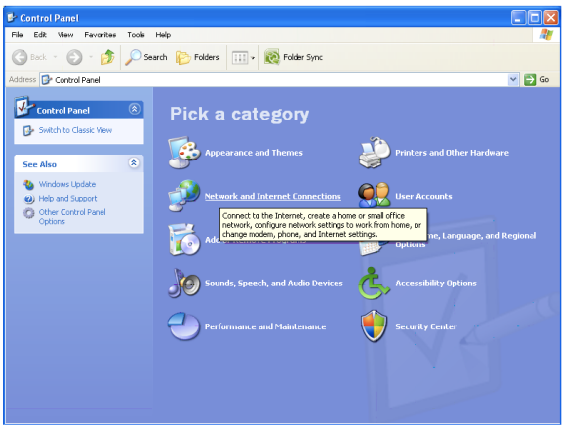
1.2.3 Access Network Connection Settings

Click on the link to access network connection settings.

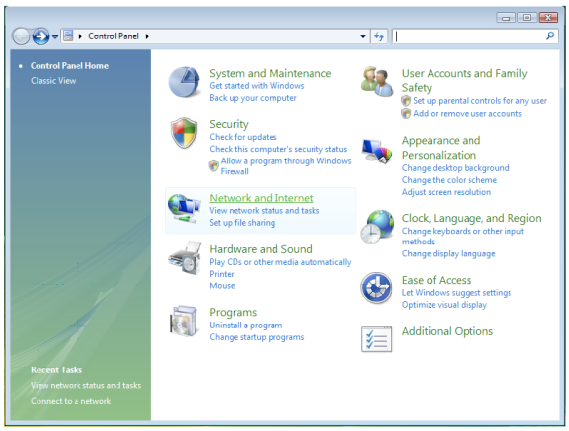
- XP - “Network Connections”
- Vista/Windows 7 - “Network and Sharing Center”

The display should look similar to the following:

XP



VISTA/WINDOWS 7



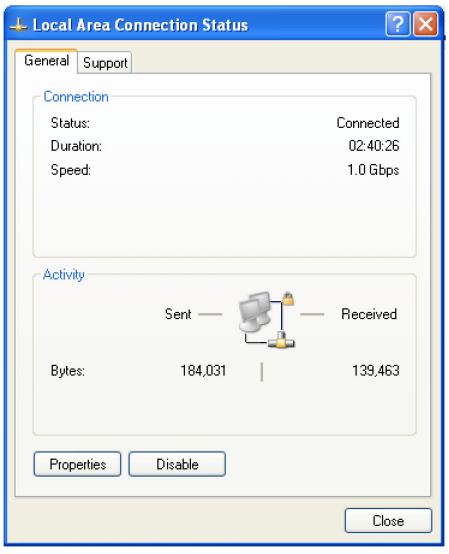
1.2.4 Access Local Area Connection

Click on the link to access the local area connection.

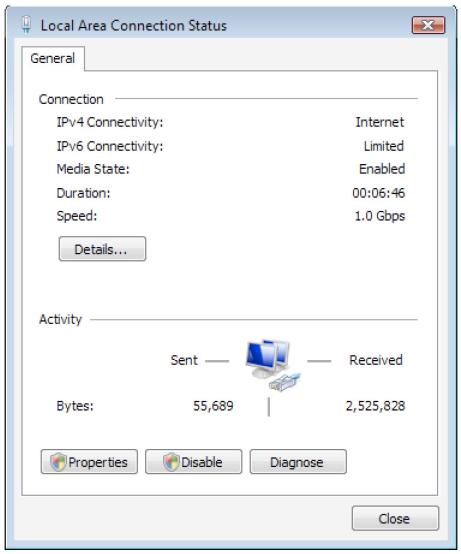
- XP - “Local Area Connection” icon
- Vista/Windows 7 - “View Status” next to Local Area Connection

The display should look similar to the following:

XP



Vista/Windows 7

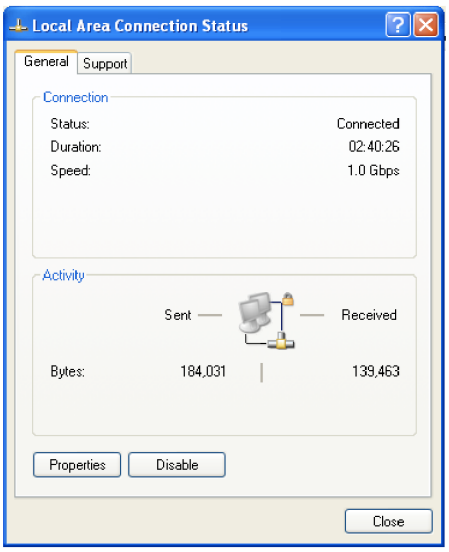


1.2.5 Open Properties

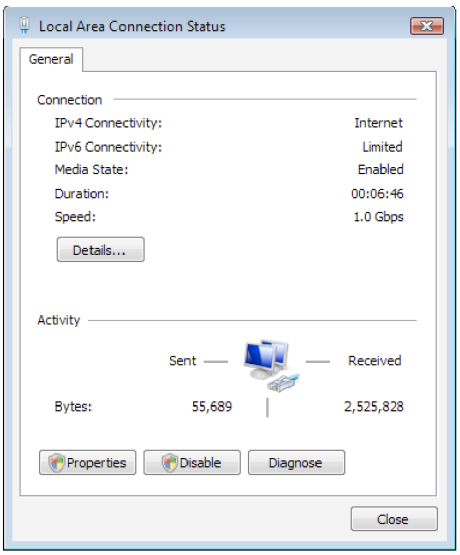
Click on “Properties” button (Vista/Windows 7 will display a popup window asking to confirm the operation).

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

XP



Vista/Windows 7



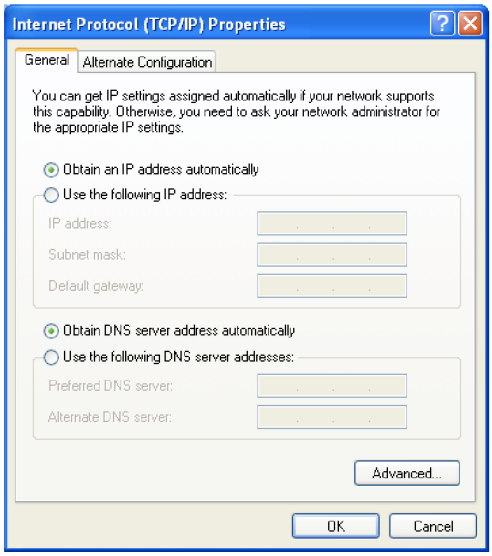
1.2.6 Access Internet Protocol Properties

Click on the Internet Protocol to highlight.

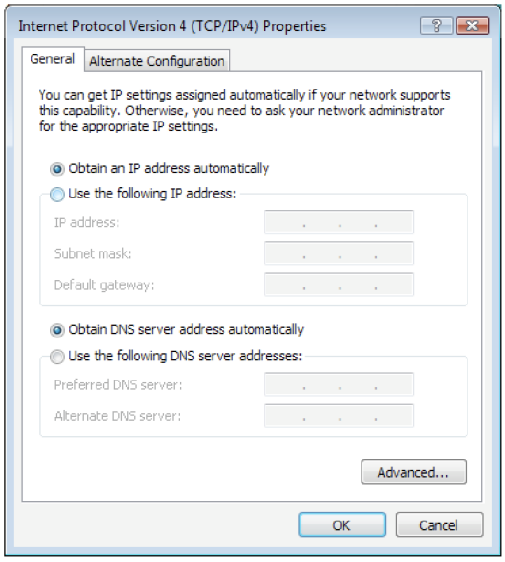
- XP - “Internet Protocol (TCP/IP)”
- Vista/Windows7 - “Internet Protocol Version 4 (TCP/IPv4)”

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

XP

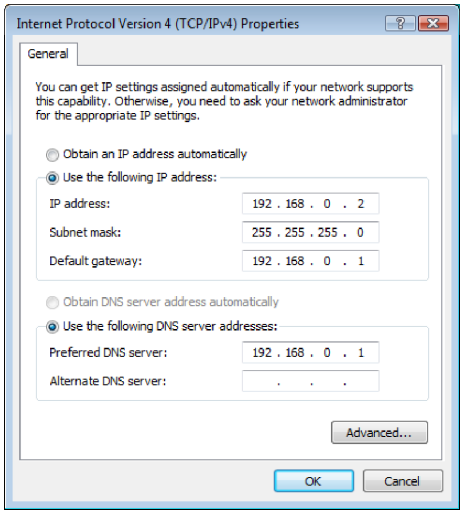


Vista/Windows 7



METHOD 1: PC to Ethernet on RAM-6021

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

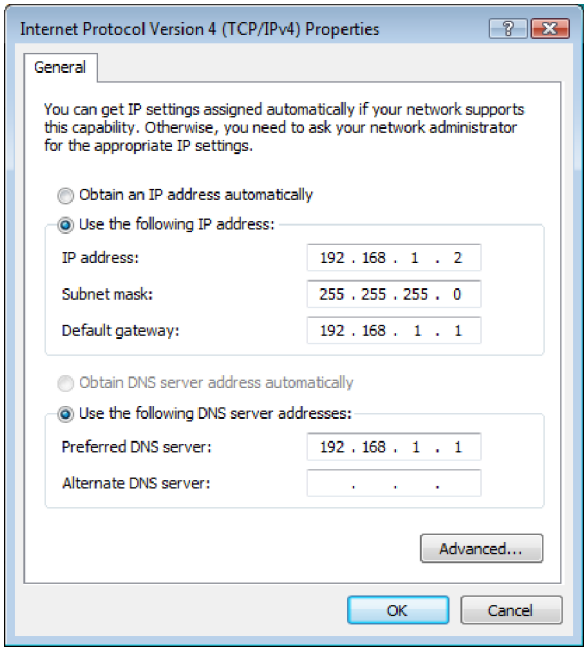
Click “OK”.

The previous screen will appear.

Click “OK”.

METHOD 2: PC to LAN (ETH1) (RAM-6021)

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”.

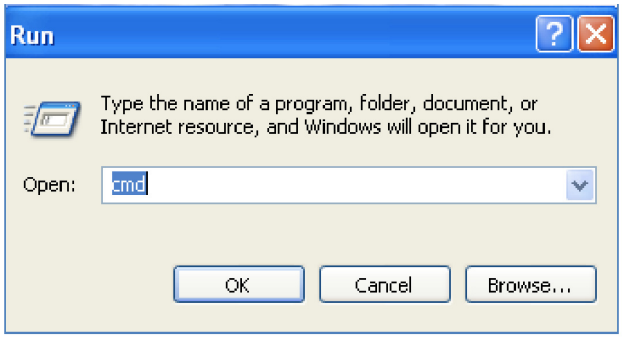
The previous screen will appear.

Click “OK”.

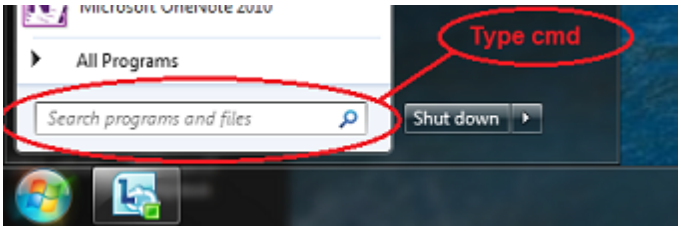
Verify that you are connected to the RAM-6021 router.

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.

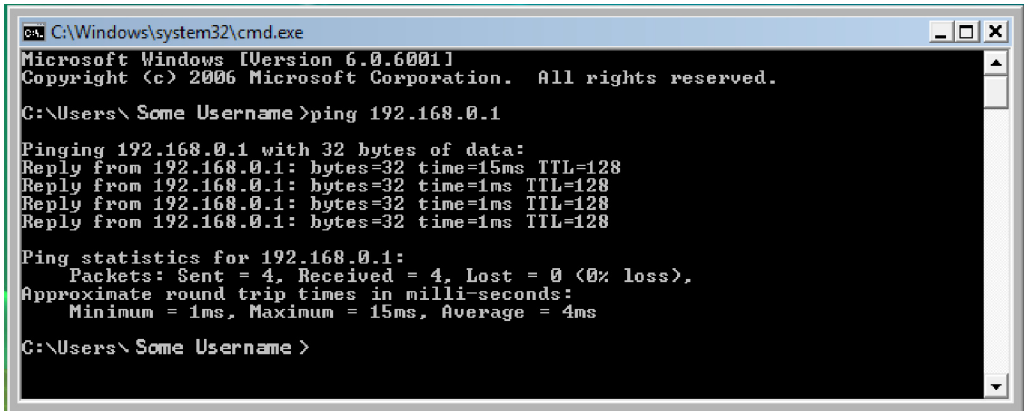


Verify connectivity to the router by running a “ping” to the IP Address of the Ethernet port you are connected to.

METHOD 1: PC to WAN (ETH0) (RAM-6021)

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

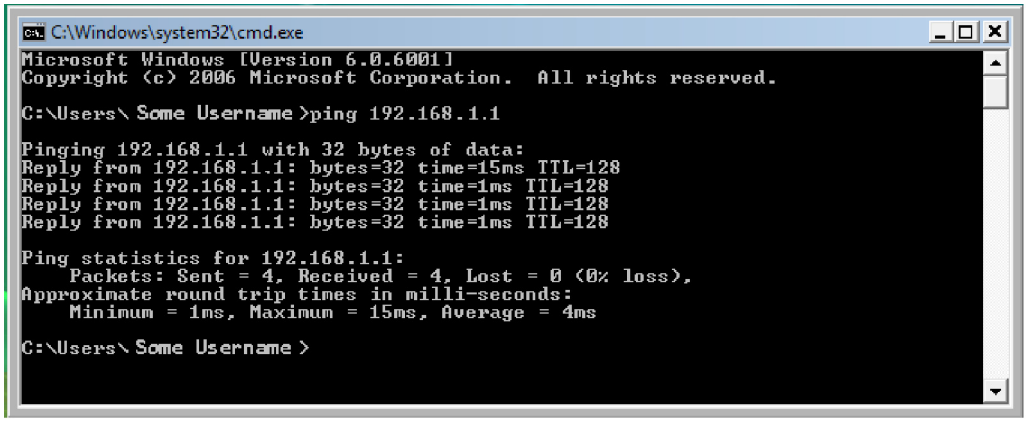
The display should look similar to the following:



METHOD 2: PC to ETH1 (LAN)

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 Access Red Lion Web Server

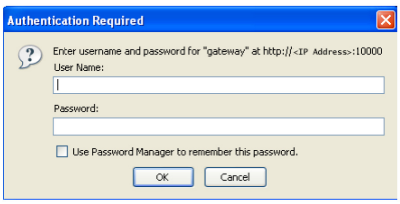
Open a web browser and enter the following in the address bar:

METHOD 1 (WAN/ETH0): http://192.168.0.1:10000/

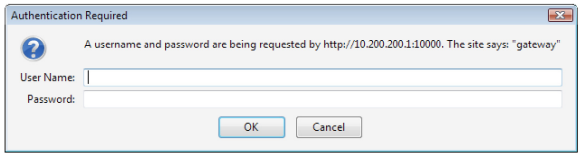
METHOD 2 (LAN/ETH1): http://192.168.1.1:10000/

You will receive a login pop-up screen.

XP



Vista/Windows 7



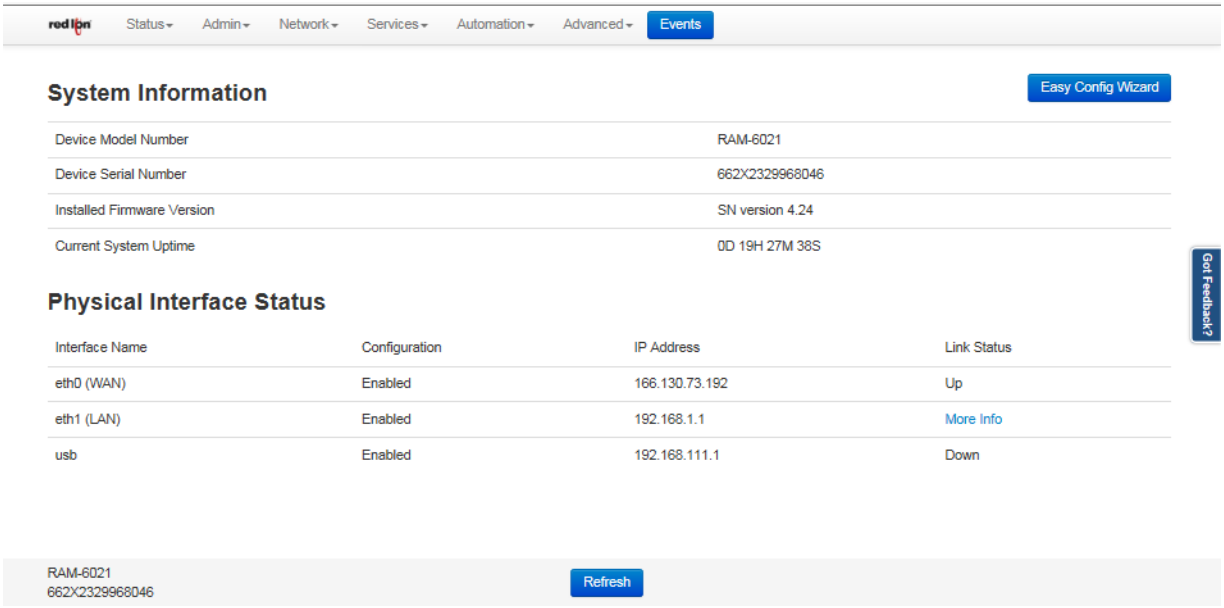
1.3.1 Red Lion Router Login Instructions

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 will appear:

Note: The following information can be used for all series of router, even if screen shots indicate other models. Some models may have reduced options.



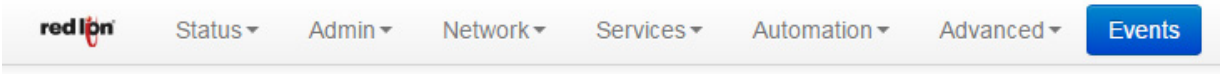
At this point, you are connected to the Red Lion router and can configure it to meet your needs.

Chapter 2 Web User Interface

2.1 Web User Interface Introduction

2.1.1 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 router. This tab is organized into 6 sections: Summary, Easy Config, Network, Diagnostics, Syslog and Gather Stats.
- Admin: The Admin Tab is used to configure how the Red Lion router is accessed, update the firmware, reset the system defaults, set the system time and reboot the router remotely. This tab is organized into 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 router to external interfaces. The Network tab is organized into 8 major categories: Cellular Connections (not applicable to the RAM-6021 Router) Interfaces, Firewall, Tunneling, DNS Settings, Static Routes, DNMR/NEMO (not applicable to the RAM-6021 Router) and TCP Global Settings.
- Services: The Services tab is used to configure the various features of the Red Lion RTU router. These services include DHCP Server, DHCP Relay, Dynamic DNS, SNProxy Settings, SixView Manager, SSH/TELNET Server, SSL Connections, SNMP Agent, Ping Alive, Crimson Connect, Email Client, SD Card Manager and Serial IP.
- Automation: The Automation menu contains all aspects of managing your Modbus and DNP3 based I/O. The Automation menu is organized into six categories: Local Station, Serial Ports, Tags, Data Logger, Modbu,sDNP3 and I/O Settings.
- Advanced: The Advanced Tab is used to configure the advanced features of the Red Lion router, which include IP Fallback, IP Transparency, Out-of-Band Management, VRRP, Expert Mode, GWLNX and Classic View.
- 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.

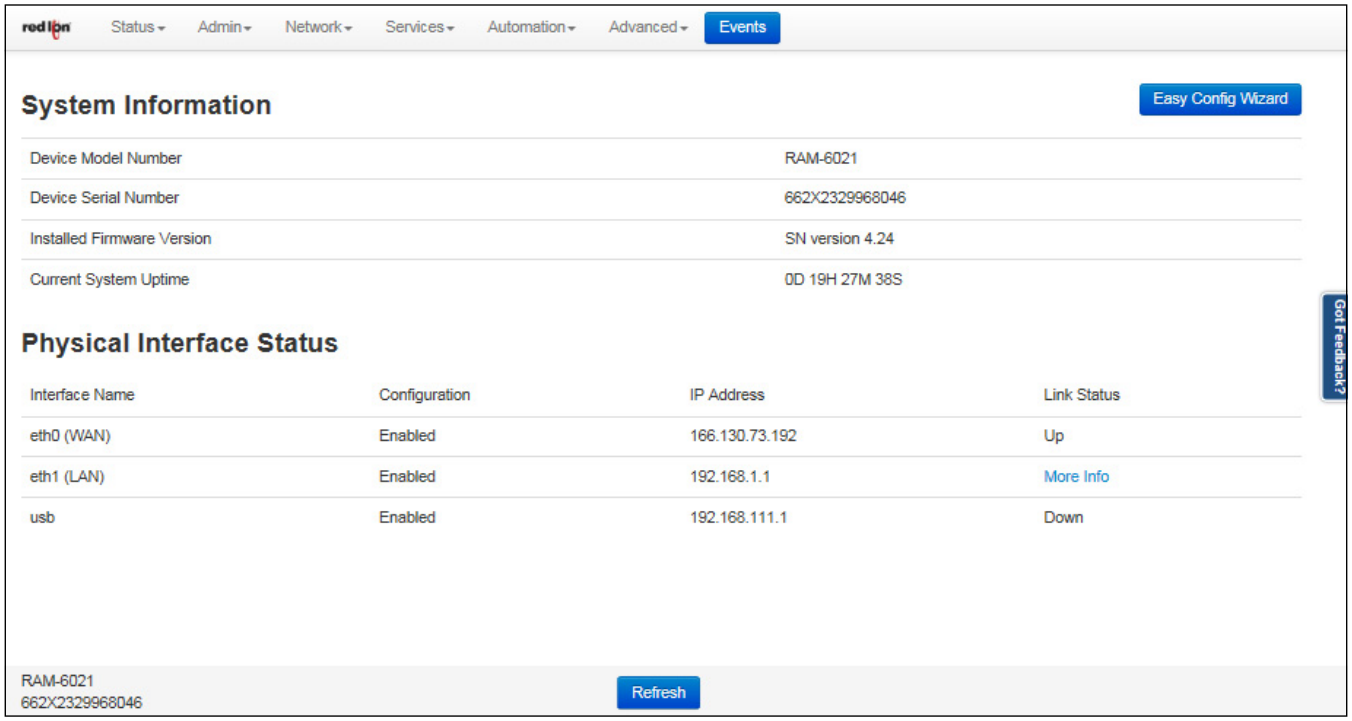
All tabs are described further in the manual as well as functionality of each dialog window.

2.2 Status Tab

The Status Tab allows you to review the state of the 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'.

2.2.1 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.

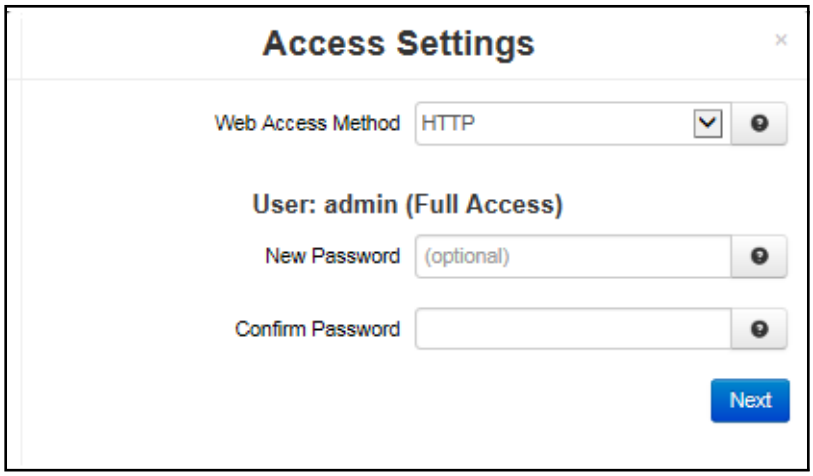


2.2.2 EZ Config Wizard

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.

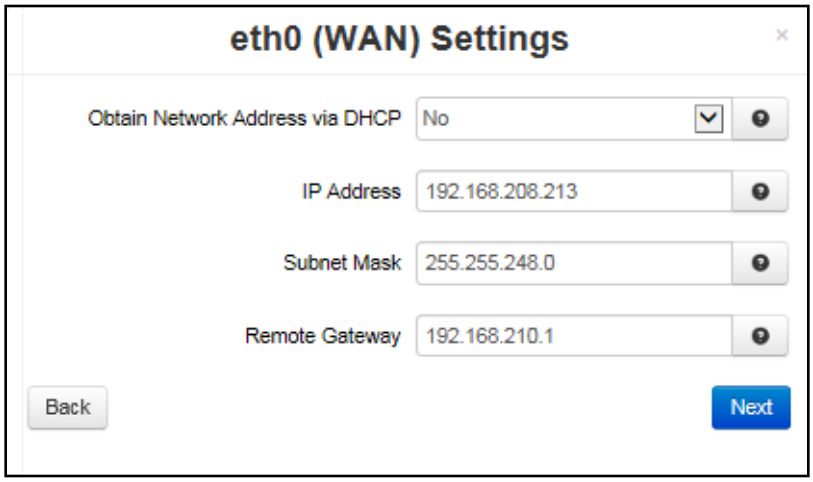
New Password: Enter the new password in this field.

> **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: 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 and the IP address assigned to the device is 192.168.1.1 through 192.168.1.254 as 192.168.1.255 is the value reserved for 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: 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*.

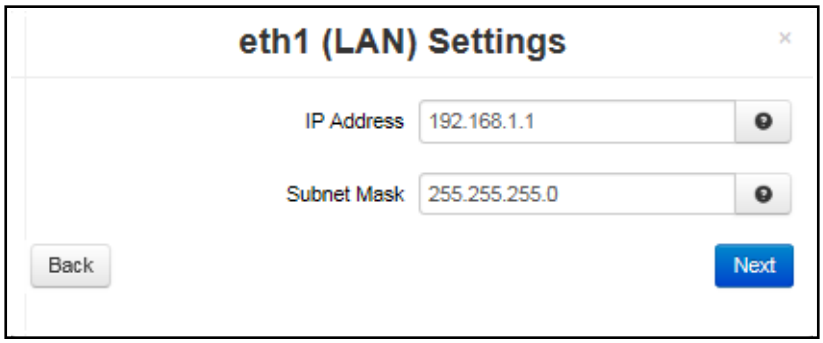
> **Recommended Setting***:* Your network administrator should be able to provide an appropriate value. This value determines the valid range of IP addresses allowed in the "Enter IP Address" field.

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 will appear:



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.

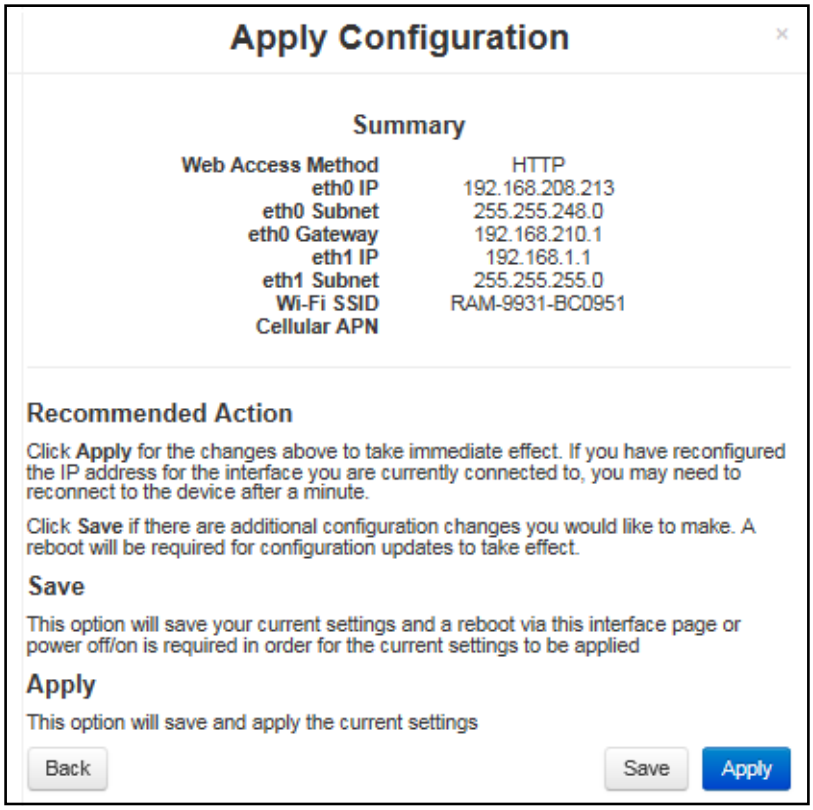
For example, if a netmask is 255.255.255.0 and the IP address assigned to the device is 192.168.1.1 through 192.168.1.254 as 192.168.1.255 is the value reserved for the broadcast address.

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: 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 a Apply Configuration dialog window will appear.



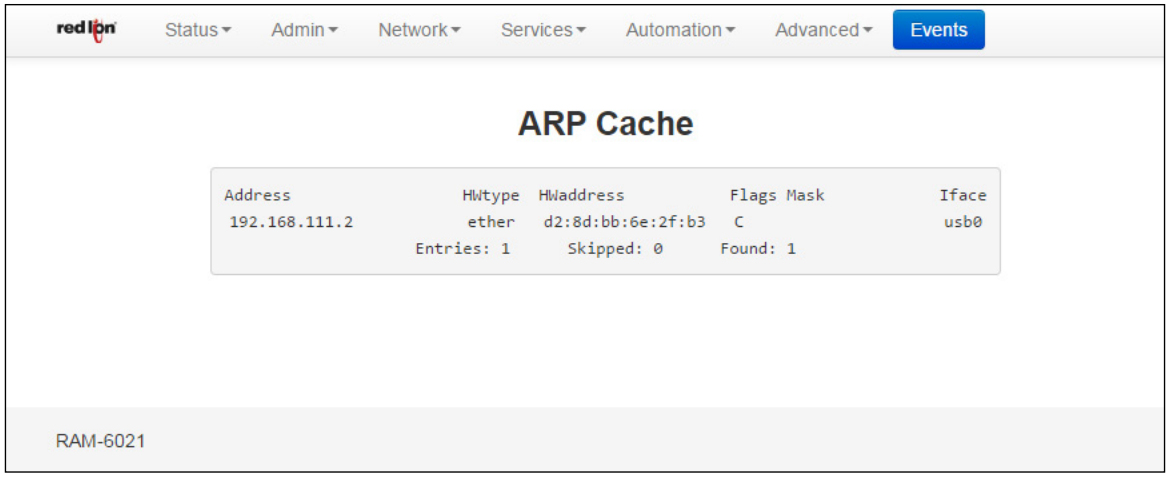
Click on *Back*, *Save* or *Apply* (*see explanation of each setting in dialog window above*).

2.2.3 Network

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

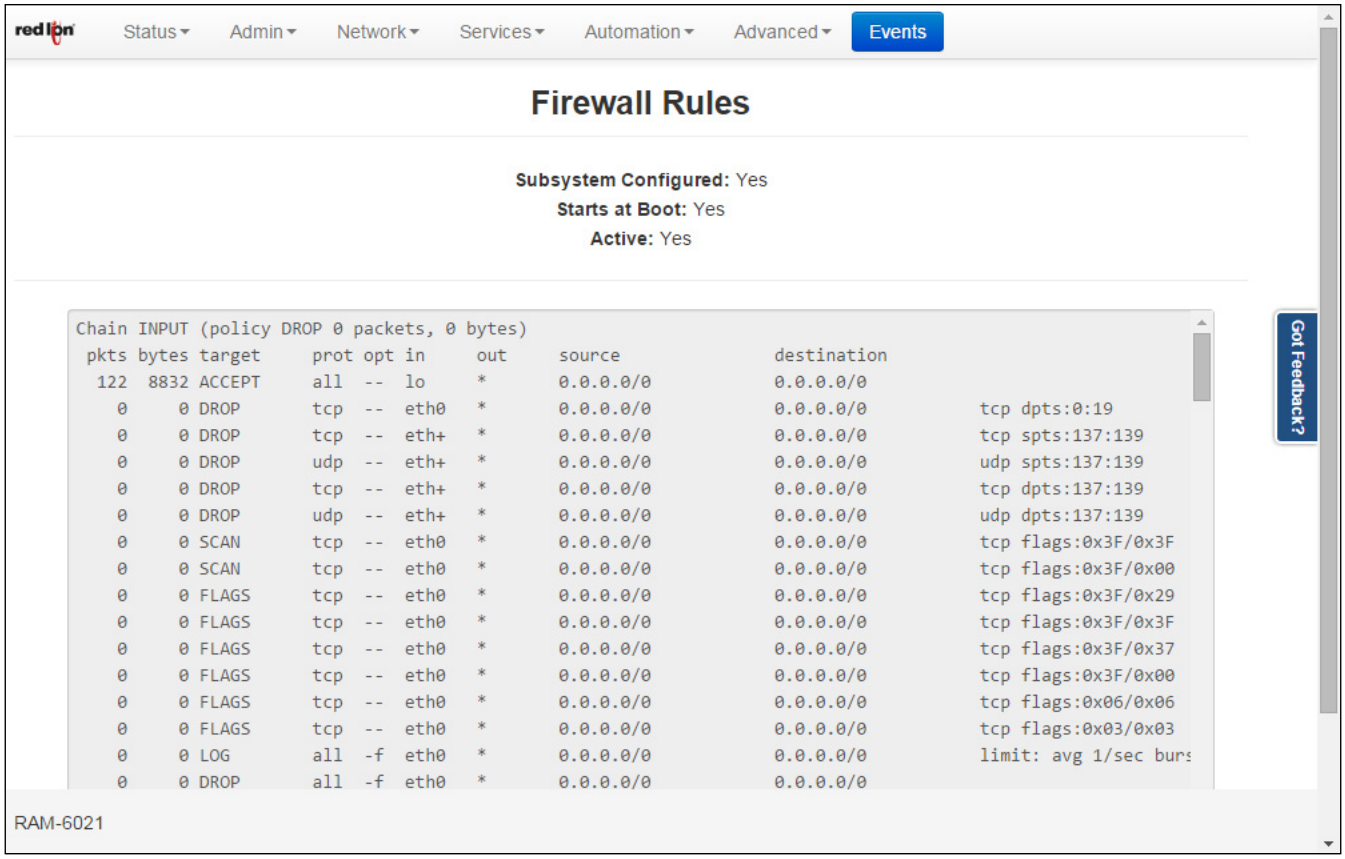
ARP Cache

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 router. When you click on the ARP Cache menu item, the ARP Cache dialog window will appear.



Firewall Rules

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

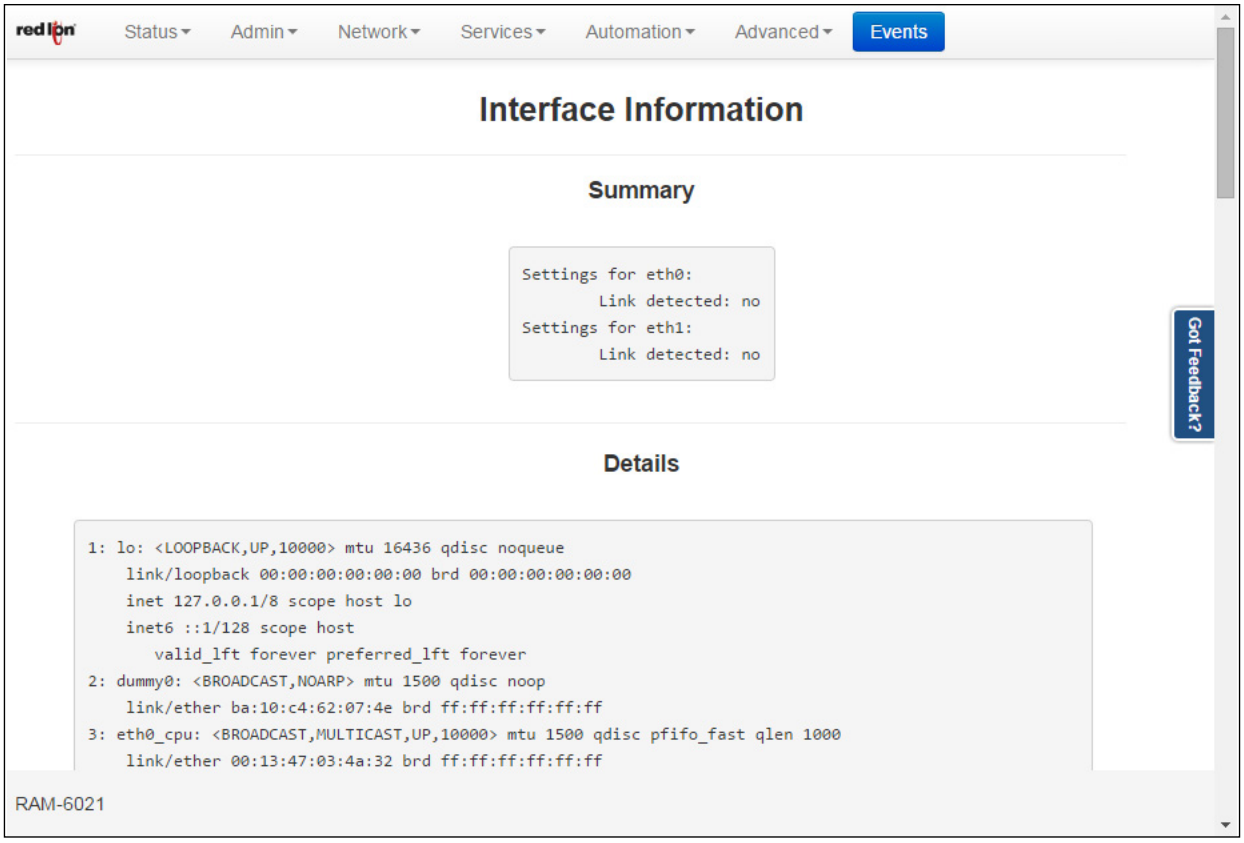



```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  122  8832 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpts:0:19
    0     0 DROP       tcp  --  eth+   *       0.0.0.0/0            0.0.0.0/0           tcp spts:137:139
    0     0 DROP       udp  --  eth+   *       0.0.0.0/0            0.0.0.0/0           udp spts:137:139
    0     0 DROP       tcp  --  eth+   *       0.0.0.0/0            0.0.0.0/0           tcp dpts:137:139
    0     0 DROP       udp  --  eth+   *       0.0.0.0/0            0.0.0.0/0           udp dpts:137:139
    0     0 SCAN       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x3F
    0     0 SCAN       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
    0     0 FLAGS      tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x29
    0     0 FLAGS      tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x3F
    0     0 FLAGS      tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x37
    0     0 FLAGS      tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
    0     0 FLAGS      tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x06/0x06
    0     0 FLAGS      tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x03/0x03
    0     0 LOG        all  -f  eth0   *       0.0.0.0/0            0.0.0.0/0           limit: avg 1/sec burs
    0     0 DROP       all  -f  eth0   *       0.0.0.0/0            0.0.0.0/0
```

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 router.

Interfaces

The Interfaces menu item has three sections. Summary, Details and Multicast.



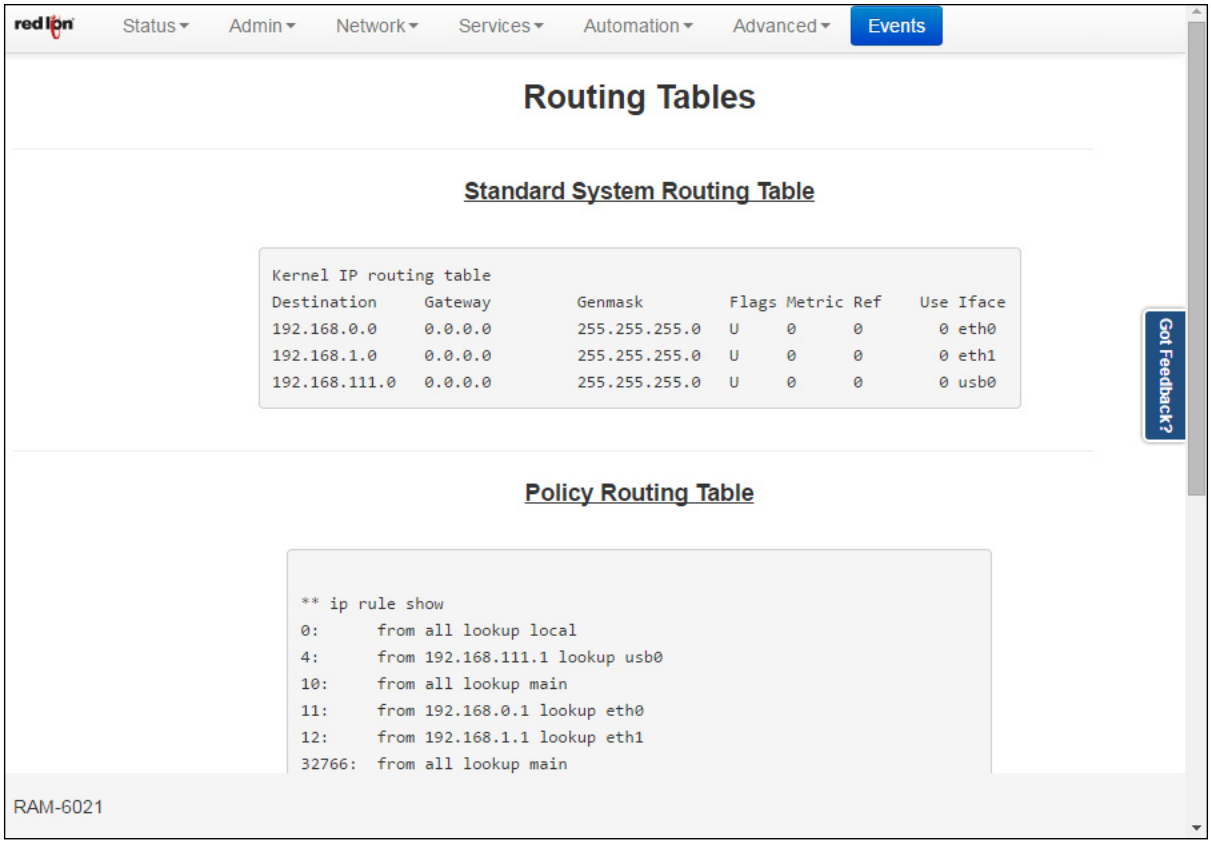
The Summary table displays a brief description of the interfaces of the Red Lion router.

The Details table displays a system specific description of the interfaces on the Red Lion 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 router and the static routes that have been configured for the 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 router.

Socket Statuses

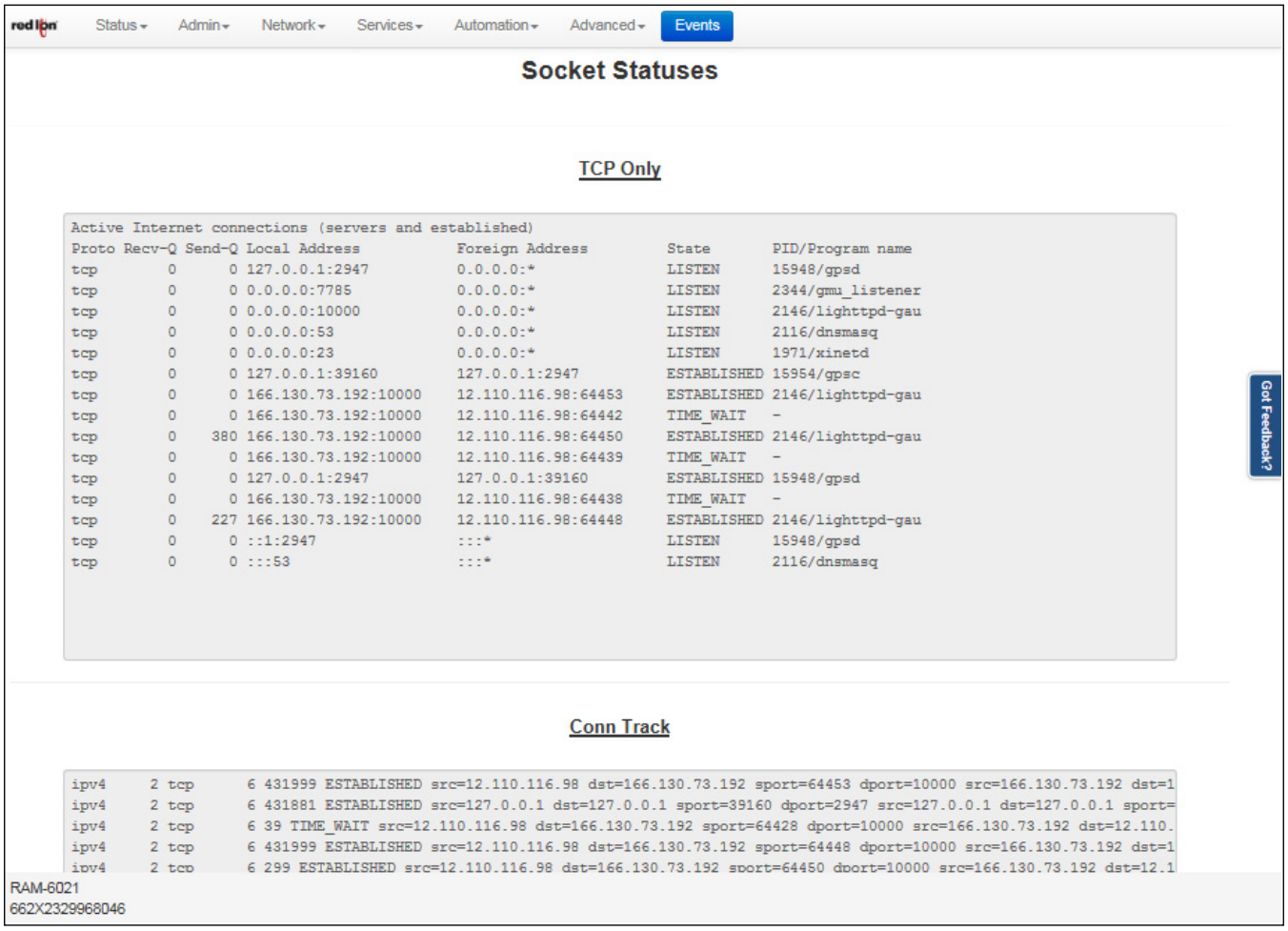
Sockets are end-points to communication over the Internet. Much like PBX phone systems, where the IP address is the phone number and the port is the extension. Every paired (connected) socket has a source IP/port and a destination IP/port.

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”).

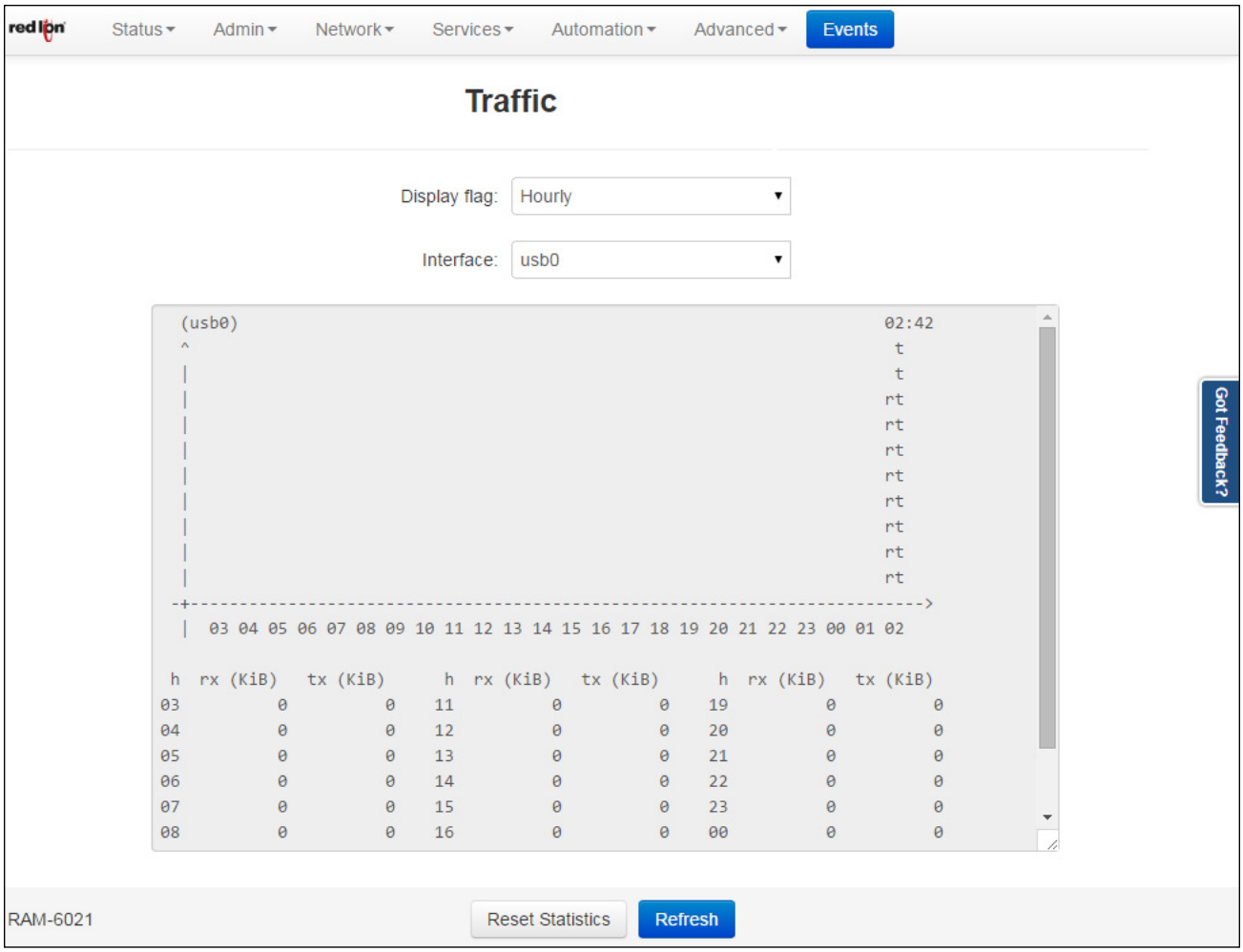
Conn Track is a connection tracker that displays more thorough information about the current socket connections. Connection tracking allows the kernel to keep track of all logical network connections or sessions, and thereby relate all of the packets which may make up that connection. NAT relies on this 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 on the dialog window.

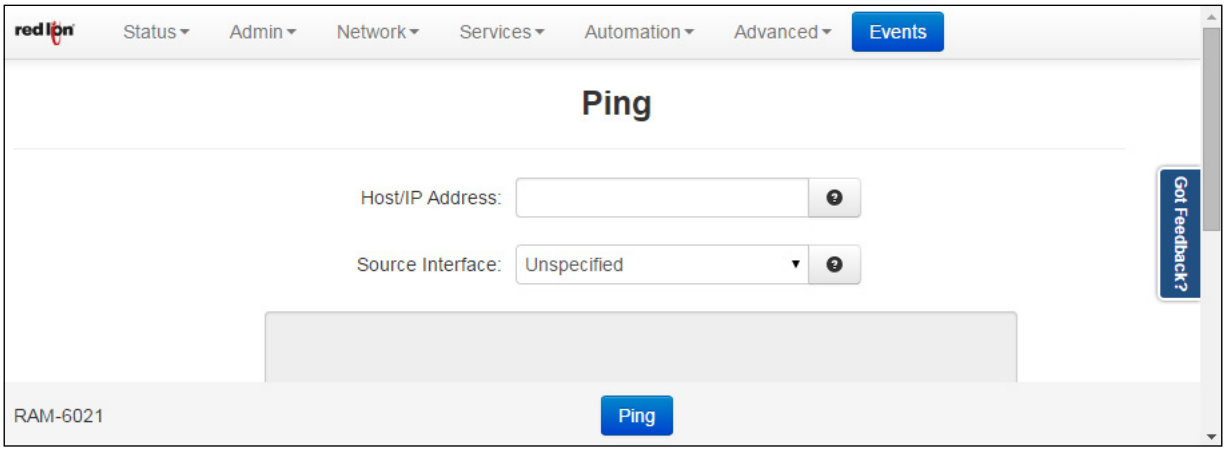


2.2.4 Diagnostics

The Diagnostics menu is sub-sectioned into Ping, Traffic Capture, Socket Test, Traceroute and System Info sub menus. These are useful in troubleshooting connectivity of the Red Lion router to the Internet or the Network the router is connected to.

Ping

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



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 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.

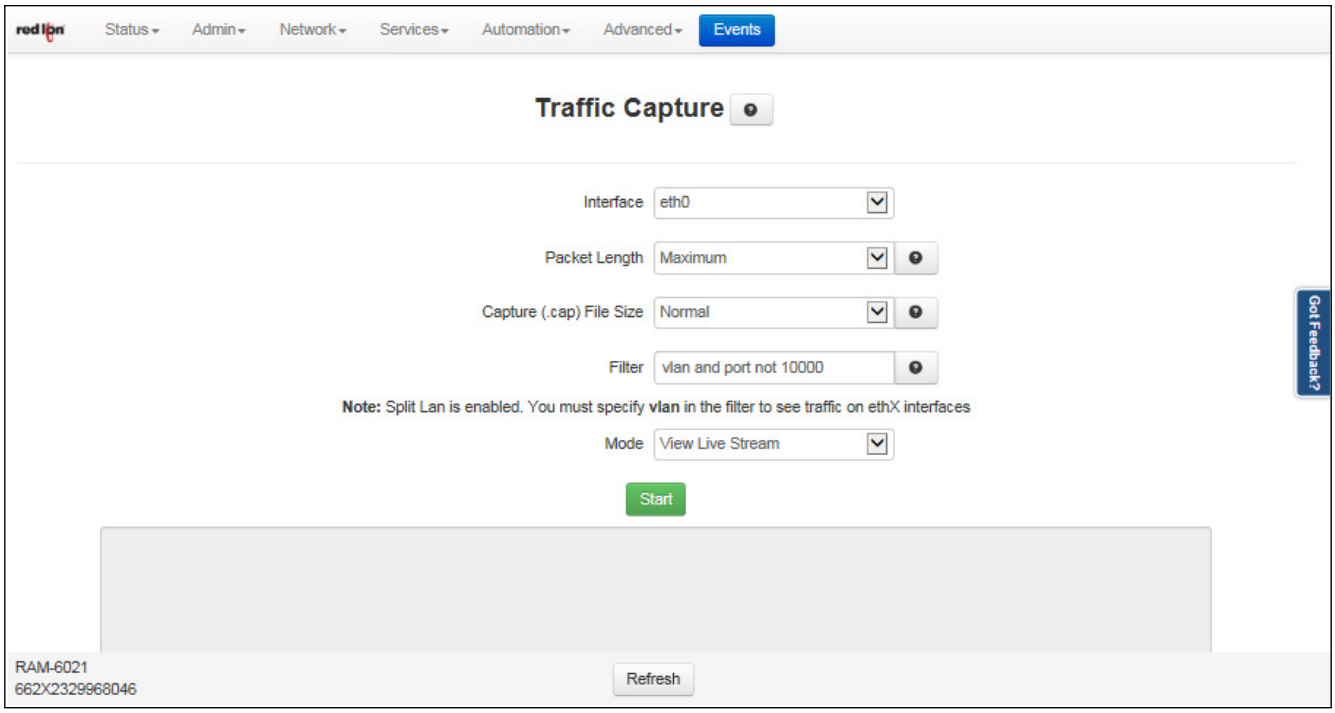
Choose the interface that the VPN Tunnel has listed for the Local Subnet end-point, i.e. if the Left Subnet is 10.100.100.0/24 and eth1 (LAN) has 10.100.100.1 as its IP Address, then choose Source Interface eth1 (LAN).

