User Guide

VUE™ Series

User Guide

User Guide
For Intuicom VUE Series

Intuicom, Inc.
4909 Nautilus Ct. Ste. 111
Boulder, CO 80301
(303) 449-4330
www.intuicom.com

INTVUE.U.01.1.0.2209

This Document is for internal use by Intuicom employees or by Resellers and Distributors who are authorized and/or licensed to install Intuicom products. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, or for any purpose without the express written permission of Intuicom Inc.

Intuicom reserves the right to make changes to this manual without notice. Unless otherwise agreed to in writing, Intuicom assumes no responsibility or liability for the use of this manual or for the infringement of any copyright or other proprietary right and Intuicom shall deem nothing contained in this manual a warranty or guarantee.

Intuicom® and VUE™ are trademarks or trade names of Intuicom, Inc.

Other product names mentioned in this manual may be copyrights, trademarks, or registered trademarks of their respective companies and are hereby acknowledged.

ATTENTION:

Incorrect termination of supply wires may cause internal damage and will void warranty. To ensure your VUE module enjoys a long life, double check ALL your connections with the user manual before turning the power on.

CAUTION:

To comply with FCC RF Exposure requirement in section 1.1310 of the FCC Rules, antennas used with this device must be installed and provide a separation distance of at least 20 cm from all persons to satisfy RF exposure compliance.
Avoid:

- Operating the transmitter when someone is within 20cm of the antenna
- Operating the transmitter unless all RF connectors are secure and any open connectors are properly terminated
- Operating the equipment near electrical blasting caps or in an explosive atmosphere
- All equipment must be properly grounded for safe operations
- All equipment should be serviced only by a qualified technician

SAFETY Notice:

Exposure to RF energy is an important safety consideration. The FCC has adopted a safety standard for human exposure to radio frequency electromagnetic energy emitted by FCC regulated equipment as a result of its actions in Docket 93-62 and OET Bulletin 65 Edition 97-01.

Avoid

- Operating the transmitter unless all RF connectors are secure and any open connectors are properly terminated

- Operating the equipment near electrical blasting caps or in an explosive atmosphere

  Note: All equipment must be properly grounded for safe operations. All equipment should be serviced only by a qualified technician.

FCC notice

Part 15.19—This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Part 15.21—The grantee is not responsible for any changes or modifications not expressly approved by the party responsible for compliance. Such modifications could void the user's authority to operate the equipment.

Part 15.105(b)—This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Part 90—This device has been type accepted for operation by the FCC in accordance with Part 90 of the FCC rules (47CFR Part 90). See the label on the unit for the specific FCC ID and any other certification designations.

Note: This device should only be connected to PCs that are covered by either a FCC DoC or are FCC certified.

Hazardous Location Notices

This device complies with Directive 2014/34/EU—ATEX Directive Ex nA IIC T4 Gc –40 °C ≤ Ta ≤ +70 °C.

Special conditions

1. This equipment is designed to be installed as a component in an enclosure that meets IP54.
2. This equipment is to be mounted in a vertical orientation to facilitate effective heat dissipation.

WARNING: EXPLOSION HAZARD

Do not disconnect equipment unless power has been switched off or the area is known to be non-hazardous.

This product is suitable for use in Class 1, Division 2, Groups A, B, C and D; Tamb –40° C to +70° C or non-hazardous locations only.

This equipment shall only be installed in locations meeting Pollution degree 2, and shall be installed according to installation category 2. The maximum altitude of the installation is not to exceed 2000m.

This equipment shall be installed in accordance with the requirements specified in Article 820 of the National Electrical Code (NEC), ANSI/NFPA 70-2011. Section 820-40 of the NEC provides guidelines for proper grounding, and in particular specifies that the antenna ground (shield) shall be connected to the grounding system of the building, as close to the point of cable entry as practical.

This equipment shall be installed in a Restricted Access Location (such as a dedicated equipment room or service closet).

1) The Wireless Ethernet module is to be installed by trained personnel or licensed electricians only, and installation must be carried out in accordance with the instructions listed in the Installation Guide and applicable local regulatory codes.
2) The units are intended for Restricted Access Locations.
3) The Wireless Ethernet module is intended to be installed in a final enclosure, rated IP54, before use outdoors.
4) The Equipment shall be powered using an external Listed Power Supply with LPS outputs, or a Class 2 Power Supply.
5) The Wireless Ethernet module must be properly grounded for surge protection

Important Notice
Intuicom products are designed to be used in industrial environments by experienced industrial engineering personnel with adequate knowledge of safety design considerations.

Intuicom radio products are used in communications channels that are subject to noise and interference. The products are designed to operate in the presence of noise and interference, but in an extreme case radio noise and interference can cause product operation delays or operation failure. Like all industrial electronic products, Intuicom products may fail in a variety of modes due to misuse, age, or malfunction. We recommend that users and designers design systems using design techniques intended to prevent personal injury or damage during product operation, and provide failure tolerant systems to prevent personal injury or damage in the event of product failure. Designers must warn users of the equipment or systems if adequate protection against failure has not been included in the system design. Designers must include this important notice in operating procedures and system manuals.

These products should not be used in non-industrial applications, or life-support systems, without consulting Intuicom first.

To avoid accidents during maintenance or adjustment of remotely controlled equipment, all equipment should be first disconnected from the VUE module during these adjustments. Equipment should carry clear markings to indicate remote or automatic operation. For example: “This equipment is remotely controlled and may start without warning. Isolate at the switchboard before attempting adjustments.”

To avoid the risk of electrocution, the serial cables, and all terminals of the VUE module should be electrically protected. To provide maximum surge and lightning protection, the module should be connected to a suitable ground and the serial cables, and the module should be installed as recommended in the VUE Series Installation Guide

The VUE series module is not suitable for use in explosive environments without additional protection.

The VUE Series modules operate proprietary protocols to communicate. Nevertheless, if your system is not adequately secured, third parties may be able to gain access to your data or gain control of your equipment via the radio link. Before deploying a system, make sure that you have carefully considered the security aspects of your installation.

Release Notice
This is the update release of the VUE Wireless I/O and Gateway User Manual version 1.0, which applies to firmware version 2.20. This user manual covers all Intuicom VUE Series models.

Follow Instructions
Read this entire manual and all other publications pertaining to the work to be performed before installing, operating, or servicing this equipment. Practice all plant and safety instructions and precautions. Failure to follow the instructions can cause personal injury and/or property damage.

Proper Use
Any unauthorized modifications to or use of this equipment outside its specified mechanical, electrical, or other operating limits may cause personal injury and/or property damage, including damage to the equipment. Any such unauthorized modifications: (1) constitute “misuse” and/or “negligence” within the meaning of the product warranty, thereby excluding warranty coverage for any resulting damage; and (2) invalidate product certifications or listings.

Product disposal
When your product reaches the end of its useful life, it is important to take care in the disposal of the product to minimize the impact on the environment.

General instructions

The product housing is made of die-cast aluminum (aluminium) and may be recycled through regular metal reclamation operators in your area.

The product circuit board should be disposed according to your country’s regulations for disposing electronics equipment.

Europe
In Europe, you can return the product to the place of purchase to have the product disposed in accordance with EU WEEE legislation.

Deployment of Intuicom products in customer environment
There is increasing concern regarding cybersecurity across industries, where companies are steadily integrating field devices into enterprise-wide information systems. This is why Intuicom has incorporated secure development life cycle in their product development to ensure that cybersecurity is addressed at all levels of development and commissioning of our products.

There is no protection method that is completely secure. Industrial Control Systems continue to be the target for attacks. The complexities of these attacks make it very difficult to have a complete secure system. A defense mechanism that is effective today may not be effective tomorrow as the ways and means of cyber-attacks constantly change. Therefore, it’s critical that our customers remain aware of changes in cybersecurity and continue to work to prevent any potential vulnerability of their products and systems in their environment.

At Intuicom we are focusing on analyzing emerging threats and ensuring that we are developing secure products and helping our customers deploy and maintain our solutions in a secure environment. We continue to evaluate cybersecurity updates that we become aware of and provide the necessary communication on our website as soon as possible.

Intuicom strongly recommends our customers to apply the deployment practices that are outlined in the appendix to this document – “Secure hardening guidelines” on pages 156 – 158.

GNU General public license
Intuicom is using a part of Free Software code under the GNU General Public License in operating the VUE products. This General Public License applies to most of the Free Software Foundation’s code

and to any other program whose authors commit by using it. The Free Software is copyrighted by Free Software Foundation, Inc., and the program is licensed “as is” without warranty of any kind. Users are free to contact Intuicom at the following web address: www.intuicom.com for instructions on how to obtain the source code used for the VUE products.

Contents

I – Introduction 14
A – Overview 14
B – VUE Series Product Versions 15
C – Module Structure 16
II - Installation 19
A – General Information 19
B - Thermal 19
1 – VUE Power Levels and Modulation 19
2 – Thermal Derating Charts 20
C – Power Supply 23
1 – Powering from the SUP(+) and SUP(-) terminals 23
2 – Connecting a Back-up Battery to the BAT+ and GND Terminals 24
3 – Powering Expansion I/O Modules 25
4 – Powering Directly from the BAT+ and GND Terminals 26
5 – Internal I/O 26
6 – Grounding 27
D – Antenna 28
1 – Directional Antennas 29
2 – Antenna Installation Tips 30
E – Bottom Panel Connections 31
1 – Ethernet Port 31
2 – USB Device Port for Configuration 31
3 – RS-232 Port 31
4 – RS-485 Port with Modbus Support 32
III – Getting Started 33
A – Step 1 – Connect an Antenna 33
B – Step 2 – Connect Ethernet Cable 34
C – Step 3 – Connect the Power Supply 34
D – Step 4 – Set the IP Address of the Computer 34
1 – Windows Tip 35
E – Step 5 – Enabling Web Browser Access 37
F – Step 6 – Log Into the VUE 39
III – Configuration Webpages 40
A – Quick Start Settings 40
1 – Security 41
a – Enable Remote Webserver Access 41
2 – Identification 41

a – System Name 41
b – Device Name 41
3 – Wireless Interface 41
a – Networking Mode 41
b – Device Mode 41
c – Encryption Passphrase 42
4 – Radio Setup 42
a – Bandwidth 42
b – Transmit Power Level 42
c – Transmit Frequency 43
d – Receive Frequency 43
5 – Network Settings 43
a – IP Address 43
b – Subnet Mask 44
c – Default Gateway 44
6 – Filter Settings 44
a – First Radio Device IP 44
b – Last Radio Device IP 44
7 – I/O Back-to-Back Configuration 44
8 – Quick Start Additional Information 46
9 – Saving Settings 47
IV – Basic Provisioning 48
A – Quick Start 48
B – Network 48
1 – Identification 49
2 – Wireless Interface 49
3 – Networking Mode 51
C – Radio 54
1 – Basic Radio Setup 54
D – Advanced Radio Configuration 57
1 – Link Management Settings 58
2 – Performance and Contention Settings 58
a – Compression and Statistics Settings 59
3 – Roaming Settings 59
4 – Traffic Control 60
V – Configuration 62
A – Onboard I/O 62
1 – Analog Output Configuration 62
2 – Analog Input Configuration 63
a – Calculating Span 65
b – Calculating Zero 65

