



# FlexEdge™ DA50N Gateway

Software Guide | March 2020

LP1114 | Revision A

## **COPYRIGHT**

©2020 Red Lion Controls, Inc. All rights reserved. Red Lion and the Red Lion logo are registered trademarks of Red Lion Controls, Inc. All other company and product names are trademarks of their respective owners.

## **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.

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: 8 am-6 pm Eastern Standard Time  
(UTC/GMT -5 hours)

### **ASIA-PACIFIC**

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

### **EUROPE**

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

Website: [www.redlion.net](http://www.redlion.net)  
Support: [support.redlion.net](http://support.redlion.net)

# Table of Contents

<b>Preface</b> .....	7
Trademark Acknowledgments.....	7
Document History and Related Publications.....	7
Additional Product Information.....	7
<b>Chapter 1 Accessing the Web User Interface</b> .....	<b>9</b>
Configure Using AutoNet Method.....	9
Setup PC IP Address.....	9
Open the Control Panel.....	9
Access Network and Settings.....	10
Access Network Connection Settings.....	10
Access Local Area Connection.....	10
Open Properties.....	11
Access Internet Protocol Properties.....	11
Installing RNDIS Driver for Ethernet Connectivity Over USB.....	13
Accessing the Red Lion Web Server.....	15
DA50N Login Instructions.....	15
<b>Chapter 2 Cellular Connections</b> .....	<b>17</b>
Cellular Configuration.....	17
Cellular Interface Configuration.....	18
Set the User Name, Password, and APN.....	18
Provisioning.....	19
Verify Cellular Connectivity.....	19
Cellular Connectivity Troubleshooting.....	20
<b>Chapter 3 Web User Interface</b> .....	<b>25</b>
Web User Interface Introduction.....	25
Organization.....	25
Status Tab.....	25
Summary.....	25
Easy Config Wizard.....	26
Network.....	29
ARP Cache.....	29
Firewall Rules.....	29
Interfaces.....	30
Routing Tables.....	31
Socket Statuses.....	32
Traffic.....	34
Diagnostics.....	34
Ping.....	34
Traffic Capture.....	35

- Socket Test..... 36
- Traceroute ..... 37
- System Info ..... 37
- Syslog..... 38
- Gather Stats..... 40
- Admin Tab..... 41
  - Access Settings..... 41
  - System Time ..... 43
  - Certificate Manager ..... 44
  - Firmware Update..... 46
  - Configuration Manager ..... 47
  - Package Installation..... 48
  - Factory Defaults/Reboot..... 49
  - Job Control..... 50
- Network Tab..... 52
  - Cellular Connection ..... 52
    - Sled Cellular Configuration..... 52
    - Provisioning..... 56
  - Interfaces..... 57
    - Ethernet Port 1 (eth0) and Ethernet Port 2 (eth1) – (Network Interfaces)..... 57
    - Sled Ethernet Interfaces..... 63
    - Wi-Fi (WLAN) ..... 68
    - USB..... 71
    - IPv6..... 72
  - Firewall..... 73
    - General Settings..... 73
    - ACL Rules..... 77
    - Masquerade/NAT/DMZ Rules..... 81
    - Port Allow/Forwarding Rules..... 87
  - Tunneling ..... 90
    - GRE..... 90
    - IPSec..... 92
    - IPSec/L2TP ..... 98
  - DNS Settings..... 102
  - Static Routes..... 103
  - TCP Global Settings..... 105
- Services Tab ..... 107
  - DHCP Server..... 107
  - DHCP Relay ..... 111
  - Dynamic DNS..... 114
  - SN Proxy Settings..... 114

Sixview Manager .....	115
GPS Settings .....	118
SSH/TELNET Server .....	123
SSL Connections .....	124
SSL Client.....	124
SSL Server .....	127
SNMP Agent .....	130
Ping Alive .....	131
Crimson Connect.....	133
Email Client.....	142
SMS Handling.....	144
FTP Server.....	146
SD Card Manager.....	150
Serial IP .....	152
Automation Tab .....	162
Serial Ports.....	162
Tags.....	163
Data Logger.....	166
I/O Settings.....	170
I/O Control.....	170
Test I/O .....	172
Advanced Tab .....	174
IP Fallback .....	174
IP Transparency.....	176
Out-of-Band Mgt.....	181
VRRP (Virtual Router Redundancy Protocol).....	183
Expert Mode .....	185
Configure Sub-Systems.....	185
Predefined Interface Names .....	186
GWLNX .....	186
Connect Table Configuration.....	186
Install Configuration .....	191
Install Application.....	191
IP Destinations.....	191
CLI Status.....	193
GWLNX Status.....	194
GWLNX Log.....	195
About.....	196
Events.....	197
<b>Appendix A .....</b>	<b>209</b>
RED-LION-RAM.MIB Contents.....	209

**Appendix B.....221**  
IODB Status Module.....221  
**Appendix C.....225**  
SMS Handler Commands.....225

# Preface

This software guide provides guidance on how to use the FlexEdge™ DA50N. 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.

This guide is intended to be used by personnel responsible for configuring and commissioning DA50N devices for use in visualization, monitoring, and control applications. Users of this document are urged to heed warnings and cautions used throughout the document.

## Trademark Acknowledgments

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

- AT&T® is a registered trademark of AT&T Intellectual Property II., L.P.
- Ethernet™ is a registered trademark of Xerox Corporation.
- Google® and Google Maps™ mapping service are registered trademark of Google LLC.
- Microsoft®, Windows®, Windows 7®, and Windows 10® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Verizon Wireless® is a trademark of Verizon Trademark Services LLC.

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. Tech Notes and/or product addendums will be provided as needed between major releases to describe any new information or document changes.

The latest online version of this document can be accessed through the Red Lion website at: <https://www.redlion.net/support/documentation/user-manuals>.

## Additional Product Information

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





# Chapter 1 Accessing the Web User Interface

There are three connection methods available for first time connection to configure your new DA50N.

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

## Set Up

Connect a CAT-5 or CAT-6 Ethernet cable between the local PC and the DA50N's Ethernet port(s).

**Note:** If the Ethernet port's green LED is lit, this indicates that the connection is running at 100 Mb speed. If the Ethernet port's green LED is not lit, this indicates that the connection is running at 10 Mb speed. The yellow LED indicates the "link" status of the connection. Yellow steady = Link established. Yellow flashing = Data packets are being transferred.

## Configure Using AutoNet Method

When using AutoNet, connect Ethernet Port 1 (eth0) to any Ethernet network or directly to a PC. It will discover other DHCP networks and will either join automatically or provide a DHCP address to the connected PC.

Inspect the product label on your unit to find the field "MAC1 id" and notice the last 6 digits or letters.

If your MAC address was 01-02-03-1A-2B-3C, then the unit can be accessed by entering <https://da50n-1A2B3C.local> in your browser.

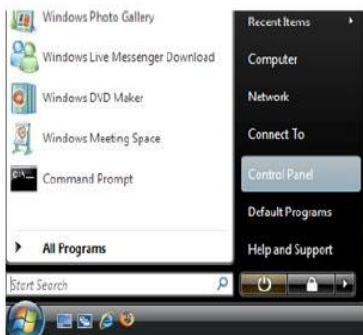
Once you configure your Ethernet port for use in production, AutoNet will be automatically disabled. If AutoNet does not seem to be working in your environment, you can always fall back to the other supported methods of access described in the following sections.

## Setup PC IP Address

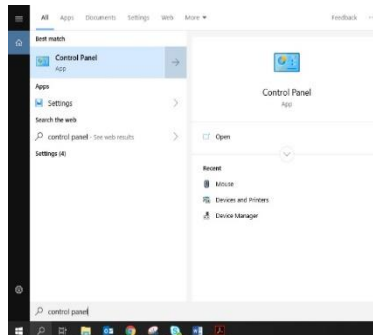
### Open the Control Panel

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

Windows 7

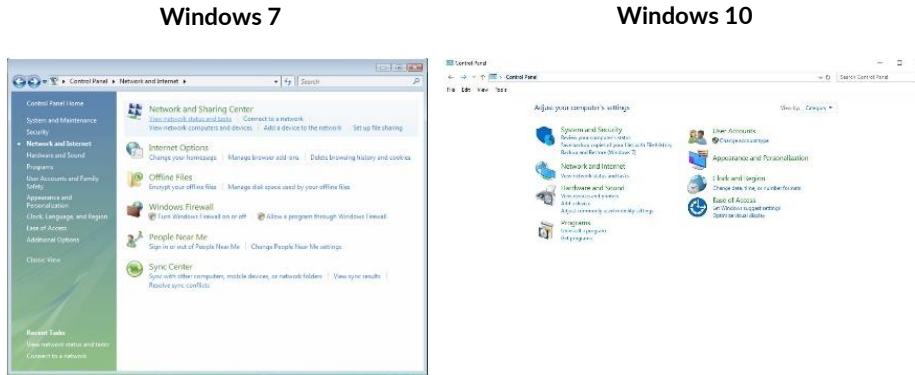


Windows 10



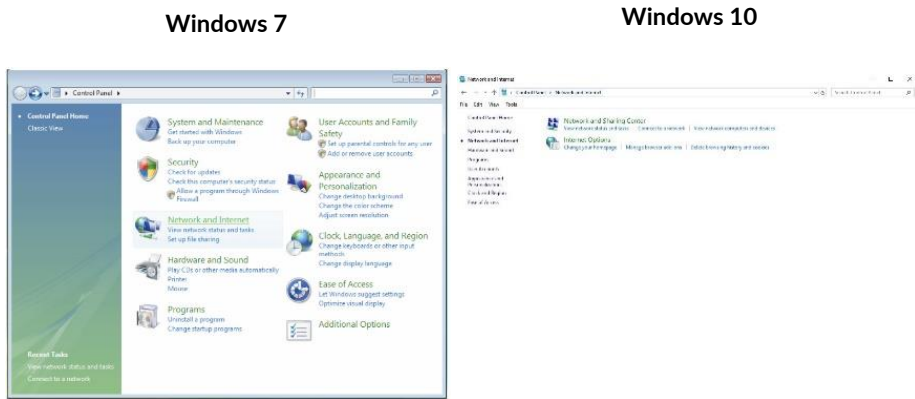
## Access Network and Settings

Click on the link to access network and Internet settings  
Windows 7 – “Network and Internet”  
Windows 10 – “Control Panel”  
The displays should be similar to the following:



## Access Network Connection Settings

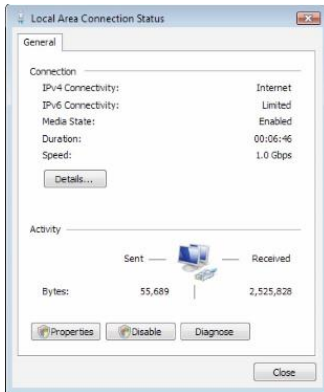
Click on the link to access network connection settings  
Windows 7 – “Network and Internet”  
Windows 10 – "Network and Internet"  
The display should look similar to the following.



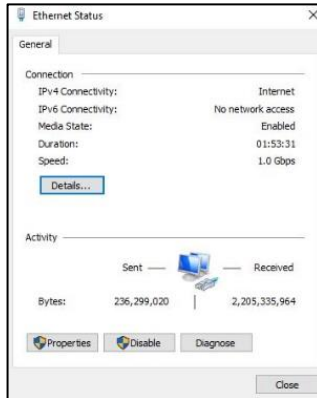
## Access Local Area Connection

Click on the link to access the local area connection.  
Windows 7 – “View Status” next to Local Area Connection.  
Windows 10 – “View network status and tasks” underneath Network and Sharing Center and click on “Ethernet”.  
The display should look similar to the following.

Windows 7



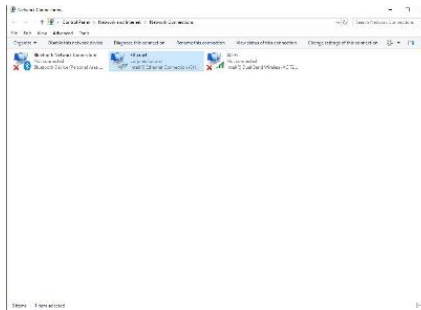
Windows 10



Windows 7



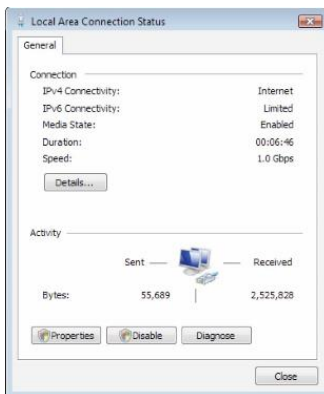
Windows 10



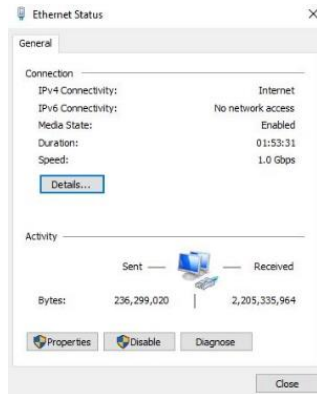
## Open Properties

Click on the *Properties* button (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:

Windows 7



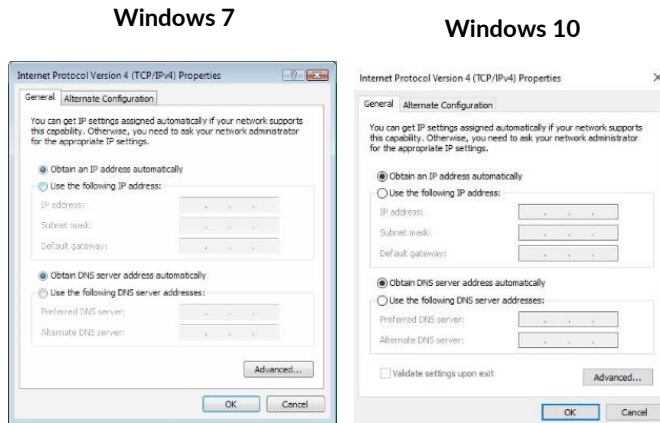
Windows 10



## Access Internet Protocol Properties

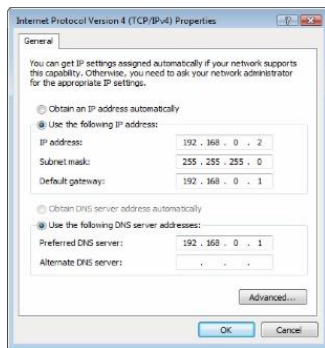
Click on the Internet Protocol to highlight.  
Windows 7 - "Internet Protocol Version 4 (TCP/IPv4)"  
Windows 10 - "Internet Protocol Version 4 (TCP/IPv4)"

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



### METHOD 1: PC to Ethernet Port 1

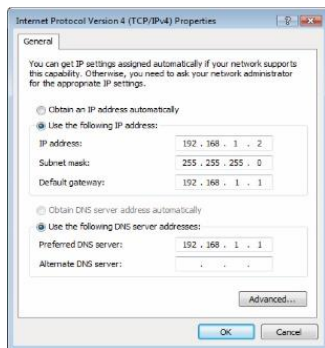
Use the following IP address and fill in the blank fields with the information below.



Click OK.  
The previous screen appears.  
Click OK.

### METHOD 2: PC to Ethernet Port 2

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



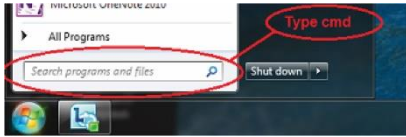
Click OK.  
The previous screen appears.  
Click OK.

## Test the Connection

Verify that you are connected to the DA50N.

Open a Command Prompt window on your laptop.

Window 7→Start→Search window just above the Start icon, type in cmd, wait for Windows 7 to locate the program and click on the cmd program it finds.



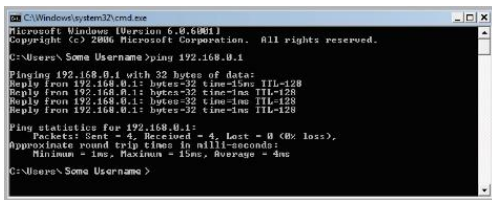
Windows 10→search window beside the Start icon, type in cmd, wait for Windows 10 to locate the program and click on the cmd program it finds.



Verify connectivity to the DA50N by running a "ping" to the IP address of the Ethernet port you are connected to.

## METHOD 1: PC to Ethernet Port 1 or Ethernet Port 2

Type in "ping 192.168.0.1" (Ethernet Port 1) or "ping 192.168.1.1" (Ethernet Port 2) and then press the ENTER key. The display should look similar to the following:



This shows the connection is up and functioning.

## Installing RNDIS Driver for Ethernet Connectivity Over USB

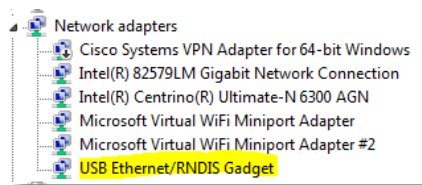
This section outlines the required method to manually install the correct RNDIS driver for DA50N. This will enable the unit to connect via USB and behave as an Ethernet device.

**Note:** Windows 10 RNDIS support is limited. If issues are encountered and a Windows 7 device is not available for RNDIS configuration, Ethernet-based setup is recommended.

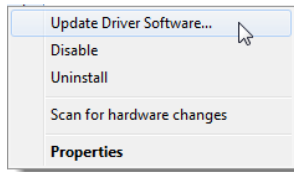
Power on the DA50N and connect to your Windows PC via the USB Type B cable.

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

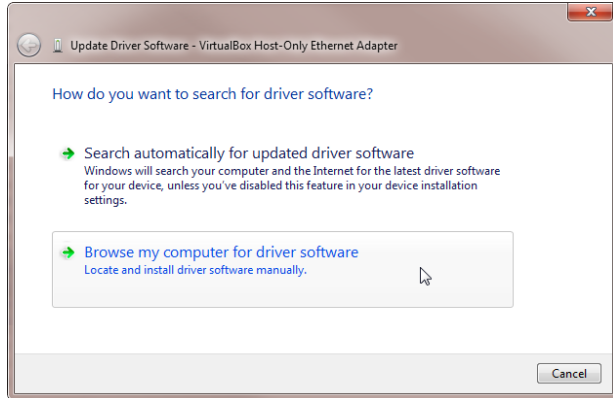
Most Windows systems will automatically locate and install a driver. The device would appear in the Windows Device Manager as seen below:



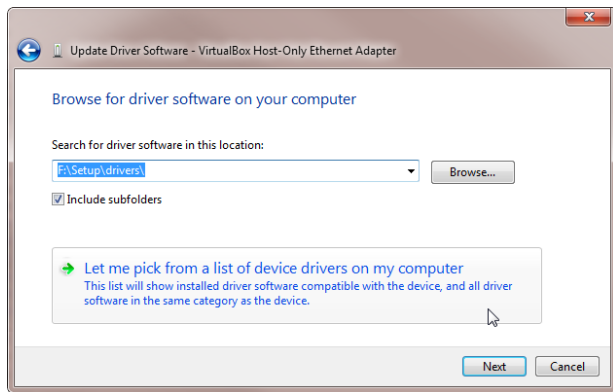
Right-click on the USB Ethernet/RNDIS Gadget adapter, and select Update Driver Software.



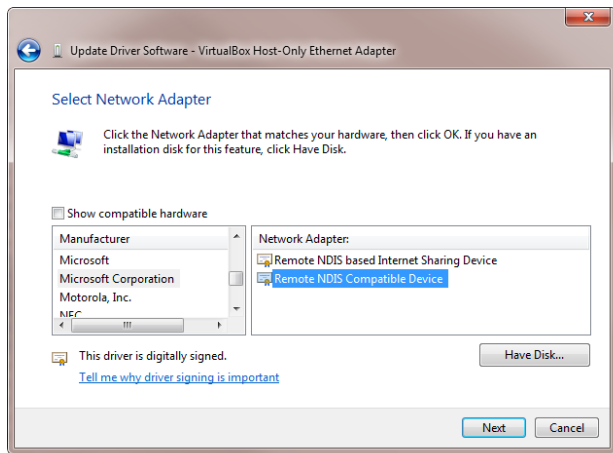
Select “Browse my computer for driver software”:



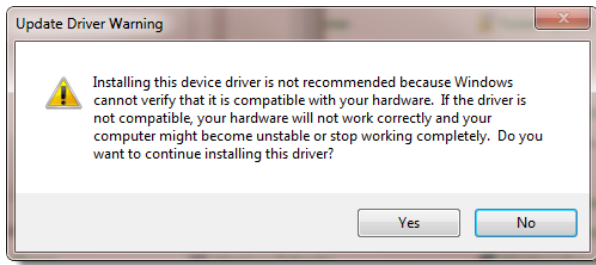
Select “Let me pick from a list”...



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



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



Once the install is complete, click on Close.

The USB Ethergadget driver should now be loaded and you should be able to access the DA50N via USB/Ethernet at 192.168.111.1:10001.

## Accessing the Red Lion Web Server

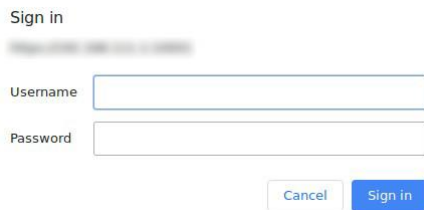
Open a web browser<sup>1</sup> and enter the following in the address bar.

METHOD 1 (Ethernet Port 1): <https://192.168.0.1:10001>

METHOD 2 (Ethernet Port 2): <https://192.168.1.1:10001>

METHOD 3 (USB): <https://192.168.111.1:10001>

You will receive a login pop-up screen.

A screenshot of a login pop-up screen. At the top, it says 'Sign in'. Below that, there is a blurred line of text. Underneath, there are two input fields: 'Username' and 'Password'. At the bottom, there are two buttons: 'Cancel' and 'Sign in'.

## DA50N Login Instructions

For the User Name, enter: **admin** (all lowercase)

For Password, enter the **last six digits of the serial number**, located on the product label (all lowercase).

Upon successfully logging in, the following screen appears:

**Note:** The following information can be used for all DA50N Gateway devices.

---

<sup>1</sup> Browsers currently supported: Internet Explorer 10 & 11, Chrome 42 through 75.

The screenshot shows the web interface for a DA50N-d35004 device. At the top, there is a navigation bar with menu items: Status, Admin, Network, Services, Automation, Advanced, and Events. A Logout button is in the top right corner. Below the navigation bar, the device name "DA50N-d35004" is displayed. Underneath, there is a "System Information" section with a table of device details and an "Easy Config Wizard" button. The "Physical Interface Status" section contains a table listing the status of various interfaces.

Interface	Configuration	IP Address	Link Status
Ethernet Port 1 (eth0)	Enabled	192.168.1.100	Up
Ethernet Port 2 (eth1)	Enabled	192.168.1.101	Down
USB (usb0)	Enabled	192.168.1.102	Up

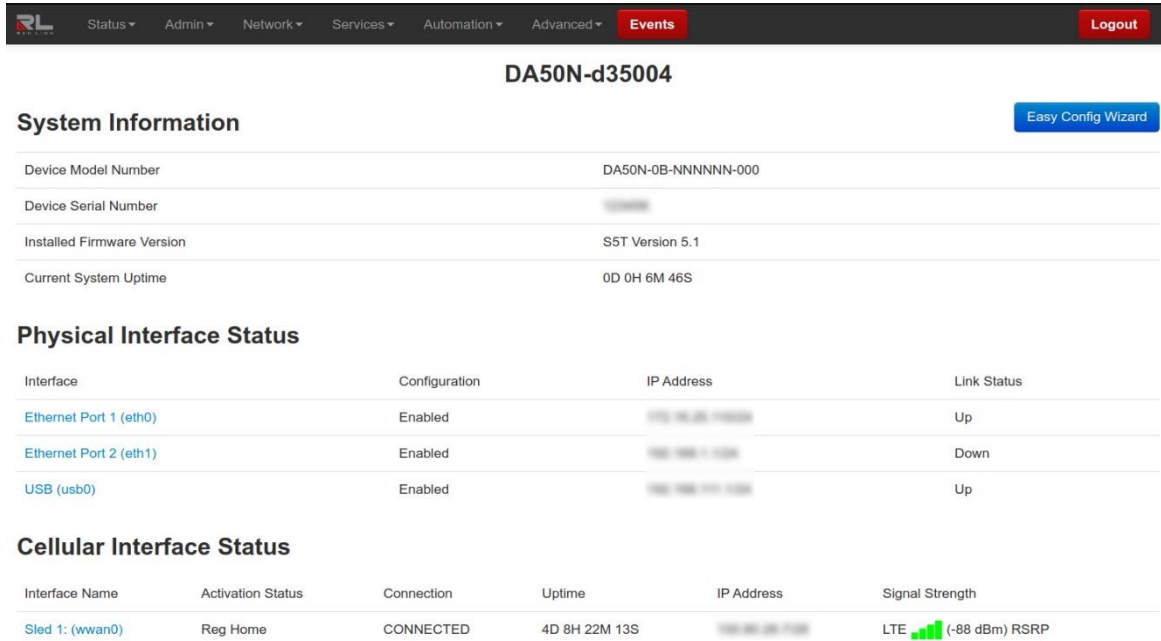
At this point, you are connected to the DA50N and can configure it to meet your needs.



# Chapter 2 Cellular Connections

## Cellular Configuration

Cellular connectivity is obtained through the use of a cellular sled accessory.



Your DA50N Gateway device may have a cellular sled accessory that has been detected and may be configured for the intended carrier. If you are using a carrier that supports the use of an Access Point Name (APN), you may have to set your specific APN manually, as covered in the next section. For GSM and LTE service, carriers may provide custom APNs for static IP addresses of VPN scenarios depending on the type of account.

The cellular sled accessory supports switching between multiple carriers. Navigate to the Network→Cellular Connection→Provisioning screen to verify your carrier has been provisioned correctly for these models.

Navigate through the Web UI menu to Networking→Cellular Connection→Sled Cellular Configuration to see the screen shown in the [Cellular Interface Configuration](#) section. Carriers such as Verizon and AT&T® will require a SIM card be inserted into the unit and an APN code to be entered to confirm you are the verified user of that SIM card. Be sure to only insert and remove the SIM card while the unit is powered off.

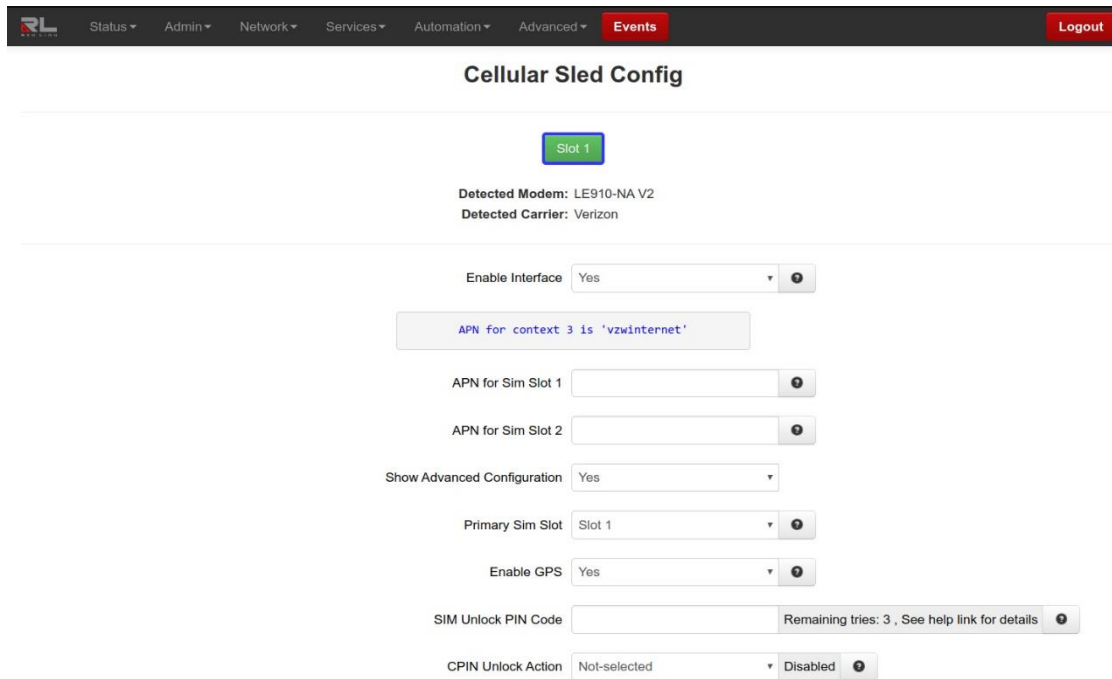
You can verify your cellular connectivity by viewing the Status Summary page of the web UI screen and observe if the Cellular Interface status shows an IP address. On the Home screen you should see: Interface, Activation, Connection, Uptime, IP Address and Signal Strength. If you do not see an IP address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

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

CDMA	HSPA/LTE
Running – Connection/Activation is running.	Not Reg – Modem is not registered.

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

## Cellular Interface Configuration



On the Cellular Configuration page, the Slot 1 button will be black if there is no sled installed or detected, red if detected but not enabled, or green if detected and enabled.

Select Yes to enable the interface so it becomes active after the new settings are applied and upon subsequent system start-up. Select No to disable the cellular connection feature. More information on setting up the unit’s cellular connection can be found in the [Cellular Connection](#) section.

### Set the User Name, Password, and APN

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

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

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

## Provisioning

This page is used to select the correct carrier profile and firmware images for the cellular module to authenticate on the LTE carrier networks. Contact Technical Support for the latest update package for your carrier if you are using one of these models. Navigate to Network→Cellular Connection→Provisioning.

The screenshot shows the 'Cellular Sled Provisioning' page in a web browser. At the top, there is a navigation bar with a logo on the left and menu items: Status, Admin, Network, Services, Automation, Advanced, Events, and Logout. The main heading is 'Cellular Sled Provisioning'. Below this, there is a 'Slot 1' button. The main content area displays the following information: Module Model: LE910-NA V2, SIM Carrier: Verizon, Detected IMEI: 358148061063025, Module Firmware Version: 20.00.006, Firmware Slot: 2, Dual Firmware: Yes, SIM ID: 8914800001636923731, SIM IMSI: 311480165354055, SIM Slot: 1, MDN Number: 17178731251, and Activation Status: Registered, Home Network. Below this information is a 'Manage Module Firmware' section. It shows 'Active: Verizon' and a 'Select Firmware Version' dropdown menu currently set to 'None Selected...'. A note below the dropdown states: 'Note: If you recently installed or reflashed a firmware package, you may need to update this list by clicking Refresh below'. There are two input fields for 'Update APN for Sim Slot 1 (optional)' and 'Update APN for Sim Slot 2 (optional)'. At the bottom of this section are 'Update Module' and 'Delete' buttons. Below the 'Manage Module Firmware' section is a 'Show Diagnostic Information' button, and at the very bottom is a 'Show Cellular Module Status' button.

## Verify Cellular Connectivity

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

The screenshot shows the web interface for a DA50N-d35004 device. At the top, there is a navigation bar with menu items: Status, Admin, Network, Services, Automation, Advanced, Events, and Logout. Below the navigation bar, the device model number 'DA50N-d35004' is displayed. A blue button labeled 'Easy Config Wizard' is located in the top right corner.

**System Information**

Device Model Number	DA50N-0B-NNNNNN-000
Device Serial Number	[REDACTED]
Installed Firmware Version	S5T Version 5.1
Current System Uptime	0D 0H 6M 46S

**Physical Interface Status**

Interface	Configuration	IP Address	Link Status
Ethernet Port 1 (eth0)	Enabled	[REDACTED]	Up
Ethernet Port 2 (eth1)	Enabled	[REDACTED]	Down
USB (usb0)	Enabled	[REDACTED]	Up

**Cellular Interface Status**

Interface Name	Activation Status	Connection	Uptime	IP Address	Signal Strength
Sled 1: (wwan0)	Reg Home	CONNECTED	4D 8H 22M 13S	[REDACTED]	LTE  (-88 dBm) RSRP

As shown, the DA50N is receiving good signal from the cellular network, it is connected and has been issued an IP address.

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

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

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

If you were able to successfully access the Internet or your corporate network, your DA50N is up and running. You have successfully configured your cellular sled accessory and you may skip the troubleshooting section.

## Cellular Connectivity Troubleshooting

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

If you are reading this section, you have followed all previous instructions and your DA50N is not communicating. This section will provide additional information to isolate the cause of difficulties.

### Cellular Reception

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

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

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

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

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

### Important Note About Cellular Antennas

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

### Diversity/MIMO

This port is used for MIMO for LTE connections. MIMO is a transmission technique that consists of using two separate antennas to achieve the most robust cellular signal possible. This antenna is required for compliance with LTE MIMO operation.

To get the best performance, this second antenna should be placed at a minimum of 5/8 of a wavelength away from the other antenna. Therefore, the minimum spacing for antennas in the 800 MHz frequency is  $5/8 * 13.5" = 8.5"$ . Orienting the antennas differently from one another may also improve performance, particularly when the antennas are close together.

### Verifying IP Connectivity

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

Navigate to the Web UI Status screen shown below:

The screenshot shows the Red Lion Web UI for device DA50N-d35004. The navigation bar includes Status, Admin, Network, Services, Automation, Advanced, Events, and Logout. The main content is divided into three sections:

#### System Information

Device Model Number	DA50N-0B-NNNNNN-000
Device Serial Number	[REDACTED]
Installed Firmware Version	S5T Version 5.1
Current System Uptime	0D 1H 17M 56S

#### Physical Interface Status

Interface	Configuration	IP Address	Link Status
Ethernet Port 1 (eth0)	Enabled	[REDACTED]	Up
Ethernet Port 2 (eth1)	Enabled	[REDACTED]	Down
USB (usb0)	Enabled	[REDACTED]	Up

#### Wi-Fi Interface Status

Interface	Configuration	SSID	IP Address	Signal Strength
Wi-Fi (wlan0s1)	Enabled (Client)	wireless_ap	[REDACTED]	[Signal Icon] (-26 dBm)

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



### Minimal Reception

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

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

#### Cellular Interface Status

Interface Name	Activation Status	Connection	Uptime	IP Address	Signal Strength
Sled 1: (wwan0)	Reg Home	Unknown	N/A	192.168.88.178	LTE  (-88 dBm) RSRP

If you refresh this screen every few minutes and notice that the IP address is changing frequently, it is possible that the DA50N is connecting to the network and obtaining an IP address and then the connection to the cellular network is being dropped. When the connection is re-established, the device is then issued a different IP address.

### Authentication Issues

If you have a reasonable amount of signal, your radio connection to the network may be just fine. The problem may lie in logging onto the cellular network.

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

**Cellular Sled Config**

Slot 1

Detected Modem: LE910-NA V2  
Detected Carrier: Verizon

Enable Interface: Yes

APN for context 3 is 'vzwinternet'

APN for Sim Slot 1

APN for Sim Slot 2

Show Advanced Configuration: Yes

Primary Sim Slot: Slot 1

Enable GPS: Yes

SIM Unlock PIN Code: Remaining tries: 3 . See help link for details

CPIN Unlock Action: Not-selected Disabled

**CPIN / PUK Status**  
CPIN: Disabled  
Status: Available  
Extended Status: N/A

Roaming: Auto

Authentication Type: CHAP

User Name: asdfgh

Password: .....

Network Speed: 3G

P-t-P Interface: No

MTU: 1500

Sync Time: Yes

Use Default Route: Yes

Use Peer DNS: Yes

Show Details Show CSQ History

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

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



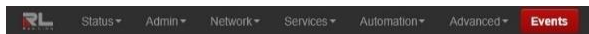


# Chapter 3 Web User Interface

## Web User Interface Introduction

### 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 DA50N. This tab is organized into six (6) sections: Summary, Easy Config, Network, Diagnostics, Syslog and Gather Stats.

**Admin:** The Admin tab is used to configure how the DA50N is accessed, update the firmware, reset the system defaults, set the system time and reboot the DA50N remotely. This tab is organized into eight (8) sections: Access Settings, System Time, Certificate Manager, Firmware Update, Configuration Manager, Package Installation, Factory Defaults/Reboot and Job Control.

**Network:** The Network tab is used to configure settings that connect the DA50N to external interfaces. The Network tab is organized into seven (7) major categories: Cellular Connection, Interfaces, Firewall, Tunneling, DNS Settings, Static Routes, and TCP Global Settings.

**Services:** The Services tab is used to configure the various features of the DA50N. These services include DHCP Server, DHCP Relay, Dynamic DNS, SN Proxy Settings, SixView Manager®, GPS Settings, SSH/TELNET Server, SSL Connections, SNMP Agent, Ping Alive, Crimson Connect, Email Client, SMS Handling, SD Card Manager and Serial IP.

**Automation:** The Automation tab contains all aspects of managing your I/O. The Automation tab is organized into the following sections: Serial Ports, Tags, Data Logger, and I/O settings.

**Advanced:** The Advanced Tab is used to configure the advanced features of the DA50N, which include IP Fallback, IP Transparency, Out-of-Band Mgt, VRRP, Expert Mode, GWLNX, and About.

**Events:** Events are used to apply a series of logic checks to a register(s) that allows the user to program an action based on the content of a specific register.

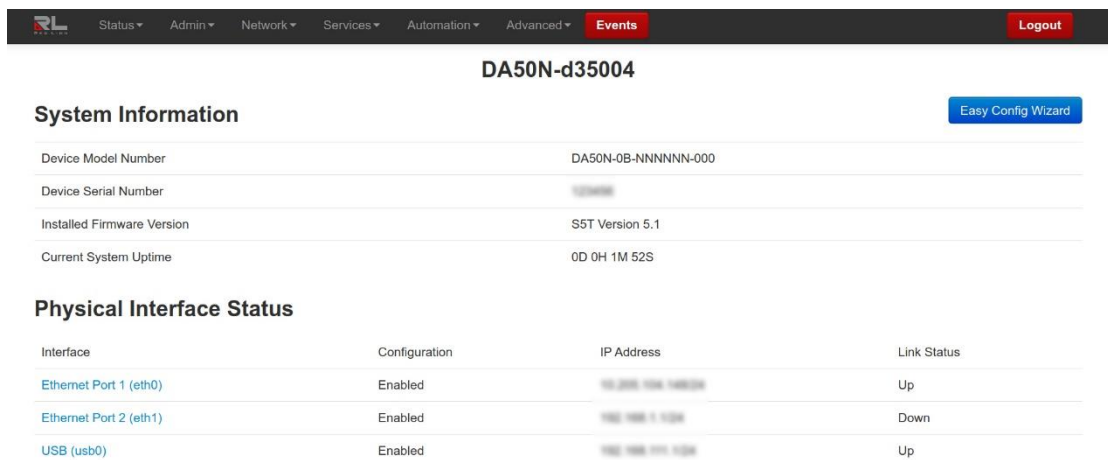
All tabs are described further in the guide along with functionality of each dialog window.

### Status Tab

The Status Tab allows you to review the state of the DA50N 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'.

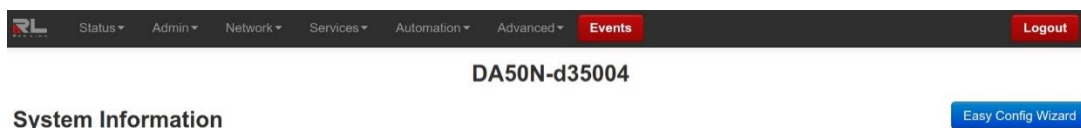
### Summary

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.

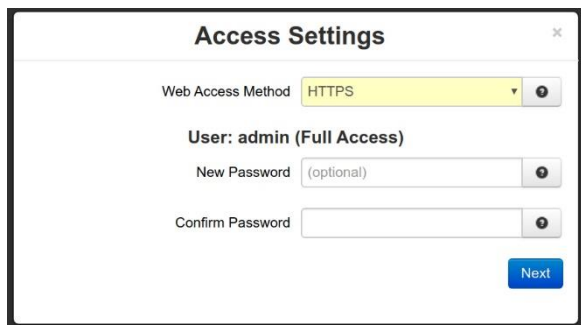


## Easy Config Wizard

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



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



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

**HTTPS/Redirect:** Use this option if you are currently using HTTP method and want to redirect existing users to the new HTTPS port.

**Note:** HTTPS modes are recommended which use data encryption to provide a secure connection.

**New Password:** Enter the new password in this field.

**Password Limitation Note:** Password Limitation, Single quote (') character is not a valid character for a 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)

**Current Password:** Enter your current password. (Required)

Click on the *Next* button. The Ethernet Port 1 Settings dialog window will open:



**Obtain Network Addresses via DHCP:** Select Yes to allow the interface to obtain address information via a DHCP server. This 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 server.

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

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

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

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

**Recommended Setting:** This address should have been provided by your Network Administrator. It must be an address valid for the network described by the value contained in the **Enter 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.

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.

**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 **Enter Subnet Mask** field and must not conflict with any other device on the target network.

**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.

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.

**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 **Enter Subnet Mask** field and must not conflict with any other device on the target network.

Once the desired settings have been entered into the Ethernet Port 1 Settings dialog window, click on the **Next** button and the following Ethernet Port 2 (eth1) Settings dialog window appears:



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

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

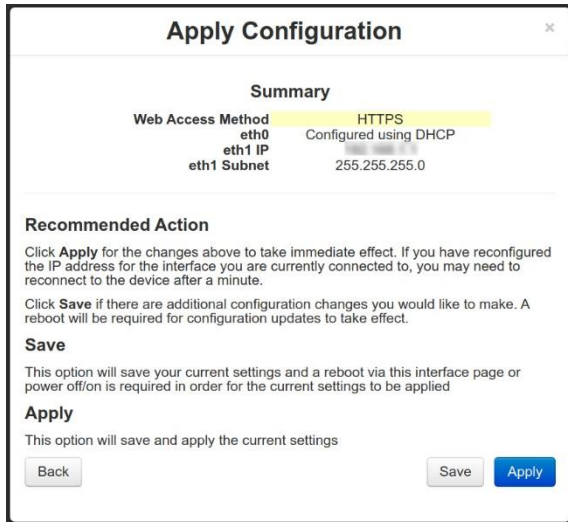
For example, if a netmask is 255.255.255.0 and the IP address assigned to the device is 192.168.1.3, then the range of valid addresses is 192.168.1.1 through 192.168.1.254 as 192.168.1.0 is the value reserved for the network and 192.168.1.255 is the value reserved for the broadcast address.

**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 **Enter Subnet Mask** field and must not conflict with any other device on the target network.

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

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

Once the desired settings have been entered in the Ethernet Port 2 Settings dialog window, click on the **Next** button and the following Apply Configuration dialog window appears:



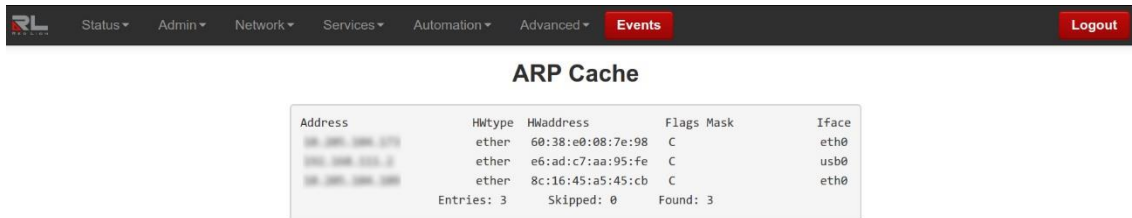
Click on *Back*, *Save* or *Apply* (see explanation of each setting in dialog window above).

## 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 that 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 DA50N. When you click on the ARP Cache menu item, the ARP Cache dialog window will open.



### Firewall Rules

The Firewall Rules menu item displays a complete listing of the rules used within the firewall for the DA50N. If you are familiar with *iptables*, this will be of great use.

**Firewall Rules**

Subsystem Configured: Yes  
 Starts at Boot: Yes  
 Active: Yes

Chain INPUT (policy DROP 0 packets, 0 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination	
42	3627	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0	
0	0	DROP	tcp	--	ppp0	*	0.0.0.0/0	0.0.0.0/0	tcp dpts:0:19
0	0	DROP	tcp	--	wwan0	*	0.0.0.0/0	0.0.0.0/0	tcp dpts:0:19
0	0	SCAN	tcp	--	ppp0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x3F
0	0	SCAN	tcp	--	ppp0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x00
0	0	SCAN	tcp	--	wwan0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x3F
0	0	SCAN	tcp	--	wwan0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x00
0	0	FLAGS	tcp	--	ppp0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x29
0	0	FLAGS	tcp	--	ppp0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x3F
0	0	FLAGS	tcp	--	ppp0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x37
0	0	FLAGS	tcp	--	ppp0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x00
0	0	FLAGS	tcp	--	ppp0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x06/0x06
0	0	FLAGS	tcp	--	ppp0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x03/0x03
0	0	FLAGS	tcp	--	wwan0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x29
0	0	FLAGS	tcp	--	wwan0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x3F
0	0	FLAGS	tcp	--	wwan0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x37
0	0	FLAGS	tcp	--	wwan0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x3F/0x00
0	0	FLAGS	tcp	--	wwan0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x06/0x06
0	0	FLAGS	tcp	--	wwan0	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x03/0x03

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 DA50N.

## Interfaces

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

**Interface Information**

Summary

```

Settings for eth0:
Supported ports: [ TP AUI BNC MII FIBRE ]
Supported link modes:  10baseT/Half 10baseT/Full
                      100baseT/Half 100baseT/Full
Supported pause frame use: No
Supports auto-negotiation: Yes
Supported FEC modes: Not reported
Advertised link modes: 10baseT/Half 10baseT/Full
                      100baseT/Half 100baseT/Full
Advertised pause frame use: No
Advertised auto-negotiation: Yes
Advertised FEC modes: Not reported
Link partner advertised link modes: 10baseT/Half 10baseT/Full
                                   100baseT/Half 100baseT/Full
Link partner advertised pause frame use: Symmetric
Link partner advertised auto-negotiation: Yes
Link partner advertised FEC modes: Not reported
Speed: 100Mb/s
Duplex: Full
Port: MII
PHYAD: 0
Transceiver: external
Auto-negotiation: on
Supports Wake-on: d
Wake-on: d
Current message level: 0x00000000 (0)

Link detected: yes
Settings for eth1:
Supported ports: [ TP AUI BNC MII FIBRE ]
Supported link modes: 10baseT/Half 10baseT/Full
    
```

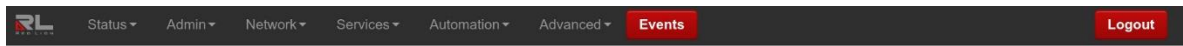


Details

```

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
   link/ether a8:10:87:d3:50:04 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.1/24 brd 192.168.1.255 scope global eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::aa10:87ff:fed3:5004/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
   link/ether a8:10:87:d3:50:06 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.2/24 brd 192.168.1.255 scope global eth1
       valid_lft forever preferred_lft forever
4: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1
   link/sit 0.0.0.0 brd 0.0.0.0
5: ip6tnl0@NONE: <NOARP> mtu 1452 qdisc noop state DOWN group default qlen 1
   link/tunne16 :: brd ::
6: usb0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 1e:dc:44:24:24:b5 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.3/24 brd 192.168.1.255 scope global usb0
       valid_lft forever preferred_lft forever
   inet6 fe80::1cdc:44ff:fe24:24b5/64 scope link
       valid_lft forever preferred_lft forever

```



Multicast

```

1: lo
   inet 224.0.0.252
   inet 224.0.0.1
   inet6 ff02::1
   inet6 ff01::1
2: eth0
   link 33:33:00:00:00:01
   link 01:00:5e:00:00:01
   link 33:33:ff:d3:50:04
   link 33:33:00:00:00:fb
   link 01:00:5e:00:00:fb
   link 01:80:c2:00:00:0e static
   link 01:80:c2:00:00:03 static
   link 01:80:c2:00:00:00 static
   link 01:00:5e:00:00:fc
   inet 224.0.0.252
   inet 224.0.0.251
   inet 224.0.0.1
   inet6 ff02::fb
   inet6 ff02::1:ffd3:5004
   inet6 ff02::1
   inet6 ff01::1
3: eth1
   link 33:33:00:00:00:01
   link 01:00:5e:00:00:01
   link 01:00:5e:00:00:fb
   link 01:80:c2:00:00:0e static
   link 01:80:c2:00:00:03 static
   link 01:80:c2:00:00:00 static
   link 01:00:5e:00:00:fc
   inet 224.0.0.252
   inet 224.0.0.251
   inet 224.0.0.1
   inet6 ff02::1
   inet6 ff01::1

```

The Summary table displays a brief description of the interfaces of the DA50N.  
 The Details table displays a system specific description of the interfaces on the DA50N.  
 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.

**Routing Tables**

---

**Standard System Routing Table**

Kernel IP routing table						
Destination	Gateway	Genmask	Flags	Metric	Ref	Use Iface
0.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0 eth0
0.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0 eth1
0.0.0.0	0.0.0.0	255.255.255.0	U	0	0	0 usb0

---

**Policy Routing Table**

```

** ip rule show
0:      from all lookup local
4:      from 192.168.1.0/24 lookup usb0
10:     from all lookup main
11:     from 192.168.1.0/24 lookup eth0
12:     from 192.168.1.0/24 lookup eth1
32766:  from all lookup main
32767:  from all lookup default

** ip route show table eth0
default via 192.168.1.1 dev eth0

** ip route show table eth1
192.168.1.0/24 dev eth1 scope link src 192.168.1.1 linkdown

** ip route show table usb0
prohibit default
192.168.1.0/24 dev usb0 scope link
    
```

The Standard System Routing Table displays the current routes and static routes that have been configured for the DA50N.