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 will use 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*

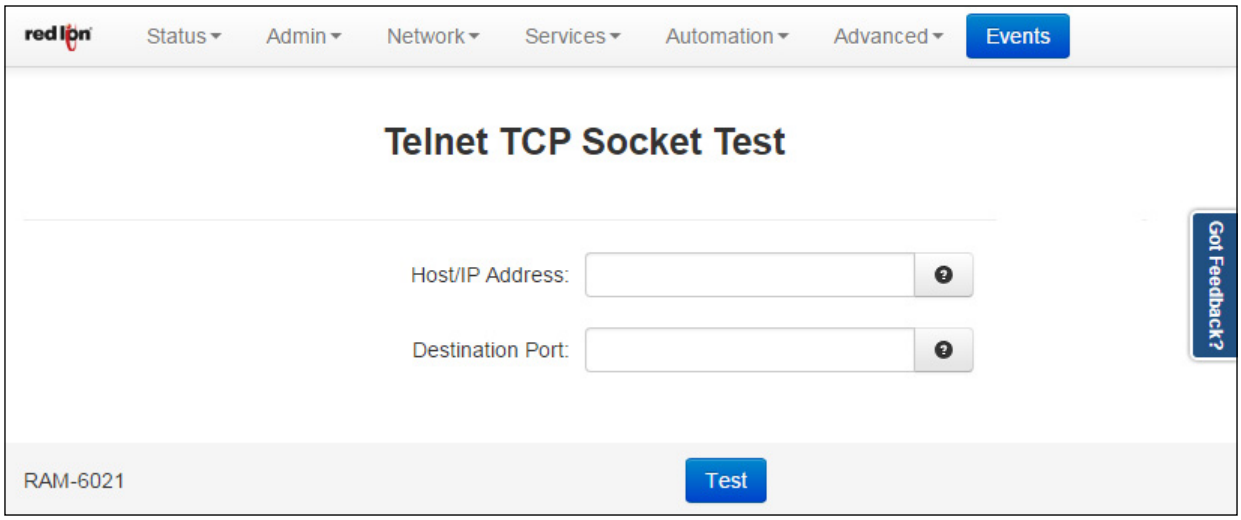
To capture only traffic from a specific port: *port 1234*

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

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

Socket Test

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



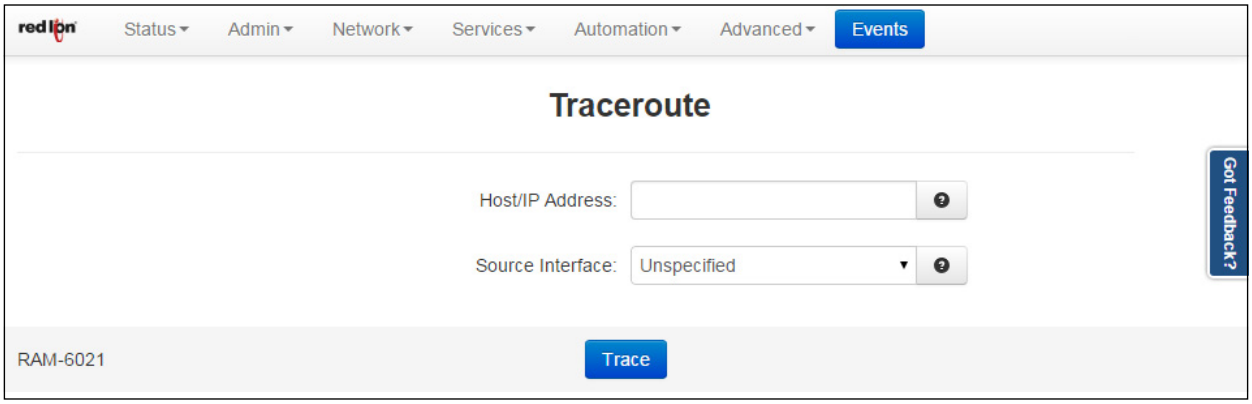
Host/IP Address field: Type in the IP Address or URL you wish to connect to via Telnet.

Destination Port field: Enter the Destination IP Address 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 will allow 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 URL 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 source interface. Choosing “Unspecified” will let the system choose the first interface found with a route to the destination. The Source Interface offers the option of using different interfaces to send the trace through. This is useful should you have a VPN Tunnel in place and testing the connection through the VPN Tunnel is required to verify connectivity through the tunnel.

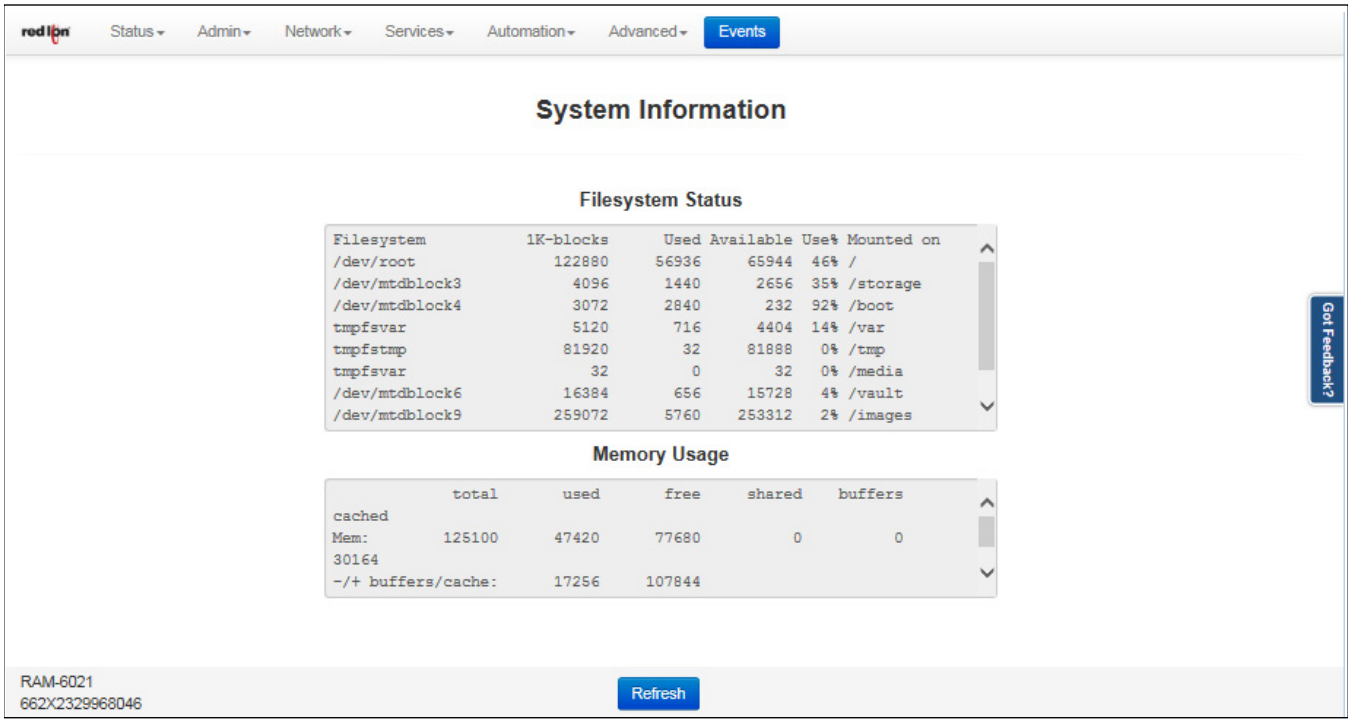
Choose the interface that the VPN Tunnel has listed for the Local Subnet end-point, i.e. if the Left Subnet is 10.100.100.0/24 and eth1 (LAN) has 10.100.100.1 as its IP Address, then choose Source Interface eth1 (LAN).

Specify a host IP Address at the head-end to ping through the tunnel.

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

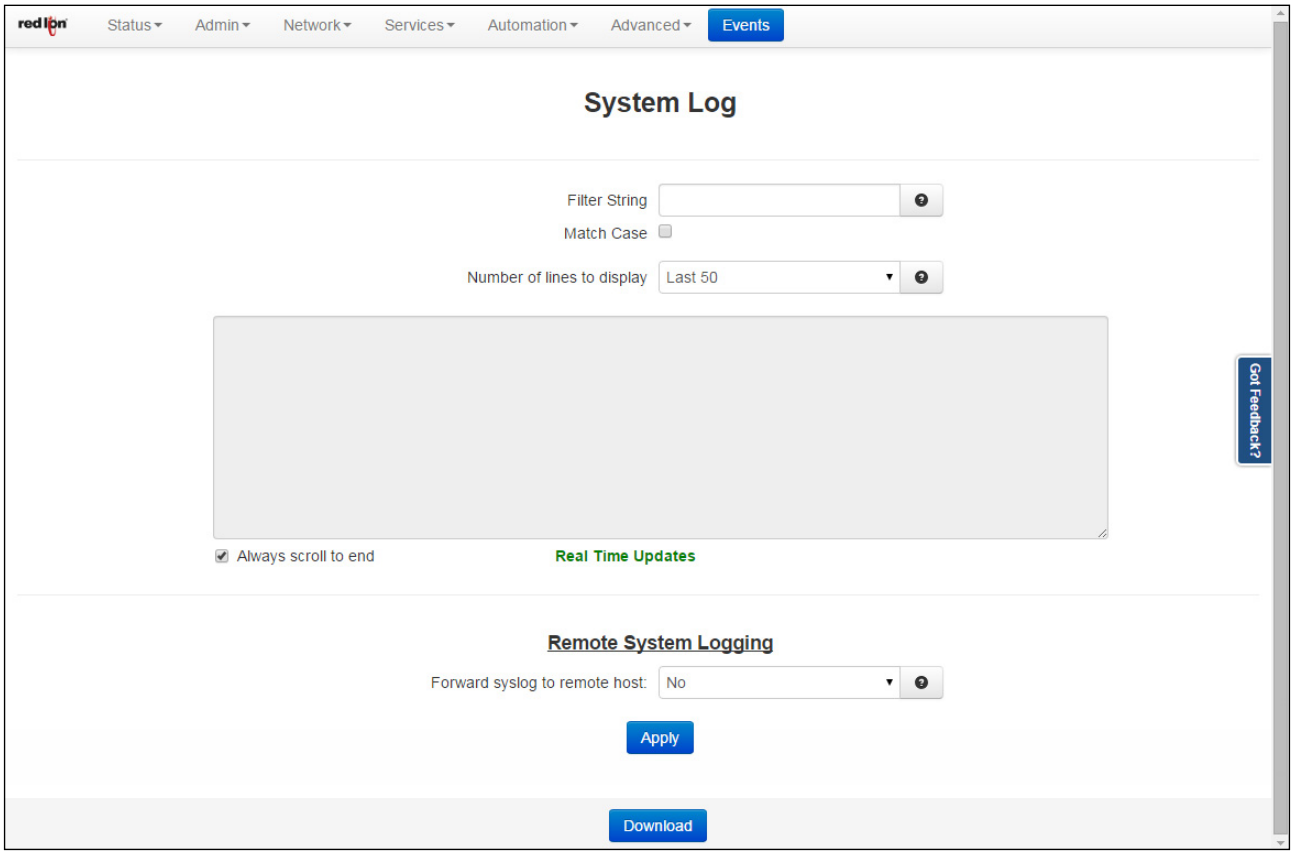
System Info

The System Information menu item displays the current usage of the files system in both the directory size and the memory utilization.



2.2.5 Syslog

The Syslog window displays the current syslog of the Red Lion 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.

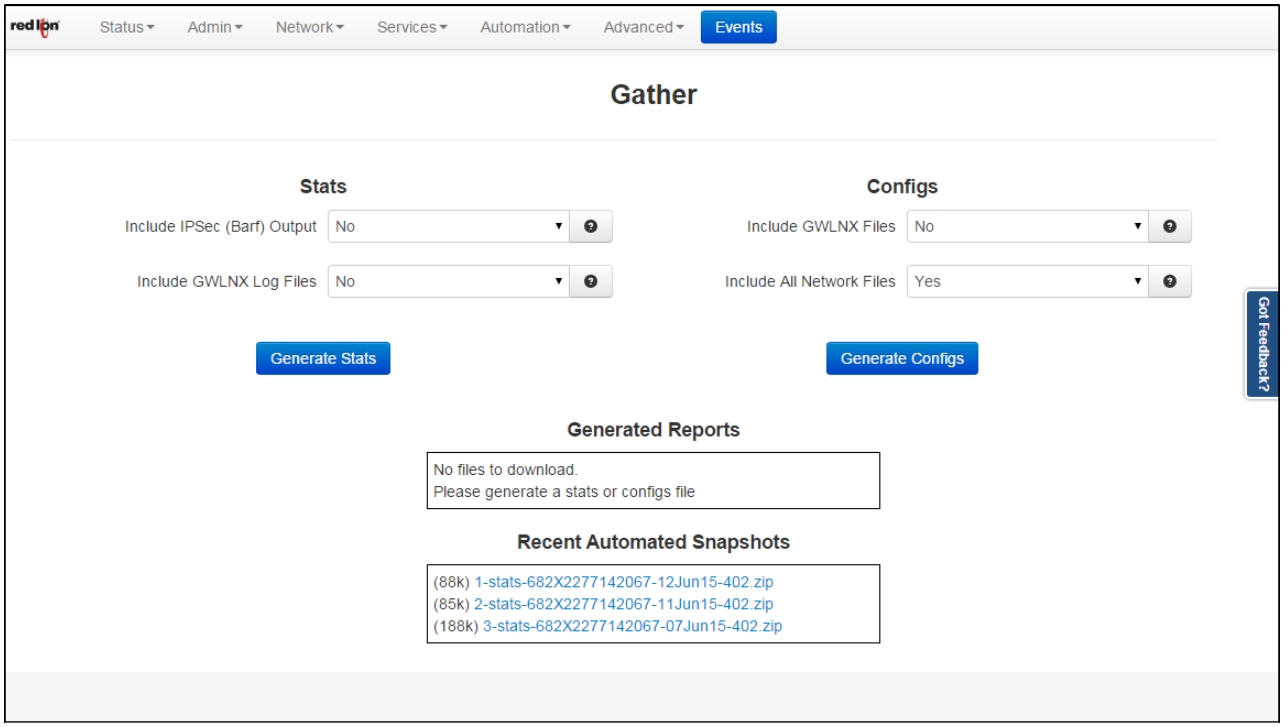
Number of lines to display: Select the number of lines to be displayed from one of the choices in the drop-down list provided.

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 will appear prompting whether to save or open the file. The download interface will be different depending on the browser used.



2.2.6 Gather Stats



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 Red Lion 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.

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.

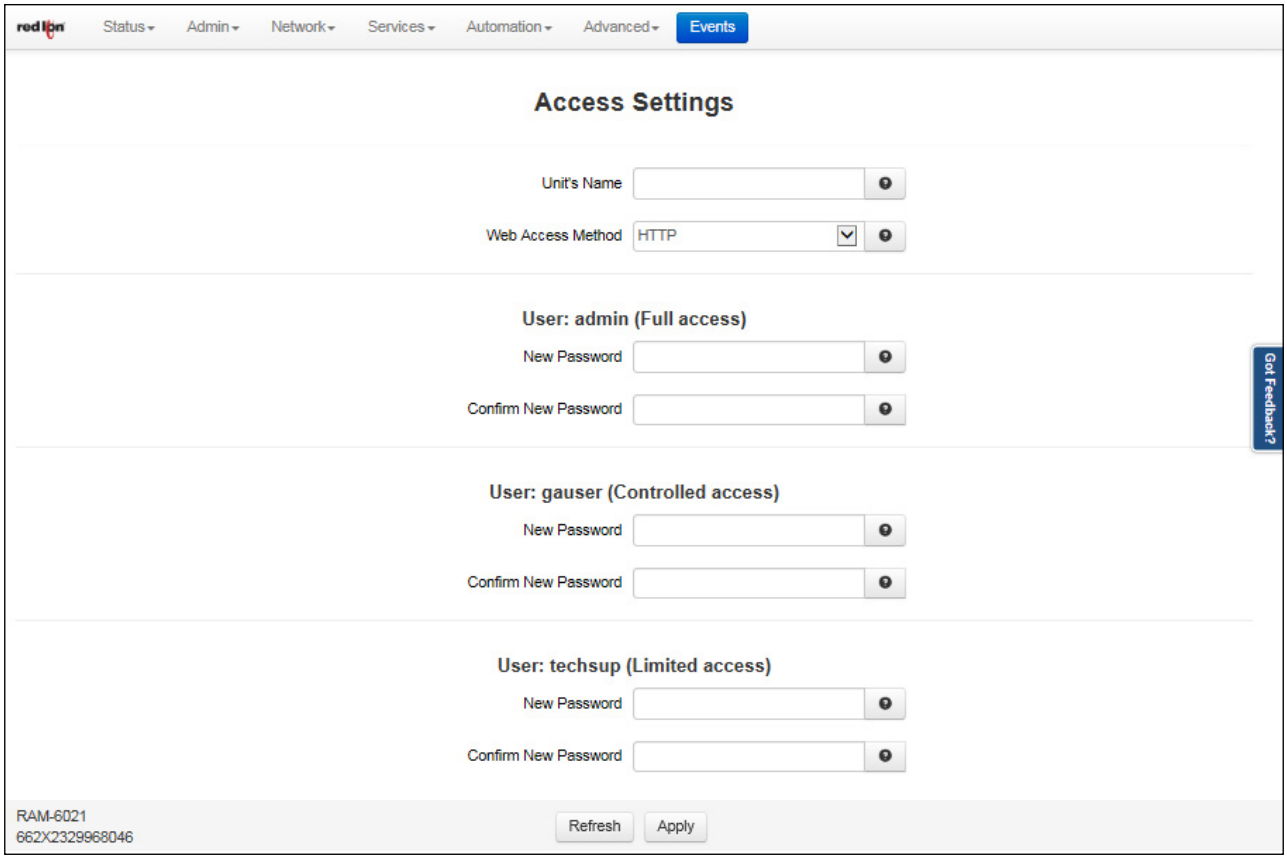
2.3 Admin Tab

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

2.3.1 Access Settings

The Access Settings menu item allows you to change how the unit's Web UI is accessed, either by HTTP or HTTPS. 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 will appear.



Unit's Name: Enter a description to identify the unit. This field is not required to support functionality. It is only for unit identification.

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.

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

User: admin (Full access)

New Password: Enter the new password in the “New Password” field.

Note: For a secure password, choose one that is at least six characters long, is not a common word and comprised of a mixture of upper and lower case characters and numbers as well as special characters. 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)

New Password: Enter the new password in the “New Password” field.

Note: 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. 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)

New Password: Enter the new password in the “New Password” field.

Note: 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. 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*.

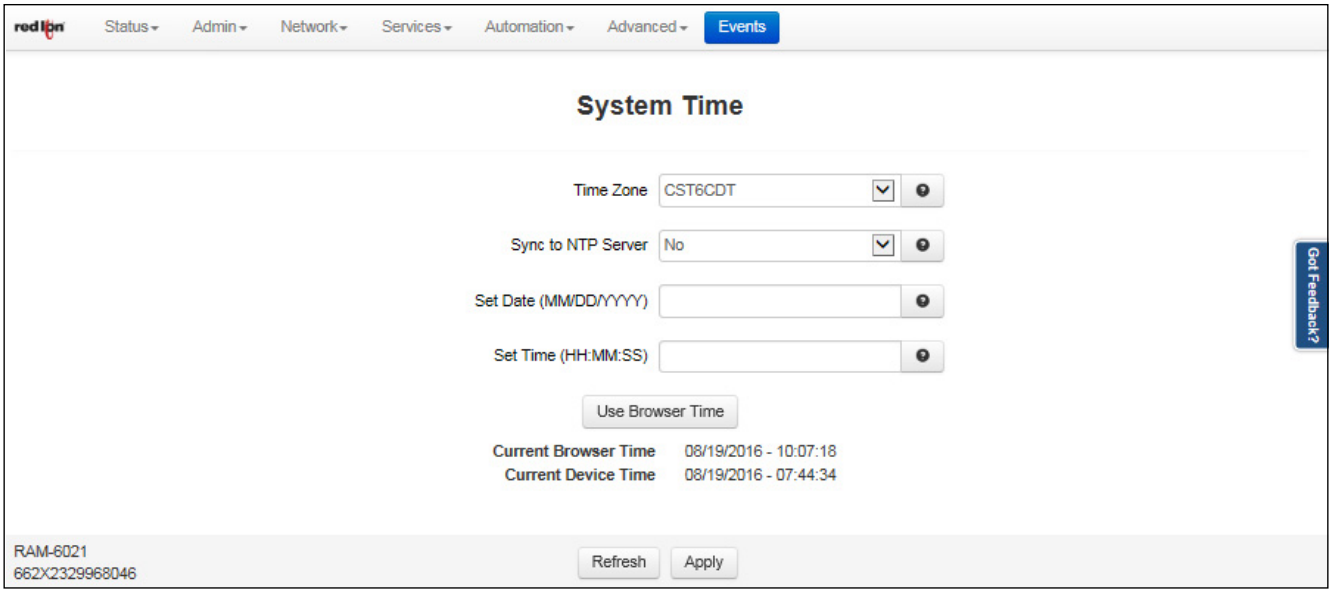
Confirm New Password: Re-enter the password entered in the New Password field.

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.

2.3.2 System Time

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

Click on the System Time menu time and the following window will appear.



Time Zone (Required): 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 router there are three options:

Option 1:

Sync to NTP Server: Select Yes to enable and configure the NTP Server settings.

Option 2 - Manual Configuration:

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

Set Time (HH:MM:SS): 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:

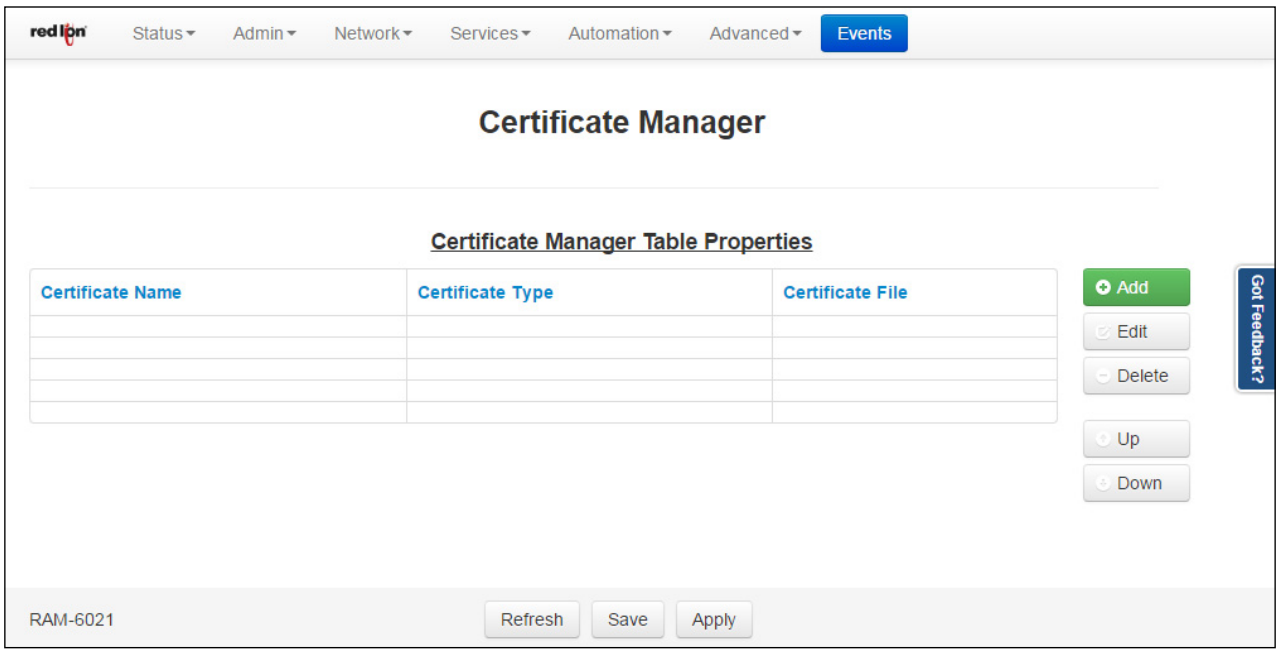
Use Browser Time: Set the Sync to NTP Server field to No and click on the Use Browser Time button. The local time as referenced from your browser is used to populate the settings.

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.

2.3.3 Certificate Manager

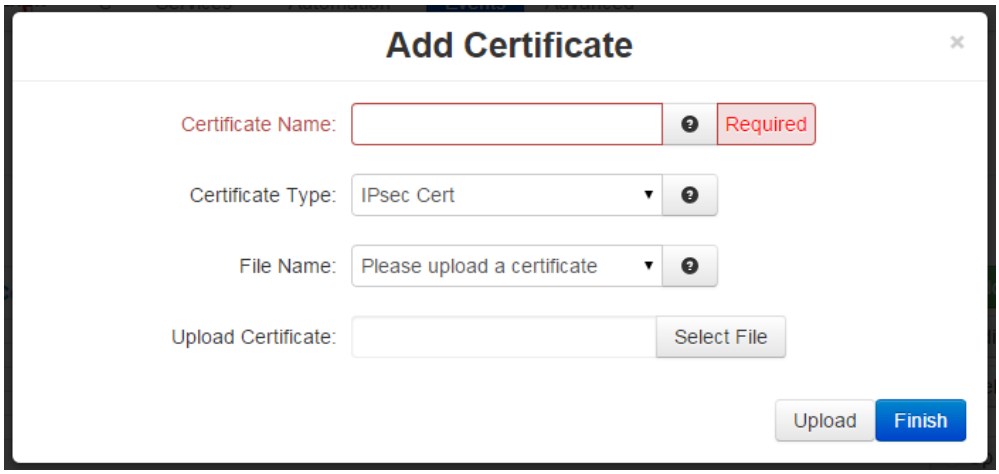
The Certificate Manager gives the option of adding a certificate, deleting or editing an existing one.

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



To create a new certificate:

Click on the *Add* button and the following dialog window will appear:



Certificate Name (Required): 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 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.

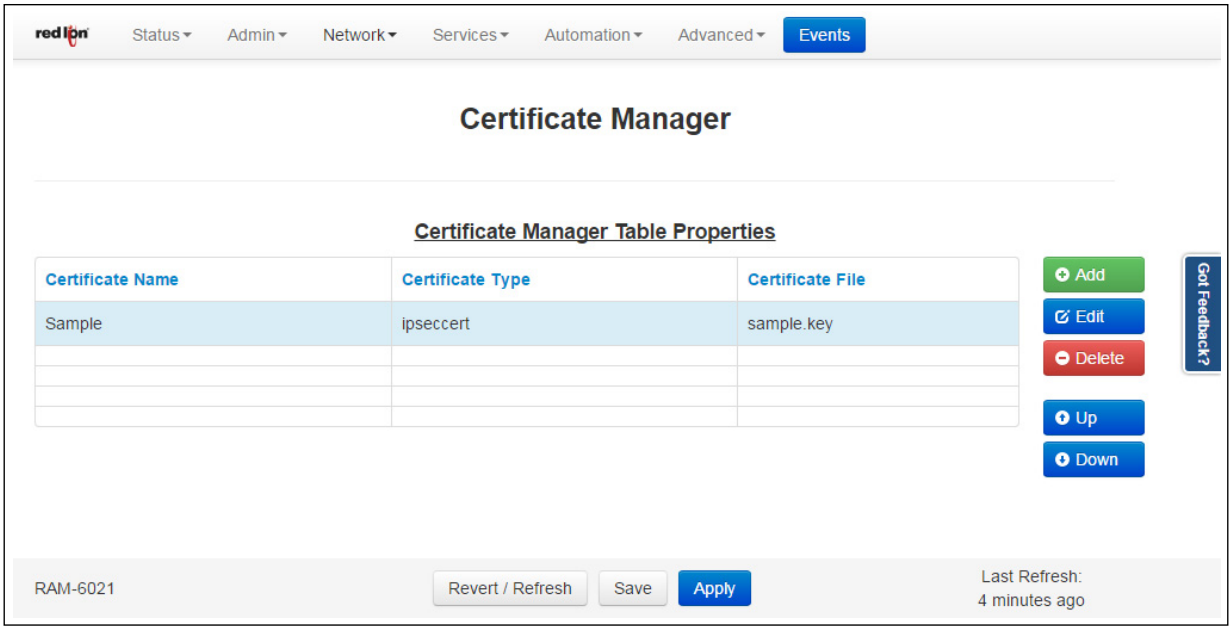
SSL: This certificate will be available for SSL Connections as a Server Certificate, or a Client Certificate.

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 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.

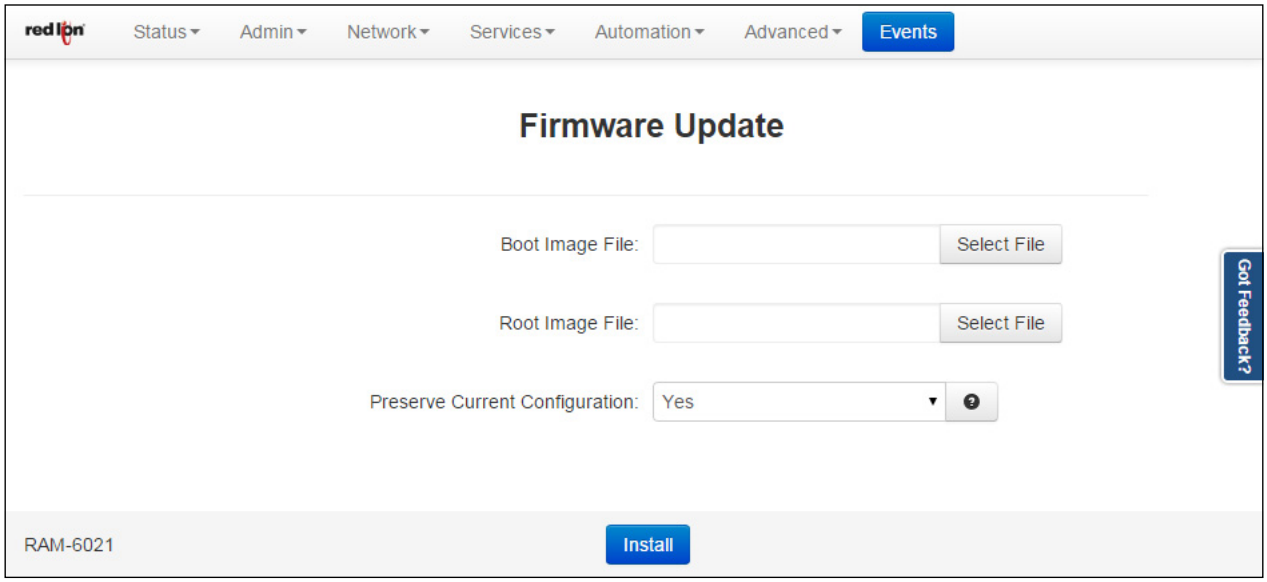
To move a certificate up or down in the table properties, use the Up and Down buttons.

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.

2.3.4 Firmware Update

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

Click on the Firmware Update menu item and the following window will appear:



To upgrade the firmware of the Red Lion router:

Boot Image File: Select the file that will perform the Kernel update.

Root Image File: Select 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.

Click on the *Install* button.

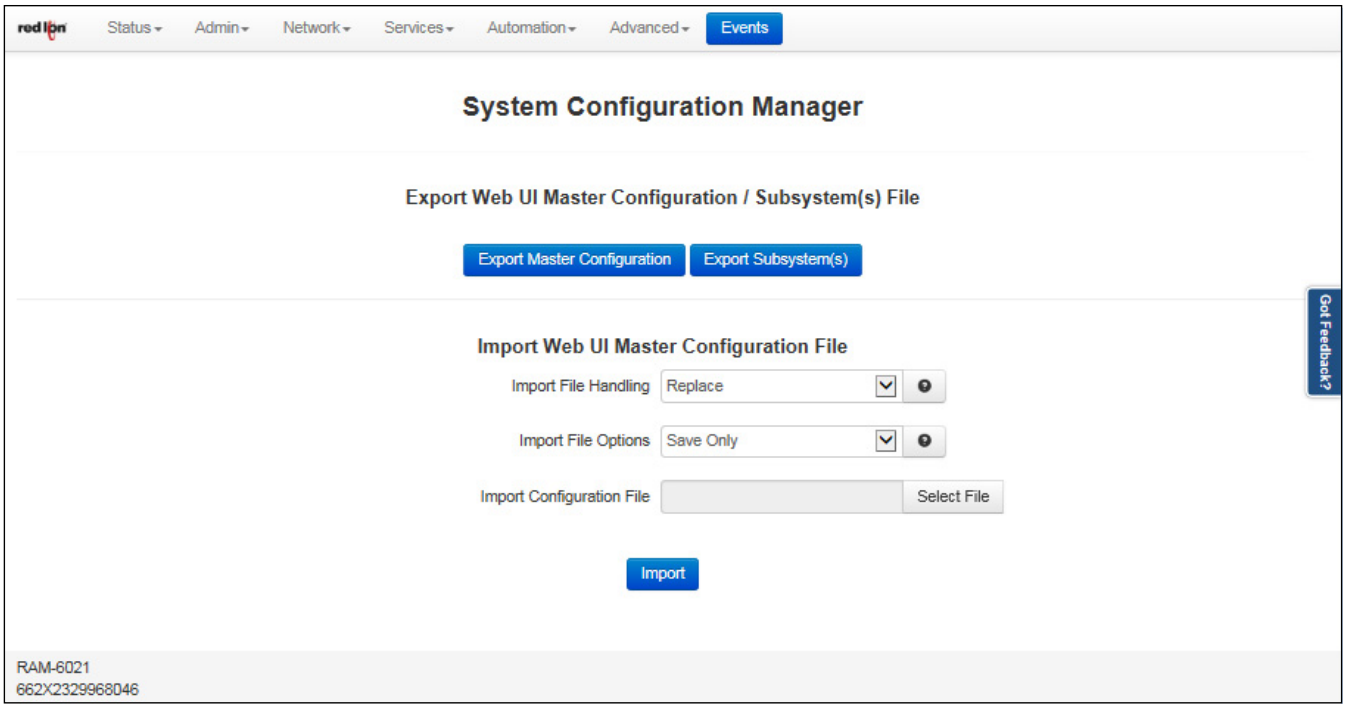
Note: This procedure could take anywhere from 6-10 minutes to complete.

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.

2.3.5 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 will appear:

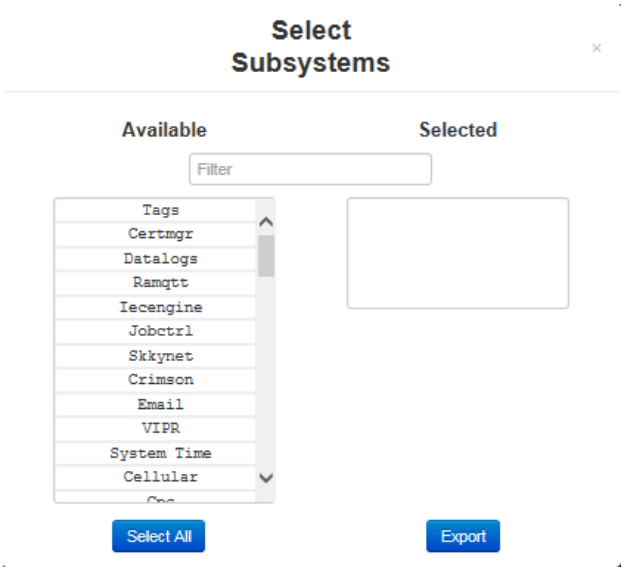


Export Master Configuration: To save a copy of the Red Lion router configuration, click on the "Export Master Configuration" button. The pop-up window below asking you to save or open the file will appear. Select the desired option.



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 router.

Export Subsystem(s): To save a copy of the Red Lion router individual subsystem configurations, click on the "Export Subsystem(s)" button. The Select Subsystems pop-up window appears allowing you to select any or all of the subsystem configurations you would like to export. Click on the Export button after making selections.



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

Import File Handling: Select Replace to completely replace the device configuration file with your import. Select Merge if you are importing a snippet of the main configuration.

Import File Options:

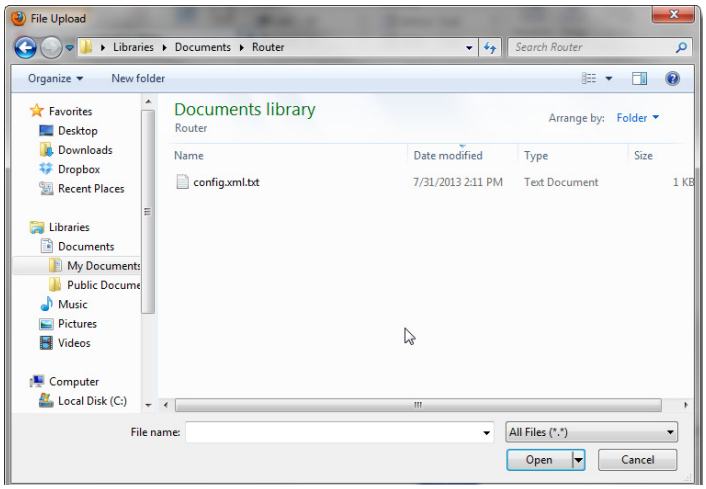
Save Only: If you want to save the new configuration without immediately applying it, select the *Save Only* option. In order for the changes to take effect, a system reboot is required.

Apply: When this option is selected, any imported configuration sections will be applied only if they have changed values. If imported sections are identical to the current configuration, that section will not be applied.

Forced Apply: If this option is selected, every section imported will be applied immediately. This option is not commonly required.

Note: If your configuration file has many sections, this process may take a while.

Import Configuration File: Click on the Select File button, and the dialog window below will appear.



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

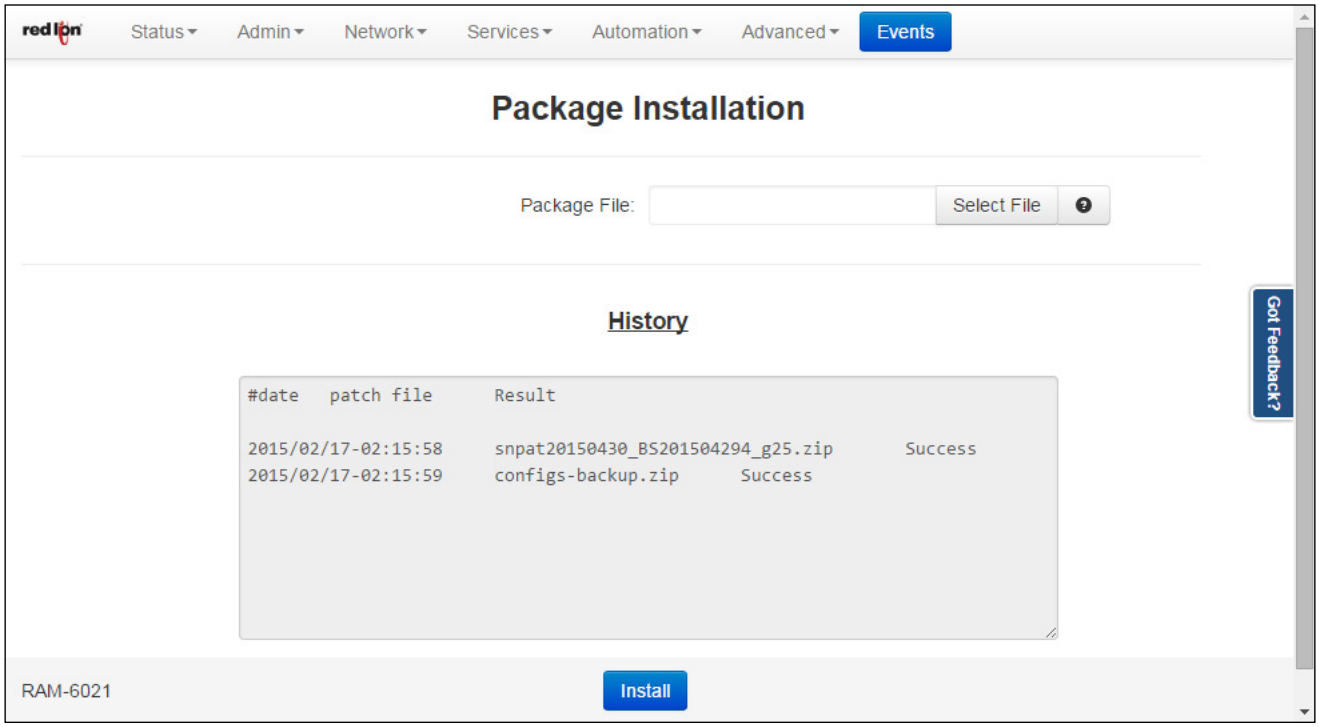
Select the config.xml.txt file and click on the Open button to populate the Browse window. If needed, you can change the file or remove it from the field by clicking the appropriate button

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

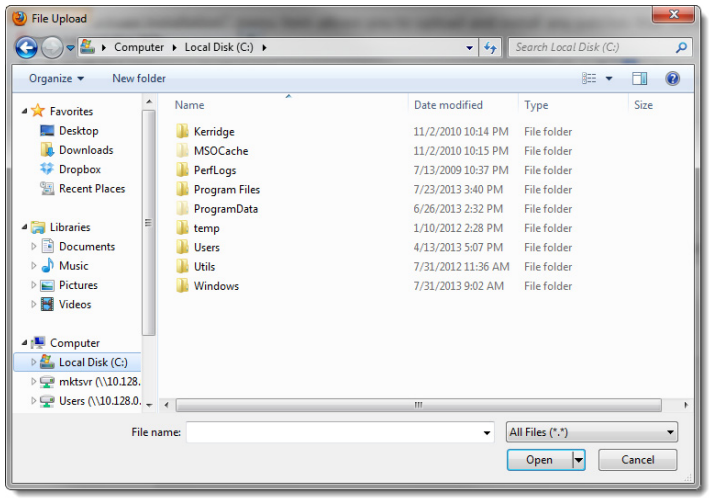
2.3.6 Package Installation

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 will appear:



In the Package File field, click the Select File button, and the following dialog window appear:



Browse to the directory where the patch is located.

Select the filename to select the file.

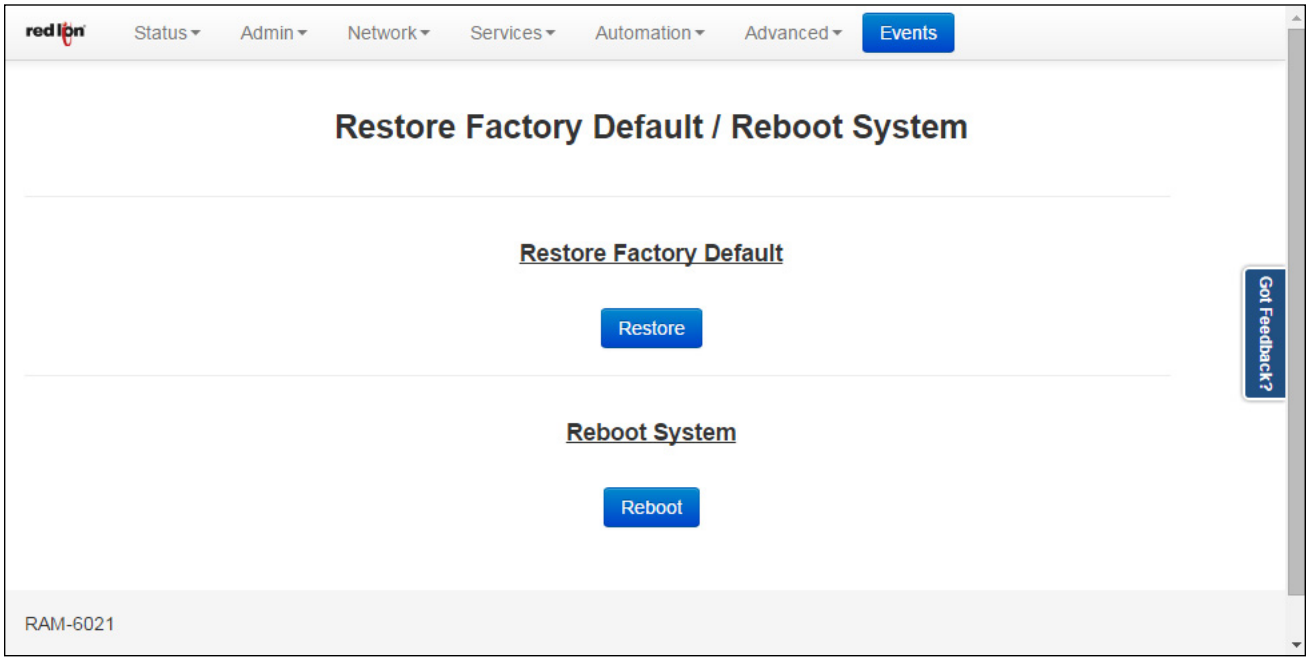
Note: Be sure to use only genuine Red Lion provided packages in the form of filename.zip.

Click on the Open button to populate the Package File field and click on the Install button. When install is complete, a table will appear at the bottom of the dialog window listing the modified files.

2.3.7 Factory Defaults/Reboot

The Factory Defaults 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 will appear:



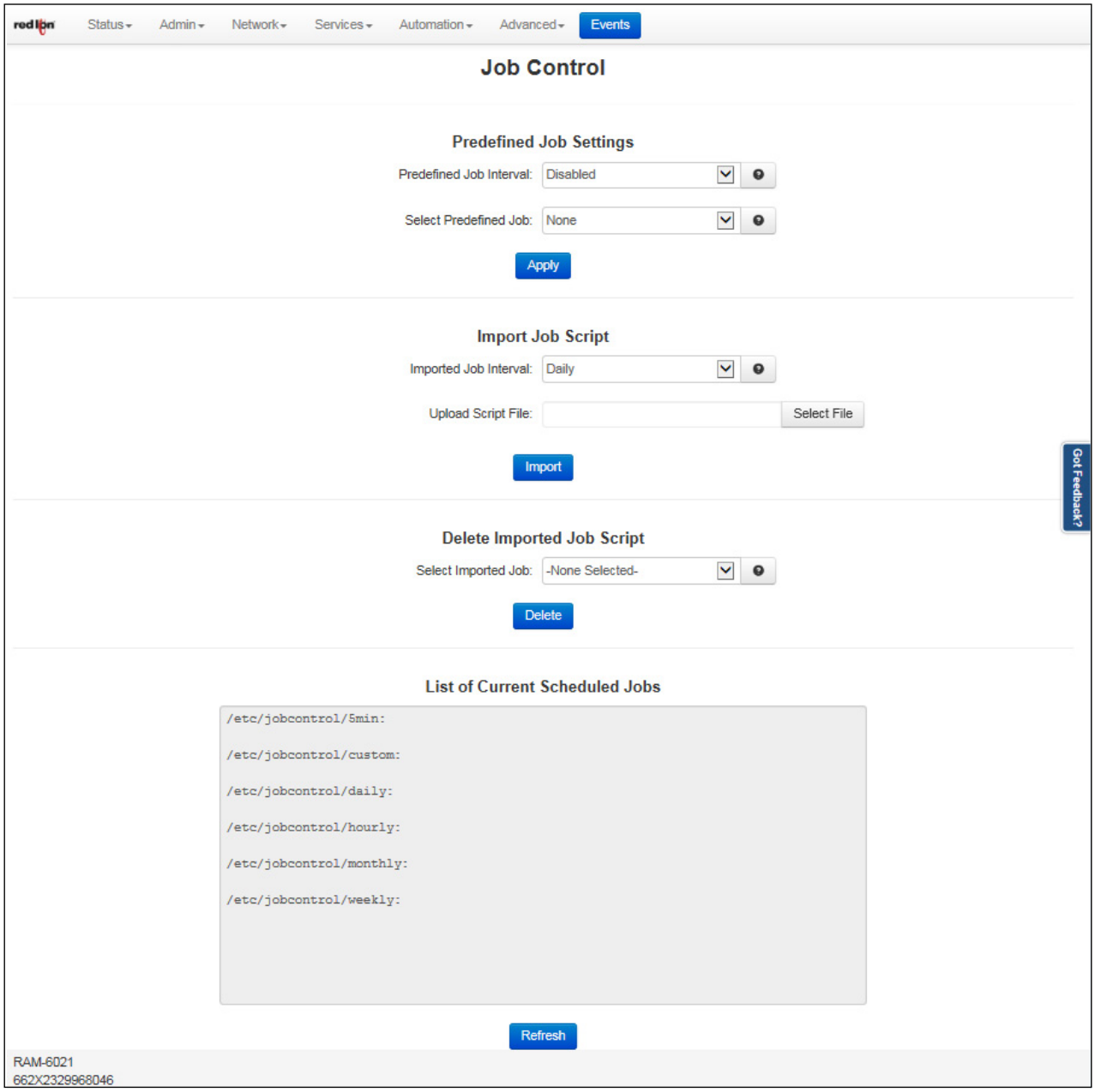
Restore Factory Default: Click on the Restore button to restore the factory default settings. A warning will appear, read through the information and click OK. The restore may take 2-5 minutes.

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

2.3.8 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 will appear:



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 all scheduled job intervals.

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.

2.4 Network Tab

The Network Tab configures aspects of the Red Lion router affecting the networking functionality of the unit. From here you can configure the Ethernet Interfaces, Firewall, Static Routes, TCP Keep-Alives and VPN Tunnel configuration and more.

2.4.1 Interfaces

The Interfaces menu allows the administrator to configure the Ethernet ports of Red Lion routers to meet their network topology needs.

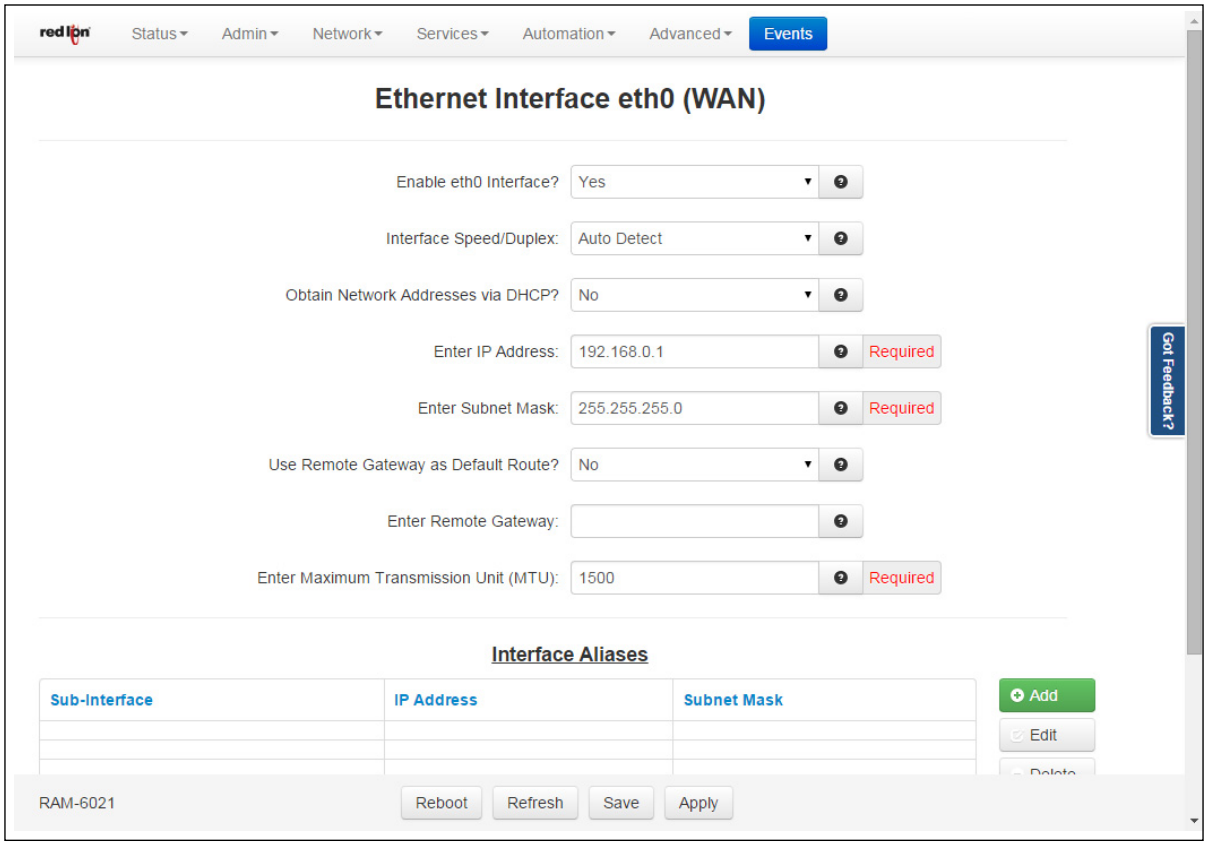
Interfaces available may include eth0 (WAN), eth1 (LAN), USB and IPv6. These will only be present if your hardware supports these interfaces.

These ports are 'auto-sensing', allowing for greater flexibility.

eth0 (WAN) and eth1 (LAN)

The configuration of the Ethernet ports is the same for eth0 (WAN) and eth1 (LAN), 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 and the following window will appear:



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

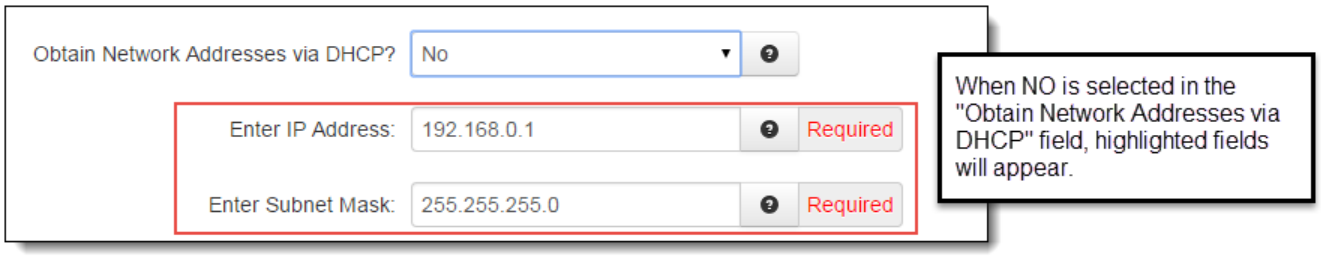
Interface Speed/Duplex: This configuration parameter controls the speed and duplex behavior of the Ethernet port. Valid selections are:

- Auto Detect: Use the 'best negotiated' speed and duplex. (default)
- 10Mbps/Half: If selected, the interface will communicate at 10 Mbps and half duplex.
- 100Mbps/Half: If selected, the interface will communicate at 100 Mbps and half duplex.
- 100Mbps/Full: If selected, the interface will communicate at 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 router with the IP address that it should use. This is a required 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.

Enter Subnet Mask: This field specified the subnet mask to be assigned to the Ethernet port when a 'Static' IP address configuration is selected. This field is only available when Obtain Network Addresses via DHCP has been set to NO. This is a required field.

Your Network Administrator should be able to provide an appropriate value for this field. This value determines the valid range of IP addresses 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 will use 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.

Use Peer DNS: Select **YES** to allow the interface to obtain DNS Server settings via DHCP. This field is only available when *Obtain Network Addresses via DHCP* has been set to **YES**. Select **NO** to allow the interface to use the DNS settings from the **Networking -> DNS Settings** screen. The recommended setting for this field is YES.

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 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 accessed indirectly through a router and that 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.

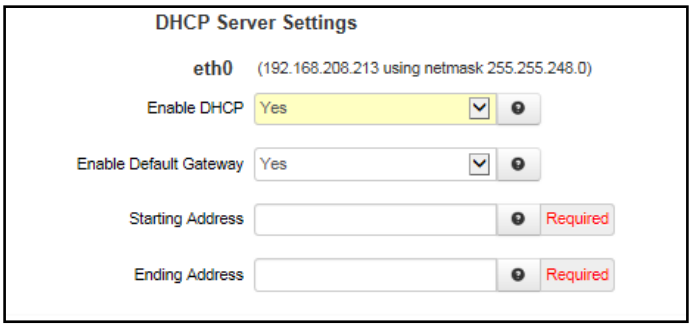
Your Network Administrator should be able to provide an appropriate value. The address must be one within the valid range for the network.

Enter Maximum Transmission Unit (MTU): 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 improvements 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.

Interface Aliases: 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.

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.