3 – Digital Output Configuration 66
4 – Digital Input Configuration 67
5 – Pulsed Output Configuration 67
6 – Thermocouple Settings 68
B – (I/O) Mapping Configuration 69
1 – Enable All Configured Mappings 69
2 – Mappings 69
a – Block Write Mappings 69
b – Gather/Scatter Write Mappings 71
c – Block Read Mappings 73
d – Sensitivity Mappings 75
e – Advanced Configuration 76
C – DNP3 Outstation 77
1 – Global Parameters 78
2 – Advanced 79
3 – DNP3 I/O Configuration 80
a – Binary Inputs and Binary Outputs 81
b – Counter Inputs 82
c – Analog Inputs 83
d – Analog Outputs 84
4 – Modbus TCP 85
5 – Fail Safe Configuration 86
a – Fail Safe Blocks 87
b – Fail Safe Reboot 88
6 – Data and Event Logging Configuration 89
a – Retrieving Logged Data 91
D – Serial 93
1 – RS-232 Serial Port Configuration 93
2 – RS-232 Additional Settings 94
a – Modbus TCP to RTU Gateway 99
b – RS-485 Serial Port Configuration 100
c – RS-485 Additional Settings 101
E – Dashboard 108
1 – Dashboard Configuration 109
F – I/O Plus Logic 114
G – Feature Keys 114
VI – Advanced Networking 115
A – Repeaters 115
B – Roaming 116
C – IP Routing 116
D – Network Filtering 117

E – DHCP Server 119
F – VLAN 120
1 – VLAN Mode 120
2 – Add VLAN Group 121
3 – Interface Membership for VLAN 121
VII – User Management 123
A – Change My Password 123
B – Manage Users 123
1 – To add a user 125
2 – To retire a user 125
3 – To change a user password 125
C – Logout 125
VIII – Network Diagnostics 126
A – Connectivity 126
1 – Connected Wireless Devices 126
2 – Available Access Points 127
B – Channel Suvey 127
C – Custom Survey 128
D – Network Connectivity Diagnostics 129
E – Monitor Radio Communications 129
F – Capture IP Comms 131
IX – Unit Diagnostics 133
A – I/O Diagnostics 133
B – Statistics 134
1 – Interface Statistics 134
2 – Time 135
3 – System Log 135
4 – Routes 135
5 – IP Statistics 136
6 – TCP/UDP Statistics 136
7 – Memory Statistics 136
8 – Serial Statistics 137
B – System Tools 137
1 – Configuration Export 138
2 – Patch File Firmware Upgrade 138
3 – Setting the Date and Time 139
X – Unit Information 142
A – Configuration Summary 142

B – Logs and Archives 142
C – View Dashboard 143
D – Module Information 143
E – Home 144
Appendix A - Specifications 145
Appendix B – LED Function 146
Appendix C – Register Memory Map 149
Appendix D – Expansion I/O Registers 153
Appendix E – Modbus Error Codes 155
Appendix F – Secure Hardening Guidelines 156
Appendix G – Firmware Upgrade 159
Appendix H – Intuicom Support 160
Appendix I - Warranty 161

I – Introduction

A – Overview

The Intuicom VUE Ethernet Networking I/O and Gateway is a multiple I/O node that extends communications to sensors and actuators in local, remote, or difficult to reach locations. Designed to work with wired and wireless devices, the Intuicom VUE is capable of providing IP-based I/O across sprawling industrial environments typical of industrial applications.

The VUE can serve as an end node or network gateway and is scalable to thousands of nodes. Gather-scatter and block mapping technology offers the efficient use of network resources, allowing point-to-point transfer of process signal within complex monitoring and control systems. Integrated Modbus® server capability allows further I/O expansion through the use of VUE expansion modules.

The module can monitor the following types of signals:

- Digital (on/off) signals, such as a contact closure or switch
- Analog (continuously variable) signals, such as tank level, motor speed, or temperature
- Pulsed signal, frequency signals, such as metering, accumulated total, or rainfall
- Internal signals, such as supply voltage, supply failure, or battery status

The modules monitor the input signals and transmit the values by radio or Ethernet cabling to another module (or modules) that have been configured to receive this information. The VUE radio is available in models to support both unlicensed and licensed operation depending on your country.

Input signals that are connected to the module are transmitted and appear as output signals on other modules. A transmission occurs whenever a change of state (COS) occurs on an input signal. A COS of a digital or an internal digital input is a change from “off” to “on,” or a change from “on” to “off.” For an analog input, internal analog input, or pulse input rate, a COS is a configurable value referred to as sensitivity. The default sensitivity is 1000 counts (3%), but you can change this value using the sensitivity block configuration webpage, which is covered later in this manual.

In addition to COS messages, update messages are automatically transmitted on a configurable time basis. These updates ensure system integrity. Pulse inputs counts are accumulated and the total count is transmitted regularly according to the configured update time.

The VUE modules transmit the input/output data using radio or Ethernet. The data frame includes the address of the sending module and the receiving module, so that each transmitted message is acted upon only by the correct receiving unit. Each message includes error checking to ensure that no corruption of the data frame has occurred due to noise or interference. The module with the correct receiving address will acknowledge the message with a return transmission (acknowledgment). If the original module does not receive a correct acknowledgment, it will retry multiple times before setting the communications status of that message to "fail." For critical messages, this status can be reflected on an output on the module for alert purposes. The module will continue to try to establish communications and retry each time an update or COS occurs.

The VUE comes from the factory with WIB, Modbus TCP/RTU and DNP3 protocols as standard. WIB protocol provides powerful enhanced features, including IP addressing and it allows thousands of modules to exist in a system. Modbus TCP and DNP3 protocols provide a standards-based interface to a multitude of commercially available controls systems, including PLCs, DCS, and SCADA.

A system can be a complex network or a simple pair of modules. An easy-to-use configuration procedure allows you to specify any output destination for each input. Each VUE device can have up to 19 VUE expansion I/O modules connected by RS-485 twisted pair cable. Any input signal at any module may be configured to appear at any output on any module in the entire system.

The units can be configured using the web browser utility via Ethernet, remotely over the radio, or USB.

B – VUE Series Product Versions

The chart on the next page is a listing of the different VUE product versions available from Intuicom.

Model Code	Description
VUE-1	VUE Ethernet Modem/Gateway: 148-174MHz, 10mW-5W 140kbps, I/O=(2) DI/O, DNP3 Capable, SMA Antenna Connector
VUE-4	VUE Ethernet Modem/Gateway: 400-480MHz, 10mW-10W 140kbps, I/O=(2) DI/O, DNP3 Capable, SMA Antenna Connector
VUE-1-IO	VUE I/O Gateway Radio: 148-174MHz, 10mW-5W 140kbps, I/O=(8) DI/O + (4) AI + (2) AO + (4) PI/O, DNP3, Modbus RTU/TCP master/slave gateway, SMA Antenna Connector
VUE-4-IO	VUE I/O Gateway Radio: 400-480MHz, 10mW-10W 140kbps, I/O=(8) DI/O + (4) AI + (2) AO + (4) PI/O, DNP3, Modbus RTU/TCP master/slave gateway, SMA Antenna Connector
VUE-9-L1-IO	VUE I/O Gateway Radio: 894-902MHz, 10mW-5W 140kbps, I/O=(8) DI/O + (4) AI + (2) AO + (4) PI/O, DNP3, Modbus RTU/TCP master/slave gateway, SMA Antenna Connector
VUE-9-L2-IO	VUE I/O Gateway Radio: 928-960MHz, 10mW-5W 140kbps, I/O=(8) DI/O + (4) AI + (2) AO + (4) PI/O, DNP3, Modbus RTU/TCP master/slave gateway, SMA Antenna Connector
VUE-9-IO	VUE I/O-Gateway Radio: 900MHz, 1W, FHSS, WIBmesh or WIBnet compatible, I/O = (8)DI/O + (4)AI + (2)AO + (4)PI/O, SMA Antenna Connector
VUE-9-IO2	VUE I/O-Gateway Radio: 900MHz, 1W, FHSS, WIBmesh or WIBnet compatible, I/O = (8)DI/O + (4)AI + (2)AO + (4)PI/O, SMA Antenna Connector
VUE-24-IO	VUE I/O-Gateway Radio: Basic Unit 2.4GHz, 802.11b/g, 200mW, SMA Antenna Connector

C – Module Structure

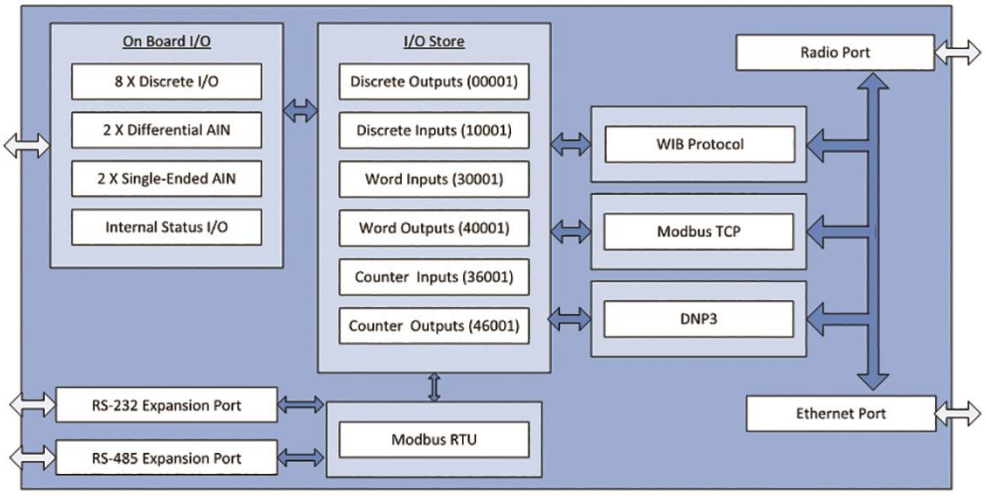
The VUE module is made up of different interface areas with a central input and output storage area (I/O store). The I/O store is an area of memory made available for the status of the physical on-board I/O and internal I/O registers. It also provides services for other processes within the module.

The I/O store is split into eight different block types:

- Two blocks made available for bit data (discrete)
- Two blocks made available for word data (analog)
- Two blocks made available for 32-bit words data (counters)
- Two blocks made available for floating point data (analogs)

Each of these block types in turn support input and output locations that can interface with the physical I/O on the local machine and also be used for data storage when used as a gateway to external devices. These block type locations are illustrated in the figure below and are described in “Register memory map” on page 149 (Appendix C).

There are other registers within the database that can be used for system management.



Module Structure

The radio and Ethernet interfaces (see Figure above) allow the VUE to communicate with other modules within the system using a proprietary protocol called WIB. I/O Messages from other VUE modules are received on the communication ports and then passed to the I/O store which will in turn update the register locations accordingly. The WIB protocol is designed to provide reliable communications suitable for an Ethernet channel or for an open license-free radio channel. It is an extremely efficient protocol for radio communications because the messages are sent using exception reporting (only transmitting when there is a change of an input signal) rather than transmitting all of the time. Update messages can also be configured at a predetermined time for integrity checks.