The Policy Routing Table displays information on the policy rules, the route tables for each individual interface and the general routes for the DA50N.

**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 that 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).




Status ▾
Admin ▾
Network ▾
Services ▾
Automation ▾
Advanced ▾
Events
Logout

### Socket Statuses

#### TCP Only

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.1:2947	*.*.*.*:*	LISTEN	2765/gpsd
tcp	0	0	0.0.0.0:7785	*.*.*.*:*	LISTEN	4280/gmu_listener
tcp	0	0	0.0.0.0:80	*.*.*.*:*	LISTEN	3996/lighttpd-gau
tcp	0	0	0.0.0.0:53	*.*.*.*:*	LISTEN	3971/dnsmasq
tcp	0	0	0.0.0.0:22	*.*.*.*:*	LISTEN	3907/ssh
tcp	0	0	0.0.0.0:23	*.*.*.*:*	LISTEN	3941/xinetd
tcp	0	0	127.0.0.1:56948	127.0.0.1:2947	ESTABLISHED	2771/gpsc
tcp	0	0	127.0.0.1:2947	127.0.0.1:56948	ESTABLISHED	2765/gpsd
tcp	0	0	:::3996	:::*	LISTEN	3996/lighttpd-gau
tcp	0	0	:::3996	:::*	LISTEN	3996/lighttpd-gau
tcp	0	0	:::53	:::*	LISTEN	3971/dnsmasq
tcp	0	0	:::22	:::*	LISTEN	3907/ssh
tcp	0	0	:::FFFF:::280:284:3996	:::FFFF:::280:284:56948	ESTABLISHED	3996/lighttpd-gau
tcp	0	0	:::FFFF:::280:284:3996	:::FFFF:::280:284:56948	ESTABLISHED	3996/lighttpd-gau
tcp	0	0	:::FFFF:::280:284:3996	:::FFFF:::280:284:56948	ESTABLISHED	3996/lighttpd-gau
tcp	0	0	:::FFFF:::280:284:3996	:::FFFF:::280:284:56948	ESTABLISHED	3996/lighttpd-gau


Status ▾
Admin ▾
Network ▾
Services ▾
Automation ▾
Advanced ▾
Events
Logout

#### Conn Track

ipv4	2	tcp	0.110 TIME_WAIT src=08.285.284.189 dst=08.285.284.148 sport=58534 dport=443 src=08.285.284.148 dst=08.285.284.148
ipv4	2	tcp	0.432888 ESTABLISHED src=08.285.284.189 dst=08.285.284.148 sport=58549 dport=443 src=08.285.284.148 dst=08.285.284.148
ipv4	2	udp	17.58 src=08.285.284.111 dst=08.285.284.255 sport=138 dport=138 [CONNPL320] src=08.285.284.255 dst=08.285.284.111
ipv4	2	tcp	0.110 TIME_WAIT src=08.285.284.189 dst=08.285.284.148 sport=58534 dport=443 src=08.285.284.148 dst=08.285.284.148
ipv4	2	udp	17.5 src=08.285.284.111 dst=08.285.284.255 sport=138 dport=138 [CONNPL320] src=08.285.284.255 dst=08.285.284.111
ipv4	2	tcp	0.110 TIME_WAIT src=08.285.284.189 dst=08.285.284.148 sport=58534 dport=443 src=08.285.284.148 dst=08.285.284.148
ipv4	2	tcp	0.110 TIME_WAIT src=08.285.284.189 dst=08.285.284.148 sport=58534 dport=443 src=08.285.284.148 dst=08.285.284.148
ipv4	2	tcp	0.110 TIME_WAIT src=08.285.284.189 dst=08.285.284.148 sport=58534 dport=443 src=08.285.284.148 dst=08.285.284.148
ipv4	2	tcp	0.110 TIME_WAIT src=08.285.284.189 dst=08.285.284.148 sport=58534 dport=443 src=08.285.284.148 dst=08.285.284.148
ipv4	2	tcp	0.110 TIME_WAIT src=08.285.284.189 dst=08.285.284.148 sport=58534 dport=443 src=08.285.284.148 dst=08.285.284.148
ipv4	2	tcp	0.110 TIME_WAIT src=08.285.284.189 dst=08.285.284.148 sport=58534 dport=443 src=08.285.284.148 dst=08.285.284.148
ipv4	2	tcp	0.110 TIME_WAIT src=08.285.284.189 dst=08.285.284.148 sport=58534 dport=443 src=08.285.284.148 dst=08.285.284.148
ipv4	2	udp	17.4 src=08.285.284.111 dst=08.285.284.255 sport=138 dport=138 [CONNPL320] src=08.285.284.255 dst=08.285.284.111
ipv4	2	tcp	0.432888 ESTABLISHED src=08.285.284.189 dst=08.285.284.148 sport=58549 dport=443 src=08.285.284.148 dst=08.285.284.148
ipv4	2	udp	17.23 src=08.285.284.138 dst=08.285.284.255 sport=57621 dport=57621 [CONNPL320] src=08.285.284.255 dst=08.285.284.138
ipv4	2	tcp	0.429673 ESTABLISHED src=127.0.0.1 dst=127.0.0.1 sport=58549 dport=2947 src=127.0.0.1 dst=127.0.0.1
ipv4	2	tcp	0.110 TIME_WAIT src=08.285.284.189 dst=08.285.284.148 sport=58549 dport=443 src=08.285.284.148 dst=08.285.284.148
ipv4	2	tcp	0.110 TIME_WAIT src=08.285.284.189 dst=08.285.284.148 sport=58549 dport=443 src=08.285.284.148 dst=08.285.284.148
ipv4	2	udp	17.4 src=08.285.284.111 dst=08.285.284.255 sport=57621 dport=57621 [CONNPL320] src=08.285.284.255 dst=08.285.284.111
ipv4	2	udp	17.4 src=08.285.284.148 dst=08.285.284.255 sport=57621 dport=57621 [CONNPL320] src=08.285.284.255 dst=08.285.284.148

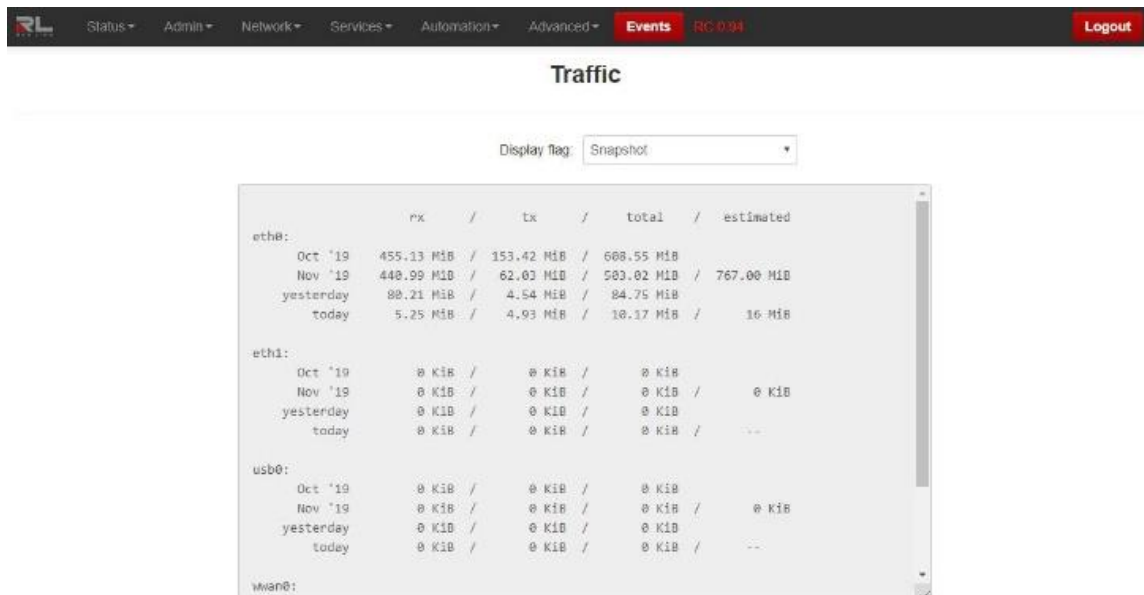
#### Socket Statuses All

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.1:2947	*.*.*.*:*	LISTEN	2765/gpsd
tcp	0	0	0.0.0.0:7785	*.*.*.*:*	LISTEN	4280/gmu_listener
tcp	0	0	0.0.0.0:80	*.*.*.*:*	LISTEN	3996/lighttpd-gau
tcp	0	0	0.0.0.0:53	*.*.*.*:*	LISTEN	3971/dnsmasq
tcp	0	0	0.0.0.0:22	*.*.*.*:*	LISTEN	3907/ssh
tcp	0	0	0.0.0.0:23	*.*.*.*:*	LISTEN	3941/xinetd
tcp	0	0	127.0.0.1:56948	127.0.0.1:2947	ESTABLISHED	2771/gpsc
tcp	0	0	127.0.0.1:2947	127.0.0.1:56948	ESTABLISHED	2765/gpsd
tcp	0	0	:::3996	:::*	LISTEN	3996/lighttpd-gau
tcp	0	0	:::3996	:::*	LISTEN	3996/lighttpd-gau
tcp	0	0	:::53	:::*	LISTEN	3971/dnsmasq
tcp	0	0	:::22	:::*	LISTEN	3907/ssh
tcp	0	402	:::FFFF:::280:284:3996	:::FFFF:::280:284:56948	ESTABLISHED	3996/lighttpd-gau
tcp	0	0	:::FFFF:::280:284:3996	:::FFFF:::280:284:56948	ESTABLISHED	3996/lighttpd-gau
tcp	0	0	:::FFFF:::280:284:3996	:::FFFF:::280:284:56948	ESTABLISHED	3996/lighttpd-gau
tcp	0	0	:::FFFF:::280:284:3996	:::FFFF:::280:284:56948	ESTABLISHED	3996/lighttpd-gau
udp	0	0	0.0.0.0:53	*.*.*.*:*		3971/dnsmasq
udp	0	0	0.0.0.0:67	*.*.*.*:*		3956/dhcpd
udp	0	0	0.0.0.0:4795	*.*.*.*:*		4079/avahi-daemon:

## Traffic

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

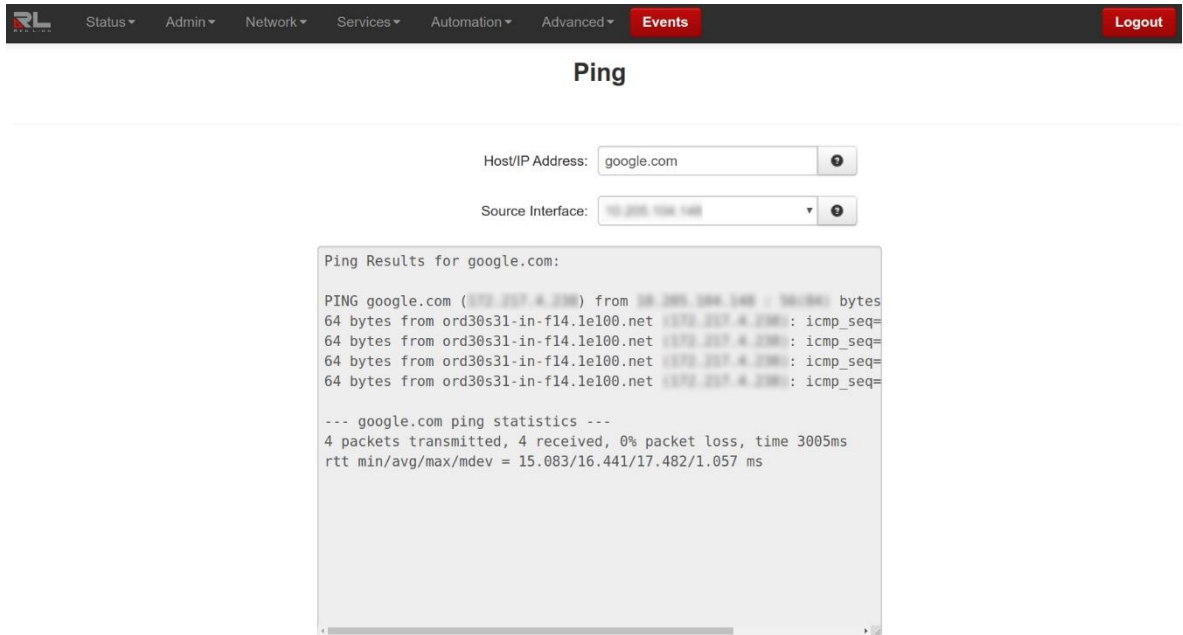


## Diagnostics

The Diagnostics menu is sub-sectioned into Ping, Traffic Capture, Socket Test, Traceroute and System Info sub menus. This information is useful in troubleshooting connectivity between the DA50N and the Internet or another Network connection.

### Ping

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



**Host/IP Address field:** Enter the IP Address or domain name (if DNS enabled) of the destination host to Ping. (Required)

**Recommended Setting**

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. A commonly available internet server available to test against is 4.2.2.2.

**Source Interface:** Select the interface to be used from which to originate the Ping test.

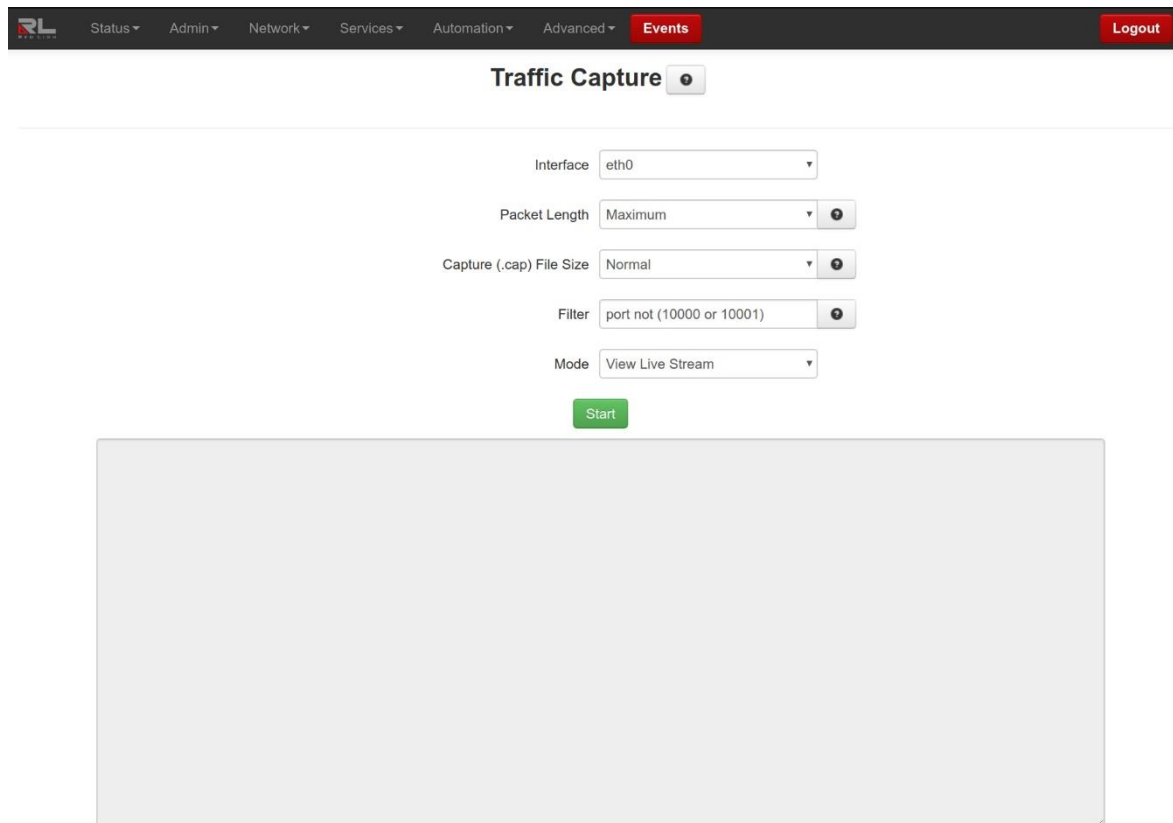
**Recommended Setting**

Choosing "Unspecified" will let the system choose the first interface found with a route to the destination.

**Traffic Capture**

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

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



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

**Packet Length:** Select how much detail about packets to record.

**Truncated** will include the packet headers and the first few bytes of the start of the data packet. Use Truncated to trace network and connection behavior.

**Maximum** will capture the entire packet with contents. Use Maximum to investigate the contents of the data exchange, such as Serial IP packets.

**Recommended Setting:** **Truncated** unless deep packet inspection is required.

**Capture (.cap) File Size:** Cap files are generated on a rotating basis. This sets the maximum size for each of 3 individual files.

**Normal:** 1 Megabyte

**Large:** 3 Megabytes

**Maximum:** 1/6 system memory

**Recommended Setting:** **Normal** to use minimal system resources.

**Filter:** Additional options to specify tcpdump filter.

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

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

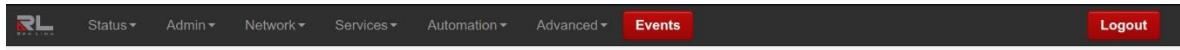
To combine these filters use: `host not 192.168.1.2 and port 1234`

**Recommended:** `port not 10000` to ignore browser traffic while capturing.

For more information about tcpdump filters, please click on the following [link](#).

### Socket Test

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



### Telnet TCP Socket Test

Host/IP Address:

Destination Port:

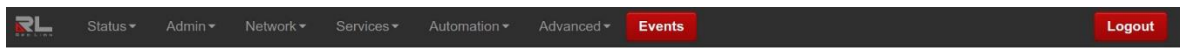
**Host/IP Address field:** Enter the Destination IP Address of the server to which you would like to connect.

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

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

### Traceroute

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



### Traceroute

Host/IP Address  Required

Source Interface

**Host/IP Address field:** Enter the IP address or domain name (if DNS enabled) of the destination host to Trace Route. (Required)

**Recommended Setting:** 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 your routing table. A commonly available internet server available to test against is 4.2.2.2.

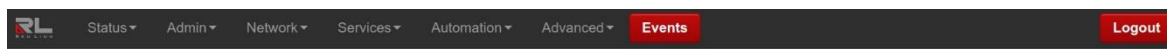
**Source Interface field:** Select the interface to be used from which to originate the Traceroute test.

**Recommended Setting:** Choosing "Unspecified" will let the system choose the first interface found with a route to the destination.

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

### System Info

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



### System Information

#### Filesystem Status

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
ubi0_0	160580	72380	88200	45%	/
devtmpfs	254876	0	254876	0%	/dev
/dev/ubi2_0	582708	2772	575100	0%	/opt
tmpfs	122880	368	122512	0%	/tmp
tmpfs	5120	232	4888	5%	/var
tmpfs	32	0	32	0%	/media
ubi0_0	160580	72380	88200	45%	/var/lib/dpkg

#### Memory Usage

	total	used	free	shared	buffers
cached					
Mem:	510780	60284	450496	600	0
30104					
+/+ buffers/cache:	30180	480600			

## Syslog

The Syslog window will display the current syslog of the DA50N.



### System Log

Filter String

Match Case

Number of lines to display

```

like Gecko) Chrome/80.0.3987.122 Safari/537.36'
Feb 28 04:35:01 crond: (root) CMD (run-parts /etc/cron.5min)
Feb 28 04:39:43 lighttpd[3996]: (mod_auth.c.188) Login success: user ' admin ', IP '
::ffff:10.205.104.109 ', Agent ' Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/80.0.3987.122 Safari/537.36'
Feb 28 04:40:01 crond: (root) CMD (run-parts /etc/cron.5min)
Feb 28 04:43:37 kernel: [ 1267.876144] nf_contrack: default automatic helper assignment has
been turned off for security reasons and CT-based firewall rule not found. Use the iptables
CT target to attach helpers instead.
Feb 28 04:44:50 lighttpd[3996]: (mod_auth.c.188) Login success: user ' admin ', IP '
::ffff:10.205.104.109 ', Agent ' Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/80.0.3987.122 Safari/537.36'
Feb 28 04:45:01 crond: (root) CMD (run-parts /etc/cron.5min)
Feb 28 04:49:57 lighttpd[3996]: (mod_auth.c.188) Login success: user ' admin ', IP '
::ffff:10.205.104.109 ', Agent ' Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/80.0.3987.122 Safari/537.36'
Feb 28 04:50:01 crond: (root) CMD (run-parts /etc/cron.5min)
Feb 28 04:55:04 Last line repeated 1 time(s).
Feb 28 04:55:04 lighttpd[3996]: (mod_auth.c.188) Login success: user ' admin ', IP '
::ffff:10.205.104.109 ', Agent ' Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/80.0.3987.122 Safari/537.36'
    
```

Always scroll to end

Real Time Updates

#### Remote System Logging

Forward syslog to remote host:

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 '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.

Choices include:

50  
100  
250  
1000  
2000

**Note:** Be advised that when connected via a Cellular interface, the log file data collected will count towards your total data plan usage.

**Always scroll to end:**

**Forward syslog to remote host:** Select **Yes** to enable forwarding of syslog messages to another host. (Required)

**Recommended Setting:** No.

**IP/Hostname of remote:** Enter the IP address of the remote syslog server to which you want to forward messages. (Required)

**Enter Whitelist String:** When configuring Remote Syslog, there are many cases when the entire contents of the onboard syslog are not of interest. In order to reduce the amount of data used to transmit the message, these lists allow configurable strings to match messages that are of interest. When creating a blacklist, any of the search terms added are matched against each syslog message. If any terms are found, the message is discarded and not sent to the remote syslog server. The whitelist operates similarly, but all messages sent must have at least one search term listed in the whitelist.

All search terms for whitelist and blacklist are case sensitive. All search terms must be between 5 and 80 characters long.

**Example:** Configured whitelist members are **error** and **warning**. The blacklist members are **ipsec** and **pluto**.

Only messages that contain the word **error** or **warning** will be allowed to be transmitted, however if the message also has the word **ipsec** or **pluto**, then it will be discarded. A message with just **Error** in it would be discarded.

**Enter Blacklist String:** When configuring Remote Syslog, there are many cases where the entire contents of the onboard syslog are not of interest. In order to reduce the amount of data used to transmit message, these lists allow configurable strings to match on messages that are of interest. When creating a blacklist, any of the search terms added are matched against each syslog message. If any terms are found, the message is discarded and not sent to the remote syslog server. The whitelist operates similarly, but all messages sent must have at least one search term listed in the whitelist.

All search terms for whitelist and blacklist are case sensitive. All search terms must be between 5 and 80 characters long.

**Example:** Configured whitelist members are **error** and **warning**. The blacklist members are **ipsec** and **pluto**.

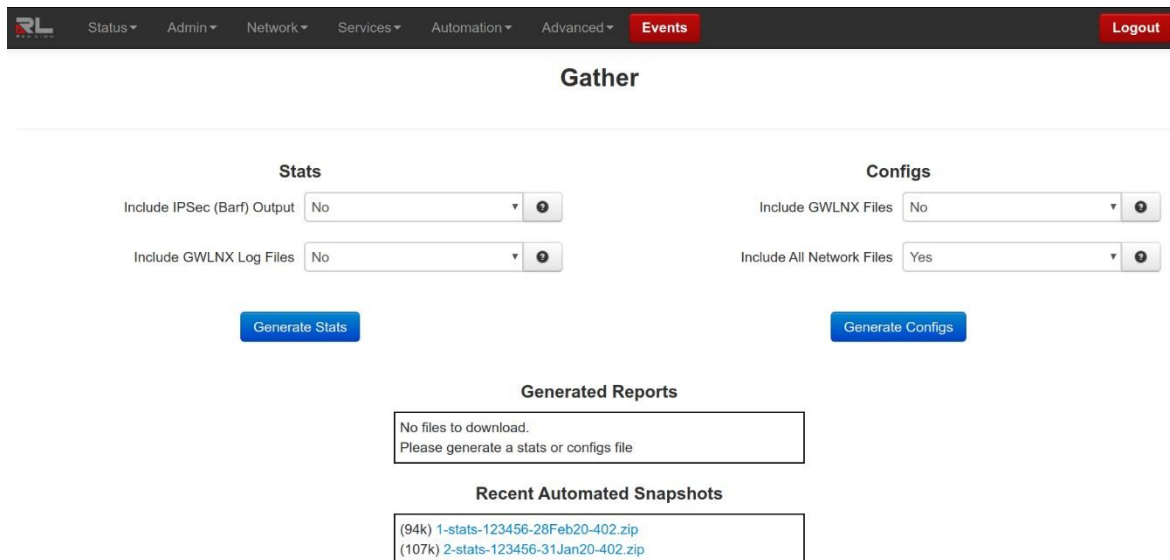
Only messages that contain the word **error** or **warning** will be allowed to be transmitted, however if the message also has the word **ipsec** or **pluto**, then it will be discarded. A message with just **Error** in it would be discarded.

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



## Gather Stats

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



**Include IPSec (Barf) Output:** Select **Yes** to include all IPSec (Internet Protocol Security) related files.

**Recommended Setting:** Please choose yes for this option if you are running a VPN connection on this unit.

**Include GWLNX Log Files:** Select **Yes** to include all GWLNX related logs.

**Recommended Setting:** Please choose "yes" if you are running GWLNX for protocol conversion. This will increase the size of the resulting zip file.

**Include GWLNX Files:** Select **Yes** to include the GWLNX protocol conversion application file. This will considerably increase the size of your resulting zip file.

**Recommended Setting:** Only choose yes for this option if directed by Technical Support staff, 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.

**Recommended Setting:** 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.



## Admin Tab

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

### Access Settings

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

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

The screenshot shows the 'Access Settings' page in a web browser. The top navigation bar includes the RedLion logo and several menu items: Status, Admin, Network, Services, Automation, Advanced, Events, and Logout. The main content area is titled 'Access Settings' and is divided into several sections. The first section contains three fields: 'Unit's Name' (text input with 'DA50N-d35004'), 'Web Access Method' (dropdown menu with 'HTTPS' selected), and 'Enable ZeroConf Network Utilities' (dropdown menu with 'Yes' selected). The second section is for 'User: admin (Full access)' with a 'New Password' text input. The third section is for 'User: rlcuser (Controlled access)' with a 'New Password' text input. The fourth section is for 'User: techsup (Limited access)' with a 'New Password' text input.

**Unit's Name:** Enter a description to identify this Unit. This field is not required for the unit's functionality and it is just for the unit's 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.

**HTTPS/Redirect:** Use this option if you are currently using HTTP method and want to redirect existing users to the new HTTPS port.

**Note:** HTTPS modes are recommended which use data encryption to provide a secure connection.

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

**Example:** With a Unit Name of MyDevice and ZeroConf enabled, you will be able to access the device Web UI at:

MyDevice:10000 Windows

MyDevice.local: 10000 Mac/Linux

**Recommended Setting:** Yes.

User: admin (Full access)

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

**New Password:** Enter the new password in this field.

**Password Limitation Note:** 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 case characters and numbers.

The screenshot displays the 'Access Settings' page. At the top, there is a navigation bar with 'Events' highlighted and a 'Logout' button. The main content area is titled 'Access Settings' and contains several configuration fields: 'Unit's Name' (DA50N-d35004), 'Web Access Method' (HTTPS), and 'Enable ZeroConf Network Utilities' (Yes). Below these is a section for 'User: admin (Full access)' with a 'New Password' field (masked with dots) and a 'Confirm New Password' field (empty). A 'Full access password strength' indicator shows a strength of 'Strong' and a score of '105'. A 'Logout' button is visible in the top right corner.

**Confirm New Password:** Enter the new password in this field.

**Password Limitation Note:** 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 case characters and numbers.

User: rlcuser (Controlled access)

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

**New Password:** Enter the new password in this field.

**Password Limitation Note:** 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 case characters and numbers.

**Confirm New Password:** Enter the new password in this field.

**Password Limitation Note:** 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 case characters and numbers.

User: techsup (Limited access)

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

**New Password:** Enter the new password in this field.

**Password Limitation Note:** 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 case characters and numbers.

**Confirm New Password:** Enter the new password in this field.

Click on the *Apply* button to save and apply changes immediately. To refresh the Access Settings menu, click the *Refresh* button.

## System Time

The System Time menu item is used to configure the time zone on the DA50N to correspond to your location.

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

The screenshot shows the 'System Time' configuration page. At the top is a navigation bar with the following items: Status, Admin, Network, Services, Automation, Advanced, Events (highlighted in red), and Logout (in a red button). The main heading is 'System Time'. Below the heading are four configuration fields, each with a refresh icon (a circle with a dot):  
1. Time Zone: A dropdown menu currently set to 'CST6CDT'.  
2. Sync to NTP Server: A dropdown menu currently set to 'No'.  
3. Set Date (MM/DD/YYYY): An empty text input field.  
4. Set Time (HH:MM:SS): An empty text input field.  
Below these fields is a button labeled 'Use Browser Time'. At the bottom of the page, there is a status section showing:  
Current Browser Time: 03/01/2020 - 23:07:02  
Current Device Time: 02/28/2020 - 05:15:03

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

**Recommended Setting:** User Preference.

To configure the date and time for your DA50N there are three options:

Option 1:

**Sync to NTP Server:** Select **Yes** to enable synchronizing the system clock to an NTP server. (Required)

**NTP Server Name/IP:** Enter the URL or IP address of the NTP Server to which the system clock should be synchronized. (Required)

**Recommended Setting:** The [NTP Pool Project](#) offers a virtual cluster of timeservers providing free and reliable public NTP services. These servers are organized into groups by region and selecting the pool nearest to your location will provide the best results.

United States - [us.pool.ntp.org](http://us.pool.ntp.org)

Canada - [ca.pool.ntp.org](http://ca.pool.ntp.org)

Europe - [europe.pool.ntp.org](http://europe.pool.ntp.org)

Asia - [asia.pool.ntp.org](http://asia.pool.ntp.org)

Australia - au.pool.ntp.org

**Update Frequency:** Select the interval at which the NTP server should be queried by choosing the appropriate value from the drop-down list provided. (Required)

**Note:** If using a cellular connection, time synchronization packets will count towards your total data plan usage.

Option 2 – Manual Configuration:

**Current Date (MM/DD/YYYY) (Required):** Set the Sync to NTP Server field to No and format the date as MM/DD/YYYY.

Click the Use Local System Time button to use the current date as displayed on the browser, obtained from your local PC.

**Current Time (HH:MM:SS) (Required):** Set the Sync to NTP Server field to No and format the time as HH:MM:SS.

Click the Use Local System Time button to use the current date as displayed on the browser, obtained from your local PC.

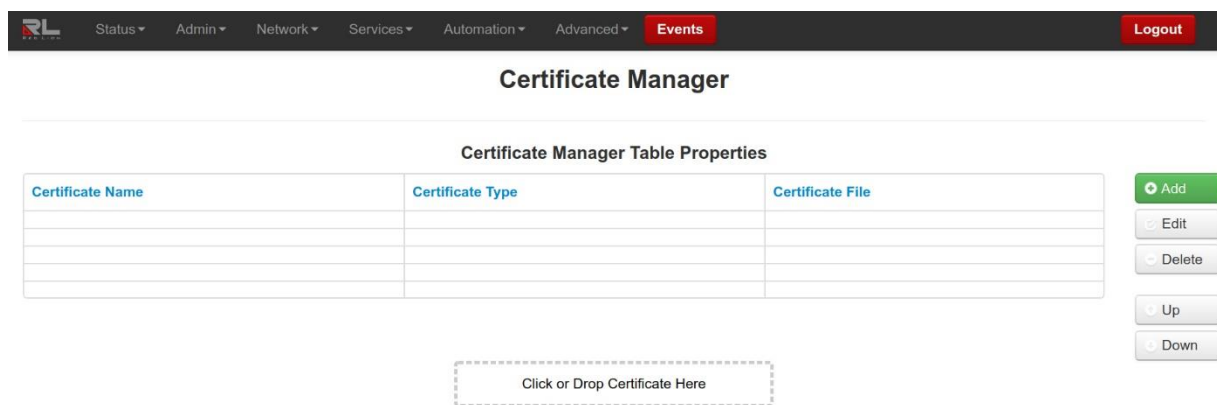
Option 3:

**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 refresh the System Time menu, click the *Refresh* button.

## Certificate Manager

The Certificate Manager gives the option of adding a certificate, deleting or editing an existing one. Click on the *Certificate Manager* menu item and the following dialog window appears:



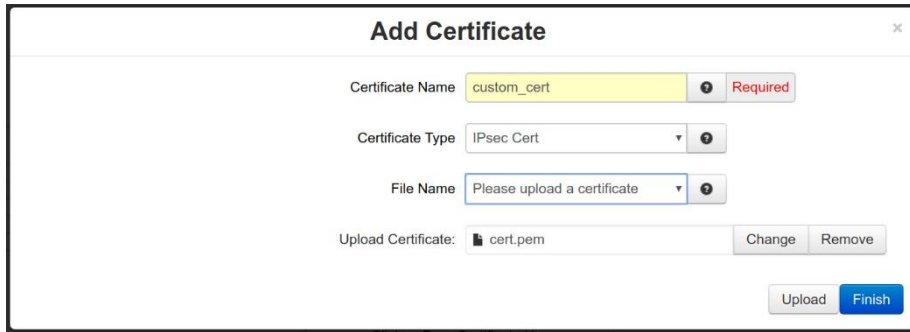
There are two ways to add a certificate to the Certificate Manager Table. One way is by using the “Click or Drop Certificate Here” hot spot and the second is by creating a new certificate.

To add a new certificate using the hot spot:

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

To create a new certificate:

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



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

**Certificate Type:** Select the type of certificate that you will be uploading. Each certificate is stored in a unique repository, depending on the service that will be using it.

The certificate file name can contain only upper and/ or lower case letters, digits, '-', '\_' and must end with .ca, .cert, .cer, .crt, .csr, .srl, .cnf, .key, or .pem.

Possible choices include:

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

**HTTPS:** This certificate will be used for the HTTPS engine, and replace the onboard automatically generated self-signed 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 self-signed 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.

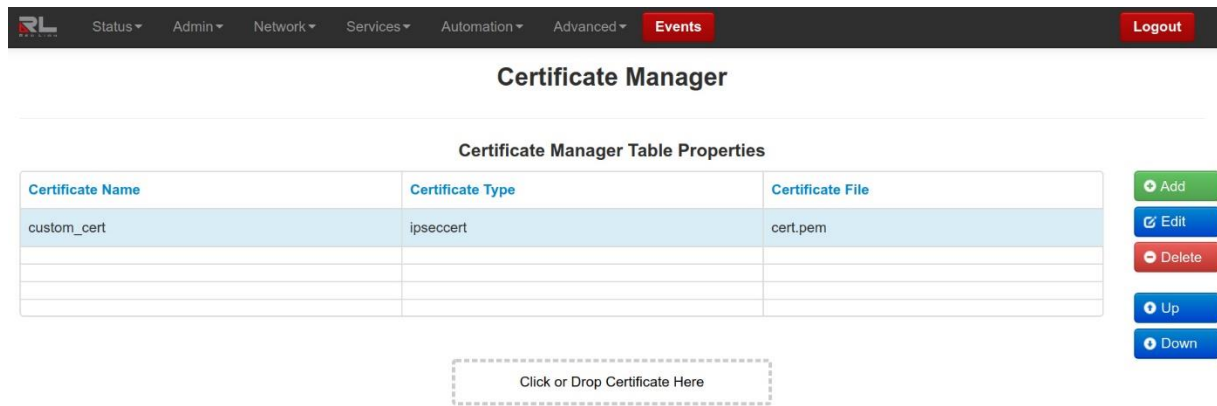
**File Name:** Once you have entered a value into the **Certificate Name** field, the **Browse** button will be enabled and can be clicked to select a file from your local system for upload. When a valid file name is selected, the **Upload** button is enabled and can be clicked to upload the selected file to the device.

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.

**Note:** SSL type certificates must include the key and cert portions, and the key must not be password encrypted.

**Upload Certificate:** Select a file to upload.

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



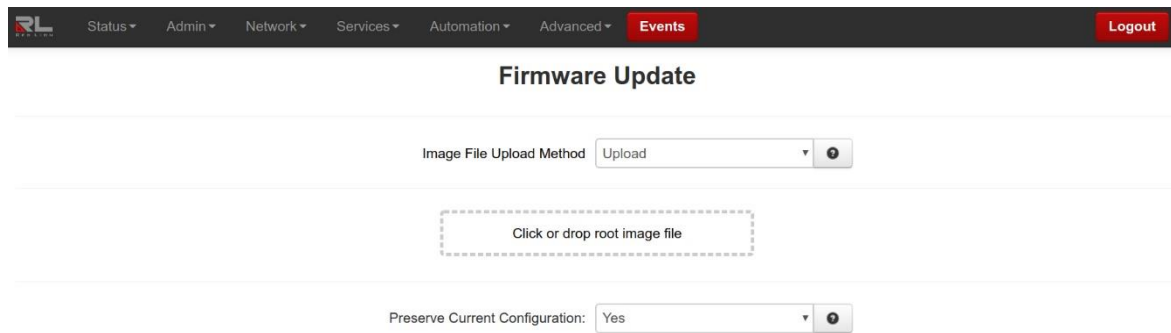
To delete an existing certificate, select it in the table and click on the *Delete* button. To edit an existing certificate, select it in the table and click on the *Edit* button.

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

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately. To refresh the Certificate Manager menu, click the *refresh* button.

## Firmware Update

The Firmware Update menu item is used to upgrade the firmware of the DA50N. Click on the Firmware Update menu item and the following window appears:



To upgrade the firmware of the DA50N:

**Image File Upload Method:** Select the method by which you would like to upload images to be installed.

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

**Preserve current configuration:** Select **Yes** to cause the device to save its current configuration and restore it after the firmware image is installed.

Click on the *Install* button.

**Note:** This procedure can take up to 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 factory service.

## Configuration Manager

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

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

### Export Web UI Master Configuration / Subsystem(s) File

**Export File Method:** Select the method by which you would like to download the master or multi subsystem configuration file.

**Encryption Key:** Encryption key to use when exporting an encrypted configuration file.

**Note:** It is strongly recommended to export configurations with an encryption key to ensure sensitive unit data is protected. Configuration exports without an encryption key will be readable in clear-text.

After clicking Export Master Configuration or Export Subsystem(s), the following message appears:

#### Backup/Clone of this unit

This option will export all fields in selected configurations.

#### Copying details to a similar unit

This option will prompt to exclude certain device-specific config fields like interface IP addresses. These fields are typically device-specific.

**Note:** Please note the directory where the file was saved in order to retrieve it when needed to put the file back onto the DA50N.

## Import Web UI Master Configuration

**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 file. Do not use this option for cloning an entire unit's config.xml. This should only be used to add new records to existing tables.

**WARNING:** Multiple attempts of the same **Merge** process will duplicate table entries.

**Import File Options:** If you want to save the new configuration without immediately applying it, simply select **Save Only** option. To make your changes take effect, a reboot is required.

If you select **Apply** to apply the settings, 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.

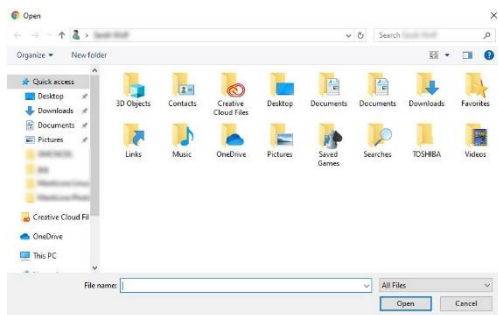
If you select **Forced Apply** to apply the settings, every section imported will be applied immediately. This is not frequently required.

**WARNING:** If your configuration file has many sections, the import process can take a long time.

**Import File Method:** Select the method by which you would like to import the configuration file.

**Decryption Key:** Decryption key is used when importing an encrypted configuration file.

**Import Configuration File:** Select the method by which you would like to import the configuration file.



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

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

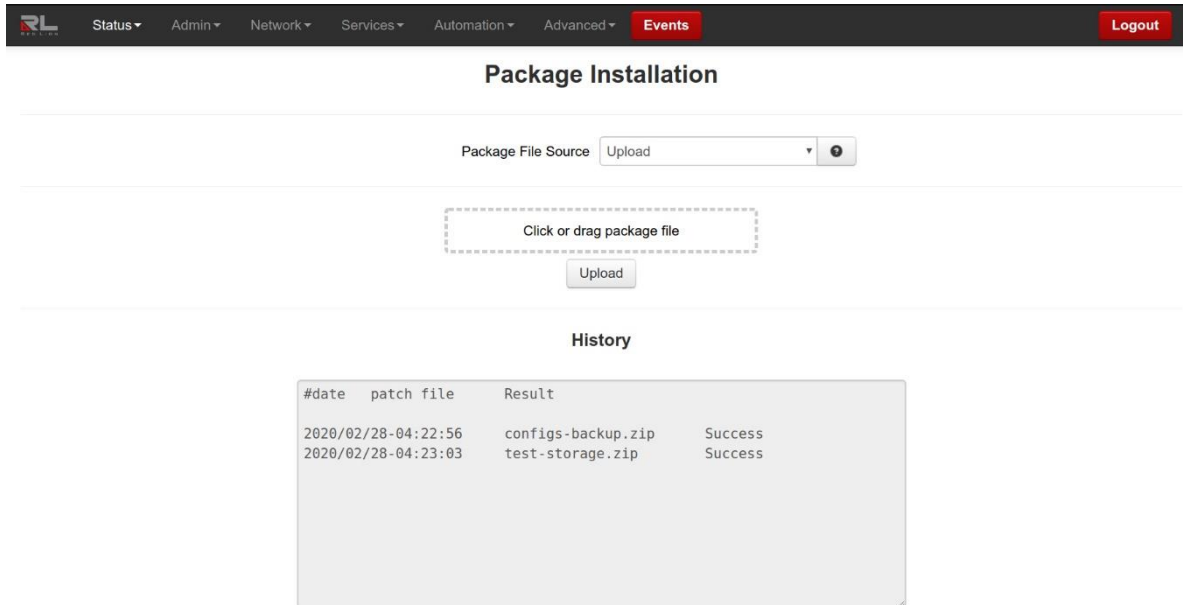
Click on the *Import* button. When import is complete, a table appears at the bottom of the dialog window listing the modified files.

## Package Installation

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

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



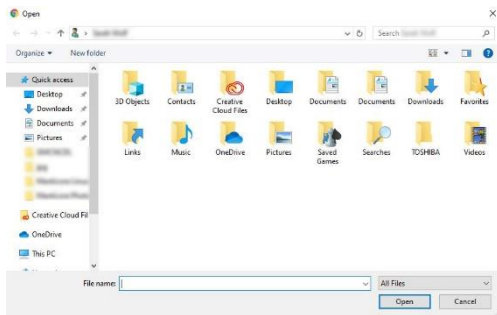


**Package File Source:** Select the source to provide the package to be installed.

The package must be a valid .zip file.

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

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



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

Select the filename to select the file.

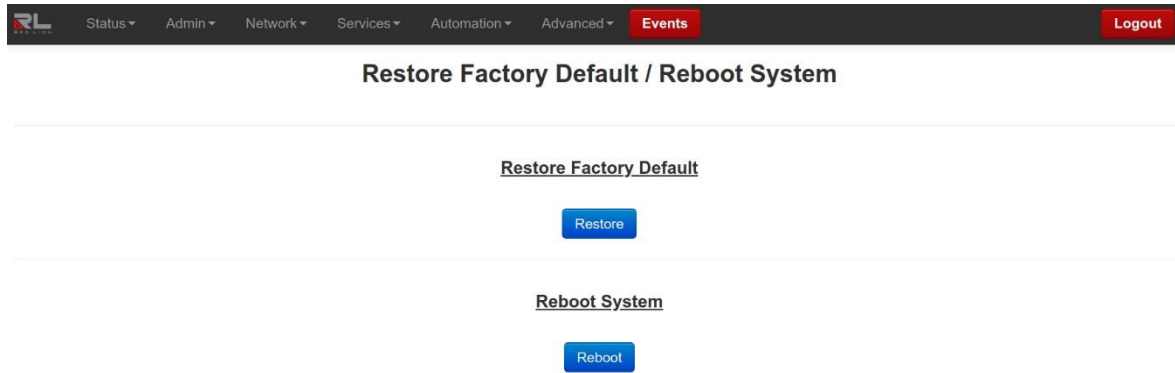
**Note:** Be sure to use only genuine Red Lion provided packages in the form of filename.zip.

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

## Factory Defaults/Reboot

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

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



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

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

## Job Control

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

**Job Control**

**Predefined Job Settings**

Predefined Job Interval: Disabled

Select Predefined Job: None

Apply

**Import Job Script**

Imported Job Interval: Daily

Click or Drag Script File

Import

**Delete Imported Job Script**

Select Imported Job: -None Selected-

Delete

**List of Current Scheduled Jobs**

```
/etc/jobcontrol/5min:  
/etc/jobcontrol/custom:  
/etc/jobcontrol/daily:  
/etc/jobcontrol/hourly:  
/etc/jobcontrol/monthly:  
/etc/jobcontrol/weekly:
```

Refresh

### 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.

#### Periodic Job Interval

**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 job to be scheduled for the selected interval.

#### Job Categories

**Reboot:** Reboot the unit at selected job interval.

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

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

## Import Job Script

**Imported Job Interval:** Select appropriate job interval from provided drop down list to run at the scheduled job interval.

### Import Job Interval

**5 minutes:** Will run every 5 minutes.

**Hourly:** Will run every hour.

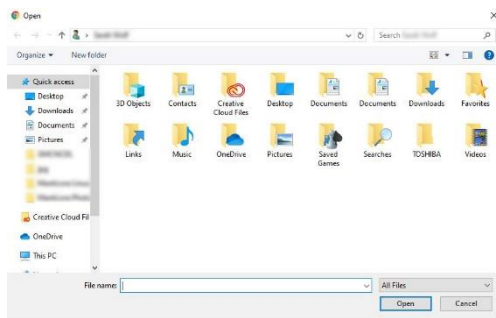
**Daily:** Will run at 4:02 am.

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

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

**Click or Drag Script File:** Click on to select the script file that will be imported or drag and drop the script file to be imported.

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



Browse to the directory where the script file is located.

Select the filename to select the file.

Click on the *Open* button to populate the Script File field.

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

## Delete Imported Job Script

**Select Imported Job:** Select an imported job to be removed 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.

## Network Tab

The Network Tab configures aspects of the DA50N affecting the networking functionality of the unit. From here you can configure the Cellular Connection, Ethernet Interfaces, Firewall, Tunneling, DNS Settings, Static Routes, and TCP Global Settings.

### Cellular Connection

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

#### Sled Cellular Configuration

The Cellular Sled Config menu item is used to make configuration changes to the cellular connection settings on the DA50N.

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

**Cellular Sled Config**

Slot 1

Detected Modem: LE910-NA V2  
Detected Carrier: Verizon

Enable Interface Yes

APN for context 3 is 'vzwInternet'

APN for Sim Slot 1

APN for Sim Slot 2

Show Advanced Configuration Yes

Primary Sim Slot Slot 1

Enable GPS Yes

SIM Unlock PIN Code Remaining tries: 3 . See help link for details

CPIN Unlock Action Not-selected Disabled

**CPIN / PUK Status**  
CPIN: Disabled  
Status: Available  
Extended Status: N/A

Roaming Auto

Authentication Type CHAP

User Name asdfgh

Password \*\*\*\*\*

Network Speed 3G

P-I-P Interface No

MTU 1500

Sync Time Yes

Use Default Route Yes

Use Peer DNS Yes

Show Details Show CSQ History

**Enable Interface:**

Select Option:

**Yes** - Enable the interface to become IP active after the new settings are applied and upon subsequent system start-up, SMS and statistics.

**No** - Disable IP Data interface, SMS and statistics available.

**Off** - Power off Cellular. No IP Data, SMS, or statistics.

**APN for Sim Slot 1:** Enter the APN used to access your cellular wireless data service in this field.  
(Optional)

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

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

**APN for Sim Slot 2:** Enter the APN used to access your cellular wireless data service in this field.  
(Optional)

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

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

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

**Primary SIM Slot:** Choose SIM Slot to use according to the following available options:

Slot 1: Use the SIM card in Slot 1.

Slot 2: Use the SIM card in Slot 2.

**Note:** A SIM card must be inserted into the SIM slot choice.

**Enable GPS:** Select **Yes** to enable the Cellular GPS chipset, if available.

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

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

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

**Disable:** Unlock SIM to no longer require a SIM PIN password for use. The current SIM PIN must be known in order to disable. The SIM PIN will still be set, but will no longer be required for use.

**Change:** Enter a new SIM PIN to use to unlock the SIM. The current SIM PIN must be known in order to change. This will replace the old SIM PIN and automatically ENABLE SIM PIN use.