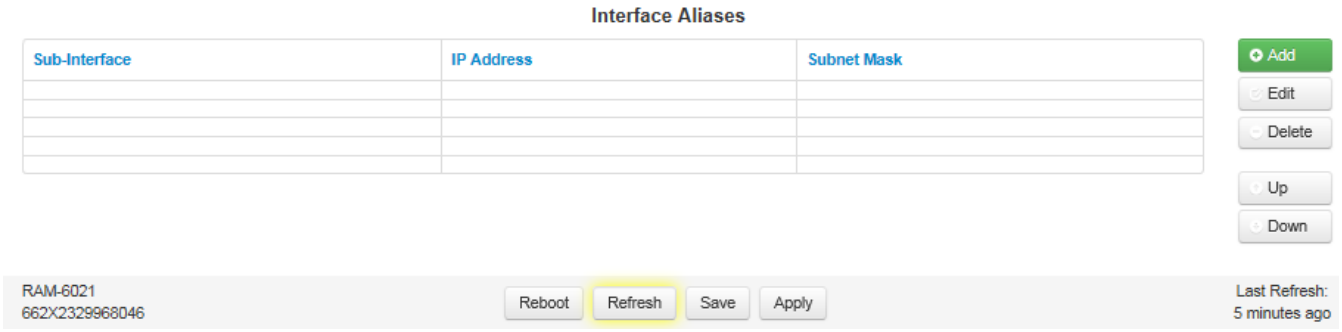
Enable Default Gateway: Provide Default Gateway IP address to DHCP Client.

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.

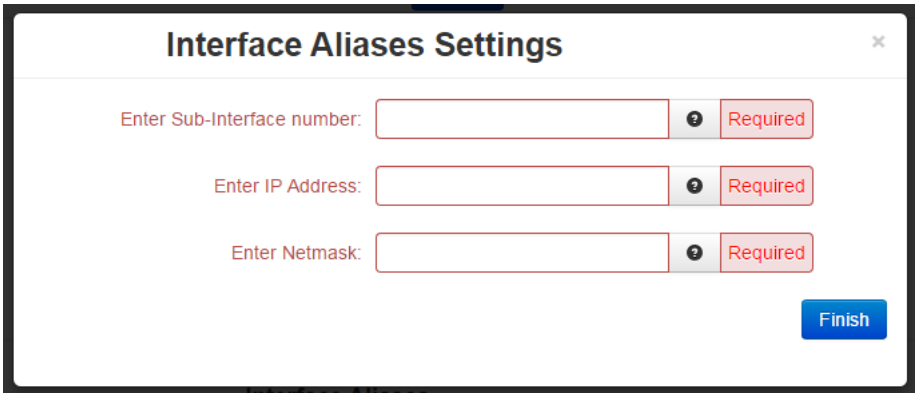
Ending Address: Enter the ending IP address of a range you want the DHCP Server to provide for clients. The recommended setting is a valid address for the subnet for which the interface is configured, beyond that chosen for the starting value of the range. Use care to ensure that there is no conflict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



Note: To work with the eth1 (LAN) Interface, follow the steps documented for eth0 (WAN).

To configure a sub-interface:

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

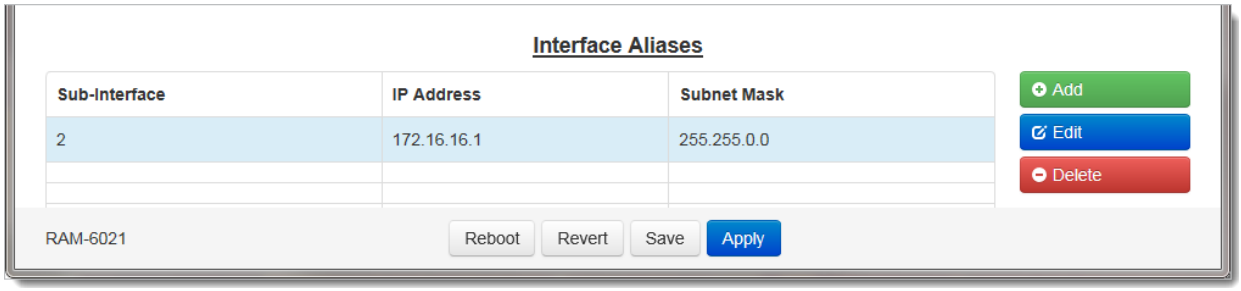


Enter Sub interface number (Required): This field is where you enter the sub interface number. The valid range is 0-99, and each aliased interface must be uniquely numbered. The final sub interface name will then be in the form **ethx:y** where **x** is the root interface number and **y** is the sub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

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

Enter Netmask (Required): This field specified the netmask to be assigned to the sub interface. You Network Administrator should be able to 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.



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.

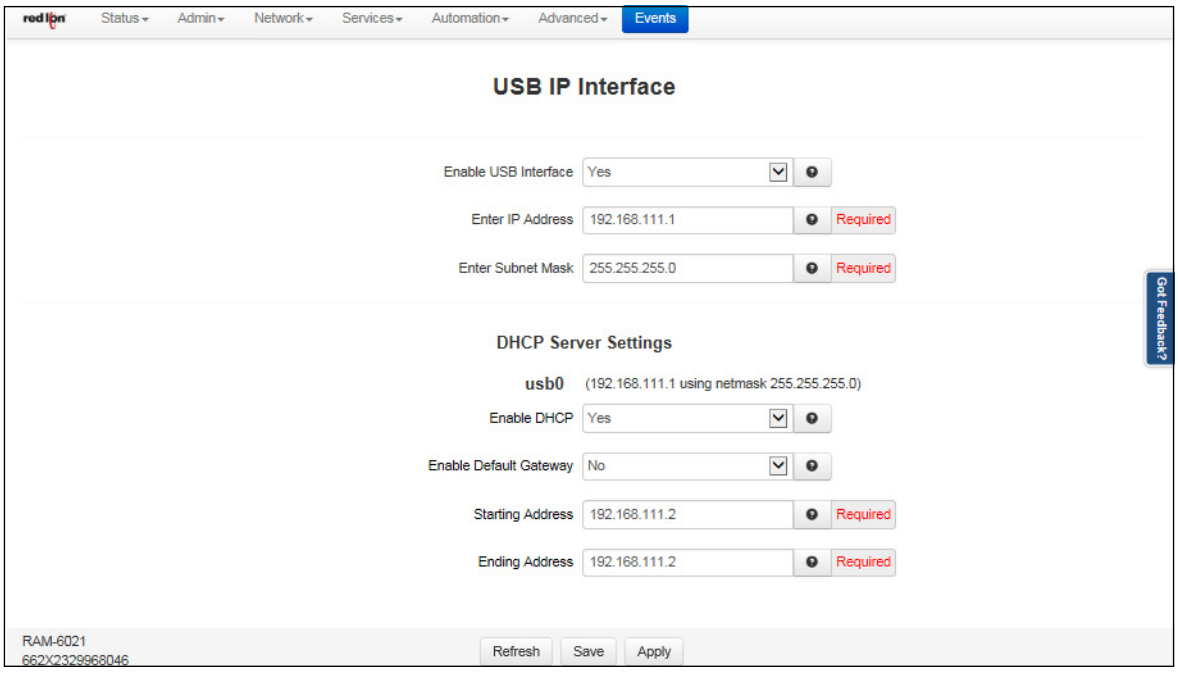
Applying new settings to the interface may result in disconnection, requiring reconnection using alternate methods.

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.

USB

The USB interfaces menu item allows the administrator to configure the USB port of the Red Lion 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 following dialog window will appear:



USB IP Interface:

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

DHCP Server Settings:

usb0: Displays the USB settings for the USB interface you are about to configure the DHCP Server Settings for.

Enable DHCP: Use to 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: Use to provide a Default Gateway IP address to the DHCP Client. Set to No if you want 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 want 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. It is necessary to use a valid address for the subnet and it is recommended that care is used to ensure that there is no conflict with any pre-existing devices on the subnet that may have already been configured to use statically assigned IP addresses.

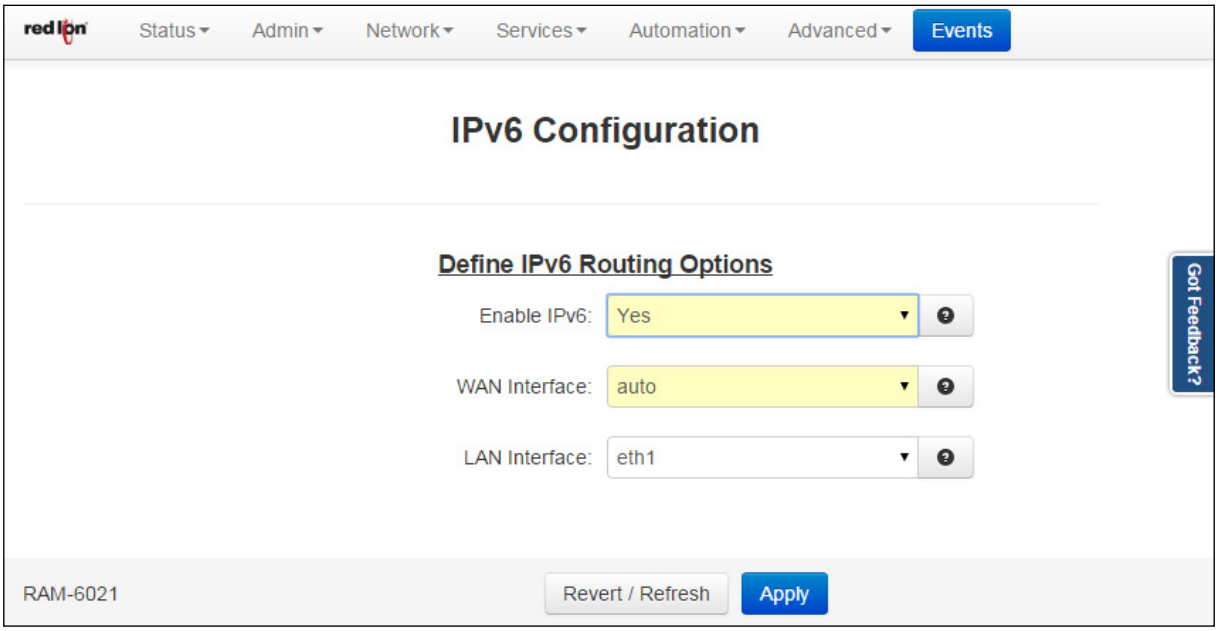
Ending Address: Enter the ending IP address of a range you want the DHCP Server to provide for clients. It is necessary to use a valid address for the subnet for which the interface is configured, beyond that chosen for the starting value of the range. Use care to ensure that there is no conflict with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

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 Configuration

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 firewalling.

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

LAN Interface: The Router Advertisements are available for one of 64 subclass 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.

Note: A reboot is required after changes to IPv6 Routing configuration.

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

2.4.2 Firewall

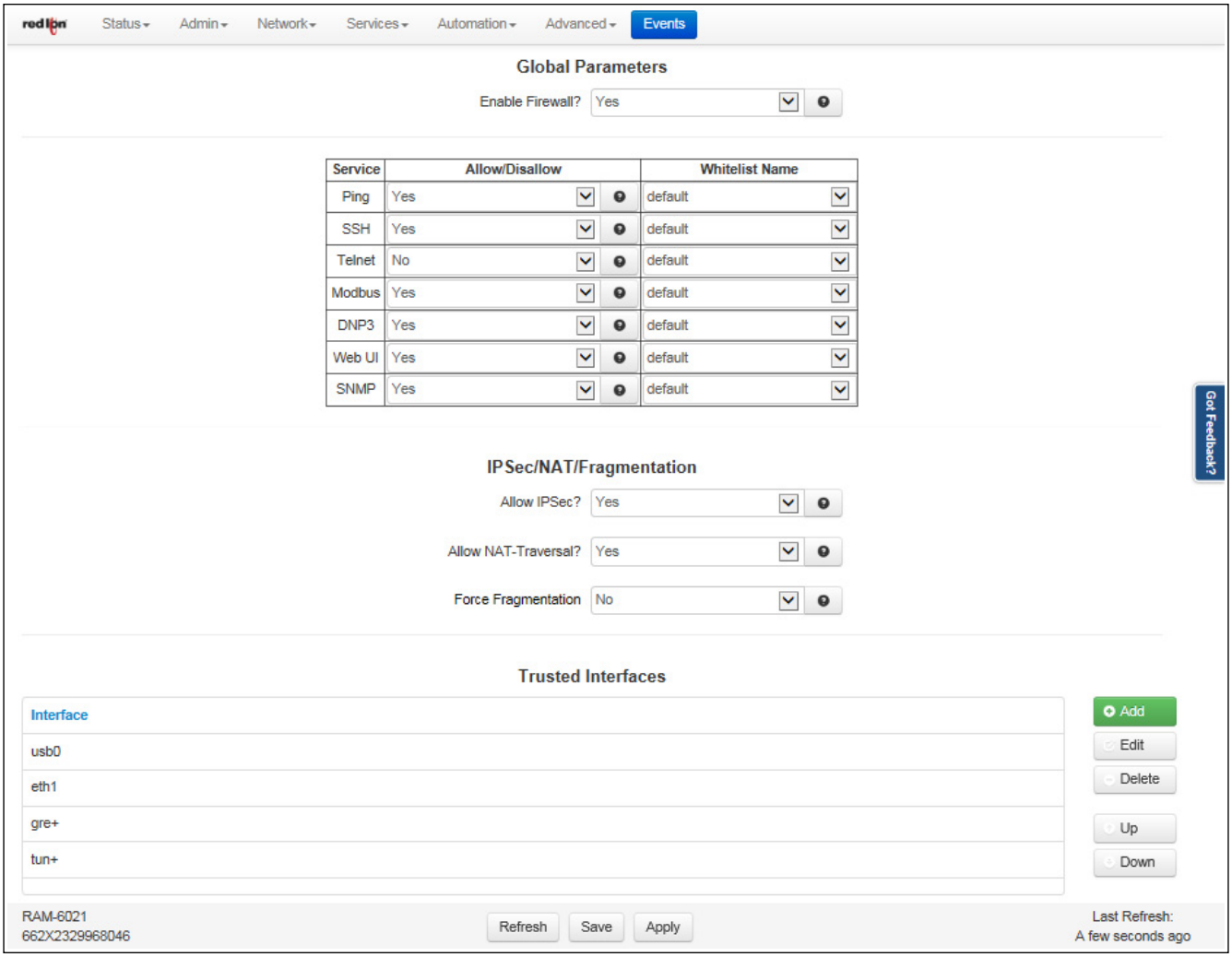
The Firewall menu item allows you to configure every aspect of the firewall on the Red Lion router.

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

General Settings

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

Click on the General Settings menu item and the following dialog window will appear:



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 *Automation* > *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.

SNMP: 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*.

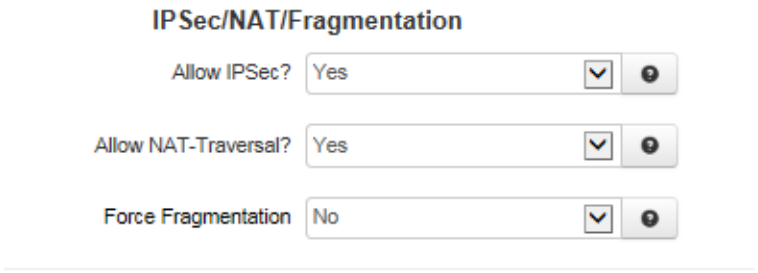
To restrict access via a configured whitelist, click the check box marked Use Whitelist and then select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined via the *Network* > *Firewall* > *ACL Rules* > *Subnet Whitelist Rules* screen.

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 IPSET: 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.

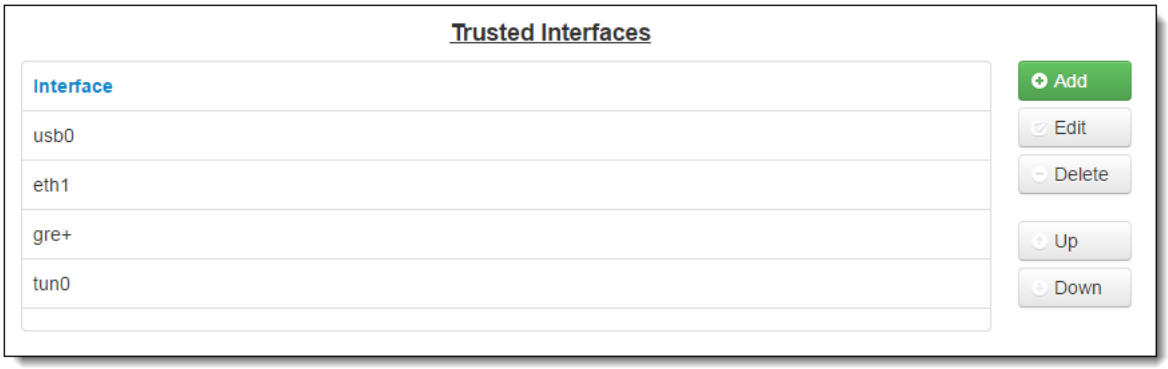
Allow NAT-Traversal: Specify whether to allow data on UDP port 4500 on untrusted interface. The recommended setting for this field is *Yes*.

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.

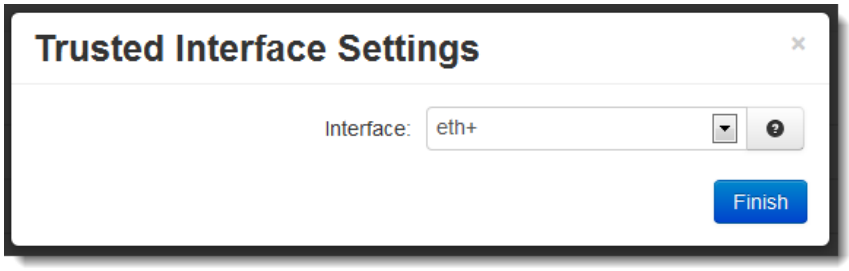
Force Fragmentation: When other hosts behind us send IP packets with the Don't Fragment (DF) bit set, this will clear the DF-bit before forwarding the packet. This will allow upstream routers to fragment the packets if smaller MTUs are encountered along the way, but performance may be impacted for fragmentation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

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 will appear:



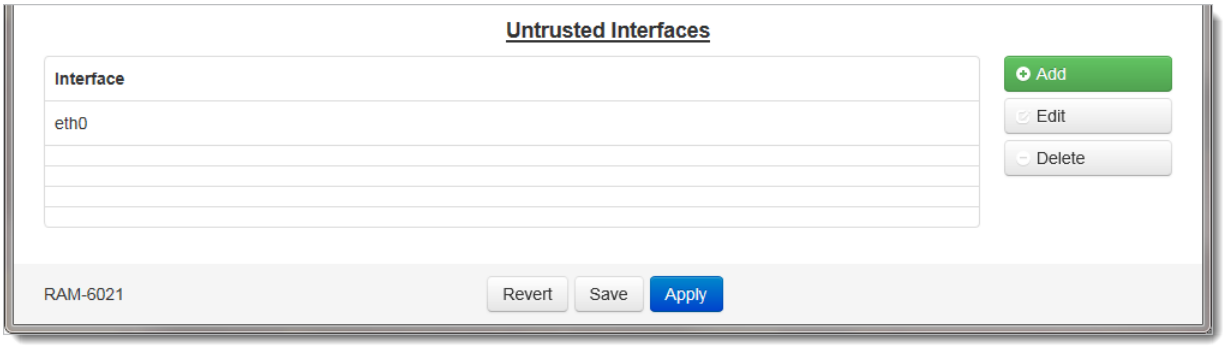
Interface: Choose an interface from the drop-down list provided. You may add as many interfaces as exist on the device. Each selection must be unique.

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. 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.

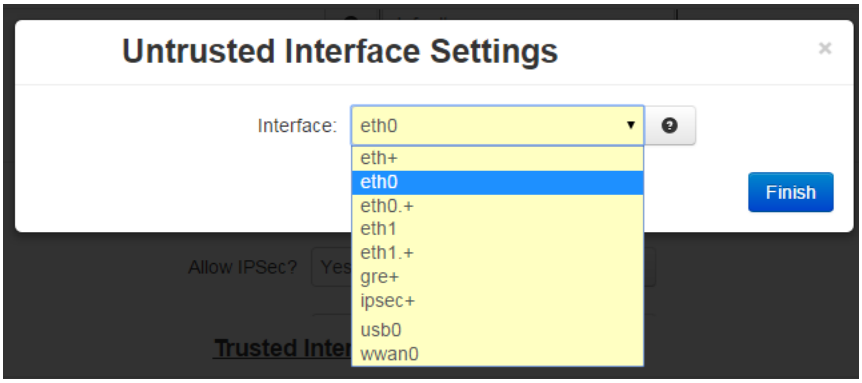
Click on the Finish button to populate the Trusted Interface screen.

Untrusted Interfaces

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



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



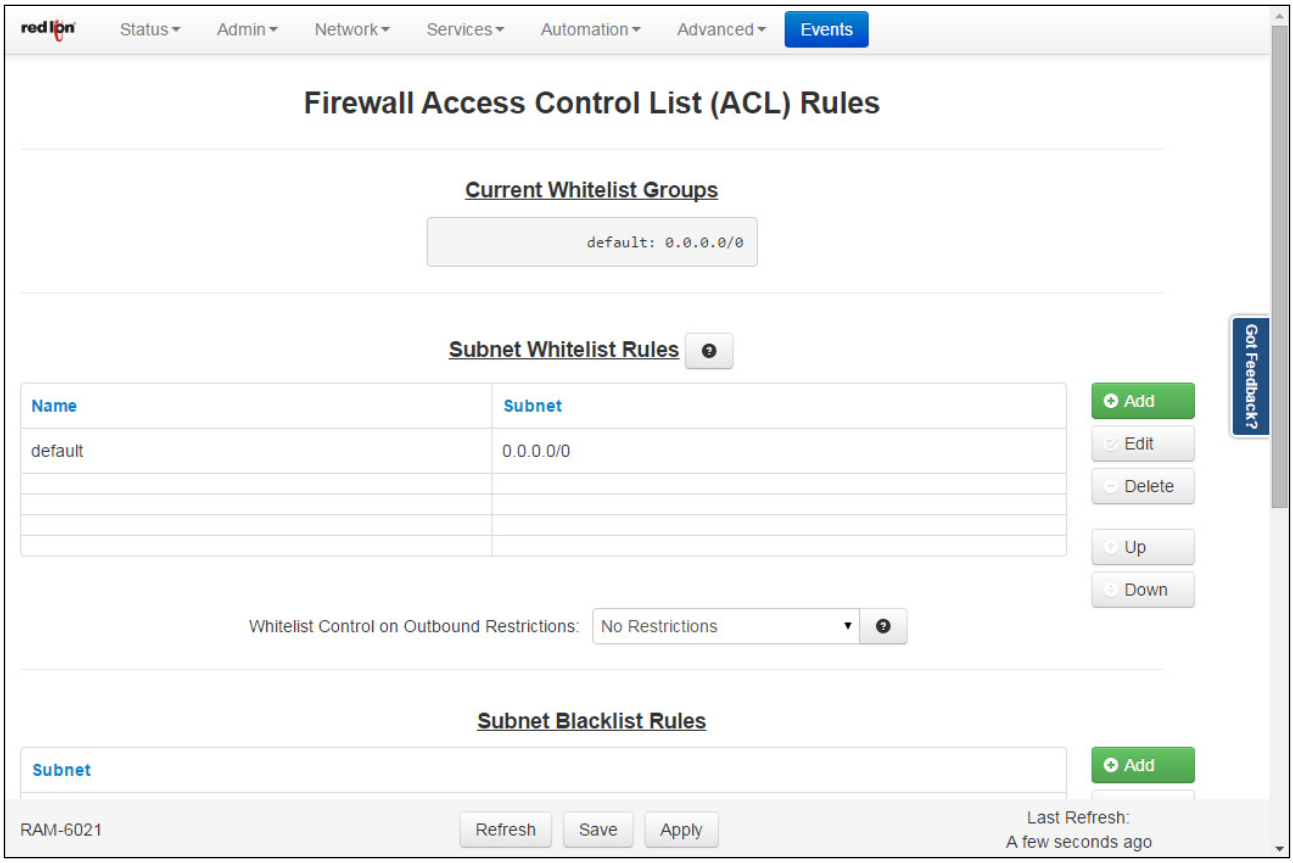
Interface: Choose an interface from the drop-down list provided. You may add any number of interfaces, up to as many exist on the device. Each selection must be unique. Untrusted interfaces will block all incoming traffic from devices connected to this interface.

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

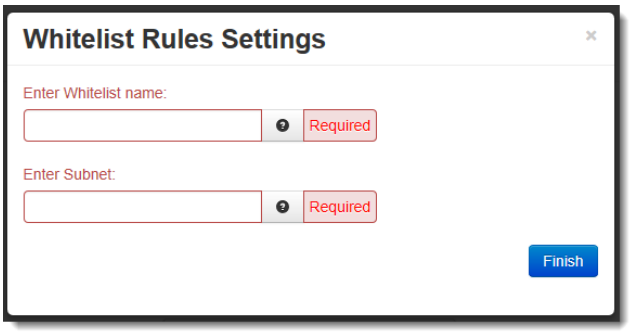
From the ACL Rules dialog window, Whitelist and Blacklist rules are defined. Whitelist Rules are used to define a single IP Address or an entire network that would be allowed to access the network behind the Red Lion router. Blacklist Rules are used to define a single IP Address or an entire network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



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

Subnet Whitelist Rules: The Subnet Whitelist Rules are used to define a single IP Address or an entire network that you want to allow access into the network behind the Red Lion RTU or router.

Click on the *Add* button and the following dialog window will appear:



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.

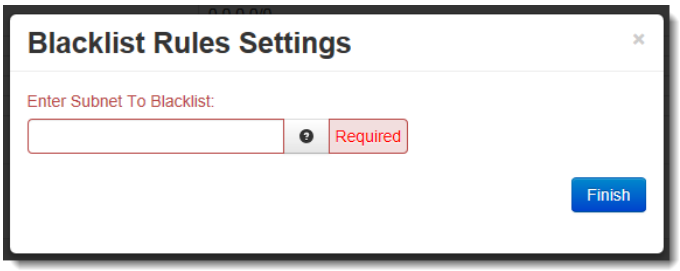
To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

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

Only to Whitelist IPs: Packets destined for subnets outside those allowed by the selected 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.

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



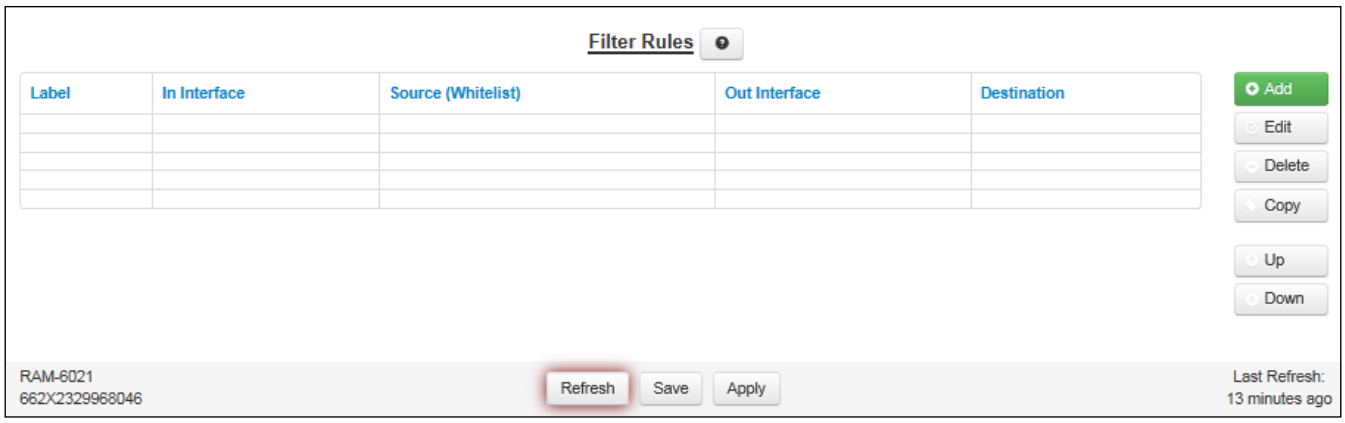
Enter Subnet To Blacklist (Required): Enter the network to be banned from making any incoming or outgoing connections, using IP/CIDR notation. To allow data from/to any source, enter 0.0.0.0/0. To specify a single host, use x.x.x.x/32, where x.x.x.x is the host's IP address. This will override any other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

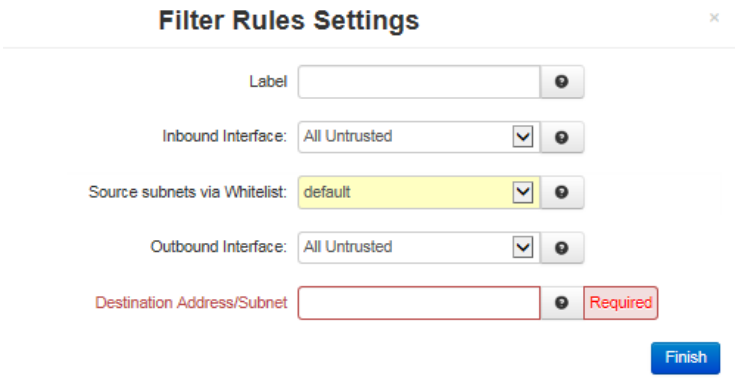
To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

Filter Rules: Trusted Interfaces are by default trusted, and do not have restrictions in place. 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 will appear:



Label: Enter a description to describe this Filter Rule. This field is not required for Filter Rules functionality and is for Filter Rule identification only.

Note: Maximum field length is 32 and supported characters are alphanumeric plus the following special characters: _@-./',;:?~! #$%^&.

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.

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

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

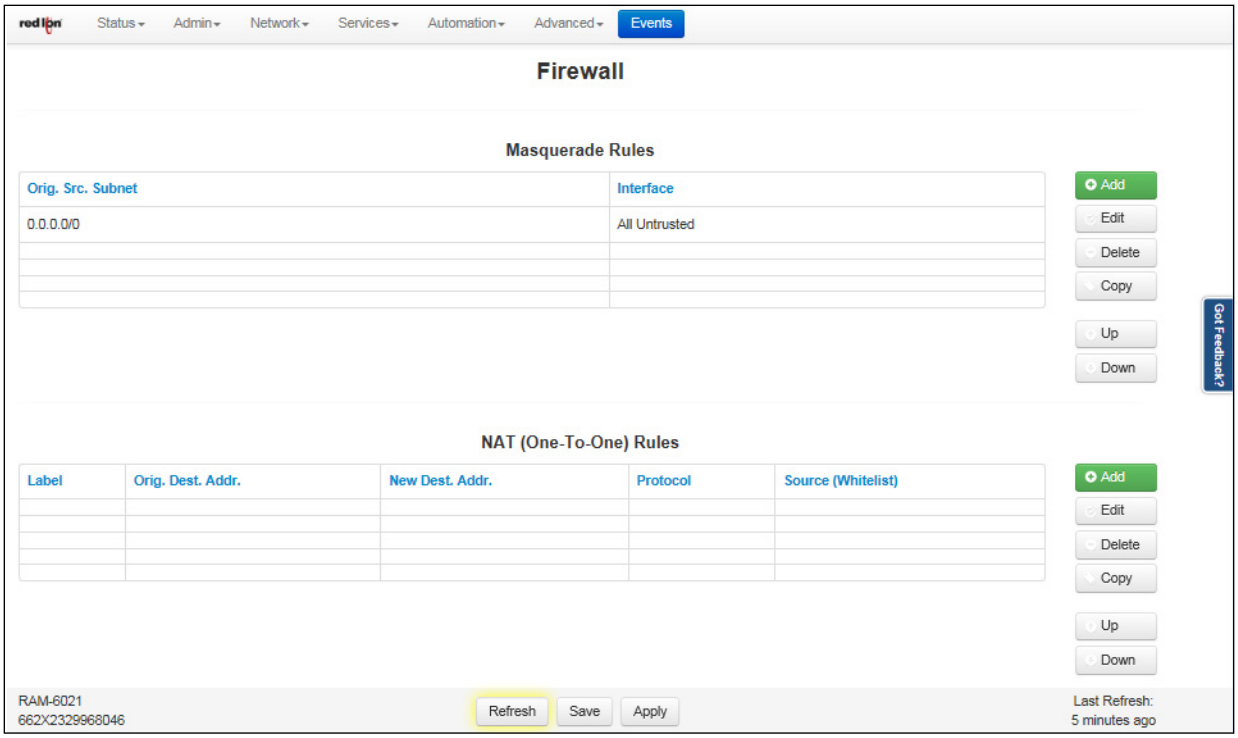
Click on the Finish button. You will be returned to the Firewall Access Control List (ACL) Rules dialog window and the Filter Rules table will now be populated with the recently entered data.

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 butt

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.

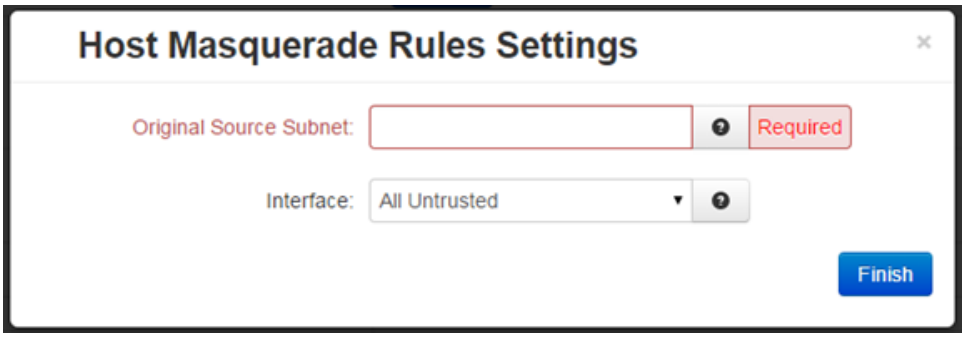
Masquerade/NAT/DMZ Rules

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 will appear::



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.

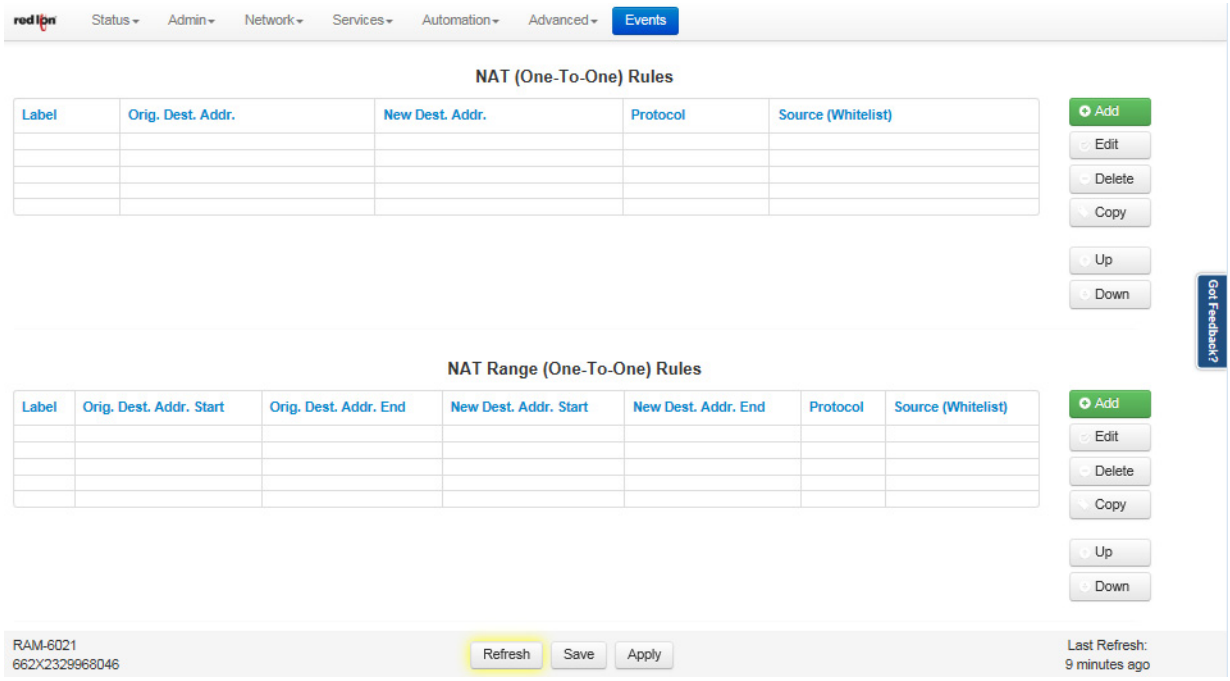
Click on the Finish button. You will be returned to the Masquerade/NAT/DMZ Rules dialog window and the Masquerade Rules table will now be populated with the recently entered data.

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. To copy an existing rule, select it in the table and click on the Copy 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.

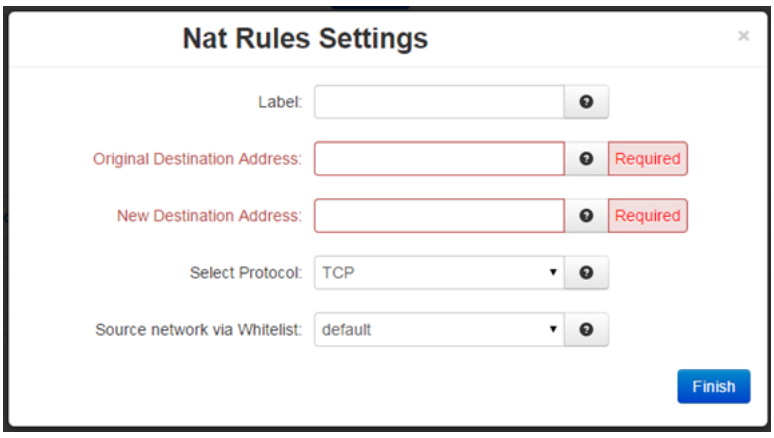
One-to-One NAT will perform a complete forwarding of app ports on the Original Destination IP to a new IP address entered in New Destination. Because the Original Destination need not be configured on this router, an interface is not required to setup.

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.



To add a new NAT (One-to-One) rule:

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



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 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 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 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: 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 NA 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.

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

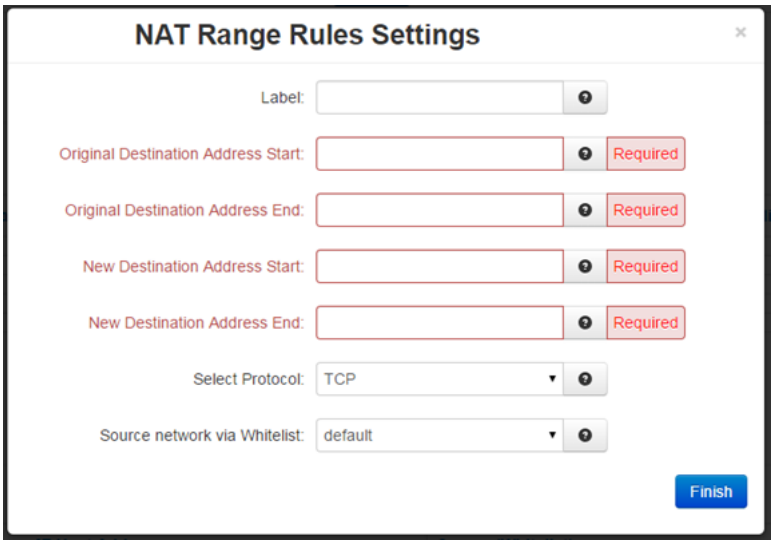
Source (Whitelist): Select a whitelist name from the list of names available in the drop-down list box provided. Whitelists may be viewed/defined via the **Network/Firewall/ACL Rules** screen.

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 rule:

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



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 fol-lowing 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, 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 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.

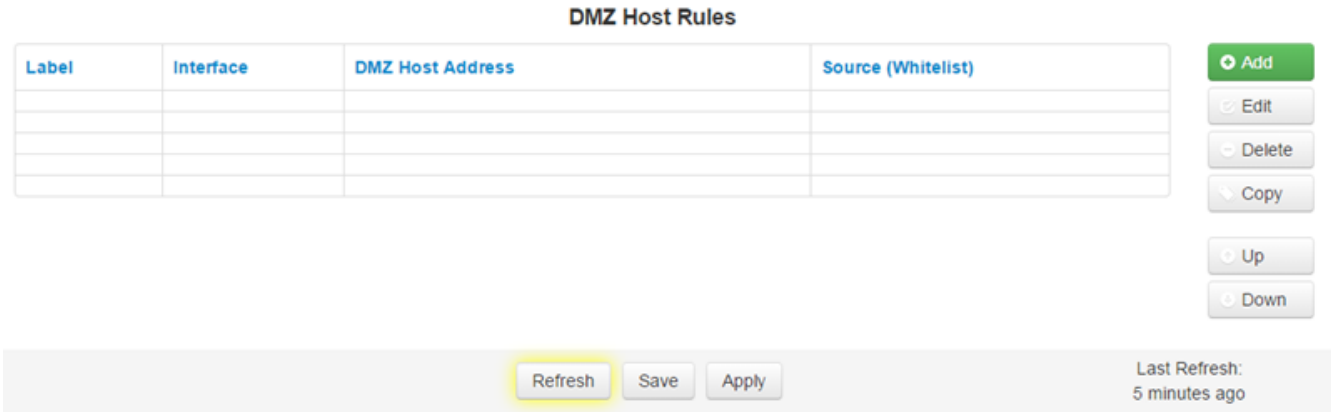
Source Network via Whitelist: Select a whitelist name for the list of names available in the drop-down list. Whitelists may be viewed/defined via the **Network/Firewall/ACL Rules** screen.

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.

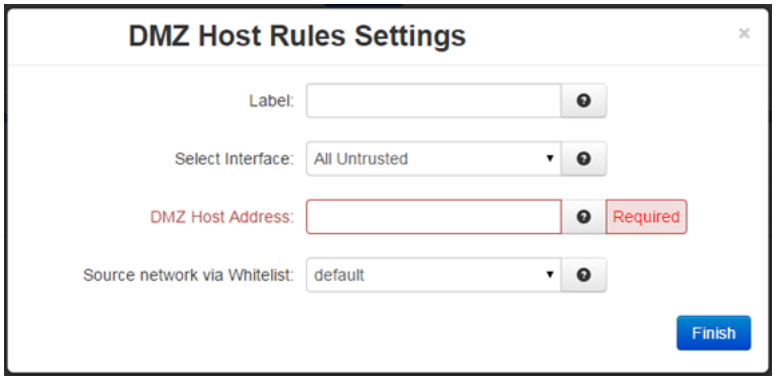
DMZ Rules:

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 will appear:



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. Supported characters are alphanumeric plus the fol-lowing 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.

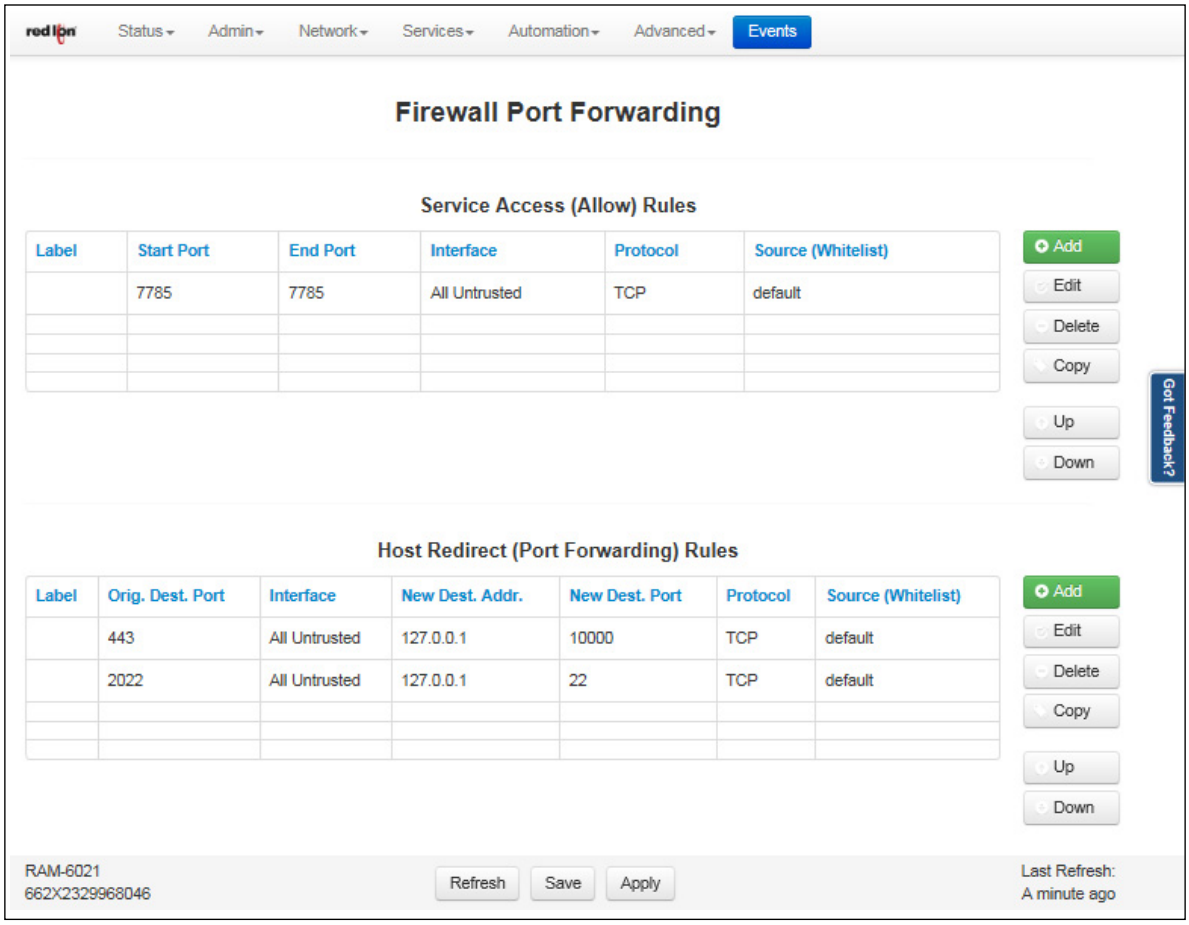
Click on the Finish button. You will be returned to the Masquerade/NAT/DMZ Rules dialog window and the NAT Rules table will now be populated with the recently entered data.

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

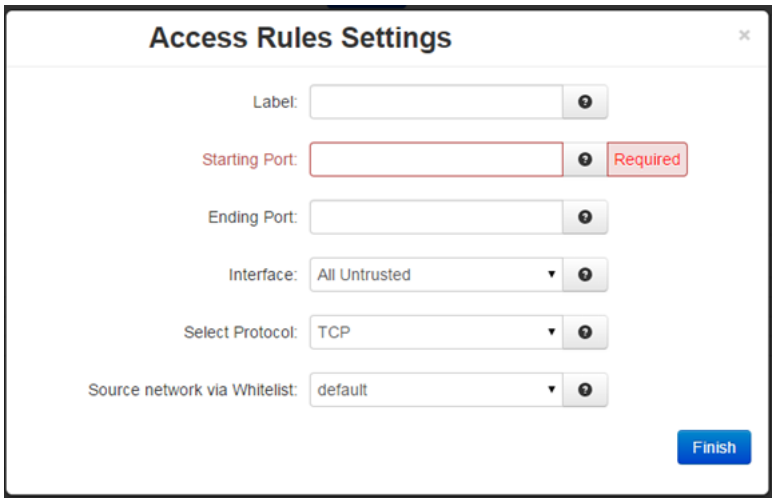
The Firewall Port Forwarding is used to configure routes from a small range of IP Addresses or all IP Addresses through one or more interfaces to a designated IP Address located behind the Red Lion router.



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 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 Service 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.

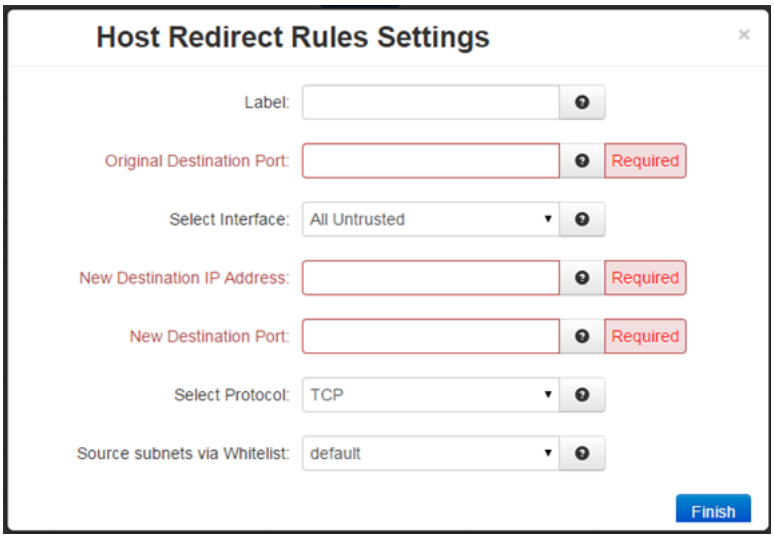
Click on the Finish button. You will be returned to the Firewall Port Forwarding dialog window and the Service Access (Allow) Rules table will now be populated with the recently entered data.

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 will appear:



Label: Enter a description to describe this Redirect Rule. This field is not required for Redirect Rules functionality and it is just for NAT Range Rule identification. Supported characters are alphanumeric plus the fol-lowing 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.

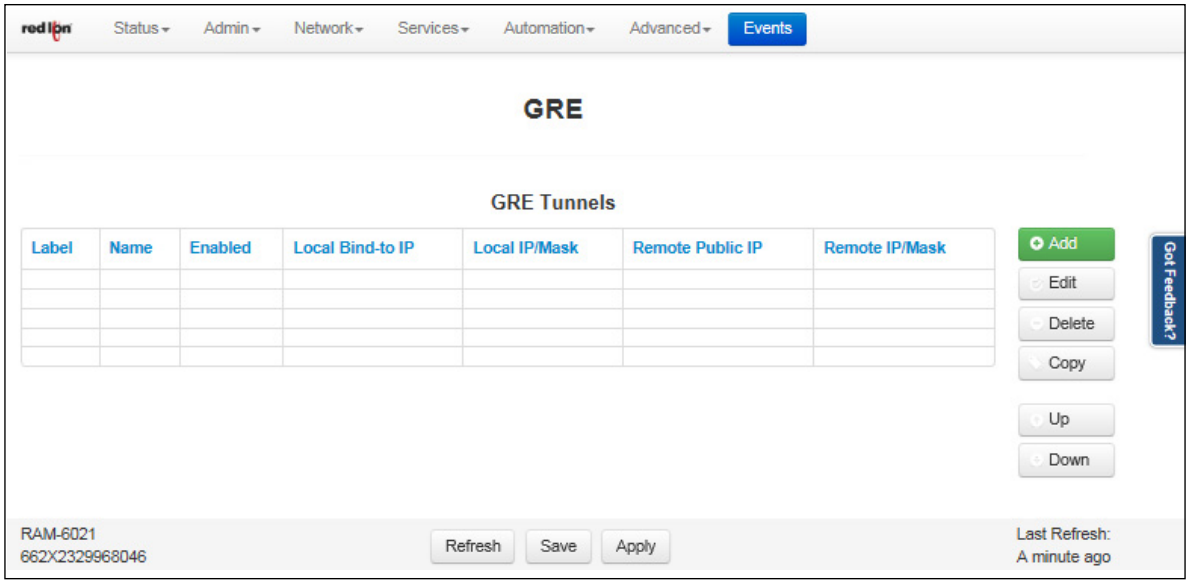
2.4.3 Tunneling

The Tunneling menu is divided into 2 sub-sections: GRE Tunnels and IPSEC.

GRE Tunnels (Generic Routing Encapsulation)

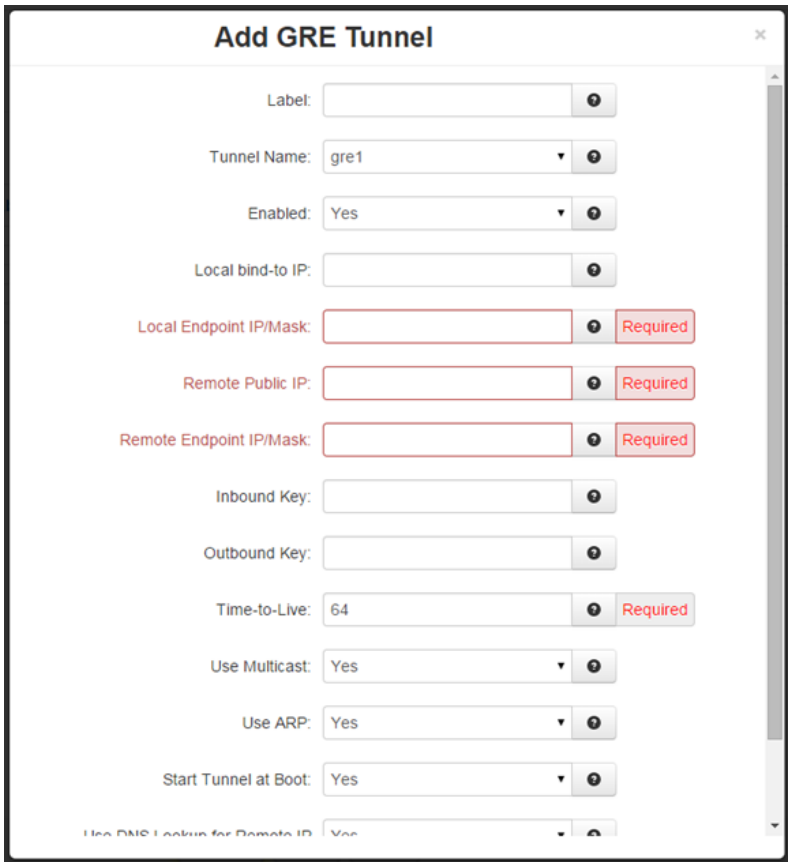
The GRE Tunnels menu item is used to configure a GRE Tunnel. GRE is a tunneling protocol that was originally developed by Cisco. It can do a few more things than IP-in-IP tunneling. For example, you can also transport multicast traffic and IPv6 through a GRE tunnel.

Click on the GRE Tunnels menu item and the following dialog window will appear:



To add a GRE Tunnel

Click on the Add button and the following window will appear:



Label: Enter a description to describe this GRE 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.

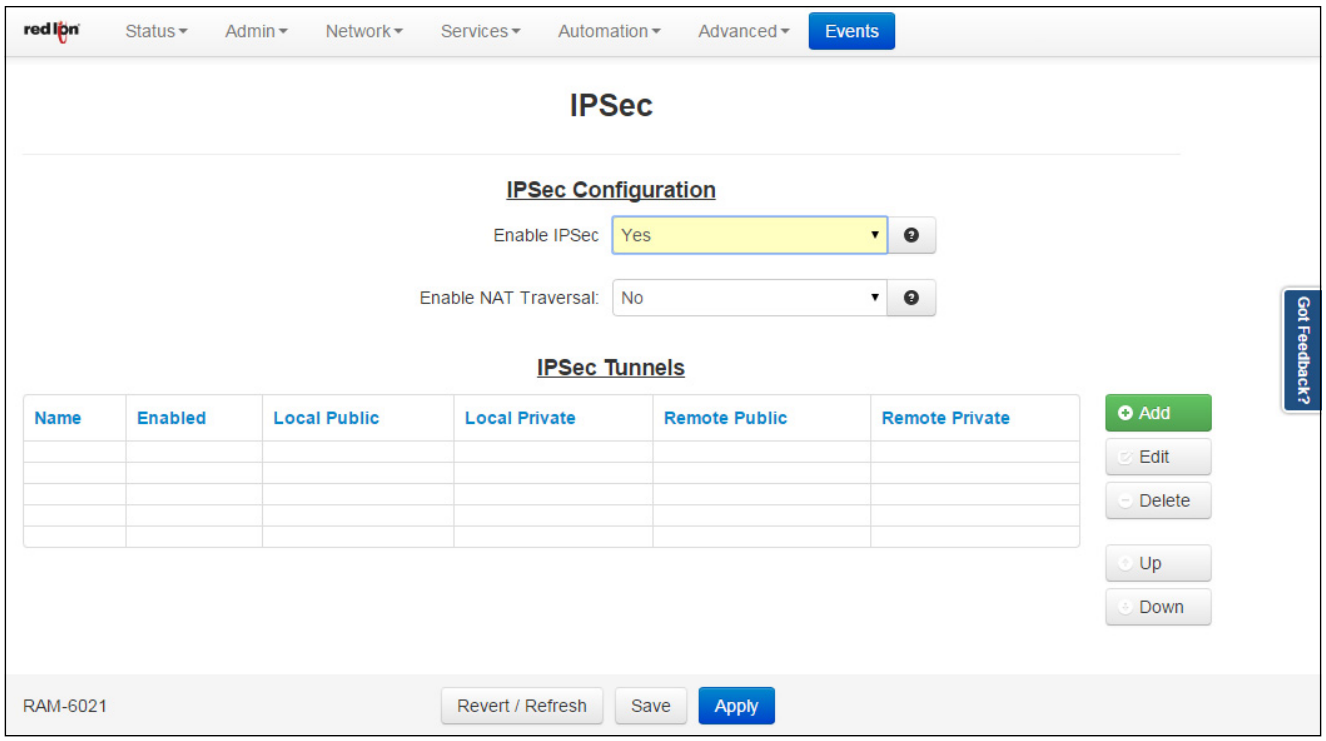
Click on the Finish button. You will be returned to the GRE Tunnels dialog window and the Configuration Table will now be populated with the recently entered data.