Each message can be comprised of multiple I/O values, referred to as a “block of I/O.” The messages use error checking and return acknowledgment for greater reliability. Up to four attempts are made when transmitting the message over each hop of the radio path, and if no acknowledgment is received a Comms indication can be flagged.

The on-board I/O includes eight discrete I/O, two single-ended analog inputs, two differential analog inputs, and two current sourcing analog outputs. Each discrete I/O can function as either a discrete input (voltage-free contact input) or discrete output (Transistor output). Each I/O point is linked to separate I/O registers within the I/O data store. The following internal I/O can be accessed from the I/O store.

The inputs can be used to interpret the status of a single module or an entire system:

- **Battery voltage**—The battery terminal voltage, displayed as an analog value.
- **Loop supply**—The +24 Vdc analog loop supply (ALS) used to power analog current loops, displayed as an analog value.
- **Expansion module volts**—The supply voltage of the connected expansion modules, displayed as an analog value.
- **RSSI**—The radio signal level for the selectable address, reported as a dB level.
- **Comms Fail**—A selectable register can indicate a Communications Fail error for a particular message transmission.

The expansion port allows VUE expansion I/O modules to be added to the module. Expansion I/O is dynamically added to the internal I/O of the VUE module by adding an offset to the address.

II - Installation

A – General Information

The VUE Series modules are housed in an aluminum enclosure with DIN rail mounting, providing options for up to 14 I/O points, and separate power and communications connectors. The enclosure measures 6.7” x 5.9” x 1.6” (170 mm x 150 mm x 40 mm), including the connectors. The antenna protrudes from the top.

B - Thermal

The VUE series modules contain a high-power radio that can generate a significant amount of heat.

For effective heat dissipation, the device must be mounted in the vertical orientation, with the antenna connection at the top, and with clearance of at least 25 mm on the right side to allow thermal convection.

When multiple circuits are active at the same time (Expansion I/O, On-Board I/O, Battery Charging, Radio Transmit), and when powered from the “SUP” inputs, the VUE can overheat if it is also operating at the high end of the allowed temperature range. If your radio transmitter will be operating in a high-duty cycle mode (for example a repeater or base-station) you must check the de-rating charts below to ensure the radio will be able to operate continuously at your expected ambient temperature.

You can calculate the expected duty cycle of your device by calculating the expected number of messages and the expected message duration, or you can check the duty cycle once the system is up and running (Network Diagnostics >> Custom Survey >> All Tx Frames).

If the device will be outside its thermal operating limit at the designed duty cycle, you can either reduce the transmit power, or you can power the device from a 13.8V supply through the BAT+ and GND terminals.

1 – VUE Power Levels and Modulation

The charts below show the radio power relative to the maximum radio power for the different VUE models. The maximum radio power depends on the radio modulation mode selected. Refer to the Table below to relate power level, modulation and the power levels on the charts shown on the following pages.

Legacy compatability (FSK)

BandWidth	Data rate	Max Tx Power	Max -2dB	Max -3dB	Max -6dB
12.5kHz, 25kHz	All	40dBm	38dBm	37dBm	34dBm

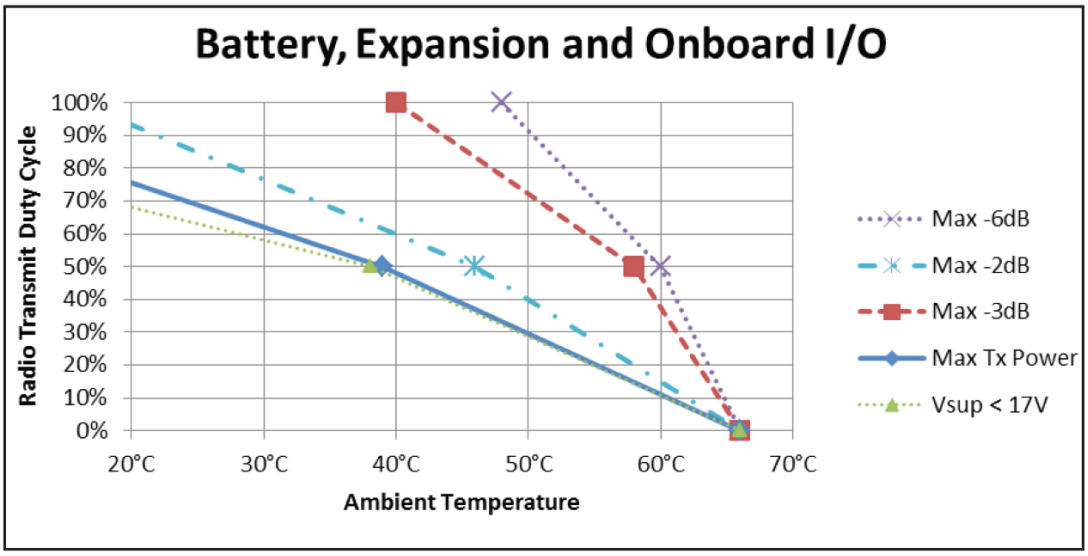
High speed mode (QAM)

BandWidth	Data rate	Max Tx power	Max -2dB	Max -3dB	Max -6dB
6.25kHz	4k,8k	36dBm	34dBm	33dBm	30dBm
	16k,24k	34dBm	32dBm	31dBm	28dBm
12.5kHz	8k,16k	36dBm	34dBm	33dBm	30dBm
	32k,48k	34dBm	32dBm	31dBm	28dBm
6.25kHz	16k,32k	36dBm	34dBm	33dBm	30dBm
	64k,96k	34dBm	32dBm	31dBm	28dBm

Table – Radio Power relative to Maximum Radio Power

2 – Thermal Derating Charts

The following are Derating Charts for the VUE series radios operating from the SUP inputs.



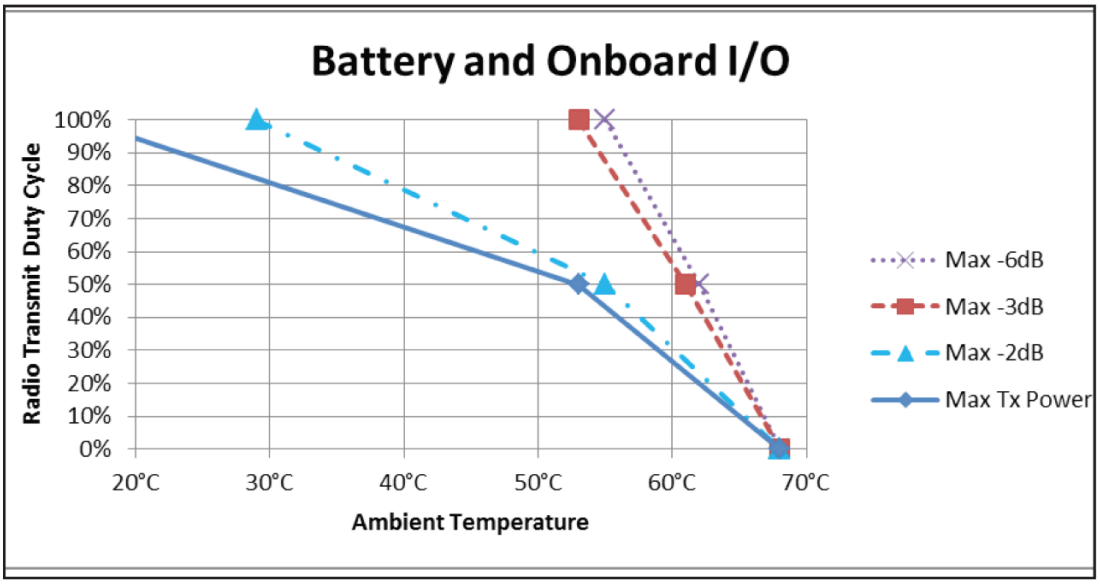
VUE Series – worst case

The worst case occurs when you are using all features of the VUE at maximum.

- Operating from the SUP+ and SUP- inputs
- All On-Board I/O circuits at maximum (analogs at 20mA, digital outputs at 200mA load)

- VUE-EX modules connected to the "Expansion" port operating at maximum rated current (500mA).
- Battery Charging at full rate (SLA battery recharging after extended power outage on BAT+ / GND terminals)
- Use the de-rating chart above to limit the radio power and duty cycle depending on the expected maximum temperature.

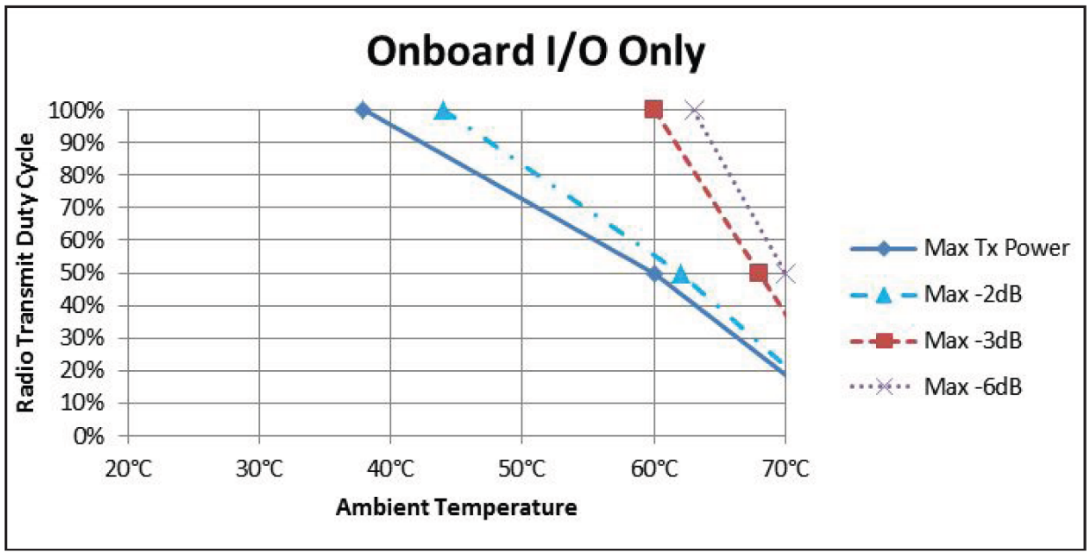
NOTE: When operating from supply voltage 17V or below and at maximum transmit power, you need to apply the additional derating shown.



VUE Series – Battery Charging and onboard I/O

As above, except without VUE-EX Expansion I/O.