**WARNING:** An incorrect current SIM PIN will result in a failure, and the allowed number of attempts left will be reduced by 1. Use with caution.

**Roaming:** Allow Cellular Roaming.

**Auto:** Allow roaming.

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

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

Choosing 'CHAP', will use CHAP authentication.

Choosing 'PAP', will use PAP authentication.

Choosing 'Auto', if available, will use either PAP/CHAP authentication.

Choosing 'OFF', if available, will clear the username/password from the profile. If a username/password are set, and authentication is 'OFF', then authentication will not be updated in the modem. To clear the authentication information in the modem, clear the username and password, and then select 'OFF' for the authentication type.

**User Name:** Enter the username assigned to you by your cellular wireless data plan provider which should have been given to you when you established your service. (Optional)

**Password:** Enter the password assigned to you by your cellular wireless data plan provided, which should have been given to you when you established your service. (Optional)

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

**Network Speed:** Select the connection speed to be used for the cellular modem connection from the drop-down list provided. Auto will use the widest available defaults, starting at the highest speed available (4G-LTE, if present).

Possible values include:

Default: Do not adjust the module settings.

Auto

LTE: 4G/LTE only.

2G3G: 3G/2G only, no LTE.

3G Only: 3G only service.

2G Only: 2G only service.

**Recommended Setting:** Auto or Default.

**MTU:** Enter the MTU size you desire to use.

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

**Recommended Setting:** 1500.

**Sync Time:** This option will attempt to take the local time as reported by the cellular tower, and set the unit's system time to match.

**Recommended Setting:** Yes.

**Use Default Route:** Select **Yes** to have the cell connection use the default route once it is connected.

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

Click on the *Show/Hide Details* button to show or hide details. Click on the *Show/Hide CSQ History* to show or hide CSQ history.

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

## Provisioning

The Cellular Sled Provisioning menu item is used to select the correct carrier profile and firmware images for the cellular module to authenticate on the LTE carrier networks.

**Cellular Sled Provisioning**

Slot 1

Module Model: LE910-NA V2  
SIM Carrier: Verizon  
Detected IMEI: 358148061063025  
Module Firmware Version: 20.00.006  
Firmware Slot: 2  
Dual Firmware: Yes  
SIM ID: 8914800001636923731  
SIM IMSI: 311480165354055  
SIM Slot: 1  
MDN Number: 17178731251  
Activation Status: Registered, Home Network

**Manage Module Firmware**  
Active: Verizon

Select Firmware Version  
None Selected...

Note: If you recently installed or reflashed a firmware package, you may need to update this list by clicking Refresh below

Update APN for Sim Slot 1 (optional)

Update APN for Sim Slot 2 (optional)

Update Module Delete

Show Diagnostic Information

Show Cellular Module Status

**Select Firmware Version:** Select a firmware version to update. A firmware update takes 15-30 seconds to complete, and another 30-60 seconds for the device information to update. If the firmware update fails (see diagnostic information), attempt the update again.

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

**WARNING:** Do not remove the sled or power off the device while the update is in place.

**Update APN for Sim Slot 1 (optional):** Enter the APN used to access your cellular wireless data service in this field.

**Note:** If specified, this will be automatically applied after the module has been updated.

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

**Note:** Entering an APN value in this field will overwrite any APN stored in the modem. (Optional)

**Update APN for Sim Slot 2 (optional):** Enter the APN used to access your cellular wireless data service in this field.

**Note:** If specified, this will be automatically applied after the module has been updated.

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

**Note:** Entering an APN value in this field will overwrite any APN stored in the modem.(Optional)



### Update Module

Click on the Update Module button to update the firmware on the cellular sled.

**Note:** Rebooting or unplugging the device during this process may cause your unit to become INOPERABLE and require an RMA. The device will reboot after this operation.

### Delete

Click on the Delete button to delete firmware on the cellular sled.

**Note:** Rebooting or unplugging the device during this process may cause your unit to become INOPERABLE and require an RMA. The device will reboot after this operation.

### Shown Diagnostic Information

Click on the Show Diagnostic Information to show diagnostic information.

### Show Cellular Module Status

Click on the Show Cellular Module Status button to show the cellular module status.

To refresh the page, click on the *refresh* button.

## Interfaces

The Interfaces menu allows the administrator to configure the Ethernet ports of DA50N to incorporate within their existing network topology.

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

### Ethernet Port 1 (eth0) and Ethernet Port 2 (eth1) – (Network Interfaces)

The configuration procedure of the Ethernet ports is the same for Ethernet Port 1 and Ethernet Port 2, therefore this section will only reference the configuration of Ethernet Port 1 (eth0). Please refer to this section when configuring "eth1"/Ethernet Port 2'.

Click on the *Ethernet Port 1 (eth0)* menu item, select **Yes** in Enable Interface and the following window appears:

RL
Status ▾ Admin ▾ Network ▾ Services ▾ Automation ▾ Advanced ▾ **Events** Logout

### Ethernet Port 1 (eth0)

---

Enable Interface Yes ▾ ⓘ

Interface Speed/Duplex Auto Detect ▾ ⓘ

Obtain Network Addresses via DHCP Yes ▾ ⓘ

Use Remote Gateway as Default Route No ▾ ⓘ

Use Peer DNS Yes ▾ ⓘ

Enter Maximum Transmission Unit (MTU) 1500 ⓘ Required

---

#### DHCP Server Settings

**Ethernet Port 1 (eth0)** (Obtaining addresses via DHCP - unable to act as server)

Enable DHCP No ▾ ⓘ

---

#### Interface Aliases

Sub-Interface	IP Address	Subnet Mask

+ Add  
Edit  
Delete  
Up  
Down

---

#### Interface VLANs

VLAN ID	IP Address	Subnet Mask

+ Add  
Edit  
Delete  
Up  
Down

### Enable Interface

**Auto Configure:** In this mode, the Ethernet Port 1 (eth0) interface will attempt to adapt to your existing network. It will start in DHCP **client** mode, but if it fails to obtain an IP address, then it will fall back to a static IP, with a DHCP server running on the interface.

Otherwise, select Yes to enable the interface, or No to disable the interface.

When the **Save** button is clicked, the interface will not be immediately activated or deactivated, but will be after the device is rebooted. This allows for other configuration changes to be made to the device that can be committed at a later time.

When the **Apply** button is clicked, the current settings will be saved and the interface will immediately be either deactivated or activated. If the interface was already active, then it will be deactivated 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 reconnect 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.**

**Interface Speed/Duplex:** Select the Speed and Duplex to be used for the physical interface.

The following options are available:

**Auto Detect:** Use the 'best negotiated' speed and duplex. (default)

**10Mbps/Half:** Force the interface to 10Mbps and half-duplex.

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

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

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

**Recommended Setting:** Auto-Detect.

**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, subnet mask and remote gateway addresses. DNS information can be provided by navigating to **Network→DNS Settings**.

The screenshot shows a web form for network configuration. It contains five fields: 1. 'Obtain Network Addresses via DHCP' is a dropdown menu set to 'No'. 2. 'Enter IP Address' is a text input field with a red border and a 'Required' label. 3. 'Enter Subnet Mask' is a text input field containing '255.255.255.0' with a red border and a 'Required' label. 4. 'Use Remote Gateway as Default Route' is a dropdown menu set to 'Yes'. 5. 'Enter Remote Gateway' is an empty text input field with a red border and a 'Required' label.

**Enter IP Address:** 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. (Required)

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.

**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 **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.

This field is only available when **Obtain Network Addresses via DHCP** has been set to No. (Required)

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

**Enter Remote Gateway:** Enter the IP Address for the gateway device.

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, it 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 **Network→DNS Settings** screen.

**Recommended Setting:** Yes.

**Enter Maximum Transmission Unit (MTU):** Enter the MTU size you desire to use.

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

**Recommended Setting:** 1500.

## DHCP Server Settings

**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.

### DHCP Server Settings

**Ethernet Port 1 (eth0)** (   using netmask 255.255.255.0)

Enable DHCP Yes ⓘ

Enable Default Gateway Yes ⓘ

Starting Address   ⓘ Required

Ending Address   ⓘ Required

**Enable Default Gateway:** Provide Default Gateway IP Address to DHCP Client.

**Recommended Setting:**

- 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.
- 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. (Required)

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

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

**Recommended Setting:** A valid address 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.

Interface Aliases

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

Interface Aliases		
Sub-Interface	IP Address	Subnet Mask

+ Add
Edit
Delete
  
Up
Down

To configure a sub-interface:  
Click on the *Add* button and the following pop-up window appears:

**Enter Sub-Interface number:** Enter the desired Sub-Interface number in the field provided. (Required)

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.

**Recommended Setting:** Your Network Administrator should be able to provide guidance as to an appropriate value.

**Enter IP Address:** Enter the desired interface IP Address into this field. (Required)

**Recommended Setting:** This address should have been provided by your Network Administrator.

**Enter Netmask:** Enter the desired Netmask for the sub interface (alias) in the field provided. (Required)

**Recommended Setting:** Your 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.

Sub-Interface	IP Address	Subnet Mask
6	192.168.1.1	255.255.255.0

Add
Edit
Delete
Up
Down

### Interface VLANs

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

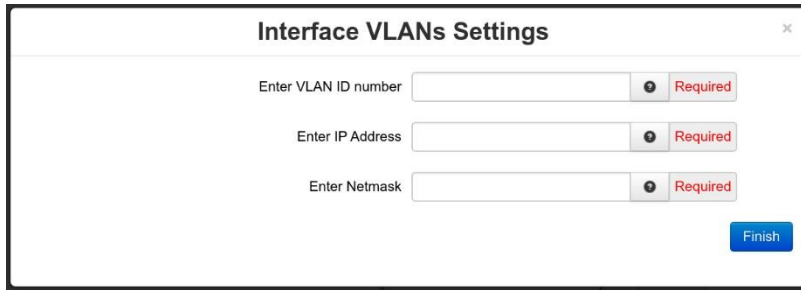
**Note:** VLANs are available for any unit with Split LAN enabled under Switch Control.

VLAN ID	IP Address	Subnet Mask

Add
Edit
Delete
Up
Down

To configure an Interface VLAN:

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



The screenshot shows a dialog box titled "Interface VLANs Settings" with a close button (X) in the top right corner. Inside the dialog, there are three input fields, each with a "Required" label and a help icon (i) to its right. The first field is labeled "Enter VLAN ID number", the second "Enter IP Address", and the third "Enter Netmask". A blue "Finish" button is positioned at the bottom right of the dialog.

**Enter VLAN ID number:** Enter the desired VLAN ID interface number in the field provided. (Required)

The valid range is 0-4094, and each VLAN interface must be uniquely numbered. The final VLAN ID will then be in the form ethx.y where x is the root interface number and y is the VLAN ID number.

**Recommended Setting:** Your Network Administrator should be able to provide guidance as to an appropriate value.

**Enter IP Address:** Enter the desired interface IP Address into this field. (Required)

**Recommended Setting:** This address should have been provided by your Network Administrator.

**Enter Netmask:** Enter the desired Netmask for the VLAN interface in the field provided. (Required)

**Recommended Setting:** Your 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 VLANs table will be populated with the entered data.

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

**Refresh:** Will refresh the current screen.

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

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

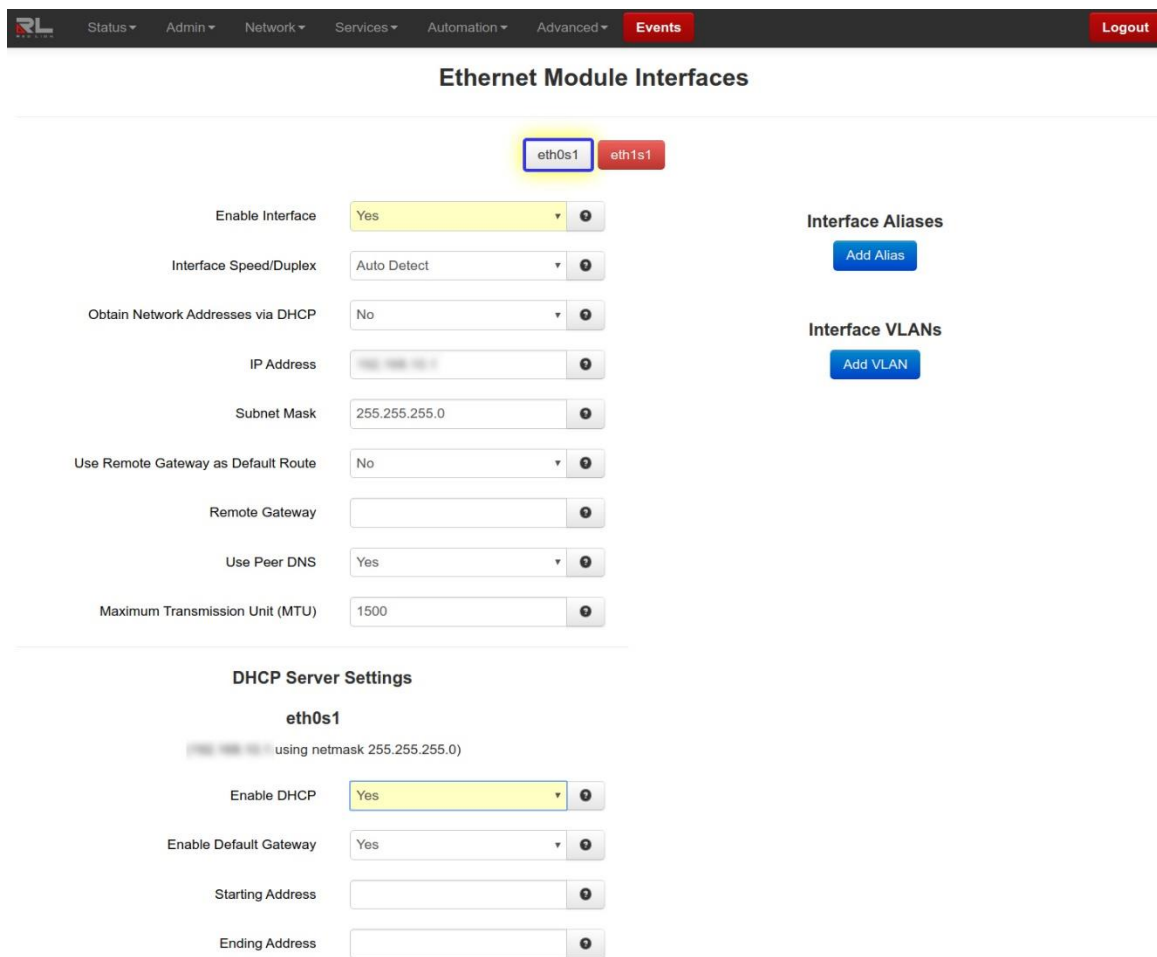
Applying new settings to the interface may result in disconnection, requiring reconnection using alternate methods.

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

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

## Sled Ethernet Interfaces

The Ethernet Modules Interfaces option is used to configure the network settings of any installed Dual Ethernet sled.



**Enable Interface:** Select Yes to enable the interface, or No to disable the interface.

When the **Save** button is clicked, the interface will not be immediately activated or deactivated, but will be after the device is rebooted. This allows for other configuration changes to be made to the device which can be committed at a later time.

When the **Apply** button is clicked, the current settings will be saved and the interface will immediately be either deactivated or activated. If the interface was already active, then it will be deactivated 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.**

**Interface Speed/Duplex:** Select the Speed and Duplex to be used for the physical interface.

The following options are available:

- Auto Detect** – Use the 'best negotiated' speed and duplex (default)
- 10Mbps/Half** – Force the interface to 10Mbps and half-duplex
- 100Mbps/Half** – Force the interface to 100Mbps and half-duplex
- 100Mbps/Full** – Force the interface to 100Mbps and full-duplex.

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



**Recommended Setting:** Auto-Detect.

**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, optionally, 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 the IP address, netmask and remote gateway addresses. DNS information can be provided by navigating to **Network→DNS Settings**.

**IP Address:** 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. (Required)

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.

**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 **Enter Subnet Mask** field and must not conflict with any other device on the target network.

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

This field is only available when **Obtain Network Addresses via DHCP** has been set to No. (Required)

**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.

**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, it 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.

**Remote Gateway:** Enter the IP Address for the gateway device in the field provided. (Required, if **Use Remote Gateway as Default Route** is set to Yes.)

A gateway is a device 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 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).

**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.

**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 **Network→DNS Settings** screen.

**Recommended Setting:** Yes

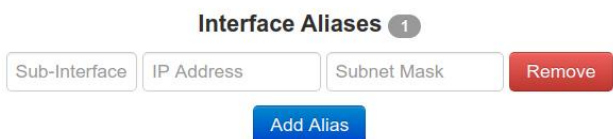
**Maximum Transmission Unit (MTU):** Enter the MTU size you desire to use.

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

**Recommended Setting:** 1500.

### Interface Aliases

Click on the Add Alias button and the following options will appear:



**Sub-Interface:** Enter a valid Sub-Interface number. Range: 0-99.

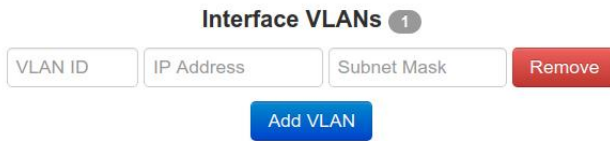
**IP Address:** Enter a valid IP Address for the selected Sub-Interface.

**Subnet Mask:** Enter a valid Subnet Mask for the selected Sub-Interface.

Click on the Add Alias button and click again on the Add VLAN button to define additional VLAN interfaces as required.

## Interface VLANs

Click on the Add VLAN button and the following options will appear:



**VLAN ID:** Enter a valid VLAN ID number. Range: 0-4094.

**IP Address:** Enter a valid IP Address for the selected VLAN ID.

**Subnet Mask:** Enter a valid Subnet Mask for the selected VLAN ID.

Click the Add VLAN button and Click again on the Add VLAN button to define additional VLAN interfaces as required.

## DHCP Server Settings

**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.

**Recommended Setting:**

**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.

**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. (Required)

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

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

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

## Wi-Fi (WLAN)

The screenshot displays the 'Wi-Fi WLAN Module Config' page. At the top, a navigation bar includes 'Status', 'Admin', 'Network', 'Services', 'Automation', 'Advanced', 'Events', and 'Logout'. The main content area is titled 'Wi-Fi WLAN Module Config' and features a dropdown menu for selecting the interface, currently showing 'wlan0s1'. Below this, several configuration options are presented as dropdown menus: 'Enable Wi-Fi' (Yes), 'Wireless Mode' (Client), 'Obtain Network Addresses via DHCP' (Yes), and 'Use Remote Gateway as Default Route' (No). A blue 'Scan for Access Points' button is located below these options. Further down, the 'SSID' field is set to 'wireless\_ap' and is marked as 'Required'. The 'Pre-shared Key' field contains masked characters, and the 'Hide Pre-shared Key Characters' checkbox is checked. A section titled 'DHCP Server Settings' for 'Wi-Fi (wlan0s1)' includes a note '(Obtaining addresses via DHCP - unable to act as server)' and an 'Enable DHCP' dropdown set to 'No'.

**Enable Wi-Fi:** If selected (Yes), this page is used to configure the parameters for the wireless LAN interface as either a client or Access point. Here you may change wireless encryption settings as well as wireless network parameters.

**Wireless Mode:** Select "Client" to connect the wireless interface to an Access Point, or "Access Point" to accept client connections.

**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, optionally, 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 the IP address, netmask and remote gateway addresses. DNS information can be provided by navigating to **Network**→**DNS Settings**.

**IP Address:** Enter the wireless IP Address into this field.

**Note:** Wi-Fi in bridge mode uses eth1 interface and this Wi-Fi IP address will overrides eth1's IP address. (Required)

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.

**Recommended Setting:** Your Network Administrator should be able to provide an appropriate value.

**Default Setting:** 192.168.1.1.

**Subnet Mask (Required):** Enter the desired Netmask for the wireless interface in the field provided.

**Note:** Wi-Fi in bridge mode uses eth1 interface and this Wi-Fi Netmask will overrides eth1's Netmask. (Required)

**Recommended Setting:** Your Network Administrator should be able to provide an appropriate value.

**Default Setting:** 255.255.255.0.

**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, it 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.

**Remote Gateway:** Enter the IP Address for the gateway device in the field provided. (Required, if **Use 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 be 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).

**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.

Click the "Scan for Access Points" button to scan for access points.

**SSID:** The SSID is a unique name for your wireless network. It is case sensitive and must not exceed 32 characters. All wireless devices in your network must use the same SSID. Verify that you are using the correct SSID and click the **Apply** button to set it.

**Country Code:** The country code restricts allowed device frequencies and power levels based on country-specific regulatory domains.

**WARNING:** Operating a device outside these limits can have legal implications.

**Note:** Country Code is only shown when configuring as an Access Point.

**Band:** This determines the wireless standard to use (802.11b/g/n). Channel 14 is only permitted in 802.11b mode. If available in your region, use 802.11b to enable channel 14.

**Recommended:**

802.11g/n for best performance.

802.11b/g for best compatibility with older clients.

**Note:** Band is only shown when configuring as an Access Point.

**Channel:** Select appropriate channel from the list provided to correspond with your network settings, between 1 and 11. All points in your wireless network must use the same channel in order to function correctly. Verify that the correct channel is selected and click the **Apply** button to set it.

**Note:** Channel is only shown when configuring as an Access Point.

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

**Note:** Broadcast SSID is only shown when configuring as an Access Point.

**Encryption Mode:** This option allows you to setup the wireless security. If security is disabled, any client can connect to the access point. Turning on WPA requires clients to know an encryption key before connecting to the network.

**Note:** Encryption Mode is only shown when configuring as an Access Point.

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

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

**WPA Pre-Shared Key:** This option allows the sender and recipient to share a secret key.

## DHCP Server Settings

**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.

**Recommended Setting:**

**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.

**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. (Required)

**Recommended Setting:** A valid address for the subnet for which the interface is configured.

Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

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

**Recommended Setting:** A valid address 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.

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 or refresh the screen, click on the Revert/Refresh button.

## USB

The USB interfaces menu item allows the administrator to configure the USB port of the DA50N to meet their needs. The default address is set for 192.168.111.1 with the subnet mask of 255.255.255.0. Click on the USB menu item and the USB IP Interface dialog window appears:

**Enable USB Interface:** Select **Yes** to enable the USB Interface.

**Recommended Setting:** Yes, if using this Interface.

**Enter IP Address:** Enter the desired interface IP Address into this field. (Required)

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.

**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 **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. (Required)

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

## DHCP Server Settings

**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.

### Recommended Setting

**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.

**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. (Required)

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

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

**Recommended Setting:** A valid address 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.

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 or refresh the screen, click on the *Revert/Refresh* button.

## IPv6

**Enable IPv6:** This will enable IPv6 routing for devices behind our router. Router Advertisement messages will be sent periodically to the specified LAN segment, and 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 our upstream IPv6 Router on the WAN side. Each IPv6 device behind us 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.

A reboot is required after changes to IPv6 Routing configuration.

The screenshot shows a web interface for IPv6 Configuration. At the top, there is a navigation bar with links for Status, Admin, Network, Services, Automation, Advanced, Events, and Logout. The main heading is 'IPv6 Configuration'. Below this, the section 'Define IPv6 Routing Options' contains three configuration items: 'Enable IPv6' with a dropdown menu set to 'Yes', 'WAN Interface' with a dropdown menu set to 'auto', and 'LAN Interface' with a dropdown menu set to 'eth0'. Each dropdown menu includes a small circular icon with an information symbol.



**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 (default untrusted/external interface) may also lead to an upstream IPv6 router.

A reboot is required after changes to IPv6 Routing configuration.

**Recommended:** Auto.

**LAN Interface:** The Router Advertisements are available for one /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.

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 or refresh, click on the *Revert/Refresh* button.

A reboot is required after changes to IPv6 routing configuration.

## Firewall

The Firewall menu item allows you to configure every aspect of the firewall on the DA50N.

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

### General Settings

The General Settings menu is used to configure common access services to the DA50N and configure how the interfaces are interpreted.

Click on the *General Settings* menu item.

**Global Parameters**

Enable Firewall: Yes

Service	Allow/Disallow	Whitelist Name
Ping	Yes	default
SSH	Yes	default
Telnet	No	default
Web UI	Yes	default
SNMP	Yes	default

**Other Options**

Allow IPSec: Yes

Allow NAT-Traversal: Yes

Force Fragmentation: No

Packet Drop Logging: Normal

Local HTTP Redirect: Yes

Global Parameters

**Enable Firewall:** The firewall functions are no longer allowed to be disabled. Disabling the Firewall will compromise not only security, but many router functions of the unit. If you wish to not restrict traffic between two interfaces, you can add both to the Trusted Interface list.

**Ping:** To allow ICMP echo responses (Ping) from external devices through untrusted interfaces on this unit, select Yes, otherwise select No.

To restrict access via a configured 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→Subnet Whitelist Rules** screen.

**Note:** This setting will **NOT** override any firewall rules defined on other pages, such as service access (allow) or redirect rules.

**Recommended Setting:** Yes.

**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.

To restrict access via a configured 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→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.

**Recommended Setting:** Yes.

**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.

To restrict access via a configured 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→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.

**Recommended Setting:** No.

**Modbus:** Reserved for future use.

**DNP3:** Reserved for future use.

**Web UI:** To allow external devices to connect to the Web UI, through untrusted interfaces on this unit, select Yes, otherwise select No.

To restrict access via a configured 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→Subnet Whitelist Rules** screen.

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

**Recommended Setting:** Yes.

**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.

To restrict access via a configured 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→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.

**Recommended Setting:** Yes.

## Other Options

**Allow IPSec:** Specify whether to allow ESP data, as well as UDP port 500, to communicate with external devices through untrusted interfaces.

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

**Recommended Setting:** Yes.

**Allow NAT-Traversal:** Specify whether to allow data on UDP port 4500 on untrusted interface.

**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.

**Recommended Setting:** Yes

**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 upstream router is preventing PMTU discovery from operating properly.

**Recommended Setting:** No.

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

**Normal:** 2 messages per second max

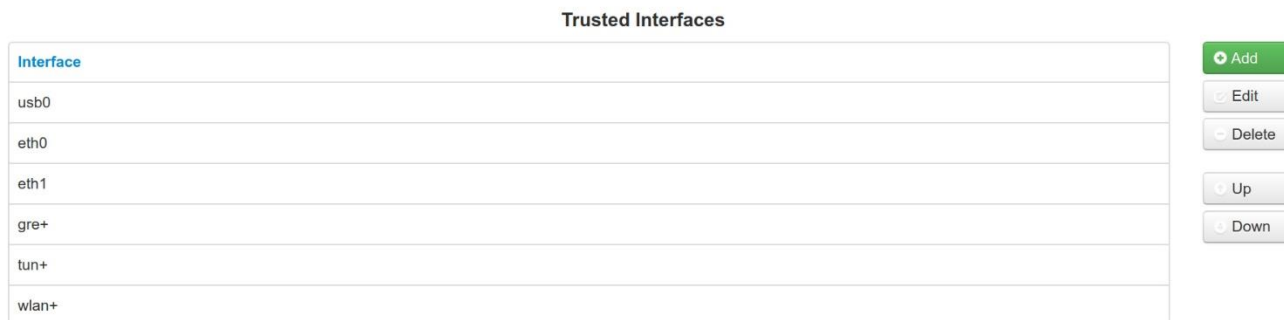
**Quieter:** 10 messages per minute max  
**Silent:** No messages are logged

**Local HTTP Redirect:** This option will control the automatic generation of local interface HTTP/HTTPS redirect firewall rules. If enabled, then when Trusted Ethernet/USB interfaces come up, automatic rules are added so any local traffic going to the IP address of that interface with a destination of port 80 or 443 will be automatically redirected to port 10000 and 10001 respectively.

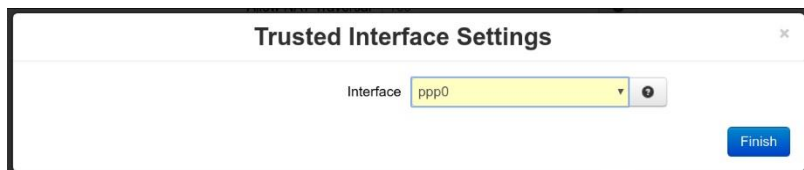
**Recommended Setting:** Yes.

### Trusted Interfaces

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



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



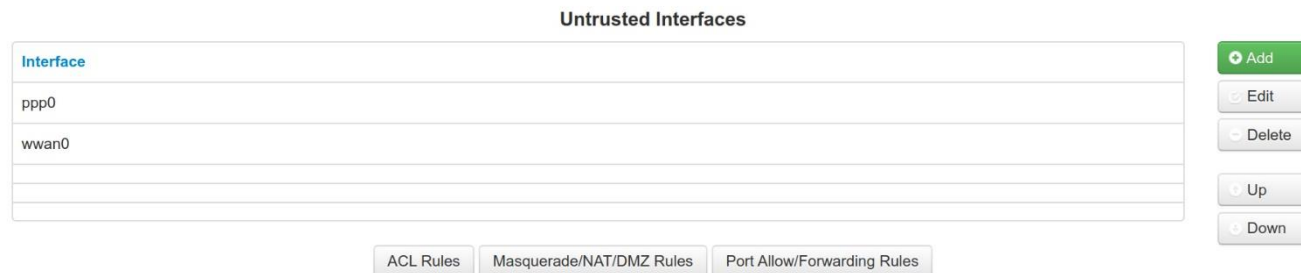
**Interface:** Trusted interfaces will not block traffic to/from devices connected to that interface. Filter Rules are the only rules that will control traffic on these interfaces.

Choose an interface from the drop-down lists 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 appears:



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



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

Choose an interface from the drop-down lists 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 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

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 DA50N. Blacklist Rules are used to define a single IP Address or an entire network that are NOT allowed to access the network behind the DA50N.

**Firewall Access Control List (ACL) Rules**

**Current Whitelist Groups**

default: 0.0.0.0/0

**Subnet Whitelist Rules**

Name	Subnet
default	0.0.0.0/0

Whitelist Control on Outbound Restrictions: No Restrictions

**Subnet Blacklist Rules**

Subnet

**Filter Rules**

Label	In Interface	Source (Whitelist)	Out Interface	Destination

[General Settings](#)
[Masquerade/NAT/DMZ Rules](#)
[Port Allow/Forwarding Rules](#)

### Current Whitelist Groups

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

### Subnet Whitelist Rules:

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

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

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

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

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



The image shows a dialog window titled "Whitelist Rules Settings" with a close button (X) in the top right corner. It contains two input fields: "Enter Whitelist name" and "Enter Subnet". Each field has a red border and a "Required" label to its right. Below the input fields is a blue "Finish" button.

**Enter Whitelist name:** 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 you click the **OK** button, you will see the entry 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 nor have its name changed, but its subnet value may be changed. Additional entries may be added, edited and deleted as needed. (Required)

**Enter Subnet:** 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. (Required)

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

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

**Whitelist Control on Outbound Restrictions:** This setting controls whether or not the whitelist rules apply to packets originating from this device and being routed through the device.

There are two (2) choices:

- Only to Whitelist IPs from local
- No Restrictions

When Only to Whitelisted IPs from local is selected, packets that originate locally from the device that are destined for subnets outside those specified in any whitelist will be suppressed by the firewall.

When No Restrictions is selected, the device may send a packet to any subnet and the whitelist rules apply only to packets received.

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

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

### Subnet Blacklist Rules

These rules are used to define a single IP Address or an entire network that are NOT allowed to access the network behind the DA50N.

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



**Enter Subnet to Blacklist:** 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 section's rules (Allow/Redirect/DMZ/NAT/etc). (Required)

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.

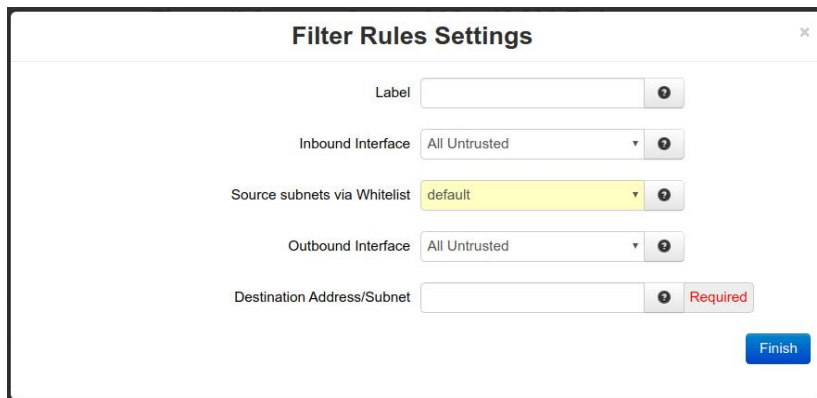
### Filter Rules

**Firewall 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 appears:



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



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

**Recommended Setting:** Optional.

**Inbound Interface:** Select the interface associated with the Source Address/Subnet. (Required)

**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**→**Subnet Whitelist Rules** screen.

**Outbound Interface:** Select the interface associated with the Destination Address/Subnet. (Required)

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

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

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

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

### Masquerade/NAT/DMZ Rules

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

## Firewall

### Masquerade Rules

Orig. Src. Subnet	Interface
0.0.0.0/0	All Untrusted

- [+ Add](#)
- [Edit](#)
- [Delete](#)
- [Copy](#)
- [Up](#)
- [Down](#)

### NAT (One-To-One) Rules

Label	Orig. Dest. Addr.	New Dest. Addr.	Protocol	Source (Whitelist)

- [+ Add](#)
- [Edit](#)
- [Delete](#)
- [Copy](#)
- [Up](#)
- [Down](#)

### NAT Range (One-To-One) Rules

Label	Orig. Dest. Addr. Start	Orig. Dest. Addr. End	New Dest. Addr. Start	New Dest. Addr. End	Protocol	Source (Whitelist)

- [+ Add](#)
- [Edit](#)
- [Delete](#)
- [Copy](#)
- [Up](#)
- [Down](#)

### DMZ Host Rules

Label	Interface	DMZ Host Address	Source (Whitelist)

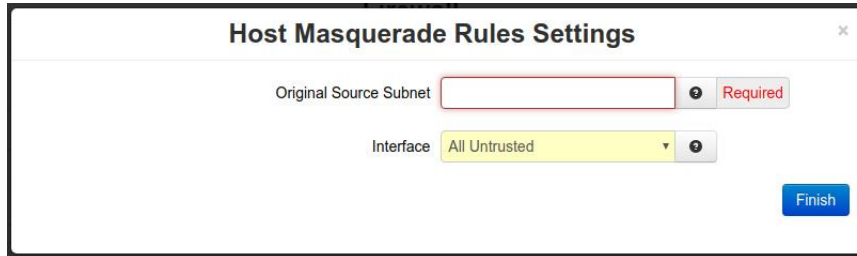
- [+ Add](#)
- [Edit](#)
- [Delete](#)
- [Copy](#)
- [Up](#)
- [Down](#)

[General Settings](#)
[ACL Rules](#)
[Port Allow/Forwarding Rules](#)

## Masquerade Rules

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

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



The dialog window titled "Host Masquerade Rules Settings" contains the following fields and controls:

- Original Source Subnet:** A text input field with a red border and a "Required" label to its right.
- Interface:** A dropdown menu currently showing "All Untrusted" with a "Required" label to its right.
- Finish:** A blue button located at the bottom right of the dialog.

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

**Interface:** Select the interface through which you wish to masquerade source addresses. (Required)

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

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

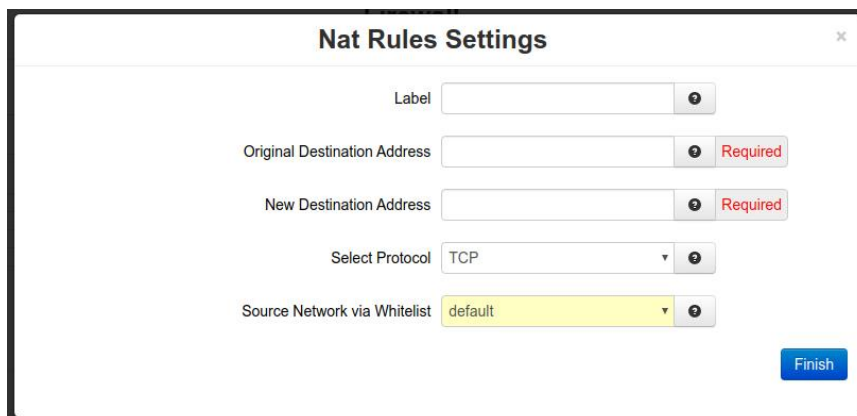
## NAT (One-To-One) Rules

The NAT (Network Address Translation) 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 the DA50N, 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.

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



The dialog window titled "Nat Rules Settings" contains the following fields and controls:

- Label:** A text input field with an information icon to its right.
- Original Destination Address:** A text input field with a "Required" label to its right.
- New Destination Address:** A text input field with a "Required" label to its right.
- Select Protocol:** A dropdown menu currently showing "TCP" with an information icon to its right.
- Source Network via Whitelist:** A dropdown menu currently showing "default" with an information icon to its right.
- Finish:** A blue button located at the bottom right of the dialog.

**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.

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

**Recommended Setting:** Optional

**Original Destination Address Start:** This field holds the address being transformed by NAT, the IP seen by a remote host. This address may be owned by an interface on this device, or an unowned/fake range with a corresponding route (static or default).

One-to-one NAT will perform a complete forwarding of all ports on the Original Destination IP to a new IP address entered in New Destination. Both fields can be any valid IP. Neither need to be already present/configured/owned on a local interface of this device. (Required)

**Note:** Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.  
Ports 1-19 are excluded.

**New Destination Address Start:** This field holds the starting range of real LAN IP of the destination device behind this 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. (Required)

**Note:** Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.  
Ports 1-19 are excluded.

**Select Protocol:** Choose the protocol type for this port's data. Options are TCP, UDP, All. TCP or All will restrict incoming source ports to be 1024 or higher. Choosing UDP will allow source ports lower than 1024. (Required)

**Source network via Whitelist:** Select a whitelist name from the list of names available in the drop-down list box provided.

Whitelists may be viewed/defined via the **Network→Firewall→ACL Rules→Subnet Whitelist Rules** screen.

Click on the *Finish* button. You will be returned to the Masquerade/NAT/DMZ Rules dialog window and the NAT (One-To-One) 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 (One-To-One) Rules

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

The screenshot shows a web form titled "NAT Range Rules Settings". It contains several input fields: "Label" (text input), "Original Destination Address Start" (text input with "Required" label), "Original Destination Address End" (text input with "Required" label), "New Destination Address Start" (text input with "Required" label), "New Destination Address End" (text input with "Required" label), "Select Protocol" (dropdown menu with "TCP" selected), and "Source Network via Whitelist" (dropdown menu with "default" selected). A "Finish" button is located at the bottom right of the form.

**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.

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

**Recommended Setting:** Optional.

**Original Destination Address Start:** 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 **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. (Required)

**Note:** Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.  
Ports 1-19 are excluded.

**Original Destination Address End:** 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. (Required)

**Note:** Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.  
Ports 1-19 are excluded.

**New Destination Address Start:** This field holds the starting range of real LAN IP of the destination device behind this 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. (Required)

**Note:** Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.  
Ports 1-19 are excluded.

**New Destination Address End:** This field holds the ending range of real LAN IP of the destination device behind this DA50N.

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. (Required)

**Note:** Host Redirect and Service Access rules will apply first, and may prevent certain ports from reaching the New Destination.  
Ports 1-19 are excluded.

**Select Protocol:** Choose the protocol type for this port's data. Options are TCP, UDP, and All. TCP or All will restrict incoming source ports to be 1024 or higher. Choosing UDP will allow source ports lower than 1024. (Required)

**Source Network via Whitelist:** Select a whitelist name from the list of names available in the drop-down list box provided.

Whitelists may be viewed/defined via the **Network→Firewall→ACL Rules→Subnet Whitelist 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.

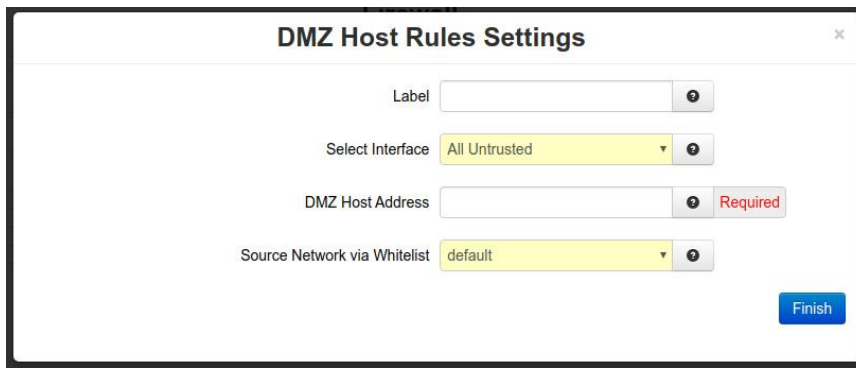
To delete an existing rule, select it in the table and click on the *Delete* button. To edit an existing rule, select it in the table and click on the *Edit* button.

### DMZ Host Rules

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



To add a DMZ host rule, click on the Add button and the following dialog window appears:



**Label:** Enter a description to describe this **DMZ Rule**. This field is not required for **DMZ Rules** functionality and it is just for **DMZ Rule** identification.

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

**Recommended Setting:** Optional.

**Select Interface:** 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. (Required)

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

**DMZ Host Address:** Enter the IP address of the DMZ Host. This IP address will receive all packets destined for the interface specified. (Required)

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

**Source Network via Whitelist:** Select a whitelist name from the list of names available in the drop-down list box provided.

Whitelists may be viewed/defined via the **Network**→**Firewall**→**ACL Rules**→**Subnet Whitelist 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 DA50N.

### 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 DA50N.

To add a new Service Access Rule, click on the Add button and the following dialog window:

**Label:** Enter a description to describe this **Allow Rule**. This field is not required for **Allow Rules** functionality and it is just for **Allow Rule** identification.

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

**Recommended Setting:** Optional.

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

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

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



**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. (Required)

**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. TCP will restrict incoming source ports to be 1024 or higher. Choosing UDP will allow source ports lower than 1024. (Required)

**Source Network via Whitelist:** Select a whitelist name from the list of names available in the drop-down list box provided.

Whitelists may be viewed/defined via the **Network→Firewall→ACL Rules→Subnet Whitelist 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 and the following dialog window appears:

The screenshot shows a dialog box titled "Host Redirect Rules Settings". It contains the following fields and controls:

- Label:** A text input field.
- Original Destination Port:** A text input field with a "Required" label to its right.
- Select Interface:** A dropdown menu currently showing "All Untrusted".
- New Destination IP Address:** A text input field with a "Required" label to its right.
- New Destination Port:** A text input field with a "Required" label to its right.
- MASQ Interface:** A dropdown menu currently showing "No".
- Select Protocol:** A dropdown menu currently showing "TCP".
- Source Subnets via Whitelist:** A dropdown menu currently showing "default".
- Finish:** A blue button at the bottom right of the dialog.

**Label:** Enter a description to describe this **Redirect Rule**. This field is not required for **Redirect Rules** functionality and it is just for **Redirect Rule** identification.

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

**Recommended Setting:** Optional.

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

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

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

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

**MASQ Interface:** This option hides the IP address of the remote incoming device and makes redirected traffic look like local LAN traffic. This is accomplished by masquerading. Useful when the target host does not have / cannot have a default gateway set in its routing table.

**Recommended Setting:** No.

**Select Protocol:** Choose the protocol type for this port's data. Options are TCP and UDP. TCP will restrict incoming source ports to be 1024 or higher. Choosing UDP will allow source ports lower than 1024. (Required).

**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→Subnet Whitelist 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.

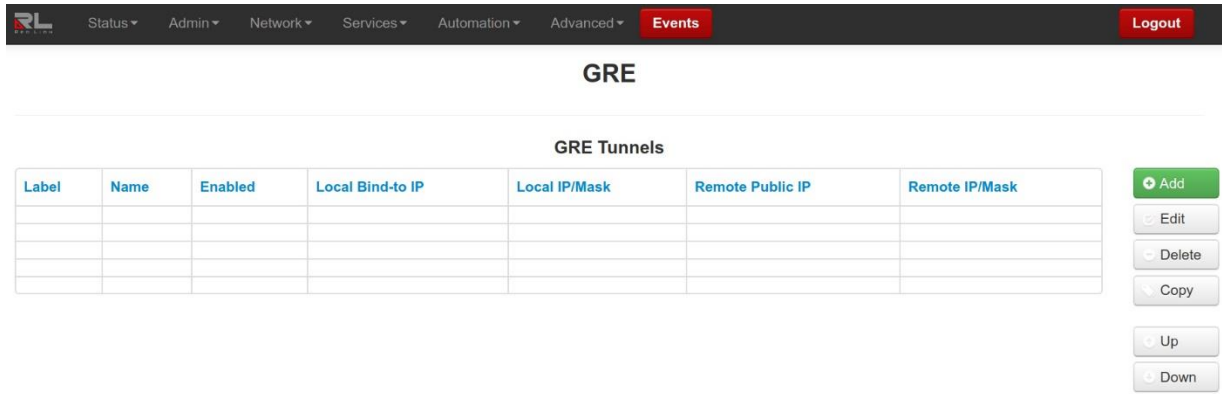
## Tunneling

The Tunneling menu is divided into three (3) sub-sections: GRE Tunnels, IPSec, and IPSec/L2TP.

### GRE

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

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



### GRE Tunnels

To add a GRE Tunnel:  
Click on the Add button and the Add GRE Tunnel pop-up window appears:

**Label:** Enter a description to describe this tunnel. This field is not required for GRE tunnel functionality and it is just for tunnel identification.

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

**Recommended Setting:** Optional.

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

**Enabled GRE Tunnel:** Select **Yes** to enable the tunnel. (Required)

**Local bind-to IP:** Set the local bind IP address for tunneled packets. This is useful when the tunnel should not originate on the default interface. Examples include a GRE tunnel used on and internal LAN

interface, or inside another tunnel such as IPSec. If your tunnel is not working, try entering the IP of the source interface here. (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:** Set the local GRE IP Endpoint IP/mask. (Required)

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

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

**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. (Optional)

**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. (Optional)

**Time-to-Live (Required):** Set a fixed Time-To-Live for tunneled packets. The valid values are 4 through 255.

**Note:** The Values over 64 may cause connection failures.

**Recommended Setting:** 64.

**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. **(Required)**

**Use DNS Lookup for Remote IP:** 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.

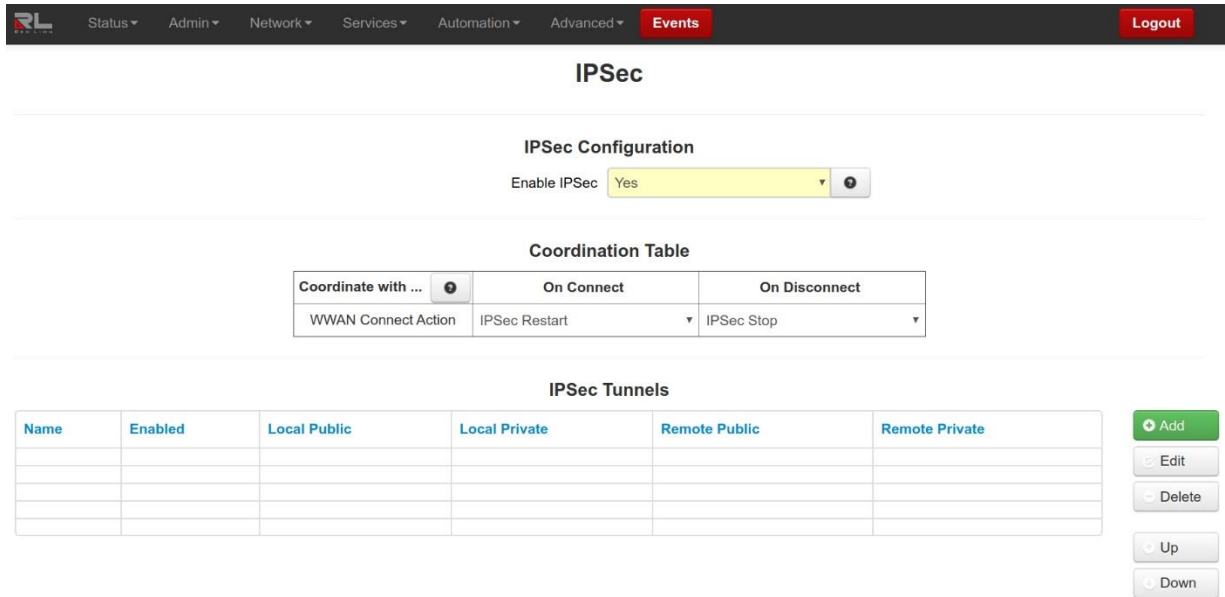
Click on the *Finish* button. You will be returned to the GRE Tunnels dialog window and the Configuration Table will now be populated with the recently entered data.

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.

### Coordination Table

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

The available actions include:

- Do Nothing:** Perform no action.
- Restart:** IPsec is restarted.
- Stop:** IPsec is stopped.