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.

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.

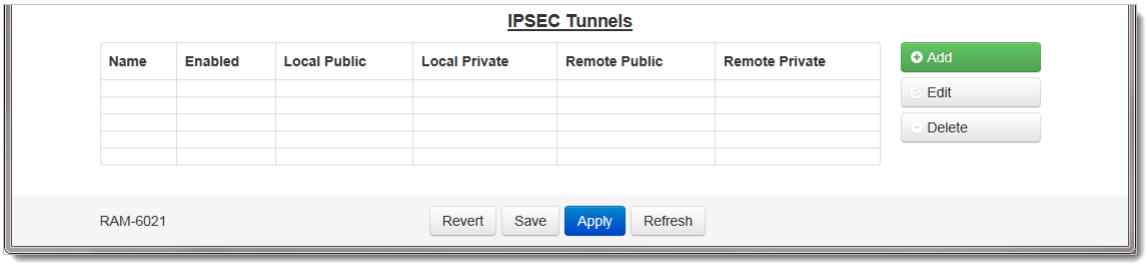


IPSEC Configuration

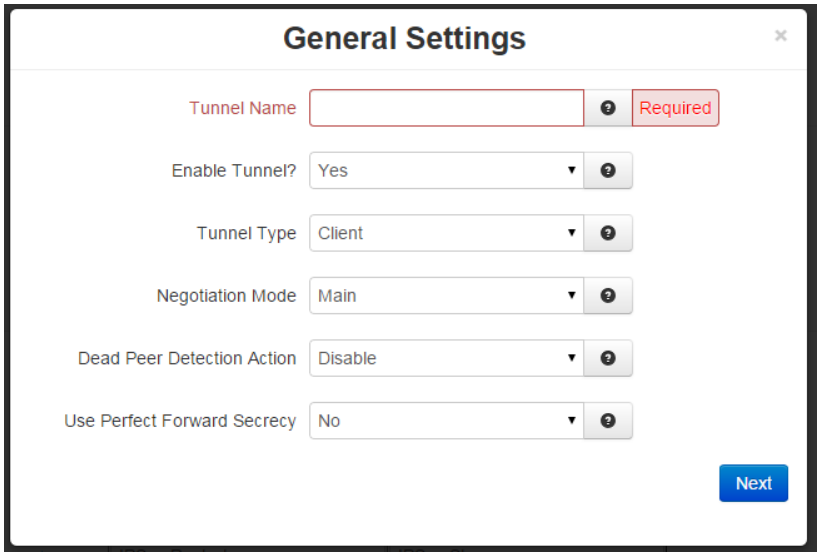
Enable IPSEC: Specify whether you want to enable the IPSEC service. If you select No, all tunnels will be disabled.

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

IPSEC Tunnels



Click on the Add button and the *General Settings* dialog window will appear.



Tunnel Name (Required): Enter some descriptive text in this field as an aid identifying it. The value 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 will be:

Client: auto=start

Server: auto=add

Dynamic: auto=route

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

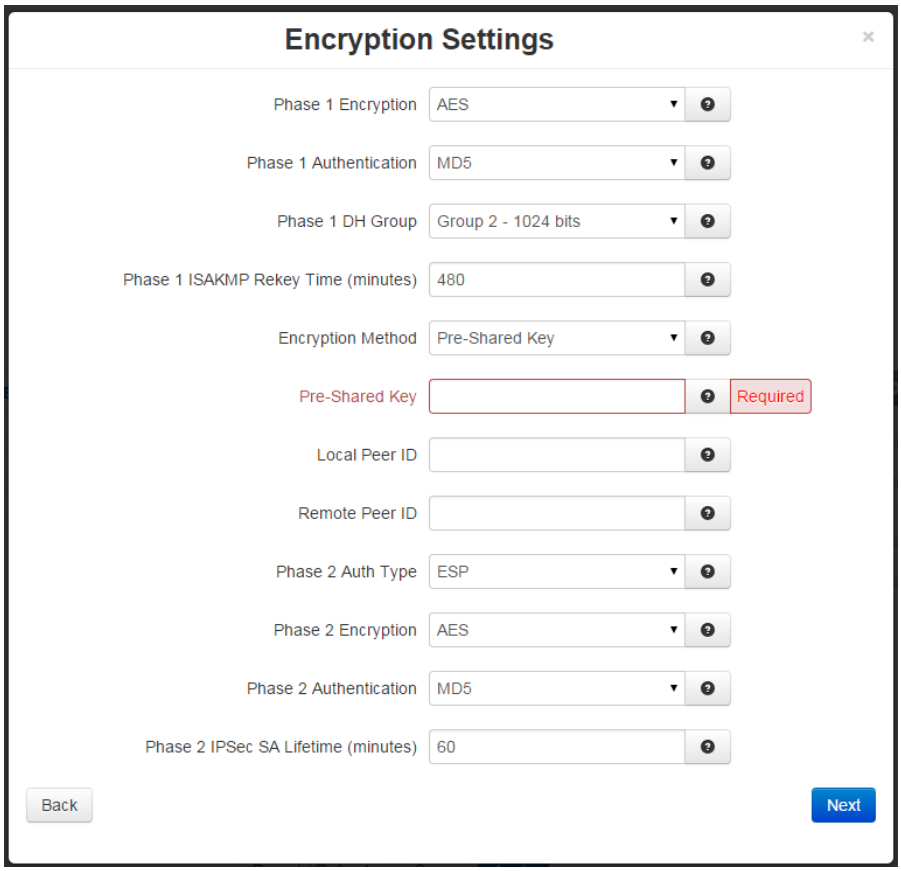
Negotiation Mode: To use Aggressive ISAKMP Negotiations, select Yes from the list provided or No to prevent it's use.

Dead Peer Detection Action: This feature can help detect when a remote end-point is no longer communicating properly. Once an error is detected, the "hold" state will only renegotiate the tunnel after new traffic destined for the tunnel is detected. 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: Specifies whether or not the tunnel will use 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 will appear:.



Phase 1 Encryption: Select the type of encryption needed for phase 1 (IKE).

Phase 1 Authentication: Select the type of authentication needed for phase 1 (IKE).

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 Group 1 (768 bits), Group 2 (1024 bits), Group 5 (1536 bits) or 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. 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.

Phase 1 ISAKMP Time (minutes): Select how long, in minutes, the keying channel of a connection (ISAKMP SA) should last before being renegotiated.

Encryption Method: Specify how the two end-points for this tunnel will 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.

Pre-Shared Key (Required): Specify the key to be exchanged for encryption negotiation during phase (IKE). 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. 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. Can be an IP address of a fully qualified domain name preceded by @ (which is used as a literal string and not resolved).

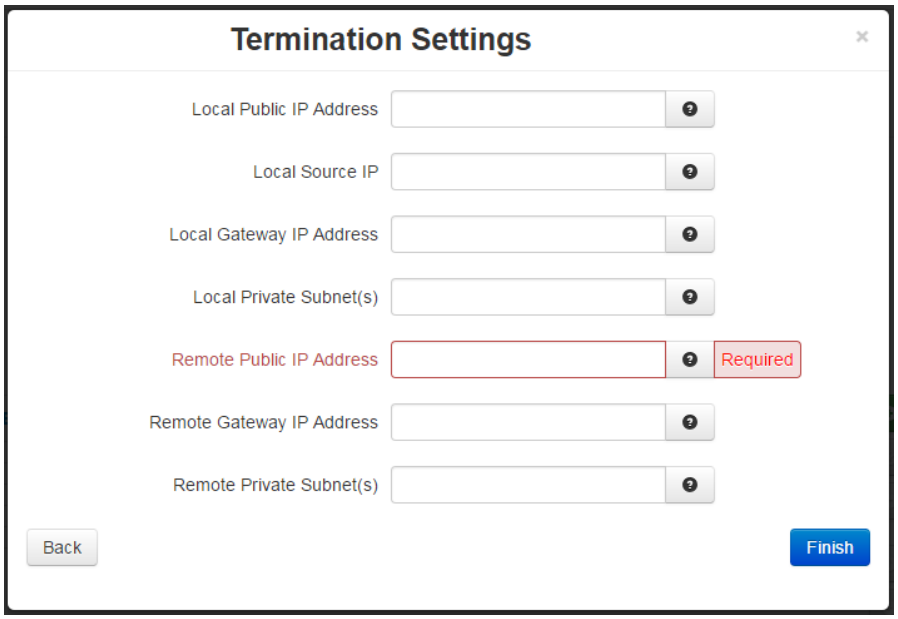
Phase 2 Auth Type: Defines whether authentication should be done as part of ESP encryption, or separately using the AH protocol.

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 following Termination Settings dialog window will appear:



Local Public IP Address: Specify the IP Address of the left participant's public network interface.

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 subnet or right. Otherwise, it will use 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, 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 will use the right participant as its next hop.

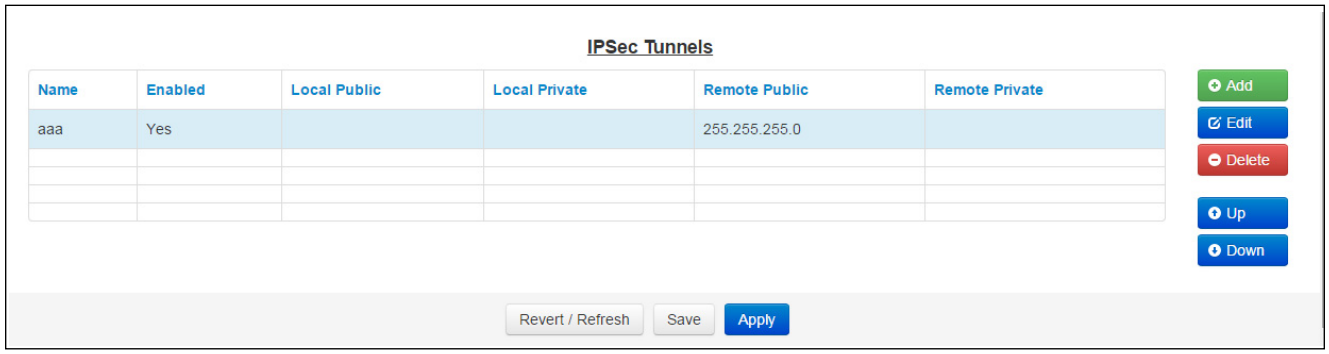
Local Private Subnet(s): Specify the private subnet(s) behind the left participant, expressed in CIDR format (xxx.xxx.xxx.xxx/nn) as network/netmask. More than one subnet can be specified by using a semi-colon to separate each entry.

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 will use 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 Firewall Port Forwarding dialog window and the IPSEC Tunnels table will now be populated with the recently entered data.

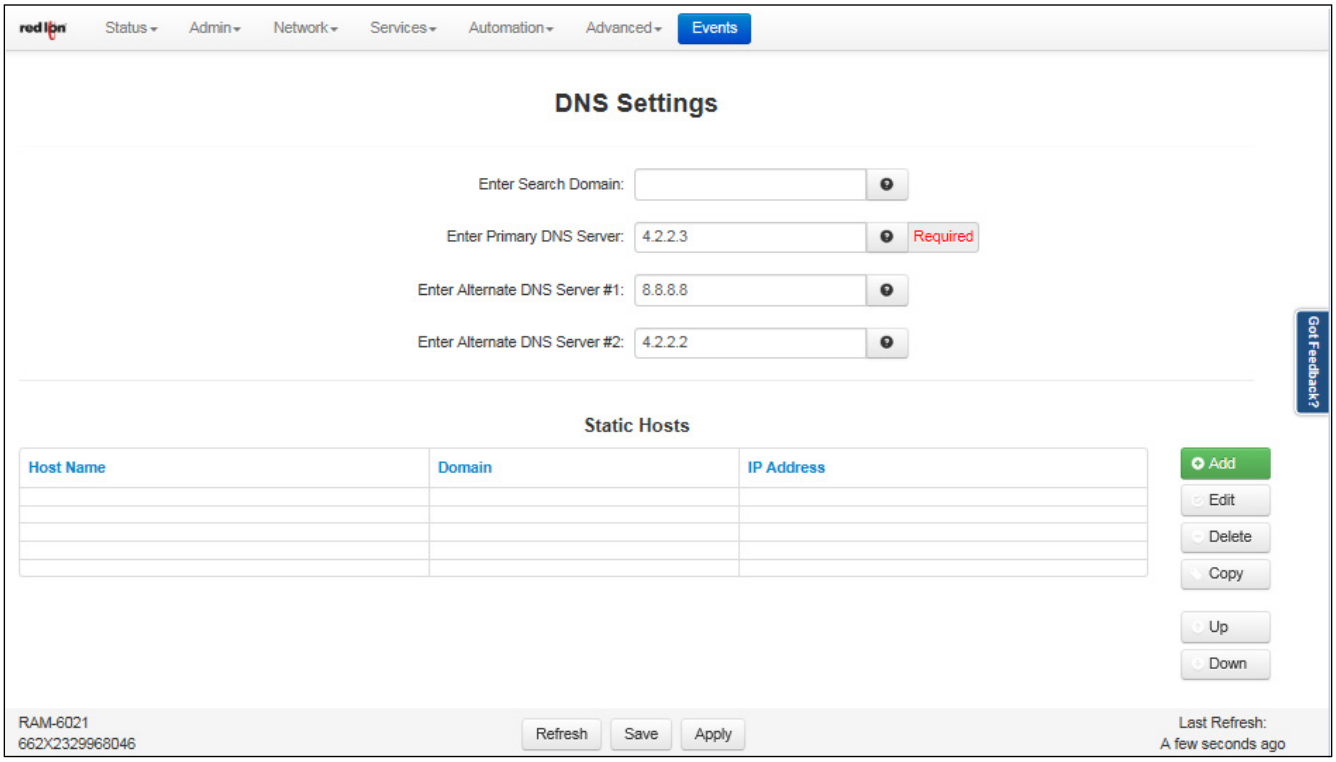


To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.

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.

2.4.4 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.



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.

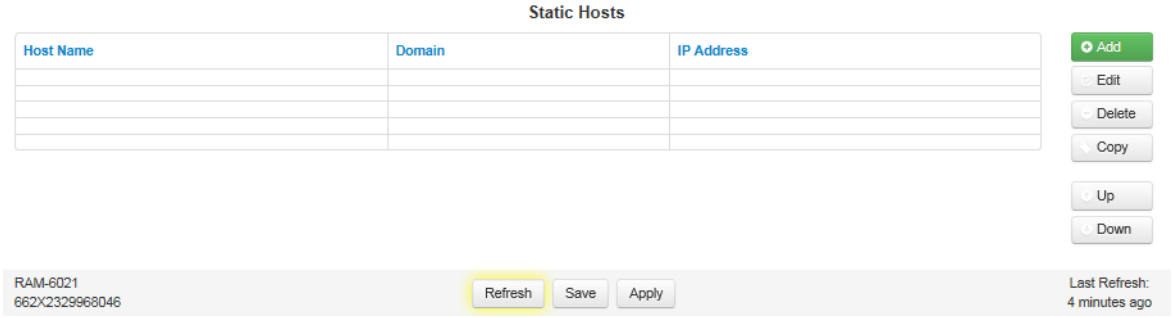
Note: This setting may be overridden if a network interface is set to obtain its configuration information from its peer (either via PPP or DHCP).

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).

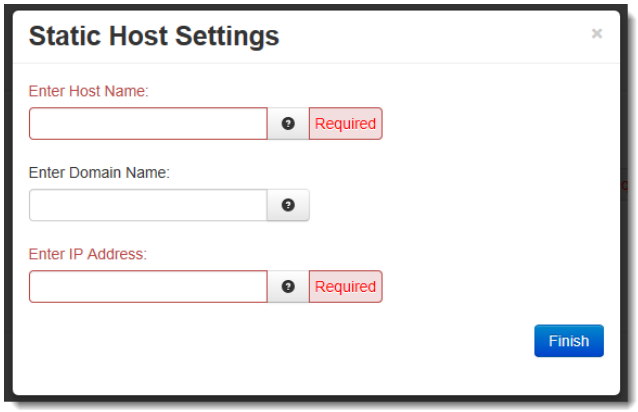
Enter Alternate DNS Server #2: *This field is already filled in; it is showing the current server in use by the Red Lion server.* Enter the IP Address of a Backup DNS Server you want to use, if the Primary DNS Server is unable to perform a DNS lookup. **Note:** This setting may be overridden if a network 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 router to resolve local host names to IP addresses.



Click on the Add button on the following dialog window will appear:



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.

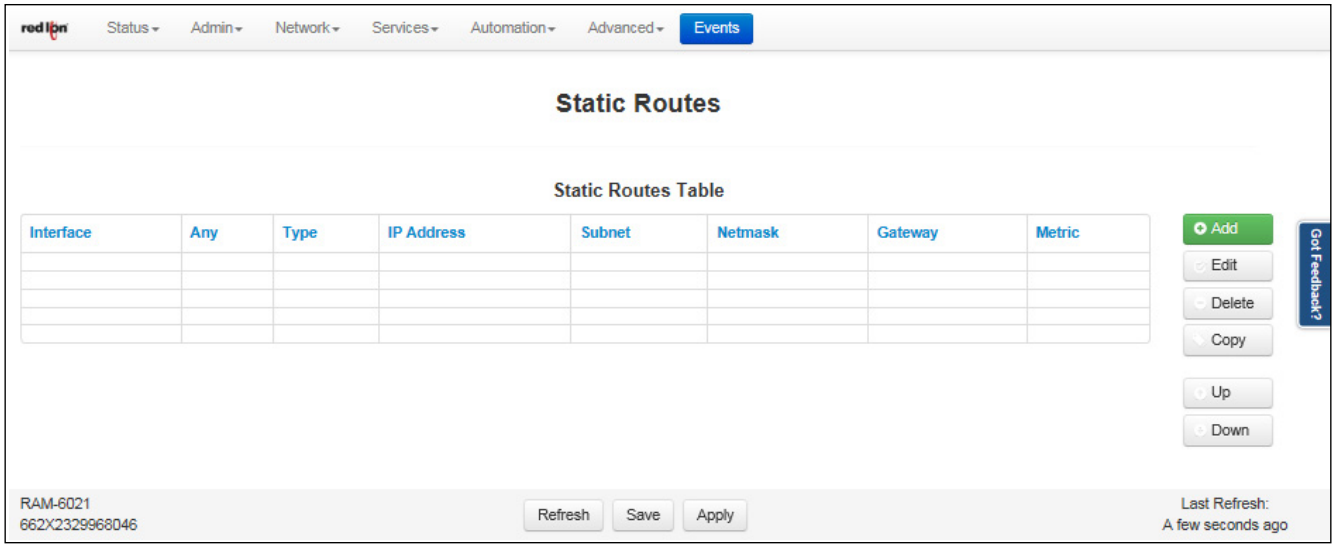
To delete an existing host, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.

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.

2.4.5 Static Routes

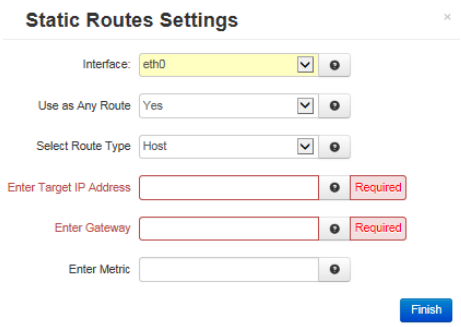
The Static Routes menu allows you to configure a route to a network through an interface manually.

Click on the Static Routes menu item and the following dialog window will appear:



To add a Static Route on the Red Lion router:

Click on the Add button and the dialog window below will appear:



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 (WAN), and the ppp0 interface becomes active, then the route will be reapplied to eth0 (WAN).

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 (LAN), then the route will be assigned only when eth1 (LAN) 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 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 router and that 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.

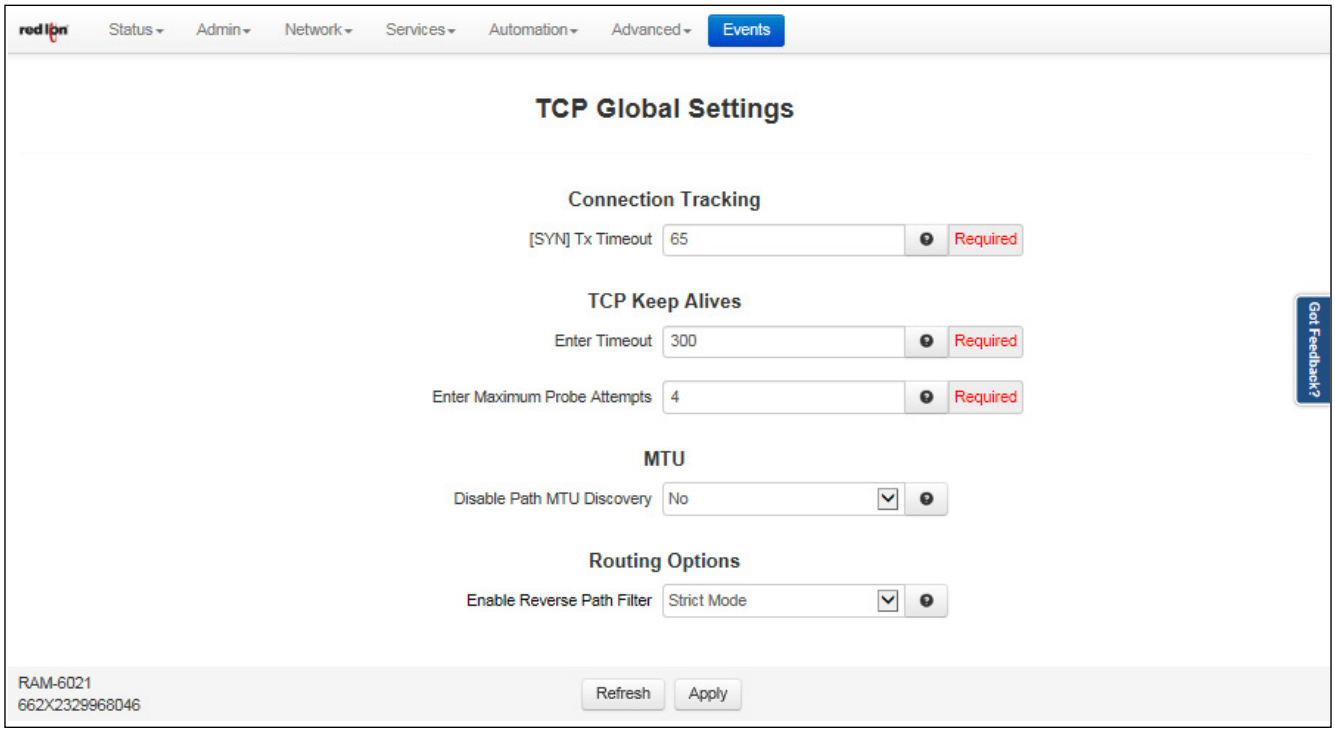
Click on the Finish button. You will return to the Static Routes dialog window and the Static Routes table will now be populated with the recently entered data.

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.

2.4.6 TCP Global Settings

Click on the TCP Global Settings menu item the following dialog window will appear:



[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.

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 settings are 3-6.

Disable Path MTU Discovery: Disable/Enable Path MTU Discovery. The recommended value for this field is No (off).

Routing Options: Select the desired Reverse Path Filter (rp_filter) option.

Reverse path filtering is a mechanism within the Linux kernel, as well as many non-Linux networking devices, to check whether a receiving packet source address is routable.
In other words, 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.

- 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**.

Available Options:

- 0 - No source validation.
- 1 - Strict mode as defined in RFC3704 Strict Reverse Path Each incoming packet is tested against the FIB and if the interface is not the best reverse path the packet check will fail. By default failed packets are discarded.
- 2 - Loose mode as defined in RFC3704 Loose Reverse Path Each incoming packet's source address is also tested against the FIB and if the source address is not reachable via any interface 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.

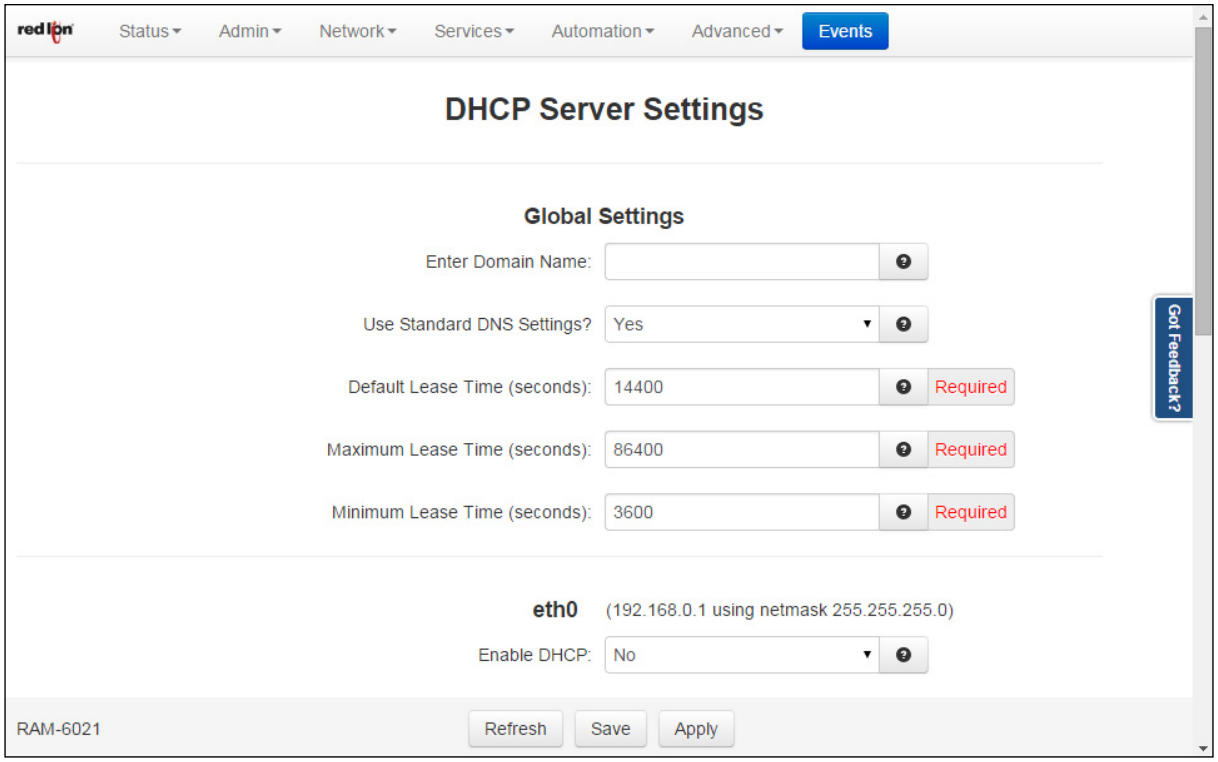
2.5 Services Tab

The Services Tab is where you can configure the various service offerings of the Red Lion router. These services include DHCP Server, DHCP Relay, Dynamic DNS, SN Proxy Settings, SixView Manager, SSH/TELNET Server, SSL Connections, SNMP Agent, Ping Alive, RAMQTT and Serial IP.

2.5.1 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 router.

Click on the DHCP Server menu item and the following dialog window will appear:



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” will allow 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 will allow 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 will allow clients to maintain their leases. Default “**86400**”(24 hours).

Minimum Lease Time (seconds): Specify the amount of time, in seconds, that the DHCP Server will allow clients to maintain their leases. Default "**3600**"(1 hour).

eth0: (WAN)

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.

eth1: (LAN)

Enable DHCP: Specify whether you want to enable a DCHP 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 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): Enter the Ending 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.

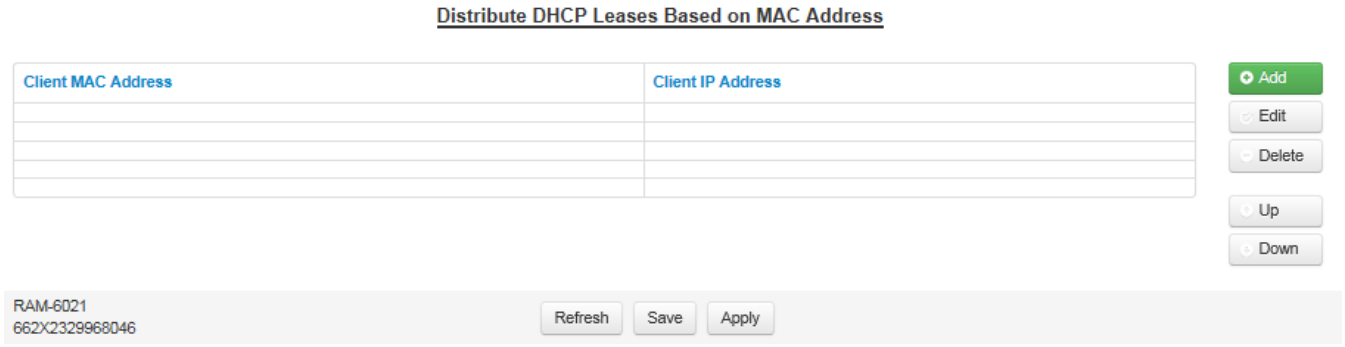
Recommended Setting: An address valid for the subnet for which the interface is configured. Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

Ending Address (Required Field): Enter the Ending IP Address of a range you want the DHCP Server to provide for clients.

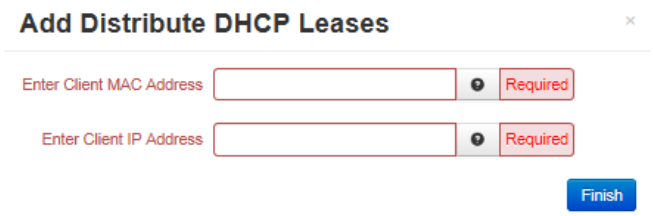
Recommended Setting: An address valid for the subnet for which the interface is configured, beyond that chosen for the starting value of the range. Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically 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 will appear::



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.

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 sue statically assigned IP addresses.

This address should have been 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.

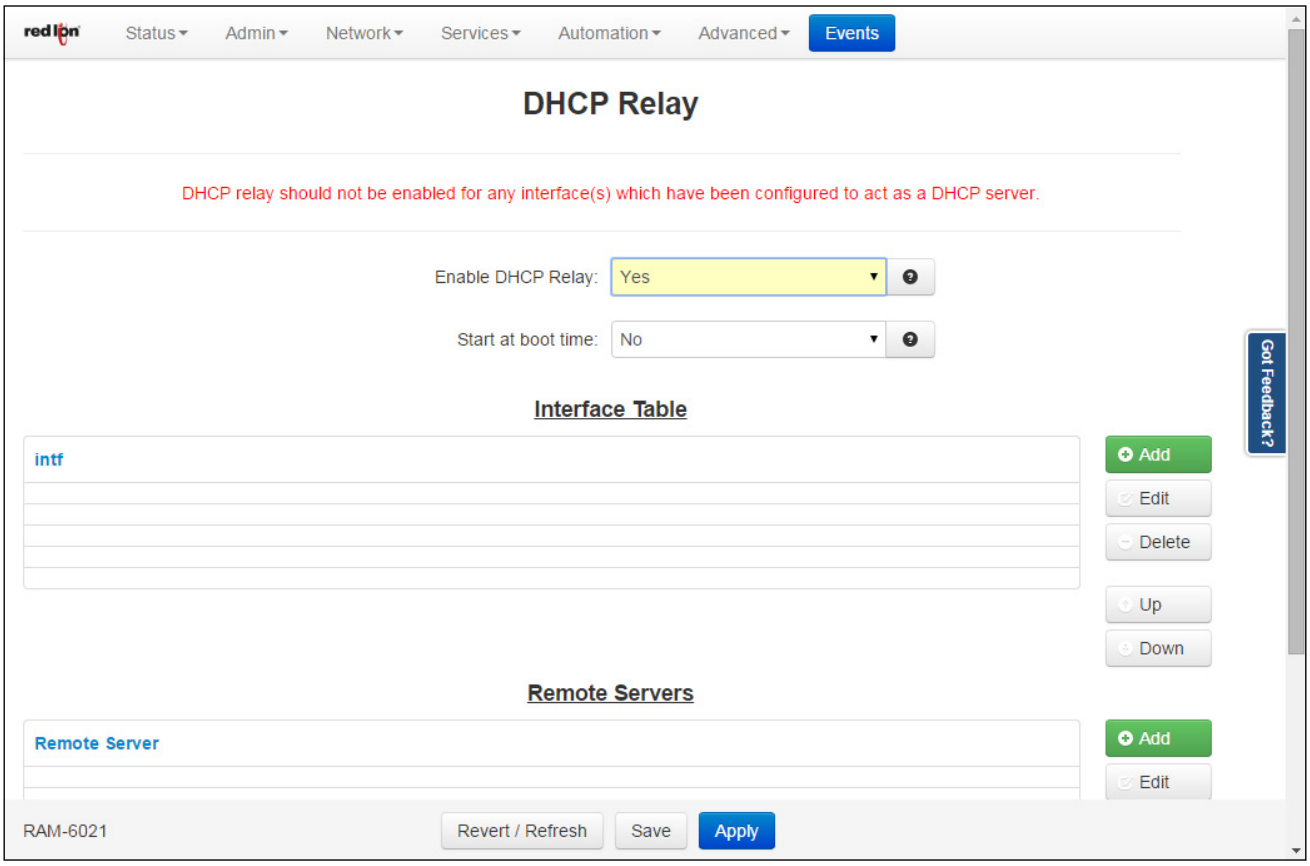
To delete an address, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.

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.

2.5.2 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.

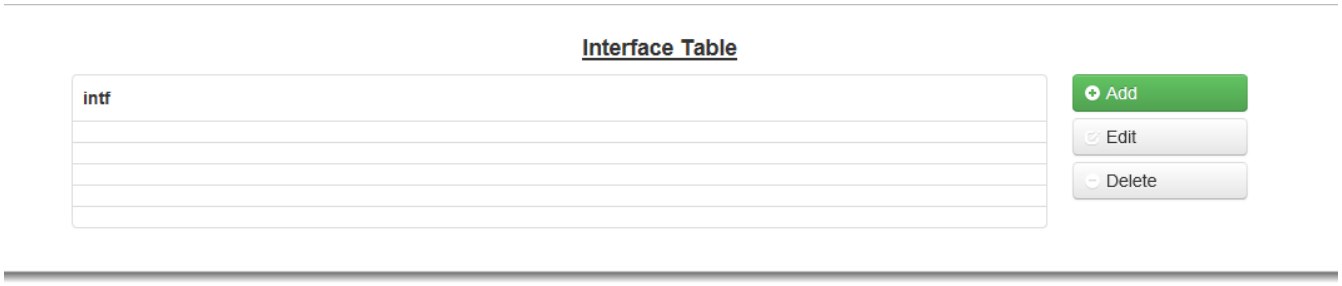
Click on DHCP Relay the following dialog window will appear:



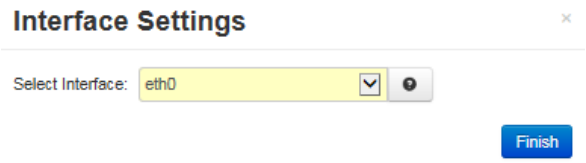
Enable DHCP Relay: Select YES to enable the DHCP Relay, or NO to disable it. The service will start once the Apply button is clicked. If the Save button is clicked, the service will not be started until the device is rebooted and then **only** if the *Start at boot time* option has also been set to YES.

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:

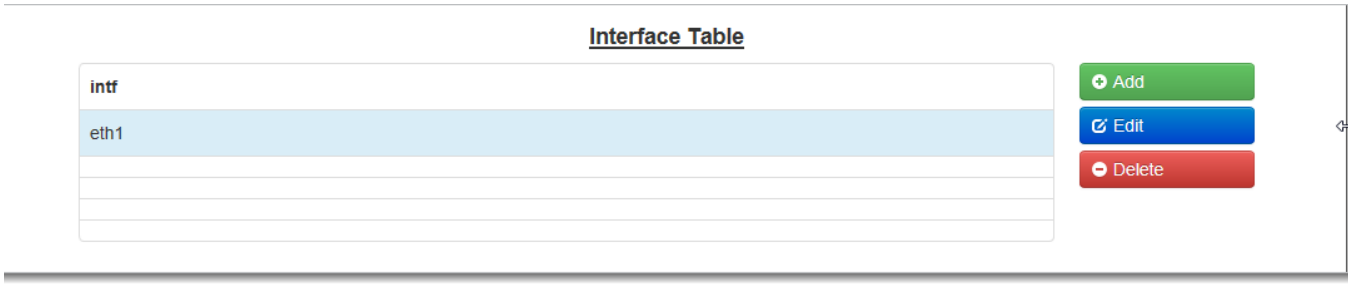


Click on the ADD button and the following dialog window will appear::



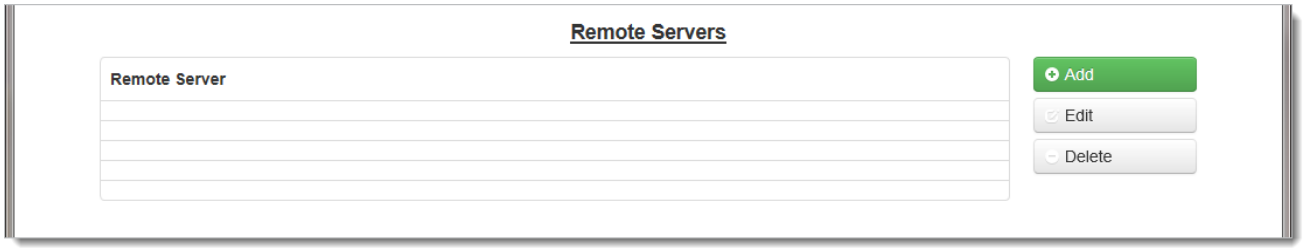
Select Interface: Select the interface to receive its IP from the remote DHCP server from the drop down menu.

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.

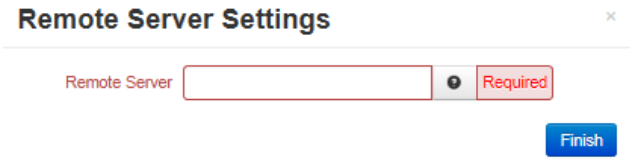


To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.

Remote Servers:

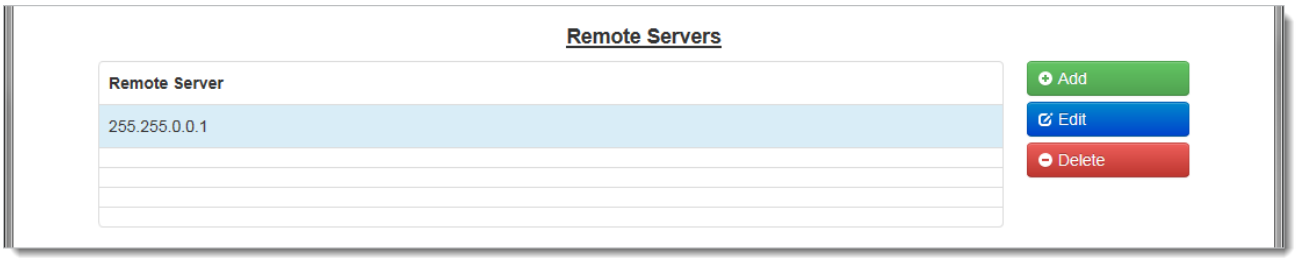


Click on the ADD button and the following dialog window will appear::



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.



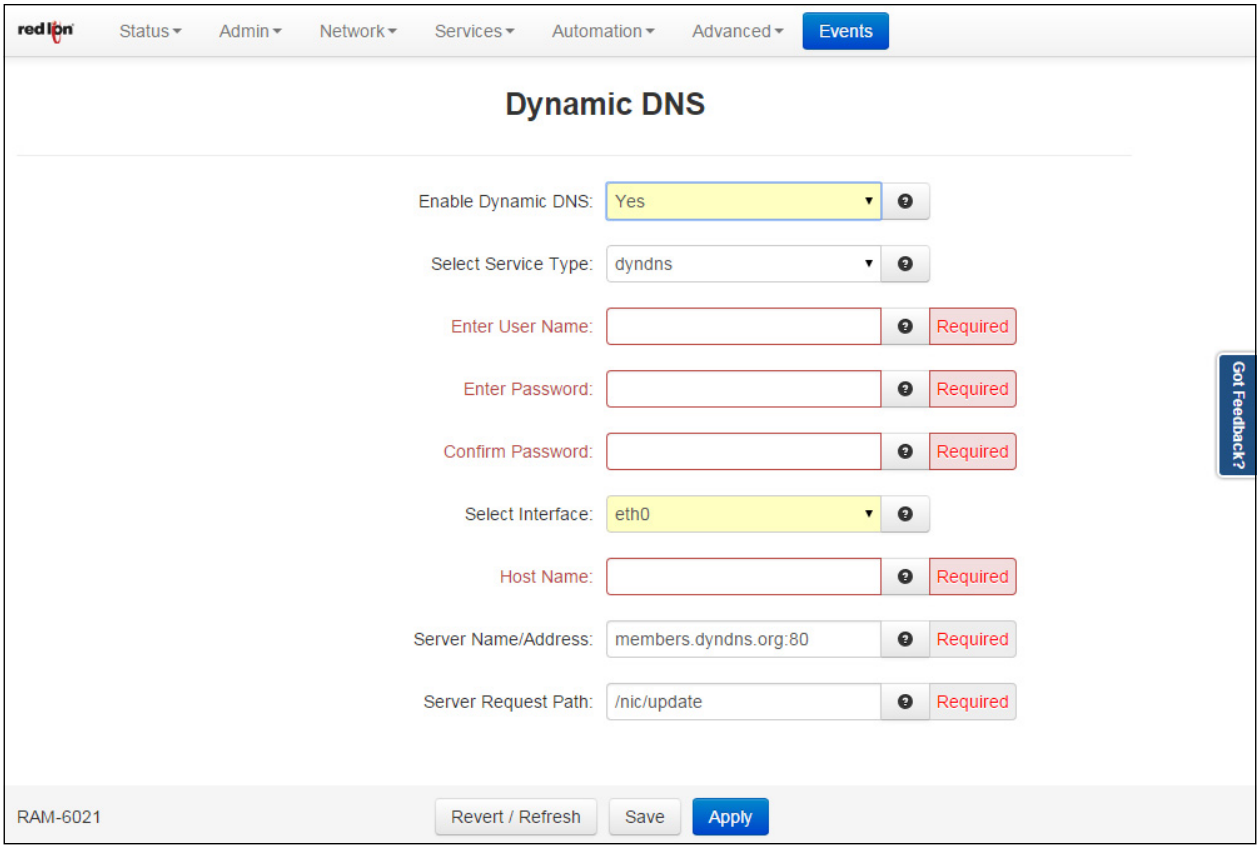
To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the *Edit* button.

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.

2.5.3 Dynamic DNS

The Dynamic DNS menu item is used to configure a dynamic DNS name for the Red Lion 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 will appear:



Enable Dynamic DNS: Select YES to enable the Dynamic DNS service.

Select Service Type: Select the desired Dynamic DNS Service from the list provided: dhs, dyndns, dnydns-Custom, dyndns-Static, dyns, easydns, easynds-partner, ods, zoneedit, Duckdns.

Enter User Name (Required): Enter the User Name used to access your Dynamic DSN 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 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 wish 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 provide the appropriate value, which can be entered manually.

Server Request Pate (Required): Enter the Request URI required to connect to the Dynamic DNS Service in this field.

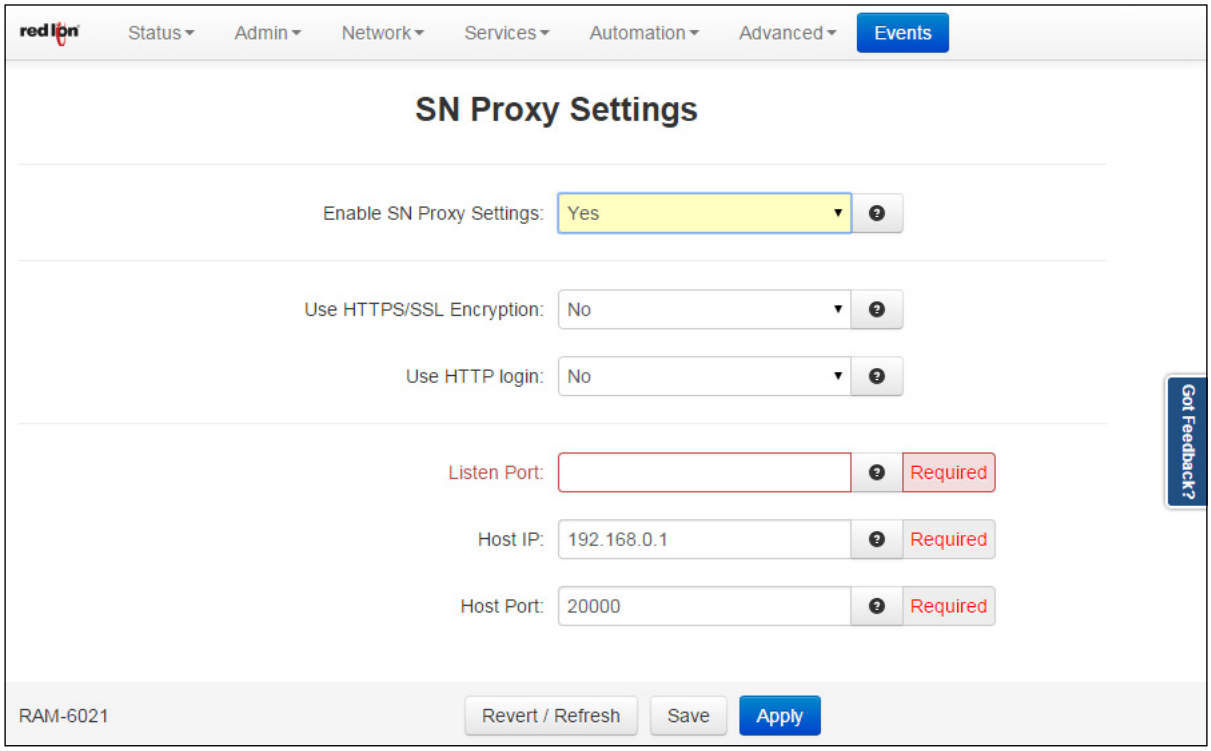
The recommended setting for this field is automatically provided when a Service type is selected. If you require a value other than the recommended value, your Network Administrator or Dynamic DNS Service Provider should be able to provide the appropriate value, which can be entered manually.

Click on the Save button changes to saved with 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.

2.5.4 SN Proxy Settings

SN Proxy is a web relay proxy service used to gain access to devices that are behind our Red Lion 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 following dialog window will appear:



Enable SN Proxy Settings: Enables or disables the SN Proxy feature. If NO is selected, all other fields in the dialog window will disappear.

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.

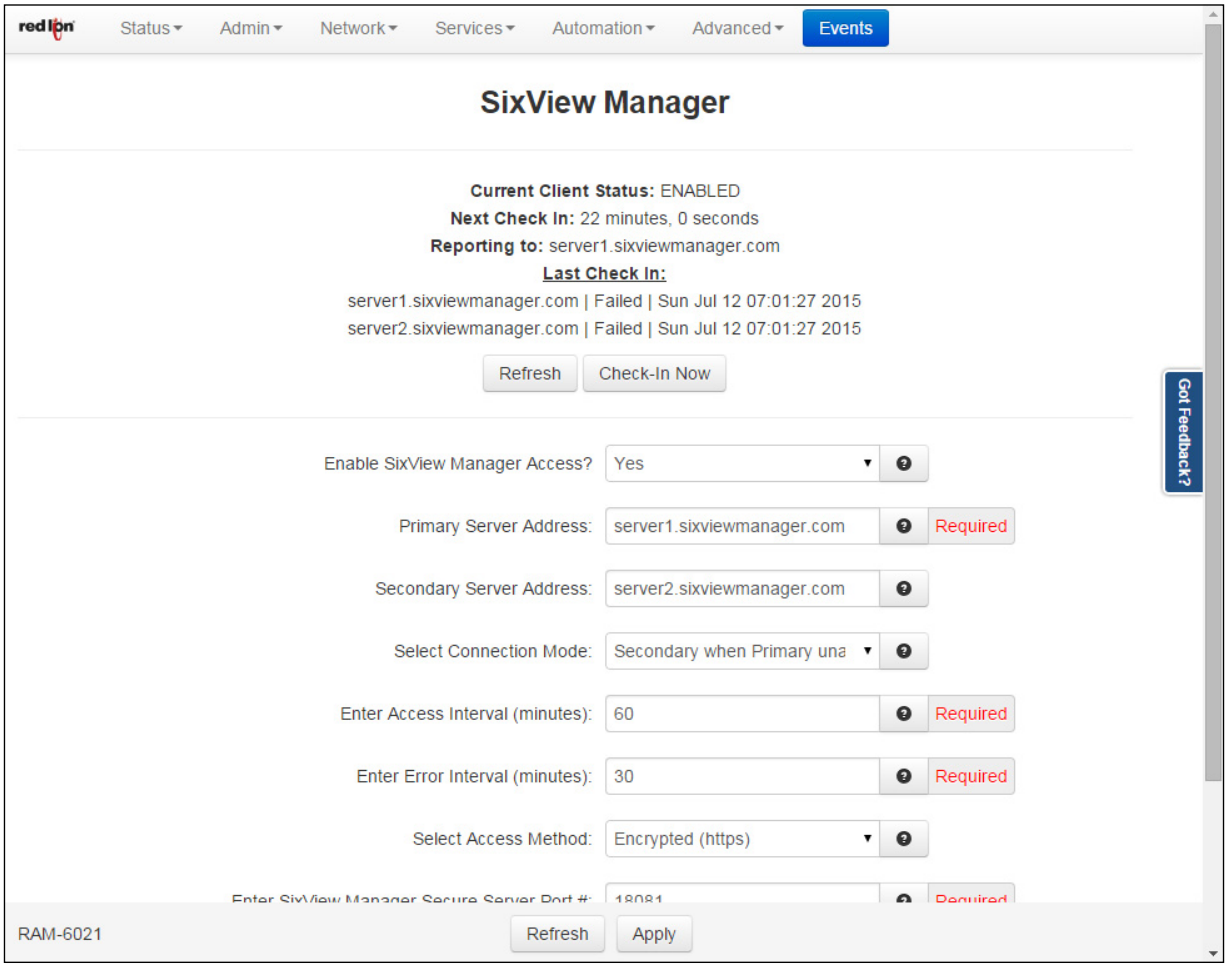
Host Port (Required): Enter the proxy server host port number.

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.

2.5.5 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 will appear:



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 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.

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.

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 value for this field is 30.

Select Access Method: Select the desired Access Method from the provided drop-down.

- **Unencrypted (http):** Faster, but less secure.
- **Encrypted (https):** Slower, but more secure.

Note: The encrypted method adds significant overhead. 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 18080 for http and 18081 for https.

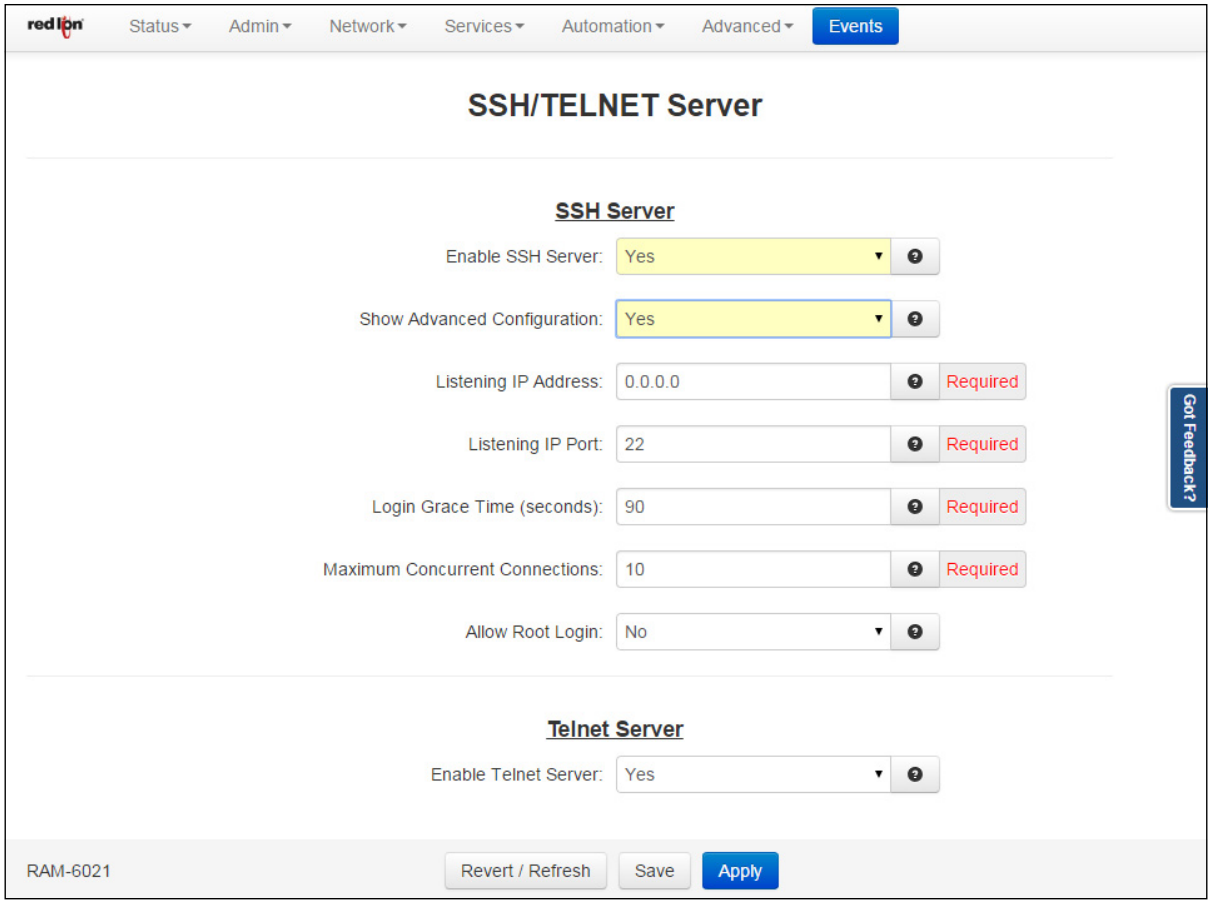
Select Interface: Select the name of the interface to which the SixView Manager Client will bind for communications with the SixView Manager Server. The recommended setting for this field is *None*.

Note: This option will only be necessary if the SixView Manager Client is required to communicate through a configured IPSEC, GRE or IPIP tunnel.

2.5.6 SSH/TELNET Server

The SSH/TELNET Server menu allows you to configure whether the Red Lion router will communicate with the network via Secure Shell (SSH) and to enable or disable TELNET on the Red Lion router.

When you click on the SSH/TELNET Server menu item, the following window will appear:



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.

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.