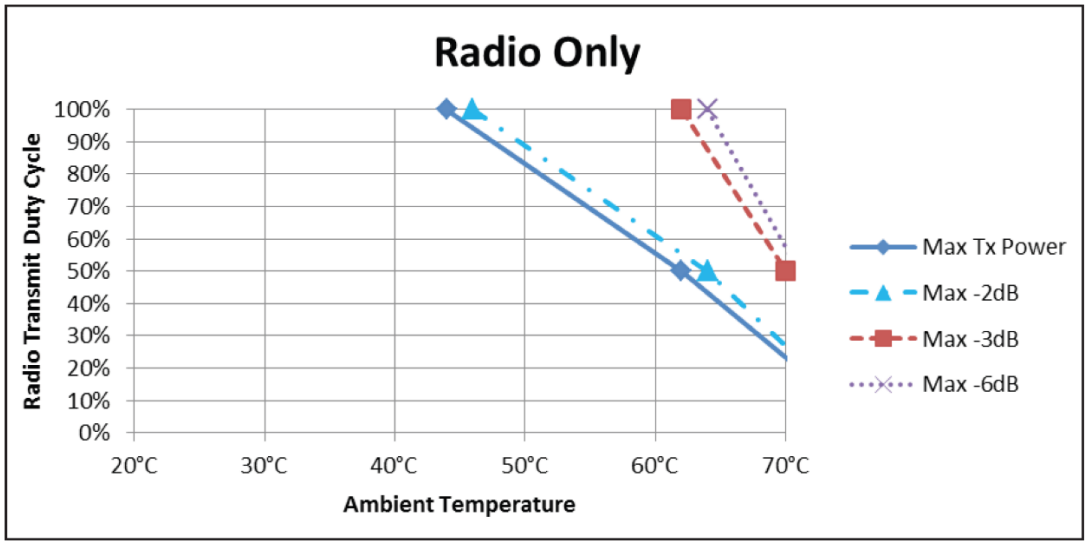
- Operating from the SUP+ and SUP- inputs
- All On-Board I/O circuits at maximum (analogs at 20mA, digital outputs at 200mA load)
- Battery Charging at full rate (SLA battery recharging after extended power outage)
- Use the de-rating chart above to limit the radio power and duty cycle depending on the expected maximum temperature.



VUE Series – onboard I/O Only

Figure "VUE Series – Battery Charging and onboard I/O" shows duty cycle, except without the need to charge an SLA battery.

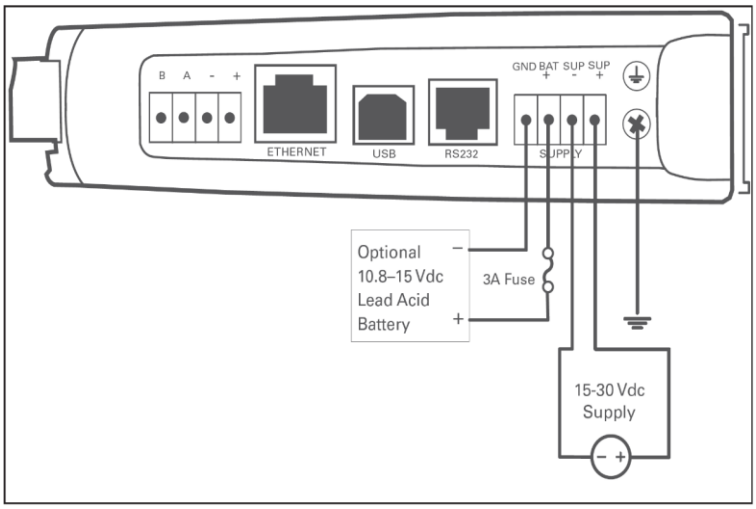
- Operating from the SUP+ and SUP- inputs
- All On-Board I/O circuits at maximum (analogs at 20mA, digital outputs at 200mA load)
- VUE-EX modules connected to the "Expansion" port operating at maximum rated current (500mA).
- Use the de-rating chart above to limit the radio power and duty cycle depending on the expected maximum temperature.



VUE Series – Radio Only

Use the above chart "VUE Series – Radio Only" when operating without active I/O, and without the need to charge an SLA battery.

- Operating from the SUP+ and SUP- inputs
- All On-Board I/O circuits unused
- Use the de-rating chart above to limit the radio power and duty cycle depending on the expected maximum temperature.



Power Supply Connections

C – Power Supply

The VUE Series radios will operate from 15-30Vdc supply (nominal 24Vdc) connected to the SUP+ and SUP- terminals. It will charge a 13.8V sealed lead acid (SLA) battery connected to the BAT+ and GND terminals and run off this battery if the main supply fails.

1 – Powering from the SUP(+) and SUP(-) terminals

The power supply on the SUP+ and SUP– terminals must be able to supply enough current to operate the device, to power all of the I/O circuits connected to the VUE, and to power the device's radio transmitter when it is sending data. A 24 Vdc 2.5 A power is suitable for all configurations, including configurations requiring battery charging and expansion I/O.

If you need to use a supply with a lower power rating; or if you need to power additional equipment in your installation; use these guidelines to determine your required power supply current. Add the relevant elements from table below to determine your power supply current requirement. Remember you also need to

add current for any other equipment being powered from the same power supply, including relays, loop isolators, indicators, etc.

	Supply voltage		
	17 Vdc	**24 Vdc**	**30 Vdc**
Base operating current	180 mA	140 mA	100 mA
Radio transmit current			
10W FSK	2100 mA	1300 mA	1100 mA
5W FSK	1000 mA	650 mA	500 mA
4W QAM	1800 mA	1200 mA	950 mA
Discrete I/O (per active input or output)	11 mA	7 mA	5 mA
Analog inputs and outputs (per 20 mA loop)	55 mA	38 mA	30 mA

Power Supply Current Requirements

2 – Connecting a Back-up Battery to the BAT+ and GND Terminals

You can connect a 13.8 V SLA battery to the BAT+ and GND terminals to provide a backup power source if the main supply fails. While the main supply is present, the battery will charge at up to 0.5 A rate until the battery voltage reaches 14.3 V. The battery charger will then maintain a float charge on the battery at this voltage. To fully charge the SLA battery, the main supply must be at least 17 Vdc.

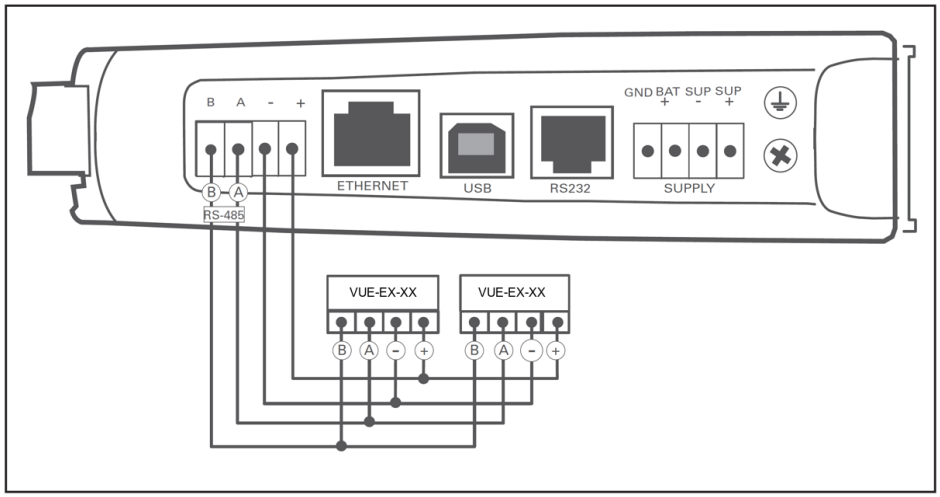
When you connect a backup battery, you need to provide sufficient power to support the additional charge current required when the battery is discharged (when it is recovering from an extended power interruption). The table below shows the additional current from your power supply to support battery charging.

Supply voltage (V_{sup})	**Current required (I_{sup})**
17 Vdc	600 mA
24 Vdc	450 mA
30 Vdc	350 mA
Formula	$I_{sup} = \frac{10.5}{V_{sup}}$

Additional Current to Support Battery Charging

3 – Powering Expansion I/O Modules

The VUE Series modules allow connection of VUE-EX Series modules to the RS-485 port to provide expanded I/O capacity. You can use the "+" and "–" connections on the VUE to provide up to 500 mA supply for expansion I/O modules. If you have a back-up SLA battery connected to the VUE, then this connection will also be powered from the back-up supply, so that the expansion I/O modules receive the backup power as well as the main module.



Expansion I/O power and RS-485

When the module is being powered from the main supply (SUP+ and SUP– terminals), you need to provide sufficient power to support the additional current required by the expansion I/O modules. The table below shows the additional current from your power supply to support expansion I/O connection.

	Expansion I/O current (I_{exp})	Current required (I_{sup}) Supply voltage		
		17 Vdc	24 Vdc	30 Vdc
Base operating current 115S	120 mA	130 mA	90 mA	75 mA
Discrete inputs (per active input)	13 mA	14 mA	10 mA	8 mA
Discrete outputs (per active output)	25 mA	27 mA	20 mA	16 mA
Analog inputs and outputs (per 20 mA loop)	50 mA	55 mA	38 mA	30 mA
Formula	$I_{sup} = \frac{I_{exp} \times 18.4}{V_{sup}}$			

Additional Current Supply to support Expansion I/O

4 – Powering Directly from the BAT+ and GND Terminals

In some situations, you may want to power the module directly from a 13.8 Vdc supply. This could be because this voltage supply is already available at an installation; because the power requirements for VUE-EX modules are more than can be supplied by the "+" and "–" expansion I/O connections; or because the installation cannot meet thermal requirements when being powered from the SUP inputs (refer to "Thermal" section on page 17).

Use the table below to determine the device's current requirements at 13.8 Vdc. Remember you also need to add current for any other equipment being powered from the same power supply, including relays, indicators, and any additional VUE-EX modules.

	Supply current at 13.8 Vdc
Base operating current	180 mA
Radio transmit current	
10W FSK	2500 mA
5W FSK	1300 mA
4W QAM	2100 mA
Discrete I/O (per active input or output)	10 mA
Analog inputs and outputs (per 20 mA loop)	50 mA

Current Requirements

5 – Internal I/O

The internal supply voltage register locations shown in the following table can be monitored using the Diagnostics Web page within the module's Web-based configuration utility (see "IO diagnostics" on page 133 for details). The values can also be mapped to a register or an analog output on another module within the network.

Register	Description
30005	Local supply voltage (0–40 V scaling).
30006	Local 24 V loop voltage (0–40 V scaling). Internally generated +24 V supply used for analog loop supply. Maximum current limit is 100 mA.
30007	Local battery voltage (0–40 V scaling).
30008	VUE-EX supply voltage (0–40 V scaling).
38005–38008	Floating point registers that display the actual supply voltage, battery voltage, +24 V supply, and VUE-EX supply. Note that these are actual voltage values, whereas registers 30005–30008 display a number between 8192 and 49152 that represents the voltage scale 0–40 V.