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

### IPsec Tunnels



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

The screenshot shows a 'General Settings' window with the following fields and options:

- Tunnel Name: Text input field with a 'Required' label and a help icon.
- Enable Tunnel: Dropdown menu set to 'Yes' with a help icon.
- Tunnel Type: Dropdown menu set to 'Client' with a help icon.
- Negotiation Mode: Dropdown menu set to 'Main' with a help icon.
- Dead Peer Detection Action: Dropdown menu set to 'Disable' with a help icon.
- Use Perfect Forward Secrecy: Dropdown menu set to 'Yes' with a help icon.
- Next: A blue button at the bottom right.

**Tunnel Name:** Enter some descriptive text in this field as an aid identifying it. The value must be alphanumeric characters plus (dash and underscore) and must not contain spaces or digits only. (Required)

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

**Tunnel Type:** 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 Negotiation, select Yes from the list provided, or No to prevent its 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 reestablish the connection to the concentrator. For this reason, "restart" may use more bandwidth and may not be the ideal choice for a limited data plan. However, if a host at the central site needs to initiate connections down to a local device through the tunnel, "restart" may be necessary so that the tunnel is always up and waiting for new data from the concentrator.

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

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

**Recommended Setting:** Yes.

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

The screenshot shows the 'Encryption Settings' dialog box. It features a title bar with a close icon. The settings are organized as follows:

- Phase 1 Encryption: AES256
- Phase 1 Authentication: SHA1
- Phase 1 DH Group: Group 14 - 2048 bits
- IKEv1 Padding: Yes
- Phase 1 ISAKMP Rekey Time (minutes): 480
- Encryption Method: Pre-Shared Key
- Pre-Shared Key: (empty field) with a red 'Required' label
- Local Peer ID: (empty field)
- Remote Peer ID: (empty field)
- Phase 2 Encryption: AES256
- Phase 2 Authentication: SHA1
- Phase 2 IPsec SA Lifetime (minutes): 60

Navigation buttons: 'Back' (grey) and 'Next' (blue).

**Phase 1 Encryption:** Select the type of encryption to use for Phase 1 (IKE).

Setting this option to "Default" will omit the specific settings for Phase 1 IKE Encryption-PRF-DHkey, and use a range of defaults that will try to match the remote end. If 'Default' is not used, then both ends must match if a specific Encryption-PRF-DHkey combination is used.

**Recommended Setting:** Default or AES256.

**Phase 1 Authentication:** Select the IKE authentication algorithm to be used for the connection.

**Recommended Setting:** Must match the other side of the connection. SHA2\_256 is recommended if supported by both.

**Phase 1 DH Group:** Select the DH Group you want to use for phase 1 (IKE) by choosing one of the values from the drop-down list provided.

Options include:

- Group 2 – insecure
- Group 5
- Group 14
- Group 15
- Group 16
- Group 17
- Group 18

This option selects the encryption level of the Diffie-Hellman keys, and these are Group 2 (1024 bits), Group 5 (1536 bits), Group 14 (2048 bits), Group 15 (3072 bits), Group 16 (4096 bits), Group 17 (6144 bits) or Group 18 (8192 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.

**Recommended Setting:** Group 14 or higher.

**IKEv1 Padding:** Choose whether or not to pad IKEv1 messages to a multiple of 4 bytes. Valid values are **Yes** (the default) and **No**.

**Phase 1 ISAKMP Rekey Time (minutes):** Select how long, in minutes, the keying channel of a connection (ISAKMP SA) should last before being renegotiated. It is recommended that the Phase 2 IPsec SA Lifetime is less than the Phase 1 ISAKMP Rekey timer.

**Encryption Method:** Specify how the two end-points for this tunnel should authenticate with each other. Current options are **Pre-Shared Key** and **X.509 Certificates**. You may select certificates only after they are loaded in the **Admin→Certificate Manager**. (Required)

**Pre-Shared Key:** Specify the key to be exchanged for encryption negotiation during phase 1 (IKE). Key must not contain a double-quote character. (Required)

**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 or 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 or a fully-qualified domain name preceded by @ (which is used as a literal string and not resolved).

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

Setting this option to "Default" will omit the specific settings for Phase 2 ESP Encryption-Auth, and use a range of defaults that will try to match the remote end. If 'Default' is not used, then both ends must match if a specific Encryption-Auth combination is used.

**Recommended Setting:** Default or AES256.

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

**Note:** Integrity algorithm 'NONE' can and must only be used with Phase 2 Encryption type AES\_CMM\_\* or AES\_GCM\_\* or the tunnel will not load. See syslog output for errors.

**Recommended Setting:** SHA1.

**Phase 2 IPsec SA Lifetime (minutes):** Select how long, in minutes, this IPsec SA (Security Association) should last, from successful negotiation to expiration. It is recommended that the Phase 2 IPsec SA Lifetime is less than the Phase 1 ISAKMP Rekey timer.

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



**Local Public IP Address:** Set the local bind IP address for tunneled packets. This is useful when the tunnel should not originate on the default interface. Examples include a GRE tunnel used on an internal LAN interface, or inside another tunnel such as IPsec. If your tunnel is not working, try entering the IP of the source interface here. (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 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 leftsubnet, to communicate to the rightsubnet or right. Otherwise, it uses its nearest IP address, which is its public IP address. This option is mostly used when defining subnet-subnet connections, so that the gateways can talk to each other and the subnet at the other end, without the need to build additional host-subnet, subnet-host and host-host tunnels.

**Local Gateway IP Address:** Specify the next-hop gateway IP address for the left participant's connection to the public network.

**Note:** If no value is provided, the tunnel uses the right participant as its next-hop.

**Local Private Subnet(s):** Specify the private subnet(s) behind the left participant, expressed in CIDR format (xxx.xxx.xxx.xxx/nn) as network/netmask.

More than one can be specified by using ',' to separate each entry.

**Remote Public IP Address:** Specify the IP address or Hostname of the right participant's public-network interface.

(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 configuration file.

**Remote Gateway IP Address:** Specify the next-hop gateway IP address for the right participant's connection to the public network.

**Note:** If no value is provided, the tunnel uses the left participant as its 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 can be specified by using ',' to separate each entry.

Click on the *Finish* button. You will be returned to the IPSec dialog window and the IPSec Tunnels table will not be populated with the recently entered data.

Name	Enabled	Local Public	Local Private	Remote Public	Remote Private
tunnel1	Yes			192.168.1.0/24	

Add  
Edit  
Delete  
Up  
Down

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

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

### IPSec/L2TP

The IPSec/L2TP dialog window is split into three sections. The top section pertains to L2TP Configuration. The middle section is where the Coordination Table is defined. The last section is where IPSec/L2TP Static Routes are created and edited.

**IPSec/L2TP**

**L2TP Configuration**

Enable L2TP Yes

---

**Coordination Table**

Coordinate with ...	On Connect	On Disconnect
WWAN Connect Action	IPSec Restart	IPSec Stop

Tunnel Name

User Name

Password

Redial Timeout (seconds)

Dead Peer Detection Action Disable

Pre-Shared Key  Required

Local Peer ID

Local Public IP Address

Local Gateway IP Address

Local Private Subnet(s)

Remote Peer ID

Remote Public IP Address  Required

Remote Gateway IP Address

Remote Private Subnet(s)

Maximum Transmission Unit (MTU)

Maximum Receive Unit (MRU)

**IPSec/L2TP Static Routes Configuration**

[Add Static Route](#)

### L2TP Configuration

**Enable L2TP:** Specify whether you want to enable the IPsec service. If you select No, all tunnels will be disabled.

### Coordination Table

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

The available actions include:

**Do Nothing:** Perform no action.

**Restart:** IPSec is restarted.  
**Stop:** IPSec is stopped.

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

## L2TP Configuration

**Tunnel Name:** Enter some descriptive text in this field as an aid identifying it. The value must be alphanumeric characters plus (dash and underscore) and must not contain spaces or digits only. **(Required)**

**User Name:** Enter the descriptive name of the interface for this VPN connection. The username must be alphanumeric characters plus special characters.

**Password:** Enter the password to use for authenticating. **(Required)**

**Redial Timeout (seconds):** Enter the redial timeout for this VPN connection. The valid values are 15 seconds to 300 seconds.

**Recommended Setting:** Default: 30 seconds.

**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 reestablish 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.

**Pre-Shared Key:** Specify the key to be exchanged for encryption negotiation during phase 1 (IKE). Key must not contain a double-quote character. **(Required)**

**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 or a fully-qualified domain name preceded by @ (which is used as a literal string and not resolved).

**Local Public IP Address:** Set the local bind IP address for tunneled packets. This is useful when the tunnel should not originate on the default interface. Examples include a GRE tunnel used on an internal LAN interface, or inside another tunnel such as IPSec. If your tunnel is not working, try entering the IP of the source interface here. **(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 Gateway IP Address:** Specify the next-hop gateway IP address for the left participant's connection to the public network.

**Note:** If no value is provided, the tunnel uses the right participant as its next-hop.

**Local Private Subnet(s):** Specify the private subnet(s) behind the left participant, expressed in CIDR format (xxx.xxx.xxx.xxx/nn) as network/netmask.

More than one can be specified by using ',' to separate each entry.

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

**Remote Public IP Address:** Specify the IP address or Hostname of the right participant's public-network interface.

(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 configuration file.

**Remote Gateway IP Address:** Specify the next-hop gateway IP address for the right participant's connection to the public network.

**Note:** If no value is provided, the tunnel uses the left participant as its 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 can be specified by using ',' to separate each entry.

**Maximum Transmission Unit (MTU):** Enter maximum transmission unit (MTU). The valid values are 800 – 1400.

**Recommended Setting:** 1400.

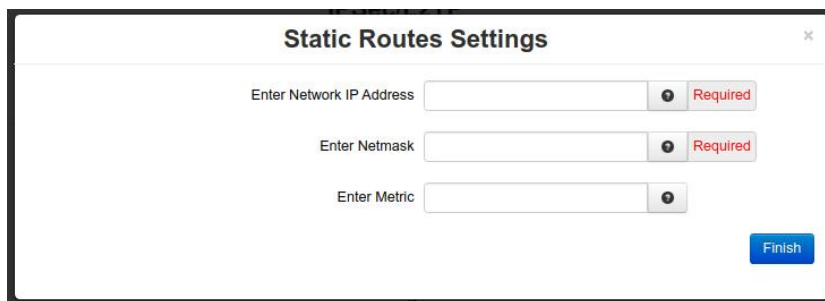
**Maximum Receive Unit (MRU):** Enter maximum receive unit (MRU). The valid values are 800 – 1400.

**Recommended Setting:** 1400.

## IPSec/L2TP Static Routes Configuration

### Add Static Route

Click on the *Add Static Route* button and the following **Static Routes Settings** dialog window appears:



**Enter Network IP Address:** Enter the Network IP Address of the destination network to which the route should be created. This must be a valid Network IP address for the value entered in the **Enter Netmask** field. (Required)

**Enter Netmask:** Enter the desired Netmask for the router in the field provided.

This field is only available when **Select Route Type** has been set to Network. (Required)

**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 Network IP Address** field.

**Enter Metric:** Enter a value for the route metric in this field.

This parameter may be used routing protocols to determine the best way to route traffic.

**Recommended Setting: 0.**

Click the *Finish* button. You will be returned to the IPSec/L2TP dialog box and the IPSec/L2TP Static Routes Configuration table will now be populated with the recently entered data.

**IPSec/L2TP Static Routes Configuration**

Interface	Target IP Address	Netmask	Metric	
ppp100		255.255.255.0	0	<span>Edit</span> <span>Delete</span>

Add Static Route

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

## DNS Settings

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

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

**DNS Settings**

Enter Search Domain

Enter Primary DNS Server  Required

Enter Alternate DNS Server #1

Enter Alternate DNS Server #2

**Static Hosts**

Host Name	Domain	IP Address

Add  
Edit  
Delete  
Copy  
Up  
Down

**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:** Enter the IP Address of the Primary DNS Server you want to use. **(Required)**

**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:** 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:** 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 DA50N to resolve local host names to IP addresses.

Host Name	Domain	IP Address

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

**Static Host Settings** ✕

Enter Host Name  ⓘ Required

Enter Domain Name  ⓘ

Enter Client IP Address  ⓘ Required

**Enter Host Name:** Enter the desired Host Name in this field. **(Required)**

**Enter Domain Name:** Enter the desired Domain Name in this field.

**Enter Client IP Address:** Enter the host IP Address in this field. **(Required)**

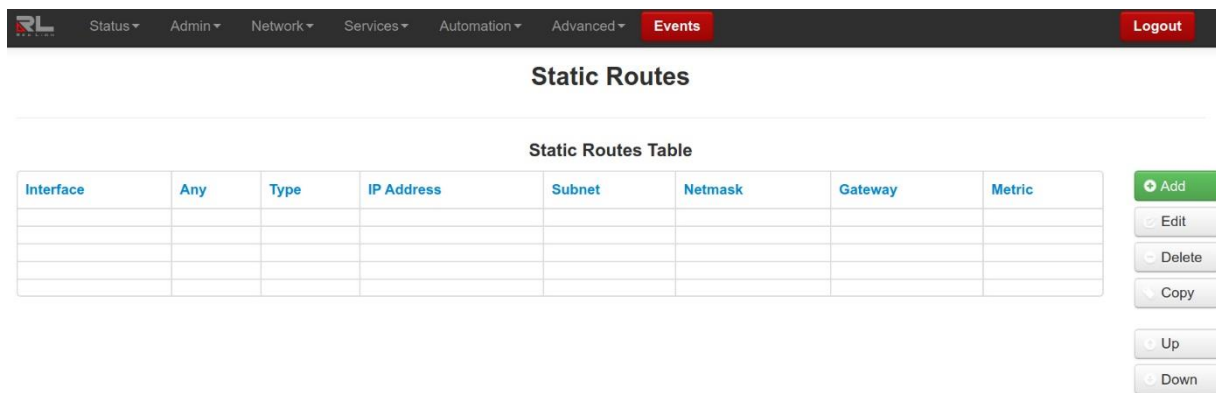
Click on the *Finish* button. You will return to the DNS Settings dialog window and the Static Hosts table will now be populated with the recently entered data.

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

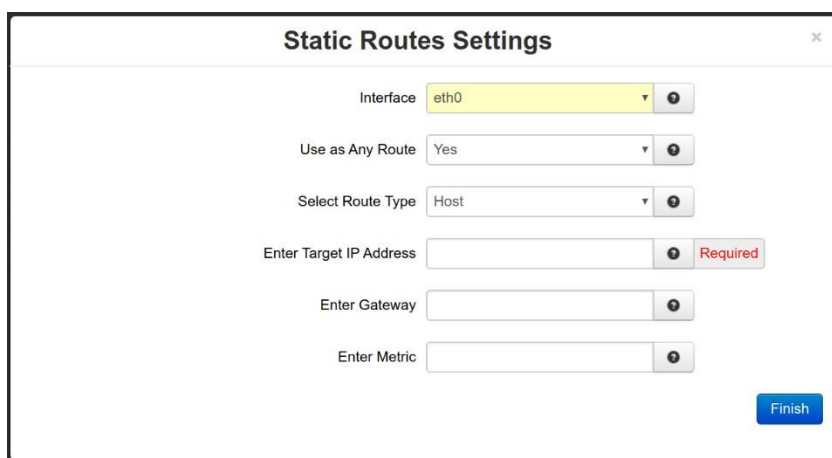
Click on the *Save* button for changes to be saved without activating them until you reboot the unit. The *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

## Static Routes

The Static Routes menu allows you to configure a route to a network through an interface manually. Click on the *Static Routes* menu item and the Static Routes dialog window will open:



To add a Static Route on the DA50N:  
Click on the Add button and the dialog window below appears:



**Interface:** Select the interface to which the route should apply by selecting one of the available options from the drop-down list provided.

The available interfaces varies depending on the particular model of device, as well the current configuration and may include those created as aliases, VPN tunnels and/or ppp interfaces related to a cellular modem.

**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 dropdown 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 eth0, and the ppp0 interface becomes active, then the route will be reapplied to eth0.

When set to No, the route will take effect only when a network change occurs on the configured interface.

For example, if the configured interface is eth1, then the route will be assigned only when eth1 has a network change to an active state.

**Select Route Type:** Select the type of route to be created by choosing one of the available options from the provided drop-down list.



Choices include:

- Host
- Network

Select Host to create a route to a specific device.

This will require setting the **Target 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:** Enter the IP Address of the destination host to which the route should be created. (Required)

**Enter Gateway:** Enter the IP Address of the gateway for the specified host or network.  
(Required) for non point-to-point type interfaces.

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 be 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.

**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 on which the designated interface resides.

**Enter Metric:** Enter a value for the route metric in this field.

This parameter may be used routing protocols to determine the best way to route traffic.

**Recommended Setting:** 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.

## TCP Global Settings

Click on the *TCP Global Settings* menu item the following dialog window appears:

**Connection Tracking**  
[SYN] Tx Timeout (seconds) 65 Required

**TCP Keep Alives**  
Enter Timeout (seconds) 300 Required  
Enter Maximum Probe Attempts 4 Required

**MTU**  
Disable Path MTU Discovery No

**Routing Options**  
Enable Reverse Path Filter Strict Mode

**Arp Filtering**  
Eth0 Arp Filtering On  
Eth1 Arp Filtering On

### Connection Tracking

**[SYN] Tx Timeout:** Specifies the timeout value, in seconds, for SYN packets for connection tracking.

**Recommended Setting:**

65 is the generally recommended default which differs from the system default of 120.  
30 - 120 is the recommended tuning range.

### TCP Keep Alives

**Enter Timeout (seconds):** 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.

**Recommended Setting:**

10 - 30 for Ethernet connections where data usage is not an issue.  
60 - 300 for cellular connections where total data usage must be considered.

**Enter Maximum Probe Attempts:** 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.

**Recommended Setting:** 3 - 6.

### MTU

**Disable Path MTU Discovery:** Enable / Disable Path MTU Discovery. This might be useful if a private cellular network is restricting MTU sizes along the network path and causing packet drops.

**Recommended Setting:** No.

### Routing Options

**Enable Reverse Path Filter:** Select desired Reverse Path Filter (rp\_filter) option.

Reverse path filtering is a mechanism adopted by the Linux kernel, as well as most of the networking devices out there 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.

## Arp Filtering

**Eth0 Arp Filtering:** Turning this option on will force eth0 to only answer ARP requests for IPs configured on the eth0 interface.

**Eth1 Arp Filtering:** Turning this option on will force eth1 to only answer ARP requests for IPs configured on the eth1 interface.

Click on the *Apply* button to save the newly entered values. To refresh the window, click on the *Refresh* button.

## Services Tab

The Services Tab is where you can configure the various service offerings of the DA50N. These services include DHCP Server, DHCP Relay, Dynamic DNS, SN Proxy Settings, SixView Manager, GPS Settings, SSH/TELNET Server, SSL Connections, SNMP Agent, Ping Alive, Crimson Connect, Email Client, SMS Handling, FTP Server, SD Card Manager, and Serial IP.

### 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 DA50N.

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

RL
Status ▾ Admin ▾ Network ▾ Services ▾ Automation ▾ Advanced ▾ **Events** Logout

### DHCP Server Settings

---

**Global Settings**

Enter Domain Name

Use Standard DNS Settings

Default Lease Time (seconds)  Required

Maximum Lease Time (seconds)  Required

Minimum Lease Time (seconds)  Required

---

**Ethernet Port 1 (eth0)** (Obtaining addresses via DHCP - unable to act as server)

Enable DHCP

---

**Ethernet Port 2 (eth1)** ( using netmask 255.255.255.0)

Enable DHCP

---

**USB (usb0)** ( using netmask 255.255.255.0)

Enable DHCP

Enable Default Gateway

Starting Address  Required

Ending Address  Required

---

**Wi-Fi (wlan0s1)** (Obtaining addresses via DHCP - unable to act as server)

Enable DHCP

---

---

**Distribute DHCP Leases Based on MAC Address**

Client MAC Address	Client IP Address

### Global Settings

**Enter Domain Name:** Enter the Domain Name that will be passed to DHCP Clients.

**Recommended Setting:** User Preference.

**Use Standard DNS Settings:** Choosing **Yes** will automatically use the DNS Servers obtained by this unit's internet connection and/or entries specified in Network→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.

**Recommended Setting:** Yes.

**Primary DNS Server IP Address:** Enter the IP address of the Primary DNS Server that will be passed to DHCP clients. (Required)

**Secondary DNS Server IP Address:** Enter the IP address of an alternate DNS Server that will be passed to DHCP clients. (Required)

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

**Recommended Setting:** User Preference, default 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.

**Recommended Setting:** User Preference, default is 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.

**Recommended Setting:** User Preference, default is 3600 (1 hour).

Ethernet Port 1 (eth0)

**Enable DHCP:** Specify whether you want to enable a DHCP Server for the interface.

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

**Enable Default Gateway:** Provide Default Gateway IP Address to DHCP Client.

**Recommended Setting:**

**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.

**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. (Required)

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

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

**Recommended Setting:** A valid address 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.

Ethernet Port 2 (eth1)

**Enable DHCP:** Specify whether you want to enable a DHCP Server for the interface.

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

**Enable Default Gateway:** Provide Default Gateway IP Address to DHCP Client.

**Recommended Setting:**

**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.

**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. **(Required)**

**Recommended Setting:** A valid address for the subnet for which the interface is configured.

Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

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

**Recommended Setting:** A valid address 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.

USB (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.

**Recommended Setting:**

**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.

**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. **(Required)**

**Recommended Setting:** A valid address for the subnet for which the interface is configured.

Care should be used to ensure that there is no conflict with any pre-existing devices on that subnet which may have been already configured to use statically assigned IP addresses.

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

**Recommended Setting:** A valid address 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 Leases* button to to display the current DHCP leases logged on to the unit.

## Distribute DHCP Leases Based on MAC Address

**Distribute DHCP Leases Based on MAC Address**

Client MAC Address	Client IP Address

Click on the *Add* button to assign an IP Address to a device based on a MAC address, so that device obtains the same IP each time it requests a new IP from the DHCP server. The following window appears:

**Add Distribute DHCP Leases** ✕

Enter Client MAC Address  ? Required

Enter Client IP Address  ? Required

**Enter Client MAC Address:** Enter the Client's computer or device MAC address.

**Client MAC Address:** The Media Access Control (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 on to the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

When entering the MAC address information, you will type the 12-digit MAC address in this format, **xx:xx:xx:xx:xx:xx** including the hyphens.

**Enter Client IP Address (Required):** Enter the IP address for which you wish to assign to a client's computer or device MAC address.

**Client IP 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 use statically assigned IP addresses.

**Recommended Setting:** 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.

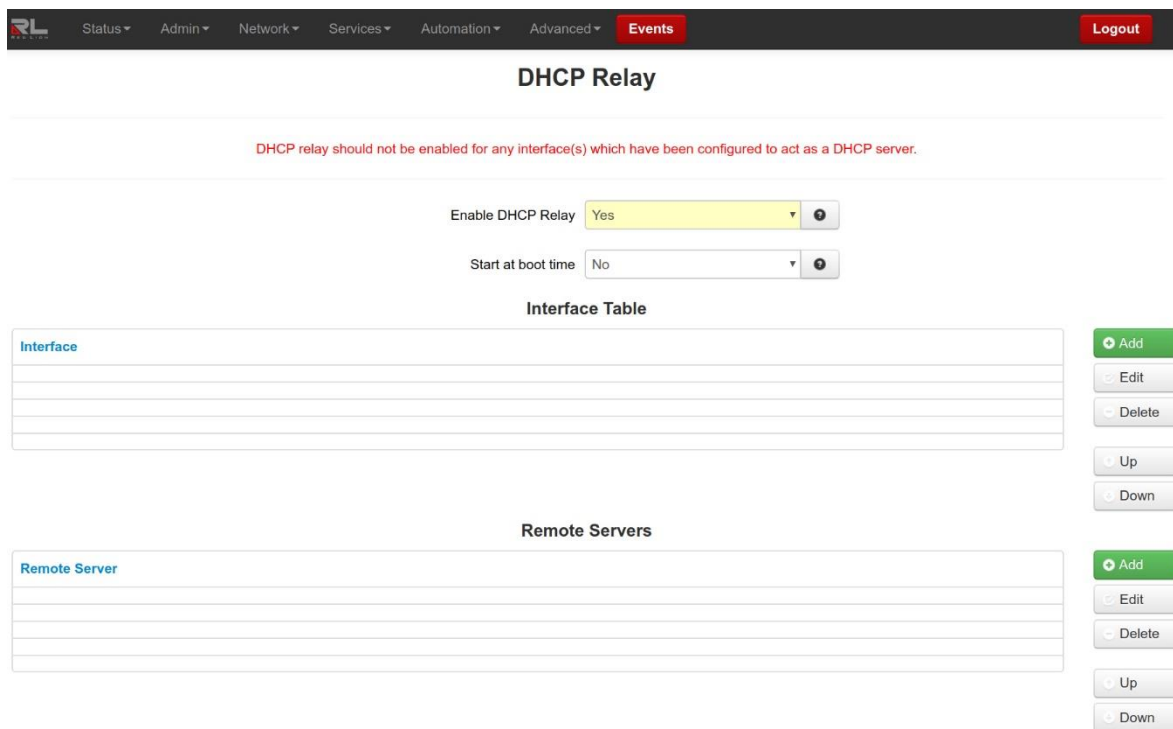
To delete an address, select it in the table and click on the *Delete* button. To edit an existing address, select it in the table and click on the *Edit* button.

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

## 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) that have been configured to act as a DHCP server.

Click on *DHCP Relay* and the following dialog window appears:



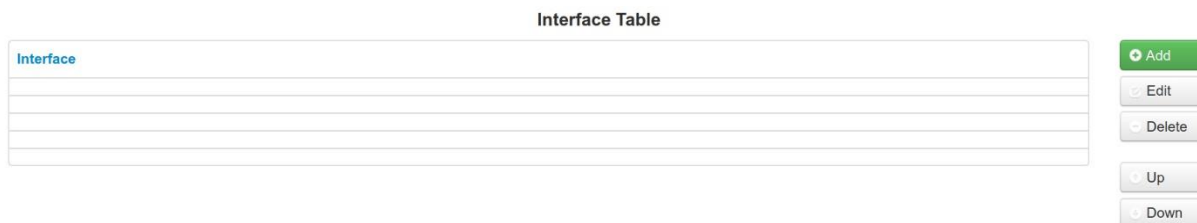
**Enable DHCP Relay:** This will enable a DHCP Relay service, which will connect a local interface with a remote DHCP Server.

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 after the device is rebooted and then only if the **Start at boot time** option has been also set to Yes.

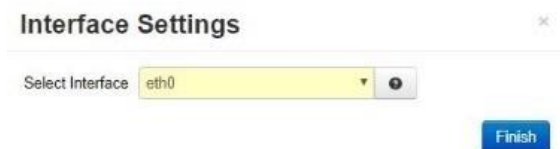
**Start at boot time:** Select Yes to enable the DHCP Relay at boot time, or No for manual control.

If the DHCP Relay service is required to be operational at all times, then set to Yes. If another process, such as VRRP, is going to dynamically enable/disable DHCP Relay service as needed, then set to No.

Interface Table



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

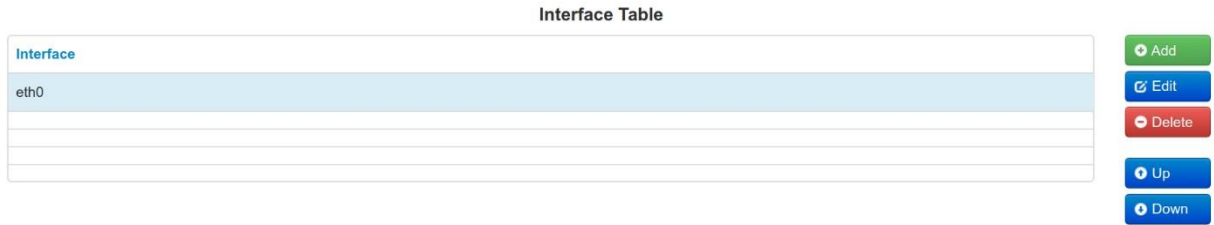


**Select Interface:** Select the interface for which DHCP relay is to be employed by selecting one of the available options from the drop-down list provided. If an interface is not specified, then DHCP Requests from that interface will be ignored.



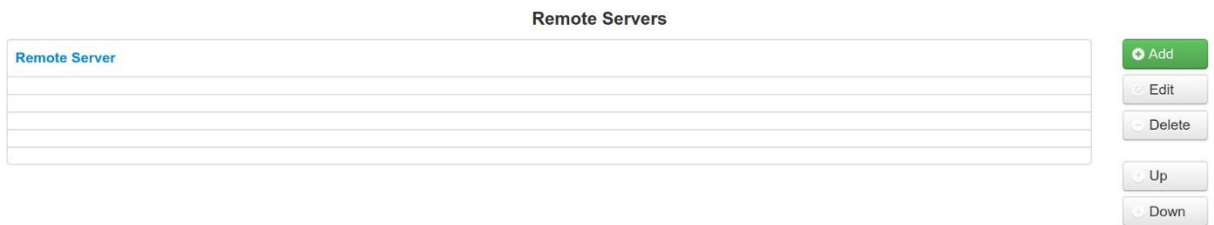
The available interfaces varies depending on the particular model of this device, as well the current configuration.

Click on the *Finish* button. You will be returned to the DHCP Relay dialog window and the Interface Table will be populated with the entered data.



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

### Remote Servers

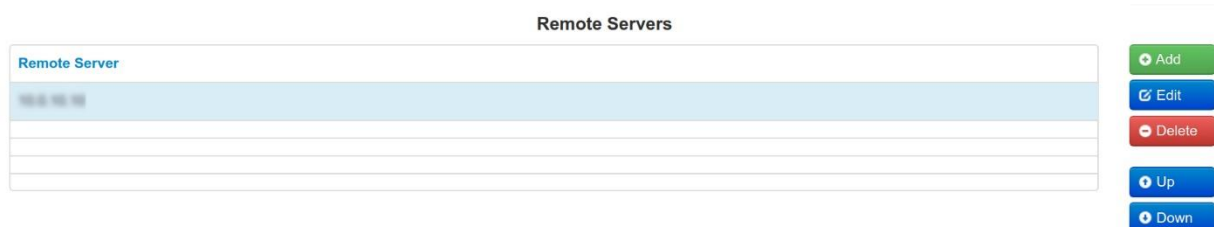


Click on the *Add* button and the following dialog window appears:



**Remote Server:** Enter the IP Address or Fully Qualified Domain Name of all remote DHCP Servers available. It is the responsibility of the remote DHCP Server to coordinate the issuing of DHCP addresses.

Click on the *Finish* button. You will be returned to the DHCP Relay dialog window and the Remote Servers table will be populated with the entered data.



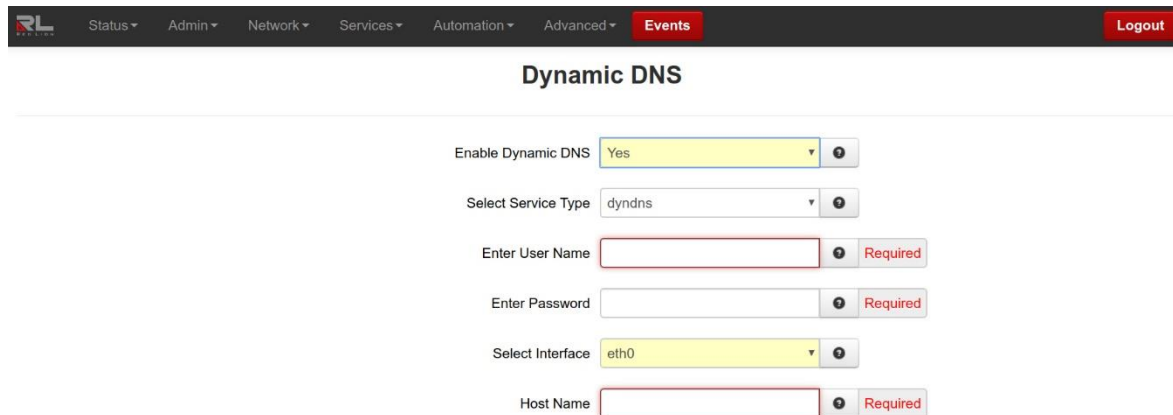
To delete an existing server, select it in the table and click on the *Delete* button. To edit an existing server, select it in the table and click on the *Edit* button.

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

## Dynamic DNS

The Dynamic DNS menu item is used to configure a dynamic DNS name for the DA50N that does not have a static public IP Address. A subscription to a service providing Dynamic DNS, such as DYNDNS.ORG, is required.

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



The screenshot shows the 'Dynamic DNS' configuration dialog window. At the top, there is a navigation bar with the following items: Status, Admin, Network, Services, Automation, Advanced, Events (highlighted in red), and Logout. The dialog title is 'Dynamic DNS'. The configuration options are as follows:

- Enable Dynamic DNS:** A dropdown menu set to 'Yes'.
- Select Service Type:** A dropdown menu set to 'dyndns'.
- Enter User Name:** A text input field with a red border and a 'Required' label.
- Enter Password:** A text input field with a red border and a 'Required' label.
- Select Interface:** A dropdown menu set to 'eth0'.
- Host Name:** A text input field with a red border and a 'Required' label.

**Enable Dynamic DNS:** Select **Yes** to enable the Dynamic DNS Service.

**Select Service Type:** Select the desired Dynamic DNS Service from the list provided.

**Enter User Name:** Enter the User Name used to access your Dynamic DNS service in this field. Allowable characters are alphanumeric and - and \_ characters. (Required)

**Enter Password:** Enter the Password used to access your Dynamic DNS Service in this field. (Required)

**Confirm Password (Required):** Re-enter the Password entered in the field above. The passwords must match or you will be prompted to re-enter it.

**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:** Enter the host name and domain you wish to be assigned by the Dynamic DNS service. (Required)

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.

## SN Proxy Settings

SN Proxy is a web relay proxy service used to gain access to devices that are behind our DA50N providing additional security and access control to devices that may not offer such functionality. A proxy based service provides a more robust connection than just using a port forward rule, including the ability to add an additional user login for authentication, encryption via SSL as well as isolation via Access Control Lists.

Click on the *SN Proxy Settings* menu item and the SN Proxy Settings dialog window will open.

**SN Proxy Settings**

Enable SN Proxy Settings: Yes

Use HTTPS/SSL Encryption: No

Use HTTP login: No

Listen Port: [ ] Required

Host IP: [ ] Required

Host Port: 20000 Required

**Enable SN Proxy Settings:** Select **Yes** to configure SN proxy server.

**Use HTTPS/SSL Encryption:** Select **Yes** to enable HTTPS/SSL encryption between you and the proxy server.

**Use HTTP login:** Require username and password to connect to proxy server.

**User Name:** Enter username required to connect to proxy server.

**Password:** Enter password required to connect through this proxy server.

**Listen Port:** Enter the port number the proxy server listens on.

**Note:** You may need to open this port in the firewall via **Network→Firewall→Port Allow/Forwarding Rules→Service Access Rules**.

**Host IP:** Enter the IP address of your destination host.

**Host Port:** Enter the listening port of your destination host.

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.

## Sixview Manager

The SixView Manager menu item allows you to configure various aspects of the SixView Manager Client to communicate with a SixView Manager hosted at Red Lion or at your location.

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

The screenshot shows the SixView Manager web interface. At the top, there is a navigation bar with tabs for Status, Admin, Network, Services, Automation, Advanced, and Events (which is active), and a Logout button. Below the navigation bar, the title "SixView Manager" is centered. The main content area displays the current client status as "ENABLED". It shows the next check-in time as "5 hours, 50 minutes, 25 seconds" and the reporting to "engineering.sixviewmanager.com". A "Last Check In:" section shows two successful check-ins: "engineering.sixviewmanager.com | Success | Tue Aug 6 05:09:39 2019" and "server2.sixviewmanager.com | N/A | Tue Aug 6 05:09:39 2019". Below this, there are "Refresh" and "Check-In Now" buttons. The configuration section includes several fields: "Enable SixView Manager Access" (set to Yes), "Primary Server Address" (engineering.sixviewmanager.com, Required), "Secondary Server Address" (server2.sixviewmanager.com), "Select Connection Mode" (Secondary when Primary unav), "Enter Access Interval (minutes)" (480, Required), "Enter Error Interval (minutes)" (120, Required), "Select Access Method" (Encrypted (https)), "Enter SixView Manager Secure Server Port" (18081, Required), and "Select Interface" (None).

**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.

**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.

**Recommended Setting:** Yes.

**Primary Server Address** Enter the IP Address or host name of your SixView Manager primary server. **(Required)**

**Recommended Setting:** When changing the Primary Address to your own private SixView Manager server, you may want to consider setting the Secondary Address to the SixView Manager test server (server1.sixviewmanager.com) for trial and initial production rollouts. This will enable 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.

**Recommended Setting:** When changing the Primary Address to your own private SixView Manager server, you may want to consider setting the Secondary Address to the SixView Manager server (server2.sixviewmanager.com) for trial and initial production rollouts. This will enable support staff to monitor the progress and better assist in diagnosing potential problems.

**Select Connection Mode:** Select the desired Connection Mode from the provided drop-down.

There are four connection modes:

**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.

**Recommended Setting:** "Secondary when Primary unavailable" or "Both" are the preferred methods in configurations supporting dual SixView Manager servers.

**Enter Access Interval (minutes):** Enter the number of minutes the SixView Manager Client process should wait before connecting to the SixView Manager server. (Required)

**Note:** While lower values can result in more timely status reports with the SixView Manager Server, it comes at an expense of increased data traffic, which may be an issue when the connection utilizes a cellular modem with a service plan where cost is based on bandwidth usage.

**Recommended Setting:** A value of 220 is suggested for Cellular carriers that use an inactivity timeout of four hours.

**Enter Error Interval (minutes):** Enter the number of minutes the SixView Manager Client process should wait before connecting to the SixView Manager server. (Required)

**Recommended Setting:** 30.

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

There are two access methods:

**Unencrypted (http):** Faster, but less secure.

**Encrypted (https):** Slower, but more secure.

Note that the encrypted method adds significant overhead which may be a consideration when using a cellular modem connection.

**Recommended Setting:** Should be coordinated with the Administrator of your particular SixView Manager server. Choose **http** when using the server1.sixviewmanager.com server.

**Enter SixView Manager Secure Server Port:** 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. (Required)

**Recommended Setting:** 18081 - For https Access Method.

**Select Interface:** Select the name of the interface to which the SixView Manager Client will bind for communications with the SixView Manager Server.

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

**Recommended Setting:** None.

Click *Apply* for the settings to take effect immediately. Selecting *Revert*, will reset all fields to factory defaults.

## GPS Settings

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

GeoFence Engine State: Options and descriptions are listed in this field. Eventable register state is listed in parenthesis next to the label.

**Monitor Only (0):** Reporting GPS location only. No GeoFence Lockdown.

**Lockdown – Waiting for Data (1):** Waiting on GPS data to compute lockdown fence.

**Lockdown – Wait for Entries (2):** Have data, but waiting on more entries to compute fence.

**Lockdown – Wait on Satellites (3):** Have entries, but waiting on better satellites to compute fence.

**Lockdown – Failed (4):** Lockdown failed to build GeoFence (same behavior as Monitor Only).

**Lockdown – Good (5):** Successful lockdown. Fence built, and we are inside the GeoFence.

**Lockdown – Unstable (6):** ALERT. We are ok, but stray data points keep going outside fence, but are within satellite.

**Lockdown – Violation Alert (7):** ALERT. We are out of lockdown GeoFence. No Action Taken Yet.

**Lockdown – Violation Outside (8):** ERROR. We are out of lockdown GeoFence. Violation Action Taken.

**Lockdown – Violation no Data (9):** ERROR. We lost GPS data for enough time, that we don't know where we are. Violation Action Taken.

**Lockdown – Unknown State:** Undefined action type.

**View in Google Maps™:** Click on the button to view the physical location of the unit on Google maps.

**Start GeoFence Lockdown:** Click on this button to lock the device into a specific area. If the device moves from this location, the Select Violation Action selected in the GeoFence Violation Control section will come into effect. To disable the GeoFence Lockdown, start Monitor Only Mode.

**Start Monitor Only Mode:** Click on this button to log a violation. A violation will be logged but the option selected in the Select Violation Action field will not be performed.

### GPS Data Source

**GPS Data Source:** Select the data source from which the GPS data will be gathered. The available choices are:

**Internal** GPS location data will be sourced from the GPSd process. This process will automatically poll GPS data from supported devices as they are attached.

**External:** GPS location data will be gathered from an external serial GPS device. The serial port will need to be configured to select the onboard port as well as the serial data rate (defaulted to 4800, found in Advanced). The port may not be used with any other service simultaneously.

**Serial Interface:** When the **Data Source** has been set to External this field is enabled to allow selection of the TTY port to which an external GPS device has been attached. The available options will include one or more possible selections depending on the specific device model being used. For example, SN-5800 users should select ttyS5 here.

**Serial port speed:** When the **Data Source** is set to TTY Port, this field is enabled by which the Serial Port Speed may be selected using the drop-down list provided. The available options are:

1200

2400

4800 (default)

9600

**Recommended Setting:** 4800

**Note:** This setting should not typically need to be changed, only if instructed by Support personnel or when provided with custom installation instructions.

**Fixed:** GPS data will not be collected from an actual source, but will be emulated as the fixed values entered by the user. Any Lat/Long point may be specified, in decimal format, with negative meaning S or W.

**Latitude:** Entering a specific latitude value here will override the actual GPS measurements, if available.

Valid range is between +/-90.000000.

**Longitude:** Entering a specific longitudinal value here will override the actual GPS measurements, if available.

Valid range is between +/-180.000000.

## GeoFence Radius Control

**Lockdown Radius Multiplier:** The value of the **Lockdown Radius Multiplier** may be entered in this field.

When the GeoFence engine begins to build a fence, it will create a Calculated Minimum Radius allowed using an accuracy figure based on the acquisition 200 GPS location points obtained over an initial settling interval of about 15 - 20 minutes. This value is then multiplied by the **Lockdown Radius Multiplier** to obtain the Modified Minimum Radius.

The **Modified Minimum Radius** will not be allowed to become less than the **Minimum Accuracy**, and will be adjusted to the **Minimum Accuracy** as prevailing conditions require.

The allowable range is 1.0 – 5.0. **(Required)**

**Recommended Setting:** 2.0.

**Minimum Accuracy:** The value of the **Minimum Accuracy** may be entered in this field.

When the GeoFence engine begins to build a fence, it will calculate an allowed Minimum Radius using an accuracy figure based on an average of 200 location points acquired over an interval of 15-20 minutes. This value is then multiplied by the **Lockdown Radius Multiplier** to obtain the Modified Minimum Radius.

The Modified Minimum Radius will not be allowed to be less than the **Minimum Accuracy**, and will be increased to the **Minimum Accuracy** as needed.

The **Minimum Accuracy** will also provide a lower limit for the **Fixed Lockdown Radius**.

The allowable range is 0 - 2000. **(Required)**

**Recommended Setting:** 50 – 200.

**Fixed Lockdown Radius:** The value of the Fixed Lockdown Radius may be entered in this field.

GeoFence behavior can be described in the following ways:

### **Flexible radius**

### **Flexible radius with additional fixed buffer**

### **Fixed radius**

During the establishment of a GeoFence, a set of 200 location points are obtained over a period of 15-20 minutes to determine an initial 'minimum radius' possible for the device. The Flexible radius behavior uses the Calculated Minimum Radius and the configured **Lockdown Radius Multiplier** values to set the GeoFence boundary. Setting the **Fixed Lockdown Radius** to a positive offset (+20, for example) has the effect of adding a fixed amount of buffer space to the Calculated Minimum Radius, and the **Lockdown Radius Multiplier** has no effect.

For **Fixed Radius** behavior, the configured value for the **Fixed Lockdown Radius** is used to set an absolute minimum radius for the GeoFence, subject to increase by the configured **Minimum Accuracy** or Calculated Minimum Radius values as needed.

To select **Flexible Radius**, the **Fixed Lockdown Radius** must be set to 0.

To select **Flexible radius with additional fixed buffer**, enter a value, preceded with '+'.

To select **Fixed radius** behavior, enter any non-zero value.



Note that since the calculated minimum radius may change over time depending on acquired GPS location data, this value will never be allowed to become less than the **Minimum Accuracy** nor the Calculated Minimum Accuracy.

This allowable range is 20 – 2000. **(Required)**

**Recommended Setting:** 0 = Off.

### GeoFence Violation Control

**Number of Violation to ignore:** The value of the **Number of Ignored Violations** may be entered in this field.

To limit false alarms from occasional drifting GPS points, this value will ignore a certain number of anomalous points before alerting a SixView Manager server. This prevents an inaccurate site from constantly updating the SixView Manager with dubious information. New points are received about every 2 seconds.

The allowable range is 0 – 300. **(Required)**

**Recommended Setting:** 10 – 30 points (approximately 20 – 60 seconds).

**Violation Grace Period:** The value of the **Grace Period** may be entered in this field.

Once we have ignored the first few anomalous location fixes, points outside the GeoFence are considered a **Violation**. This timer specifies (in seconds) how long to tolerate points outside the GeoFence boundary, before declaring a full "Violation Outside" and enacting the "Violation Action".

The allowable range is 30 – 600. **(Required)**

**Recommended Setting:** 60.

**Maximum Loss-of-data time:** The maximum number of seconds for which no GPS data is received may be entered in this field.

Ordinarily, a GPS device generates location information updates on a continuous regular periodic basis. A loss of these updates may be due to a temporary or intermittent reception issue, or due to the device having been moved to an area devoid of GPS reception or disconnection of an external GPS receiver, either deliberately or accidentally by persons authorized to do so or not.

This parameter sets the period of GPS data loss beyond which the device may be considered having been tampered with and subject to securing actions. **(Required)**

The allowable range is 30 – 1200.

**Recommended Setting:** 120.

**Select Violation Action:** Select the action to be taken when a protected perimeter violation occurs using the drop-down list provided. The available options are:

**Report Only:** The device reports violation events to a SixView Manager server.

**Block Network:** All network traffic, except to a SixView Manager server, will be blocked.

**Block All:** In addition to the actions taken in **Block Network**, all access to the device including via physical ports (console, etc.) is blocked.

**Custom:** Configured special actions are applied.

**Notify SVM Server:** Control whether GeoFence status changes are reported to the SVM Servers configured in Services→SixView Manager.

### Advanced Options

**Show Advanced Configuration:** Select **Yes** to configure advanced GPS parameters.

**Valid Points Required:** The maximum number of valid GPS location entries required for GeoFence boundary establishment may be entered in this field.

This configures the number of GPS Data points to collect before building the GeoFence boundary. These points are collected when instructed to go into initial Lockdown mode. Larger values require more time to build the initial fence, yet may yield a more accurate Calculated Minimum Radius.

The allowable range is 100 - 1000. (Required)

**Recommended Setting:** 200.

**Distance Reporting Threshold:** The value for the **Distance Reporting Threshold** may be entered in this field.

When not in GeoFence Lockdown, a Distance Threshold exceeded message will be sent to a SixView Manager server every time the unit is moved more than the configured amount (in feet) from its previously recorded location. This is typically only useful in a mobile application.

The allowable range is 200 - 1000000 (feet). **(Required)**

**Required User Cleared Violations:** Select whether the user is required to clear perimeter violations using the drop-down list provided. Available values are:

- No
- Yes

Whenever a full violation state has been reached (Violation Outside or Violation No Data), the next good GPS data point received will automatically clear the violation and return the unit to "Lockdown Good". When this option is set to Yes, then the Violation will NOT be cleared until a SixView Manager server or user sends down a command to re-initiate Lockdown. This will build a new GeoFence boundary based on current location and radius parameters.

**Recommended Setting:** No.

**Maximum log entries:** The value for Maximum log size may be entered in this field.

Number of log entries to keep in a GPS raw log in NMEA format. Raw GPS Log access is available upon request. A new log entry will be generated according to the setting in Raw Log Interval. A maximum of 50k is saved.

The allowable range is 100 - 1000. (Required)

**Recommended Setting:** 600.

**Discardable # outlier points:** The value of the **# Outlier Points to ignore** may be entered in this field.

When a GeoFence is being established, the GPS engine ignores a certain number of the first few anomalous location fixes before points outside the GeoFence are subject to **Violation** actions. After that initial 'settling period', each new GPS point must be examined in relation to the established boundary. Even under ideal conditions, intermittent signal reception and/or multipath interference issues can result in points being erroneously reported beyond the GeoFence boundary. This parameter can be used to tune the filtering of this 'jitter' to reduce the likelihood of a false positive GeoFence violation.

The allowable range is 0 - 50. **(Required)**

**Recommended Setting:** 5.

**Log Update Interval (seconds):** This parameter determines how often (in seconds) the current GPS data point will be saved in NMEA format in a Raw GPS logfile.

The allowable range is 5 - 10000.

**Recommended Setting:** 10.

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.

## SSH/TELNET Server

The SSH/TELNET Server menu allows you to configure whether the DA50N will communicate with the network via Secure Shell (SSH) and whether to enable or disable TELNET.