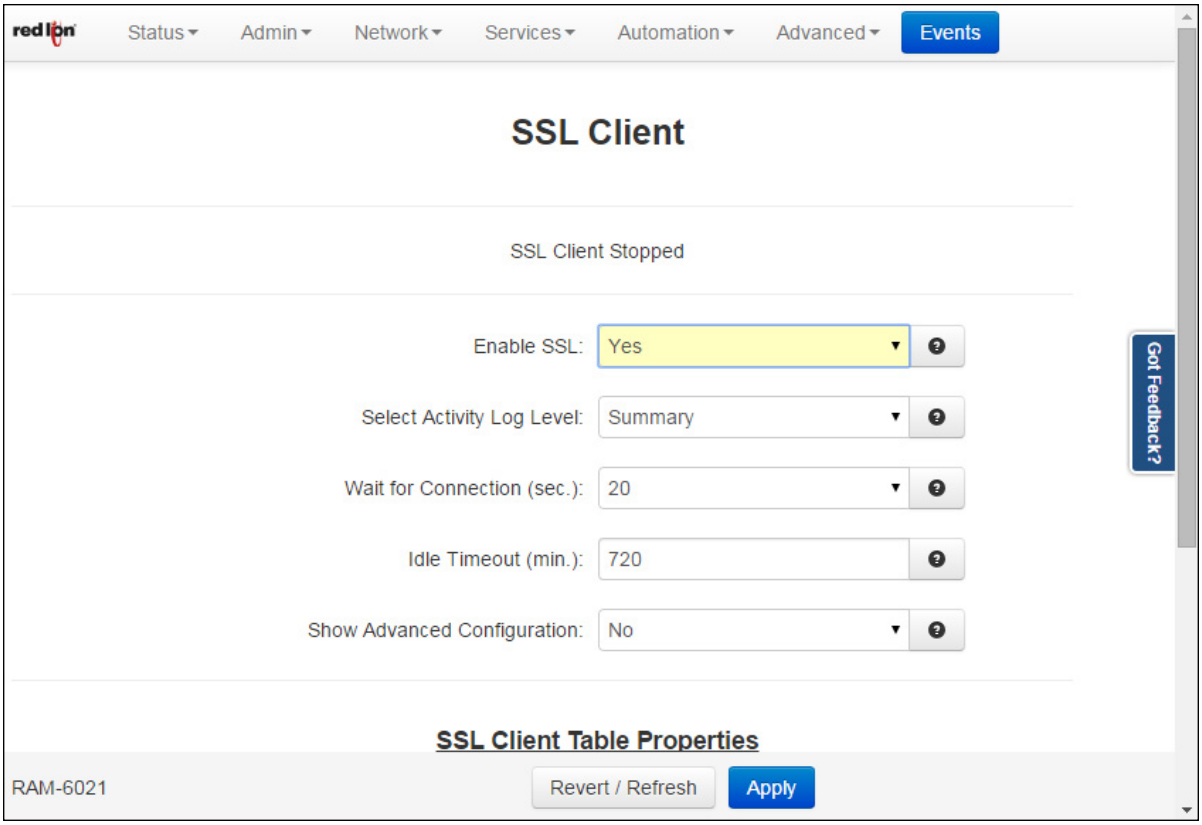
2.5.7 SSL Connections

The SSL Connections option is used to configure the Red Lion router to either act as a Secure Locket Layer (SSL) Client to receive certificates or as an SSL Server to issue certificates. The SSL Connections tab is sub-sectioned in two parts: SSL Client and SSL Server.

SSL Client

The SSL Client option is used to configure the Red Lion router to act as an 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 will appear:



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 un-encrypted 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 will use this certificate chain as a client side certificate chain. Using client side certs is optional. The certificates must be in PEM format, with an un-encrypted key (not password protected when generated). Use Admin->Certificate Manager to install/update certs.

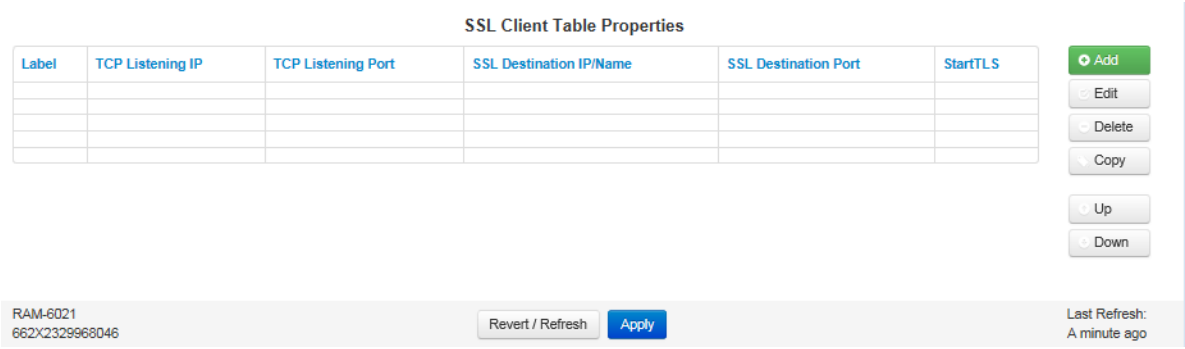
Select Keep-Alive behavior: This option enables TCP Keep-alives on the underlying sockets. The following options are supported:

- **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.

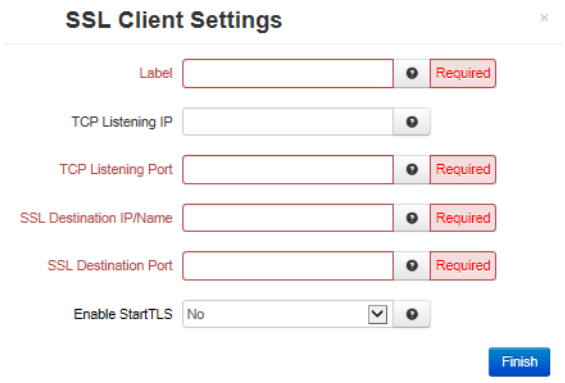
You may need to adjust the master Keep-alive timer via Network->TCP Global Settings->TCP Keep Alives.

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 will appear:



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/Name (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.

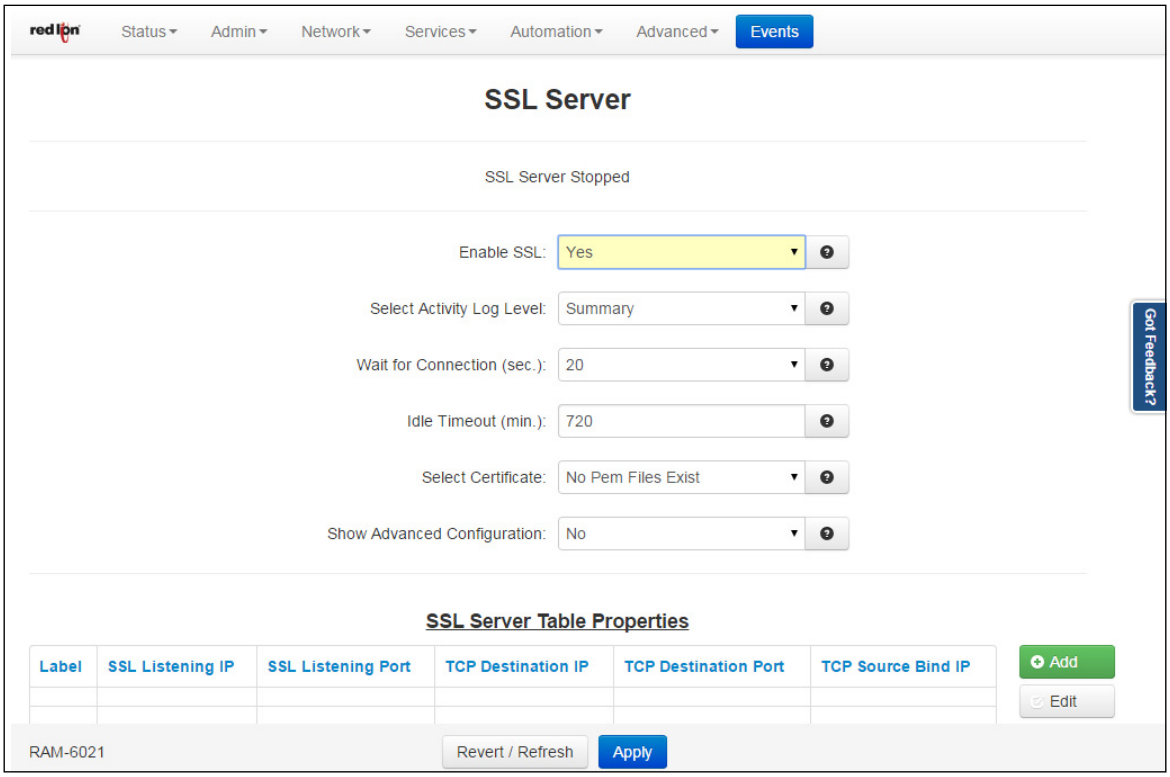
To delete an existing rule, select it in the table and click on the Delete button. To edit an existing rule, select it in the table and click on the Edit button.

Click 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 option is used to configure the Red Lion router to issue SSL certificates to requesting SSL clients.

Click on the SSL Server menu item and the following dialog window will appear:



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 un-encrypted 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 un-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 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:

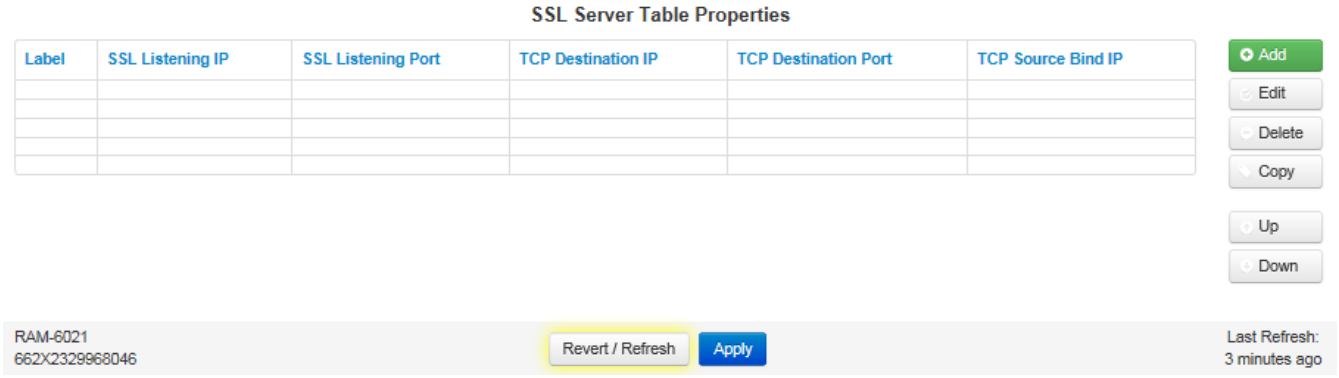
Select Keep-Alive behavior: This option enables TCP Keep-alives on the underlying sockets. The following options are supported:

- **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.

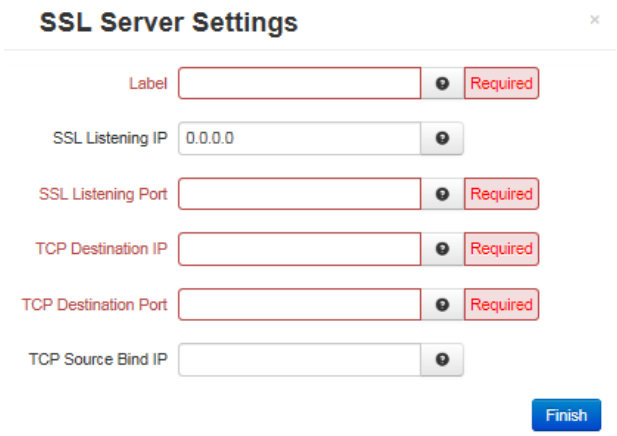
You may need to adjust the master Keep-alive timer via Network->TCP Global Settings->TCP Keep Alives.

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 will appear:



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 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 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.

2.5.8 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 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.

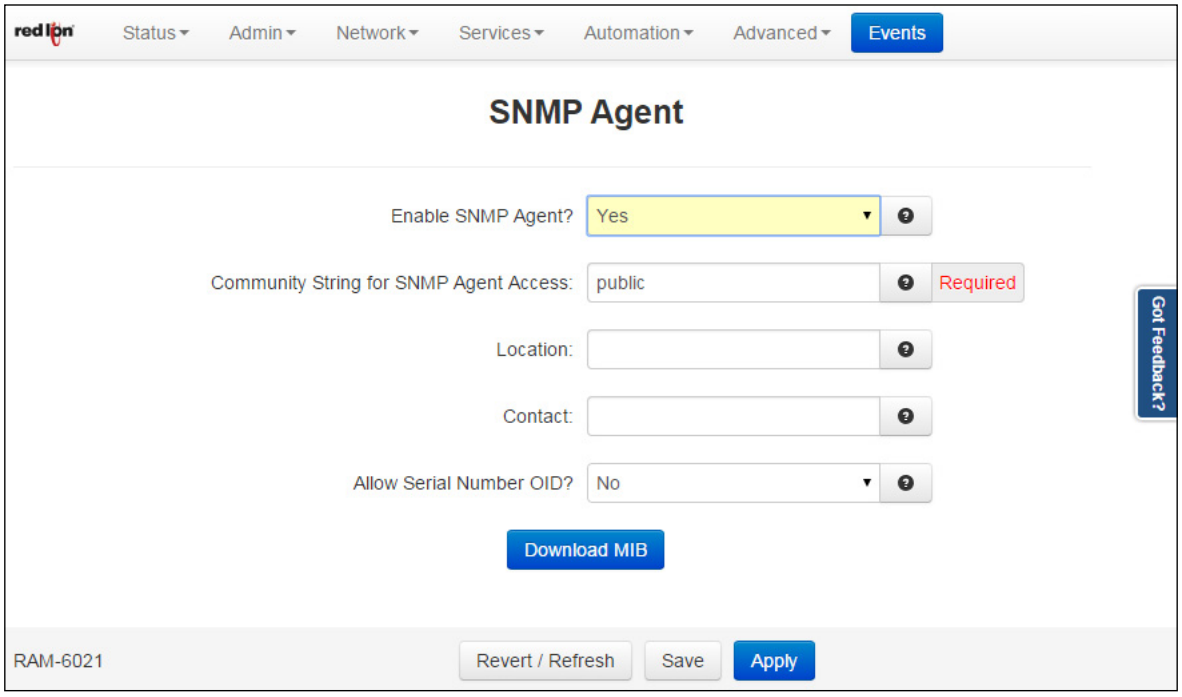
The SNMP Agent allows you to query the unit for information via SNMP using what is called a MIB (Management Information Base). Standard MIB-II queries are supported, as well as a custom RED-LION-RAM.MIB. A great deal of useful information about the unit interface status and more can be queried. When 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.

You may obtain the RED-LION-RAM.MIB by contacting Red Lion support.

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 following dialog window will appear:



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.

Community String for SNMP Agent Access (Required): 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.

Our 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”.

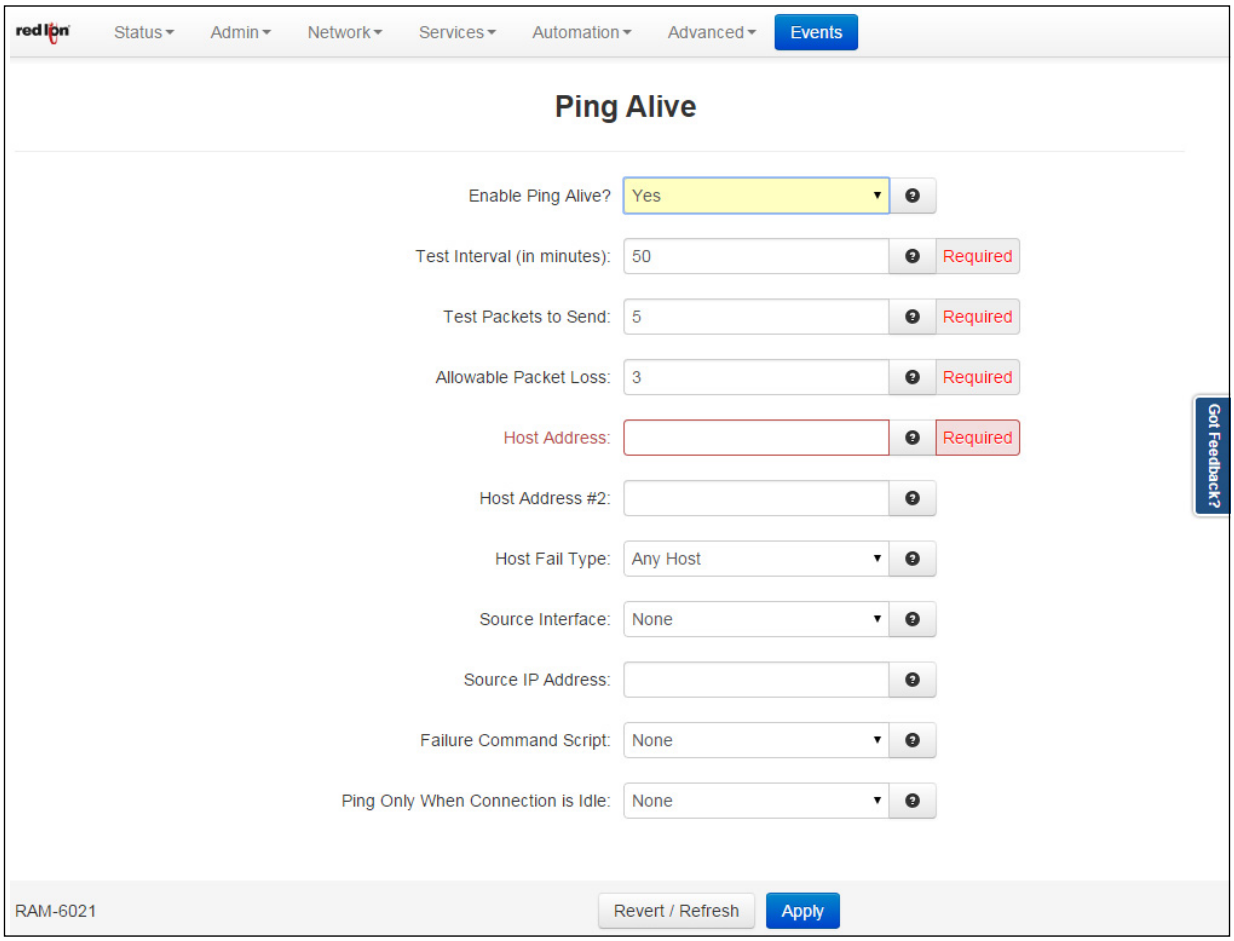
Download MIB: Click on this button to download the MIB file.

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.

2.5.9 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 will appear:



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.

Test Packets to Send (Required): Specify the number the time packets to send out to test connectivity. The minimum is 1 and the maximum is 10.

Allowable Packet Loss (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.

Host Address (Required): Enter the IP Address of the destination host to which the ping packet would be sent. Default setting is “1.0.0.1”.

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.

Host Fail Type: Choose “Any Host” to run the action when the first and last host fail the test. Choose “Last Host” to run the action when the first and lost host fail the test.

Source Interface: Select the name of the interface to which the service will bind for communications tests. 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.

Failure Command Script: Choose the name of the command script to be executed when the PING test fails. for example, if “Reboot” is an option, then when selected, the wired router will be restarted.

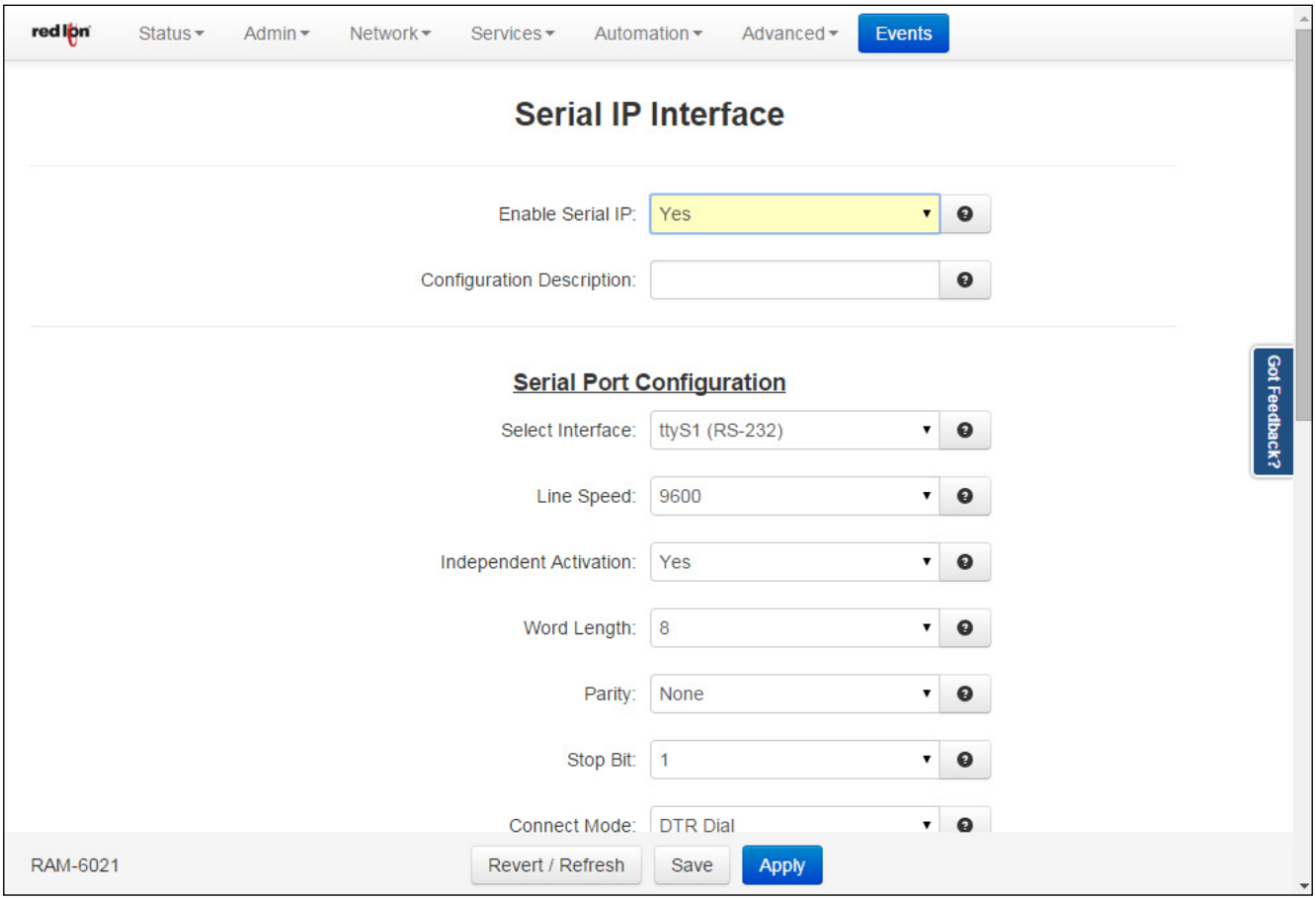
Note: Recommended setting is “None” for standard operation with no special behaviors. Reboot will restart the device.

Click on the APPLY button for the changes to take effect.

2.5.10 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 router and third party UDP or TCP/IP Client/Server application.

Select the Serial IP menu item and the following dialog window will appear:



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 via the provided drop-down

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 needs to be set to Yes in order to use the Inter Character Timeout value configured on this device. The recommended value for this field is *Yes*.

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. The recommended setting for this field is 0, to disable this action. Any other value is upon your environment requirements.

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 for 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 application 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.

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.

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 is 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 5 UDP broadcast addresses.

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 application 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.

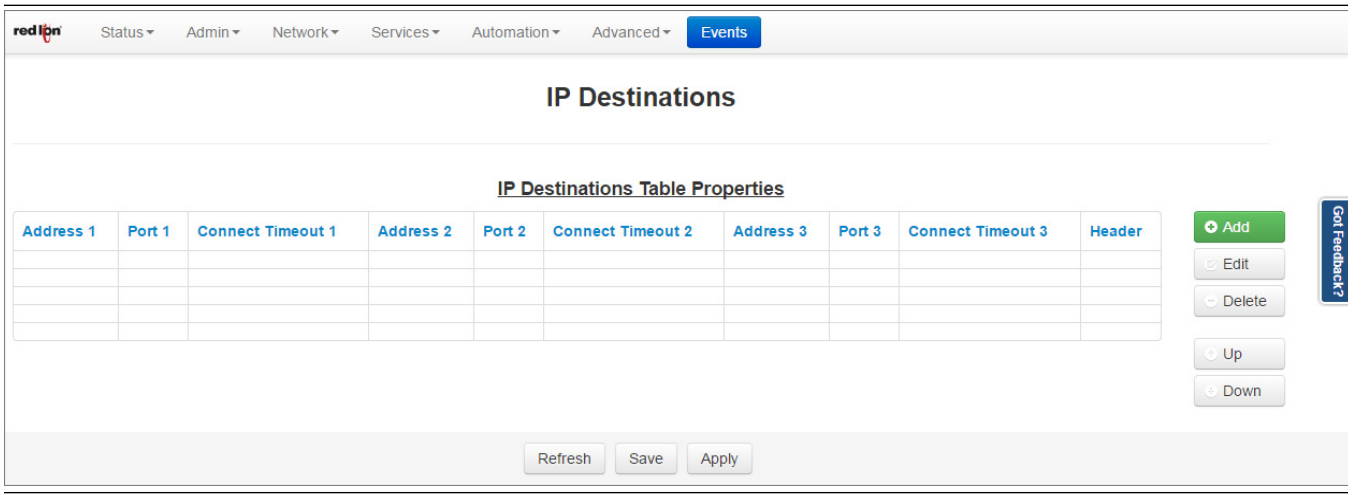
Client IP Port (Required): Enter the client IP port number into this field. This is required if the peer IP Address is set to a specific IP, then packets will be sent to specific IP at this client IP port number only. Consult your network administrator for UDP application destination port number. Set 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.

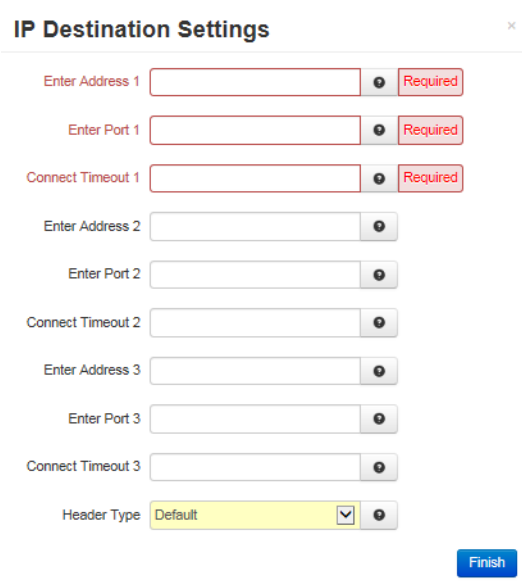
Second/Third/Fourth/Fifth Peer IP Port: Enter the second, third, fourth or fifth port number in the respective fields.

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 10 TCP Client broadcast socket using IP Destination configuration for connectivity.



Click on Add button to define the required IP Destination Settings. The following dialog window will appear:



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.

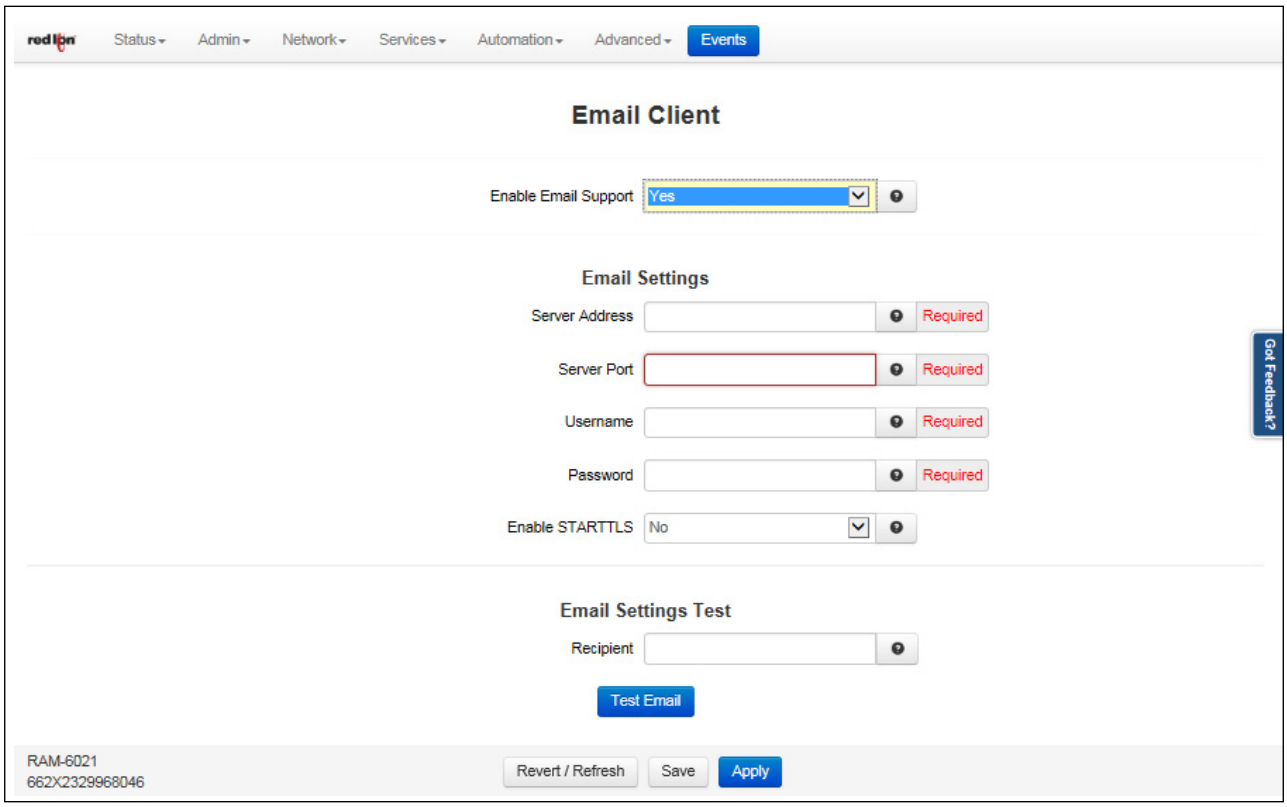
TCP Client Broadcaster Traffic Activator: If this option is selected, the device will support 10 TCP Client broadcast socket using IP Destination configuration for connectivity and would connect only if the serial

data is available to broadcast. See ***TCP Client Broadcaster*** explanation above for a description of available options.

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.

2.5.11 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.

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.

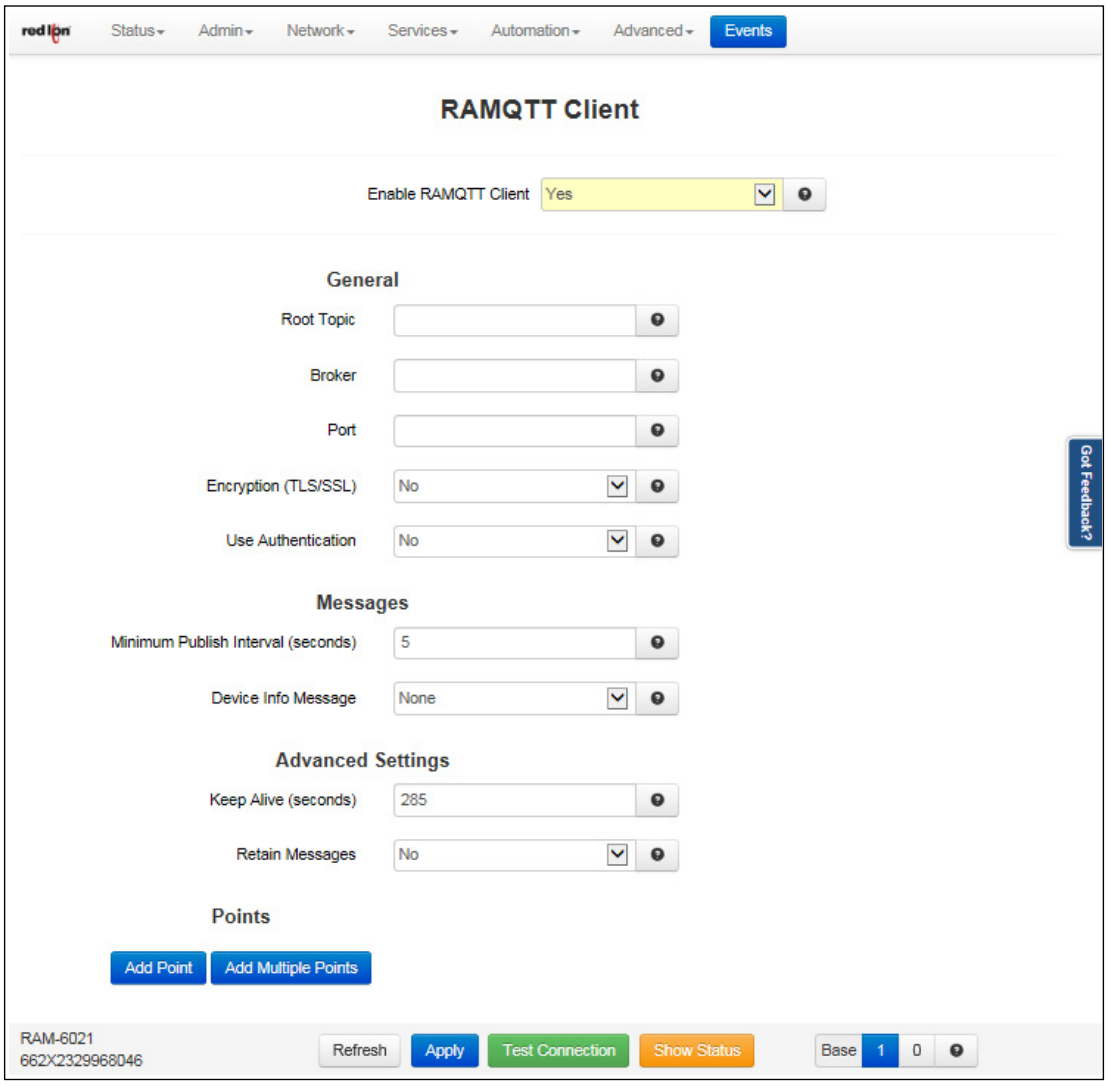
Note: The email will come from the address configured in *Sender* field or *Username* field if the Sender field is blank. Examples; username@email.com or username@email.com,usergroup@email.com

Test Email: Click on this button to execute the Email Settings Test.

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.

2.5.12 RAMQTT Client

Specify whether to enable the RAMQTT client support on this device.



Enable RAMQTT Client: Select **Yes** to enable the RAMQTT Client.

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.

Port: Enter the port number associated with the Broker IP address or Domain Name.

The standard ports for MQTT are:

- Unencrypted: 1883
- Encrypted: 8883

Encryption (TLS/SSL): Select whether the connection will be encrypted.

Use Authentication: Select whether authentication will be used.

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.

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:

- None: Sends no message
- 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 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 IP’s
  - 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 FTFROMCP
- GPS Speed

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)
  Fussion Connect: Less than 5 Minutes (285 seconds)

Retain Messages: When the device publishes a message with the retain option selected as **Yes**, all new subscribers to the topic will receive this message immediately. This allows new subscribers to get information about the device without having to wait until the next publish interval.

Points: Add 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, Apply, Test Connection, Show Status: Use these buttons to refresh the screen, 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>.

2.6 Automation Tab

The Automation menu contains all aspects of managing your Modbus and DNP3 based I/O.

If prompted for an Unlock Key, contact Red Lion Support at support@redlion.net or 1-877-432-9908.

The RAM-6021 MODBUS service allows it to function as a MODBUS Master acting 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-6021 acting as a MODBUS/DNP3 master. I/O data is stored in a local I/O database and can be polled by other remote I/O collection points.

The RAM-6021 wired router 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-6021 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.

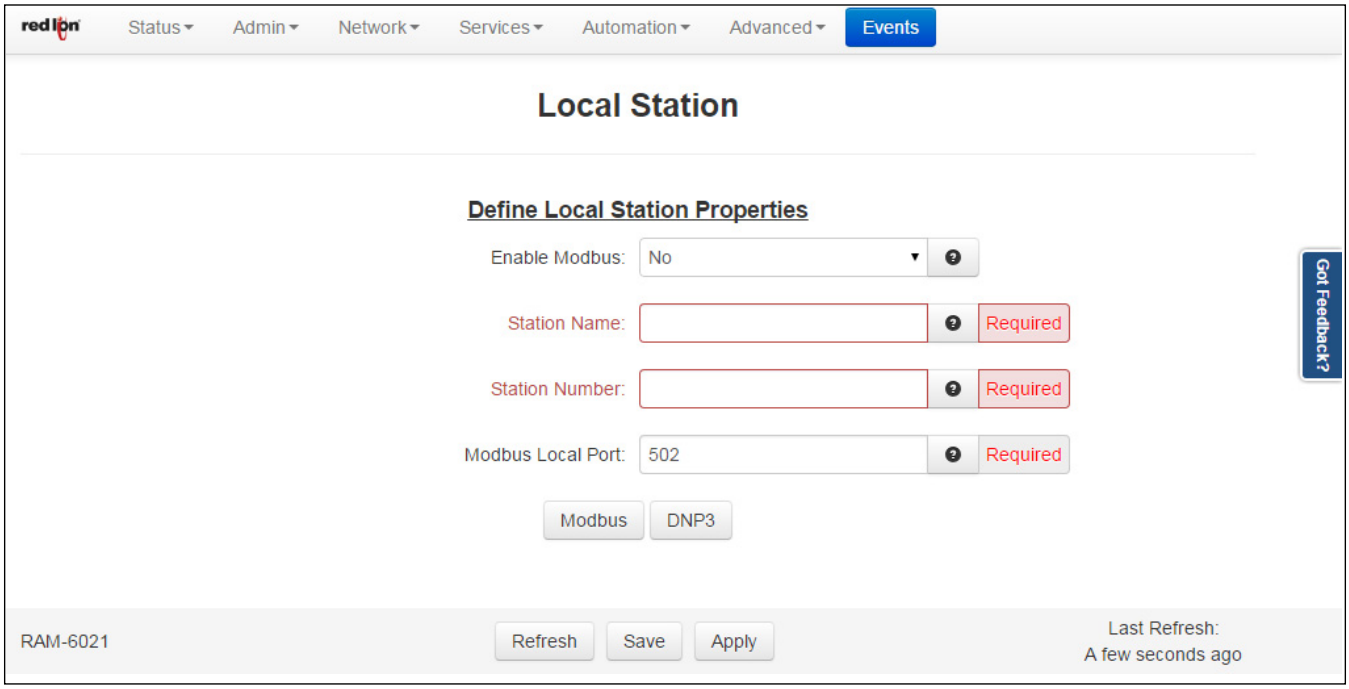
- **CLI:** The command line interface for the device provides a Cisco-style telnet command line interface. It writes an XML configuration file, which is used to drive the backend daemons.
- **Web UI:** This method is a WEB based interface which is the focus of this documentation.

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

2.6.1 Local Station

Click on the *Local Station* sub menu item and the following menu will appear:



Enable Modbus: Select *Yes* to enable the Modbus feature. Selecting *No* will disable it.

Station Name (Required): Enter the name of the local station. The station name must be less than or equal to 32 characters.

Station Number (Required): MODBUS station number to use for the local station. Values may be duplicated for other stations as long as the station can be uniquely addressed by an IP address or is connected on a serial port. Valid values: 1 - 247. **Note:** 0 is a broadcast address. 248-255 are reserved addresses.

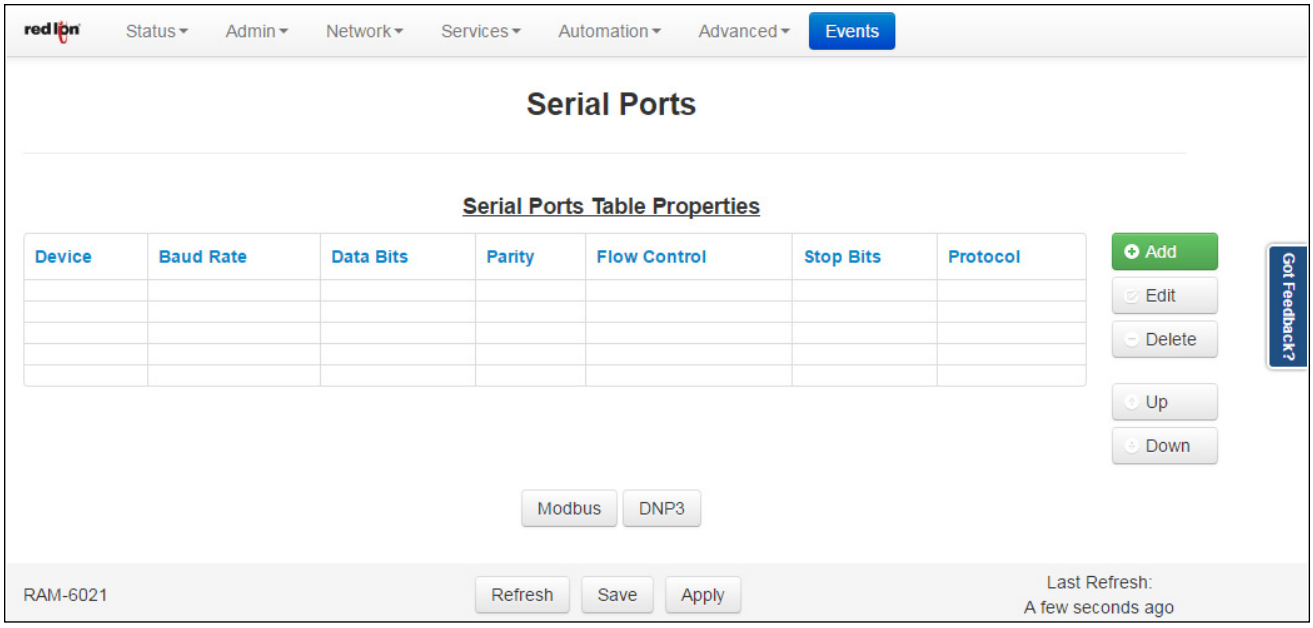
Modbus Local Port (Required): Enter a valid local port number. The port must be within the range of 1 - 65535 and the recommended default port is set to 502. Choose a port number not already used by other system services. Consult *Status->Network->Socket Statuses->TCP* Only for a list of ports currently in use. Please not that a Firewall Allow rule will need to be added for remote access (*Network->Firewall->Port Allow/ Forwarding Rules->Service Access Rules*).

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. To revert to the previous defaults, click on the Revert button.

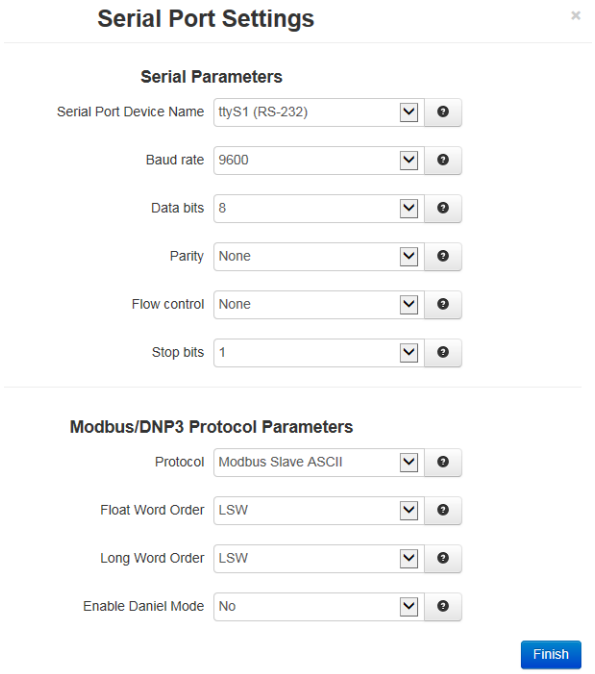
2.6.2 Serial Ports

This section is used to configure the RS-232 port that is facing the front of the Red Lion device to integrate into your Modbus/DNP3 schema.

Click on the *Serial Port* menu item and the following window will appear:



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



Serial Port Device Name: Name of the serial device. Valid values: ttys1 (RS232), ttys4

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 an address, 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.

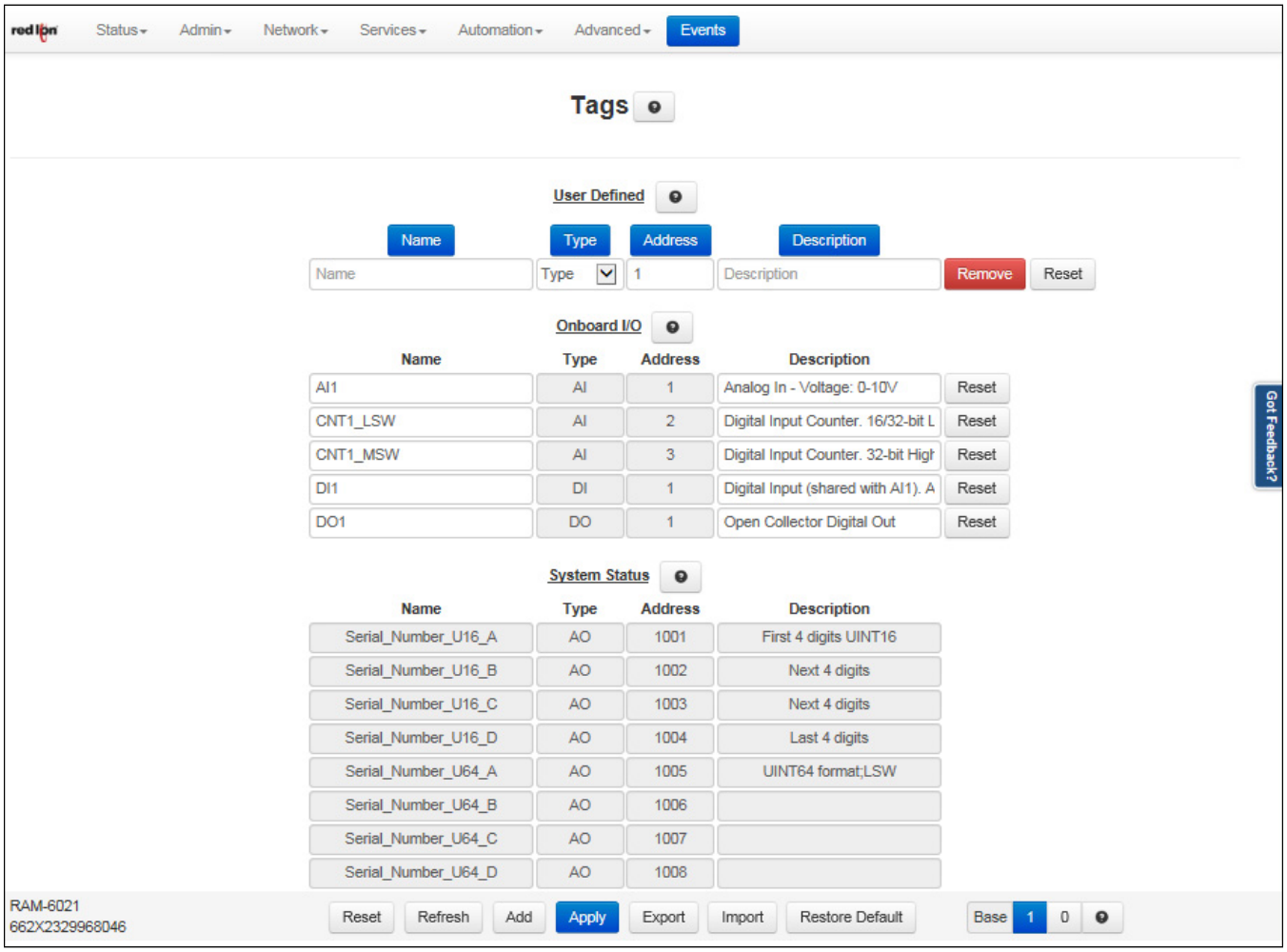
2.6.3 Tags

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.

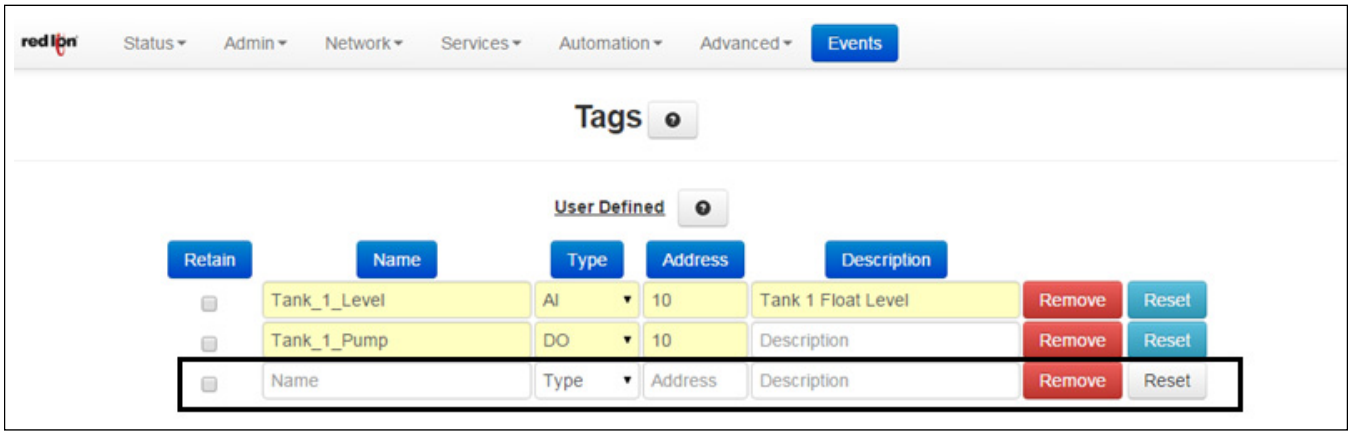
Each register label consists of the Tag name, followed by the address in two parts: type and address. Type and address will change to match the Zero (Native) and One (Modbus) formatting conventions. An untagged register will show an implied tag in <angle brackets>.



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 will appear.



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.

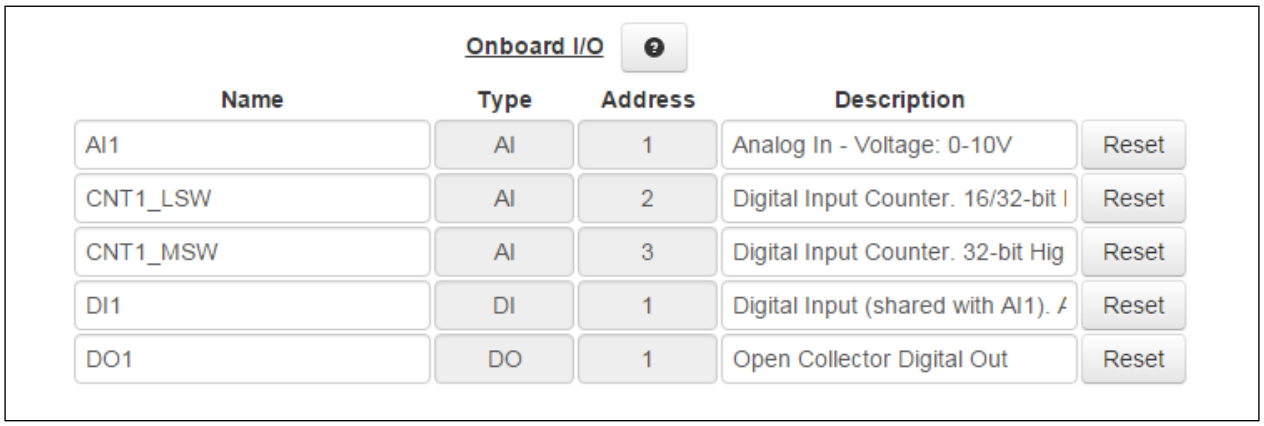
Address: Enter the desired tag address. There are 65536 registers of each data type available.

Description: Enter a description of what the tag represents.

Retain: Checking this box will allow 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 Series.**

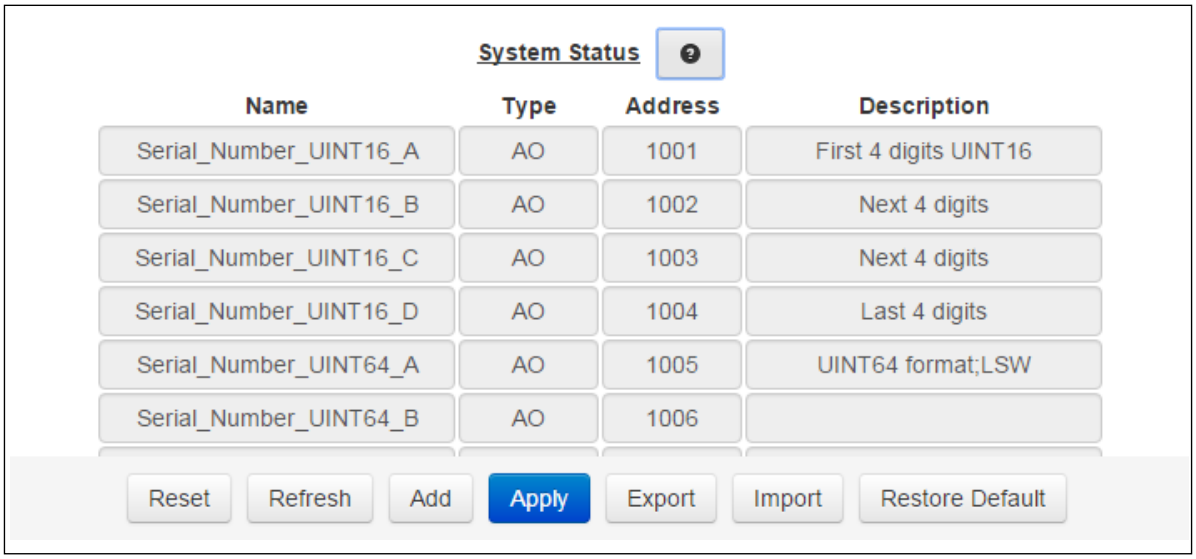
Onboard I/O

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.

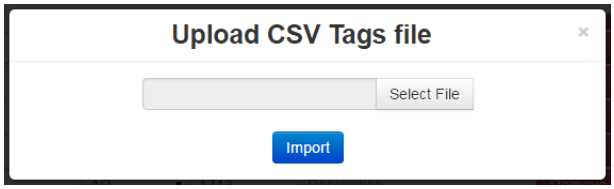


Click on the *Refresh* button to refresh screen after new entries have been entered.

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 will appear.