Internal Voltage Supply Registers

To calculate the supply voltages from the register value use the following calculation:

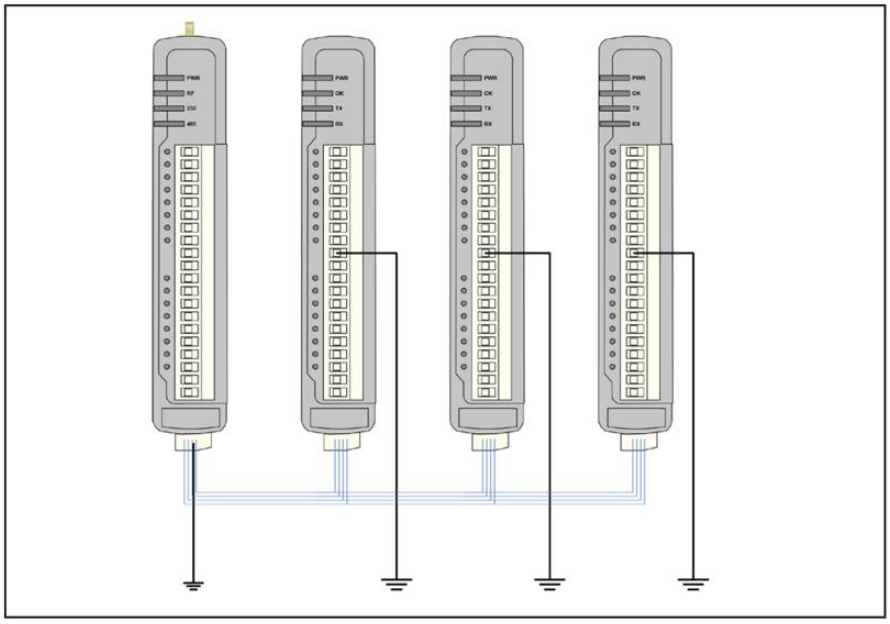
$$\text{Volts} = \frac{(\text{Register Value}) - 8192}{1024}$$

High and low voltage alarm indication may be configured for each of these supply voltages. See “Analog inputs” on page 83 for details on how to configure these alarms.

6 – Grounding

To provide maximum surge and lightning protection each module should be effectively earthed/grounded via a GND terminal on the module. This is to ensure that the surge protection circuits inside the module are effective. The module should be connected to the same common ground point as the enclosure ground and the antenna mast ground.

The VUE Series have a dedicated earth/ground connection screw on the bottom end plate next to the supply terminals. All earth/ground wiring should be minimum 0.8 in2 (2 mm2), 14 AWG. If using the VUE Series radios with the VUE-EX serial expansion I/O modules, all expansion modules must have a separate earth/ground connection from the front terminal back to the common earth or ground point. See Figure Below.



Grounding

The VUE radios use narrowband radio transmission to transfer data over licensed radio channels. There are models to support frequencies in the range 340 MHz to 480 MHz, and to support narrow (12.5 kHz) and wide (25 kHz) channels.

The VUE 4 radio module supports power levels from 10mW to 10W, and channel bandwidths of 6.25, 12.5 and 25 kHz. The VUE Series transmit data using Quadrature Amplitude Modulation (QAM), with two, four, or six bits per symbol, supporting data rates up to 96kb/s on a 25kHz channel. The VUE-1 and VUE-4 also support FSK modulation, data is transmitted using direct frequency shift keying with either one or two bits per symbol (2FSK, 4FSK). This supports data rates of 9600 baud (2FSK) and 19,200 baud (4FSK) on a wide (25 kHz) channel, and 4800 baud (2FSK) and 9600 baud (4FSK) on a narrow (12.5 kHz) channel.

The radio protocol is based on the 802.11 protocol commonly used in 2.4 GHz and 5 GHz WiFi applications. If you are familiar with 802.11, many of the radio networking concepts used in the VUE will also be familiar to you.

The data rates achievable with the VUE are significantly lower than those for WiFi applications, so care must be taken to make the best use of the available channel bandwidth.

The VUE module is shipped from the factory without any radio configuration. The radio will not send any transmission until initial device provisioning has been completed. At power-up, the device will set its OK LED to RED to indicate that this initial provisioning has not been completed.

To configure the device's radio for the first time, you must configure the radio Locale and radio Quick Start to set the radio to meet regulations at its target location. Refer to "Quick start—basic device configuration" on page 40 for instructions on how to configure the radio using the Web interface.

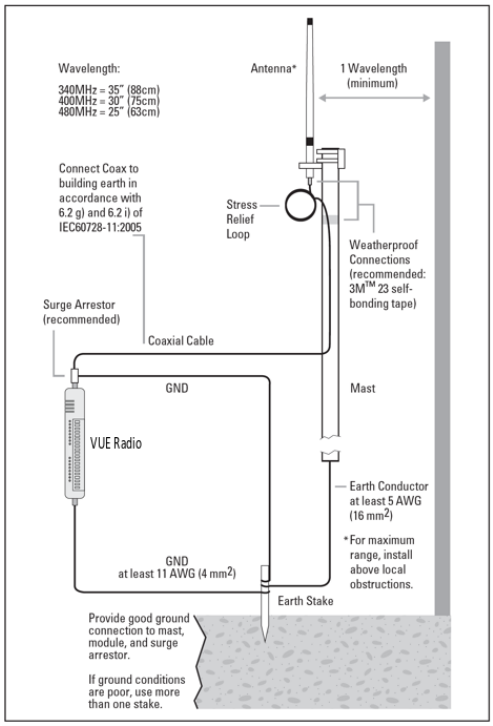
D – Antenna

Intuicom recommends that for final installation the correct sizes of Coaxial Cable and in line surge suppression be used.

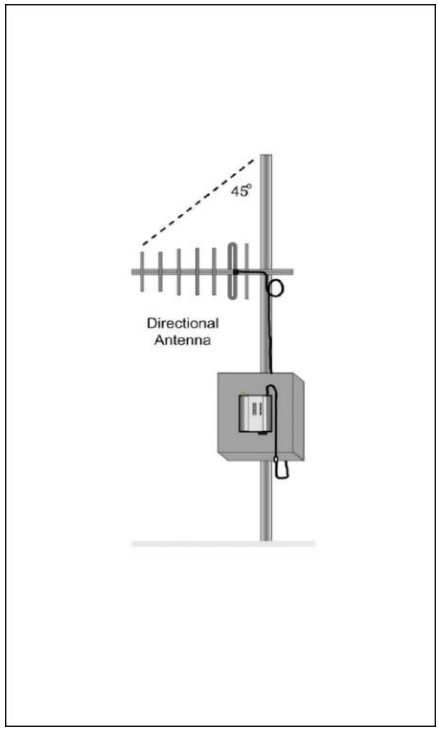
- LMR-240 3-foot section – Run from the radio module to the surge suppressor
- LMR-400 (0 to 100 feet) – Run from the surge suppressor to the antenna.

Runs longer than 100 feet will require larger coaxial cable to reduce signal loss.

Intuicom also recommends the correct antenna spacing from walls or structures be maintained, and the radio, antenna mast, antenna cables, and radio enclosure be properly grounded. See illustrations below.



Omni Antenna Installation



Directional Antenna

Omni antennas should be mounted vertically and at least one wave length away from a wall or mast, and at least 3 feet (1 meter) from the radio module.

1 – Directional Antennas

A directional antenna provides high gain in the forward direction, but lower gain in other directions. This type of antenna may be used to compensate for coaxial cable loss for installations with marginal radio path. Directional antennas can be any of the following:

- Yagi antenna with a main beam and orthogonal elements
- Directional radome, which is cylindrical in shape
- Parabolic antenna

Yagi antennas should be installed with the main beam horizontal, pointing in the forward direction. If the Yagi antenna is transmitting to a vertically mounted omni-directional antenna, the Yagi elements should be vertical. If the Yagi is transmitting to another Yagi, the elements at each end of the wireless link need to be in the same plane (horizontal or vertical).

Directional radomes should be installed with the central beam horizontal, and must be pointed exactly in the direction of transmission to benefit from the gain of the antenna.

Parabolic antennas should be mounted according to the manufacturer's instructions, with the parabolic grid at the back and the radiating element pointing in the direction of the transmission. Ensure that the antenna mounting bracket is well connected to ground.

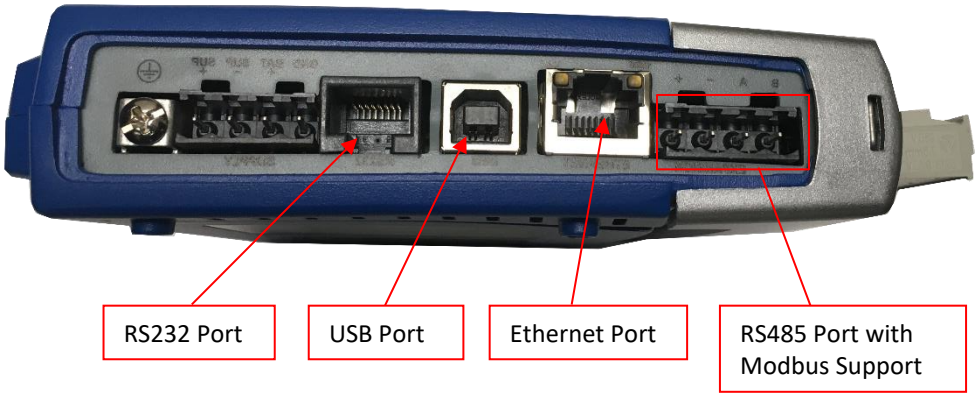
2 – Antenna Installation Tips

Intuicom recommends that all connections be thoroughly sealed to prevent moisture from entering the cable or connectors. Moisture contamination is the biggest cause of problems with wireless systems due to the increased signal loss. Intuicom recommends sealing threads on cable connector with rubber sealant, then wrap the connection with vulcanizing tape, and then cover the tape completely with high quality water proof shrink wrap.

There are numerous ways in which the coaxial cable connectors can be sealed from moisture. The installers will be responsible for sealing these connections with what ever method they chose to use.

Where antennas are mounted on elevated masts, the masts should be effectively grounded to avoid lightning surges. For high lightning risk areas, approved Intuicom surge suppression devices, should be fitted between the radio module and the antenna. If using non-Intuicom surge suppression devices, the devices must have a "turn on" voltage of less than 90 V. If the antenna is not already shielded from lightning strike by an adjacent grounded structure, a lightning rod may be installed above the antenna to provide shielding.

E – Bottom Panel Connections



1 – Ethernet Port

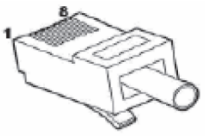
The VUE modules provide a standard RJ-45 Ethernet port compliant to IEEE 802.3 10/100Base-T. This port provides full access to the module, including configuration, diagnostics, log file download, and firmware upload of both the local and remote units. Additionally, the Ethernet port can provide network connectivity for locally connected third-party devices with Ethernet functionality.

2 – USB Device Port for Configuration

The VUE modules also provide a USB device (USB-B) connector. This connector provides configuration of the device and remote configuration access to other devices in the radio network.

3 – RS-232 Port

The VUE modules provide an RS-232 serial port that supports operation at data rates up to 230,400 baud. This port supports Modbus protocol. The RS-232 port is accessed using an RJ-45 connector wired as a DCE according to the EIA-562 Electrical Standard.