Click on the *SSH/TELNET* menu item and the following dialog window appears:

The screenshot shows the configuration page for the SSH/TELNET Server. The page has a navigation bar at the top with the RedLion logo and menu items: Status, Admin, Network, Services, Automation, Advanced, Events, and Logout. The main content area is titled 'SSH/TELNET Server' and is divided into two sections: 'SSH Server' and 'Telnet Server'. The 'SSH Server' section contains the following fields: 'Enable SSH Server' (Yes), 'Show Advanced Configuration' (Yes), 'Listening IP Address' (0.0.0.0), 'Listening IP Port' (22), 'Login Grace Time (seconds)' (90), 'Maximum Concurrent Connections' (10), and 'Allow Root Login' (No). The 'Telnet Server' section contains the field 'Enable Telnet Server' (Yes). Each field has a dropdown menu and a help icon. The 'Required' label is present next to the IP Address, IP Port, Login Grace Time, and Maximum Concurrent Connections fields.

### SSH Server

**Enable SSH Server:** Select **Yes** to enable the SSH server. **(Required)**

**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.

**Recommended Setting:** User Preference.

**Show Advanced Configuration:** Select **Yes** to configure advanced options for the SSH Server. **(Required)**

**Recommended Setting:** No.

**Listening IP Address:** Specifies the local IP Address on which the SSH server will accept connections. **(Required)**

**Note:** Specifying a value of **0.0.0.0** allows the SSH server to accept connections on **any** interface. Firewall rules must be present, however to allow SSH connection on untrusted interfaces.

**Recommended Setting:** 0.0.0.0.

**Listening IP Port:** Specifies the local IP port on which the SSH server will accept connections. **(Required)**

**Note:** Specifying a value other than **22** will require proper firewall rules in order to allow connections to the given port.

**Recommended Setting:** 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. **(Required)**

**Recommended Setting:** 30.

**Maximum Concurrent Connections:** Specifies the maximum number of concurrent unauthenticated connections to the SSH server. Additional connections will be dropped until authentication succeeds, or the Login Grace Time expires for a connection. **(Required)**

**Recommended Setting:** 10.

**Allow Root Login:** Specifies whether root can log in directly to the SSH server. **(Required)**

**Recommended Setting:** No.

### Telnet Server

**Enable Telnet Server:** Select Yes to enable the Telnet Server.

**Recommended Setting:** 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.

## SSL Connections

The SSL Connections menu item is used to configure the DA50N to either act as a Secure Socket Layer (SSL) Client to receive certificates or as an SSL Server to issue certificates. The SSL Connections tab is sub-sectioned into the SSL Client and the SSL Server.

### SSL Client

The SSL Client menu item is used to configure the DA50N to be a SSL client and receive a certificate of authorization from an SSL server to authenticate connections for secure communications.

Click on the *SSL Client* menu item and the following dialog window appears:

The screenshot shows the 'SSL Client' configuration page. At the top, there is a navigation bar with 'Events' highlighted in red and a 'Logout' button. Below the navigation bar, the page title is 'SSL Client'. The main content area shows the status 'SSL Client Stopped'. There are five configuration fields, each with a dropdown menu and an information icon:

- Enable SSL: Yes
- Select Activity Log Level: Summary
- Wait for Connection (seconds): 20
- Idle Timeout (minutes): 20
- Show Advanced Configuration: No

Below the configuration fields is a table titled 'SSL Client Table Properties'. The table has six columns: Label, TCP Listening IP, TCP Listening Port, SSL Destination IP/Name, SSL Destination Port, and StartTLS. The table is currently empty. To the right of the table are several action buttons: Add, Edit, Delete, Copy, Up, and Down.

**Enable SSL:** Select Yes to configure SSL client/server. Select No and then the Apply button to disable SSL.

**Select Activity Log Level:** This controls the logging level for SSL Connection activity.

**Recommended Setting:** For a production environment: Summary. For a test environment: Full.

**Wait for Connection (seconds):** Time (in seconds) allowed after sending SYN packets, to wait for SYN-ACK.

**Recommended Setting:** 20 (seconds).

**Idle Timeout (minutes):** Time (in minutes) allowed for no traffic over an SSL connection, before closing down the link.

**Recommended Setting:** 720 (minutes).

**Show Advanced Configuration:** Select Yes to modify advanced SSL options.

**Bind Interface for accepting TCP Connections:** This will restrict the unencrypted listening socket to allow connections coming into the specified interface only.

**Recommended Setting:** 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.

**Recommended Setting:** Any.

**Ciphers:** This field is a list of openssl ciphers supported. Please consult support staff before attempting to change. Reference Google **openssl ciphers list** for more information.

**High Security Default:** ALL:!ADH:!aNULL:!eNULL:!LOW:!EXP:!SSLv2:!SSLv3:+HIGH:+MEDIUM

**More Compatible Option:** ALL:!ADH:!aNULL:!eNULL:!LOW:!EXP:-SSLv2:+HIGH:+MEDIUM:-DES:-3DES:-RC4:-SEED

**Select Certificate:** Specifying a certificate in client mode uses this certificate chain as a client side certificate chain. Using client side certs is optional. The certificates must be in PEM format, with an unencrypted key (not password protected when generated). Use **Admin**→**Certificate Manager** to install/update certs.

**Note:** When adding a connection to the table, spaces and special characters are not allowed for **Label** entry.

**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 subscribed plan.

### SSL Client Table Properties

**SSL Client Table Properties**

Label	TCP Listening IP	TCP Listening Port	SSL Destination IP/Name	SSL Destination Port	StartTLS

+ Add

Edit

Delete

Copy

Up

Down

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

**SSL Client Settings** ×

Label  Required

TCP Listening IP

TCP Listening Port  Required

SSL Destination IP/Name  Required

SSL Destination Port  Required

Enable StartTLS No ▼ ⓘ

Finish

**Label:** 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.

**Recommended Setting:** 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:** 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.

**Recommended Setting:** 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 state of "LISTEN" are in use.)

**SSL Destination IP/Name:** Enter the IP or Domain Name of the SSL server to which you would like to connect.

**SSL Destination Port:** Enter the Port number of the SSL server to which you would like to connect.

**Enable StartTLS:** STARTTLS is an extension to plain text communication protocols, like SNMP, 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.

STARTTLS is primarily intended as a countermeasure to passive monitoring.

Click on the *Finish* button. You will be returned to the DHCP Relay dialog window and the Remote Servers table will be populated with the entered data.

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

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert*, will reset all fields to previously saved defaults.

### SSL Server

The SSL Server menu item is used to configure the DA50N to issue SSL certificates to requesting SSL clients.

Click on the *SSL Server* menu item and the following dialog window appears:

SSL Server Stopped

Enable SSL: Yes

Select Activity Log Level: Summary

Wait for Connection (seconds): 20

Idle Timeout (minutes): 720

Select Certificate: -No Certificate Selected- Required

Show Advanced Configuration: Yes

Bind Interface for accepting SSL Connections: Any

Bind Interface for outgoing TCP Connections: Any

Ciphers: ALL:!ADH:!aNULL:!eNULL:!LOW

Select Keep-Alive behavior: None

Label	SSL Listening IP	SSL Listening Port	TCP Destination IP	TCP Destination Port	TCP Source Bind IP

Buttons: Add, Edit, Delete, Copy, Up, Down

**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.

**Recommended Setting:** For a production environment: Summary. For a test environment: Full.

**Wait for Connection (seconds):** Time (in seconds) allowed after sending SYN packets, to wait for SYN-ACK.

**Recommended Setting:** 20 (seconds).

**Idle Timeout (minutes):** Time (in minutes) allowed for no traffic over an SSL connection, before closing down the link.

**Recommended Setting:** 720 (minutes).

**Select Certificate:** A server certificate must be provided. This will be used to encrypt communication with all clients. The certificates must be in PEM format, with an unencrypted key (not password protected when generated). Self signed certificates are highly recommended. Use **Admin→Certificate Manager** to install/update certs.

**Note:** When adding a connection to the table, spaces and special characters are not allowed for **Label** entry.

**Show Advanced Configuration:** 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.

**Recommended Setting:** Any.

**Bind Interface for outgoing TCP Connections:** This will restrict the unencrypted socket to initiate connections out the specified interface only. Specifying an interface here may conflict with policy routing, however it may be required in a GRE/VPN or other tunneled environment. Please consult with a network architect for additional assistance.

**Recommended Setting:** Any.

**Ciphers:** This field is a list of openssl ciphers supported. Please consult support staff before attempting to change. Reference Google **openssl ciphers list** for more information.

**High Security Default:** ALL:!ADH:!aNULL:!eNULL:!LOW:!EXP:!SSLv2:!SSLv3:+HIGH:+MEDIUM

**More Compatible Option:** ALL:!ADH:!aNULL:!eNULL:!LOW:!EXP:-SSLv2:+HIGH:+MEDIUM:-DES:-3DES:-RC4:-SEED

**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 subscribed plan.



### SSL Server Table Properties

Label	SSL Listening IP	SSL Listening Port	TCP Destination IP	TCP Destination Port	TCP Source Bind IP

+ Add

↻ Edit

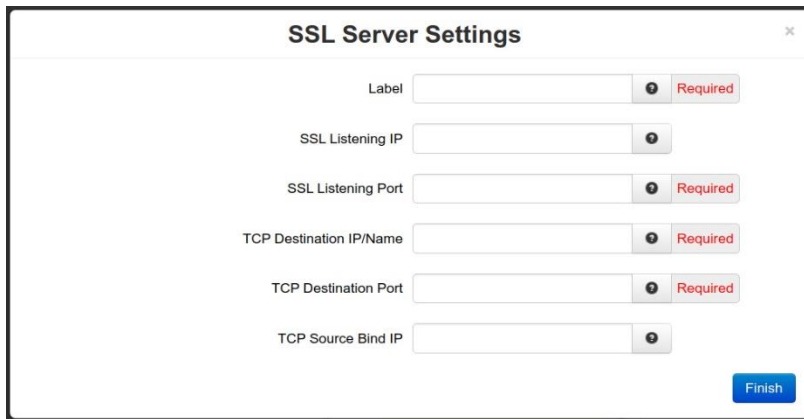
✖ Delete

↺ Copy

↶ Up

↷ Down

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



The dialog window titled "SSL Server Settings" contains the following fields:

- Label: Text input field with a required indicator (red "Required" text).
- SSL Listening IP: Text input field.
- SSL Listening Port: Text input field with a required indicator (red "Required" text).
- TCP Destination IP/Name: Text input field with a required indicator (red "Required" text).
- TCP Destination Port: Text input field with a required indicator (red "Required" text).
- TCP Source Bind IP: Text input field.

A "Finish" button is located at the bottom right of the dialog.

**Label:** 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.

**Recommended Setting:** Leave blank (0.0.0.0) to allow connections from any interface.

**SSL Listening Port:** 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.

**Recommended Setting:** 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 state of "LISTEN" are in use.)

**TCP Destination IP/Name:** 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:** 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 to for outgoing TCP connections. If not using static IP addresses, it is recommended to use the Advanced option "Bind Interface for outgoing TCP Connections".

**Recommended Setting:** Leave blank for normal operation (no binding).

Click on the *Finish* button. You will be returned to the DHCP Relay dialog window and the Remote Servers table will be populated with the entered data.

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

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert*, will reset all fields to previously saved defaults.

## SNMP Agent

SNMP (Simple Network Management Protocol) is an industry standard way of querying networking devices to obtain statuses, updates, alerts and behaviors.

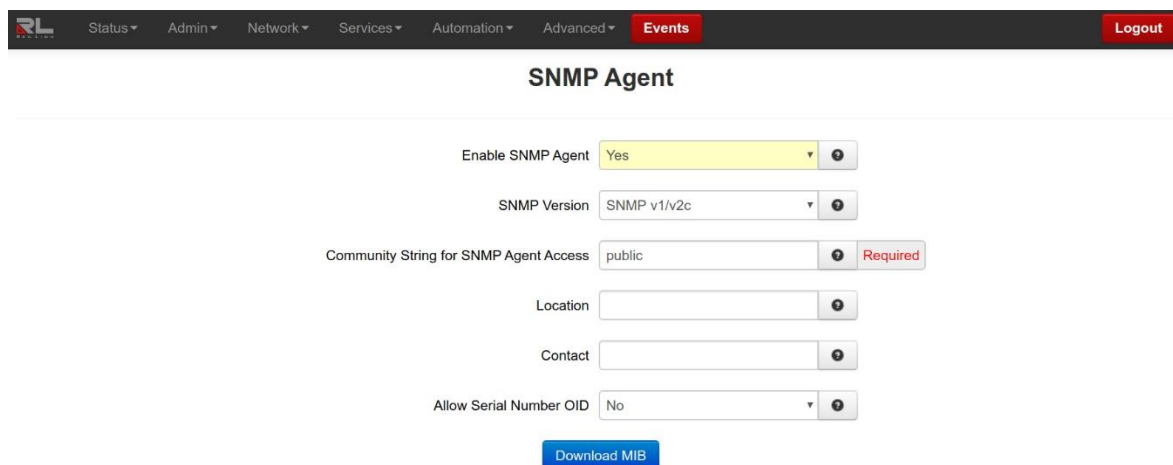
To retrieve SNMP data from the DA50N you must have an SNMP manager or Server at the head end. The DA50N will only act as an SNMP client, providing data it is polled for. It will not act as a manager to poll other devices.

The SNMP Agent allows you to query the unit for information via SNMP using what is called a MIB (Management Information Base). Standard MIB-II queries are supported, as well as a custom RED-LION-RAM.MIB. A great deal of useful information about the unit interface, including cellular signal strength, interface status, and more can be queried. When configuring firewalls to allow SNMP traffic, be sure to allow access to port 161 so that the device may return its results. This is the industry standard port number for SNMP traffic.

A complete listing of the OIDs found in the RED-LION-RAM.MIB can be found in the Appendix at the end of this guide.

\* The community string is “public” (do not enter the quotes).

Click on the SNMP Agent menu item and the SNMP Agent dialog window appears:



The screenshot shows the 'SNMP Agent' configuration page. At the top, there is a navigation bar with menu items: Status, Admin, Network, Services, Automation, Advanced, Events (highlighted), and Logout. Below the navigation bar, the title 'SNMP Agent' is centered. The configuration form includes several fields: 'Enable SNMP Agent' is a dropdown menu set to 'Yes'; 'SNMP Version' is a dropdown menu set to 'SNMP v1/v2c'; 'Community String for SNMP Agent Access' is a text input field containing 'public', with a 'Required' label to its right; 'Location' is an empty text input field; 'Contact' is an empty text input field; and 'Allow Serial Number OID' is a dropdown menu set to 'No'. At the bottom of the form, there is a blue button labeled 'Download MIB'.

**Enable SNMP Agent:** Select **Yes** to enable the SNMP Agent. **(Required)**

**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.

**Recommended Setting:** User Preference.

**SNMP Version:** Select the desire SNMP version for the device SNMP agent.

**SNMP v1/v2c:** Provides a community string sent in plaintext with no authentication or privacy.

**SNMP v3:** Provides both authentication and privacy, which can be used separately or together.

**Community String for SNMP Agent Access:** Specify the community string to use for authentication between the SNMP Agent and Manager. Alpha-numeric strings are supported. **(Required)**

**Note:** The community string must match on both ends of the connection in order to work.

**Location:** Enter the physical location of this node. This particular object is useful for determining where a device is located. This kind of practical information is essential in a large network, particularly if it is spread over a wide area.

Maximum size for location input field is 250 ASCII characters.

**Contact:** Enter the textual identification of the contact person for this managed node. It identifies the primary contact for the device in question. It is important to set this object with an appropriate value, as it can help your operations staff determine who needs to be contacted in the event of an issue.

Maximum size for contact input field is 250 ASCII 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**. (Required)

**Recommended Setting:** User Preference.

**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.

## Ping Alive

Ping is a diagnostic tool used for verifying connectivity between two hosts on a network. It sends ICMP (Internet Control Message Protocol) echo request packets to a remote IP address and watches for ICMP responses.

Select the *Ping Alive* tab menu and the following dialog window appears:

The screenshot shows the 'Ping Alive' configuration page. At the top, there is a navigation bar with tabs: Status, Admin, Network, Services, Automation, Advanced, Events (selected), and Logout. The main content area is titled 'Ping Alive' and contains the following settings:

- Enable Ping Alive: Yes
- Test Interval (in minutes): 50 (Required)
- Host Address: (Required)
- Host Address #2:
- Failure Command Script: None
- Ping Only When Interface is Idle: None
- Show Advanced Options: Yes
- Source Interface: None
- Source IP Address:
- Packets to Send per Cluster: 5 (Required)
- Allowable Packet Loss per Cluster: 3 (Required)
- Ping Clusters To Attempt: 2
- Time Between Cluster Attempts (s): 30 (Required)

**Enable Ping Alive:** Select **Yes** to enable the Ping Alive Service.

Ping Alive will send the specified number of packets in **Test Packets to Send** option, every interval defined in **Test Interval** option. 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.

**Recommended Setting:** No.

**Test Interval (minutes):** Enter the time interval (in minutes) to wait between ping tests.

**Recommended Setting:** 50.

**Host Address:** Enter the IP Address of the destination host to which the ping packet would be sent.

**Default Setting:** 127.0.0.1.

**Host Address #2:** Enter the IP Address of the second destination host to which the ping packet would be sent.

This second host is tested only when the first fails.

**Default Setting:** None.

**Failure Command Script:** Choose the name of the command script to be executed when the PING test fails.

For example, if RestartWireless is an option, then when selected, the wireless interface will be restarted.

**Recommended Setting:**

None for standard operation with no special behaviors.

Reboot will start the entire unit.

Restart Wireless is useful when using a wireless (cellular) interface.

Restart IPsec will restart all IPsec tunnels.

**Ping Only When Interface is Idle:** Select the name of the interface which the ping alive service will monitor for activity. This service will send a ping **ONLY** when the connection for the selected interface is idle or reset.

**Note:** If **None** is selected, this functionality is disabled.

**Recommended Setting:** None.

**Show Advanced Options:** Displays the following fields when selected.

**Source Interface:** Select the name of the interface to which the service will bind for communication tests. Packets will be forced to leave this interface. This may not alter the IP used as the source IP in the packets themselves. When set to **None**, the system will choose automatically.

**Recommended Setting:** None.

**Source IP Address:** Enter the IP address to use as a source for communication tests.

**Note:** This will be the source IP address of the PING packets, but does not necessarily reflect the interface from which packets will traverse the unit.

**Recommended Setting:** Leave Blank.

**Packets to Send per Cluster:** Specify the number of ping packets to send out to test connectivity. The minimum is 1, maximum is 10.

**Recommended Setting:** 5 - 10.

**Allowable Packet Loss per Cluster:** Specify the number of lost packets that are acceptable before the link is considered unavailable.

**Note:** The value must be less than the number of test packets set via **Test Packets to Send**.

Example: If **Test Packets to Send** is set to 5, and **Allowable Packet Loss** is set to 3, then 2 pings of the 5 sent out must have replies for connectivity to be declared successful. If only 1 ping reply is received, then a failure to that host will be declared.

**Ping Cluster to Attempt:** Enter the number of cluster ping attempts to retry before determining a failure. If one set of pings succeeds to pass, the next test will be performed on the next interval. If all attempts fail, then the configured action(s) are performed. The valid cluster ping attempts range is 1 - 5.

**Time Between Cluster Attempts:** Enter the number of seconds to wait between Cluster Ping Attempts. The valid grace period wait range is 15 - 300.

Click on the *Apply* button for the changes to take effect. Selecting *Revert / Refresh*, will reset all fields to previously saved defaults.

## Crimson Connect

Crimson Connect provides a consolidated way to streamline multiple configuration options when coordinating with a Red Lion DSP or HMI product. Using this interface provides HTTPS encapsulation, SMS support, Email encryption and Crimson Link access for remote reconfiguration.

Settings for this feature work in conjunction with settings from the Crimson® software. Please consult your Crimson Software Guide for setup information as indicated in sections below.

The screenshot shows the Crimson Connect web interface. At the top is a navigation bar with menu items: Status, Admin, Network, Services, Automation, Advanced, Events, and Logout. The main heading is "Crimson Connect". Below the heading is a descriptive paragraph: "Crimson Connect provides a consolidated way to streamline multiple configuration options when coordinating with a Red Lion DSP or HMI product. Using this interface, we can provide HTTPS encapsulation, SMS support, Email encryption and Crimson Link access for remote reconfiguration." The interface is divided into several sections: 1. Local Network Device: Includes a text input for "Crimson Device IP Address" (with a "Required" label) and a dropdown for "Select Local Interface" (currently set to "eth0"). 2. Crimson Services Setup: Contains two buttons: "Walkthrough" and "Quick Config". 3. Remote Link Setup: Contains two buttons: "Walkthrough" and "Quick Config". 4. Services Status: A table showing the status of various services: "Crimson SMS API" (Pending Apply), "SMTP Email Gateway" (Not configured), "SSL SMTP Destination" (Not configured), "HTTP/HTTPS" (Not configured), and "Login" (No Login). 5. Remote Link Status: Shows "Cellular IP:" followed by a redacted IP address. Below this is a note: "Once the Remote Link is running, enter this unit's cellular IP in the Remote Address field of the Download Tab." with a link to "Crimson Link Example". At the bottom right, there is a "Not Running:" label and a green "Start" button.

Local Network Device

**Crimson Device IP Address:** Enter the IP address of your local Crimson device. Use **Status→Diagnostics→Ping** to test connectivity to your device.

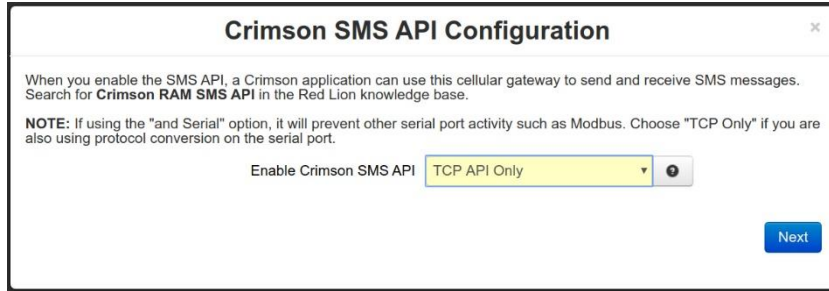
**Select Local Interface:** Select local interface used to connect to Crimson device.

## Crimson Services Setup

### Walkthrough

This option provides step-by-step instructions for Crimson Services setup.

Click on the Walkthrough button to begin the Crimson Services setup. The Crimson SMS API Configuration window will pop-up.



The screenshot shows a window titled "Crimson SMS API Configuration". It contains the following text: "When you enable the SMS API, a Crimson application can use this cellular gateway to send and receive SMS messages. Search for **Crimson RAM SMS API** in the Red Lion knowledge base." Below this is a note: "NOTE: If using the 'and Serial' option, it will prevent other serial port activity such as Modbus. Choose 'TCP Only' if you are also using protocol conversion on the serial port." There is a label "Enable Crimson SMS API" followed by a dropdown menu set to "TCP API Only" and a "Next" button.

**Enable Crimson SMS API:** Enable the Crimson SMS API interface on port 1000. See Crimson HOWTO guide for more information and instructions on how to configure your Crimson application to connect to these SMS services.

### SMS API Interface Options

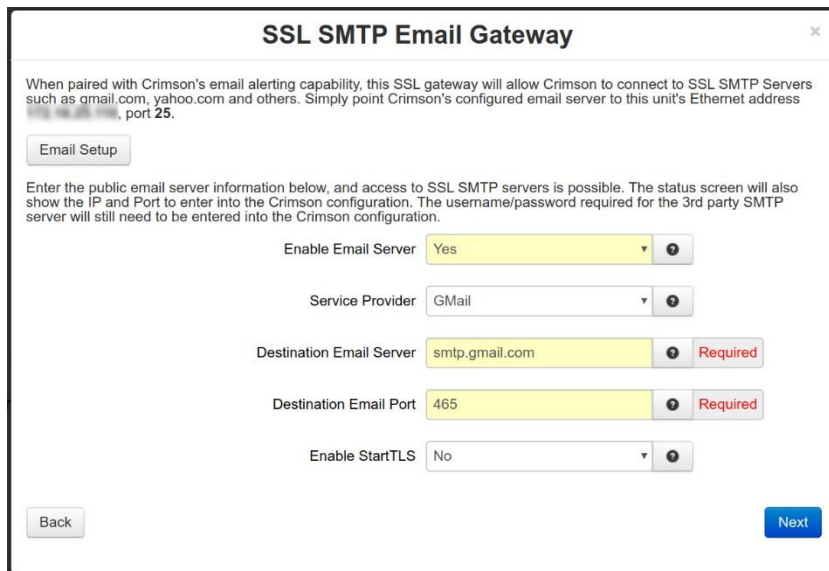
**No:** SMS API Disabled.

**TCP API Only:** Allows you to send SMS messages via TCP.

**Note:** If using the "and Serial" option, it will prevent other serial port activity such as Modbus.

Choose "TCP Only" if you are also using protocol conversion on the serial port.

Click on the Next button.



The screenshot shows a window titled "SSL SMTP Email Gateway". It contains the following text: "When paired with Crimson's email alerting capability, this SSL gateway will allow Crimson to connect to SSL SMTP Servers such as gmail.com, yahoo.com and others. Simply point Crimson's configured email server to this unit's Ethernet address 192.168.208.136, port 25." There is an "Email Setup" button. Below this is a note: "Enter the public email server information below, and access to SSL SMTP servers is possible. The status screen will also show the IP and Port to enter into the Crimson configuration. The username/password required for the 3rd party SMTP server will still need to be entered into the Crimson configuration." There are five configuration fields: "Enable Email Server" (Yes), "Service Provider" (GMail), "Destination Email Server" (smtp.gmail.com, Required), "Destination Email Port" (465, Required), and "Enable StartTLS" (No). There are "Back" and "Next" buttons.

**Email Setup:** When paired with Crimson's email alerting capability, this SSL gateway allows Crimson to connect to SSL SMTP Servers such as gmail.com, yahoo.com and others. Simply point Crimson's configured email server to this unit's Ethernet address **192.168.208.136** and Server Port **25**. Please view the Crimson Software Guide for instructions on how to setup Mail Manager.

Next, enter the public email server information below, and access to SSL SMTP servers is possible. The status screen will also show the IP and Port to enter into the Crimson configuration. The username/password required for the 3rd party SMTP server will still need to be entered into the Crimson configuration.

**Enable Email Server:** Select **Yes** to enable and configure the Email Server settings.

**Service Provider:** Select the Domain Name of the remote SSL email server.

**Destination Email Server:** Enter the IP or Domain Name of the remote SSL email server.

Example: smtp.gmail.com

**Destination Email Port:** Enter the Port number of the remote SSL email server. Common Secure SMTP ports are 25, 465, and 587.

Example: smtp.gmail.com requires port 465.

**Note:** Port 587 commonly requires StartTLS to be enabled.

**Enable StartTLS:** **STARTTLS** is an extension to plain text communication protocols, like SNMP, 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.

STARTTLS is primarily intended as a countermeasure to passive monitoring.

Click on the *Next* button.

**SN Proxy Settings**

When the proxy is enabled, these settings can offer improved performance of cellular access to the web interface of a Crimson product. Screen updates over cellular can be more efficient and additional security can be achieved with an HTTPS (Secure SSL) connection and an extra user login step.

Enable SN Proxy: Yes

Use HTTPS: No

Use Login: No

User Name: [Empty]

Password: [Empty]

Cellular carriers often block port 80, so we recommend an alternate access port for browsers connecting to the cellular IP address. The status screen will show the full browser link to use.

External Web Server Listening Port: [Empty] Required

Allow alternate Crimson Web Server Port

Internal Crimson Web Server Port: 20000

Back Finish

When the proxy is enabled, these proxy settings can offer improved performance of cellular access to the web interface of a Crimson product. Screen updates over cellular can be more efficient and additional security can be achieved with an HTTPS (Secure SSL) connection and an extra user login step.

**Enable SN Proxy:** Select **Yes** to enable and configure the SN Proxy settings.

**Use HTTPS:** Specify whether access to the Crimson Web server will be encapsulated in HTTPS encryption.

**Use Login:** Specify whether you want to enable additional user login requirements. This HTTP login will occur prior to accessing the Crimson Web interface, which may require additional login steps.

**Note:** If you enable this login, you are also required to enter the username and password. This is separate and distinct from access to this DA50N's GUI interface.

**User Name:** Enter username required to connect to proxy server.

**Password:** Enter password required to connect through this proxy server.

Cellular carriers often block port 80, so we recommend an alternate access port for browsers connecting to the cellular IP address. The status screen will show the full browser link to use.

**External Web Server Listening Port:** Enter the port number that will be available for external access to your Crimson device. This port will be open on all untrusted interfaces (as defined in the firewall). External browsers that connect to this port and complete authentication will then be allowed to connect to the Crimson device on the local network.

Some cellular carriers block certain incoming ports (like 80). You may need to experiment with different values here.

**Recommended Setting:** 8080.

**Allow alternate Crimson Web Server Port:**

**Internal Crimson Web Server Port:** The common listening web server port on Crimson devices is port 80. If you are using a non-standard port on your Crimson device, enter it here.

Click on the *Finish* button.

### Quick Config

This option has the same fields as the Walkthrough setup, but can be configured in one dialog window.

**Crimson Services Quick Config**

**Crimson SMS API Configuration**

Enable Crimson SMS API: TCP API Only

**SMTP Email Gateway**

Enable Email Server: Yes

Service Provider: GMail

Destination Email Server: [Empty] Required

Destination Email Port: [Empty] Required

Enable StartTLS: No

**SN Proxy Settings**

Enable SN Proxy: Yes

Use HTTPS: No

Use Login: No

User Name: [Empty]

Password: [Empty]

External Web Server Listening Port: [Empty] Required



**Enable Crimson SMS API:** Enable the Crimson SMS API interface on port 1000. See Crimson HOWTO guide for more information and instructions on how to configure your Crimson application to connect to these SMS services.

**SMS API Interface Options**

**No:** SMS API Disabled.

**TCP API Only:** Allows you to send SMS messages via TCP.

**Note:** If using the "and Serial" option, it will prevent other serial port activity such as Modbus. Choose "TCP Only" if you are also using protocol conversion on the serial port.

**Email Setup:** When paired with Crimson's email alerting capability, this SSL gateway allows Crimson to connect to SSL SMTP Servers such as gmail.com, yahoo.com and others. Simply point Crimson's configured email server to this unit's Ethernet address **192.168.208.136** and Server Port **25**. Please view the Crimson Software Guide for instructions on how to setup Mail Manager.

Next, enter the public email server information below, and access to SSL SMTP servers is possible. The status screen will also show the IP and Port to enter into the Crimson configuration. The username/password required for the 3rd party SMTP server will still need to be entered into the Crimson configuration.

**Enable Email Server:** Select **Yes** to enable and configure the Email Server settings.

**Service Provider:** Select the Domain Name of the remote SSL email server.

**Destination Email Server:** Enter the IP or Domain Name of the remote SSL email server.

Example: smtp.gmail.com

**Destination Email Port:** Enter the Port number of the remote SSL email server. Common Secure SMTP ports are 25, 465, and 587.

Example: smtp.gmail.com requires port 465.

**Note:** Port 587 commonly requires StartTLS to be enabled.

**Enable StartTLS:** **STARTTLS** is an extension to plain text communication protocols, like SNMP, 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.

STARTTLS is primarily intended as a countermeasure to passive monitoring.

When the proxy is enabled, these proxy settings can offer improved performance of cellular access to the web interface of a Crimson product. Screen updates over cellular can be more efficient and additional security can be achieved with an HTTPS (Secure SSL) connection and an extra user login step.

**Enable SN Proxy:** Select **Yes** to enable and configure the SN Proxy settings.

**Use HTTPS:** Specify whether access to the Crimson Web server will be encapsulated in HTTPS encryption.

**Use Login:** Specify whether you want to enable additional user login requirements. This HTTP login will occur prior to accessing the Crimson Web interface, which may require additional login steps.

**Note:** If you enable this login, you are also required to enter the username and password. This is separate and distinct from access to this router's GUI interface.

**User Name:** Enter username required to connect to proxy server.

**Password:** Enter password required to connect through this proxy server.

Cellular carriers often block port 80, so we recommend an alternate access port for browsers connecting to the cellular IP address. The status screen will show the full browser link to use.

**External Web Server Listening Port:** Enter the port number that will be available for external access to your Crimson device. This port will be open on all untrusted interfaces (as defined in the firewall). External browsers that connect to this port and complete authentication will then be allowed to connect to the Crimson device on the local network.

Some cellular carriers block certain incoming ports (like 80). You may need to experiment with different values here.

**Recommended Setting:** 8080.

**Allow alternate Crimson Web Server Port:**

**Internal Crimson Web Server Port:** The common listening web server port on Crimson devices is port 80. If you are using a non-standard port on your Crimson device, enter it here.

Click on the *Finish* button.

## Services Status

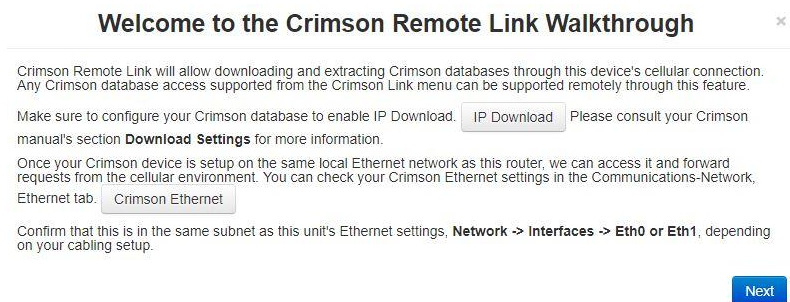
The status of the Crimson Services will show in this section of the Crimson Connect section.

## Remote Link Setup

### Walkthrough

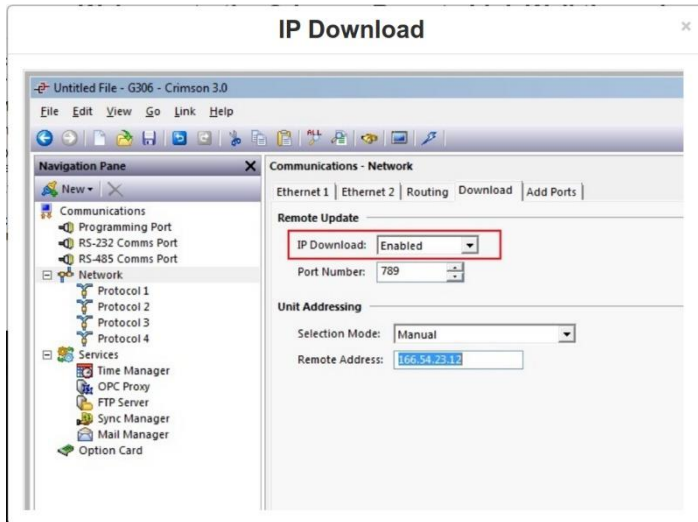
This option provides step-by-step instructions for Crimson Services setup.

Click on the Walkthrough button to begin the Crimson Remote Link setup. The Crimson Remote Link Walkthrough window will pop-up.

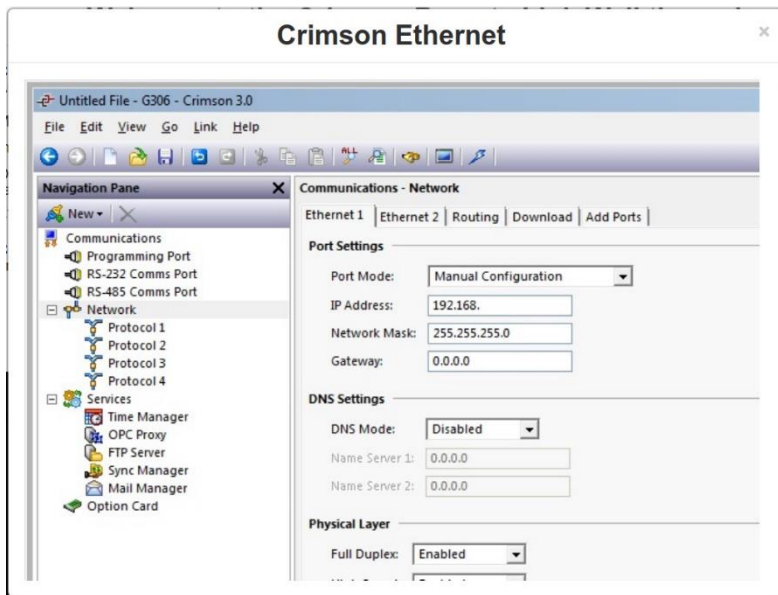


Crimson Remote Link allows downloading and extracting Crimson databases through this device's cellular connection. Any Crimson database access supported from the Crimson Link menu can be supported remotely through this feature. **Please consult your Crimson Software Guide's section "Download Settings" for more information.**

Make sure to configure your Crimson database to enable IP Download.



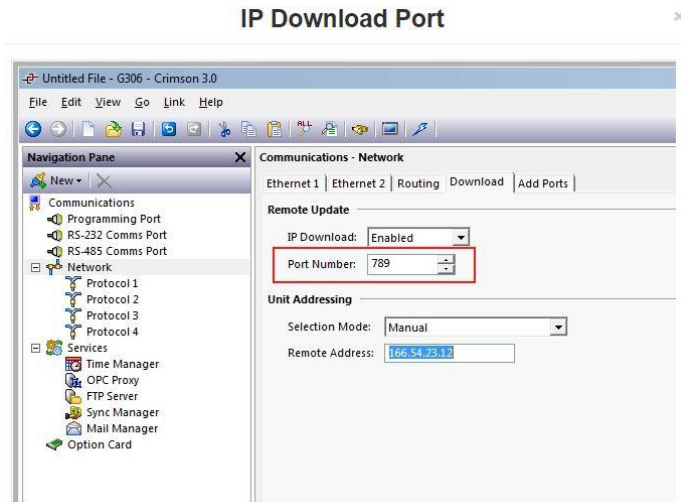
Once your Crimson device is setup on the same local Ethernet network as this router, we can access it and forward requests from the cellular environment. You can check your Crimson Ethernet settings in the Communications- Network, Ethernet tab.



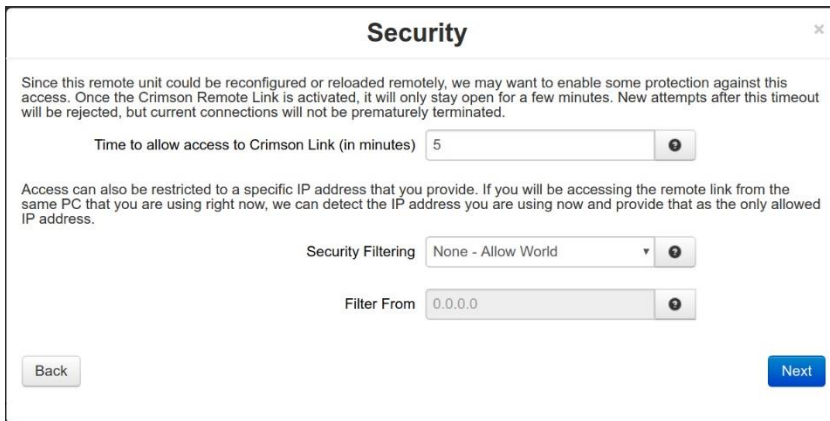
Confirm that this is in the same subnet as this unit's Ethernet settings, **Network→Interfaces→Eth0** or **Eth1**, depending on your cabling setup.  
Click on the *Next* button.



**Crimson IP Download Port:** Enter the port number configured for IP Download. This should match the option chosen when configuring the Crimson database.



Click on the Next button.



**Time to allow access to Crimson Link (in minutes):** Enter time to allow access to Crimson Link (in minutes). Once the Crimson Remote Link is Started, it will only allow the initial connection within the number of minutes specified here. New attempts after this timeout will be rejected, but current connections will not be prematurely terminated.

**Note:** Minimum time to allow access to Crimson Link is 5 minutes and the maximum is 240 minutes (4 hours).

**Security Filtering:** Connections from the IP (or IP range) listed here will be allowed to connect to the Crimson Link enabled device.

**None - Allow World:** This allows connections from any remote IP Address. Choose this if you are unsure what IP to enter, or if multiple people may access this link.

**Allow Currently Connected IP Only:** This will auto detect the IP in use from this current browser session. If you are running Crimson on the same PC that is accessing this page in a browser, try this option first.

**Allow Specific IP:** Enter a specific IP in the **Filter From** field. Only this IP will be allowed to connect to the Crimson Link. If your endpoints are connecting through a firewall, a computer's assigned IP might not be the same IP used when connecting to this remote unit.

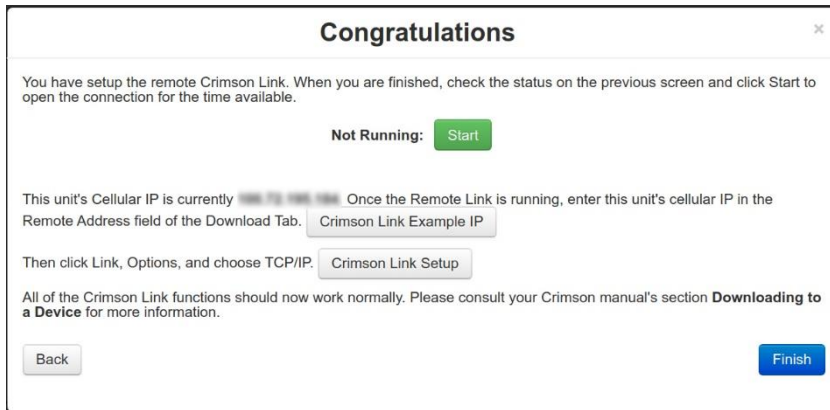
**Filter From:** Connections from the IP (or IP range) listed here will be allowed to connect to the Crimson Link enabled device.

**None - Allow World:** This will allow connections from any remote IP Address. Choose this if you are unsure what IP to enter, or if multiple people may access this link.

**Allow Currently Connected IP Only:** This will autodetect the IP in use from this current browser session. If you are running Crimson on the same PC that is accessing this page in a browser, try this option first.

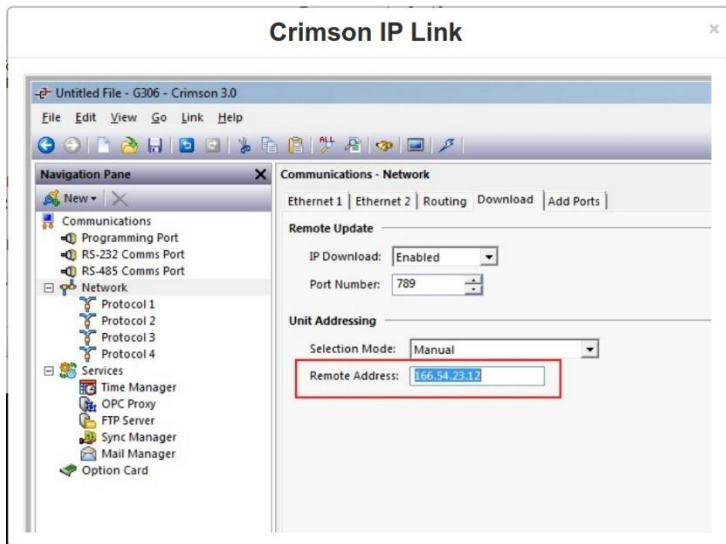
**Allow Specific IP:** Enter a specific IP in the **Filter From** field. Only this IP will be allowed to connect to the Crimson Link. If your endpoints are connecting through a firewall, a computer's assigned IP might not be the same IP used when connecting to this remote unit.

Click on the Next button.

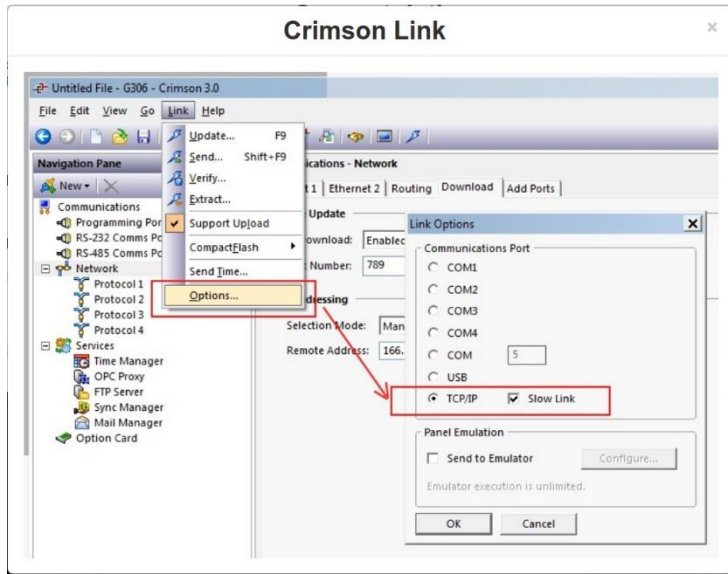


Now that the remote Crimson Link has been setup, click the status on the Crimson Connect main dialog window and click *Start* to open the connection for the time available.

Once the Remote Link is running, enter this unit's cellular IP in the Remote Address field of the Download Tab. **Please consult the Crimson Software Guide for more detailed information.**



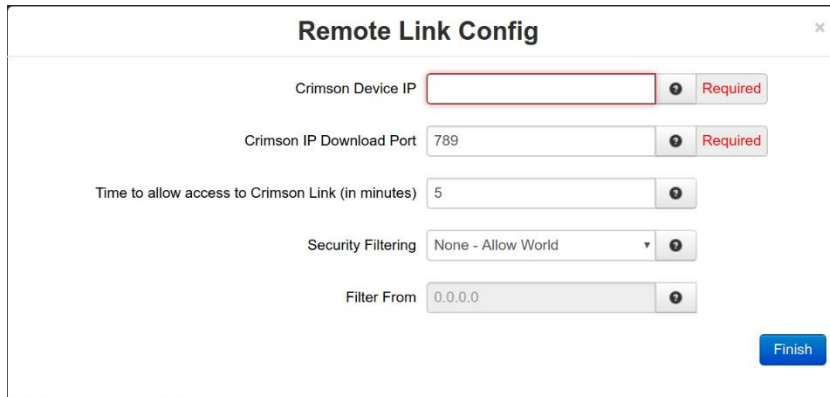
Then click Link, Options, and choose TCP/IP.



All of the Crimson Link functions should now work normally. Please consult your Crimson Software Guide's section “**Downloading to a Device**” for more information.  
Click on the *Finish* button.

### Quick Config

This option has the same fields as the Walkthrough setup, but can be configured in one dialog window.



### Remote Link Status

Once the remote link is running, enter the unit’s cellular IP in the Remote Address field of the download tab.

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately.

### 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 Yes

### Email Settings

Server Address  Required

Server Port  Required

Username  Required

Password  Required

Enable STARTTLS No

Auth Type Plain

### Email Settings Test

Recipient

Test Email

**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.

**Recommended:** Consult your email service provider or system administrator for your server settings.

## Email Settings

**Server Address:** Enter your SMTP server address.

**Note:** 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:** Enter your SMTP server port.

**Username:** Enter the **username** used to connect to your SMTP server account.

**Password (Required):** Enter the **password** used to connect to your SMTP server account.

**Enable STARTTLS:** Specify whether to enable the STARTTLS option for your email server.

**Note:** **STARTTLS** is an extension to plain text communication protocols, which offers a way to upgrade a plain text connection to an encrypted (TLS or SSL) connection instead of using a separate port for encrypted communication.

**Auth Type** Select the authentication type for email client that may log in using an authentication mechanism chosen among those supported by the email server.

**Available Options**

**Any:** Any authorization method supported.

**Plain:** Force server to use plain mode (for compatibility).

## Email Settings Test

**Recipient:** Enter an email address for the email message destination. Multiple email addresses may 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.

**Example:**

username@email.com  
username@email.com, [usergroup@email.com](#)

## Test Email

Click on this button to execute the Email Settings Test. An email will be sent to the recipient using the Email Client server settings and an Email Debug window will display the log of the email sending process for diagnostics.

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert/Refresh*, will reset all fields to previously saved defaults.

## SMS Handling

Specify whether to enable the SMS Command Handling Engine. If this option is disabled, all incoming SMS messages will be ignored unless SDK applications are processing them.

The screenshot shows the 'SMS Handling' configuration page. At the top is a navigation bar with 'Events' highlighted and a 'Logout' button. The main content area is titled 'SMS Handling' and contains several sections:

- Enable SMS processing:** A dropdown menu set to 'Yes'.
- SMS System Configuration:**
  - Limit outgoing messages:** A dropdown menu set to 'None'.
  - Access security:** A dropdown menu set to 'Allow any number'.
  - Login session inactivity timeout (minutes):** A text input field containing '60'.
  - Respond to all login attempts:** A dropdown menu set to 'Ignore non-whitelist numbers'.
- General Passwords:**
  - Admin user:** A text input field.
  - Tech user:** A text input field.
  - Basic user:** A text input field.
- SMS Whitelist Configuration:** A blue button labeled 'Add Whitelist Number'.

**Enable SMS Processing:** Select **Yes** to enable SMS handling service.

## SMS System Configuration

**Limit outgoing messages:** Select the desired Limit Period for operational permission. This is the time period for which you want to restrict the amount of messages that are sent by the device.