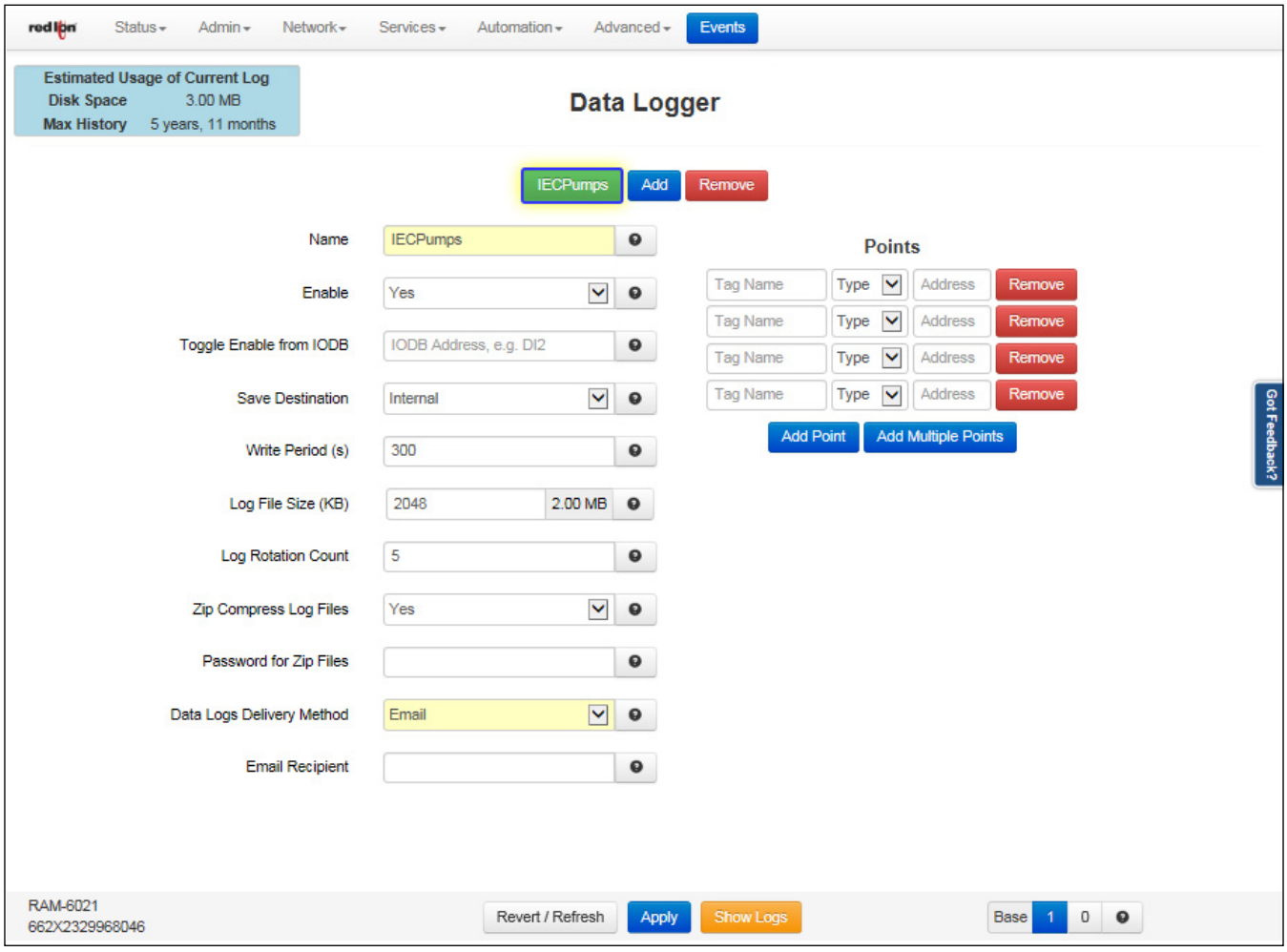


Click on the *Select File* button and browse to the location where the *.csv* file is located, then press the *Import* button.

To restore the system default Tags, click on the *Restore Defaults* button. All user defined tags will be removed from the list.

2.6.4 Data Logger

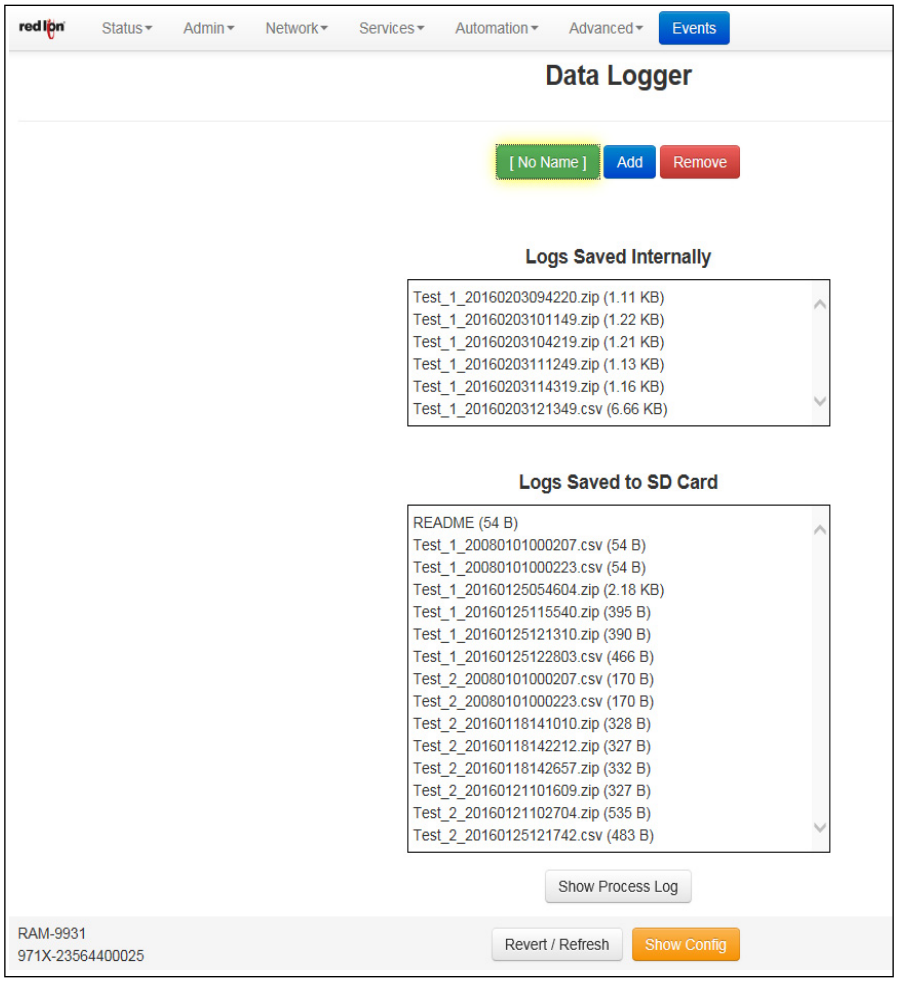
Click on the *Automation* menu item, select Data Logger from the drop-down menu and the following Data Logger configuration screen will appear:



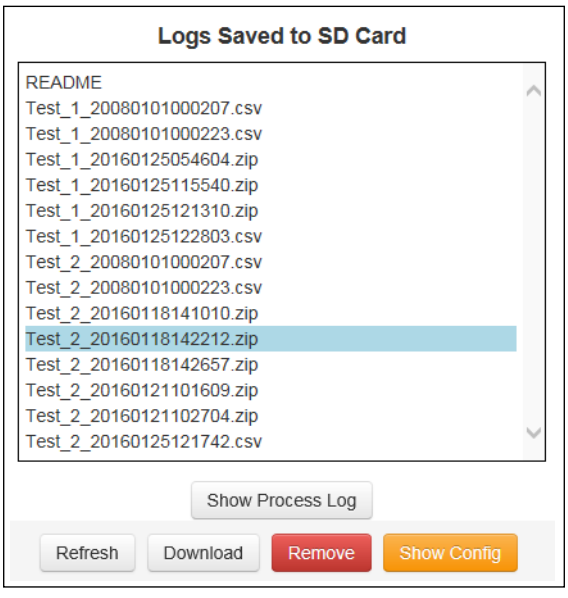
Data Logger allows for the collection of data from defined points and save them as a log file to an internal destination or to an SD card. The Data Logger feature is available on all models using release 3.23 / 4.23 and newer.

Navigation

Click on the green named log file button to display the data logs associated with the displayed log file name (IECPumps in this example).



Click on any to select the log file to Download, View, Remove or show the Process log associated with the log file. You can also shift/click to select multiple log files to Download or Remove.



Click on the *Show Config* button to return to the Data Logger configuration screen.

Click on the *Add* button to create a new file and configure the data log file parameters.

Click on the *Remove* button to delete a log file.

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/

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: Paired with the write period, this will control what conditions create a data log record.

Options:

Write a record every period: If the Write Period is 30 seconds, this will create a new data log record every 30 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 (30 seconds in this example)

Write only if data has changed: The IODB list is sampled every Write Period (30 seconds in this example), and a data record is created only if the data has changed from the last time it was sampled. If data values are mostly stable, this can save a lot of space to not record redundant information.

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

Points: Configure fields to create data points

Tag Name: Enter the name

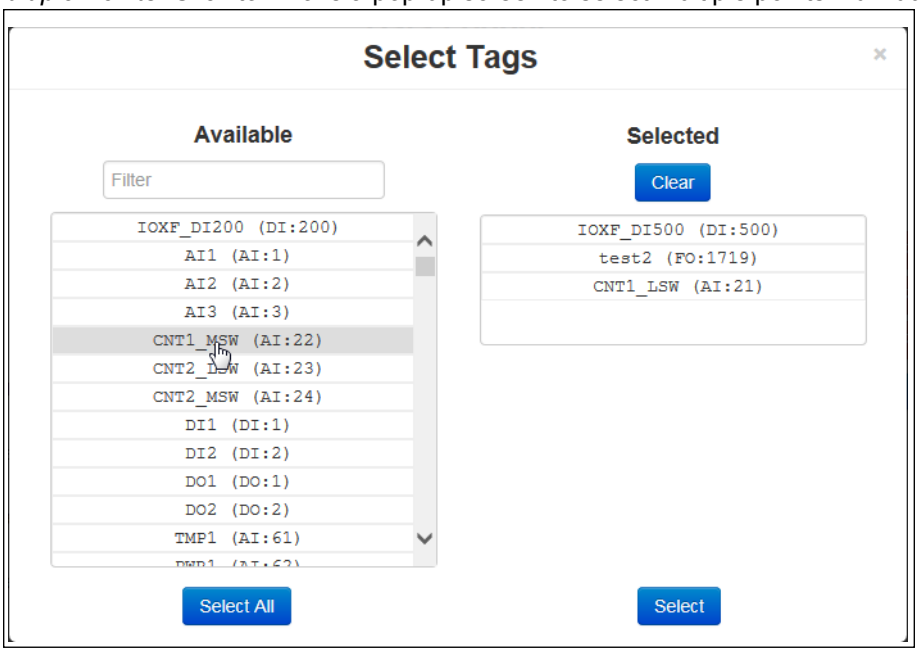
Type: Select from the drop-down menu options

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.



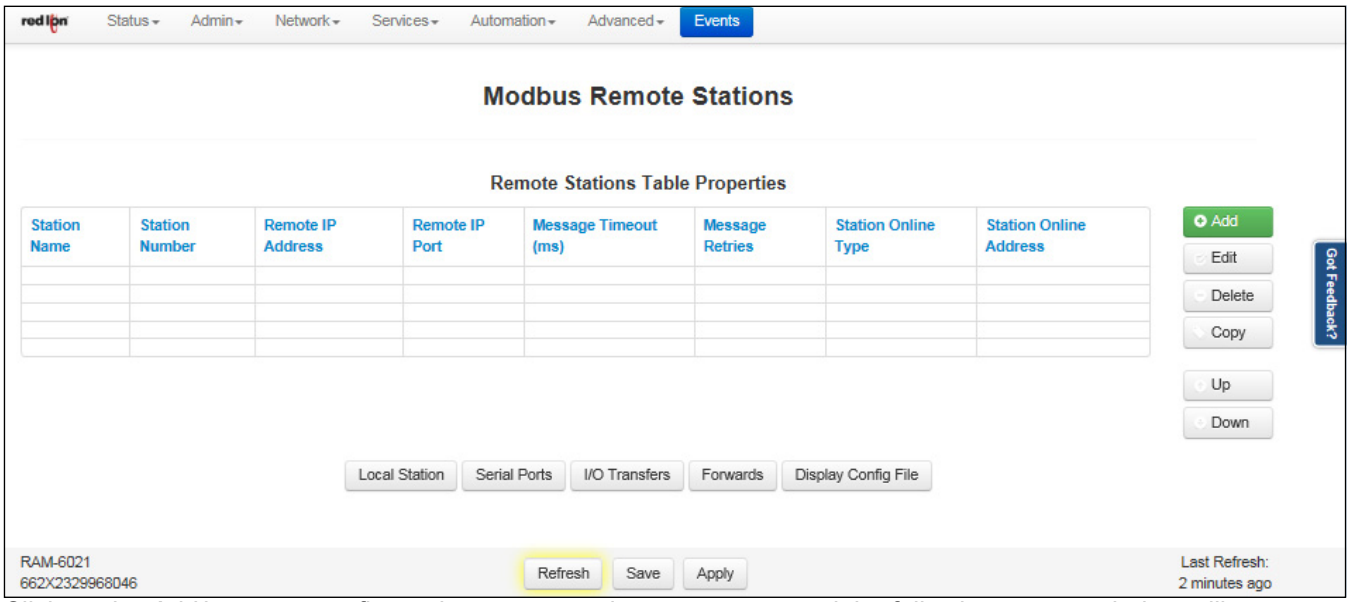
Selected Tags move from Available Selected list. Click *Select* button when finished making selections.

Click the *Apply* button to save and apply the new data log configuration.

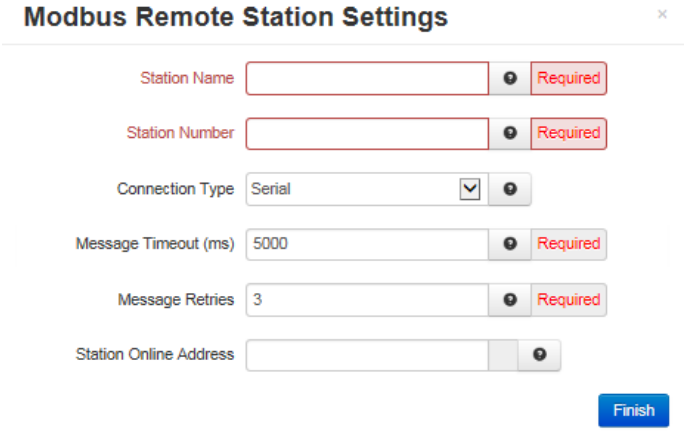
2.6.5 Modbus

2.6.5.1 Remote Stations

Click on the *Remote Stations* menu item and the following dialog window will appear:



Click on the *Add* button to configure the remote station parameters and the following pop-up window will appear:



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 stations 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 desired connection type in the drop down menu. The options are: IP or Serial.

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.

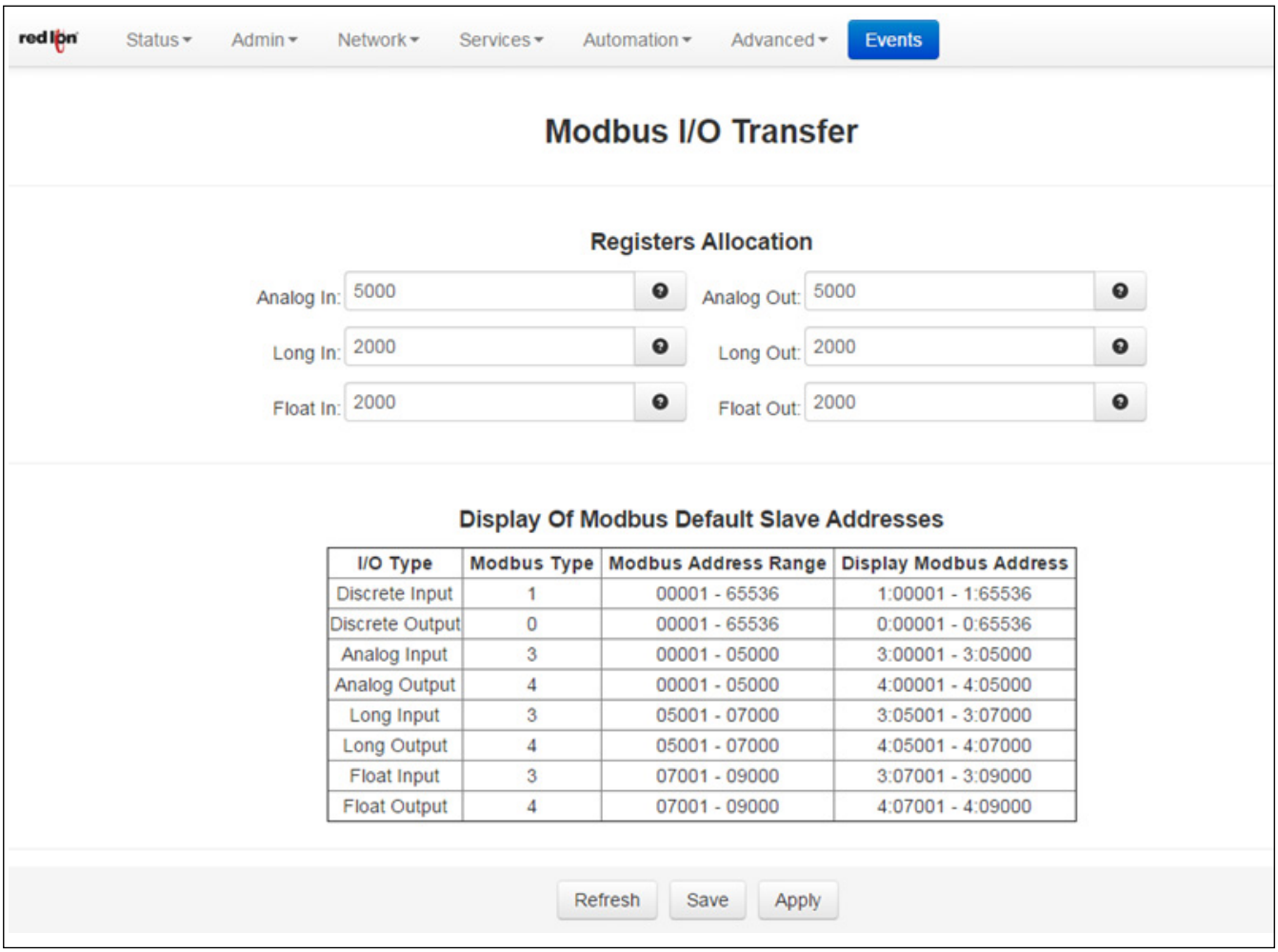
Station Online Address: Discrete input address is used as a station status indicator. If provided, it is set to True when any I/O transfers to a remote station complete successfully, and false otherwise. Enter the Address of a local discrete input or blank if not used.Click on the Finish button to populate 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 will appear:



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 - 65535.

Analog Out: By default we support 5000 Analog Output registers, but the range is 1 - 65535.

Long In: By default we support 2000 Long Input registers, but the range is 1 - 65535.

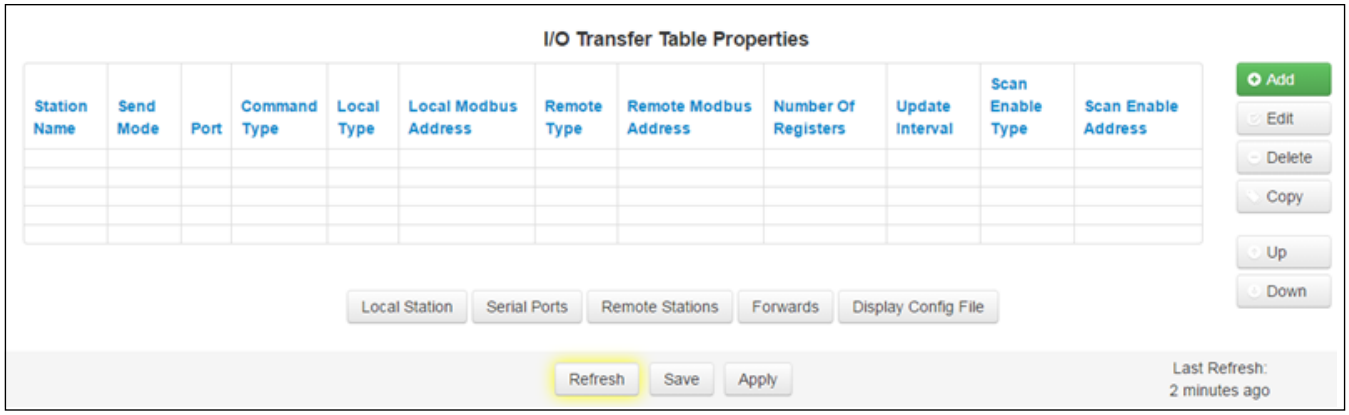
Long Out: By default we support 2000 Long Output registers, but the range is 1 - 65535.

Float In: By default we support 2000 Float Input registers, but the range is 1 - 65535.

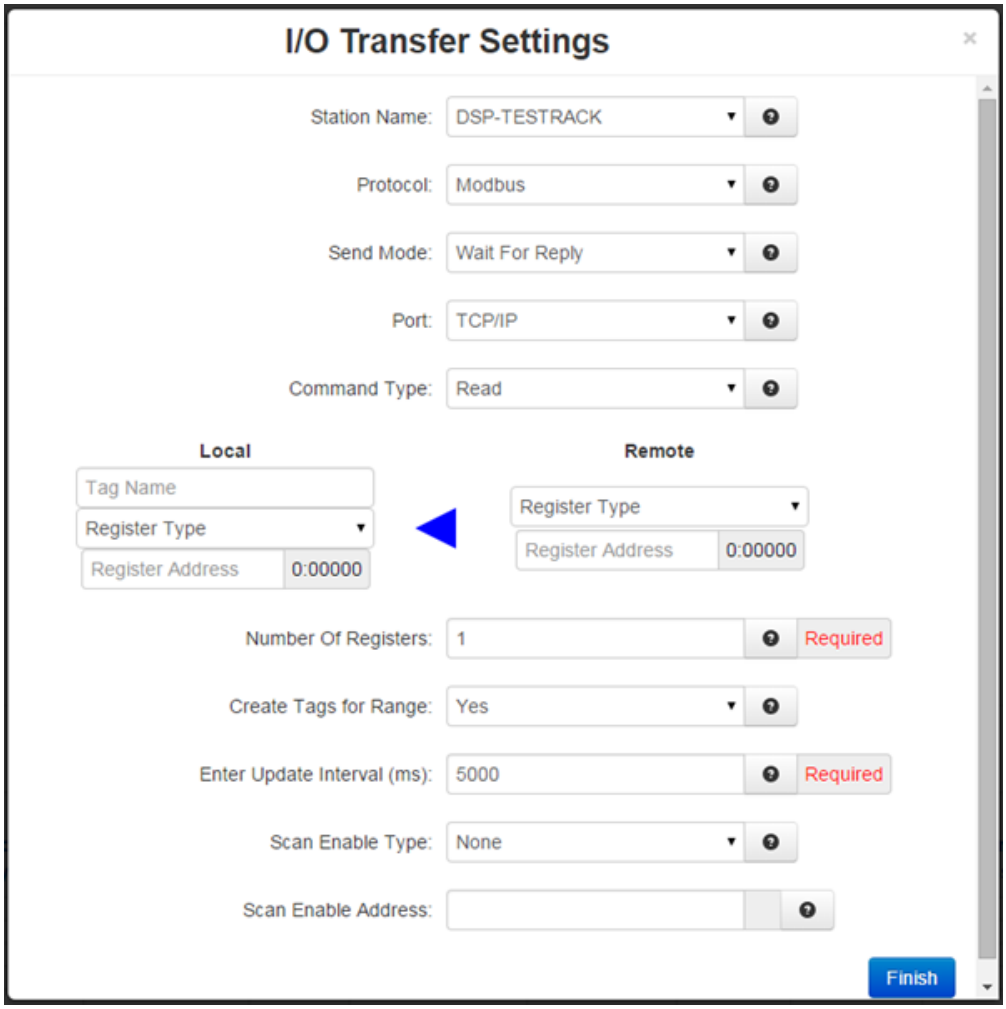
Float Out: By default we support 2000 Float Output registers, but the range is 1 - 65535.

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 *I/O Transfer Settings* pop-up window will appear:



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: Modbus is currently the only supported protocol used for I/O transfers.

Send Mode: Mode used to send an I/O transfer.

> **Wait for Reply:** The MODBUS master must wait for an I/O request that it has sent to complete before sending another request to the remote station.
>
> **Rapid Fire:** 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 TCP/IP, UDP/IP, ttys1 (RS232) and ttys5 (RS485). If UDP/IP or TCP/IP port are used, 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: Write MODBUS output registers to the remote stations.

WRITE_SINGLE: Write a single MODBUS discrete or analog output register to the remote station.
Note*:* Only an option when writing a singe discrete output or single analog output.

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: 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): 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.

Click on the *Finish* button to populate the IO 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.

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

I/O Type		Number of regs supported in I/O transfer
Long Output	LO	62

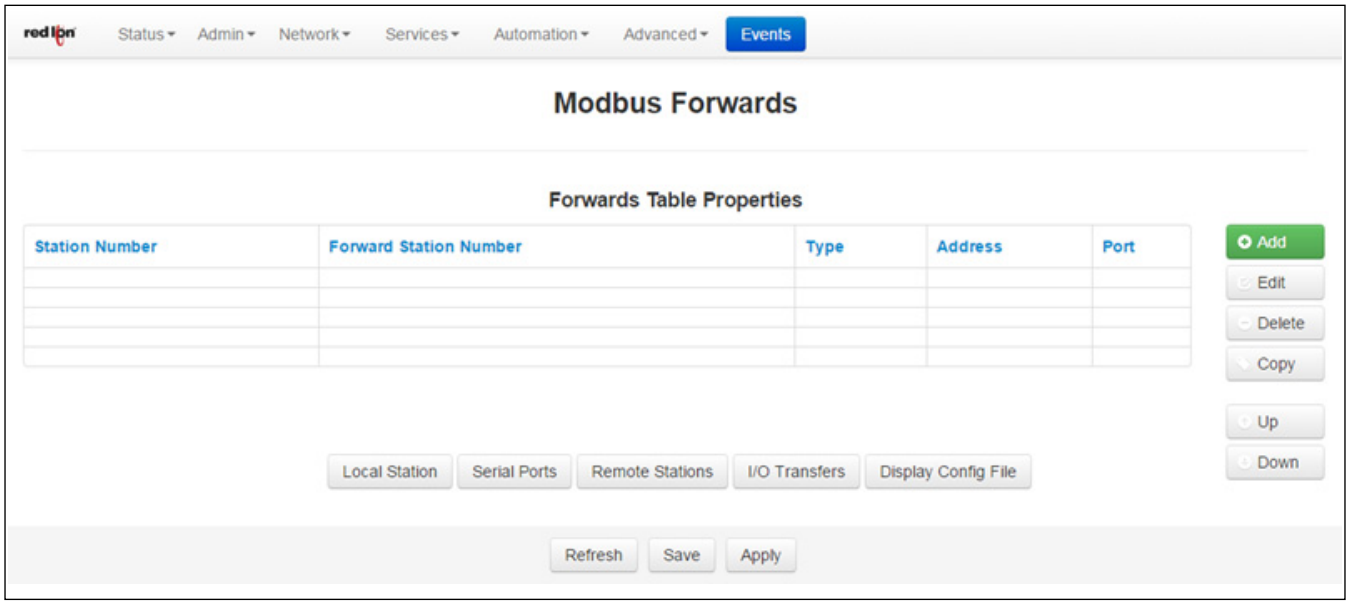
I/O Type		Number of regs supported in I/O transfer
Discrete Input	DI	1968
Discrete Output	DO	1968
Analog Input	AI	123
Analog Output	AO	123
Float Input	FI	61
Float Output	FO	61
Long Input	LI	61
Long Output	LO	61

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

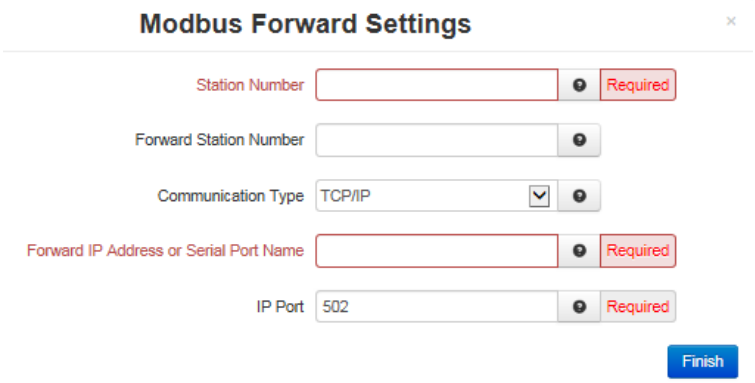
Local Type	Valid Remote Type
DI	DO
DO	DO
AI	AO
AO	AO
FI	FO
FI	FO
LI	LO
LO	LO

Forwards

Click on the *Forwarding* menu item and the Modbus Forwards dialog window will appear:



Click on the *Add* button to configure the Forwarding and the *Modbus Forward Settings* pop-up window will appear:



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: 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.

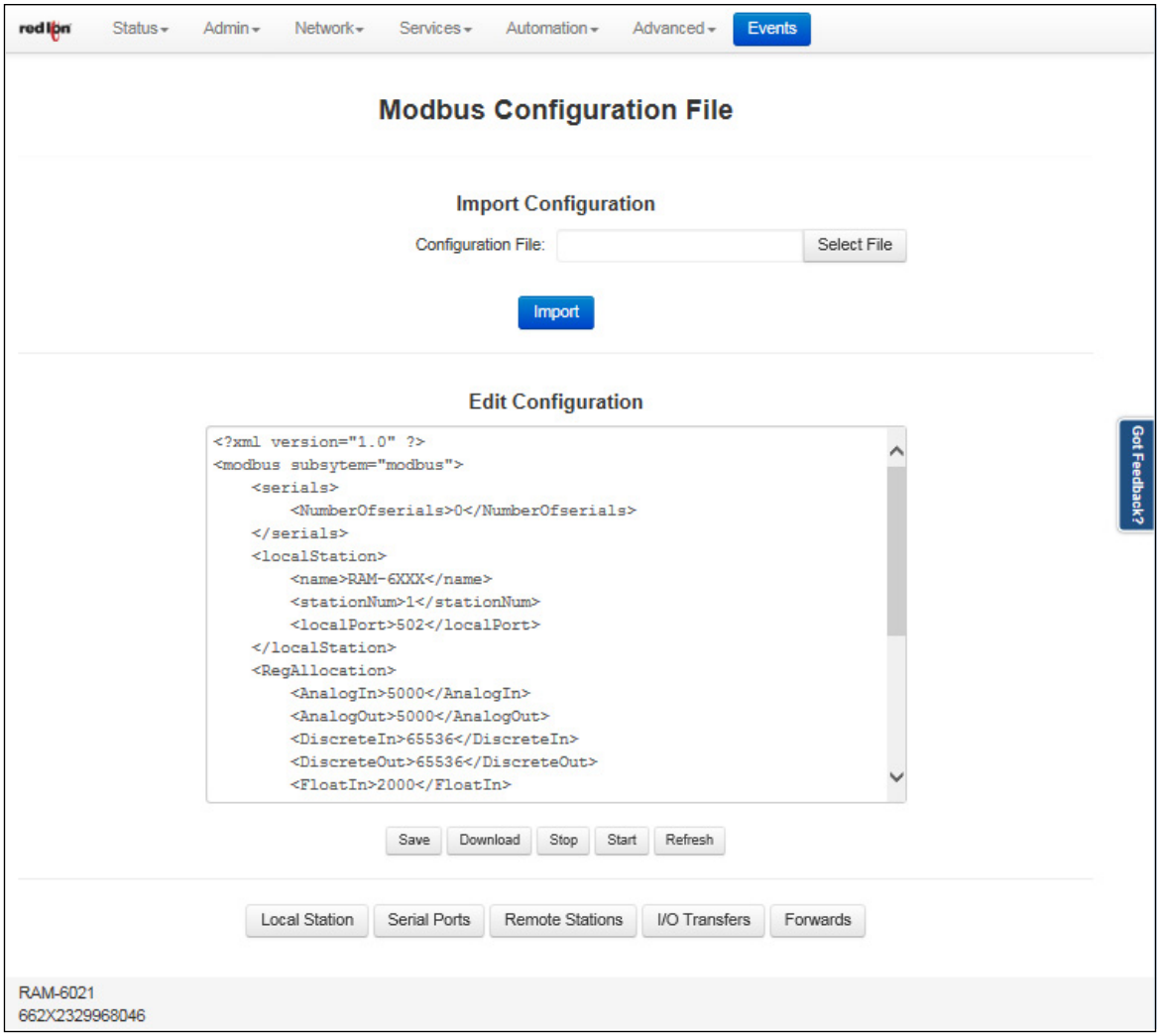
IP Port: Enter a valid port number (1-65535) to be used to forward the request to on the remote station. It is recommended that a port number not already used by other system services is chosen. Consult **Status-> Network->Socket Statuses->TCP Only** for a list of ports currently in use. Please note 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 window will appear:



Configuration File: This option will allow you to import a configuration file to replace your existing Modbus configuration file. Click on "Select File" button 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 following controls (buttons) are available:

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.

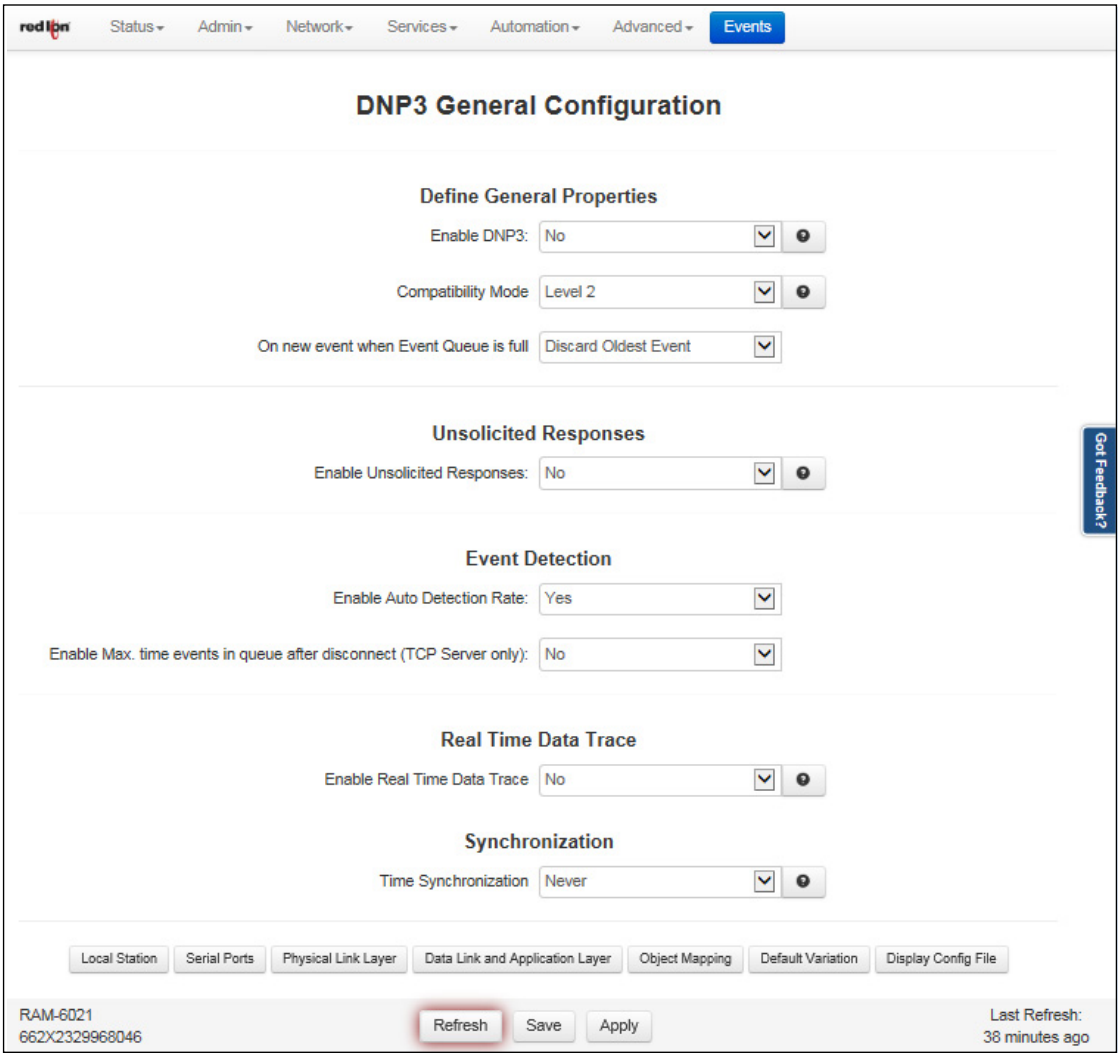
Download - Download the current Modbus configuration file to your PC as **"**modbus.xml.txt**"**.

2.6.6 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

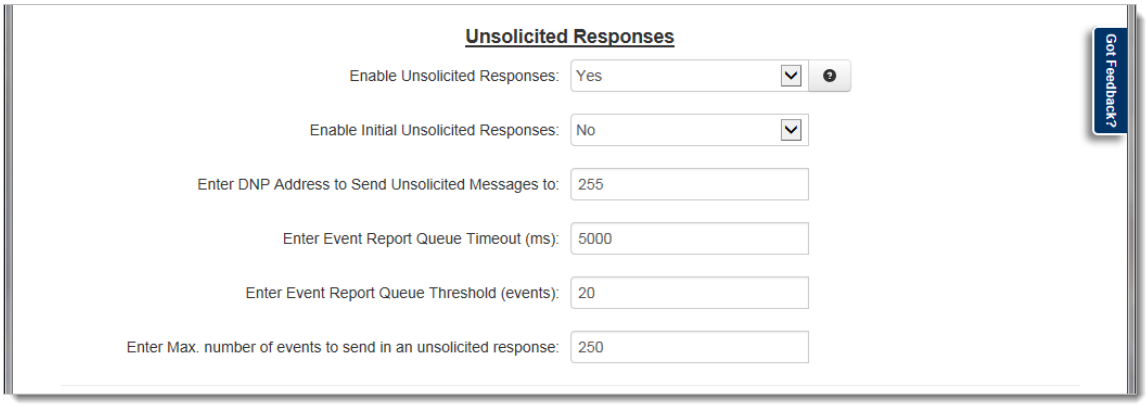
Click on the *General* menu option and the DNP3 General Configuration screen will appear:



Compatibility Mode: The DNP3 Slave driver can work under 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.

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:



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.

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).

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.

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.

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.

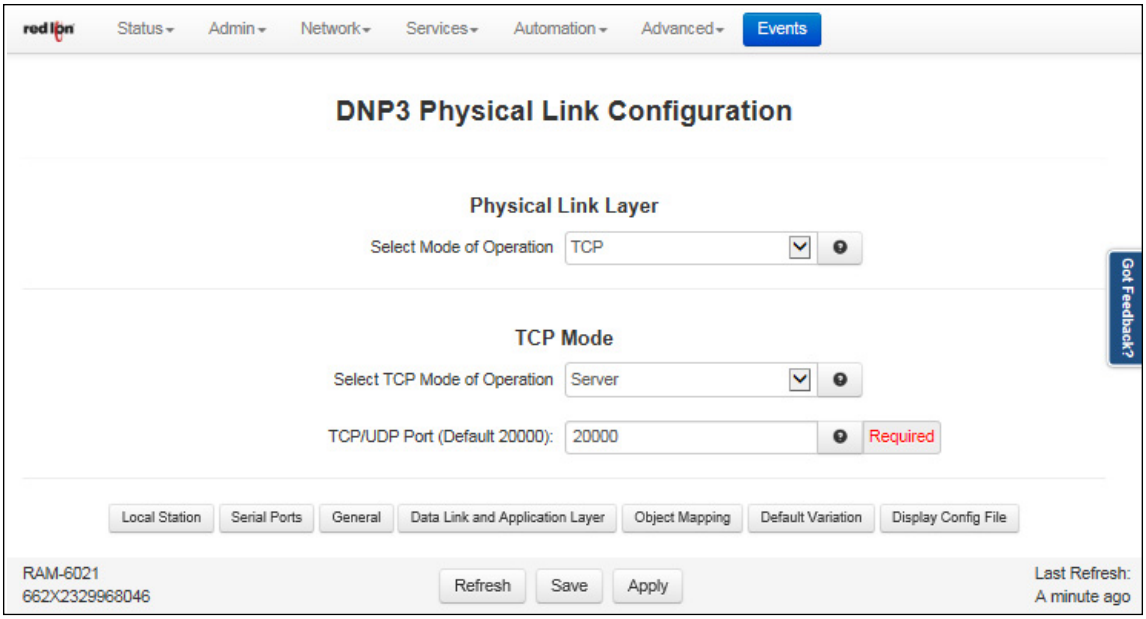
Enable Real Time Data Trace: The DNP3 Slave Driver can be configured to generate real time traces of every Master-Slave DNP3 transaction for diagnosis and debugging purposes. The real time communication data traces can be enabled/disabled at any time from the DNP3 configuration Add-On and its ASCII output can be redirected either to a text file within the file system for later upload, to a dumb terminal attached to an unassigned serial port of the station, or even to a remote Telnet terminal session over the TCP/IP network by entering the corresponding /dev/ttyp (/dev/ttyp0 to /dev/ttyp3) telnet device.

Time Synchronization: The station can be configured to request Time Synchronization from the DNP3 V3.00 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 RS232 and RS485 (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 will 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.

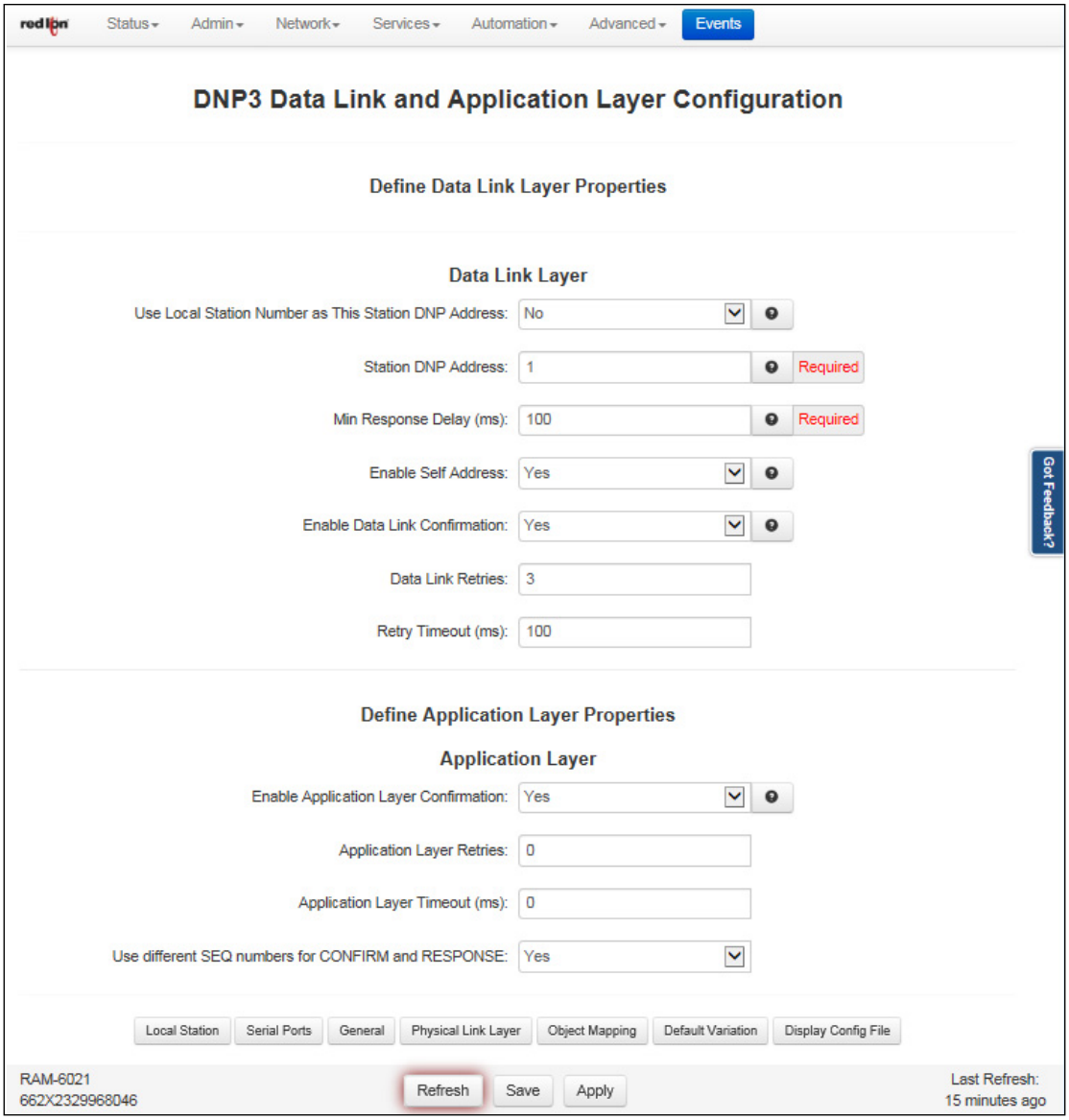
UDP: This section is enabled when the Mode of Operation is set to UDP. The parameters to be configured are:

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.

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.

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.

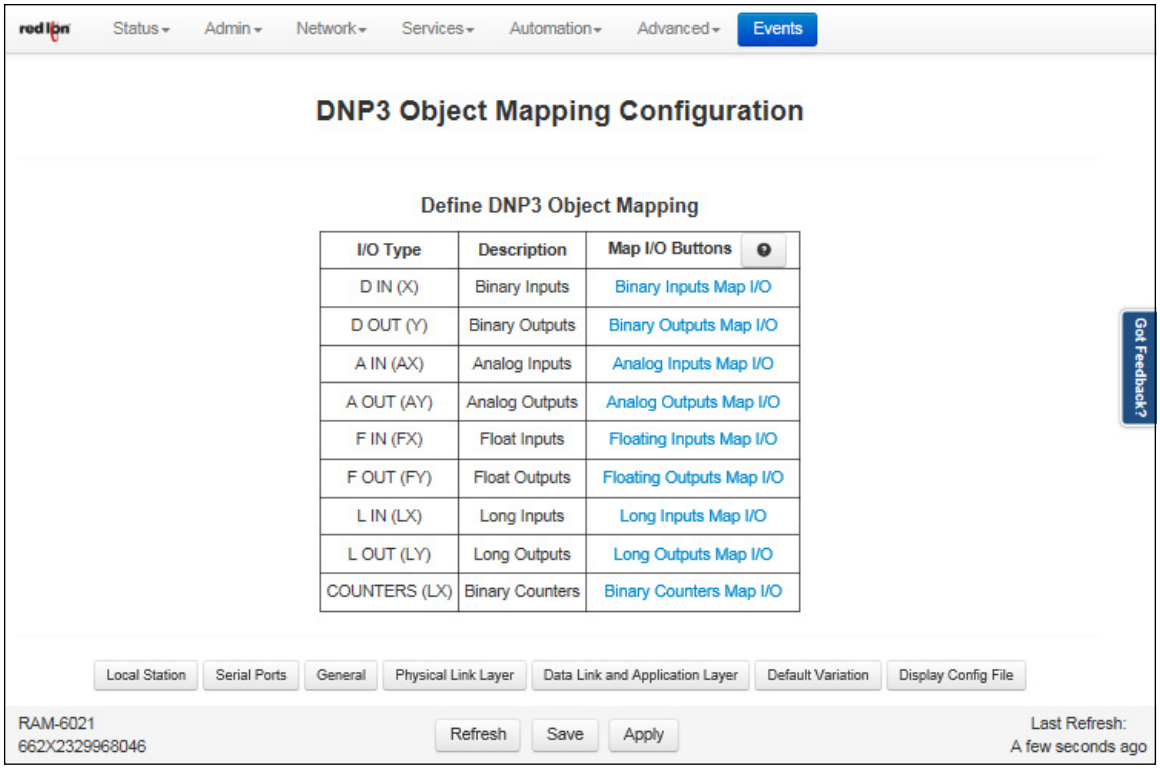
Application Layer Retries: The number of Retries is configurable between 0 (Application Link Retries disabled) and 255.

Application Layer Timeouts (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

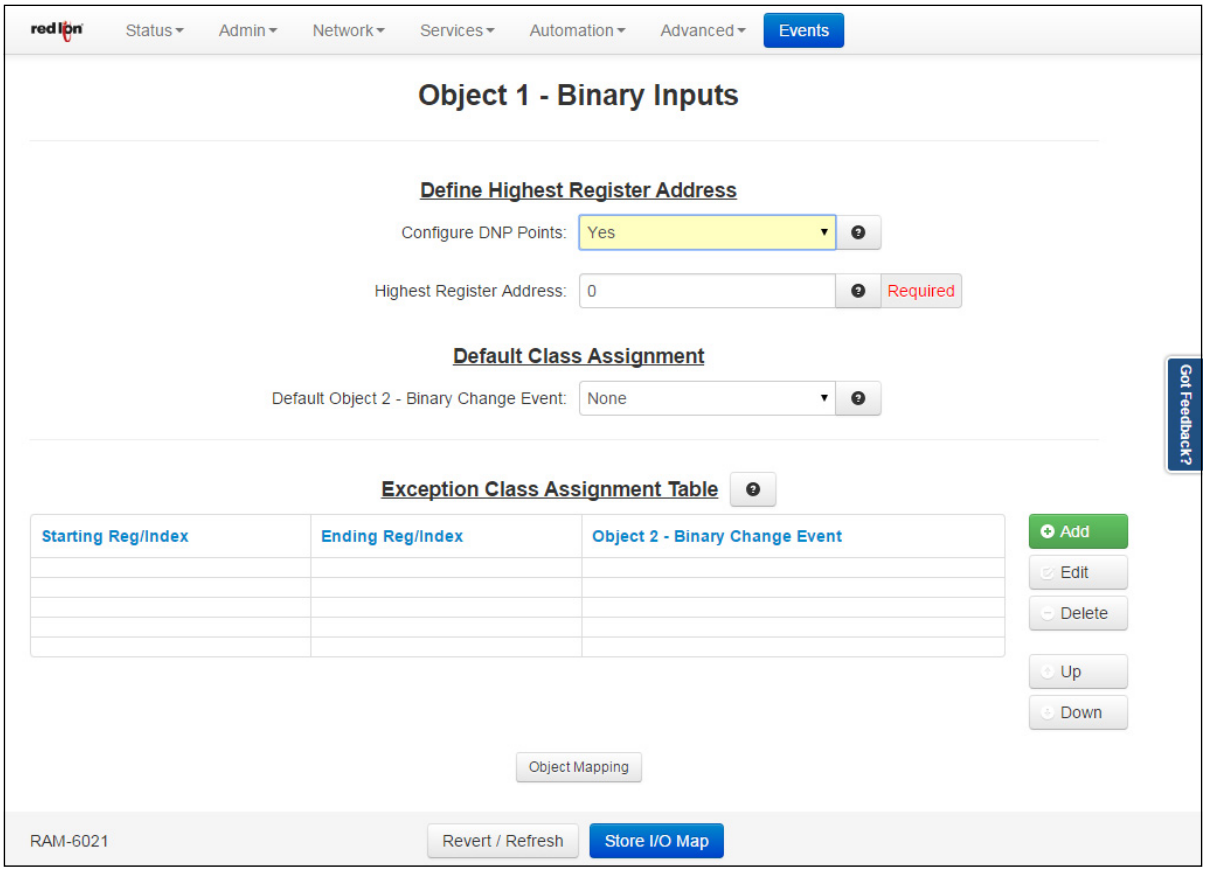


Object Mapping: When clicking on each link a dialog window appears. The dialog window is used to configure and map every DNP3 point to a specific I/O. ***Note:*** *Each type of I/O must have its corresponding Object Mapping Window opened at least once, or else the I/O won't be mapped.*

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 shown 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.

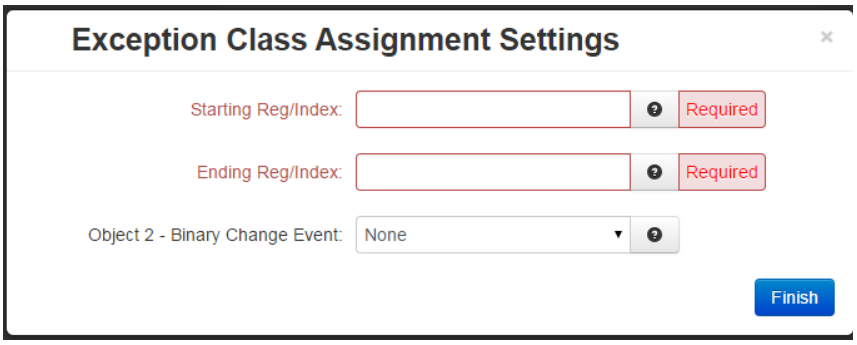
Exception Class Assignment Table: The Exception table provides you with the ability to define Reg/Index ranges that are needed to be configured differently than Default Class Assignments.

> **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.

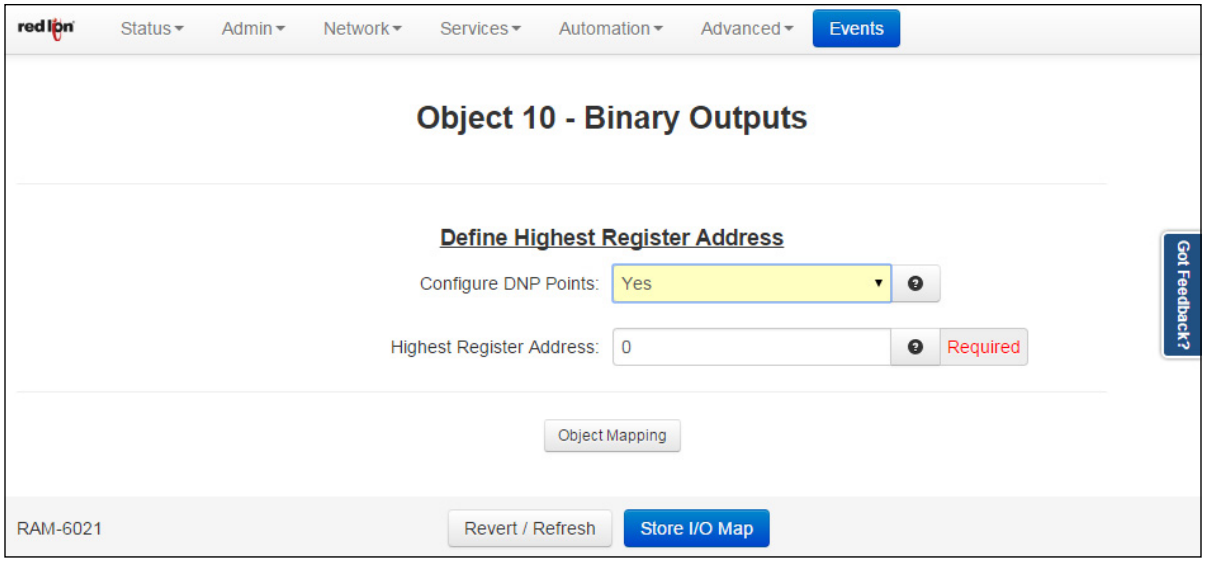
Object 2 - Binary Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should 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.