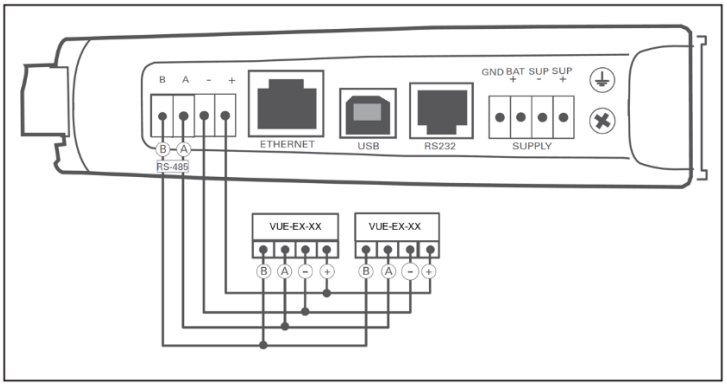
RJ-45	Signal	Required	Signal name	Connector
1	RI	—	Ring Indicator	
2	DCD	—	Data Carrier Detect	
3	DTR	Y	Data Terminal Ready	
4	GND	Y	Signal Common	
5	RXD	Y	Receive Data (from module)	
6	TXD	Y	Transmit Data (to module)	
7	CTS	—	Clear to Send	
8	RTS	—	Request to Send	

RS232 RJ45 Connector Pinout

4 – RS-485 Port with Modbus Support

The VUE modules provide an RS-485 serial port that supports operations at data rates up to 230,400 baud. The default baud rate is 9600 baud, no parity, 8 data bits and 1 stop bit, which matches the VUE-EX serial expansion module default settings. This port supports the Modbus protocol.

The RS-485 port terminal is hosted on the four-way expansion connector on the bottom edge of the module. An on-board RS-485 termination resistor provides line termination for long runs. As a general rule, termination resistors should be enabled at each end of the RS-485 cable. When using VUE-EX expansion I/O modules, remember to enable the RS-485 termination resistor switch that is located on the end module.



RS-485 Connections

III – Getting Started

The following is a list of steps necessary to program the radios and get a wireless link up and connected. Intuicom recommends setting the radio up in a lab or work bench environment and getting them configured prior to deployment.

The VUE products have many sophisticated features, but if you do not require these features, you can use this section to configure units quickly.

Intuicom recommends configuring the radios in a lab or work bench environment prior to deploying them into the field. This will ensure that the radios are functioning as programmed and deployment can take place with little to no adjustments to the configuration.

In addition to the VUE radio from Intuicom, you will need the following items:

1. Power Supplies
2. Ethernet Cables
3. Rubber duck antenna with an SMA male connector.

A – Step 1 – Connect an Antenna

When working on the bench if you have a duck antenna with an SMA male connector, connect it to the radio.

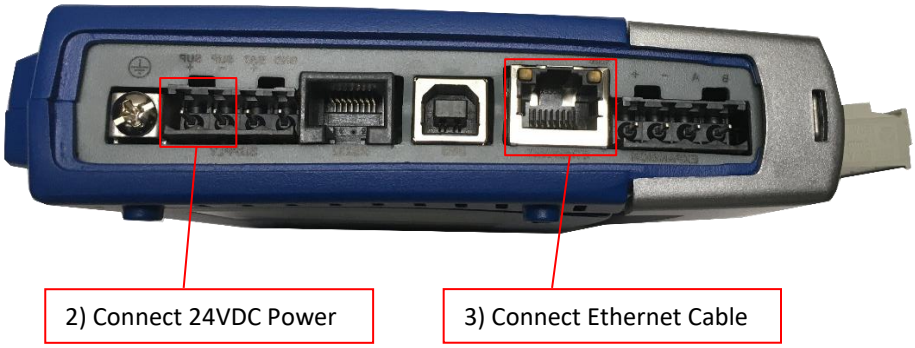
VUE Series – Antenna Connection (SMA)

For bench testing and configuration prior to deployment, connecting the antenna directly to the SMA connector on the radio is acceptable.

For details on connecting the antenna for final installation see pages 28 – 30.

B – Step 2 – Connect Ethernet Cable

Connect an Ethernet (CAT5) cable from the port on the radio to your computer.



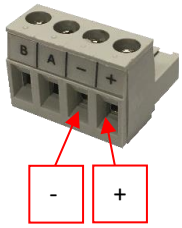
C – Step 3 – Connect the Power Supply

Connect a 12VDC 1 to 5 Amp power supply to the BAT+ and GND connections on the side of the VUE. Phoenix plug is provided to connect the DC power leads.

Connecting a 24V 1 amp power supply to the SUP+ and SUP- lugs on the phoenix connector, for configuration on the bench is acceptable.

For more information on final installation power requirements see pages 22-28. Make sure that the unit is properly grounded when permanently installed.

NOTE: The Phoenix Connector is not labeled the same as the connections on the radio. SUP+ and SUP- are the plus and minus sign on the connector. Wire in 15 to 30Vdc to these terminals.



D – Step 4 – Set the IP Address of the Computer

You must set the IP Address and subnet mask of Ethernet adapter on your computer that is being used to program the VUE, to the same range as the IP Address of the radio. The configuration or default IP Address of the VUE should be printed on label. If the IP Address is not printed on the label, you can use the format: 192.168.0.1XX – where XX is the last two digits in the serial number of the VUE.

- IP Address is 192.168.0.1XX, where XX is the last two digits of the radio serial number (the default IP address is shown on the printed label on the back of the unit).
- Subnet Mask is 255.255.255.0.

Once you have your IP Address set on your computer, use the Command Prompt in Windows and ping the radio. If you can ping the IP Address of the radio, proceed to Step 5.

NOTE: Do not use the same IP Address on your PC as the IP Address of the radio.

1 – Windows Tip
You cannot ping a device connected to your windows PC unless the IP Address of your computer is in the same range as the device you are trying to ping or access.

Problem: When changing IP Address on Intuicom radios from default to the desired range, users have to change the IP Address of their LAN adapter after every IP Address change on a radio.

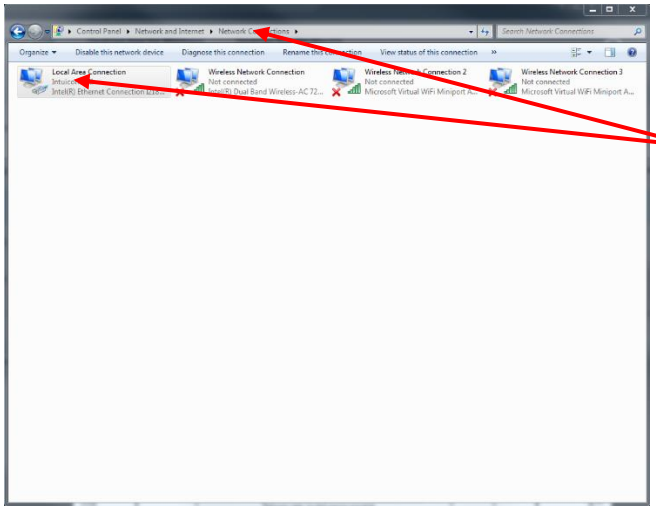
Example: You are programming the radios to 10.24.X.X addresses using a 255.255.0.0 subnet mask. You already have a 10.24.25.30 IP Address statically set on your LAN adapter connected to the radios.

Task: You need to connect a radio to your computer that is new and at default IP configuration and program it to the 10.24.X.X range.

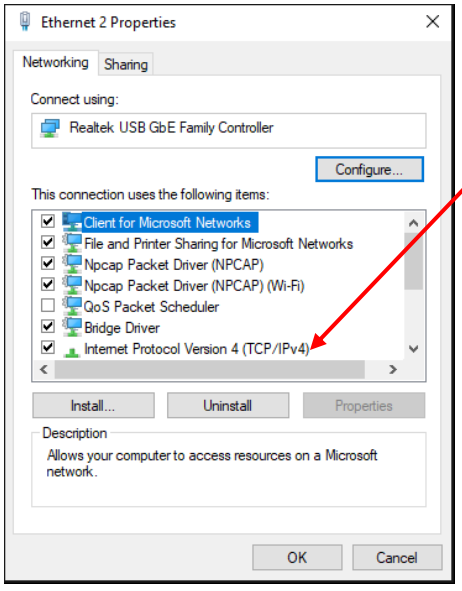
Fix: Navigate to Control Panel – Network and Internet – Network Connections window of your computer, and right click on your Local Area Connection that is connected to the radio, and double click on TCP/IP v4 Properties.

Leave the 10.24.25.30 address already programmed on your adapter there, and below the DNS address boxes click on the rectangular button named “Advanced…” and below the box labeled IP addresses click the “Add” button and type in the IP address 192.168.0.10 with a 255.255.255.0 subnet mask. After you click “Add” button, the IP address window now has two addresses in it, your original 10.24.25.30, and the 192.168.0.10 address, click OK three times, on each window all the way out and close the Network Connections window.

After you have completed this you will be able to ping and log into the radios at default IP address, and once you have changed them to the new IP address, you will still be able to ping and log into them without having to change the IP address on your network adapter.

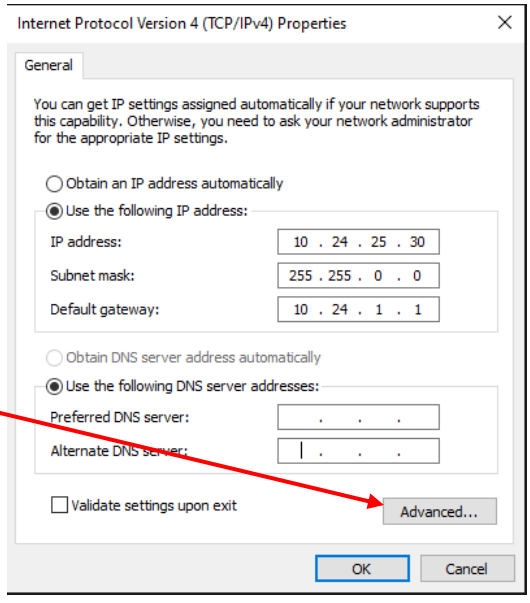


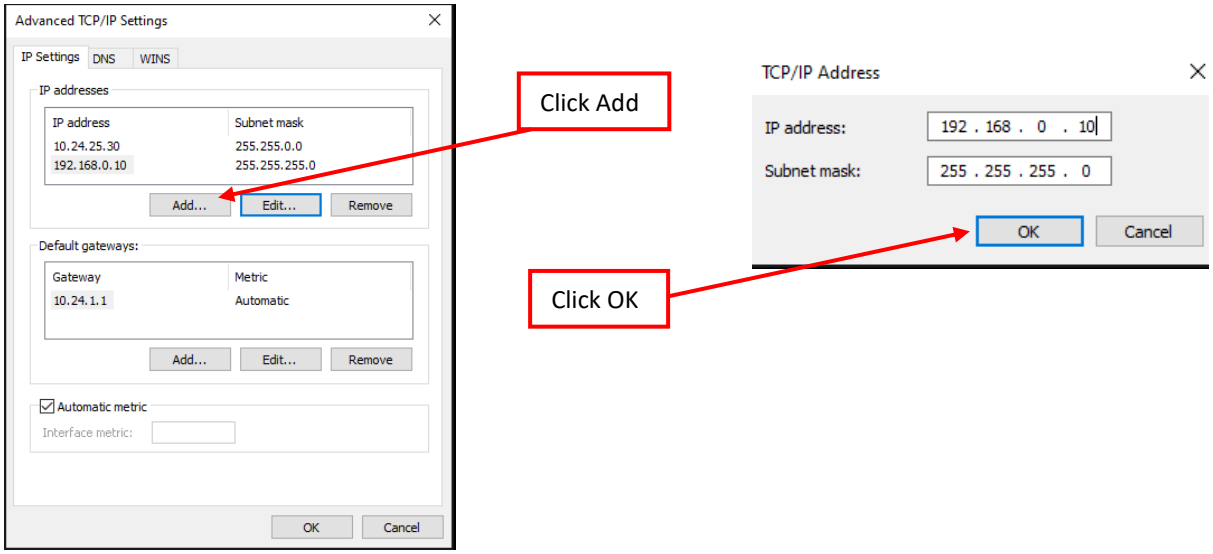
Navigate to the "Network Connections" Window and right click the Local Area Connection and select properties