**Available Options:**

**None:** No time bound restrictions on sent messages.



**Hourly:** Messages will be restricted by the number of messages per HOUR.

**Daily:** Messages will be restricted by the number of messages sent per DAY.

**Access Security:** Select the Access security profile for who will be allowed access to the device.

**Available Options:**

**Allow any number:** Any number can access features for all user types. Login is still required.

**Allow any number, Admin must be on the whitelist:** Any number can access Basic/Tech functions, but only Whitelist users can access Admin functions. Login is still required.

**Allow only Whitelist numbers:** Only Whitelist users can login. All users will need to login to have the functions of their access level. Non-whitelist users' requests will be ignored.

**Login session inactivity timeout (minutes):** Set the amount of inactivity time, in minutes, the system will keep an incoming number logged in and accepting commands before timing out and requiring a new log in.

**Available Range:** 1-1440 minutes.

**Respond to all login attempts:** This option determines when the device will respond to invalid login attempts.

**Available Options:**

**Yes:** Respond to ALL invalid login attempts.

**Ignore non-whitelist numbers:** Respond only to numbers that are on the whitelist and ignore all others.

## General Passwords

**Admin user:** Set the password to be used by Admin users for unlimited Read / Write Access.

**Tech user:** Set the password to be used by Tech users for Basic level Read Only access for IODB values and Write permissions for Event alarm clearance only.

**Basic user:** Set the password to be used by the Basic users for Read Only access.

**Note:** The password for ALL users may be alphanumeric, minimum 4 to maximum 20 alphanumeric characters including the following special characters: `~!@#\$\$%^&\*()\_- =+[]{}|\ \ ; , < . > / ? .

## SMS Whitelist Configuration

To control access via a whitelist by incoming number, select the Add Whitelist Number button and complete the SMS Whitelist Settings screen to add members to the whitelist and set permission levels.

### Add Whitelist Configuration

**Incoming number:** Enter the incoming number (phone number without parenthesis) to allow this number to access the SMS command handler. Incoming number must be numeric digits with or without - (hyphen) character(s).

**Note:** All - (hyphen) characters are being stripped from the phone number. The total number of digits must be at least 4, but cannot exceed 20 digits.

**Example:** 717-555-5555, 1112223333, 222-3333 or 2223333 are all acceptable formats.

**Reply-To number:** Enter the Reply-To number (phone number without parenthesis) to allow this Reply-To number to use the SMS command handler. Reply-To number must be numeric digits with or without - (hyphen) character(s).

**Note:** All - (hyphen) characters are being stripped from the phone number. The total number of digits must be at least 4, but cannot exceed 20 digits.

**Example:** 717-555-5555, 1112223333, 222-3333 or 2223333 are all acceptable formats.

**Password:** Enter the password required for the selected incoming number to access the SMS handler system.

**Note:** The password may be alphanumeric, minimum 4 to maximum 20 alphanumeric characters including the following special characters: `~!@#\$%^&\*()\_-=+[]{}|\;\:;<.>/?.

**Permission Level:** Select the desired permission level for this incoming number.

**Available Options:**

**Admin:** Unlimited Read and Write access for all features.

**Tech:** Basic level Read Only access for IODB values and write permissions for Event alarm clearance only.

**Basic:** Read Only access to the IODB and cannot write or clear any event alarms.

**Machine-to-Machine Messaging:** Select the desired Machine-to-Machine mode for this incoming number. This option provides ability to send SMS messages to another device when the **Reply-To number** is configured for remote device account phone number.

**Available Options:**

**Disable:** Disables the Machine-to-Machine mode functionality.

**Enable without reply:** Provides processing of incoming Machine-to-Machine SMS message, but will not send a reply message.

**Enable with reply:** Provides processing of incoming Machine-to-Machine SMS message and the reply message will be sent to configured **Reply-To number** in Machine-to-Machine mode.

**Note:** Machine-to-Machine SMS messaging is always a single message only where each message contains a flag showing this is a machine-sent message, and may contain multiple commands per message. Therefore there will be no more time session security.

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert/Refresh*, will reset all fields to previously saved defaults. Select *Show Details* to view current status, send a test message or to Rotate the SMS log.

## FTP Server

The FTP Server menu item is used to .

Click on the *FTP Server* menu item and the FTP Server window appears.

**FTP Server**

Enable FTP Server Yes

**FTP System Configuration**

Enable Encryption Yes

Port Number 990

**Curl Command Example**

```
curl -k -u <username>:<password> ftps://mant50:990/
```

**FTP Device Certificate**

Select FTP Certificate vsftpd.pem

**FTP User Configuration**

Add User

**Enable FTP Server:** Select **Yes** to enable FTP Server on-device.

#### FTP System Configuration

**Enable Encryption:** Select **Yes** to enable secure SSL (Encryption) for FTP Server.

**Port Number:** Enter port number to be used for FTP Server connection.

**SSL Disabled** - The default port number is **21**.

**SSL Enabled** - The default port number is **990**.

You can also choose any port number beside defaults, if it is desired.

#### Curl Command Example

The following sections provides curl command examples for downloading or uploading the desired file from configured home-directory with or without SSL (encryption) using configured Username, Password, Home Directory and Permission Level.

Examples of Possible Curl Command Usage:

#### Download

Configure the FTP Server page with the following options:

Enable FTP Server = Yes, Enable Encryption = No, Port Number = 21

Add user with the following options:

Username = bob, Password = bobisgreat, Home Directory = datalog, Permission Level = Read

Apply the Settings.

On device, execute the following command:

```
cat 'hello world' > /datalog/ftp-test-file.txt
```

From your PC, execute the following command:

```
curl -u bob:bobisgreat ftp:///ftp-test-file.txt > /tmp/ftp-test-file.txt
```

Verify that '/tmp/ftp-test-file.txt' exists and contains the text 'hello world'.

## Upload

Configure the FTP Server page with the options similar to **Download Test** section.

Add user with the options similar to **Download Test** section except set the `Permission Level = Read/Write`.

Apply the settings.

From local host, create a text file named 'ftp-test-file.txt' containing 'hello world'.

From local host, execute the following command:

```
curl -T ftp-test-file.txt -u bob:bobisgreat ftp:///
```

On device execute the following command:

```
ls /dataalog/
```

Verify that command output contains 'ftp-test-file.txt'.

On the device execute the following command:

```
cat /dataalog/ftp-test-file.txt
```

Verify that the command output contains 'hello world'.

## SSL

Configure the FTP Server page with the following options:

Enable FTP Server = Yes, Enable Encryption = Yes, Port Number = 990.

Add user with the options similar to **Upload Test** section.

Apply the settings.

From a local host, create a text file named 'ftp-test-file.txt' containing 'hello world'.

From local host, execute the following command:

```
curl -K -T ftp-test-file.txt -u bob:bobisgreat ftps:///
```

Verify that command output contains 'ftp-test-file.txt'.

**Remove ftp-test-file.txt from device and from local PC.**

From local host, execute the following command:

```
curl -u bob:bobisgreat ftp:///
```

Verify that command freezes and does not return anything.

From local host, execute the following command.

```
curl -k -u bob:bobisgreat --ftp-ssl ftp://
```

Verify that command freezes and does not return anything.

### Permission

Configure the FTP Server page with the options similar to **SSL Test** section.

Add user with the options similar to **SSL Test** section except set the `Permission Level = Read`.

Apply the settings.

On device, execute the following command.

```
cat 'hello world' > /datalog/ftp-test-file.txt
```

From your PC, execute the following command:

```
curl -u bob:bobisgreat ftp://
```

Verify that command output contains 'ftp-test-file.txt'.

From local host, create a text file named 'ftp-test-file.txt' containing 'hello world'.

From local host, execute the following command:

```
curl -k -T ftp-test-file.txt -u bob:bobisgreat ftps://
```

Verify that command output contains 'curl: (25) Failed FTP upload: 550'.

### FTP Device Certificate

**Select FTP Certificate:** Select the certificate file name you desire to associate with the FTP Server.

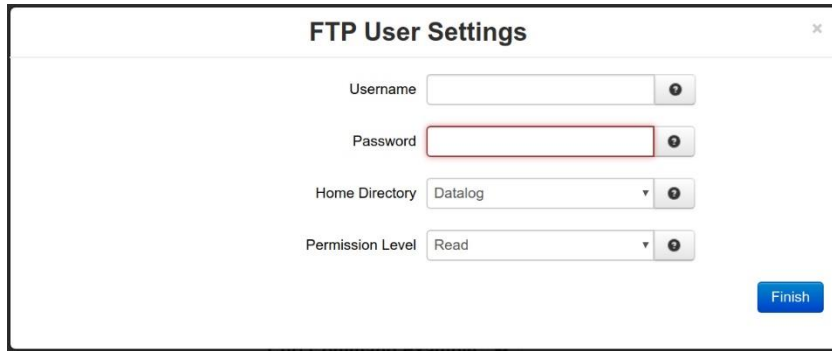
**Note:** The `vsftpd.pem` certificate is the default self signed SSL certificate generated for the device FTP Server. However you can generate and install your own self signed SSL certificate to be used for FTP Server simply by Drag and drop the server certificate into the box adjacent to the FTP Certificate field. The SSL Certificate may also be installed via **Admin**→**Certificate Manager** section of the Web UI.

**Note:** The SSL type certificates must include the key and cert portions combined in a single file with `.pem` extension, and the key must not be password encrypted.

### FTP User Configuration

#### Add User

Click the *Add User* button and the FTP User Settings window appears.



**Username:** Enter the desired username to connect to FTP Server on-device. The username must be maximum 32 alphanumeric characters plus - and \_ characters.

**Password:** Enter the desired user password to access the FTP Server on-device. The password must be alphanumeric and special characters excluding quotes.

**Home Directory:** Select the desired home directory for FTP Server on-device.

**Datalog:** Gives user FTP access to on-device datalogs.

```
datalog/
```

**SD Card:** (If available) Gives user FTP access to contents of SD Card.

```
media/sdcard/
```

**Permission Level:** Select the desired user permission level for accessing FTP Server on-device.

**Read** - Can download files from **Home Directory**.

**Read/Write** - Can upload-to and download files from **Home Directory**.

Click the *Finish* button. You will be returned to the FTP Server dialog window and the FTP User Configuration table will be populated with the entered data.

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.

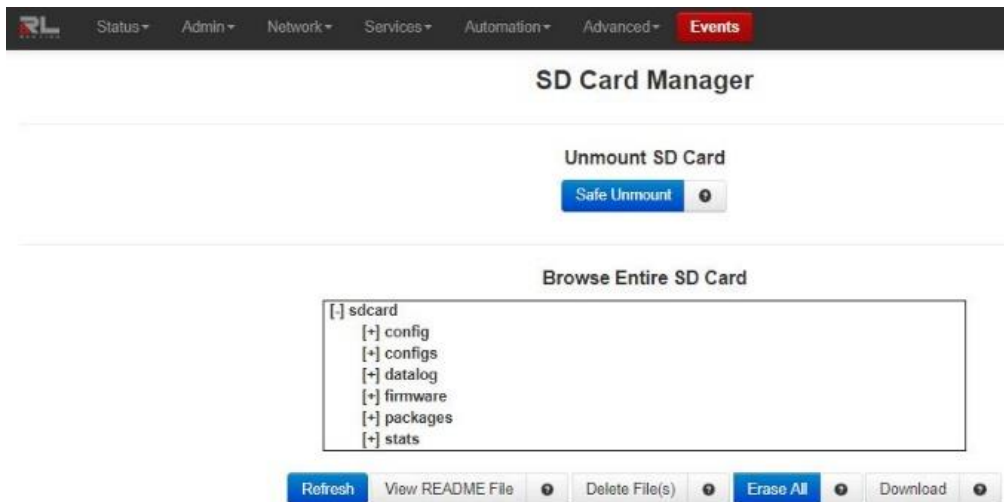
## SD Card Manager

The SD Card Manager menu item is used to safely unmount the SD Card. Options are also available to view, download, or delete files on the SD Card while it is mounted into the device.

This feature is only available on the DA50N.

The DA50N supports SD cards in the following file formats: FAT32, NTFS, and EXT3/EXT4.

Select the SD Card Manager menu item and the SD Card Manager window appears.



### Unmount SD Card

**Safe Unmount:** Clicking this button will safely unmount the SD card. It is required to **eject** the SD card and **reinsert** it or **reboot** the unit before attempting to access the SD card again.

### Browse Entire SD Card

Select any directory on the SD Card to view the files contained. Selected files appear in the Selected Files box.

#### View README File

Select the file you would like to view in the file menu above and then click View README File.

#### Delete File(s)

Remove the selected file(s) from the SD card.

**Note:** You can select multiple files to be deleted from the SD Card at once.

#### Erase All

There are two functions for this button depending on the current contents of the SD Card.

**Apply Directory Structure:** This button is visible when the SD card is inserted and there are no files found on the SD card. Click this button to create the required directories on the SD Card for use by the system. This **MUST** be done before the SD Card will be available for use by the system.

**Erase All:** This button is visible when there are files and directories on the SD card. Clicking this button will remove **ALL files and directories** from the SD card, then create the standard directory structure described below and add a README file describing the purpose of each.

**Configs** - This directory is where the user will find any export of system configuration, gather configs as well as where the user should store a config.xml that is intended to be imported from the SD Card.

**Datalog** - This is where the datalog files will be stored if SD Card is selected as the "Save Destination".

**Firmware** - This is where the user would put any firmware update files they intend to reflash from the SD Card.

**Packages** - This is where the user should store any package installation files that will be installed from the SD Card.

**Stats** - This is where any exported gatherstats files will be copied when Save Stats to SD Card is set to Yes.

#### Download

Download the selected file to your computer.

It is best practice to insert the SD Card into the DA50N, Apply Directory Structure then move the SD Card to your other environments to copy the applicable files.

## 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 DA50N and third party UDP or TCP/IP Client/Server application.

Select the Serial IP menu item and the following dialog window appears:

**Enable Serial IP:** Select **Yes** to enable the Serial IP Interface.



**Recommended Setting:** Yes, if using this Interface.

**Configuration Description:** Enter a description to describe the intent of this communication.

**Recommended Setting:** Any text up to 128 characters.

### Serial Port Configuration

**Select Interface:** Select the interface to be used by clicking on the drop-down menu. The available options are: Port 1 (RS-232) and Port 2 (RS-485).

**Line Speed:** Select the desired interface speed to be used via the provided drop-down.

**Recommended Setting:** 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 data. This function provides integrity for the device by preventing data from being accepted until it can be delivered successfully.

**Recommended Setting:**

Yes - For standard usage.

No - For serial to TCP Server configuration to insure there is a TCP Server socket available before marking the serial port active.

Negotiate - Only use if directed by technical support personnel.

**Word Length:** Select the word length (bits per character) to be used via the provided drop-down.

**Recommended Setting:** 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.

**Recommended Setting:** 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.

**Recommended Setting:** Consult the configuration of the remote device being attached, this setting must be compatible.

**Connect Mode:** If this option is set to **AT Command**, 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.

**Recommended Setting:** DTR Dial, 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.

**Recommended Setting:** Yes, if 3 wires connection is expected.

**Connection Type:** Select the connection type you desire from the drop-down list.

**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.

**Recommended Setting:** Modem Emulator for direct connection.

**Use Timer Only:** This option provides two different methods of detecting the end of message indicator on received serial port data.

Select **Yes** in order to use the Inter Character Timeout value configured on this device as the end of message indicator.

Select **No** in order to define the end of message character(s) string indicator.

**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.

**Recommended Setting:** 5 milliseconds at 9600 baud.

**Maximum Buffer Size:** This option allow you to set the maximum buffer size to be used for receiving serial data before forwarding to the remote device. A value of ZERO will allocate 8192 bytes of buffer by default and the data could be sent to the remote application based on TCP stack window size.

**Recommended Setting:**  
0 - Otherwise.

**Enable Hardware Flow Control:** Select **Yes** to set hardware flow control using RTS and CTS signals.

**Recommended Setting:**  
No - If dealing with a 3-wire port (Transmit, Receive, and Ground pins).  
Yes - If dealing with a port that has all of the signal pins present.

**Number of Missed Polls Allowed:** This option allow you to set the maximum number of missed RTU polls before reinitializing all the internal memory and buffer conditions. If a packet is transmitted out the serial port and no response packet is received, this is counted as a missed poll and data content is not evaluated.

**Recommended Setting:**  
0 - To disable this action.  
Any other value greater or equal to 5 is dependent upon your environment requirements.

**Show Advanced Configuration:** Select Yes to configure advanced Serial IP options.

**Enable DNIS Table Routing:** Select whether or not to Enable the DNIS Table Routing for this communication.

If this option is selected as **Yes**, the device will use the connect table entries to configure the device for serial and TCP/IP communication. This option will force the device to read multiple entries based on **LABEL** (phone number) and connect to appropriate TCP/IP server destination. You can access the connect Table configuration via GUI by clicking **Advanced**→**GWLNx**→**Connect Table Configuration**.

**Recommended Setting:**  
No - For standard usage.  
Yes - For routing an ATD (phone number) command to a specific remote destination.

#### TCP/UDP Port Configuration

**Socket Type:** Select the Socket Type you desire to have for Serial IP communication from the drop-down list.

**Note:** Drop-down selections vary based on Socket Type selection.  
**Recommended Setting:** Socket Type you desire to have for this communication.

## UDP

If this option is selected, the device will act as a UDP (Connectionless) and listening on the configured **Listening IP Port** for connection from the client.

**Peer IP Address:** 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 us 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.

**Recommended Setting:** <0.0.0.0> to allow any IP to send packets to the peer port number.

**Peer IP Port:** Enter the peer Port number into this field. This is **Required** for UDP communication.

**Recommended Setting:** Consult your network administrator for UDP application destination port number.

**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.

**Recommended Setting:** Consult your network administrator for UDP application destination port number.  
0, if the peer ip is set to <0.0.0.0>.

**Source Interface:** Select a source interface to bind to.

**Note:** This option could be very crucial if your connection is going through some GRE or IPsec tunnels.

**Recommended Setting:** None, if you are not using any tunnels.

## TCP Client

If this option is selected, the device will act as a TCP Client and connects to the host processor once the serial port becomes active.

**Enable IP Destination Config File:** Enabling this option allow you to configure the host destination IP/Port address or DNS Name/Port number via **Advanced**→**GWLNX**→**IP Destination** option. The advantage of this option is to change the host destination without changing any settings in Serial IP configuration screen.

**Recommended Setting:** Yes, if configuring the IP destination via **Advanced**→**GWLNX**→**IP Destination**.

**TCP/UDP Independent Activation:** This option determines if the TCP/IP port of the device will accept data **before** the remote side (Serial Port) is active. At least one of the two sides in the configuration must be set for Independent Activation. If neither side is set, then the device will not accept data. This function provides 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.

**Recommended Setting:** Yes for Servers, No for Clients.

**TCP Headers:** Select the TCP/IP Header Type (Message Length Field) required for TCP/IP communication from the drop-down list.

**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 TCP/IP packet fragmentation.

**Recommended Setting:** None, if TCP headers are not used.

**Host IP Address:** Enter the host destination IP Address into this field. This is **Required** if the device is acting as a TCP/IP Client.

**Recommended Setting:** Consult your network administrator.

**Host IP Port:** Enter the host destination Port Address into this field. This is **Required** if the device is acting as a TCP/IP Client.

**Recommended Setting:** Consult your network administrator.

**Client Source IP:** 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.

**Recommended Setting:** Leave blank to use dynamic source port from TCP stack for 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 provides 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.

**Recommended Setting:** Yes for Servers, No for Clients.

**TCP Headers:** Select the TCP/IP Header Type (Message Length Field) required for TCP/IP communication from the drop-down list.

**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 TCP/IP packet fragmentation.

**Recommended Setting:** None, if TCP headers are not used.

**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.

**Recommended Setting:** No, do not allow, if there is an active socket connection.

**Listening IP Address:** 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 specific IP can connect to our listening port.

**Recommended Setting:** <0.0.0.0> to allow any client to connect to the 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.

**Recommended Setting:** Consult your network administrator for client application destination port number.

#### TCP Client/Server 2Way

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 its status, the device will connect to the host destination to report the device's status.

**Enable IP Destination Config File:** Enabling this option allow you to configure the host destination IP/Port address or DNS Name/Port number via **Advanced**→**GWLNX**→**IP Destination** option. The advantage of this option is to change the host destination without changing any settings in Serial IP configuration screen.

**Recommended Setting:** 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.

**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 TCP/IP packet fragmentation.

**Recommended Setting:** None, if TCP headers are not used.

**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.

**Recommended Setting:** Consult your network administrator.

**Host IP Port (Required):** Enter the host destination Port Address into this field. This is **Required** if the device is acting as a TCP/IP Client.

**Recommended Setting:** Consult your network administrator.

**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.

**Recommended Setting:** Leave blank to use dynamic source port from TCP stack for 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.

**Recommended Setting:** No, do not allow, if there is an active socket connection.

**Listening IP Address:** 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 specific IP can connect to our listening port.

**Recommended Setting:** <0.0.0.0> to allow any client to connect to the listening port.

**Listening IP Port:** Enter the listening Port number into this field. This is **Required** if the device is acting as a TCP/IP Server.

**Recommended Setting:** Consult your network administrator for client application destination port number.

#### UDP Broadcaster

If this option is selected, the device will support multiple UDP broadcast addresses. Click on **Add UDP Broadcast Port** to configure the port through the **UDP Broadcast Port Settings** window.

**Peer IP Address:** 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 us 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.

**Recommended Setting:** <0.0.0.0> to allow any IP to send packets to the peer port number.

**Peer IP Port:** Enter the peer Port number into this field. This is **Required** for UDP communication.

**Recommended Setting:** Consult your network administrator for UDP application destination port number.

**Client IP Port:** 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.

**Recommended Setting:** Consult your network administrator for UDP application destination port number.

0, if the peer IP is set to <0.0.0.0>.

Click on the *Finish* button when the required information has been entered. You will be returned to the IP Destinations dialog window and the UDP Broadcast Configuration table will be populated with the entered data.

#### TCP Client BroadCaster

If this option is selected, the device will support up to 20 TCP Client broadcast socket using IP Destination configuration for connectivity. These sockets are persistent connection when the serial port become active.



Click on *Add* button to define the required IP Destination Settings.

**Enter Address 1:** This is a Client Primary IP address that GWLNX uses to connect to the Host Server. **(Required)**

**Enter Port 1:** This is a Client Primary Port address that GWLNX uses to connect to the Host Server Port. **(Required)**

**Connect Timeout 1:** 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.

**Recommended Setting:** 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. **(Not Required)**

**Enter Port 2:** This is a Client First Alternative Port address that GWLNX uses to connect to the Host Server Port. **(Not Required)**

**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.

**Recommended Setting:** 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. (Not Required)

**Enter Port 3:** This is a Client Second Alternative Port address that GWLNX uses to connect to the Host Server Port. (Not Required)

**Correct 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.

**Recommended Setting:** 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.

**Recommended Setting:** Default.

Click on the *Finish* button when the required information has been entered. You will be returned to the IP Destinations dialog window and the IP Destinations Table Properties table will be populated with the entered data.

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

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert*, will reset all fields to previously saved defaults.

### TCP Client BroadCaster Traffic Activator

If this option is selected, the device will support up to 20 TCP Client broadcast sockets using Configure IP Destinations for connectivity and would connect only if the serial data is available to broadcast. Click on the Configure IP Destinations button to enter port information into the IP Destinations Table. **See *Configure IP Destinations*** explanation below for a description of available options.

**Configure IP Destinations:** Used when TCP Client BroadCaster or TCP Client BroadCaster Traffic Activator Socket Type options are selected.

The screenshot shows a web interface for configuring IP Destinations. At the top, there is a navigation bar with a logo on the left and menu items: Status, Admin, Network, Services, Automation, Advanced, and Events (which is highlighted in red). A Logout button is on the right. Below the navigation bar, the page title is 'IP Destinations'. Underneath, there is a sub-header 'IP Destinations Table Properties' above a table. The table has 10 columns: Address 1, Port 1, Connect Timeout 1, Address 2, Port 2, Connect Timeout 2, Address 3, Port 3, Connect Timeout 3, and Header. The table is currently empty. To the right of the table, there are five buttons: 'Add' (green), 'Edit', 'Delete', 'Up', and 'Down' (all in grey).



Click on *Add* button to define the required IP Destination Settings.

The screenshot shows a dialog box titled "IP Destination Settings" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Enter Address 1:** A text input field with a red border and a "Required" label in a red box to its right.
- Enter Port 1:** A text input field with a red border and a "Required" label in a red box to its right.
- Connect Timeout 1:** A text input field containing the value "10" and a "Required" label in a red box to its right.
- Enter Address 2:** A text input field.
- Enter Port 2:** A text input field.
- Connect Timeout 2:** A text input field.
- Enter Address 3:** A text input field.
- Enter Port 3:** A text input field.
- Connect Timeout 3:** A text input field.
- Header Type:** A dropdown menu with "Default" selected.

A blue "Finish" button is located at the bottom center of the dialog.

**Enter Address 1:** This is a Client Primary IP address that GWLNX uses to connect to the Host Server. **(Required)**

**Enter Port 1:** This is a Client Primary Port address that GWLNX uses to connect to the Host Server Port. **(Required)**

**Connect Timeout 1:** 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.

**Recommended Setting:** 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. **(Not Required)**

**Enter Port 2:** This is a Client First Alternative Port address that GWLNX uses to connect to the Host Server Port. **(Not Required)**

**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.

**Recommended Setting:** 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. **(Not Required)**

**Enter Port 3:** This is a Client Second Alternative Port address that GWLNX uses to connect to the Host Server Port. **(Not Required)**

**Correct 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.

**Recommended Setting:** 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.

**Recommended Setting:** Default.

Click on the *Finish* button when the required information has been entered. You will be returned to the IP Destinations dialog window and the IP Destinations Table Properties table will be populated with the entered data.

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

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert*, will reset all fields to previously saved defaults.

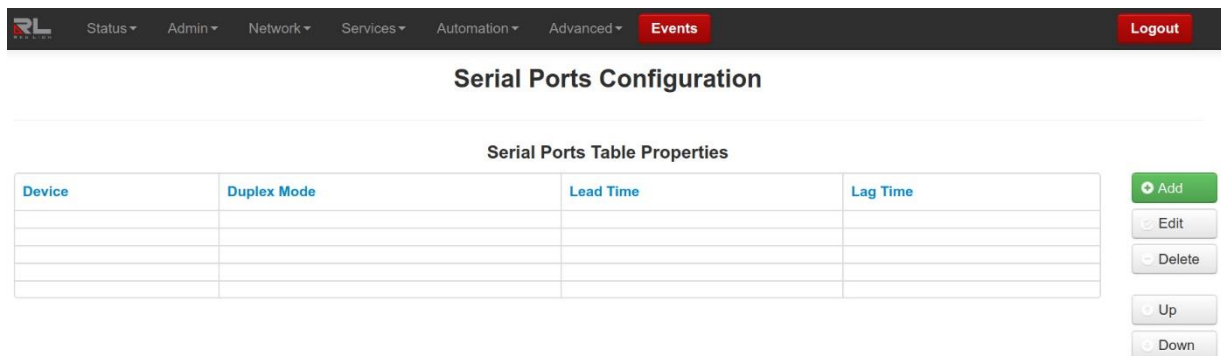
## Automation Tab

The Automation menu contains all aspects of managing, controlling, and monitoring the onboard I/O of your DA50N. I/O data is stored in a local I/O database, and can be used for development of third-party applications using our SDK based on ELDK4.2 and the Sixnet® IODB API.

## Serial Ports

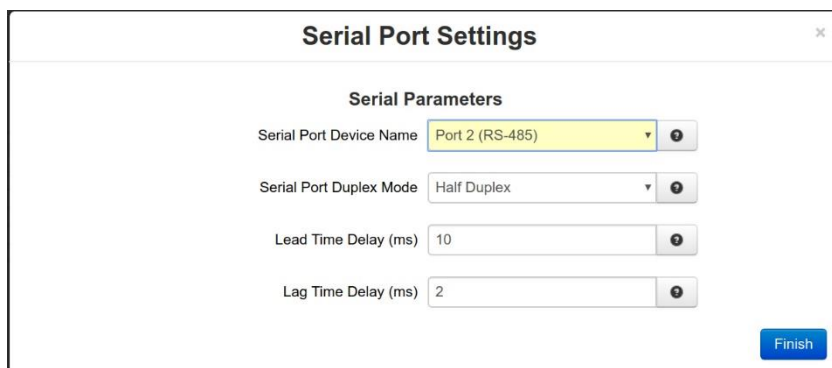
This section is used to configure the RS-232 port that is facing the front of the DA50N as well as the RS485 to integrate into your schema.

Click on the Serial Port menu item and the following window appears:



The screenshot shows the 'Serial Ports Configuration' window. At the top is a navigation bar with 'Automation' selected. Below the title is a table titled 'Serial Ports Table Properties' with columns: Device, Duplex Mode, Lead Time, and Lag Time. To the right of the table are buttons for 'Add', 'Edit', 'Delete', 'Up', and 'Down'. The table is currently empty.

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



The screenshot shows the 'Serial Port Settings' pop-up window. It contains the following fields:

- Serial Port Device Name: Port 2 (RS-485)
- Serial Port Duplex Mode: Half Duplex
- Lead Time Delay (ms): 10
- Lag Time Delay (ms): 2

A 'Finish' button is located at the bottom right of the window.

## Serial Parameters

**Serial Port Device Name:** Name of the serial device.

**Valid values:** ttys1 (RS232) | ttys5 (RS485).

**Serial Port Duplex Mode:** Select desired duplex mode control for RS-485 serial port.

**Recommended Setting:** Half Duplex.

**Lead Time Delay (ms):** RS-485 Lead and Lag Time in milliseconds.

Red Lion RS485 ports support lead time and lag time delays. Lead and lag times can be specified for Half Duplex and Full Duplex Modem flow control methods only. In Half Duplex and Full Duplex Modem modes, the RTS signal is typically used as a transmitter key. When data is to be sent, the RTS signal will be asserted. Then, after the lead time delay, data will be transmitted. (The lead time allows the transmitter to warm up.) After the data is transmitted, the RTS signal will remain asserted for the lag time duration, to help assure that the transmitted data will not be corrupted when the transmitter turns off.

**Recommended Lead and Lag Time:**

Lead Time: 10ms.

Lag Time: 2ms.

**Lag Time Delay (ms):** RS-485 Lead and Lag Time in milliseconds.

Red Lion RS485 ports support lead time and lag time delays. Lead and lag times can be specified for Half Duplex and Full Duplex Modem flow control methods only. In Half Duplex and Full Duplex Modem modes, the RTS signal is typically used as a transmitter key. When data is to be sent, the RTS signal will be asserted. Then, after the lead time delay, data will be transmitted. (The lead time allows the transmitter to warm up.) After the data is transmitted, the RTS signal will remain asserted for the lag time duration, to help assure that the transmitted data will not be corrupted when the transmitter turns off.

**Recommended Lead and Lag Time:**

Lead Time: 10ms.

Lag Time: 2ms.

Click on the *Finish* button to populate the Serial Ports Table Properties.

To delete a serial port, select it in the table and click on the *Delete* button. To edit a serial port, select it in the table and click on the *Edit* button.

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

## Tags

Tags allow you to identify registers by name in addition to a type and address.

**Name:** String identifier for the register. This will make the register available in tag drop-down fields throughout the user interface. Valid values: Alphanumeric including period (.) and underscore (\_) up to 64 characters. Tags **are** case sensitive.

**Type:** Internal I/O type associated with the register.

**Address:** I/O address associated with the register.

**Data Type:** Properties of how to decode raw register data, such as signedness. Test I/O and other contexts can interpret multiple registers as members of a larger data type.

**Units:** User editable field to specify kind of data. Ft, m, in, mB, dBm, etc.

**Deadband:** The amount of +/- fluctuation of the data value before triggering a change notification for Events, Data Logger, or other services.

**Description:** Additional identifying information. Limited to 40 characters. May **not** use a comma.

**Retain:** (*availability based on model*) Checking this box will allow the register value associated with the tag to be retained in battery-backed SRAM across a device power cycle.

Retain	Name	Type	Address	Deadband	Units	Description	
-	AI1	AI	1			Analog In	Undo
-	AI2	AI	2			Analog In	Undo
-	AI3	AI	3			Analog In	Undo
-	DI1	DI	1			Digital Input	Undo
<input type="checkbox"/>	DO1	DO	1			Digital Output	Undo

Name	Type	Address	Units	Description
Serial_Number_U16_A	AO	1001		First 4 digits UINT16
Serial_Number_U16_B	AO	1002		Next 4 digits
Serial_Number_U16_C	AO	1003		Next 4 digits
Serial_Number_U16_D	AO	1004		Last 4 digits
Serial_Number_U64_A	AO	1005		UINT64 format;LSW
Serial_Number_U64_B	AO	1006		
Serial_Number_U64_C	AO	1007		
Serial_Number_U64_D	AO	1008		
Model_Number	AO	1009		4 digit model number
Firmware_Version	AO	1010		3 digit number

### User Defined


Create custom tags for your I/O here. These tags will be listed in drop-down forms throughout this user interface. Tag names must be unique and may not copy the names of Onboard or Status tags.

To add a new tag, click on the Add button located at the bottom of the dialog window. A new blank line appears.

Retain	Name	Type	Address	Data Type	Deadband	Units	Description	
<input type="checkbox"/>	Name	Type	1				Description	Remove Undo


### Onboard I/O

These tags are linked to physical I/O on the device. You cannot change the type or address, but you may rename them according to function or connected hardware.

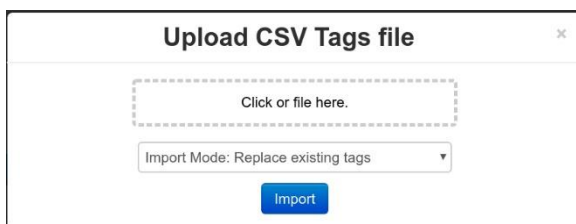
Onboard I/O 							
Retain	Name	Type	Address	Deadband	Units	Description	
-	AI1	AI	1			Analog In	Undo
-	AI2	AI	2			Analog In	Undo
-	AI3	AI	3			Analog In	Undo
-	DI1	DI	1			Digital Input	Undo
<input type="checkbox"/>	DO1	DO	1			Digital Output	Undo

### System Status

These tags are linked to status metrics internal to the device. They cannot be renamed or otherwise modified. See **Appendix B** for more information.

System Status 				
Name	Type	Address	Units	Description
Serial_Number_U16_A	AO	1001		First 4 digits UINT16
Serial_Number_U16_B	AO	1002		Next 4 digits
Serial_Number_U16_C	AO	1003		Next 4 digits
Serial_Number_U16_D	AO	1004		Last 4 digits
Serial_Number_U64_A	AO	1005		UINT64 format;LSW
Serial_Number_U64_B	AO	1006		
Serial_Number_U64_C	AO	1007		
Serial_Number_U64_D	AO	1008		
Model_Number	AO	1009		4 digit model number
Firmware_Version	AO	1010		3 digit number
Date_Year	AO	1011		Year 4 digit number
Date_Month	AO	1012		Month 1-12
Date_Day	AO	1013		Day 1-31
Date_DayOfWeek	AO	1014		Day 0-6

Click on the *Refresh* button to refresh screen after new entries have been entered.  
 To delete an existing tag, click on the *Remove* button next to the tag to be deleted.  
 To export the list of tags, click on the *Export* button and a *tags.csv* file will be created and can be found in the PC's downloads folder.  
 To import a list of tags, click on the *Import* button and the Upload CSV Tags file dialog window appears.

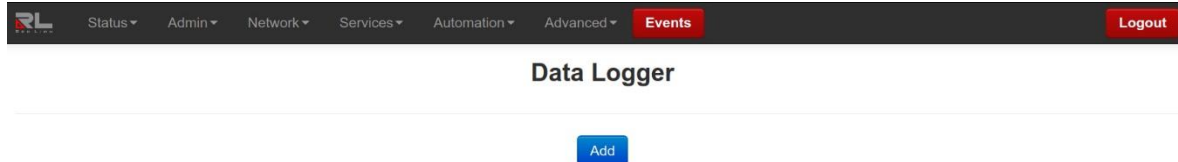


Click on the dashed button and browse to the location where the.csv file is located, select the Import Mode, then press the *Import* button. You may also drag the.csv file from a window and drop into the file upload dialog box.

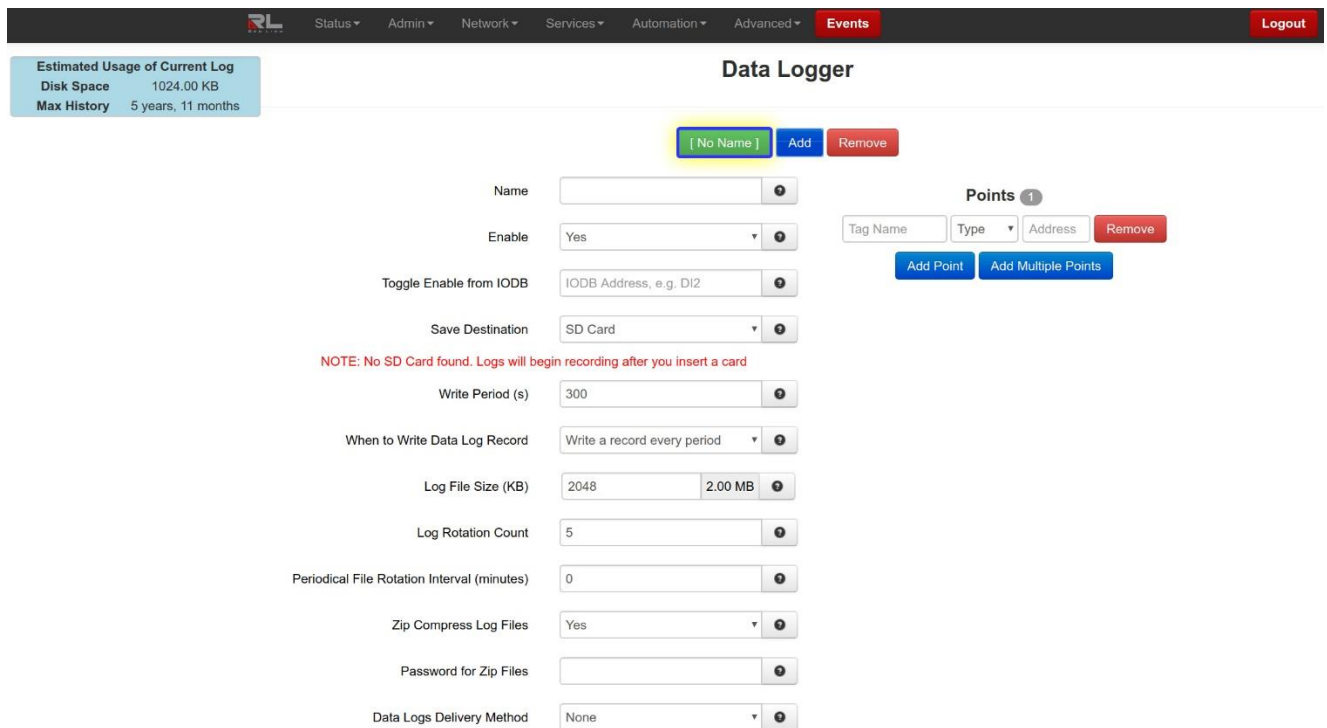
To restore the system default Tags, click on the Restore Defaults button. All user defined tags will be removed from the list.

## Data Logger

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



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



**Name:** The name of your log. This will also be a prefix for the log files.

**Allowed Characters:** A-Z, a-z, 0-9, -, ., and \_.

**Enable:** Enable this log. Points will be periodically recorded in a log file prefixed with specified Name.

**Toggle Enable from IODB:** Toggle logging based on IODB register.

For example, if set to DI42, Points will only be recorded if register DI42 is high.

**Note:** This field will also accept a tag. (Optional)

**Save Destination:** Destination for the log files.

**Internal** will configure your logs to be stored internally on the device. These can be downloaded through the Web UI or with gatherstats.

**External USB** (if applicable) will configure your logs to be stored on an attached USB storage drive (if present).

Logs will be created in this folder:

```
usb-storage/datalogs/
```

**SD Card** (if applicable) will configure your logs to be stored on the SD Card (if present).

Logs will be created in this folder:

```
sdcard/datalogs/
```

**Note:** Estimated disk usage may change based on anticipated filesystem compression. This is in addition to any zip compression.

**Write Period(s):** How often a data log record will be created (in seconds).

**Recommended:** Relative to the rate of change you expect from the logged points.

**When to Write Data Log Record:** Paired with the write period, this will control what conditions create a data log record.

**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).

**Log File Size (KB):** Log file size (per file) in Kilobytes.

Max: 10240 KB (10 MB)

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.

**Periodical File Rotation Interval (minutes):** Enter the time period in minutes for timely file rotation. It is better to be divisible by 24 hours if expected to have scheduled file rotation at the same time during day/week.

Entering a '0' value will disable the timely file rotation and only relies on file size to trigger.

**Note:** Configure the file size bigger than usual one that will be reached during each time period to avoid early size triggered file rotation outstanding from the scheduled ones.

**Zip Compress Log Files:** Compress log files using zip.

This will reduce storage space by 80%-90%.

**Password for Zip Files:** Encrypt zip-compressed log files using this password.

**Data Logs Delivery Method:** Select the delivery method for generated data logs.

**Note:** Additional menu items are dependent on Data Logs Delivery Method selection.

**FTP Mode:** Select FTP security mode.

**Passive:** In passive mode FTP the client initiates both connections to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server. When opening an FTP connection, the client opens two random unprivileged ports locally ( $N > 1023$  and  $N+1$ ). The first port contacts the server on port 21, but instead of then issuing a PORT command and allowing the server to connect back to its data port, the client will issue the PASV command. The result of this is that the server then opens a random unprivileged port ( $P > 1023$ ) and sends P back to the client in response to the PASV command. The client then initiates the connection from port ( $N+1$ ) to port P on the server to transfer data.

**Active:** In active mode FTP the client connects from a random unprivileged port ( $N > 1023$ ) to the FTP server's command port, port 21. Then, the client starts listening to port ( $N+1$ ) and sends the FTP command PORT ( $N+1$ ) to the FTP server. The server will then connect back to the client's specified data port from its local data port, which is port 20.

**FTP Security Mode:** Select FTP security mode.

**Implicit:** Negotiation is not supported with implicit FTPS configurations. A client is immediately expected to challenge the FTPS server with a TLS **ClientHello** message. If such a message is not received by the FTPS server, the server should drop the connection.

In order to maintain compatibility with existing non-FTPS-aware clients, implicit FTPS was expected to listen on the IANA well known port 990/TCP for the FTPS control channel, and port 989/TCP for the FTPS data channel. This allowed administrators to retain legacy-compatible services on the original 21/TCP FTP control channel.

**Explicit:** In explicit mode (also known as FTPES), an FTPS client must **explicitly request** security from an FTPS server and then step up to a mutually agreed encryption method. If a client does not request security, the FTPS server can either allow the client to continue in insecure mode or refuse the connection.

**FTP Server IP or Domain:** Enter the FTP server IP address or domain name.

**FTP Server Port:** Enter the Port number associated with the IP Address or domain name.

**User Name:** Enter the user name required to connect to FTP server.

**Password:** Enter the password required to connect to FTP server.

**Email Recipient:** Enter an email address destination for the logs. Multiple email addresses may be entered by separating them with a **comma**.

**Note:** No spaces are allowed in this field.

**Note:** The Email Client service must be configured independent from the Datalog before emails can be sent successfully.

## Points

Configure fields to create data points.

**Tag Name:** Enter the name.

**Type:** Select from the drop-down menu options.

**Address:** Enter the point address.



### Add Point

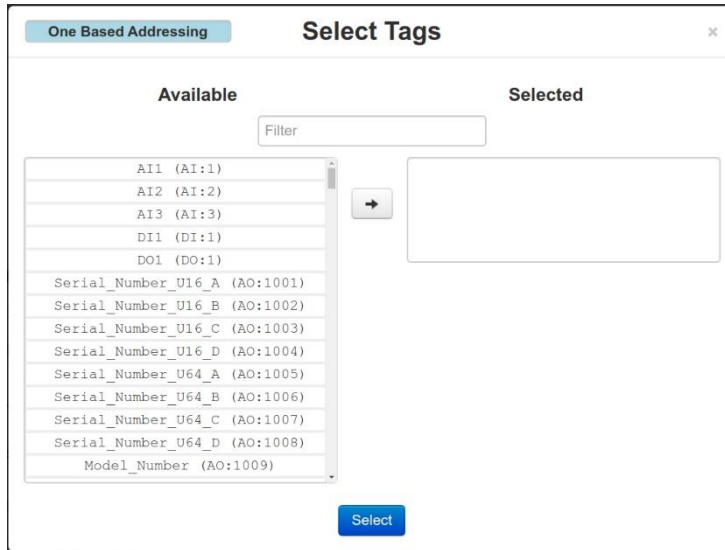
Click to add the point just configured.

### Remove

Click to remove a data point.

### Add Multiple Points

Click to invoke a pop-up screen to select multiple points individually or all at once.



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

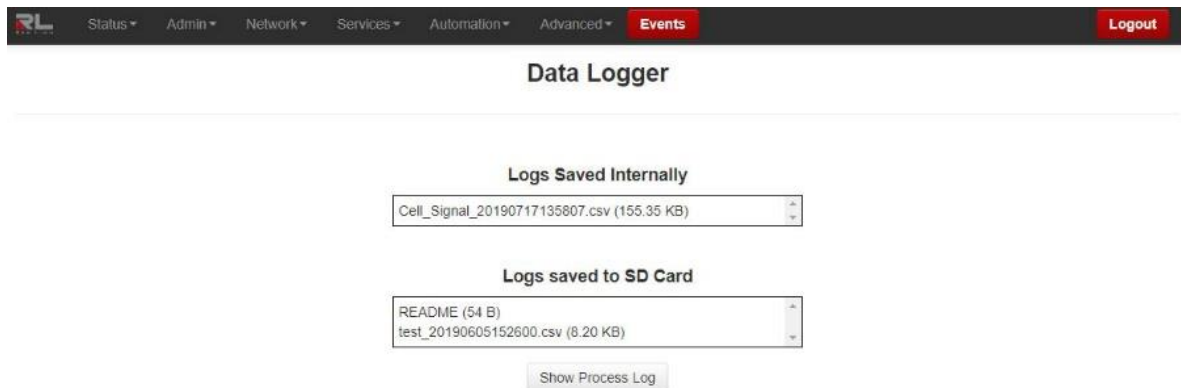
**Base 1 or 0:** Display toggle buttons located in the footer bar and will toggle the display of registers visible on the page from 0 based to 1 based.

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

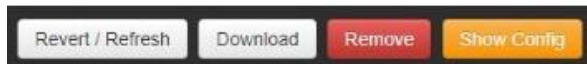
### Navigation

Click on the green named log file button to display the data log configuration associated with the displayed log file name ([GPS\_DataLog] in this example). Then click on Show Logs to display the list of datalog files.

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



Click on any file to select the log file to Download, View, Remove or show the Process log associated with the log file.



Click on the *Download* button to copy the selected Data Logger file to your PC for evaluation.  
Click on the *View* button to load a snapshot of the beginning and end of the highlighted file, but does not display the entire file.  
Click on the *Remove* button to remove the currently selected datalog config.  
Click on the *Show Config* button to return to the Data Logger configuration screen.

## I/O Settings

### I/O Control

Click on the I/O Control menu item and the I/O Control window appears.

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

**Recommended Setting:** Yes, if using this interface.

Define Internal I/O Database Addresses

**Digital Input Address:** Enter the address of internal Modbus address for Digital Input I/O control.

**Valid Address:**

**Zero Based Addressing:** 0 through 65535 as defined for specified I/O type.

**One Based Addressing:** 1 through 65536 as defined for specified I/O type.

**Note:** 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.

**Digital Input Counter Address:** Enter the address of internal Modbus address for Digital Input Counter.

**Valid Address:**

**Zero Based Addressing:** 0 through value of defined register allocation configured for Analog Input I/O type **minus 1**.

**One Based Addressing:** 1 through value of defined register allocation configured for Analog Input I/O type.

**Note:** 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 **CAN NOT** be the same address as Analog Input Address. Care to select a unique address to be used in Analog Input Modbus for Digital Input Counter.

**Digital Output Address:** Enter the address of internal Modbus address for Digital Output I/O control.

**Valid Address:**

**Zero Based Addressing:** 0 through 65535 as defined for specified I/O type.

**One Based Addressing:** 1 through 65536 as defined for specified I/O type.

**Note:** 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.

**Analog Input Address:** Enter the address of internal Modbus address for Analog Input I/O control.

**Valid Address:**

**Zero Based Addressing:** 0 through value of defined registers configured for specified I/O type minus 1.

**One Based Addressing:** 1 through value of defined registers configured for specified I/O type.

**Note:** 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):** Enter update interval, in milliseconds, for updating the internal I/O Data Base.

**Recommended Value:** 500ms or higher.

Update I/O CTRL Screen Display Value

**Enable Auto update:** Select **Yes** to enable automatic updating of the I/O ports value, 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.