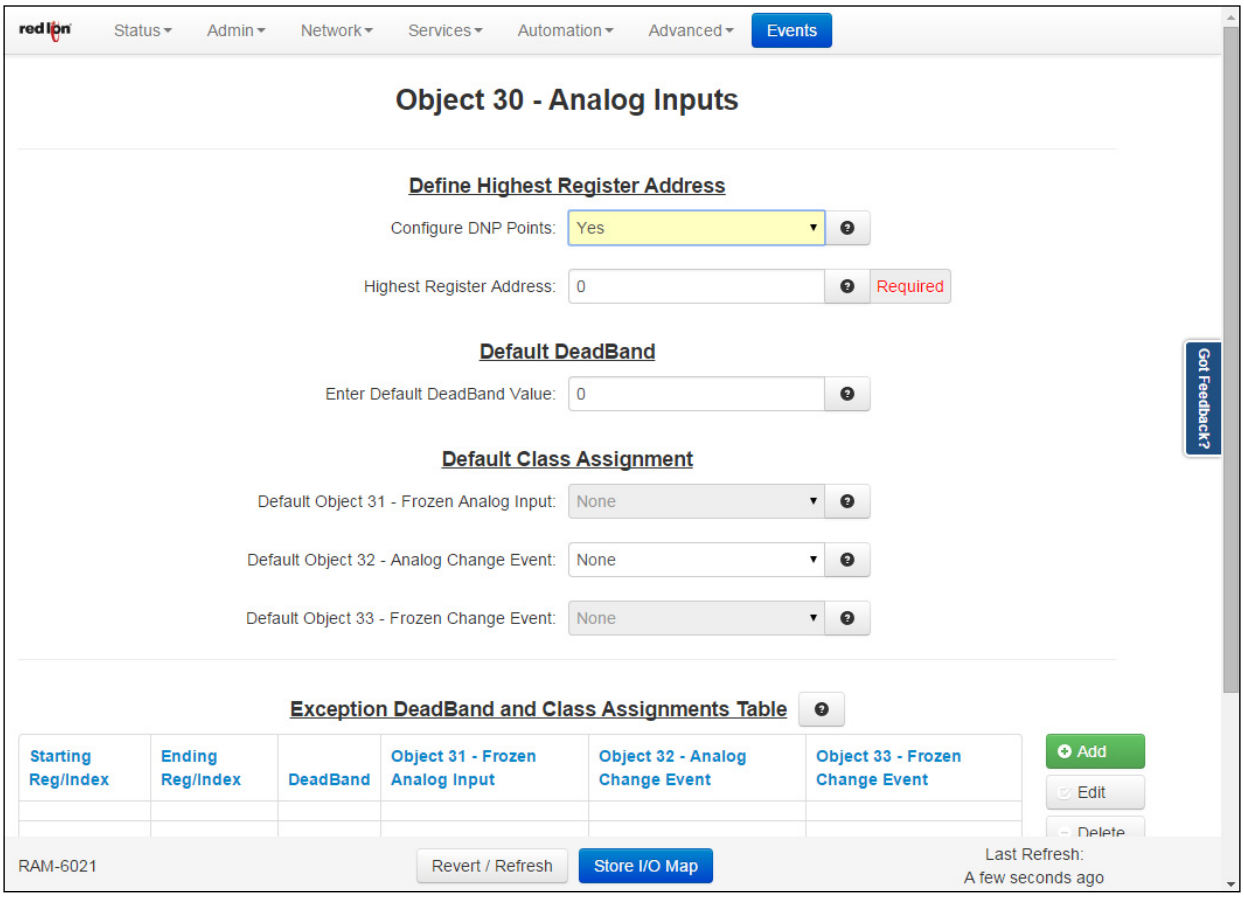
Highest Register Address (Required): This field is used to show or set the highest register address to map DNP3 points. If Configure DNP3 Points option is set to Yes, the Highest Register Address field is shown to enter a Highest Register Address value.

Click on *Store I/O Map* 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.



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.

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 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.

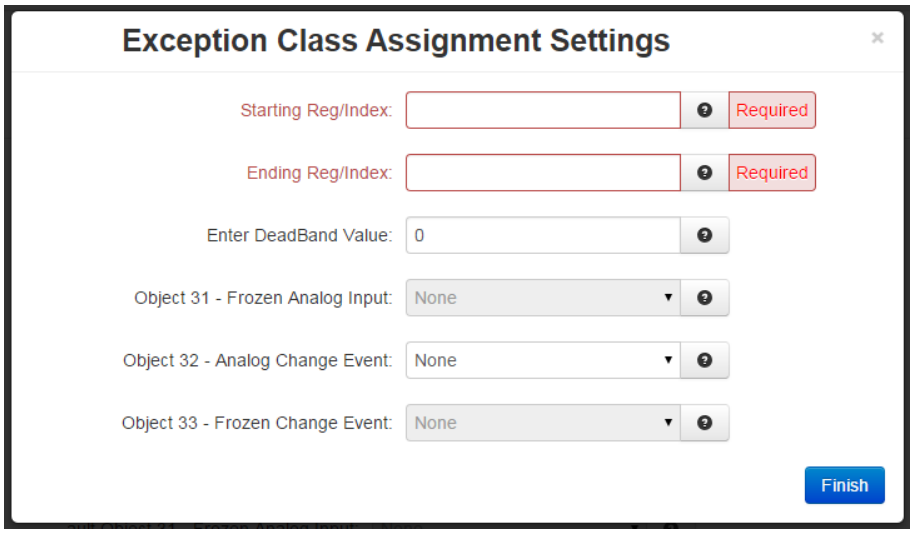
Exception DeadBand and Class Assignments Table: The Exception table provides the ability to define Reg/Index ranges that are needed to be configured differently than Default DeadBand and Class Assignments.

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 *Exception Class Assignments Settings* dialog window will appear:



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.

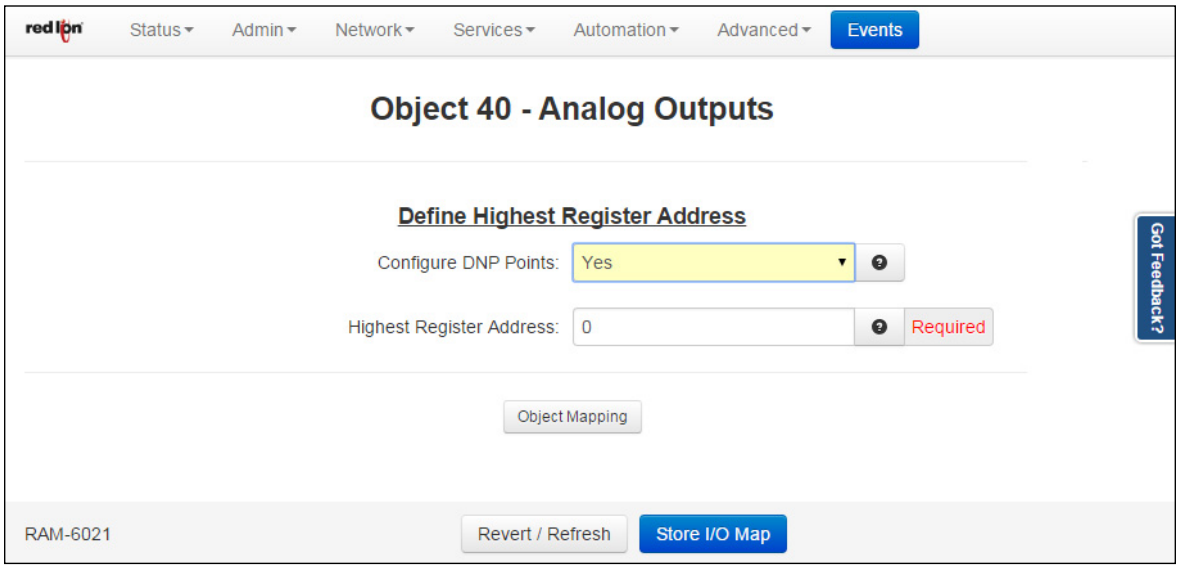
Object 33 - Frozen Change Event: This field is activated on both levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should 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 Map* 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 activated.

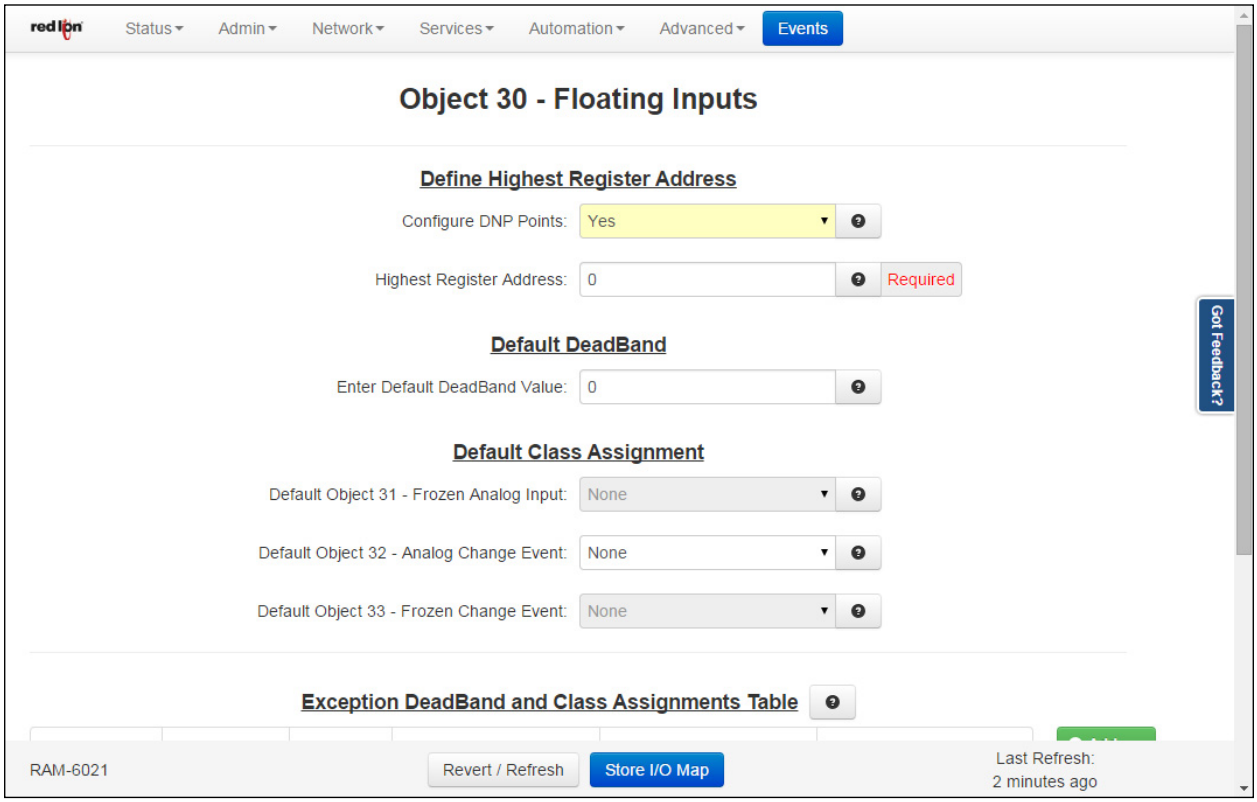
Highest Register Address (Required): This field is used to show or set the highest register address to map DNP3 points.

Click on *Store I/O Map* 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.



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.

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 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.

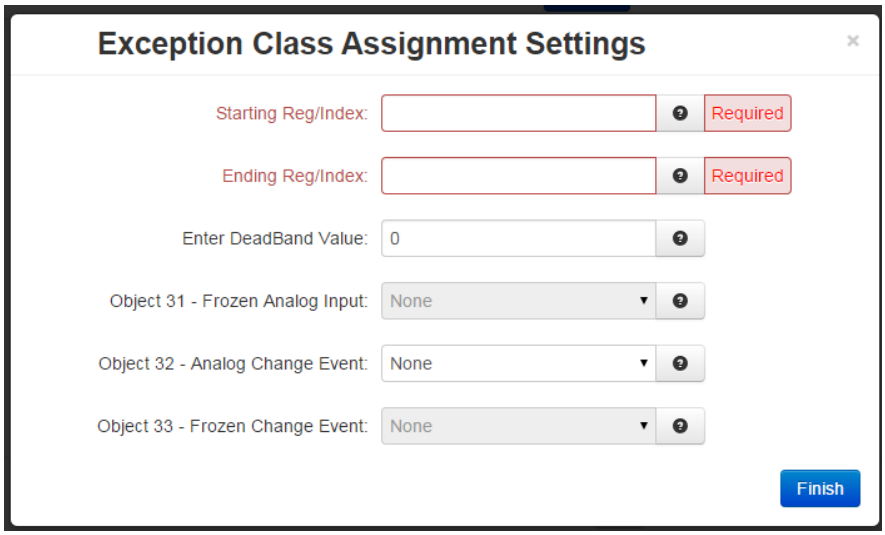
Exception DeadBand and Class Assignment Table: The Exception table provides you with the ability to define Reg/Index ranges that are needed to be configured different than Default DeadBand and Class Assignments.

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 Exception Calls Assignments Settings will appear:



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.

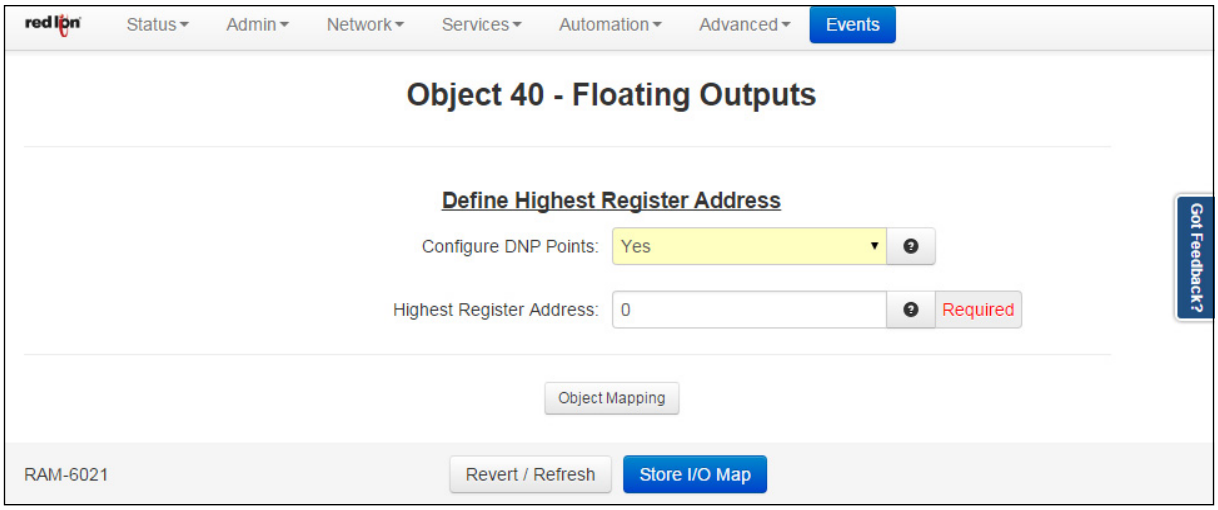
Object 33 - Frozen Change Event: This field is activate by both Levels 2 and 2+. It's used to determine if a DNP3 point will generates events (Object2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default all 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 Map* 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



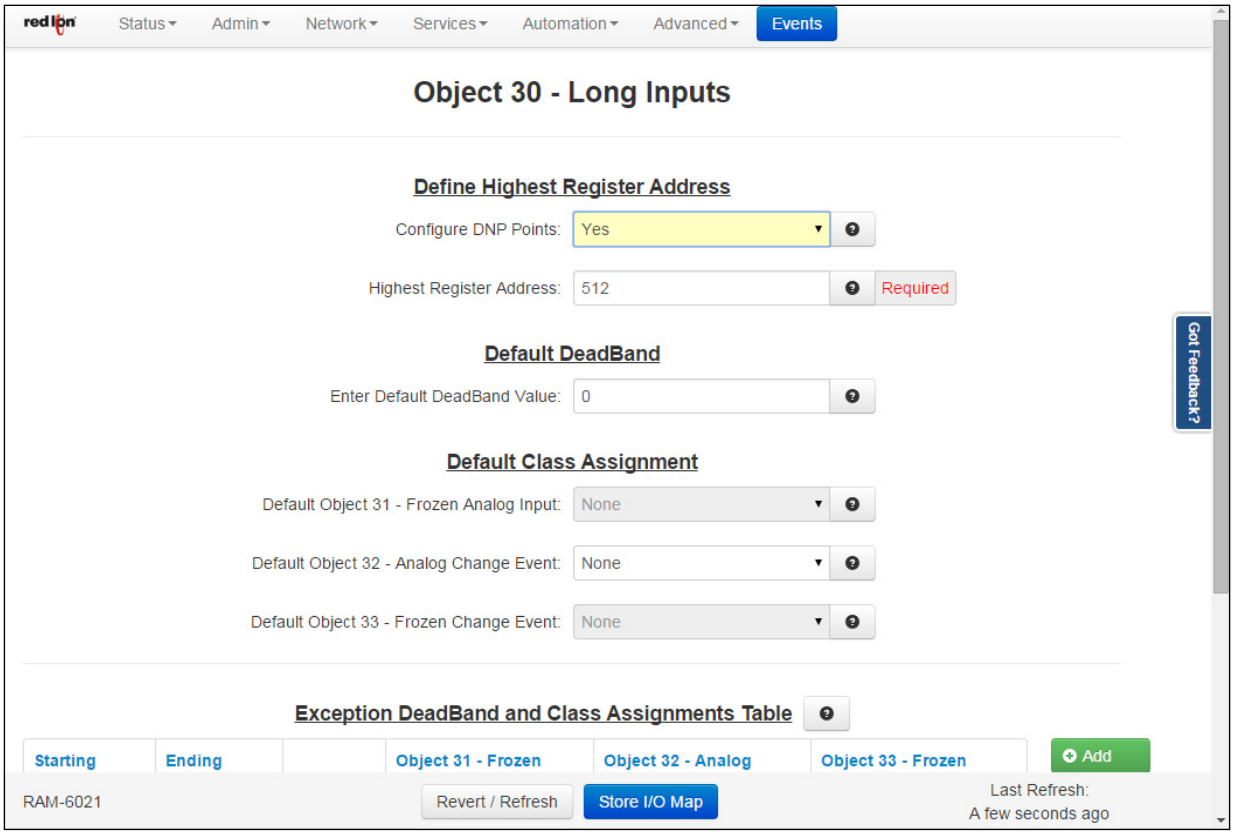
Configure DNP3 Points: If No is selected, then no Analog Outputs are mapped as DNP3 points. If set to Yes, the Highest Register Address field is activated.

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 Map* 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.



Configure DNP3 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.

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 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 DNP3 Points don’t generate events, this feature should be modified by the user.

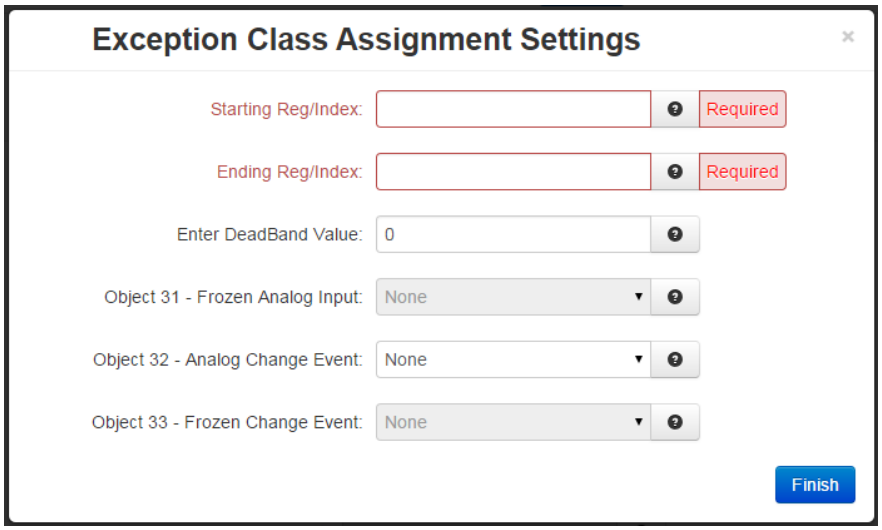
Exception DeadBand and Class Assignments Table: The Exception table provides the ability to define Reg/Index ranges that are needed to be configured differently than Default DeadBand and Class Assignments.

Example: 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 Exception Class Assignment Settings pop-up window will appear:



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.

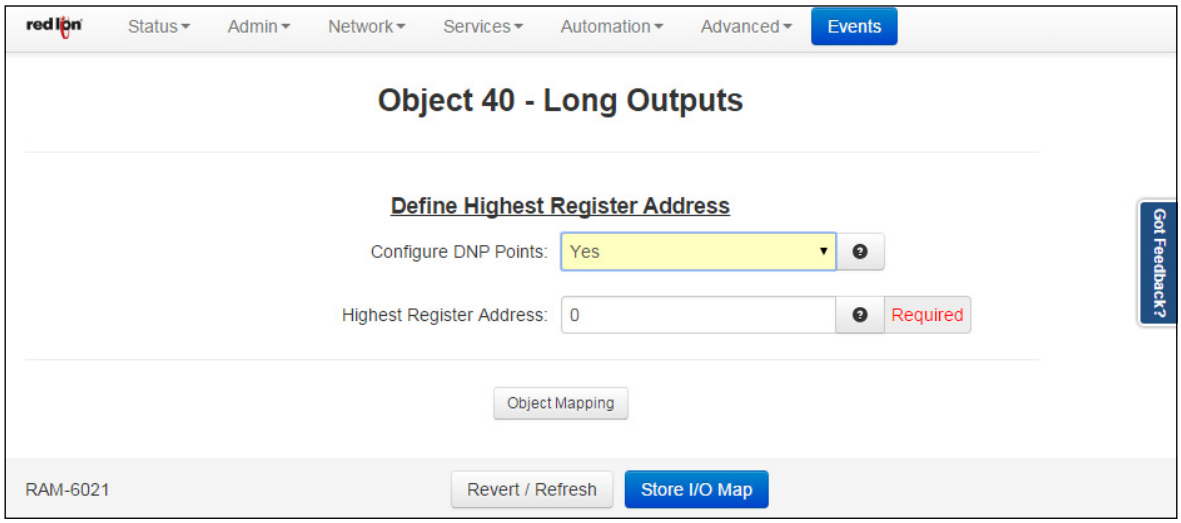
Object 33 - Frozen Change Event: This field is activated on both Levels 2 and 2+. It's used to determine if a DNP3 point will generate events. In case a DNP3 point generates events (Object 2 Binary Change Events) then it should be associated to a class (Class 1, Class 2 or Class 3), otherwise it should 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 Map* 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



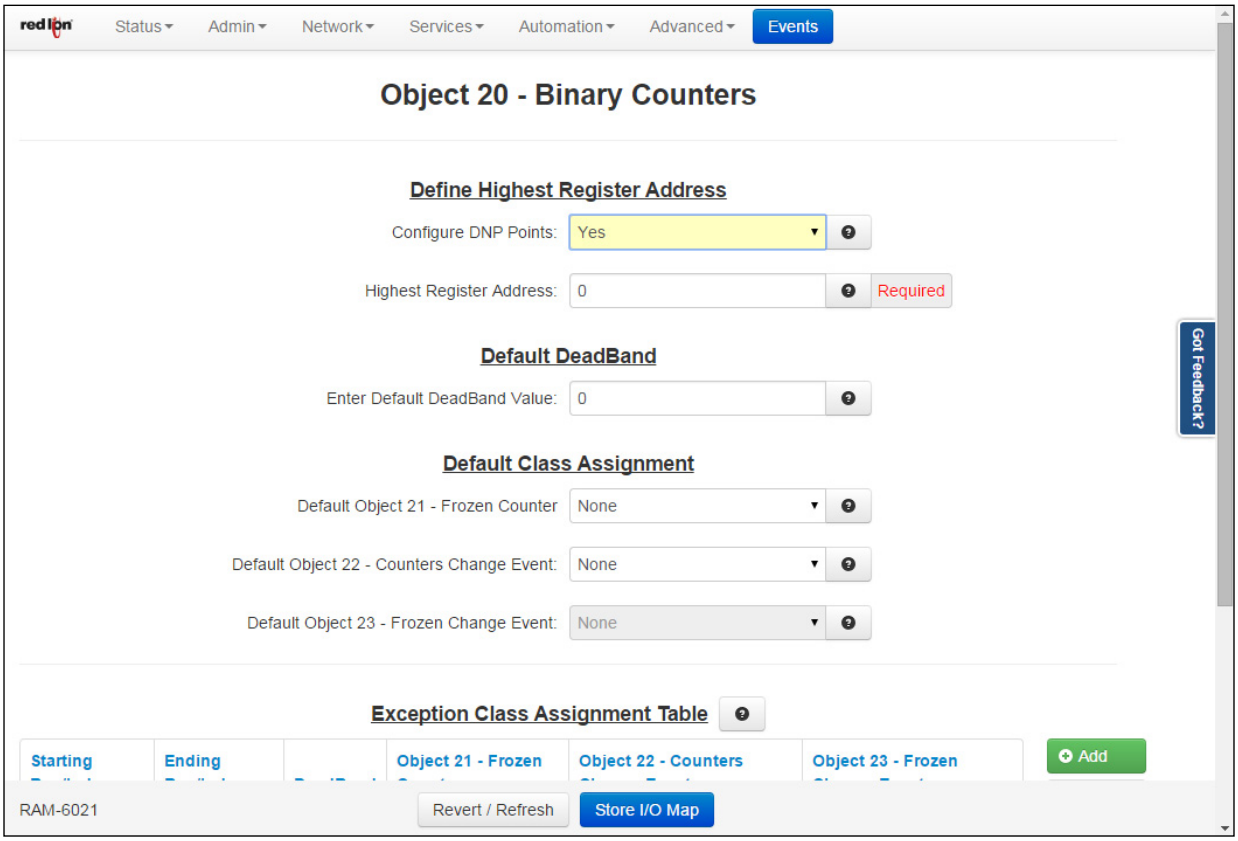
Configure DNP3 Points: If option is set to No, then no Long Outputs are mapped as DNP3 points. If set to Yes, the Highest Register Address field is shown ton enter a Highest register Address value.

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 Map* 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.



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.

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 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.

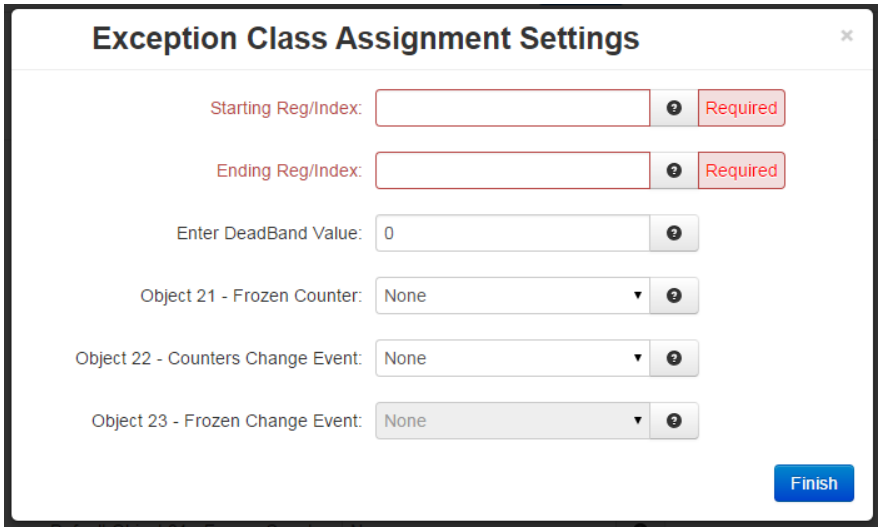
Exception Class Assignment Table: The Exception table provides you with the ability to define Reg/Index ranges that are needed to be configured different than Default DeadBand and Class Assignments.

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 Exception Class Assignment Settings pop-up window will appear:



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)

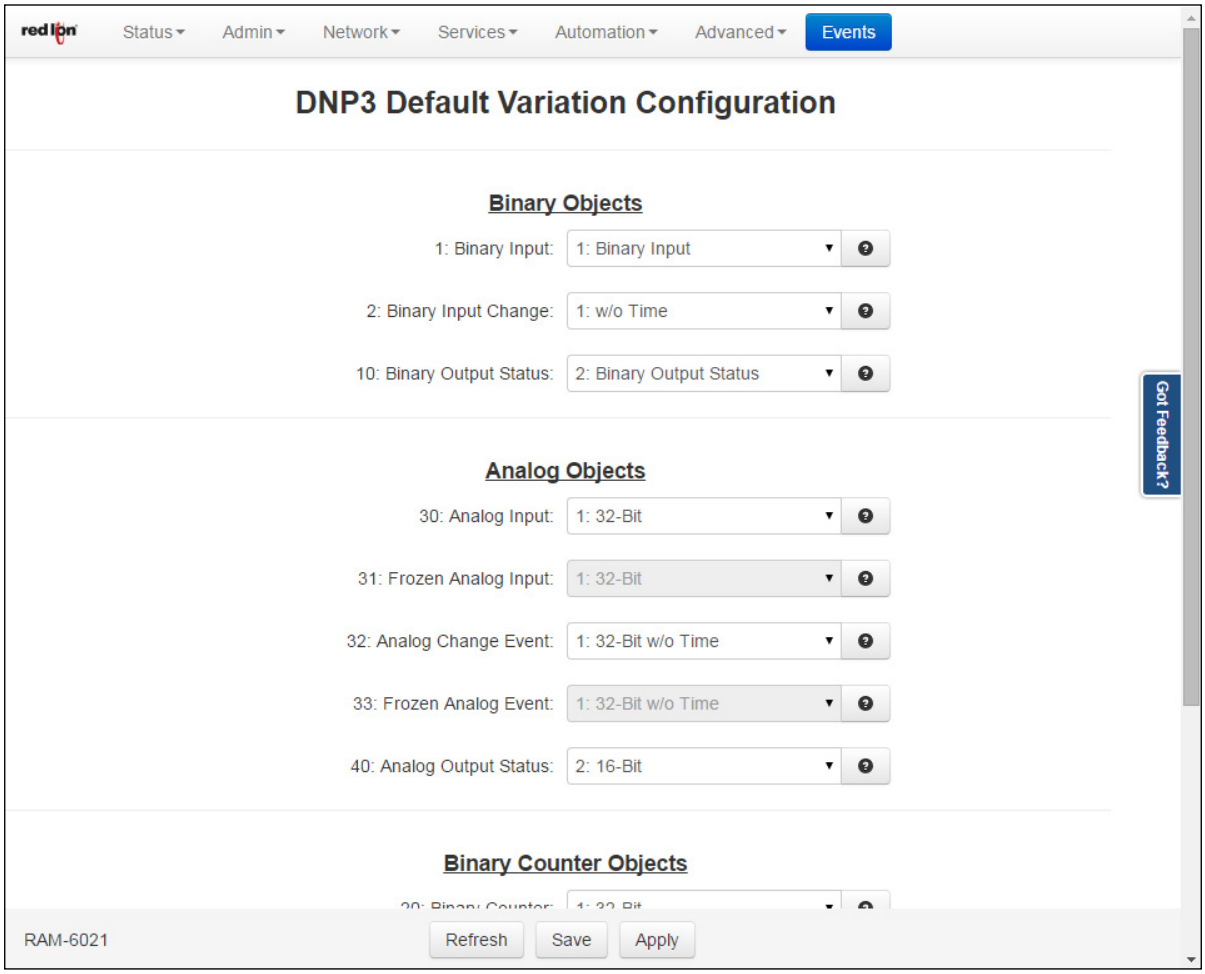
then it should be associated to a Class (Class 1, Class 2 or Class 3), otherwise it should be associated to None. By default, all DNP3 Points don't generate events, this feature should be modified by the user.

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 Map* 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.

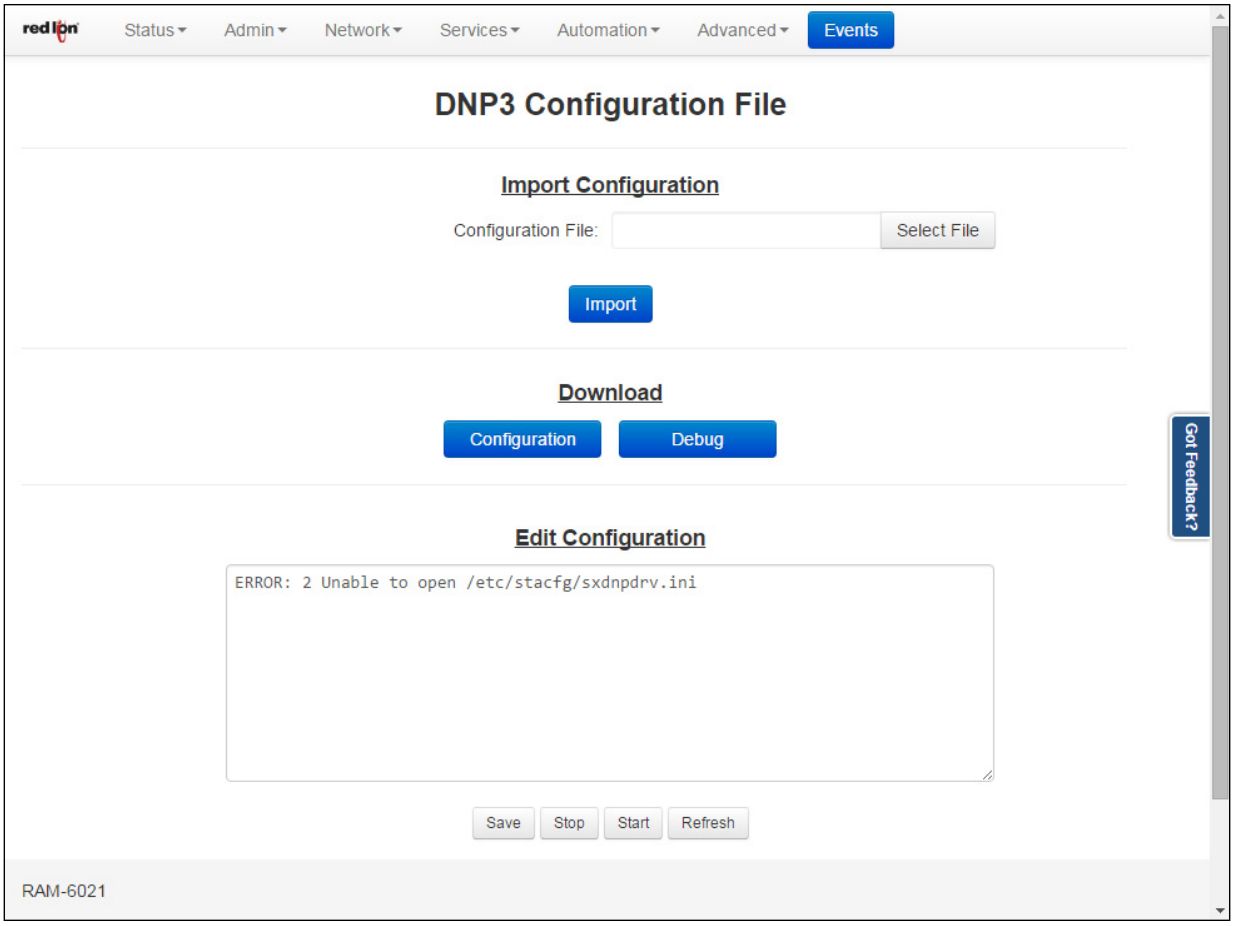
21: Frozen Counter: Combo Box that shows the different choices for Object 21 (Frozen Binary Counters) that the user can select as a default variation.

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. To revert to the previous defaults, click on the *Revert* button.

Display Config File



From this screen you are able to import, export and manually edit the DNP3 configuration file.

Import Configuration File: This option will allow you to import a configuration file to replace your existing DNP3 configuration file. Simply click on Select File button to select your DNP3 configuration file on your PC, click on the Import button to replace your existing DNP3 configuration file.

Download Appropriate File to your PC: 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.

Configure DNP3 Configuration File: This option will load the DNP3 configuration file into the text box for manual editing.

The following controls (buttons) are available:

Save: Save the contents of the text box in to the DNP3 configuration file.

Stop: Stop the DNP3 services, if it is currently running.

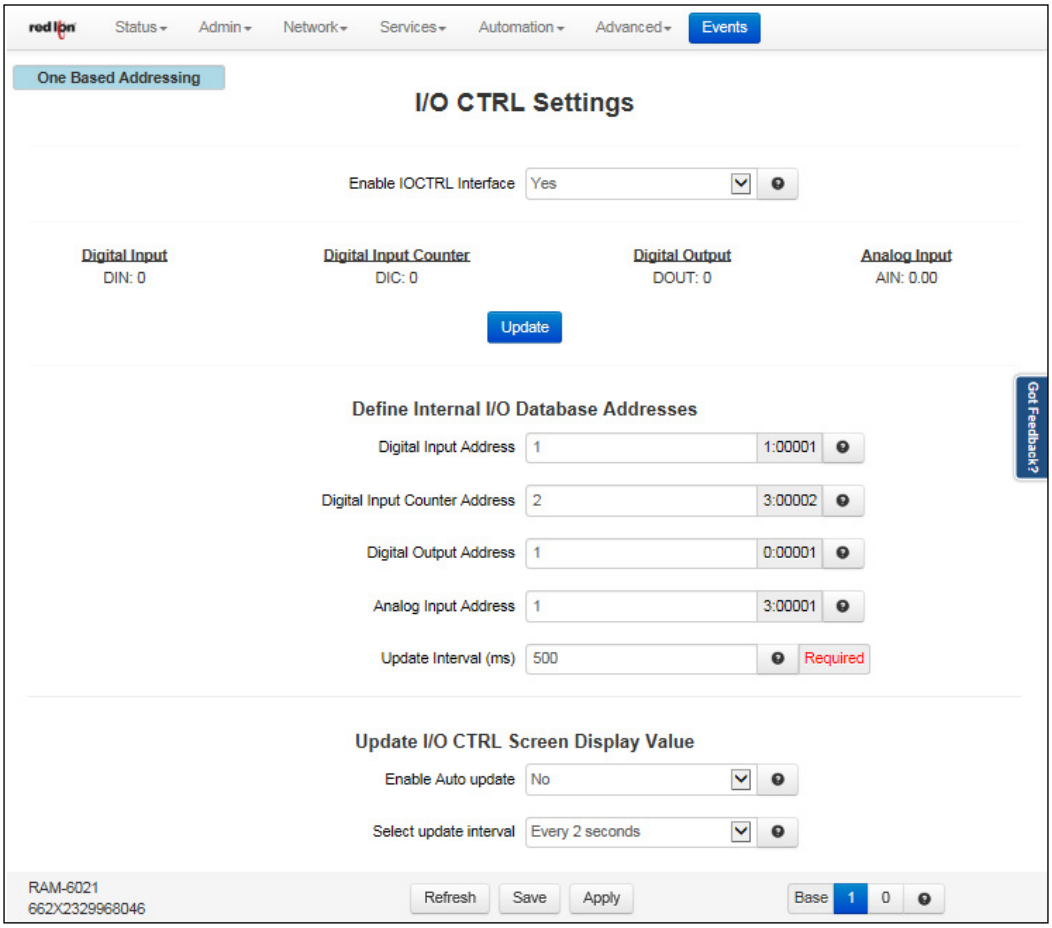
Start: Stop the DNP3 services, if it is currently running and start them back up.

Refresh: Reload the DNP3 configuration file into the text box.

2.6.7 I/O Settings

I/O CTRL

Click on the *I/O CTRL* menu item and the I/O CTRL Settings window will appear:



Enable IOCTRL Interface: Select Yes to enable the IO/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 IO/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.

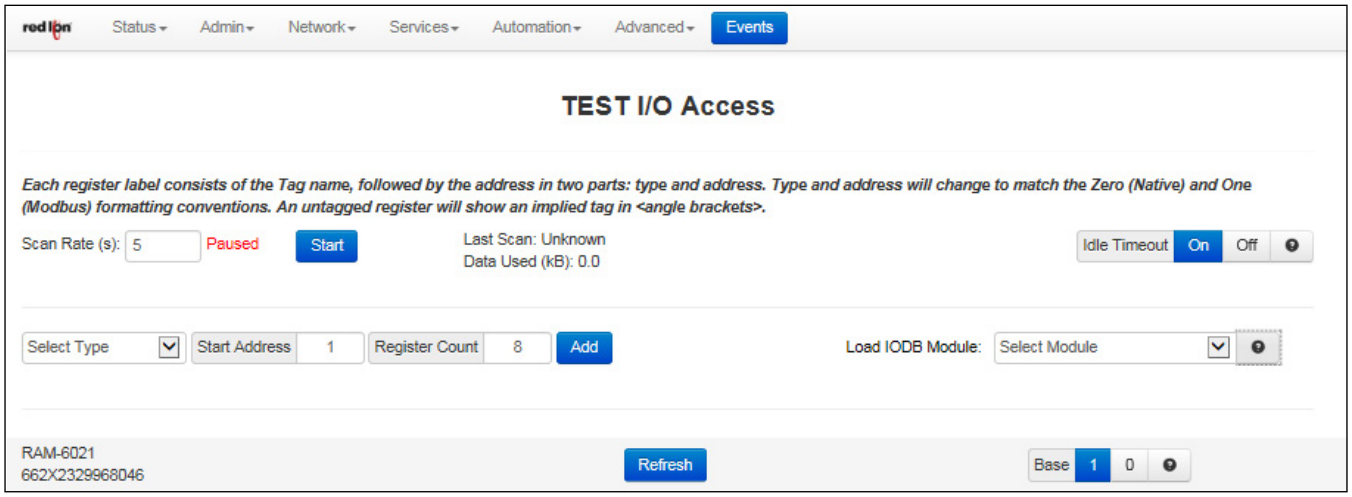
Select update interval: Select the update interval to be used when auto update is enabled from one of the choices in the drop-down list provided. Choices (in seconds) include: 3, 5, 10 or 15.

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 and I/O modules.



The Test I/O interface has been kept simple to make managing the test I/O process easier and keep the screen less cluttered and 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 I/ODB.

Idle Timeout: With this enabled (checked), the browser will stop scanning after two minutes of inactivity.

Select Type: 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.

Load IODB Module: Select the IODB Status Module from the drop down list.

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>.

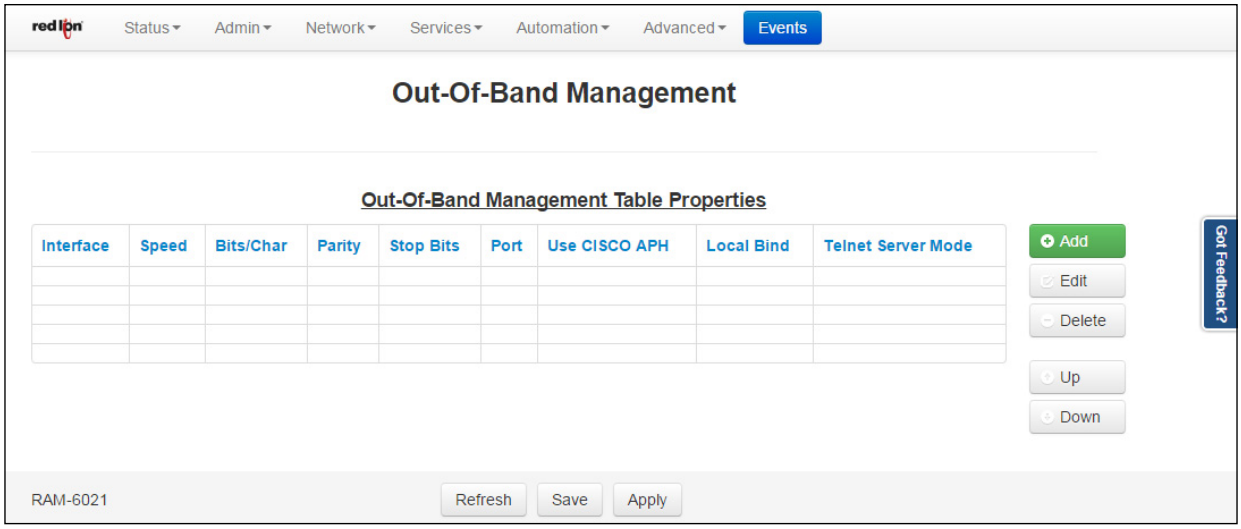
You may enter values here and observe your IODB data from another device / location to see those values get updated, or you may initiate a change from another device/input and observe the changes presented here on your Test I/O interface.

2.7 Advanced Tab

The Advanced Tab includes Out-of-Band Management, VRRP and Expert mode and the option to use the Interface's Classic View.

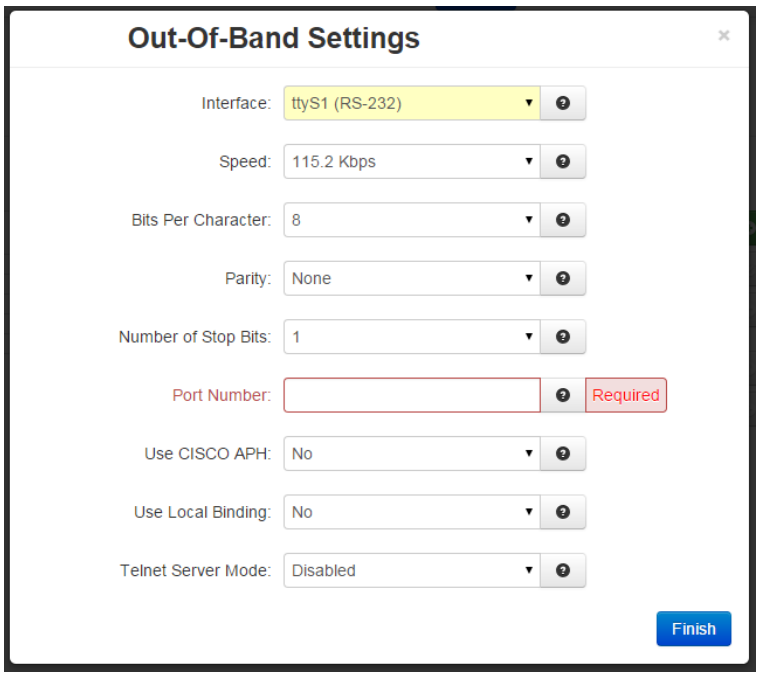
2.7.1 Out-of-Band Management

The Out-of-Band 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 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 router from the RS232 serial port.

Click on the *Add* button to add an instance for OOB Management and the following window will appear:



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.

Number of Stop Bits: Select the number of stop bits to be used.

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: Linefeed 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.

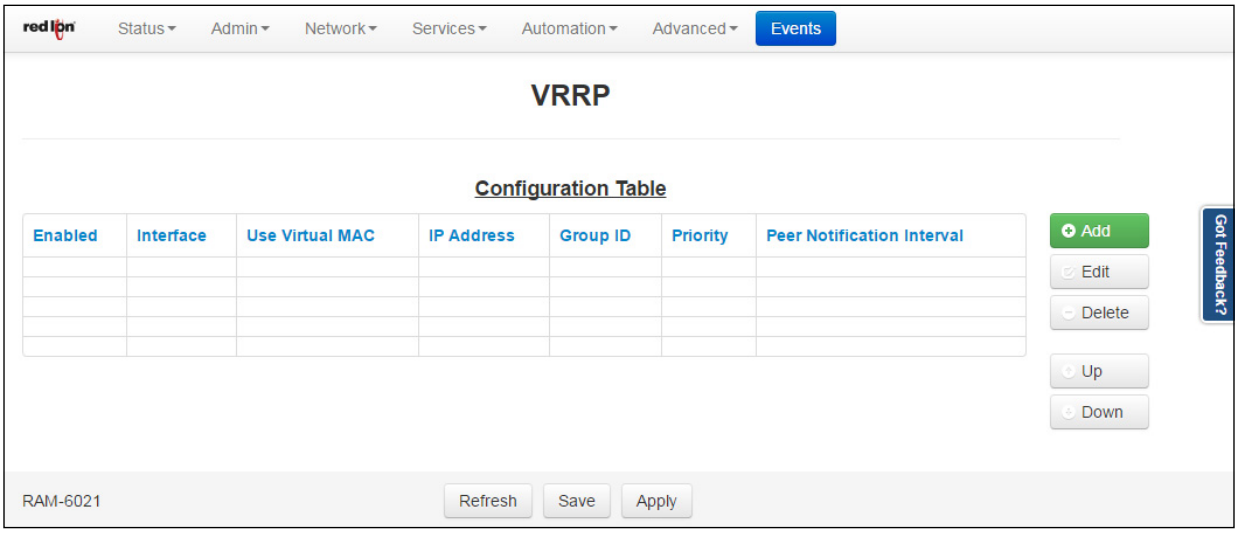
Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

2.7.2 VRRP (Virtual Redundancy Protocol)

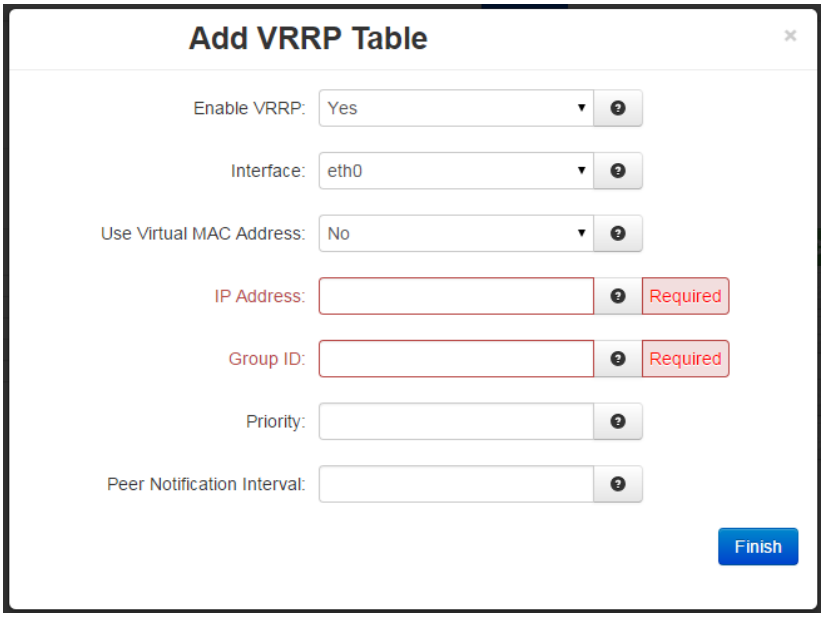
To configure VRRP, select the option from the Advanced menu.

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 VRRP dialog window will appear:



Click on the *Add* button and the following dialog window will appear:



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 handle virtual MAC addresses. The recommended setting for this field is YES.

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: 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.

Peer Notification Interval: 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.

2.7.3 Expert Mode

The Expert Mode menu allows you to edit the configuration fields of Red Lion RAM-6021 directly. This option provides the ability to perform advanced configuration capabilities for complex organizations.

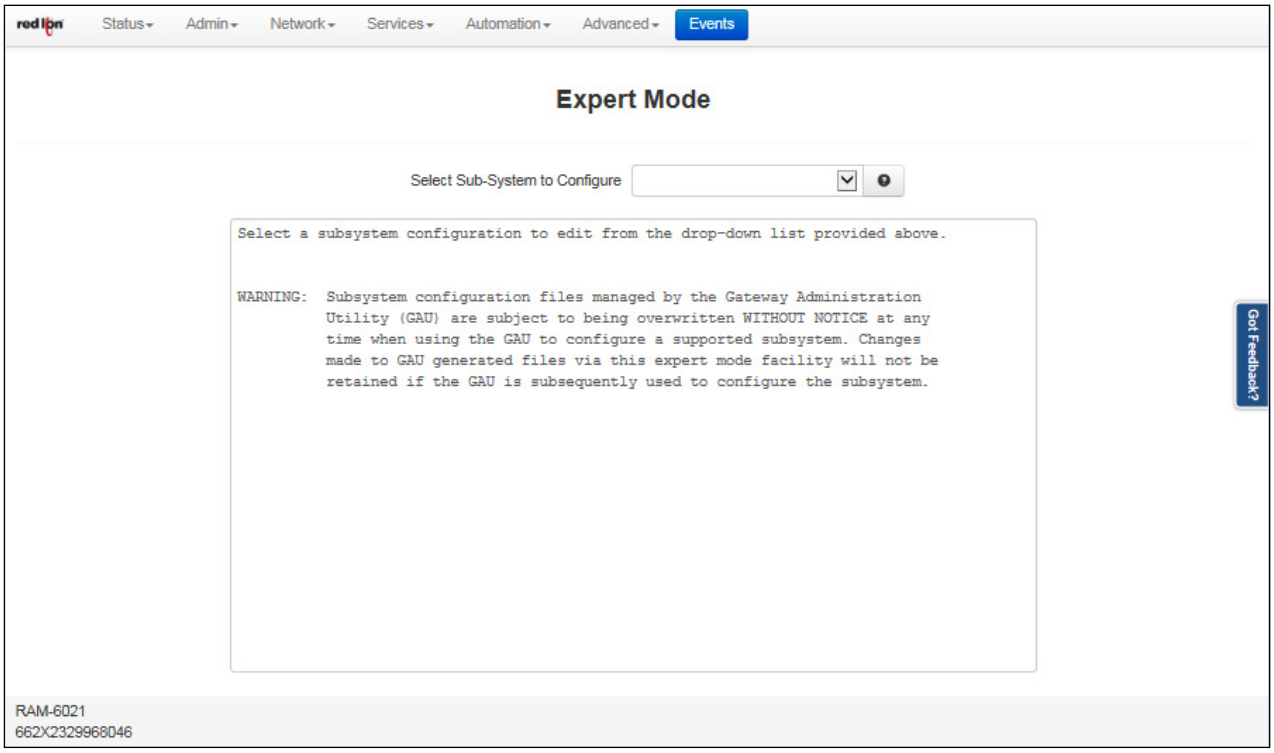
Note: Expert Mode is not recommended unless directed by Red Lion Technical Support.

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.

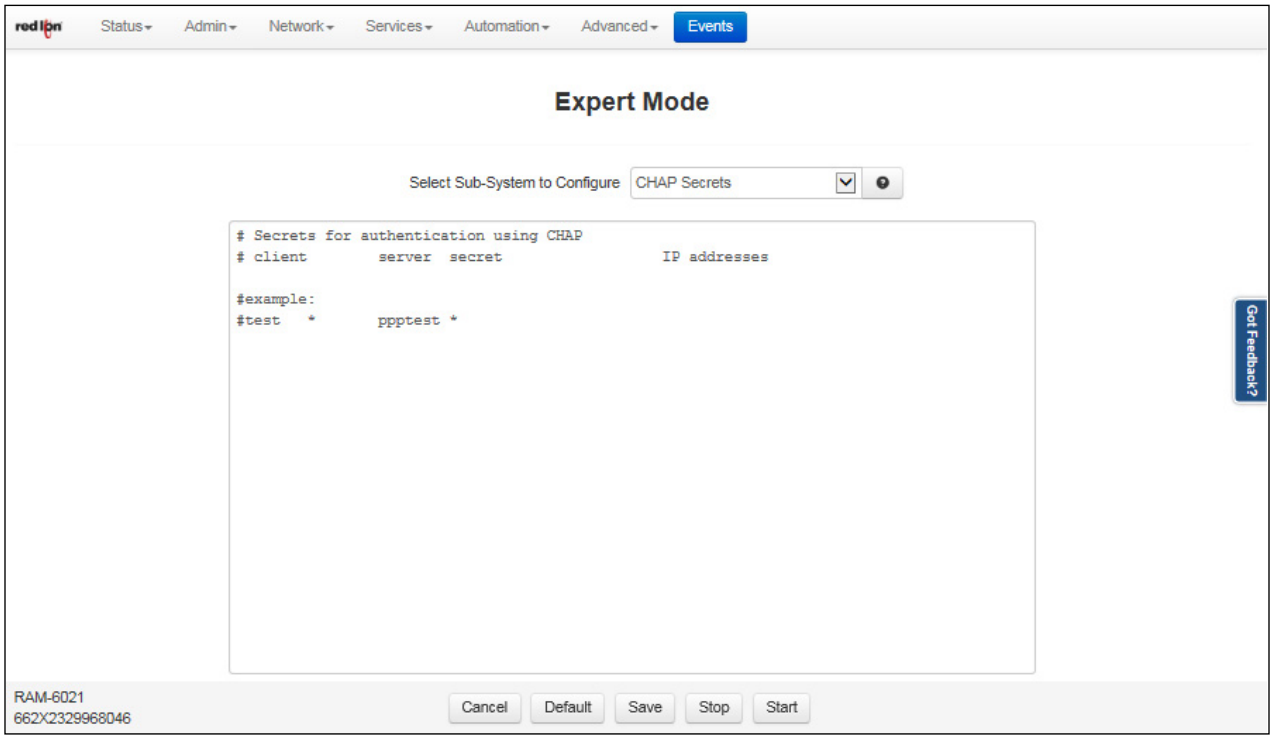
Configure Sub-Systems

The "Configure Sub-Systems" menu item allows you to edit the main configuration files of the Red Lion 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 will appear:



Select Sub-System To Configure: Select a component sub-system from the list as directed by Technical Support. Once a file is selected in the "Select Sub-System to Configure" field, the dialog window will look similar to the one below:



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.