Double Click on Internet Protocol Version 4

Click Advanced

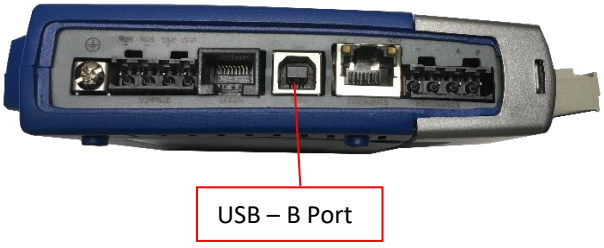




E – Step 5 – Enabling Web Browser Access

Intuicom ships the VUE product with web browser access enabled. If for any reason you can ping the radios default IP Address, but cannot access the webpages, or if you have run the factory reset on your unit. You will need to enable web browser access.

To enable web browser access, you must connect to the device through its USB port.



To connect the VUE to a PC you will need a USB-A to USB-B cable. If this is the first time you have connected to the VUE through the USB port then you will need to download the USB driver file from the Intuicom Support portal on the Intuicom website. The driver files are in the same location as the VUE user manual.

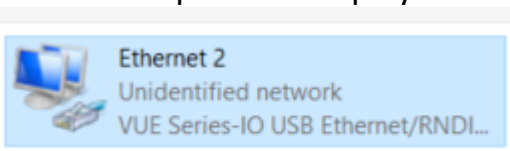
You will also need to know the username and password configured for the VUE if it has been changed from the default settings. Default username and password for the VUE series radios are, username=user, and password=user.

Follow the steps below to enable web page access on the VUE radios.

1) Install the USB Driver by double clicking on the file you have downloaded from the Intuicom website.
2) Power on the device, and wait for the device to finish booting, or for the "PWR" LED to go solid green or red. Take about 1 minute.

NOTE: If the device Locale is **not** set the "PWR" LED will be red, and if the device Locale is set the LED will be green.

3) Plug in the USB cable and wait for your computer to recognize the new USB device. The new device will identify as "VUE Series-IO USB Ethernet/RNDIS".
4) Once the driver is installed you will have an additional network adapter in your device manager list, and in your Network Connections window.
5) In Network Connections the adapter will display as follows:



6) Open your web browser (ie Chrome, Firefox, Edge, IE10 or newer).and type http://192.168.111.1 into the address line. All the VUE radios have the same address when accessing the through the USB port. The module should respond with the username and password window.
7) Enter the login credentials username=user, and password=user.

This should open the home page. In the right column of links click on the "Quick Start" link.

On the Quick Start webpage at the top of the page, place the checkmark in "Enable Remote Web Server Access" and click "Save Changes and Reset" to commit the change. After the radio has finished rebooting you should be able to connect your PC to the radio through the Ethernet port and type the IP address of the radio into the address line of your browser and log in.

NOTE: if the IP address has been changed on the radio you will need to use that IP Address to log into the radio over Ethernet. Again, if the radio was reset or the IP

address never changed from the default setting, you will use the default IP address to log into the radio.

F – Step 6 – Log Into the VUE

Open an internet browser such as Internet Explorer, Edge, Chrome, or Firefox and type into the address line on the browser the IP Address of the VUE. Log in with the credentials:

- Username: user
- Password: user

For administrative access to the VUE use the credentials:

- Username: admin
- Password: admin

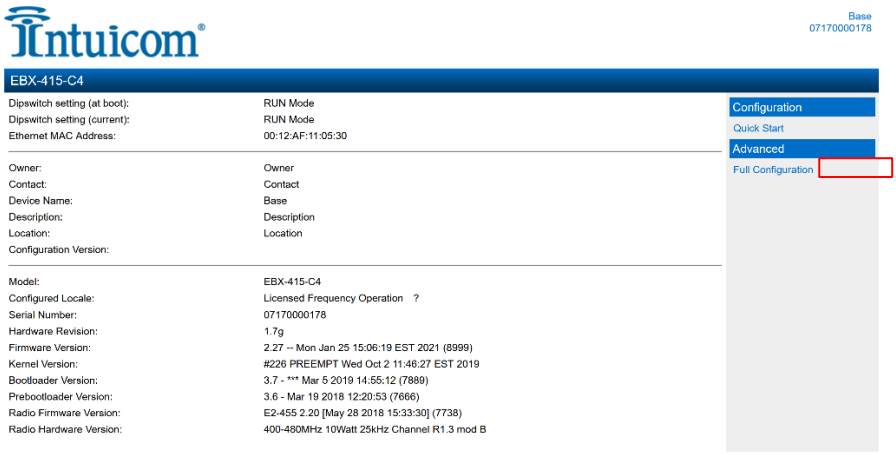
III – Configuration Webpages

In the right column the first set of webpages are the "Configuration" pages. These include A) Quick Start, B) Network, C) Security, and D) Radio. The following is an overview of each of these webpages.

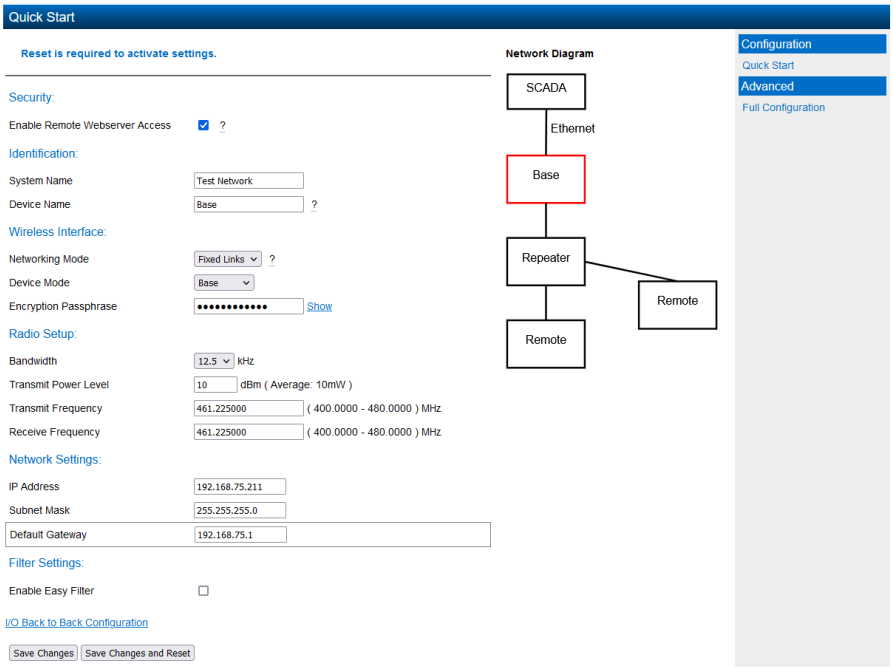
NOTE: Many of the settings on the Configuration webpages can be left at default and for most wireless applications the default settings will work with no issues.

A – Quick Start Settings

Click on the "Quick Start" link in the right column.



Home Web Page – Quick Link



Quick Start Webpage

1 – Security

a – Enable Remote Webserver Access

This should already be enabled. A check mark in this box to enables access to the device webpages from the Ethernet and Radio ports. If this is not selected, then you can only access the device webpages from the USB Configuration port.

NOTE: Access to the radio webpages is enabled by Intuicom default settings.

2 – Identification

a – System Name

This is a name common to every device in the system. This allows Remotes to be configured to connect to any device in the system. This is the same as the SSID or Network ID.

b – Device Name

This is a unique name for the individual device. Each device in the system should have a unique name. This needs to be unique so for network formation and to allow you to identify devices when performing diagnostics.

3 – Wireless Interface

a – Networking Mode

This option selects the way the devices will connect on the wireless network. Check the System design chapter in this manual for more detail. Options are:

- Fixed Links - Repeater backbone and remote sites
- ProMesh - Automatic adaptabble mesh
- Manual - Full Manual configuration of topology

b – Device Mode

This selects the device operating mode when the networking mode is set to one of the options above.

Fixed Links – Selecting this setting provides Device Mode settings shown in the diagram on the right of the page. These are Base, Repeater, and Remote.

Pro Mesh – Selecting this setting provides Device Mode settings of Base or Mesh Node. Only one Base unit is needed per network with the rest of the radios being set to Mesh Node.

Manual – When Manual is selected for Networking Node, above under Identification the System Name disappears. This is because 1) Device Mode changes to 802.11 Mode, and System Address (ESSID) appears as a new setting below 802.11 mode.

- **802.11 Mode** – The selections under 802.11 mode are "Access Point", and "Client". One radio will be set to Access Point, and the rest of the radios connecting directly to it are set to Client (Station) mode.
- **System Address (ESSID)** – This setting must be exactly the same on the Access Point and all connected Clients (Stations) to the Access Point.

c – Encryption Passphrase

This passphrase sets the Encryption used by all devices. Radio Encryption is set to AES256 bit by default. All devices in the system must be configured with the same Encryption Passphrase.

4 – Radio Setup

These items configure the physical radio setup. Values that you enter here are determined by your radio system design.

a – Bandwidth

Select the bandwidth according to your license. Larger bandwidth setting allows higher data throughput.

NOTE: All devices in the system need to be set to have the same bandwidth.

b – Transmit Power Level

This selects the transmitter power level. The transmit power level is displayed in dBm. The options here will be limited by the capabilities of your radio model, and by any restrictions for the locale selection you made during Locale configuration. Normally you will select the highest available power level.

The average power (ERP) and peak envelop power (PEP) levels are shown beside the selection, and can differ from the selected value.

NOTE: If you are using high gain antennas, you may need to select a lower power level to remain inside the restrictions of your radio license, or within the requirements for unlicensed operation within your target locale.