**Recommended Setting:** 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:

- 1
- 2
- 3
- 5
- 10
- 15

**Recommended Setting:** Be advised that when connected via a Cellular interface, the data collected will count towards your total data plan usage.

Click the *Refresh* button to refresh the page, the *Apply* button to apply changes immediately and the *Save* button to save changes.

## Test I/O

Test I/O is used to verify the functionality of I/O states in the DA50N.

During a power cycle of the DA50N, values for Tags will not be preserved unless the Retain option checkbox is checked. Since I/O data is critical for the device use, we offer the I/O Retain feature to store the configured I/O data for as long as the on-board battery can supply the SRAM. The Test I/O Access screen offers the means of testing an I/O after startup to verify critical I/O data is retained by reading the outputs and sending corresponding physical signals to devices.

**Note:** The Retain option is only available on specific tags for the DA50N.

The Test I/O Access screen offers the means of testing an I/O after startup to verify critical I/O data is present by reading the outputs and sending corresponding physical signals to devices.



**Scan Rate:** This is the time in which the screen will automatically refresh values from the internal IODB.

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

**Adding a Tag:** Start typing the tag name you would like to add and a pop up appears that lists all tags that match the pattern you entered. Click the Tag name to select it from the pop up list.

**To List:** Select the list to add the selected tag to or create a list by entering its name here and clicking on Add. Lists are used to group I/O points together for more organized viewing.

**Multiple:** Select multiple tags to add to the indicated list from the Add to set pop up screen and clicking on Select to add the selected tags to the list.

**Load Set Select Module:** Select the desired IODB Status Module from the drop down list. Valid IODB Modules are:

- System Status
- Traffic
- GPS
- Network
- Cellular
- On-board IO
- User List

**Add Raw I/O:** From the drop down list, select the type of I/O you would like to test. Valid I/O types are:

- Analog In
- Analog Out
- Analog In (16bit)
- Analog Out (16bit)
- Discrete In
- Discrete Out
- Long In
- Long Out
- Float In
- Float Out

**Start Address:** Once the I/O type has been selected, enter the Start Address.

**Register Count:** Enter the Register Count for the number of registers you would like to display.

**To List:** Select the list to add the selected tag or create a list by entering its name here and clicking on Add. Lists are used to group I/O points together for more organized viewing.

Click on the *Add* button to test the I/O.

The messages logs show the range entered and each register that can be edited and monitored for the analog inputs.

### Base 1 or 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>.

## Advanced Tab

The Advanced tab provides user access to advanced configuration features available for the DA50N, including IP Fallback, IP Transparency, Out-of-Band Mgt, VRRP, Expert Mode, GWLNX, and About.

### IP Fallback

The IP Fallback option is used to configure the DA50N to failover between two interfaces, e.g. Primary route on T1/ DSL/Cable on eth0, and secondary on Cellular if the primary loses Internet connection.

Click on the *IP Fallback* menu item and the following dialog window appears:

The screenshot shows the 'IP Fallback' configuration window. At the top, there is a navigation bar with 'Events' highlighted and a 'Logout' button. The main title is 'IP Fallback'. Below it, the section is 'Automatic Default Route Failover Settings'. The settings are as follows:

- Enable IP Fallback: Yes (dropdown menu)
- Select Primary Interface: wwan0 (dropdown menu)
- Select Primary External Command Script: None (dropdown menu)
- Select Secondary Interface: eth0 (dropdown menu)
- Select Secondary External Command Script: None (dropdown menu)
- Enter Primary Test IP Address: (text input, Required)
- Enter Request Interval (seconds): 30 (text input, Required)
- Number of Test Packets to Send: 5 (text input, Required)
- Allowable Test Packet Loss: 2 (text input)
- Ping Round Count: 0 (text input)
- Switch Back Delay (minutes): 0 (text input)
- Select Debugging Level: 0 (dropdown menu)

**Enable IP Fallback:** Specify whether you want to use IP Fallback. If yes, the service will be started after you click **Apply**, and on each subsequent re-boot.

**Recommended Setting:** Enable this option only if you have two paths (interfaces) configured with WAN (internet) support. An example would be primary Ethernet (eth0) and secondary cellular (ppp0/wwan0).

**Notes:** When using an Ethernet port setup as a DHCP Client, please choose: **Use Remote Gateway as Default Route? : No** in the Ethernet port setup screen. Default route control will be managed by IP Fallback instead.

**Select Primary Interface:** Specify your desired primary interface for IP Fallback behavior.

**Select Primary External Command Script:** Choose the name of the command script to be executed when the associated interface becomes active.

For example, if Restart IPsec is an option, then when selected, will be run whenever the fallback logic selects and activates this interface.

**Recommended Setting:**

None for standard operation with no special behaviors.

Restart IPsec is useful when using an IPsec VPN tunnel.

**Select Secondary Interface:** Select the secondary interface to be used for IP Fallback.

Selecting "vrrp" will coordinate with the VRRP process, so that when the primary interface is determined to be unavailable, VRRP will stop broadcasting availability.

**Select Secondary External Command Script:** Choose the name of the command script to be executed when the associated interface becomes active.

For example, if a Restart IPsec is a option, then when selected, will be run whenever the fallback logic selects and activates this interface.

**Recommended Setting:**

None for standard operation with no special behaviors.

Restart IPsec is useful when using an IPsec VPN tunnel.

**Enter Primary Test IP Address:** Specify the IP address of a host with which the IP Fallback service will communicate to test connectivity. Value must be a pingable address, and not a domain name. The best choice would be an address that represents end-to-end connectivity. **(Required)**

**Enter Request Interval (in seconds):** Specify the time, in seconds, to wait between connectivity tests. The minimum is 10; maximum is 600.

**Note:** This value should be 30 or higher for cellular connections.

**Number of Test Packets to Send:** Specify the number of 0 byte ping packets to send out to test connectivity. The minimum is 2, maximum is 30.

**Recommended Setting:** 5 - 10.

**Allowable Test Packet Loss:** Specify the number of lost packets that are acceptable before the IP Fallback service will consider the link unavailable, and switch to its secondary.

**Note:** The value must be less than the number of test packets set via **Test Packets to Send**.

**Ping Round Count:** This is the number of **ping rounds** that must be successful in a row to switch back from the secondary interface to the primary.

The purpose is to delay switching back to the primary until it has proven stable to multiple tests.

Must be a number from 0 to 10.

**Example:** Setting this value to 3 means 3 complete ping set rounds must be successful based on the configuration prior to switching back to the primary interface.

**Default:** 0 (disabled).

**Switch Back Delay (minutes):** The minimum number of minutes to wait prior to switching from the secondary interface back to the primary interface.

The purpose is to prevent rapid flipping in an unstable environment. A larger value will force the secondary link to be used for a longer period of time, even if the primary becomes available.

Must be a number from 0 to 10.

**Example:** Setting this value to 5 will set a minimum delay of 300 seconds (5 minutes). If the process switches to the secondary due to a failure, and after 2 minutes the primary interface is determined to be good (based on the configuration), there will still be an extra 3 minute delay prior to switching back to the primary interface.

**Default:** 0 (disabled).

**Select Debugging Level:** Specify a debug level for logging purposes. Recommended only when existing configurations do not function as expected, and when directed to change by Technical Support personnel.

Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit.

Click the *Apply* button will save your settings and apply them immediately.

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

## IP Transparency

IP Transparency is supported on DA50N. The IP Transparency menu item is used to configure the transparent bridging capability of the DA50N.

IP Transparency is a special use capability. IP Transparency will take all inbound traffic to the DA50N and pass it transparently through to the interface specified. This is useful when it is desired to pass traffic to a legacy firewall, or VPN concentrator located behind the DA50N and not to use the firewall or VPN capabilities of the DA50N itself.

Click on the *IP Transparency* menu item and the IP Transparency dialog window appears.



**Enable IP Transparency:** Select **Yes** to enable the IP Transparency feature. Settings will take effect immediately when the **Apply** button is clicked, or after a reboot when **Save** is clicked. **(Required)**

**Note:** Enabling IP Transparency will negate all configured firewall rules. The firewall and DMZ Host services will be disabled prior to using IP Transparency.

**Select Internal Interface:** Select the interface to be designated the **internal** interface by making the appropriate choice from the provided list. The Cellular IP will be issued out this interface to one and only one endpoint. **(Required)**

**Interface Speed/Duplex:** Select the Speed and Duplex to be used for the physical interface.

The following options are available:

**Auto Detect:** Use the 'best negotiated' speed and duplex (default).

**10 Mbps/Half:** Force the interface to 10 Mbps and half-duplex.

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

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

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

**Recommended Setting:** Auto-Detect.

**Enable DHCP Server:** Select Yes to allow the DHCP Server(s) to be enabled while IP Transparency is in effect. This will automatically issue the single Cellular IP to one and only one host on the internal interface.

**DHCP Subnet Type:** Subnets can be built three ways:

Calculated subnet will be based on the actual IP address received from the cellular network and choose the smallest subnet that can encompass the cellular IP. This option is more compatible with a wide variety of routers, but will mask out nearby IP addresses. This may make other IP's within the host network unreachable.

Point-to-Point uses a /32 subnet, but is not compatible with some routers.

Wide uses a Class B subnet to move the unroutable network/broadcast addresses away from the IP assigned. This will offer compatibility to reach nearby IP addresses of other cellular units. Private IP setting is required and will be enabled.

**Recommended Setting:** Wide if possible, then Calculated.

**DHCP Lease Time:** Choose the time for DHCP Leases when issuing the Transparent IP.

**Recommended Setting:** 4 Hours.

**Use Private 169.254.x.x IP:** Select whether the internal IP Transparency Interface will host a **dummy** gateway IP similar to the IP Transparency IP, or if it uses a calculated 169.254.x.x IP Address.

Some Cisco routers might not handle ARP properly when this option is turned on.

**Pros:** Option turned off may allow some Cisco routers to ARP better. With the option enabled, nearby cellular IPs may become reachable. If you are trying to connect to another cellular device with a very similar IP address, consider testing with this option enabled.

**Cons:** With the option turned off the unit will black hole some IPs, and they will not be reachable from the device behind. Example: IP from ISP is 1.2.3.2. Calculated Mask is 255.255.255.252. Edge device uses dummy IP 1.2.3.2/30. Now IPs 1.2.3.0 and 1.2.3.3 become unroutable beyond the device.

**Recommended Setting:** Yes. Required for Wide mode.

**Allow TELNET access to this device:** Select **Yes** to allow Telnet access to this device. Incoming connections on the specified port will be directed internally to port 23, instead of to the device behind the specified Internal Interface.

**Note:** For this option to function properly, the Telnet Server must be enabled on port 23 via the Services tab.

**Allow SSH access to this device:** Select **Yes** to allow SSH access to this device. Incoming connections on the specified port will be directed internally to port 22, instead of to the device behind the specified Internal Interface.

**Note:** For this option to function properly, the SSH Server must be enabled on port 22 via the Services tab.

**Allow SNMP access to this device:** Select **Yes** to allow SNMP access to this device. Incoming connections on UDP port 161 will be directed internally to port 161, instead of to the device behind the specified Internal Interface.

**Note:** For this option to function properly, the SNMP Agent must be enabled via the Services tab.

**Allow access to Web UI:** Select **Yes** to allow access (for incoming TCP Port 10000 connections) to the Web UI on **this device**. Selecting No will allow the connection through to the device behind the selected interface.

**Recommended Setting:** Yes.

**Enter Web UI:** Enter the TCP Port number to be used for Web UI access. When Web UI access has been enabled, the port chosen will be redirected locally (to internal 10000). Port 10001 will also be directed to internal 10001 to support HTTPS redirect mode. Connections on these port numbers will not reach the device behind the specified Internal Interface. **(Required)**

**Recommended Setting:** 10000 - All Web UI traffic will be redirected locally to port 10000 automatically. This behavior is built-in and not configurable.

**Allow access by SixView Manager:** Select **Yes** to allow access (for incoming TCP Port 7785 connections) to trigger this device for remote check-in by the SixView Manager server. Selecting No will allow the connection through to the device behind the selected interface.

**Recommended Setting:** Yes.

**Enter MAC filter:** Enter a valid MAC address using the following format: *nn:nn:nn:nn:nn:nn*, where *nn* is a number in hexadecimal form (0-9, a-f, A-F) to enable a MAC filter for use with IP Transparency.

A MAC filter allows only packets whose MAC address matches the filter value to be passed thru this device.

Leaving this field empty effectively disables MAC filtering.

**Enable Out-of-Band Port Redirect:** Select **Yes** to allow any Out-of-Band ports to be redirected locally to this device. When enabled, the OOB Ports specified in the Advanced→Out-of-Band Mgt section will be automatically allowed.

**Recommended Setting:** Yes – When also configuring **Out-of-Band Mgt** on this unit.

**Enable Port Redirecting:** Select **Yes** to allow redirecting of ports to a device beyond this device (the one being configured).

Example: A device beyond the IPT device is running a WEB server on Port 80, but an upstream router is blocking Port 80. Redirecting traffic to another port, say 8080, allows communication with the server. This would be setup as our External port 8080 redirected to an Internal Port 80, Protocol TCP.

When this feature is enabled a new field appears containing a table into which multiple entries can be entered. Each entry will include the External and Internal Port numbers and a traffic type (TCP or UDP).

**Enable Traffic Restrictions:** Select **Yes** to restrict traffic to a device beyond this device (the one being configured).

When this feature is enabled, a Traffic Restrictions table appears to allow selection of the restriction mode and a table into which multiple entries can be entered. Each entry will specify the network IP address range to which the restrictions will be applied.

### Port Re-directs

**Port Re-directs**

External Port	Internal Port	Protocol

+ Add  
Edit  
Delete  
Copy  
  
Up  
Down

Click the *Add* button and the following menu appears:

**Port Re-direction Settings** ✕

External Port #  ⓘ Required

Internal Port #  ⓘ Required

Protocol TCP ⓘ

Finish

**External Port #:** Enter the IP Port number to be used as the External Port for redirection. This is the port that incoming connections are **destined** to, on the cellular interface. **(Required)**

**Internal Port #:** Enter the IP Port number to be used as the Internal Port for redirection. This is the port that incoming connections are **transformed** to, in order to reach a listening process (on this same port) on the device behind the specified Internal Interface. **(Required)**

**Protocol:** Select either TCP or UDP as the protocol for which to apply the redirection from the drop down list provided.

Click on the *Finish* button to populate the Port Re-directs table.

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.

### Traffic Restrictions

**Traffic Restrictions**

Select method of traffic restriction None ⓘ

Subnet

+ Add  
Edit  
Delete  
  
Up  
Down

**Select method of traffic restriction:** This field is enabled when Traffic Restrictions have been enabled.

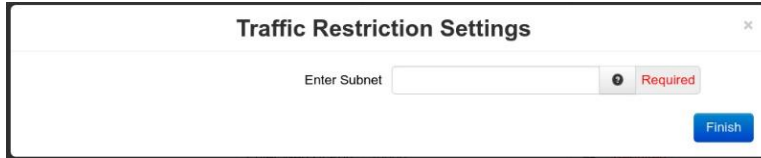
Select the restriction mode from the list provided.

Choices include:

**None** – No filtering is performed.

- In** - Allow new incoming connections from the associated subnet list only, but allow any originating outbound connections from the host behind **this** device. (Inbound Restriction)
- Only** - Allow connections to/from the associated subnet list only. (Inbound and Outbound Restrictions)

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



**Enter Subnet:** Enter subnet range for which to restrict traffic in the CIDR form **nnn.nnn.nnn.nnn/xx**, where **nnn.nnn.nnn.nnn** is the IP Address and **xx** is the subnet in Network Bits format. **(Required)**

Click on the *Finish* button to populate the Table Restrictions screen.

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

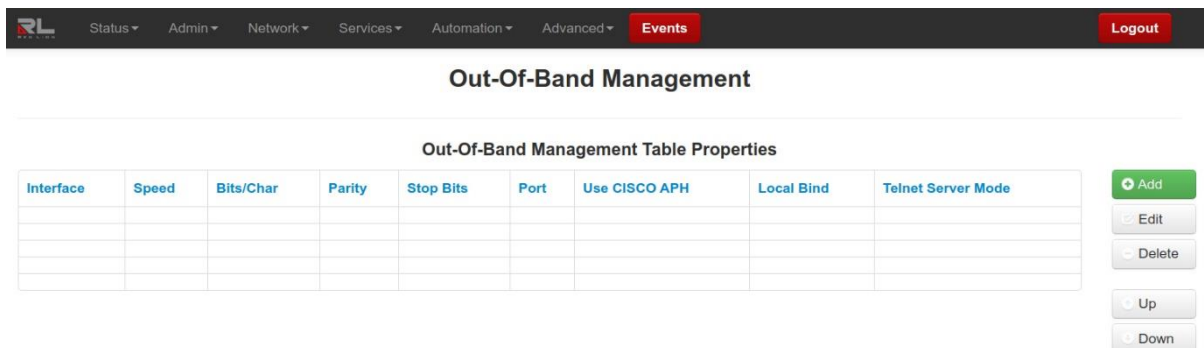
Click on the *Save* button for changes to be saved without activating the interface until you reboot the unit, the *Apply* button will save your settings and apply them immediately. To revert to the previous defaults, click on the *Revert* button.

## Out-of-Band Mgt

The Out-of-Band (OOB) Mgt menu item is used to configure the capability of remotely administrating a third-party device connected via a serial cable on the DA50N.

**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 DA50N from the RS-232 serial port.

Click on the *Out-of-Band Mgt* menu item and the following dialog window appears:



Click on the *Add* button to add an instance for OOB Management and the Out-of-Band Settings window appears.

The screenshot shows a configuration window titled "Out-Of-Band Settings". It contains the following fields and values:

- Interface: Port 1 (RS-232)
- Speed: 115.2 Kbps
- Bits Per Character: 8
- Parity: None
- Number of Stop Bits: 1
- Port Number: (empty, with a "Required" label)
- Use CISCO APH: No
- Use Local Binding: No
- Telnet Server Mode: Disabled

A "Finish" button is located at the bottom right of the window.

**Interface:** Select the interface to be used via the provided drop-down.

**Speed:** Select the desired interface speed to be used via the provided drop-down.

**Recommended Setting:** Consult the configuration of the remote device being attached, this setting must be compatible.

**Bits per Character:** Select the number of stop bits to be used via the provided drop-down.

**Recommended Setting:** 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.

**Recommended Setting:** Consult the configuration of the remote device being attached, this setting must be compatible.

**Number of Stop Bits:** Select the number of stop bits to be used via the provided drop-down.

**Recommended Setting:** Consult the configuration of the remote device being attached, this setting must be compatible.

**Port Number:** Enter a valid port number (1-65535) to be used for the connection. **(Required)**

**Recommended Setting:** Take care to choose a port number not already used by other system services. Consult **Status**→**Network**→**Socket Statuses**→**TCP Only** for a list of ports currently in use. Please note that a Firewall Allow rule will need to be added for remote access via **Network**→**Firewall**→**Port Allow/Forwarding Rules**→**Service Access Rules**.

**Use CISCO APH:** Select **Yes** to enable the CISCO APH, or **No** to prevent its use.

**Recommended Setting:** When connecting to a Cisco console port, choose **Yes**.

**Use Local Binding:** Select **Yes** to enable Local Binding.

**Recommended Setting:** 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.

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 and any characters > x'7F are dropped.

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.

**Recommended Setting:** Basic + drop LF/NUL is a commonly utilized setting.

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.

## VRRP (Virtual Router Redundancy Protocol)

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

The VRRP menu item allows you to configure the capability of providing redundancy capabilities to each other as well as other third party devices.

Click on the VRRP menu item and the following dialog window appears:



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

The screenshot shows a web-based configuration window titled "Add VRRP Table". It contains the following fields and controls:

- Enable VRRP:** A dropdown menu with "Yes" selected.
- Interface:** A dropdown menu with "eth0" selected.
- Use Virtual MAC Address:** A dropdown menu with "No" selected.
- IP Address:** A text input field with a red "Required" label to its right.
- Group ID:** A text input field with a red "Required" label to its right.
- Priority:** A text input field.
- Peer Notification Interval (seconds):** A text input field.
- Finish:** A blue button at the bottom right.

**Enable VRRP:** Specify whether you want to enable the VRRP service on **this** device. The service will be started after clicking Apply, and on each subsequent boot.

**Recommended Setting:** VRRP is designed to work with multiple systems. Enable only if you intend to setup other VRRP partners.

**Interface:** Specify the interface the VRRP service should use for communication.

**Use Virtual MAC Address:** Specify whether you want to allow the VRRP service to use virtual MAC addresses with the shared IP. If set to No, the actual interface MAC will be used.

**Recommended Setting:**

**No** – If you are using managed switches between the devices, the virtual MAC will confuse the loop detection. Many VRRP control packets will be dropped and status will bounce.

**Yes** – If you are not using managed switches, this mode will allow remote devices to reconnect faster to the backup unit in the event of an outage. This is because local ARP tables will not need to expire and reacquire different MAC addresses for the shared IP.

**IP Address:** Specify the IP address of the virtual server.

**Recommended Setting:** 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:** Specify the ID number of the virtual server. **(Required)**

**Recommended Setting:** 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. **(Required)**

**Note:** If this is the master device, the priority should be set to a higher number than the backup device. (255 is highest priority).

**Peer Notification Interval (seconds):** Specify the amount of time, in seconds, between VRRP broadcast packets. **(Required)**

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.

## Expert Mode

The Expert Mode menu allows you to edit the configuration fields of the DA50N directly. This option provides the ability to perform advanced configuration capabilities for complex organizations.

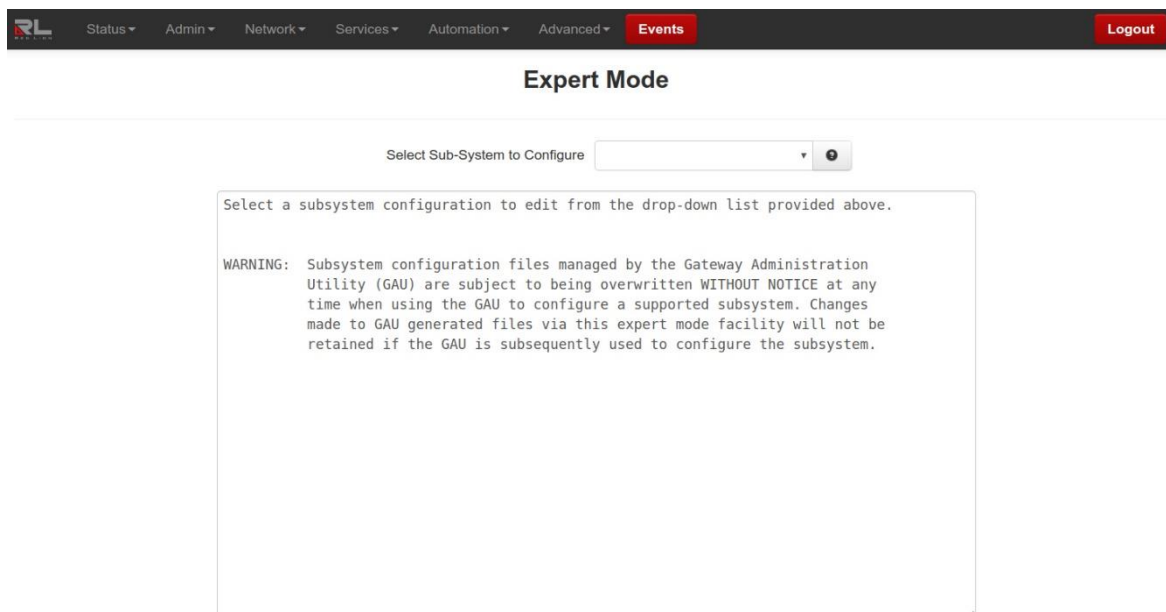
**Note:** Expert Mode is not recommended unless directed by Red Lion Technical Support.

**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 DA50N. It is not recommended that you perform configuration activities using this facility unless instructed to do so by Red Lion Technical Support.

Click on the *Configure Sub-System* menu item and the following window appears:



**Select Sub-System to Configure:** Select a component sub-system from the list.

Your choice will load the given sub-system's configuration file into the text box for editing.

The following controls (buttons) are available:

**Cancel:** Reload the file in the text box, removing all unsaved changes.

**Default:** Load a default file in to the text box for editing. All changes to the defaults file will be reflected in the “real” (rather than the default) configuration file.

**Save:** Save the contents of the text box in to the “real” sub-system configuration file.

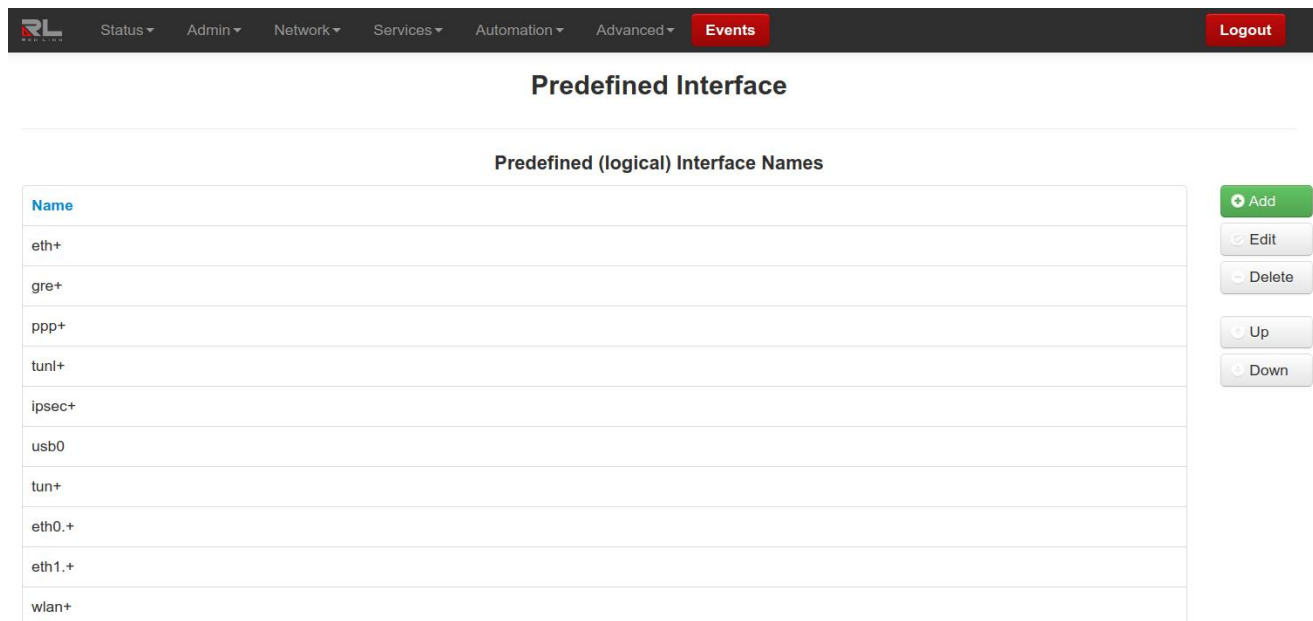
**Stop:** Stop the component sub-system service, if it is currently running.

**Start:** Start the component sub-system service, or re-start it if it is currently running. Some may need a Stop first.

## Predefined Interface Names

The Predefined Interface Names menu item allows you to create a named interface for use in applications such as OpenVPN that require a logical interface, i.e. tun0 that the Red Lion does not know about. Using the Predefined Interface Name will place the name of the interface into the pull-down menus of interface selections to be used by the system.

Click on the *Predefined Interface Names* menu item and the following dialog window appears:



Click on the *Add* button to add a named interface and the following pop-up window appears:



**Enter (logical) Interface Name:** Enter a name to be used for the logical interface. **(Required)**

Click on the *Finish* button to populate the Predefined Interface Names screen.

Click *Save* to store the settings for the next reboot. Selecting *Refresh*, will reset all fields to the previously saved defaults.

## GWLNX

The GWLNX menu item is used to define the following sub-menus: Connect Table Configuration, Install Configuration, Install Application, IP Destinations, CLI Status, GWLNX Status and GWLNX Log.

### Connect Table Configuration

The Connect Table Configuration menu item is used to configure the communication ports behavior via Serial or Modem using Dialed Number Identification Service (DNIS) method.

Click on the *Connect Table Configuration* menu item and the following dialog window appears:

### Connect Table Configuration

**Generic:** Please use the recommended setting unless directed to change by Technical Support personnel.

**Recommended Setting:** No.

**File Mode:** Please use the recommended setting unless directed to change by Technical Support personnel.

**Recommended Setting:** DTMF.

### Connect Table Properties

To create a table setting, click on the Add button and the following dialog window appears:

**Label:** 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-xxxx, 1-888, 1-866 and similar numbers.)

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. It should also match the GWLNX TCP Server port number, if using a dynamic TCP Listening port.

**Recommended Setting:** Recommended Setting is 1001 for this mode.

**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. If choosing a User Defined option, enter the full AT command.

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

**Recommended Setting:** Direct 1200 Bell212 = AT&Q6+MS=B212

**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 a support technician.

**Recommended Setting:** ANSWER\_2WAY\_RAW

**Message Mode:** This will choose between enabling the local Visa protocol engine or allowing Passthru/Transparent mode.

**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.

**Recommended Setting:** Transparent.

**Timer:**

**Transparent Mode:** This 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:** Unused.

**Recommended Setting:**

150 - Transactions

10 - Some Streaming Protocols (ATM Management Protocols)

#### Data Mode:

**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.

**Recommended Setting:**

**Transparent Mode:** As needed for various serial devices and TCP hosts.

**Visa Mode:** Leave this setting at 8N1. Automatic 7E1 detection is used.

#### Spoof ENQ:

**Transparency 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.

**Recommended Setting:** No.

#### No Rx Before Tx:

**Transparency 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.

**Recommended Setting:** No.

#### Disable Ack:

**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.

**Recommended Setting:** No.

#### Pass Through Ack:

**Transparent Mode:** Unused.

**Visa Mode:** When an ACK is received from an ATM/POS device, pass that up to the host processor.

**Recommended Setting:** No, unless using a SmartConnect device at the host processing side.

Click the *Next* button and the following menu items appear:

**Enter IP Address 1:** 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:** 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.

**Recommended Setting:** Recommended value for this mode is 1000.

**Enter IP Address 2:** This is a Client First Alternative IP address that GWLNX uses to connect to the Host Server. (Not Required)

**Enter Port 2:** This is a Client First Alternative Port address that GWLNX uses to connect to the Host Server Port. (Not Required)

**Enter IP Address 3:** This is a Client Second Alternative IP address that GWLNX uses to connect to the Host Server. (Not Required)

**Enter Port 3:** This is a Client Second Alternative Port address that GWLNX uses to connect to the Host Server Port. (Not Required)

**Host Message Format:** Following are the host message formats in supported Message Mode:

**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

After Visa processing and validation, the format sent to the host will be:

**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.

**Recommended Setting:** Default.

**Header Type:** The TCP connection to a host may require length headers. This will optionally be prepended to the data received from the serial side, for either Transparent or Visa Mode.

**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 Host Message Format set to STX-Payload-ETX, and 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).

**Recommended Setting:** Default.

**Allow Early Connect:** Only adjust this option if directed by a support technician.

**Recommended Setting:** Yes.

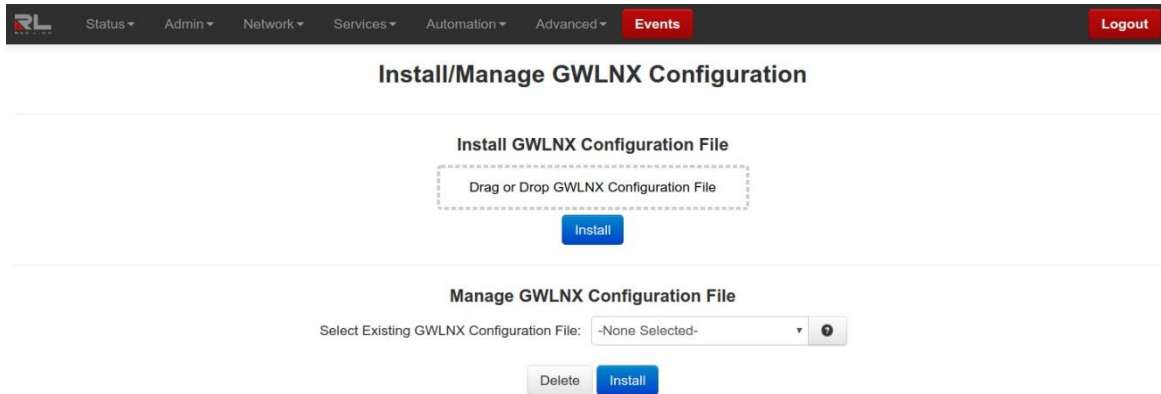
Click on the *Finish* button and you will be directed to the Connect Table dialog window and the Connect Table Properties table will be populated with the entered data.

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 DA50N. The Manage Configuration section is used to install or delete GWLNX configuration files that already reside on the DA50N.

Click on the Install Configuration menu item and the following dialog window appears:



Install GWLNX Configuration File:

**Select GWLNX Configuration File:** Click the 'Drag or Drop GWLNX' box to select a GWLNX configuration file to upload from your local system. You can also drag and drop a file into this box for uploading. It is recommended that you do not upload new files unless directed by Red Lion Technical Support.

Manage GWLNX Configuration File:

**Select Existing GWLNX Configuration File:** Select a GWLNX configuration file on the remote unit to install or to delete. **(Required)**

**WARNING:** Deleting the 'unit.cfg' file may result in the GWLNX application from not running on the next restart.

**Recommended Setting:** Do not install or delete files unless directed by Technical Support staff.

## Install Application

The Install Application menu item is used to install a new GWLNX application on the DA50N.

Click on the *Install Application* menu item and the following dialog window appears:



Click on the upload box or drag and drop your GWLNX installation file on the file upload box to select a GWLNX zip file to upload from your local system. It is recommended that you do not upload files unless directed to do so by Red Lion Technical Support.

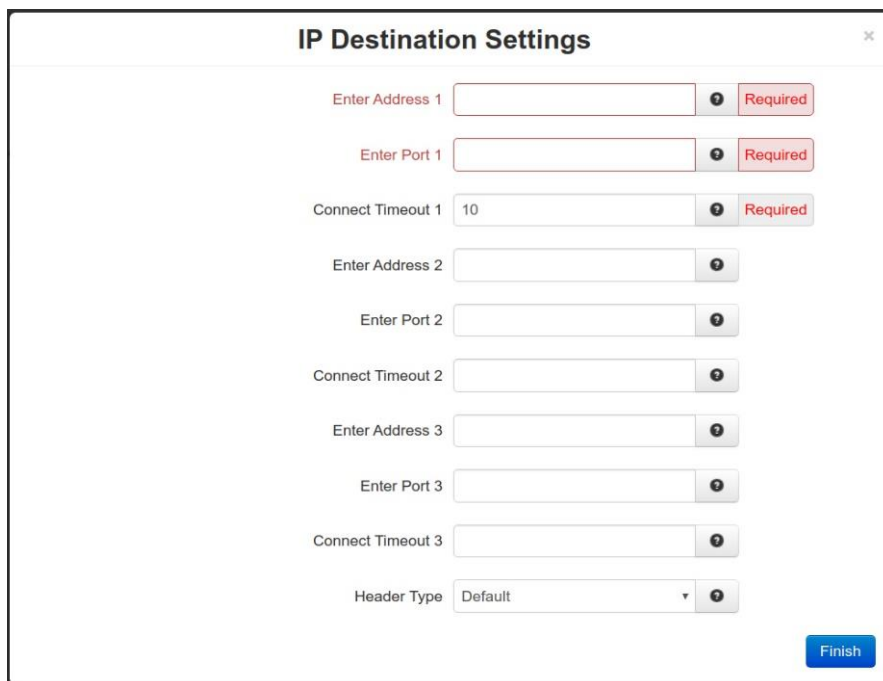
## IP Destinations

The IP Destinations menu item is used to configure the host processor (Server) IP/Port Addresses that GWLNX application uses for TCP/IP communication protocol.

Click on the *IP Destinations* menu item and the following dialog window appears:



Click on the *Add* button to define IP Destination Settings.



**Enter Address 1:** This is a Client Primary IP address that GWLNX uses to connect to the Host Server. (Required)

**Enter Port 1:** This is a Client Primary Port address that GWLNX uses to connect to the Host Server Port. (Required)

**Connect Timeout 1:** 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.

**Recommended Setting:** 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. (Not Required)

**Enter Port 2:** This is a Client First Alternative Port address that GWLNX uses to connect to the Host Server Port. (Not Required)



**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.

**Recommended Setting:** 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. (Not Required)

**Enter Port 3:** This is a Client Second Alternative Port address that GWLNX uses to connect to the Host Server Port. (Not Required)

**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.

**Recommended Setting:** 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.

**Recommended Setting:** Default.

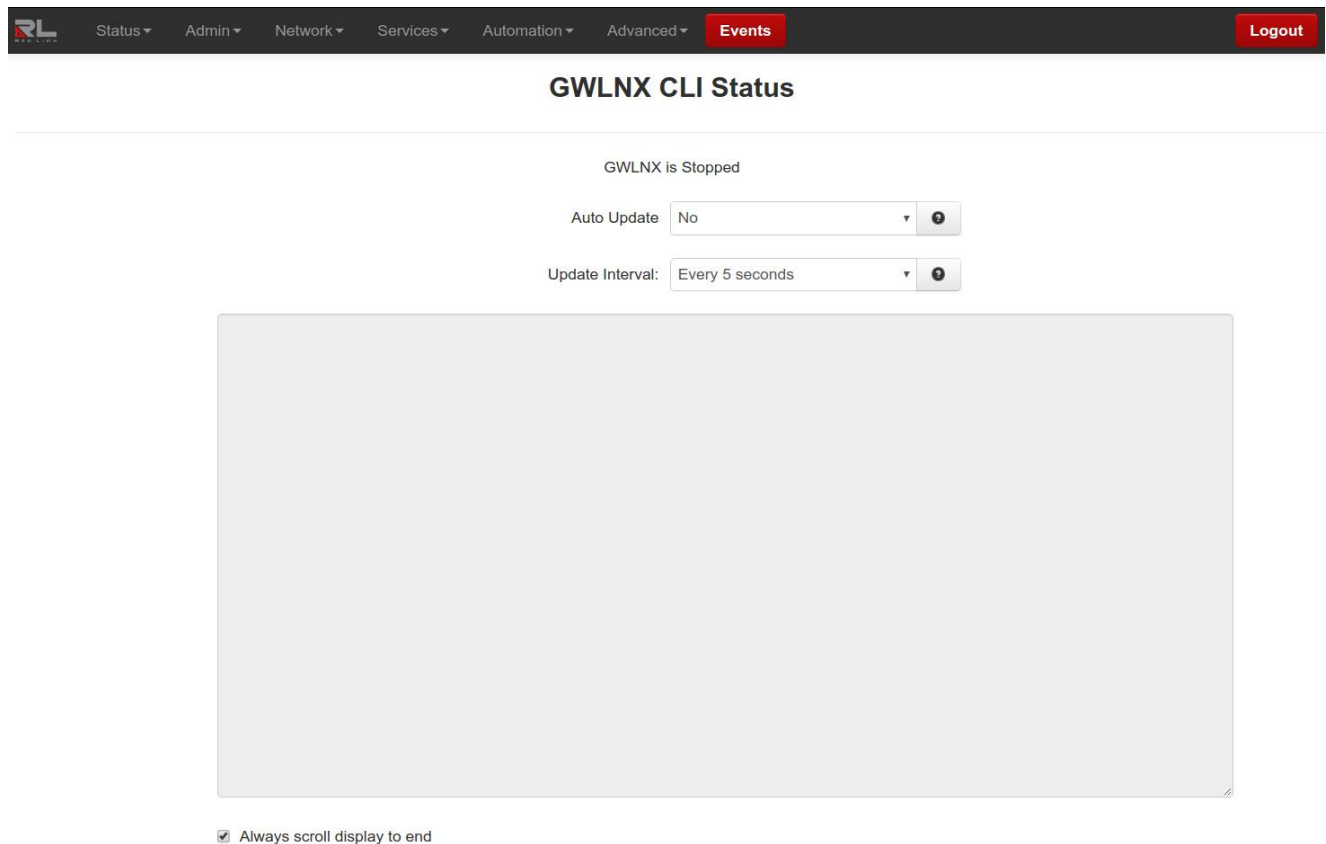
Click on the Finish button and you will be directed to the IP Destinations dialog window and the IP Destinations Table Properties will be populated with the entered data.

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 Refresh button.

## CLI Status

The CLI Status menu item is used to view the status of the ports defined in the GWLNX configuration file if the GWLNX application is running.

Click on the *CLI Status* menu item and the following dialog window appears.



**Auto Update:** Select **Yes** to enable automatic updating of the log file display, the update interval can be selected using the **Select Update Interval** provided immediately below this control. Manual updating is disabled while auto update is in effect. The current filter and maximum lines to be displayed will be used.

**Recommended Setting:** 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

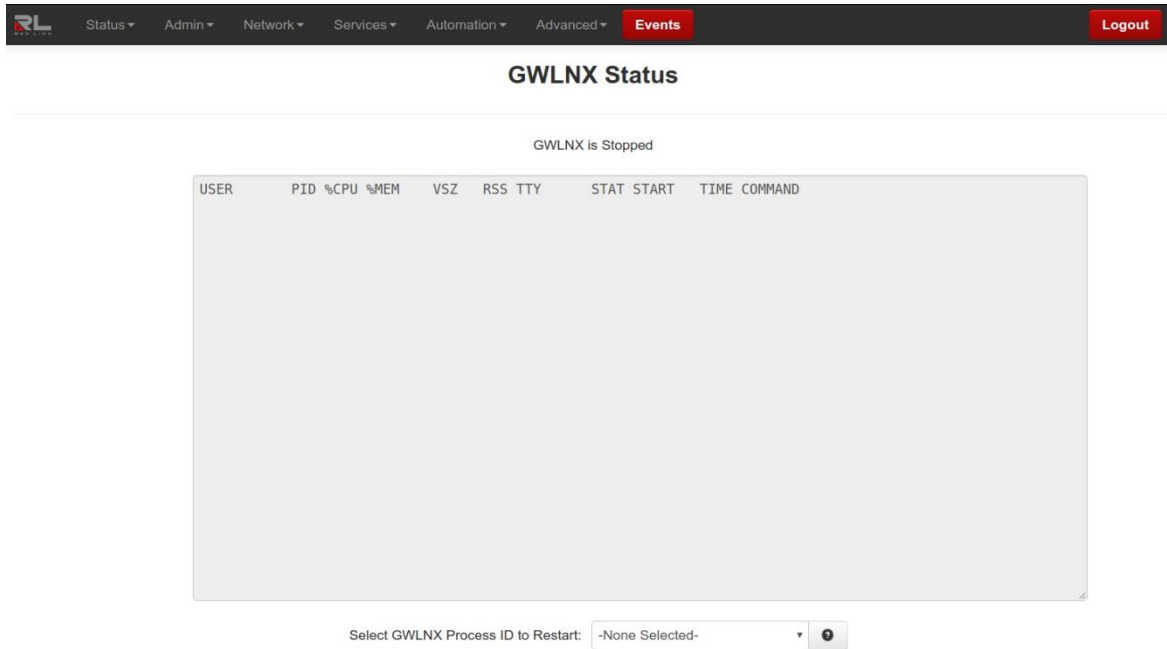
**Recommended Setting:** Be advised that when connected via a Cellular interface, the log file data collected will count towards your total data plan usage.

To refresh the screen, click the *Refresh* button.

### GWLNX Status

The GWLNX Status menu item is used to view the GWLNX process ID and has the ability to restart the application by selecting the process ID from the provided drop-down list. The Refresh button will refresh the process ID, if the GWNLX application has been restarted.

Click on the *GWLNX Status* menu item and the following dialog window appears.



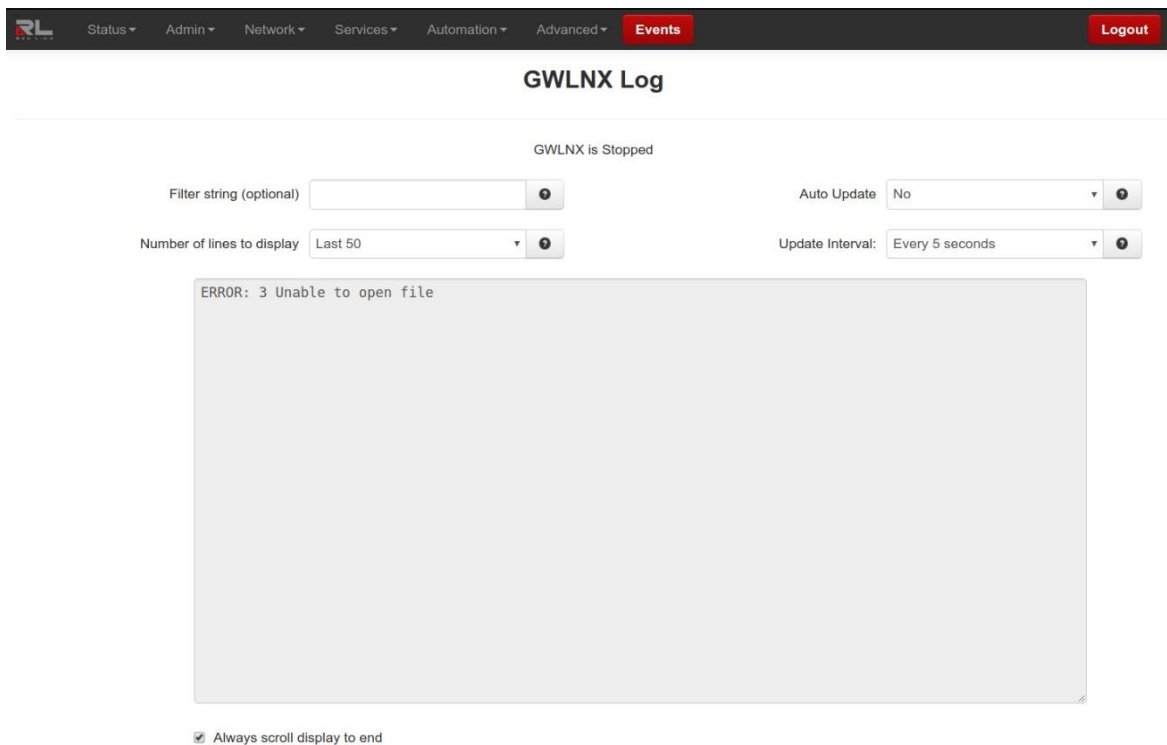
**Select GWLNX Process ID to Restart:** Select the GWLNX Process ID (PID) that you would like to restart.

Click on the *Restart* Button. This will restart the unit.

### GWLNX Log

The GWLNX Log menu item is used to view the logfile generated by GWLNX at startup, which provides the state of each port controller defined in the GWLNX configuration file and logs the Send/Receive traffics for each configured port controller.

Click on the *GWLNX Log* menu item.



**Filter string (optional):** Enter a filter string in the space provided, only lines containing the filter value(s) will be displayed via a 'grep' style filter mechanism.

**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

**Recommended Setting:** 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.

**Recommended Setting:** 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:

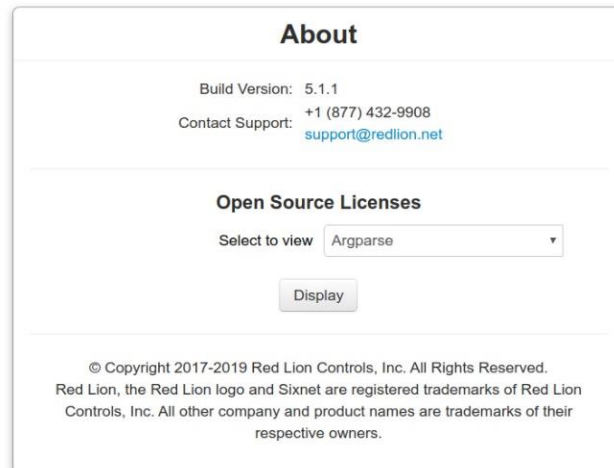
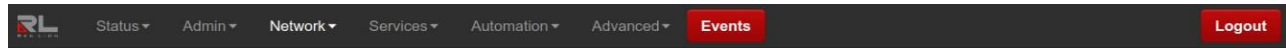
5  
15  
30  
60

**Recommended Setting:** 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.

## About

The About menu provides information on the build version, contact support, and open source licenses.