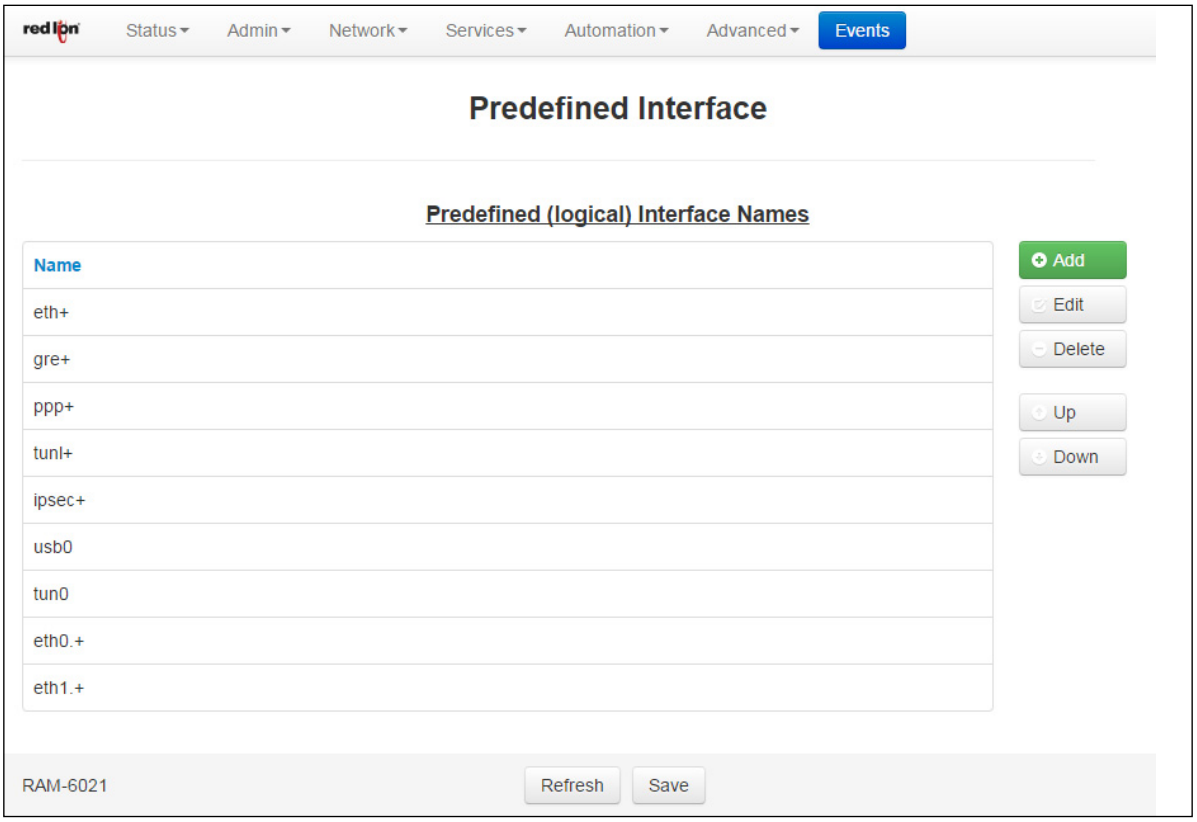
Stop: Stop the component sub-system service if it is currently running.

Start: Start the component sub-system service, or re-start it if it is currently running.

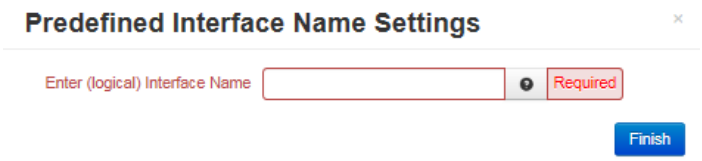
Predefined Interface

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 will appear:



Click on the *Add* button to add a named interface and the Predefined Interface Name Settings pop-up window will appear:



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.

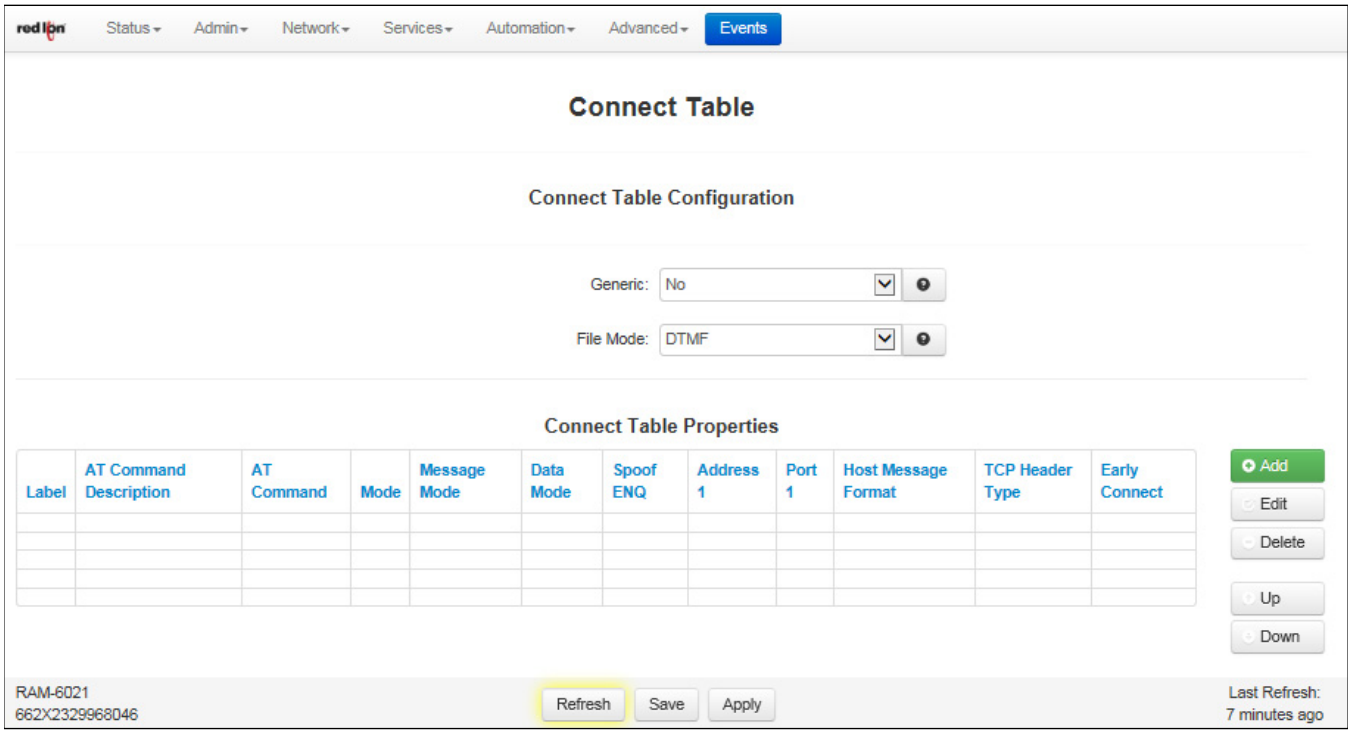
2.7.4 GWLNX

The GWLNX menu item is used to define the following sub-menu items: 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.

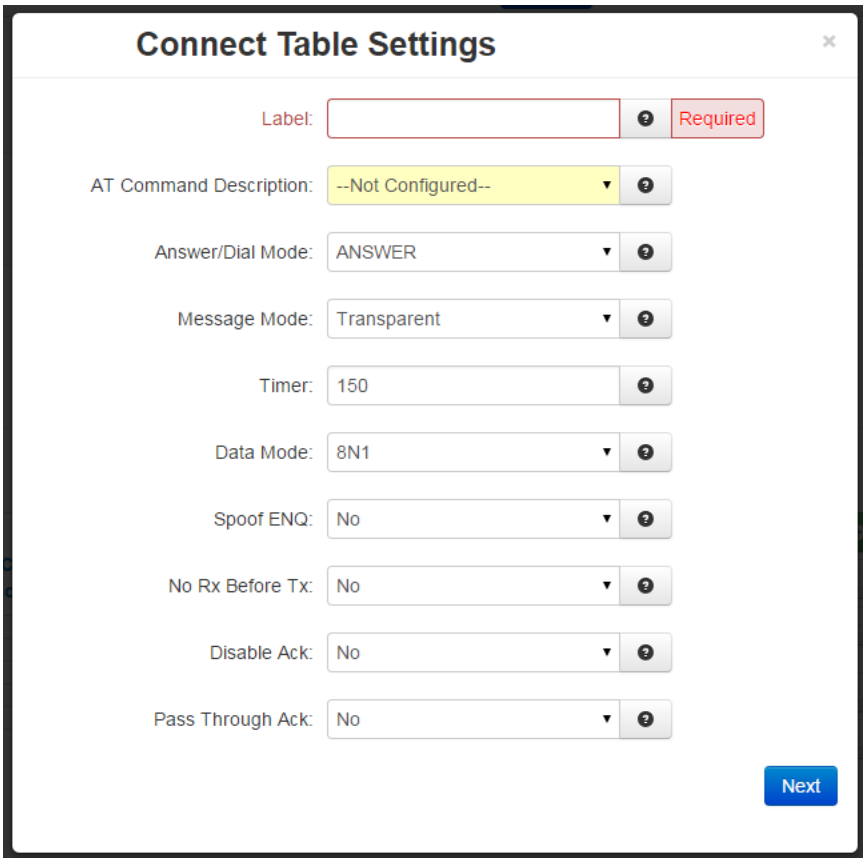
Click on the *Connect Table Configuration* menu item and the Connect Table dialog window will appear:



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 will appear:



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: Acknowledgment 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.

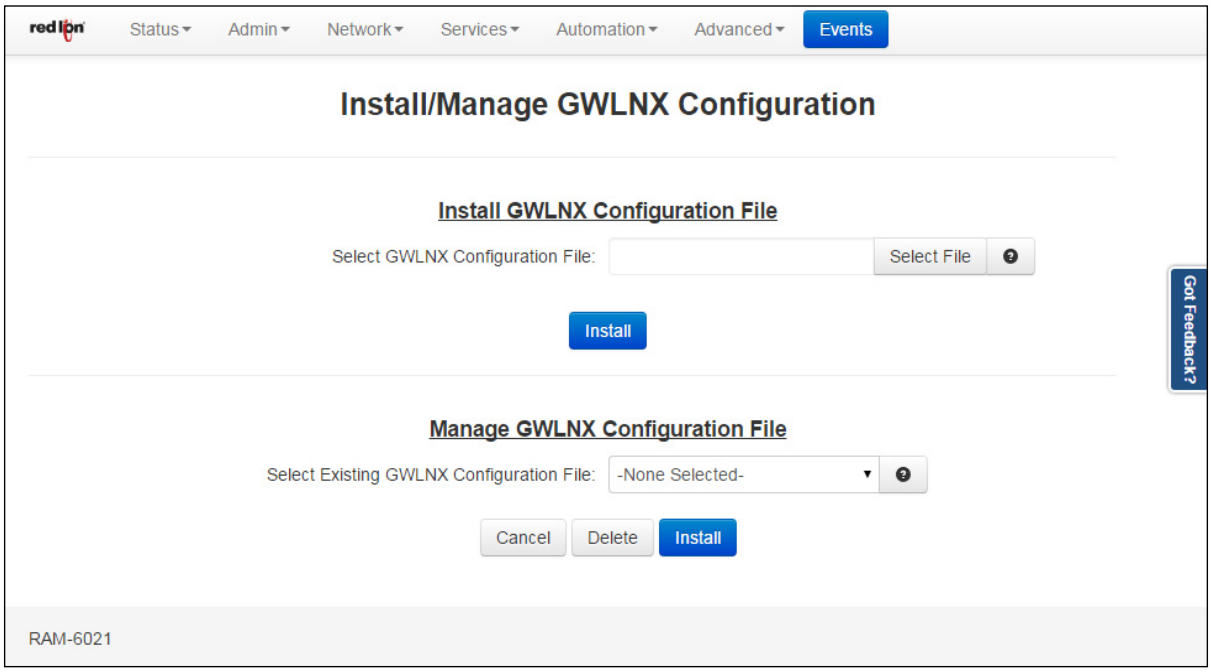
Click on the *Finish* button and you will be directed to the Connect Table dialog window and the Connect Table Properties table will be populated with the entered data.

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 the Red Lion device. The Manage Configuration section is used to install or delete Gwlnx configuration files that already reside on the Red Lion device.

Click on the *Install Configuration* menu item and the Install/Manage GWLNX Configuration dialog window will appear:



Install GWLNX Configuration File

Select GWLNX Configuration File: Click the “Select File” button to select a GWLNX configuration file to upload from your local system. It is recommended that you do no upload new files unless directed by Red Lion Technical Support.

Manage GWLNX Configuration File

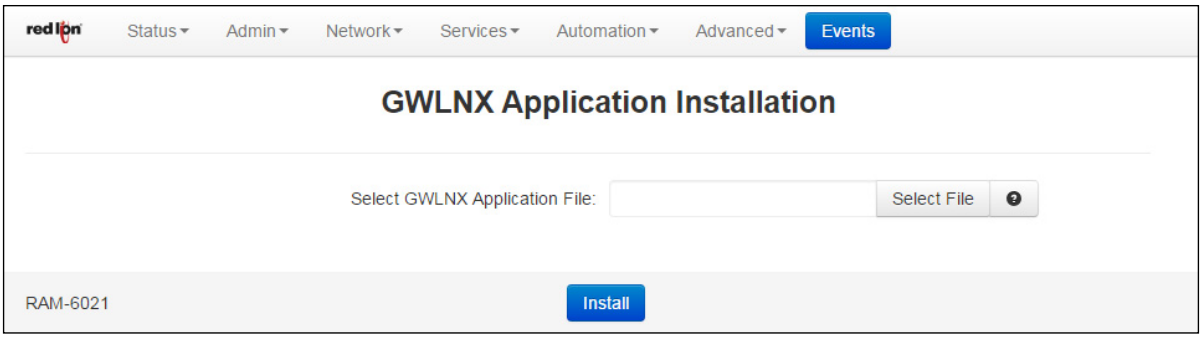
Select GWLNX Configuration File: Select a Gwlnx configuration file on the remote unit to install or to delete. It is recommended that you do not install or delete files unless directed by Red Lion Technical Support.

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 configure the new Gwlnx application on the Red Lion device.

Click on the *Install Application* menu item and the GWLNX Application Installation dialog window will appear:

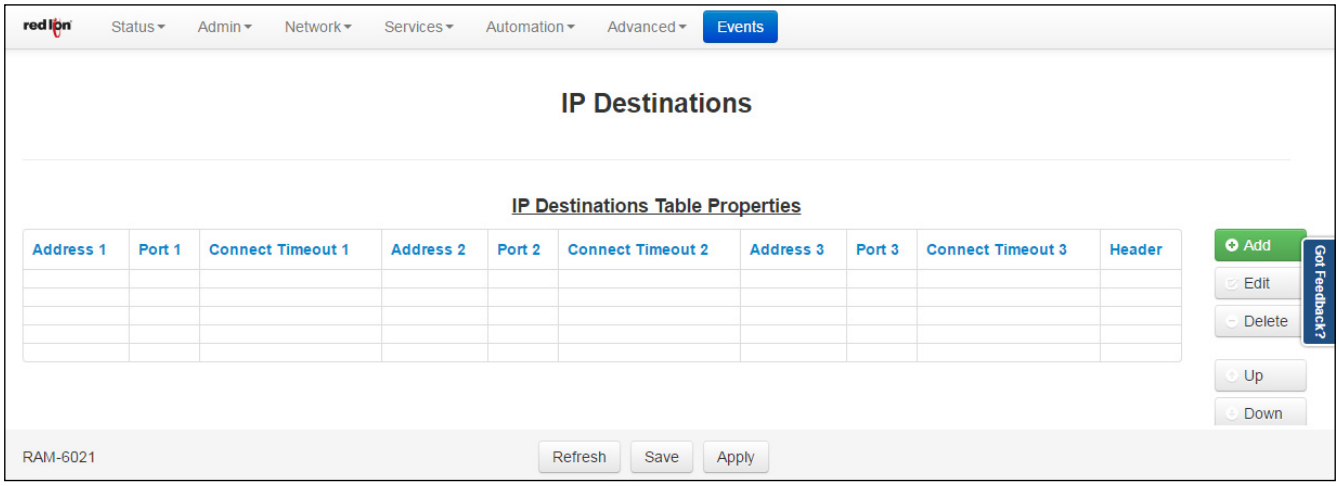


Select GWLNX Application File: Click on the Select File button to select a ‘GWLNX’ zip file to upload from your local system. It is recommended that you do not upload files unless directed to do so by Red Lion Technical Support.

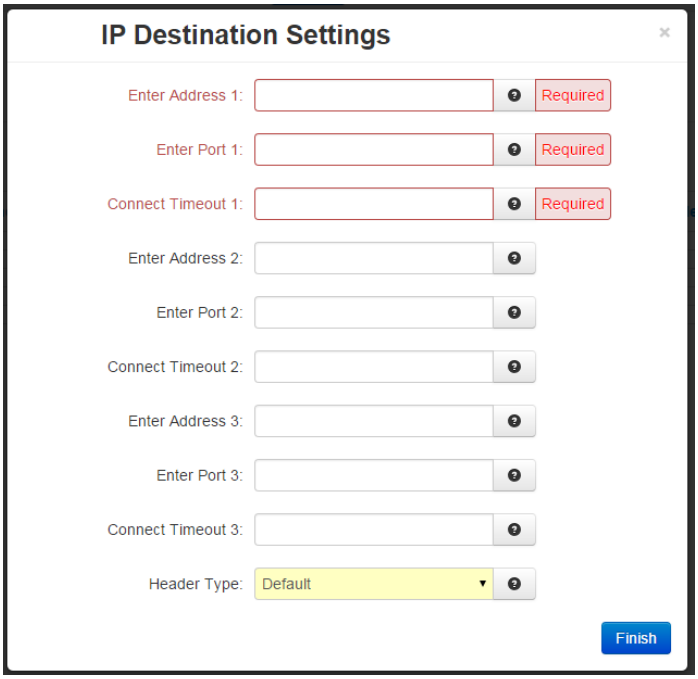
IP Destinations

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 IP Destinations dialog window will appear:



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.

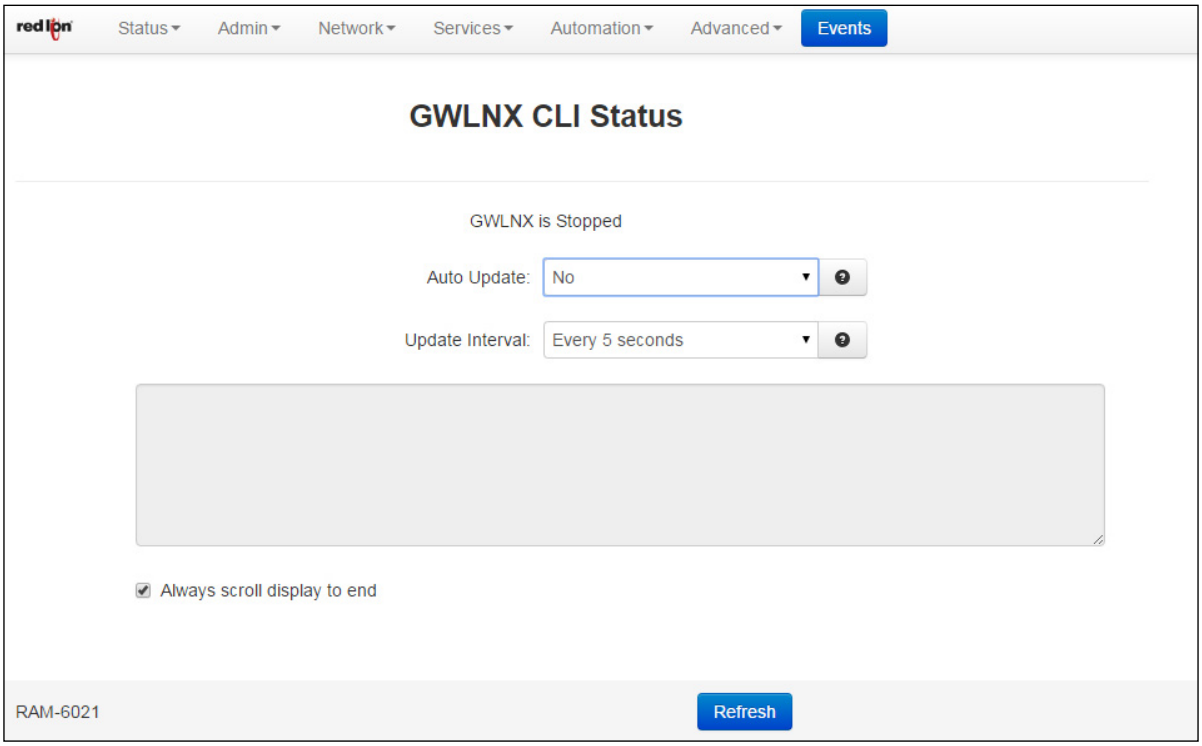
Click on the *Finish* button and you will be directed to the IP Destinations dialog window and the IP Destinations Table Properties will be populated with the entered data.

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 GWLNX CLS Status dialog window will appear:



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.

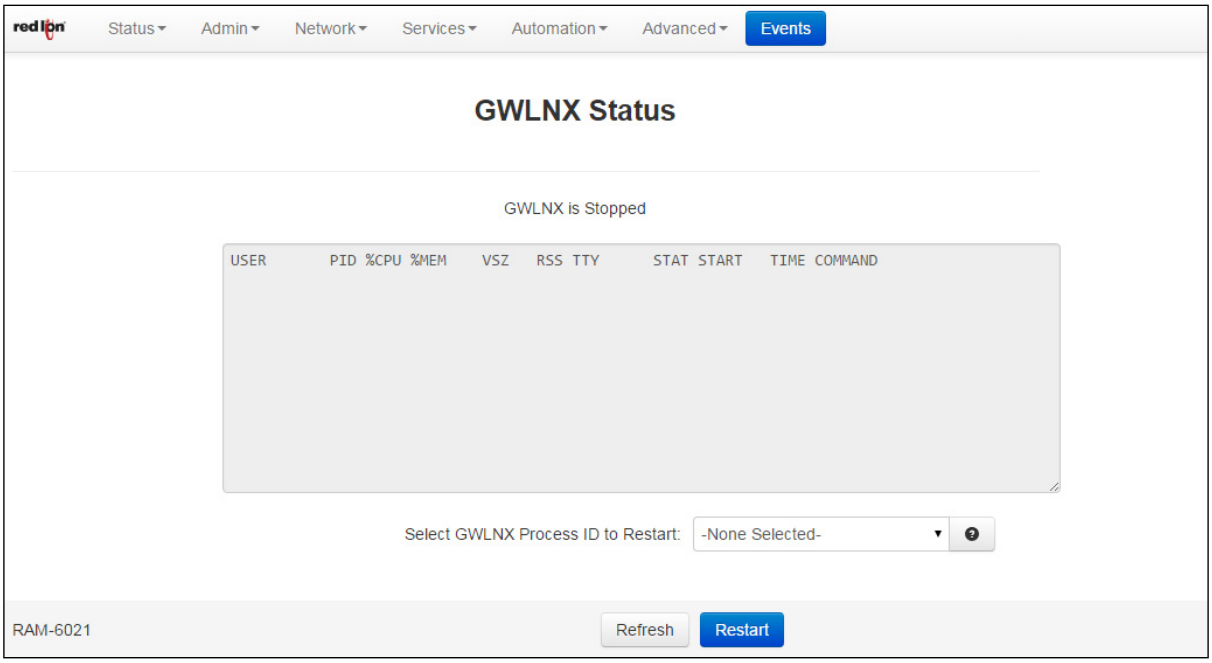
Update Interval: Select the update interval to be used when auto-update is enabled from one of the choices in the drop-down list provided. Choices (in seconds) include: 5, 15, 30 & 60.

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 GWLXN 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 GWLNX application has been restarted.

Select the GWLXN Status menu item and the corresponding dialog window will appear:



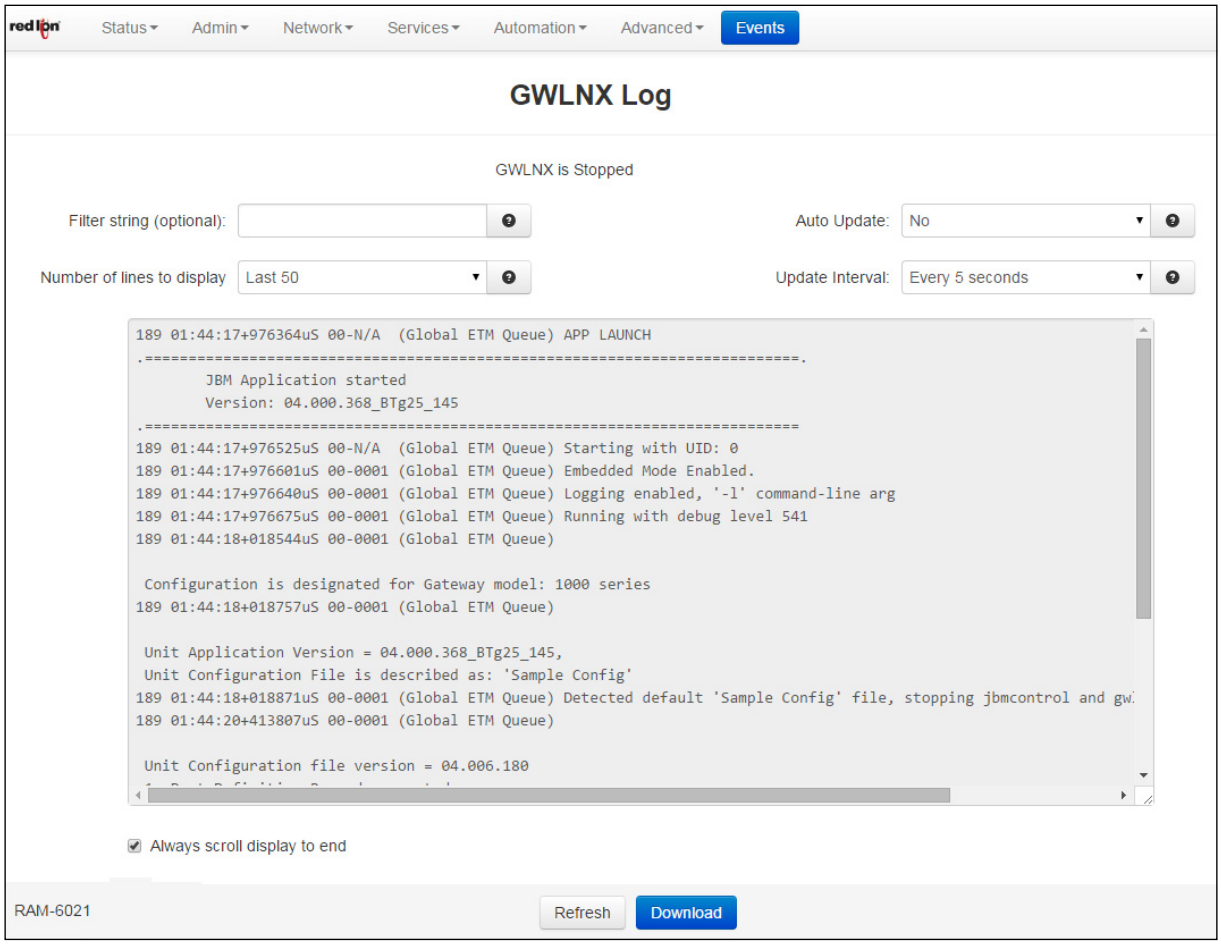
Select GWLNX Process ID to Restart: Select the GWLNX Process ID (PID) that you like to restart.

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.

Select the GWLNX Log menu item and the GWLNX Log dialog window will appear:



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.

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.

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.

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.

2.7.5 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.

2.8 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.

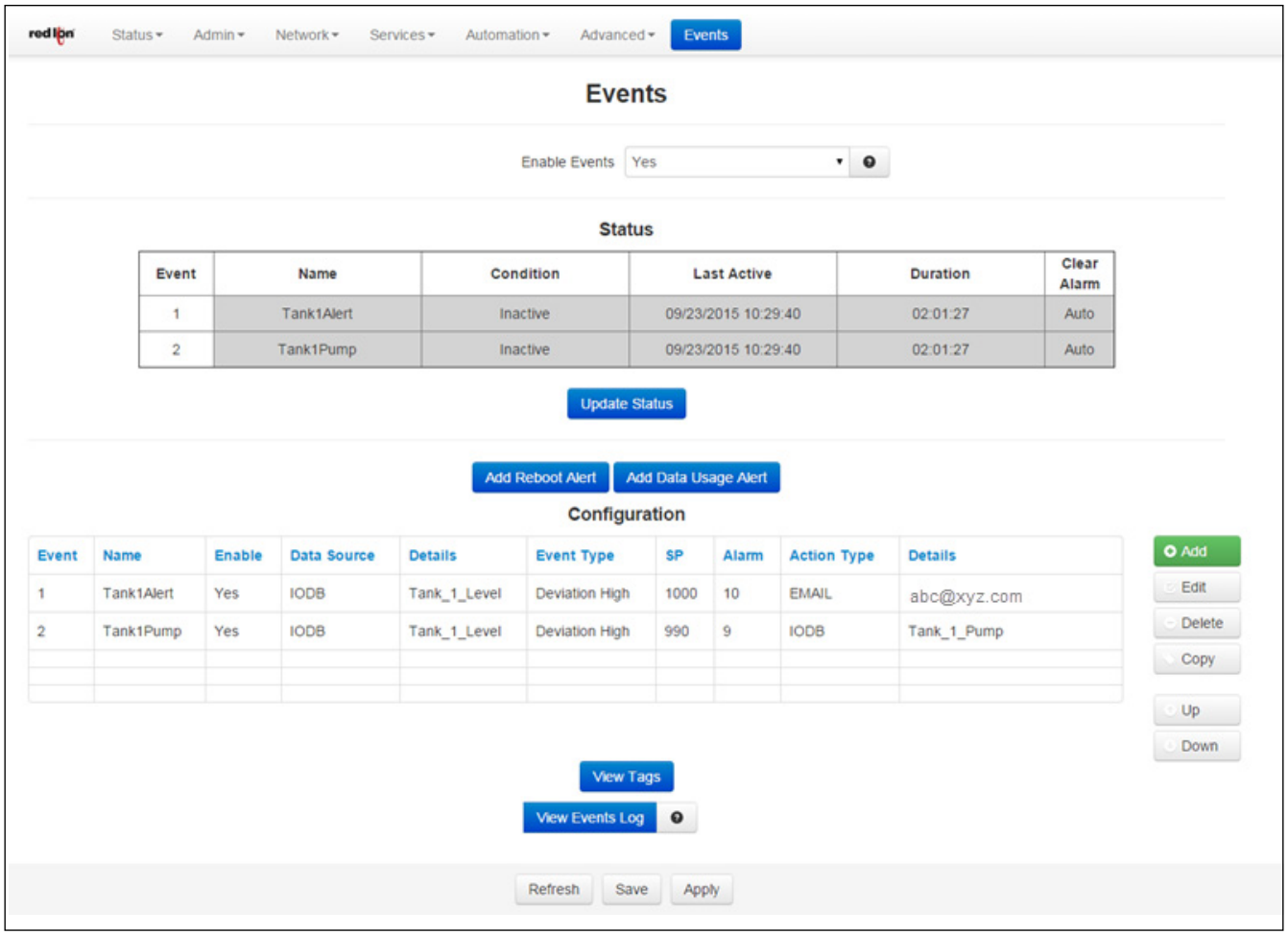
Multiple events can be used to create more advanced logic or to create multiple stages of severity for alarms.

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.

Note: The RAM-6021 Wired Router device supports email messaging.

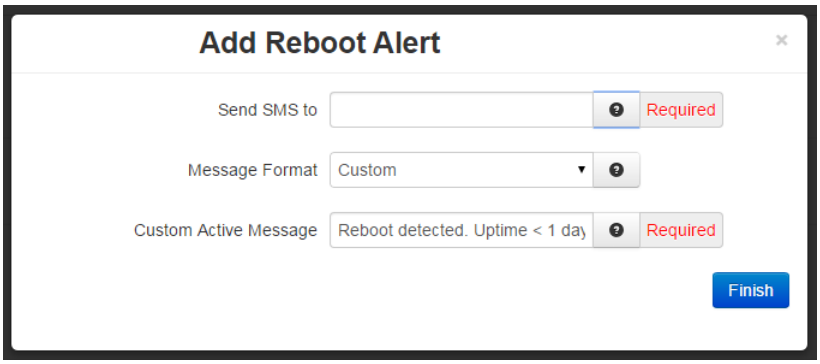
Note: The RAM-6021 Wired Router device does not support SMS messaging.



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):

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,user-group@email.com

Note: The RAM-6021 Wired Router device supports email messaging.

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

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: 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

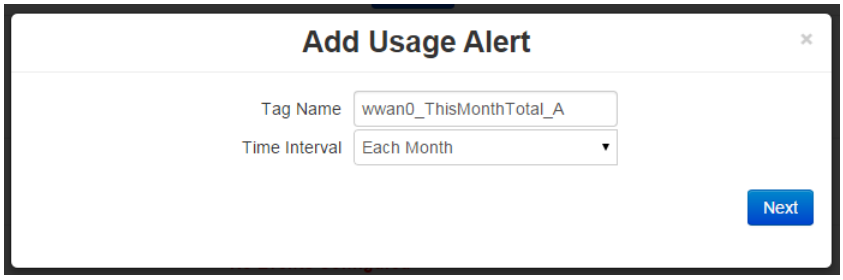
First Bit = the first event name in the expression, and so on.

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

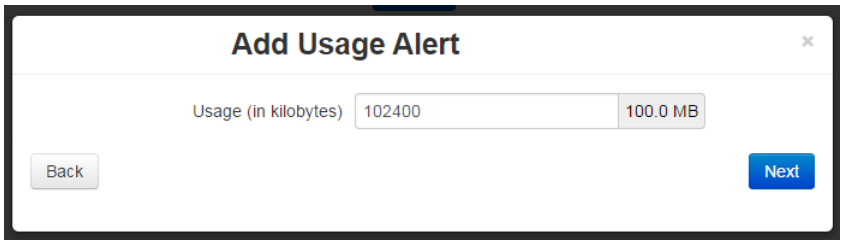
Click on the *Add Data Usage Alert* button to define parameters for data usage alerts.



Tag Name: Enter the tag name this Data Usage alert will be applied to.

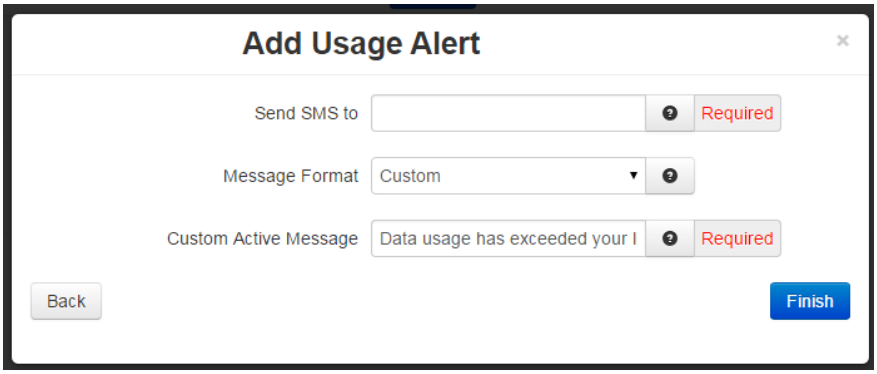
Time Interval: Select how often an alert is desired. The options are each month or each day.

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):

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,user-group@email.com.

Note: The RAM-6021 Wired Router device supports email messaging.

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.

Message Format: Define what type of content the Event 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):

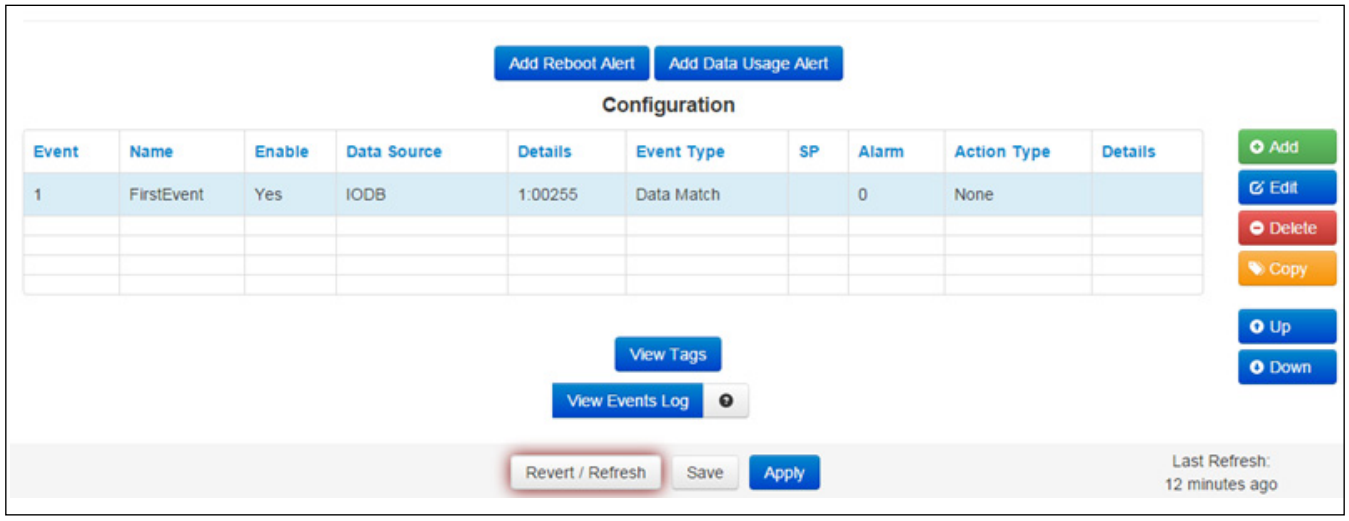
Email Message: Enter a custom message body that will be sent to the Recipient(s) when the event goes active.

Note: The RAM-6021 Wired Router device supports email messaging.

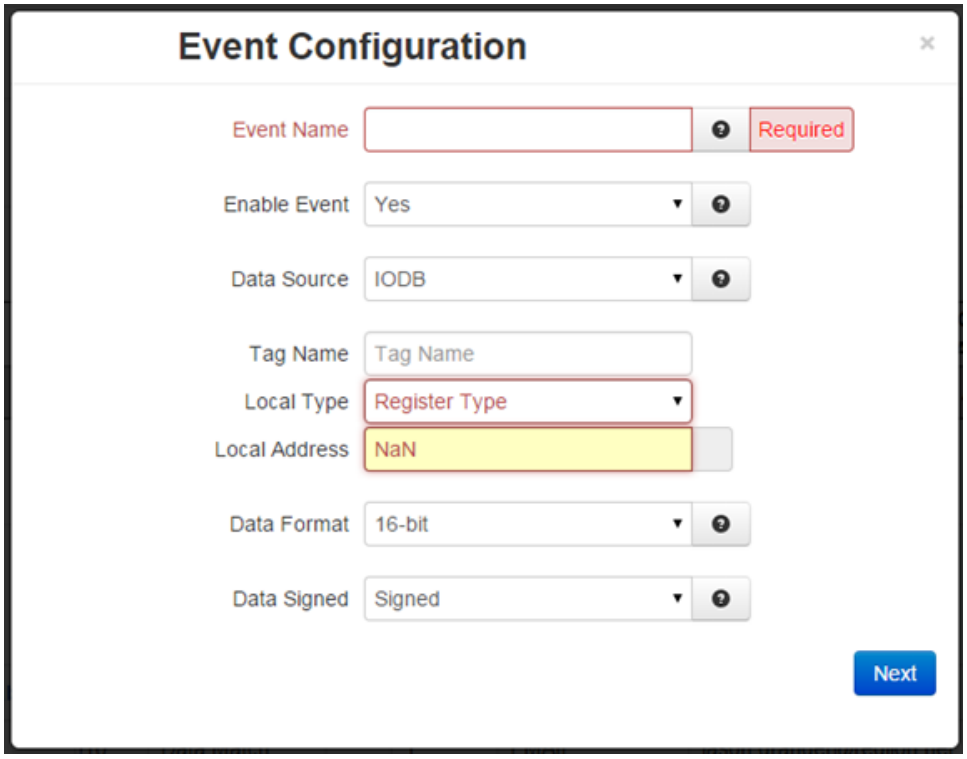
SMS Message: Enter a custom message when an event goes active to be sent to the recipient. If appended to a standard message, the length is limited to 60 characters.

Click on the *Finish* button. You will be returned to the *Events* dialog window.

Configuration



Click on the *Add* button and the Event Configuration dialog window will appear:



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 will appear.

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 will appear:

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 | $TAGNAME$

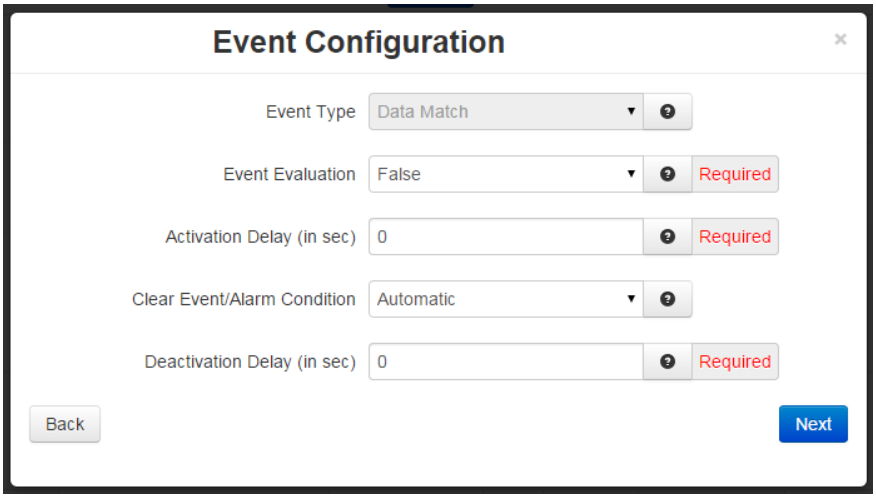
$TAG1$ & $TAG2$ | $TAG3$ & !$TAG4$

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.

Alarm Value: 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:

		Max Unsigned	Min Signed	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.

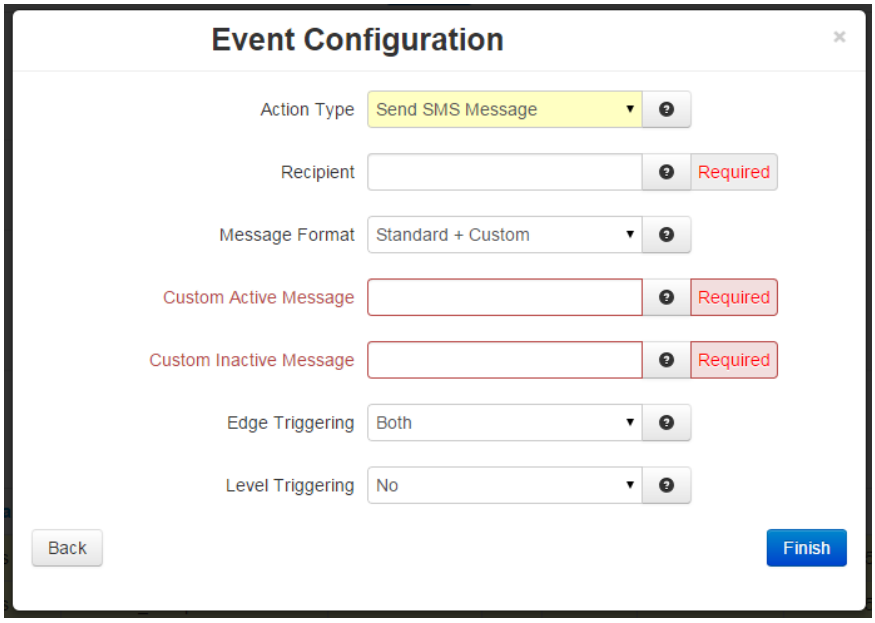
For example, if the alarm is configured to go active when an input register is an Absolute High exceeding 1000, then the register value must stay above 1000 for the activation delay period, or else it will be ignored.

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 Script: Run a Command Script that performs an Action.

SVM Alert Message: Send an alert message to the SVM server that will appear in unit history.

Recipient (Required): This references another data list for a list of contacts.

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,user-group@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 will allow 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.

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.

Ipsec Restart: Restart the IPSec service. ie: Bring the IPSec tunnel down, then reestablish the tunnel.

Ipsec Stop: Stop the IPSec service and do not reestablish the tunnel

Reboot: Reboot the entire device.

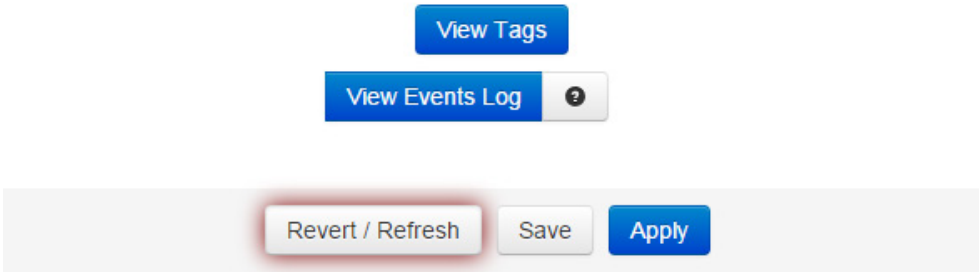
Reset Wireless: Restart the Cellular Module. (not applicable to the RAM-6021 Wired Router)

Restart Serial IP: Restart the Serial IP Service.

Alert Level: Select an Alert Level for the message that will appear 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 **2.6.3 Tags** 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 service, call Red Lion at +1 (877) 432-9908. 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 RO (Repair Order) can be obtained on the Red Lion website.

Red Lion tracks the flow of returned material with our RO system to ensure speedy service. You must include this RO 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 RO 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

Inside US: +1 (877) 432-9908
Outside US: +1 (717) 767-6511
Fax: +1 (717) 764-0839
Email: support@redlion.net
Hours: 8:00 am to 6:00 pm EST

Red Lion Controls
20 Willow Springs Circle
York, PA 17406
www.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., Sixnet Inc., N-Tron Corporation, or Blue Tree Wireless Data, 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: Please note that 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. SN6600).
unitSerialNumber	DISPLAYSTRING	Serial Number (e.g. 6621-2517560325).
unitFirmwareVersion	DISPLAYSTRING	Firmware Version Number (e.g. v3.04rc33).
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	INTEGER32	Session Initiation Protocol, used to establish sessions between multiple parties in a location-independent manner. Typically voice sessions. Cellular Session Initiation Protocol User.
sid	INTEGER32	System ID, a unique 5-digit number assigned to each carrier by the FCC. Cellular System ID.
nid	INTEGER32	Network ID, used to divide SIDs into smaller areas. Cellular Network Identifier.

prl	INTEGER32	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	INTEGER32	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	INTEGER32	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	INTEGER32	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	The vendor-provided model name of the modem/card/module (e.g. sierra598U).
hwVersion	DISPLAYSTRING	Hardware version of the module/aircard. Cellular Module hardware version #.
carrier	DISPLAYSTRING	Service provider for cellular network. Cellular Service Provider.
lowRssi	INTEGER32	Low Speed Received Signal Strength Indication. Cellular High Speed received signal strength indication. DEFAULT:0
lowEcio	INTEGER32	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. DEFAULT:0

highRssi	INTEGER32	High Speed Received Signal Strength Indication. Cellular High Speed received signal strength indication. DEFAULT:0
highEcio	INTEGER32	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. DEFAULT:0
currentRssi	INTEGER32	Current Received Signal Strength Indication. Cellular Current Received Signal Strength Indication. DEFAULT:0
currentEcio	INTEGER32	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. DEFAULT:0
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	INTEGER32	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	INTEGER32	0 or 1. 0 = currently not roaming, 1 = currently roaming. Cellular current roaming status.
currentState	INTEGER32	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	INTEGER32	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	INTEGER32	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.
rrcState	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.
mmccState	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
lteRSRP	DISPLAYSTRING	LTE Reference Signal Received Power
lteRSRQ	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
trafficppp0		
todayRxPpp0	DISPLAYSTRING	Vnstat Today RX 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	INTEGER32	Vnstat Today Rx for PPP0 Interface in Kib
todayTxPpp0Kib	INTEGER32	Vnstat Today Tx for PPP0 Interface in Kib
todayTotalPpp0Kib	INTEGER32	Vnstat Today Total Rx/Tx for PPP0 Interface in Kib
yesterdayRxPpp0Kib	INTEGER32	Vnstat Yesterday Rx for PPP0 Interface in Kib
yesterdayTxPpp0Kib	INTEGER32	Vnstat Yesterday Tx for PPP0 Interface in Kib
yesterdayTotalPpp0Kib	INTEGER32	Vnstat Yesterday Total Rx/Tx for PPP0 Interface in Kib
CurrMonthRxPpp0Kib	INTEGER32	Vnstat Current Month Rx for PPP0 Interface in Kib
CurrMonthTxPpp0Kib	INTEGER32	Vnstat Current Month Tx for PPP0 Interface in Kib
CurrMonthTotalPpp0Kib	INTEGER32	Vnstat Current Month Total Rx/Tx for PPP0 Interface in Kib
PreMonthRxPpp0Kib	INTEGER32	Vnstat Previous Month Rx for PPP0 Interface in Kib
PreMonthTxPpp0Kib	INTEGER32	Vnstat Previous Month Tx for PPP0 Interface in Kib
PreMonthTotalPpp0Kib	INTEGER32	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	INTEGER32	Vnstat Today Rx for WWAN0 Interface in Kib
todayTxWwan0Kib	INTEGER32	Vnstat Today Tx for WWAN0 Interface in Kib
todayTotalWwan0Kib	INTEGER32	Vnstat Today Total Rx/Tx for WWAN0 Interface in Kib
yesterdayRxWwan0Kib	INTEGER32	Vnstat Yesterday Rx for WWAN0 Interface in Kib
yesterdayTxWwan0Kib	INTEGER32	Vnstat Yesterday Tx for WWAN0 Interface in Kib
yesterdayTotalWwan0Kib	INTEGER32	Vnstat Yesterday Total Rx/Tx for WWAN0 Interface in Kib
CurrMonthRxWwan0Kib	INTEGER32	Vnstat Current Month Rx for WWAN0 Interface in Kib
CurrMonthTxWwan0Kib	INTEGER32	Vnstat Current Month Tx for WWAN0 Interface in Kib
CurrMonthTotalWwan0Kib	INTEGER32	Vnstat Current Month Total Rx/Tx for WWAN0 Interface in Kib
PreMonthRxWwan0Kib	INTEGER32	Vnstat Previous Month Rx for WWAN0 Interface in Kib
PreMonthTxWwan0Kib	INTEGER32	Vnstat Previous Month Tx for WWAN0 Interface in Kib
PreMonthTotalWwan0Kib	INTEGER32	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	INTEGER32	Vnstat Today Rx for ETH0 Interface in Kib
todayTxEth0Kib	INTEGER32	Vnstat Today Tx for ETH0 Interface in Kib
todayTotalEth0Kib	INTEGER32	Vnstat Today Total Rx/Tx for ETH0 Interface in Kib
yesterdayRxEth0Kib	INTEGER32	Vnstat Yesterday Rx for ETH0 Interface in Kib
yesterdayTxEth0Kib	INTEGER32	Vnstat Yesterday Tx for ETH0 Interface in Kib
yesterdayTotalEth0Kib	INTEGER32	Vnstat Yesterday Total Rx/Tx for ETH0 Interface in Kib
CurrMonthRxEth0Kib	INTEGER32	Vnstat Current Month Rx for ETH0 Interface in Kib
CurrMonthTxEth0Kib	INTEGER32	Vnstat Current Month Tx for ETH0 Interface in Kib
CurrMonthTotalEth0Kib	INTEGER32	Vnstat Current Month Total Rx/Tx for ETH0 Interface in Kib
PreMonthRxEth0Kib	INTEGER32	Vnstat Previous Month Rx for ETH0 Interface in Kib
PreMonthTxEth0Kib	INTEGER32	Vnstat Previous Month Tx for ETH0 Interface in Kib
PreMonthTotalEth0Kib	INTEGER32	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	INTEGER32	Vnstat Today Rx for ETH1 Interface in Kib
todayTxEth1Kib	INTEGER32	Vnstat Today Tx for ETH1 Interface in Kib
todayTotalEth1Kib	INTEGER32	Vnstat Today Total Rx/Tx for ETH1 Interface in Kib
yesterdayRxEth1Kib	INTEGER32	Vnstat Yesterday Rx for ETH1 Interface in Kib
yesterdayTxEth1Kib	INTEGER32	Vnstat Yesterday Tx for ETH1 Interface in Kib
yesterdayTotalEth1Kib	INTEGER32	Vnstat Yesterday Total Rx/Tx for ETH1 Interface in Kib
CurrMonthRxEth1Kib	INTEGER32	Vnstat Current Month Rx for ETH1 Interface in Kib
CurrMonthTxEth1Kib	INTEGER32	Vnstat Current Month Tx for ETH1 Interface in Kib
CurrMonthTotalEth1Kib	INTEGER32	Vnstat Current Month Total Rx/Tx for ETH1 Interface in Kib
PreMonthRxEth1Kib	INTEGER32	Vnstat Previous Month Rx for ETH1 Interface in Kib
PreMonthTxEth1Kib	INTEGER32	Vnstat Previous Month Tx for ETH1 Interface in Kib
PreMonthTotalEth1Kib	INTEGER32	Vnstat Previous Month Total Rx/Tx for ETH1 Interface in Kib

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.

Note: Status Tags may be defined for hardware not available on some models. For example, cellular fields are not available on Wired Router products, and some units may not have GPS fields updated.

Legend: Rare = 30 minutes, Sometimes = 5 minutes, Often = 30 seconds, Quickly = 5 seconds, Rapidly = 1 second

Initial offset of 1000 and type Analog Out

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	417=4.17, 317=3.17
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	
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	Often	
1302	Eth0_IP_b	Second Octet	Often	
1303	Eth0_IP_c	Third Octet	Often	
1304	Eth0_IP_d	Fourth Octet	Often	
1305	Eth0_Subnet_a	First Octet	Often	
1306	Eth0_Subnet_b	Second Octet	Often	
1307	Eth0_Subnet_c	Third Octet	Often	
1308	Eth0_Subnet_d	Fourth Octet	Often	

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	Often	
1312	Eth1_IP_b	Second Octet	Often	
1313	Eth1_IP_c	Third Octet	Often	
1314	Eth1_IP_d	Fourth Octet	Often	
1315	Eth1_Subnet_a	First Octet	Often	
1316	Eth1_Subnet_b	Second Octet	Often	
1317	Eth1_Subnet_c	Third Octet	Often	
1318	Eth1_Subnet_d	Fourth Octet	Often	
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	Often	
1322	ppp0_IP_b	Second Octet	Often	
1323	ppp0_IP_c	Third Octet	Often	
1324	ppp0_IP_d	Fourth Octet	Often	
1325	ppp0_Subnet_a	First Octet	Often	
1326	ppp0_Subnet_b	Second Octet	Often	
1327	ppp0_Subnet_c	Third Octet	Often	
1328	ppp0_Subnet_d	Fourth Octet	Often	
1329	ppp0_DHCP	NA	Often	NA, always 0
1330	ppp0_Link	Link Status	Often	0 = No Link, 1 = Link detected
1331	wwan0_IP_a	First Octet	Often	
1332	wwan0_IP_b	Second Octet	Often	
1333	wwan0_IP_c	Third Octet	Often	
1334	wwan0_IP_d	Fourth Octet	Often	
1335	wwan0_Subnet_a	First Octet	Often	
1336	wwan0_Subnet_b	Second Octet	Often	
1337	wwan0_Subnet_c	Third Octet	Often	
1338	wwan0_Subnet_d	Fourth Octet	Often	
1339	wwan0_DHCP	NA	Often	0 = Static IP, 1 = DHCP Assigned IP
1340	wwan0_Link	Link Status	Often	0 = No Link, 1 = Link detected
1341	br0_IP_a	First Octet	Often	
1342	br0_IP_b	Second Octet	Often	
1343	br0_IP_c	Third Octet	Often	
1344	br0_IP_d	Fourth Octet	Often	
1345	br0_Subnet_a	First Octet	Often	
1346	br0_Subnet_b	Second Octet	Often	
1347	br0_Subnet_c	Third Octet	Often	
1348	br0_Subnet_d	Fourth Octet	Often	

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	

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 a1 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 -dBm	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	