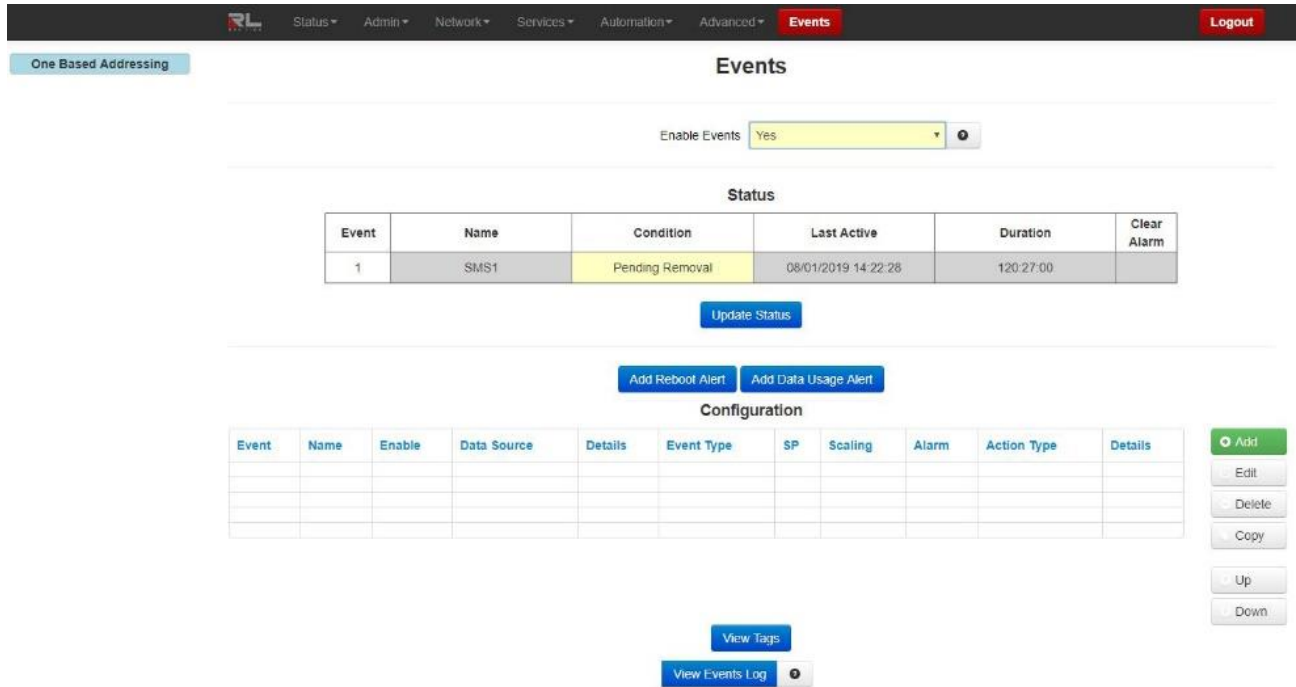
## Events

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 IO DB. For example, events can be configured to watch these values and trigger actions based on when a reboot occurs (system uptime < 2 minutes), when a cellular link is down (wwan0 connected = 0), or when data traffic measured over a month exceeds a user's threshold.

**Note:** Not all models have the same Events capabilities. Please call Red Lion Technical Support or your local representative for more details.



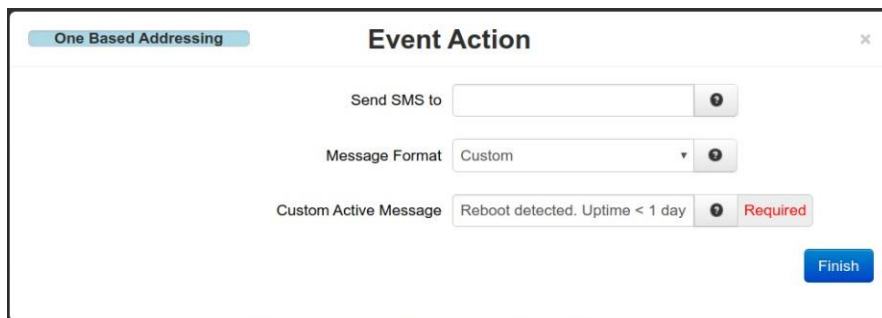
**Enable Events:** Select whether you want to enable the Events Control service. If you select No, all events will be disabled.

#### 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:

**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  
0114185551212

**Email Message:** Enter an email address for the email message destination. Multiple email addresses may be entered by separating them with a **comma**.

**Note:** The email will come **From** the address configured in Services→Email Client.

**Example:**

username@email.com  
username@email.com,usergroup@email.com

**Message Format:** Define what type of content the Event alert message will contain.

**Standard:** Send only the standard informational message.

**Custom:** Send only the custom message as specified. Tag values may be inserted as a variable by declaring the Tag Name framed in \$. ie: \$TAGNAME\$.

**Standard + Custom:** Append up to a 60 character custom message to the standard message.

The Standard message will be constructed as follows:

EVT<NUM>:<Name><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 IO DB. 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:

100000000000

010000000000

001100000000

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

**Custom Active Message:**

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

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

**Add Data Usage Alert**

Click 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.

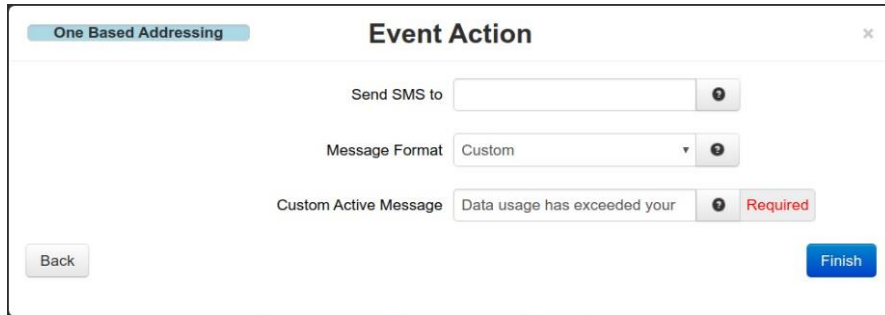
**Time Interval:** Select how often an alert is desired. The options are each month or each day.

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:**

**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

0114185551212

**Email Message:** Enter an email address for the email message destination. Multiple email addresses may be entered by separating them with a **comma**.

**Note:** The email will come **From** the address configured in Services→Email Client.

**Example:**

username@email.com

username@email.com,usergroup@email.com

**Message Format:** Define what type of content the Event alert message will contain.

**Standard:** Send only the standard informational message.

**Custom:** Send only the custom message as specified. Tag values may be inserted as a variable by declaring the Tag Name framed in **\$**. ie: **\$TAGNAME\$**.

**Standard + Custom:** Append up to a 60 character custom message to the standard message.

The Standard message will be constructed as follows:

EVT<Num>:<Name><Cond><Custom>Duration:<Time>DS:<DSValue><Clear Condition>

**Where:**

<Num> is the event number.

<Name> is the event name.

<Cond> is the current event condition or status, ACTIVE or INACTIVE.

<Custom> is the optional custom message specified by the user.

<Time> is the amount of time that the event has been active.

<DSValue> is the value of the Data Source that caused the event to activate or deactivate.

<Clear Condition> will indicate if the event “Will Auto Clear” on its own or if a “Manual Clear Required”.



**Note:** Manual Clearing can be accomplished by clicking the Clear button on the Event Status page, or by writing a "1" into the Clear Condition register defined in IODB. See Appendix B. The Data Source value will change depending on the type of Data Source configured for each event. When an Event Expression is used, a series of bits will indicated the True/False status of terms in the Event Expression. For example, if you had an expression like:

Evt1 | Evt2 | (Evt3 & Evt4)

You could get a message that would trigger with:

100000000000

010000000000

001100000000

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

**Custom Active Message (Required):**

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

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

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

Configuration

**Configuration**

Event	Name	Enable	Data Source	Details	Event Type	SP	Scaling	Alarm	Action Type	Details

+ Add

Edit

Delete

Copy

Up

Down

View Tags

View Events Log ?

Click on the Add button and the Event Configuration dialog window appears:

One Based Addressing

### Event Source

Event Name  ? Required

Enable Event Yes v ?

Data Source IODB v ?

Tag Name

Local Type Register Type v

Local Address Register Address 0:00000

Data Format 16-bit v ?

Data Signed Signed v ?

Next

**Event Name:** Enter a descriptive name in this field to aid in identifying 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. **(Required)**

**Enable Event:** This controls whether the event will be evaluated at runtime or not. You may disable an event 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 an equation form. By combining multiple events, you can create complex actions based on multiple independent conditions.

**Note:** Menu items below Data Source are selection dependent.

**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** Choose whether to treat the data as an unsigned integer or two's compliment signed value.

**Event Expression:** If Event Condition is selected in the Data Source field, the Event Expression field appears.

The **Event Expression** is a logical equation built to combine the condition/status of multiple events into a single action. Other events will be referenced by their Event Name. Tag names can be used within expressions by framing the Tag name in **\$**. ie: **\$TagName\$**. These operands will evaluate those event's condition/status to be a 0 (false/inactive) or 1 (true/active).

There are 4 logical test operations that can be performed on the operands: Once the desired information has been selected, click on the NEXT button and the next dialog window appears:

**NOT:** Represented by the ! (exclamation) symbol.

**AND:** Represented by the & (ampersand) symbol.

**OR:** Represented by the | (pipe) symbol.

**EQU:** Represented by the = (equals) symbol.

Examples:

EVT1 & EVT2 | EVT3 & !EVT4

!EVT1 & !( EVT2 || ( EVT3 & EVT4 ) ) | EVT5

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

!\$TAG1\$ & !( \$TAG2\$ || ( \$TAG3\$ & \$TAG4\$ ) ) | \$TAG5\$

EVT1 & MyEvent | \$TAGNAME\$  
\$TAG1\$ & \$TAG2\$ | \$TAG3\$ & !\$TAG4\$  
where **EVT1**, **EVT2**, **EVT3**, **EVT4**, **EVT5** and **MyEvent** represents the event name and **\$TAG1\$**, **\$TAG2\$**, **\$TAG3\$**, **\$TAG4\$**, **\$TAG5\$** and **\$TAGNAME\$** represents the I/O type register address.

Rules:

"!" only takes effect for the operand or the total result of the pair of parenthesis at its right hand side

"=" shall be between only two operands. Another "=" following is not allowed

EVT1 == EVT2 == EVT3, shall be written as EVT1 = EVT2 & (EVT2 = EVT3)

Operations are evaluated from left to right, unless parenthesis takes higher priority

Maximum level of cascaded parenthesis is 3

Maximum named event operands is 16

"!=" is not allowed. Instead, use: EVT1 = !EVT2 or !EVT1 = EVT2

Click on the *Next* button.

**Event Type:** An event is true when:

**Data Match:** The value of the register is equal to the alarm value.

**Data Mismatch:** The value of the register is not equal to the alarm value.

The following are only available if your data source is a non-discrete IOB register.

**Absolute High:** The value of the register exceeds the alarms value.

**Absolute Low:** The value of the register falls below the alarms value.

**Deviation High:** The value of the register exceeds the setpoint by an amount equal to or greater than the alarms value.

**Deviation Low:** The value of the register falls below the setpoint by an amount equal to or greater than the alarms value.

**Out of Band:** The value of the register moves outside a band, equal in width to twice the alarms value and centered on the setpoint.

**In Band:** The value of the register moves inside a band, equal in width to twice the alarms value and centered on the setpoint.

**Rate of Change:** The value of the register changes within given Time Window by the specified amount of Change Limit.

**Scaling:** Transform an input register from one range of values to another range.

**Bit Operations:** Transform a set of DI/DO values between bit locations of an AI/AO register.

**Calculations:** Perform basic math functions between registers.

**Event Evaluation:** This field will determine which state of the expression evaluation is used to perform an action.

**True:** The Event will be triggered when the expression evaluation is True  
**False:** The Event will be triggered when the expression evaluation is False.

**Activation Delay (in sec):** 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** mode will allow an event condition to clear itself to an inactive state when the input meets conditions configured.

**Manual** mode will require 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):** **Deactivation Delay** is also used to prevent an event from oscillating between the on and off states when the process is near the alarm value.

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.

**Default:** 0 to disable.

To move on to the next screen, click on the *Next* button.



**Action Type:** Select the desired Action Type for the event.

**None:** No action, log the event only.

**Send SMS Message:** Send an SMS message to a single recipient. Use multiple Events to notify more than one contact.

**Write IODB Value:** Write to a known IODB register.

**Run Command:** Run a Command Script that performs an Action.

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

**Send SMS/Email (Action Type)**

**Recipient (Required):**

**SMS Message:** Enter a single phone number for the text message destination. Leading access numbers and area codes may be required based on your carrier, location, account type, and roaming status. Dashes and periods will be ignored. Example: 1-202-555-1212 OR 0114185551212

**Email Message:** Enter an email address for the email message destination. Multiple email addresses may be entered by separating them with a comma. The email will come From the

address configured in Services→Email Client. Example: username@email.com OR  
username@email.com,usergroup@email.com

**Message Format:** Define what type of content the Event alert message will contain.

**Standard:** Send only the standard informational message.

**Custom:** Send only the custom message as specified. Tag values may be inserted as a variable by declaring the Tag Name framed in \$. ie: \$TAGNAME\$.

**Standard + Custom:** Append up to a 60 character Custom message to the standard message.

The Standard Message will be constructed as follows:

EVT<Num>:<Name><Cond><Custom>Duration:<Time>DS:<DSValue><Clear Condition>

Where

<Num> is the event number

<Name> is the event name.

<Cond> is the current event condition or status, ACTIVE or INACTIVE.

<Custom> is the optional custom message specified by the user.

<Time> is the amount of time that the event has been active.

<DSValue> is the value of the Data Source that caused the event to activate or deactivate.

<Clear Condition> will indicate if the event "Will Auto Clear" on its own or if a "Manual Clear Required".

**Note:** Manual Clearing can be accomplished by clicking the Clear button on the Event Status page, or by writing a "1" into the Clear Condition register defined in IODB. See Appendix B.

The Data Source value will change depending on the type of Data Source configured for each event. When an Event Expression is used, a series of bits will indicate 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:

100000000000

010000000000

001100000000

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

#### **Custom Active Message (Required):**

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

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

#### **Custom Inactive Message (Required):**

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

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

**Edge Triggering:** Select the desired setting for this field.

**Neither:** Executes the action based on any edge triggering options.

**Rising Only:** Executes the action only on transition of the event becoming true (active).

**Falling Only:** Executes the action only on transition of the event becoming false (inactive).

**Both:** Executes the action on any transition between true and false.

**Level Triggering:** Selecting Yes the action to execute as often as specified in the periodic action while the event remains true. Choosing NO indicates level will not be considered when evaluating the Event condition.

### Write IODB (Action Type)

**Periodic Action (in sec):** Specifying a non-zero number will cause the action to repeat every period of the number of seconds.

**Tag Name:** This field will auto-populate when the user starts to type a tag name. Tag names are managed in Automation→Tags.

**Write Type:** The WriteType will auto-populate based on the Tag Name entered. These settings are pulled from the Tags dialog window located in Automation→Tags. The Write Type may also be entered manually if no Tag has been defined for this Type: Address.

**Write Address:** The Local Address will auto-populate based on the Tag Name entered. These settings are pulled from the Tags dialog window located in Automation→Tags. The Write Address may also be entered manually if no Tag has been defined for this Type: Address.

**Value to Write:** Choose what to write into the IODB register.

**Data Source:** Writes the input of the event.

**Event Condition:** Writes a 1 = TRUE or 0 = FALSE for this event condition.

**Fixed Value:** Writes a constant fixed number to that entry, when true.

**Counter:** Increments the value in the IODB location by one.

**Run Command Script:** Choose the name of the command script to be executed when the Event is True.

**None:** Standard operation with no special behaviors.

**Rotate Data Logs:** Rotate running data logs.

**Create Data Log Entry:** Create new data log entry

**Restart IPsec:** Restart the IPsec service. i.e. Bring the IPsec tunnel down, then reestablish the tunnel.

**Stop IPsec:** Stop the IPsec service and do not reestablish the tunnel.

**Restart Modbus:** Reserved for future use.

**Reboot:** Reboot the entire device.

**Restart Serial IP:** Restart the serial IP service.

**Reset Wireless:** Restart the Cellular Module.

### SVM Alert Message (Action Type)

**Alert Level:** Select an Alert Level for the message that appears in SixView Manager. These correspond to Syslog levels, where 0 is most critical and 7 is informational.

Click on the *Finish* button. You will be returned to the Events dialog window and the Configuration table will be populated with the entered data.

To delete an existing event, select it in the table and click on the *Delete* button. To edit an existing event, select it in the table and click on the *Edit* button. To move events in the table, use the Up and Down buttons. You can also duplicate an existing Event by clicking on the Copy button.



To view existing Tags, click on the View Tags button. This will bring you to the Tags dialog window found in the Automation menu. From this screen, you can add, edit or delete tags. See section 3.6.3 for more information.

Click on the View Events Log button to view the status of each event configured on your device.

Each line consists of 7 fields that are comma separated.

Each line of events include:

- Date/Time

- Event Number
- Event Name (“N/A” if no name)
- Event Condition/Status (1/0)
- Event Condition/Status (Active/Inactive)
- Event Data Source Value (0 at initial time)
- Description (optional)

Click *Save* to store the settings for the next reboot, or click *Apply* for the settings to take effect immediately. Selecting *Revert/Refresh*, will reset or refresh all fields to previously saved defaults.





# Appendix A

## RED-LION-RAM.MIB Contents

Refers to: 3.5.10 SNMP Agent: RED-LION-DA50N.MIB Contents.

**Note:** The DA50N 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 firmware version of the DA50N. Some manufacturers allow for more information to be retrieved from the module/aircard than others.		
unitDescription	DISPLAYSTRING	DA50N Model Name.
unitSerialNumber	DISPLAYSTRING	Serial Number (e.g. 123456789012).
unitFirmwareVersion	DISPLAYSTRING	Firmware Version Number (e.g. 4.25.84.47).
unitName	DISPLAYSTRING	Unit Name (e.g. DA50N-0647e3 or User Preferred Name via GUI Access Settings)
<b>CELLULAR</b>		
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 Id entity, number used by the GSM network to identify valid devices. Cellular Intl Mobile Equipment Identifier
nai	DISPLAYSTRING	Network Access Identifier, a standard way of identifying users who request access to a network. Cellular Network Access Identifier.
sipUser	INTEGER	Session Initiation Protocol, used to establish sessions between multiple parties in a location-independent manner. Typically voice sessions. Cellular Session Initiation Protocol User.
sid	INTEGER	System ID, a unique 5-digit number assigned to each carrier by the FCC. Cellular System ID.
nid	INTEGER	Network ID, used to divide SIDs into smaller areas. Cellular Network Identifier.
Prl	INTEGER	Preferred Roaming List, a list of information that resides in the memory of the module/aircard. It lists the radio frequencies the module/aircard can use in various geographic areas.

		<p>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.</p> <p>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.</p> <p>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.</p> <p>Cellular Preferred Roaming List.</p>
activated	INTEGER	<p>Determines if the module/aircard is authorized onto the carrier's network. Values are Unknown (-1), No(0), Yes (1).</p> <p>Cellular module activation status.</p>
omaSupported	INTEGER	<p>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:</p> <p>Provisioning - Configuration of the device (including first time use), enabling and disabling features</p> <p>Configuration of Device - Allow changes to settings and parameters of the device</p> <p>Software Upgrades - Provide for new software and/or bug fixes to be loaded on the device, including applications and system software.</p> <p>Fault Management - Report errors from the device, query about status of device.</p> <p>Values are Unknown(-1), No(0), Yes (1)</p> <p>Cellular OMA Supported status.</p>
currentMipProfile	INTEGER	Cellular Mobile IP Profile.
esn	DISPLAYSTRING	Electronic Serial Number, is a permanent identification number used to recognize mobile devices accessing particular telecommunications networks.

		The ESN is assigned and embedded into a wireless communications device by the device's manufacturer. Cellular Module Electronic Serial Number.
pesn	DISPLAYSTRING	Pseudo ESN, a reversed ESN manufacturer code 128, which allow legacy equipment to recognize MEIDs. Cellular Module Pseudo ESN.
meid	DISPLAYSTRING	Mobile Equipment Identifier, 56 bits long, and like ESN's, identify the manufacturer of a mobile device as well as the serial number assigned to the device by that manufacturer Cellular Mobile Equipment Identifier.
vendor	DISPLAYSTRING	Manufacturer of the module/aircard. Cellular Module manufacturer.
modelName	DISPLAYSTRING	The vendor-provided model name of the modem/card/module (e.g. sierra598U).
fwVersion	DISPLAYSTRING	Firmware version of the module/aircard. Cellular Module Firmware version #.
hwVersion	DISPLAYSTRING	Hardware version of the module/aircard. Cellular Module hardware version #.
carrier	DISPLAYSTRING	Service provider for cellular network. Cellular Service Provider.
lowRssi	INTEGER	Low Speed Received Signal Strength Indication. Cellular High Speed received signal strength indication.
lowEcio	INTEGER	Ec/Io is a ratio of good to bad energy, representing the cell towers "cleanness" in its signal to you. In other words - signal to noise ratio. Cellular Low Speed EC/IO.
highRssi	INTEGER	High Speed Received Signal Strength Indication. Cellular High Speed received signal strength indication.
highEcio	INTEGER	Ec/Io is a ratio of good to bad energy, representing the cell towers "cleanness" in its signal to you. In other words - signal to noise ratio. Cellular High Speed EC/IO.
currentRssi	INTEGER	Current Received Signal Strength Indication. Cellular Current Received Signal Strength Indication.
currentEcio	INTEGER	Ec/Io is a ratio of good to bad energy, representing the cell towers "cleanness" in its signal to you. In other words - signal to noise ratio.

		Cellular Current EC/IO.
svcType	DISPLAYSTRING	GSM, which stands for Global System for Mobile communications, reigns as the world's most widely used cell phone technology. CDMA, or Code Division Multiple Access, uses a "spread-spectrum" technique whereby electromagnetic energy is spread to allow for a signal with a wider bandwidth. This allows multiple people on multiple cell phones to be "multiplexed" over the same channel to share a bandwidth of frequencies. Cellular Service Type.
currentChannel	INTEGER	Channels are used to different frequency range network to operate on the same frequency in the same area that do not interfere with each other. Cellular Channel.
cdmaType	DISPLAYSTRING	None, Analog, Digital - High Data Rate type normally digital. Cellular CDMA Type (e.g. None, Analog, Digital).
hdrType	DISPLAYSTRING	Unknown, None, Rev0, RevA - The CDMA/EV-DO sub type. Cellular HDR (e.g. Unknown, None, Rev0, RevA).
cdmaRoaming	DISPLAYSTRING	Home, Roaming, Roaming - unknown. Roaming type indicator inside or outside the providers home network. Cellular Roaming indicator - CDMA.
hdrRoaming	DISPLAYSTRING	None, Roaming - SIDS Guaranteed, Roaming - SIDS Not Guaranteed. EVDO Roaming state. Cellular Roaming indicator - EVDO.
roaming	INTEGER	0 or 1. 0 = currently not roaming, 1 = currently roaming. Cellular current roaming status.
currentState	INTEGER	Connecting, Dormant, Connected, Disconnected, Error, CallIncoming. Current Modem State. Cellular state (e.g. connecting, dormant, connected, disconnected, error, call incoming).
speedPref	DISPLAYSTRING	Automatic, CDMAonly, EVDOonly. What speed preference the modem is currently set to lock to. Cellular Module speed pref.
roamPref	DISPLAYSTRING	HomeOnly, HomePreferred - AUTO, RoamOnly, Aonly, Bonly, AutoA, AutoB, unknown. The current setting for the modem's network roaming preference. Cellular Module roaming pref.

devName	DISPLAYSTRING	The device name as presented by the operating system (e.g. /dev/ttyUSB0).
ifName	DISPLAYSTRING	The cellular interface name, if known, as presented by the operating system (e.g. ppp0).
txCount	INTEGER	Current Wireless PPP RX byte count since connection has been up, updated every 30 minutes. Cellular Module TX Byte Count, updated every 30 mins.
rxCount	INTEGER	Current Wireless PPP RX byte count since connection has been up, updated every 30 minutes. Cellular Module RX Byte Count, updated every 30 mins.
gprsState	DISPLAYSTRING	The "state" of the GSM connection: idle, ready, standby. Cellular GPRS State.
rxLevel	DISPLAYSTRING	The signal level seen at the receiver measured in -dBm. Cellular RX Level.
servingCell	DISPLAYSTRING	The Current Cell on which the device is camped. Cellular Serving Cell.
rccState	DISPLAYSTRING	Radio Resources Control State (also called Packet Data Transfer state): idle, CELL_DCH, CELL_FACH, CELL_PCH, and URA_PCH Cellular RCC State.
gsmChannel	DISPLAYSTRING	Indicates which GSM channel or band of frequencies the device is currently connected to. Cellular GSM Channel.
psState	DISPLAYSTRING	Pulls CELLMODEM_PS_STATE from /var/log/wireless.cardstats Cellular PS State.
mode	DISPLAYSTRING	Pulls CELLMODEM_MODE from /var/log/wireless.cardstats Cellular Mode.
temperature	DISPLAYSTRING	Pulls CELLMODEM_TEMPERATURE from /var/log/wireless.cardstats Cellular Module Temp (not available on all modules).
simContextApn0	DISPLAYSTRING	Pulls CELLMODEM_SIM_CONT_APNO from /var/log/wireless.cardstats Cellular SIM APN 0.
simContextApn1	DISPLAYSTRING	Pulls CELLMODEM_SIM_CONT_APN1 from /var/log/wireless.cardstats Cellular SIM APN 1.
simStatus	DISPLAYSTRING	Pulls CELLMODEM_SIM_STATUS from /var/log/wireless.cardstats Cellular SIM Status.

serviceDomain	DISPLAYSTRING	Pulls CELLMODEM_SERVICE_DOMAIN from /var/log/wireless.cardstats Cellular Service Domain.
availServiceType	DISPLAYSTRING	Pulls CELLMODEM_AVAIL_SERVICE_TYPE from /var/log/wireless.cardstats Cellular Available Service Type.
wCdmaL1State	DISPLAYSTRING	Pulls CELLMODEM_WCDMA_L1_STATE from /var/log/wireless.cardstats Cellular WCDMA L1 State.
mmcsState	DISPLAYSTRING	Pulls CELLMODEM_MM_CS_STATE from /var/log/wireless.cardstats Cellular MM CS State.
gmmPsState	DISPLAYSTRING	Pulls CELLMODEM_GMM_PS_STATE from /var/log/wireless.cardstats Cellular GMM PS State.
wCdmaChannel	DISPLAYSTRING	Pulls CELLMODEM_WCDMA_CHANNEL from /var/log/wireless.cardstats Cellular WCDMA Channel.
wCdmaBand	DISPLAYSTRING	Pulls CELLMODEM_WCDMA_BAND from /var/log/wireless.cardstats Cellular WCDMA Band.
systemMode	DISPLAYSTRING	Pulls CELLMODEM_SYSTEM_MODE from /var/log/wireless.cardstats Cellular System Mode.
powerOnTime	DISPLAYSTRING	Pulls CELLMODEM_POWERON_TIME from /var/log/wireless.cardstats Cellular Power On Time.
lowSpeedCsq	DISPLAYSTRING	Pulls CELLMODEM_LOWSPEED_CSQ from /var/log/wireless.cardstats Cellular Low Speed CSQ.
highSpeedCsq	DISPLAYSTRING	Pulls CELLMODEM_HIGHSPEED_CSQ from /var/log/wireless.cardstats Cellular High Speed CSQ.
band	DISPLAYSTRING	Pulls CELLMODEM_BAND from /var/log/wireless.cardstats Cellular Band.
imei	DISPLAYSTRING	Pulls CELLMODEM_IMEI from /var/log/wireless.cardstats Cellular IMEI.
simId	DISPLAYSTRING	Pulls CELLMODEM_SIM_ID from /var/log/wireless.cardstats Cellular SIM ID.
carrPLMN	DISPLAYSTRING	Carrier PLMN
rxLevelC0	DISPLAYSTRING	Receive Level C0
rxLevelC1	DISPLAYSTRING	Receive Level C1
locAreaCode	DISPLAYSTRING	Location Area Code

IteBand	DISPLAYSTRING	LTE Band
IteRxChan	DISPLAYSTRING	LTE Receive Channel
IteTxChan	DISPLAYSTRING	LTE Transmit Channel
IteBW	DISPLAYSTRING	LTE Bandwidth
IteRSRPint	DISPLAYSTRING	LTE Reference Signal Received Power
IteRSRQint	DISPLAYSTRING	LTE Reference Signal Received Quality
IteTracAreaCode	DISPLAYSTRING	LTE Trac Area Code
creg	DISPLAYSTRING	Cellmodem CREG Not registered, Searching
cellularUpTime	DISPLAYSTRING	Cellular Up Time in Seconds
IteRSRP	INTEGER	LTE Reference Signal Received Power in Integer
IteRSRQ	INTEGER	LTE Reference Signal Received Quality in Integer
IteSINRint	INTEGER	LTE Signal to Interference Plus Noise Ratio in Integer
<b>trafficppp0</b>		
todayRxPpp0	DISPLAYSTRING	Vnstat Today RX for PPP0 Interface
todayTxPpp0	DISPLAYSTRING	Vnstat Today Tx for PPP0 Interface
todayTotalPpp0	DISPLAYSTRING	Vnstat Today Total Rx/Tx for PPP0 Interface
yesterdayRxPpp0	DISPLAYSTRING	Vnstat Yesterday Rx for PPP0 Interface
yesterdayTxPpp0	DISPLAYSTRING	Vnstat Yesterday Tx for PPP0 Interface
yesterdayTotalPpp0	DISPLAYSTRING	Vnstat Yesterday Total Rx/Tx for PPP0 Interface
CurrMonthRxPpp0	DISPLAYSTRING	Vnstat Current Month Rx for PPP0 Interface
CurrMonthTxPpp0	DISPLAYSTRING	Vnstat Current Month Tx for PPP0 Interface
CurrMonthTotalPpp0	DISPLAYSTRING	Vnstat Current Month Total Rx/Tx for PPP0 Interface
PreMonthRxPpp0	DISPLAYSTRING	Vnstat Previous Month Rx for PPP0 Interface
PreMonthTxPpp0	DISPLAYSTRING	Vnstat Previous Month Tx for PPP0 Interface
PreMonthTotalPpp0	DISPLAYSTRING	Vnstat Previous Month Total Rx/Tx for PPP0 Interface
todayRxPpp0Kib	INTEGER	Vnstat Today Rx for PPP0 Interface in Kib
todayTxPpp0Kib	INTEGER	Vnstat Today Tx for PPP0 Interface in Kib
todayTotalPpp0Kib	INTEGER	Vnstat Today Total Rx/Tx for PPP0 Interface in Kib

yesterdayRxPpp0Kib	INTEGER	Vnstat Yesterday Rx for PPP0 Interface in Kib
yesterdayTxPpp0Kib	INTEGER	Vnstat Yesterday Tx for PPP0 Interface in Kib
yesterdayTotalPpp0Kib	INTEGER	Vnstat Yesterday Total Rx/Tx for PPP0 Interface in Kib
CurrMonthRxPpp0Kib	INTEGER	Vnstat Current Month Rx for PPP0 Interface in Kib
CurrMonthTxPpp0Kib	INTEGER	Vnstat Current Month Tx for PPP0 Interface in Kib
CurrMonthTotalPpp0Kib	INTEGER	Vnstat Current Month Total Rx/Tx for PPP0 Interface in Kib
PreMonthRxPpp0Kib	INTEGER	Vnstat Previous Month Rx for PPP0 Interface in Kib
PreMonthTxPpp0Kib	INTEGER	Vnstat Previous Month Tx for PPP0 Interface in Kib
PreMonthTotalPpp0Kib	INTEGER	Vnstat Previous Month Total Rx/Tx for PPP0 Interface in Kib
<b>trafficwwan0</b>		
todayRxWwan0	DISPLAYSTRING	Vnstat Today Rx for WWAN0 Interface
todayTxWwan0	DISPLAYSTRING	Vnstat Today Tx for WWAN0 Interface
todayTotalWwan0	DISPLAYSTRING	Vnstat Today Total Rx/Tx for WWAN0 Interface
yesterdayRxWwan0	DISPLAYSTRING	Vnstat Yesterday Rx for WWAN0 Interface
yesterdayTxWwan0	DISPLAYSTRING	Vnstat Yesterday Tx for WWAN0 Interface
yesterdayTotalWwan0	DISPLAYSTRING	Vnstat Yesterday Total Rx/Tx for WWAN0 Interface
CurrMonthRxWwan0	DISPLAYSTRING	Vnstat Current Month Rx for WWAN0 Interface
CurrMonthTxWwan0	DISPLAYSTRING	Vnstat Current Month Tx for WWAN0 Interface
CurrMonthTotalWwan0	DISPLAYSTRING	Vnstat Current Month Total Rx/Tx for WWAN0 Interface
PreMonthRxWwan0	DISPLAYSTRING	Vnstat Previous Month Rx for WWAN0 Interface
PreMonthTxWwan0	DISPLAYSTRING	Vnstat Previous Month Tx for WWAN0 Interface
PreMonthTotalWwan0	DISPLAYSTRING	Vnstat Previous Month Total Rx/Tx for WWAN0 Interface
todayRxWwan0Kib	INTEGER	Vnstat Today Rx for WWAN0 Interface in Kib
todayTxWwan0Kib	INTEGER	Vnstat Today Tx for WWAN0 Interface in Kib



todayTotalWwan0Kib	INTEGER	Vnstat Today Total Rx/Tx for WWAN0 Interface in Kib
yesterdayRxWwan0Kib	INTEGER	Vnstat Yesterday Rx for WWAN0 Interface in Kib
yesterdayTxWwan0Kib	INTEGER	Vnstat Yesterday Tx for WWAN0 Interface in Kib
yesterdayTotalWwan0Kib	INTEGER	Vnstat Yesterday Total Rx/Tx for WWAN0 Interface in Kib
CurrMonthRxWwan0Kib	INTEGER	Vnstat Current Month Rx for WWAN0 Interface in Kib
CurrMonthTxWwan0Kib	INTEGER	Vnstat Current Month Tx for WWAN0 Interface in Kib
CurrMonthTotalWwan0Kib	INTEGER	Vnstat Current Month Total Rx/Tx for WWAN0 Interface in Kib
PreMonthRxWwan0Kib	INTEGER	Vnstat Previous Month Rx for WWAN0 Interface in Kib
PreMonthTxWwan0Kib	INTEGER	Vnstat Previous Month Tx for WWAN0 Interface in Kib
PreMonthTotalWwan0Kib	INTEGER	Vnstat Previous Month Total Rx/Tx for WWAN0 Interface in Kib
<b>trafficeth0</b>		
todayRxEth0	DISPLAYSTRING	Vnstat Today Rx for Eth0 Interface
todayTxEth0	DISPLAYSTRING	Vnstat Today Tx for Eth0 Interface
todayTotalEth0	DISPLAYSTRING	Vnstat Today Total Rx/Tx for Eth0 Interface
yesterdayRxEth0	DISPLAYSTRING	Vnstat Yesterday Rx for Eth0 Interface
yesterdayTxEth0	DISPLAYSTRING	Vnstat Yesterday Tx for Eth0 Interface
yesterdayTotalEth0	DISPLAYSTRING	Vnstat Yesterday Total Rx/Tx for Eth0 Interface
CurrMonthRxEth0	DISPLAYSTRING	Vnstat Current Month Rx for Eth0 Interface
CurrMonthTxEth0	DISPLAYSTRING	Vnstat Current Month Tx for Eth0 Interface
CurrMonthTotalEth0	DISPLAYSTRING	Vnstat Current Month Total Rx/Tx for Eth0 Interface
PreMonthRxEth0	DISPLAYSTRING	Vnstat Previous Month Rx for Eth0 Interface
PreMonthTxEth0	DISPLAYSTRING	Vnstat Previous Month Tx for Eth0 Interface
PreMonthTotalEth0	DISPLAYSTRING	Vnstat Previous Month Total Rx/Tx for Eth0 Interface
todayRxEth0Kib	INTEGER	Vnstat Today Rx for ETH0 Interface in Kib
todayTxEth0Kib	INTEGER	Vnstat Today Tx for ETH0 Interface in Kib

todayTotalEth0Kib	INTEGER	Vnstat Today Total Rx/Tx for ETH0 Interface in Kib
yesterdayRxEth0Kib	INTEGER	Vnstat Yesterday Rx for ETH0 Interface in Kib
yesterdayTxEth0Kib	INTEGER	Vnstat Yesterday Tx for ETH0 Interface in Kib
yesterdayTotalEth0Kib	INTEGER	Vnstat Yesterday Total Rx/Tx for ETH0 Interface in Kib
CurrMonthRxEth0Kib	INTEGER	Vnstat Current Month Rx for ETH0 Interface in Kib
CurrMonthTxEth0Kib	INTEGER	Vnstat Current Month Tx for ETH0 Interface in Kib
CurrMonthTotalEth0Kib	INTEGER	Vnstat Current Month Total Rx/Tx for ETH0 Interface in Kib
PreMonthRxEth0Kib	INTEGER	Vnstat Previous Month Rx for ETH0 Interface in Kib
PreMonthTxEth0Kib	INTEGER	Vnstat Previous Month Tx for ETH0 Interface in Kib
PreMonthTotalEth0Kib	INTEGER	Vnstat Previous Month Total Rx/Tx for ETH0 Interface in Kib
<b>traffice1</b>		
todayRxEth1	DISPLAYSTRING	Vnstat Today Rx for Eth1 Interface
todayTxEth1	DISPLAYSTRING	Vnstat Today Tx for Eth1 Interface
todayTotalEth1	DISPLAYSTRING	Vnstat Today Total Rx/Tx for Eth1 Interface
yesterdayRxEth1	DISPLAYSTRING	Vnstat Yesterday Rx for Eth1 Interface
yesterdayTxEth1	DISPLAYSTRING	Vnstat Yesterday Tx for Eth1 Interface
yesterdayTotalEth1	DISPLAYSTRING	Vnstat Yesterday Total Rx/Tx for Eth1 Interface
CurrMonthRxEth1	DISPLAYSTRING	Vnstat Current Month Rx for Eth1 Interface
CurrMonthTxEth1	DISPLAYSTRING	Vnstat Current Month Tx for Eth1 Interface
CurrMonthTotalEth1	DISPLAYSTRING	Vnstat Current Month Total Rx/Tx for Eth1 Interface
PreMonthRxEth1	DISPLAYSTRING	Vnstat Previous Month Rx for Eth1 Interface
PreMonthTxEth1	DISPLAYSTRING	Vnstat Previous Month Tx for Eth1 Interface
PreMonthTotalEth1	DISPLAYSTRING	Vnstat Previous Month Total Rx/Tx for Eth1 Interface
todayRxEth1Kib	INTEGER	Vnstat Today Rx for ETH1 Interface in Kib
todayTxEth1Kib	INTEGER	Vnstat Today Tx for ETH1 Interface in Kib

todayTotalEth1Kib	INTEGER	Vnstat Today Total Rx/Tx for ETH1 Interface in Kib
yesterdayRxEth1Kib	INTEGER	Vnstat Yesterday Rx for ETH1 Interface in Kib
yesterdayTxEth1Kib	INTEGER	Vnstat Yesterday Tx for ETH1 Interface in Kib
yesterdayTotalEth1Kib	INTEGER	Vnstat Yesterday Total Rx/Tx for ETH1 Interface in Kib
CurrMonthRxEth1Kib	INTEGER	Vnstat Current Month Rx for ETH1 Interface in Kib
CurrMonthTxEth1Kib	INTEGER	Vnstat Current Month Tx for ETH1 Interface in Kib
CurrMonthTotalEth1Kib	INTEGER	Vnstat Current Month Total Rx/Tx for ETH1 Interface in Kib
PreMonthRxEth1Kib	INTEGER	Vnstat Previous Month Rx for ETH1 Interface in Kib
PreMonthTxEth1Kib	INTEGER	Vnstat Previous Month Tx for ETH1 Interface in Kib
PreMonthTotalEth1Kib	INTEGER	Vnstat Previous Month Total Rx/Tx for ETH1 Interface in Kib
<b>gpscurrent</b>		
CurrentGpsValid	DISPLAYSTRING	GPS Current Valid Fixed Quality (0 = Invalid, 1 = Valid)
CurrentGpsLat	DISPLAYSTRING	GPS Current Latitude Degrees
CurrentGpsLong	DISPLAYSTRING	GPS Current Longitude Degrees
CurrentGpsAlt	DISPLAYSTRING	GPS Current Altitude Tenths of Meter (280.2 = 2802)
CurrentGpsTimeStamp	DISPLAYSTRING	GPS Current Time Stamp
CurrentGpsNumSat	DISPLAYSTRING	GPS Current Number of Satellites
CurrentGpsFtfromcp	DISPLAYSTRING	GPS Current Feet From Lockdown Center Point
CurrentGpsSpeed	DISPLAYSTRING	GPS Current Speed, SOG tenths of knots (50.1 = 501)
CurrentGpsCourse	DISPLAYSTRING	GPS Current Course, Heading in tenths of degree (280.3 = 2803)
GpsSource	DISPLAYSTRING	GPS Source of Data (1=Internal;3=Fixed)
GpsLockdownState	DISPLAYSTRING	GPS Current Lockdown State (0 = Monitor;5 = Lockdown;7-9 = Violation)
GpsLockdownRadius	DISPLAYSTRING	GPS Current Lockdown Radius (ft), Units in Feet as calculated from centerpoint



# Appendix B

## IODB Status Module

The IODB status module is a set of IODB registers that are reserved for system use to collect device based information and make that information available to be polled by any head end or SCADA server appliances via Modbus based I/O transfers.

These registers are created as Analog OUT registers as not to interfere with any on board I/O or other commonly used register types.

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

Register type is Analog Out and the initial register offset is 1000.

SYSTEM STATUS				
INDEX	NAME	DESCRIPTION	FREQUENCY	NOTES
1001	Serial_Number_UINT16_A	First 4 digits, UINT16	Rare	16 digit field saved as 4, 4-digit numbers
1002	Serial_Number_UINT16_B	Next 4 digits	Rare	
1003	Serial_Number_UINT16_C	Next 4 digits	Rare	
1004	Serial_Number_UNIT16_D	Last 4 digits	Rare	
1005	Serial_Number_UINT64_A	UINT64 format; LSW	Rare	16 digit field saved as a single UNT64, Little Endian, LSB First.
1006	Serial_Number_UINT64_B		Rare	Serial Number = (Reg1005 + (Reg1006 * 2 <sup>16</sup> ) + (Reg1007 * 2 <sup>32</sup> ) + (Reg1008 * 2 <sup>48</sup> ))
1007	Serial_Number_UINT64_C		Rare	
1008	Serial_Number_UINT64_D		Rare	
1009	Model_Number	4 digit model number	Rare	No prefixes or suffixes
1010	Firmware_Version	3 digit number	Rare	425=4.25, 325=3.25
1011	Date_Year	Year, 4 digit number	Rapidly	
1012	Date_Month	Month, 1-12	Rapidly	
1013	Date_Day	Day, 1-31	Rapidly	
1014	Date_DayOfWeek	Day, 1-7	Rapidly	Sunday=0
1015	Date_DayOfYear	DOY, 1-365	Rapidly	
1016	Time_Hour	Hour, 0-23	Rapidly	Current Time

1017	Time_Min	Minute, 0-59	Rapidly	
1018	Time_Second	Second, 0-59	Rapidly	
1019	Uptime_Days	Days, 0-9999	Rapidly	Time since last reboot
1020	Uptime_Hours	Hours, 0-23	Rapidly	
1021	Uptime_Minutes	Minutes, 0-59	Rapidly	
1022	Uptime_Seconds	Seconds, 0-59	Rapidly	
1023	CPU Load	% CPU Load	Quickly	
1061	Onboard_Temp	Onboard-Temp, in C	Often	Units are in Celsius, 3 digits displayed, insert a decimal after the first 2 digits. i.e. 273 is 27.3
1062	Onboard_VIN1	Input Voltage 1, in mV	Often	
1063	Onboard_VIN2	Input Voltage 2, in mV	Often	
1064	Onboard_VBATT	Battery voltage, in mV	Often	
1068	AI_Calibration	Reserved; non-zero during calibration	N/A	A non-zero value indicates user calibration is in progress
1069	AO_Calibration	Reserved; non-zero during calibration	N/A	A non-zero value indicates user calibration is in progress

TRAFFIC -VNStat ENTRIES ARE IN KIB (KILOBYTES)				
INDEX	NAME	DESCRIPTION	FREQUENCY	NOTES
1071	ppp0_TodayRX_A	UINT32; LSW	Sometimes	All UINT32 values should be handled as Unsigned, 32-bit Integers, Little Endian, LSB First.
1072	ppp0_TodayRX_B	UINT32; MSW	Sometimes	Crimson settings would be a Holding Register, Data Type: Word as Long, Manipulation: Reversed, Treat As: Unsigned.
1073	ppp0_TodayTX_A	UINT32; LSW	Sometimes	
1074	ppp0_TodayTX_B	UINT32; MSW	Sometimes	
1075	ppp0_TodayTotal_A	UINT32; LSW	Sometimes	

1076	ppp0_TodayTotal_B	UINT32; MSW	Sometimes	
1077	ppp0_YesterdayRX_A	UINT32; LSW	Sometimes	
1078	ppp0_YesterdayRX_B	UINT32; MSW	Sometimes	
1079	ppp0_YesterdayTX_A	UINT32; LSW	Sometimes	
1080	ppp0_YesterdayTX_B	UINT32; MSW	Sometimes	
1081	ppp0_YesterdayTotal_A	UINT32; LSW	Sometimes	
1082	ppp0_YesterdayTotal_B	UINT32; MSW	Sometimes	
1083	ppp0_ThisMonthRX_A	UINT32; LSW	Sometimes	
1084	ppp0_ThisMonthRX_B	UINT32; MSW	Sometimes	
1085	ppp0_ThisMonthTX_A	UINT32; LSW	Sometimes	
1086	ppp0_ThisMonthTX_B	UINT32; MSW	Sometimes	
1087	ppp0_ThisMonthTotal_A	UINT32; LSW	Sometimes	
1088	ppp0_ThisMonthTotal_B	UINT32; MSW	Sometimes	
1089	ppp0_LastMonthRX_A	UINT32; LSW	Sometimes	
1090	ppp0_LastMonthRX_B	UINT32; MSW	Sometimes	
1091	ppp0_LastMonthTX_A	UINT32; LSW	Sometimes	
1092	ppp0_LastMonthTX_B	UINT32; MSW	Sometimes	
1093	ppp0_LastMonthTotal_A	UINT32; LSW	Sometimes	
1094	ppp0_LastMonthTotal_B	UINT32; MSW	Sometimes	
1095	wwan0_TodayRX_A	UINT32; LSW	Sometimes	
1096	wwan0_TodayRX_B	UINT32; MSW	Sometimes	
1097	wwan0_TodayTX_A	UINT32; LSW	Sometimes	
1098	wwan0_TodayTX_B	UINT32; MSW	Sometimes	
1099	wwan0_TodayTotal_A	UINT32; LSW	Sometimes	
1100	wwan0_TodayTotal_B	UINT32; MSW	Sometimes	
1101	wwan0_YesterdayRX_A	UINT32; LSW	Sometimes	
1102	wwan0_YesterdayRX_B	UINT32; MSW	Sometimes	
1103	wwan0_YesterdayTX_A	UINT32; LSW	Sometimes	
1104	wwan0_YesterdayTX_B	UINT32; MSW	Sometimes	
1105	wwan0_YesterdayTotal_A	UINT32; LSW	Sometimes	
1106	wwan0_YesterdayTotal_B	UINT32; MSW	Sometimes	
1107	wwan0_ThisMonthRX_A	UINT32; LSW	Sometimes	
1108	wwan0_ThisMonthRX_B	UINT32; MSW	Sometimes	
1109	wwan0_ThisMonthTX_A	UINT32; LSW	Sometimes	
1110	wwan0_ThisMonthTX_B	UINT32; MSW	Sometimes	
1111	wwan0_ThisMonthTotal_A	UINT32; LSW	Sometimes	
1112	wwan0_ThisMonthTotal_B	UINT32; MSW	Sometimes	
1113	wwan0_LastMonthRX_A	UINT32; LSW	Sometimes	
1114	wwan0_LastMonthRX_B	UINT32; MSW	Sometimes	

1115	wwan0_LastMonthTX_A	UINT32; LSW	Sometimes	
1116	wwan0_LastMonthTX_B	UINT32; MSW	Sometimes	
1117	wwan0_LastMonthTotal_A	UINT32; LSW	Sometimes	
1118	wwan0_LastMonthTotal_B	UINT32; MSW	Sometimes	



# Appendix C

## SMS Handler Commands

This appendix contains a table of all currently available commands for the SMS handler. The commands are separated into three parts: command, target, and action. Not all commands will use all three. Most commands will have an abbreviated option shown after the forward slash (/):

COMMAND	TARGET	ACTION
Login / log	<password>	
Quit / qui exit / exi		
get / g	gps  wwanip / wwa ethip / eth celldata / cel ipsec / ips openvpn / ope ssh  ramqtt / ram device / dev cmd event / eve	status / sta lat long locate / loc       status / sta active / act all <event name> <event #>
read / r	Tag name  IO Notation (1 - based)	Value  value
write / w	Tag name IO Notation (1 - based)	value value
do / d	celldata / cel ipsec / ips openvpn / ope ssh modbus / mod SVM datalog / dat  cmd event / eve	on,off, or reset on,off, or restart on,off, or restart on,off, or restart on,off, or restart trigger / tri ratate / rot newline / new  <filename>  <event_#> clear / cle <event_name> clear / cle all clear / cle
help / ?	<command>	