NOTE: For QAM modes, the actual average power level that the radio transmits may be lower than the value you selected, and the peak envelope power level may be higher. Check your license to ensure you comply with the requirements of your regulatory body.

c – Transmit Frequency
This is the radio's transmit frequency, in MHz. The number will be automatically rounded to the closest available frequency based on the Frequency Step Size available for your Locale.

d – Receive Frequency
This is the radio's receive frequency, in MHz. The number will be automatically rounded to the closest available frequency

NOTE: For Unlicensed systems, the transmit and receive frequencies will normally be the same. Many licensed systems require transmitting and receiving on a pair of frequencies. For these systems, you need to make sure that the Transmit frequency is the same as the receive frequency of the upstream device (Base or Repeater), and that the receive frequency matches the transmit frequency of the upstream device.

5 – Network Settings
Values that you enter here configure the Device's IP networking operation, and how it connects to other IP networking devices.

a – IP Address
This is the IP address you use to access the VUE radio. This IP address is part of the same sub-net as the Ethernet network.

NOTE: The VUE default networking configuration bridges between the Radio and the Ethernet networks. This simplifies network configuration as a single IP address is used to access the device from either Ethernet or Radio networks.

b – Subnet Mask
This is the net-mask for the device's IP address. This is the same net-mask as configured for other devices on the network.

c – Default Gateway
This field configures a default gateway for messages addressed to IP addresses that are not on the same subnet as the device. This can be left blank if all communication will be within a single subnet.

NOTE: The VUE default networking configuration bridges between the Radio and the Ethernet networks. This simplifies network configuration as the Ethernet and radio networks share a single sub-net, and a single IP address is used to access the device from either Ethernet or Radio networks. In most applications it is not necessary to configure any IP routing.

6 – Filter Settings
When the checkmark is placed in "Enable Easy Filter" the following two settings become available for configuration.

a – First Radio Device IP
This is the lowest IP address of the devices connected to the radio network. For the example above, this would be 192.168.10.51

b – Last Radio Device IP
This is the highest IP address of the devices connected to the radio network. For the example above, this would be 192.168.10.254.

NOTE: If you need to configure more complex filtering, you can access this functionality from the "IP filter" configuration web-page.

7 – I/O Back-to-Back Configuration
The VUE-1 and VUE-4 come pre-configured with a gather-scatter I/O mapping, allowing you to send I/O data between the Base site and one Remote site. This function is available in ProMesh mode, and maps all of the I/O to appear at the

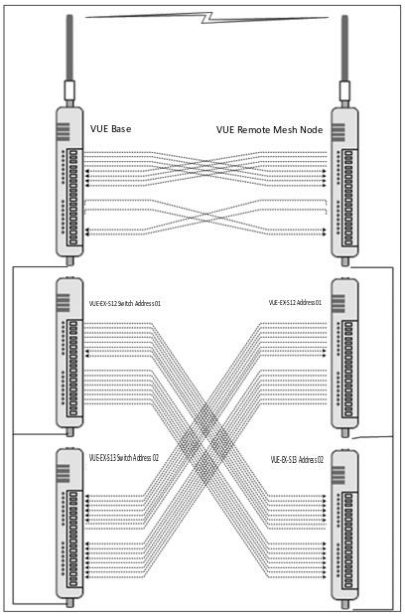
remote site. You can enable this mapping by checking the “Enable I/O Data” checkbox on the Quick Start page. You can view and edit this mapping by selecting “I/O Mappings >> Gather Scatter Mappings” from the Configuration side menu.

This pre-configured mapping supports connection of VUE-EX-S12 and VUE-EX-S13 expansion modules to your Base and Remote sites to increase the number of I/O. When you do this, you must configure the VUE-EX-S12 with address 01 and the VUE-EX-S13 with address 02. You set the address using the rotary switches on the bottom panel of the VUE-EX module. Refer to section “Adding expansion I/O modules” on page 45 & 153 (Appendix D) for instructions on how to connect VUE-EX modules.

NOTE: You don’t need to connect the VUE-EX modules. You can use only the base and remote modules, or just connect one VUE-EX-S12 module at one end, and one VUE-EX-S13 at the other end.

Input point (Local)	Output point (Remote)
VUE-1, 4-IO	**VUE-1, 4**
DI1 – DI4	DO5-DO8
AI1 – AI2 (4-20mA)	AO1-AO2
VUE-1, 4-IO	**VUE-1, 4**
DI1	DO2
Expansion VUE-EX-S12	**Expansion VUE-EX-S13**
DI1 – DI6	DO1 – DO6
AI1 – AI8	AO1 – AO8
Expansion VUE-EX-S13	**Expansion VUE-EX-S12**
DI7 – DI8	DO7 – DO8

Example of Input Output Mappings



Back-to-Back Mappings – VUE

8 – Quick Start Additional Information

If you make changes to configuration items on other configuration pages, these may appear on the Quick Start page surrounded by a red box. This acts as a reminder that these items are not set to the default values, and you need to take care that the configuration is correct.

In the example below, the Transmit Data Rate and the Base Data rate have been set to non-default values on the Radio Configuraiton page. These are shown on the Quick Start page as a reminder that they are not set to default values.

Radio Setup:

Bandwidth	12.5 ▼ kHz
Transmit Data Rate	16 ▼ kbits/s
Base Data Rate	8 ▼ kbits/s
Transmit Power Level	20 dBm (Average: 1
Transmit Frequency	472.018750 MHz
Receive Frequency	472.018750

Quick Start webpage with – non default values outlined in red

9 – Saving Settings

Once you have configured the settings on the Quick Start webpage, click “Save Changes and Reset” button at the bottom of the webpage to save and commit the changes. This will reboot the system and commit the changes.

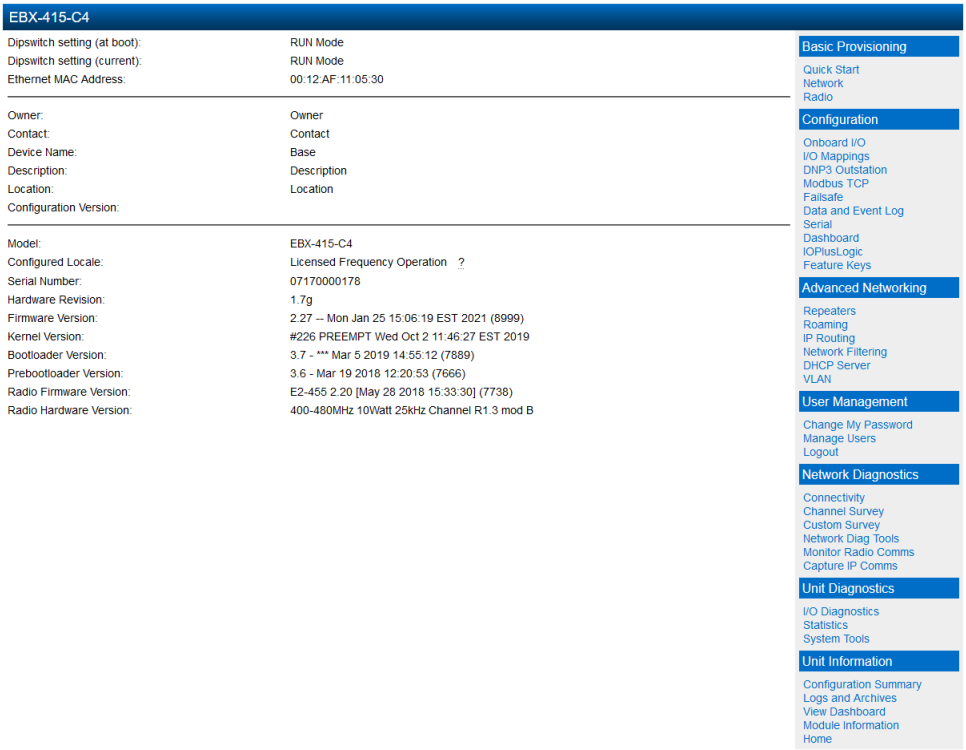
NOTE: If you navigate to other webpages and make changes click the “Save Changes” button before navigating away from that webpage. Once all settings are entered click the “Save Changes and Reset” button to commit all saved changes with a reboot of the unit.

IV – Basic Provisioning

Full Configuration – When you first log into the VUE webpage, there are only two links in the right column. The "Configuration" header with the Quick Start link below it and the "Advanced header with the "Full Configuration" link below it.

Upon click on the "Full Configuration" link, the headers change and the links to webpages expands. The upper header for "Configuration" changes to "Basic Provisioning", and the lower "Advanced" header changes to "Configuration" and the menus expand with additional headers and links below.

Each of the webpages associated with the expanded menu options are covered in the following sections of this manual.



Home Webpage after clicking "Full Configuration Link"

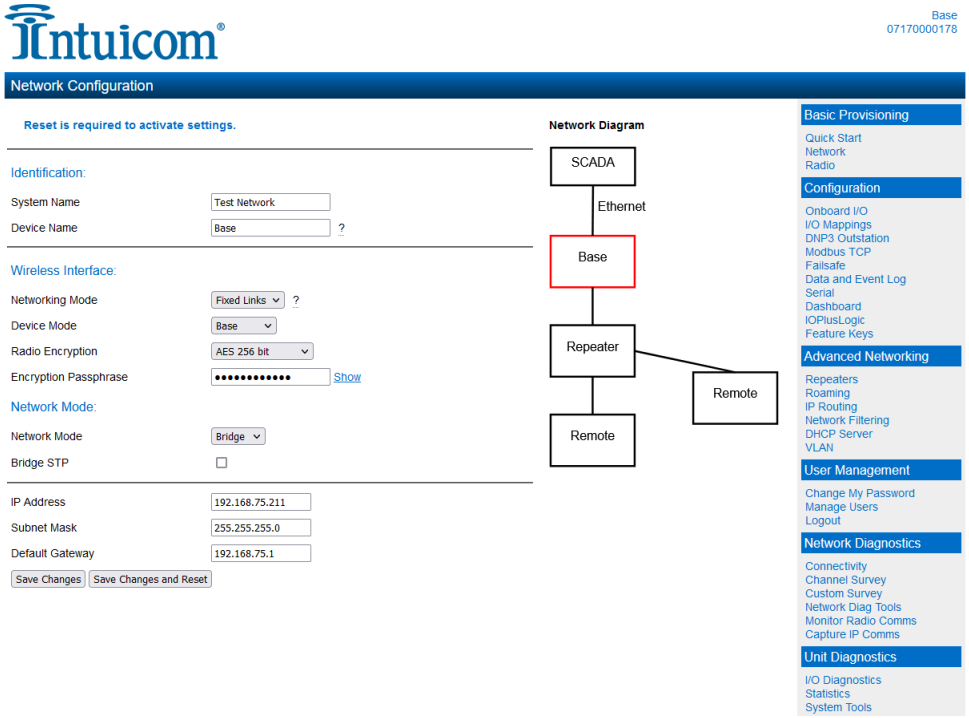
A – Quick Start

Settings for the Quick Start webpage are covered on pages 36 – 49 of this manual.

B – Network

Under "Basic Provisioning" the second link down is the "Network", clicking on the link will take you to the Network Configuration webpage. When making changes on

the Network Configuration webpage you will need to save and reboot (or reset) the radio to commit the changes.



Network Configuration Webpage

1 – Identification

System Name – This is a name common to every device in the system. This allows Remotes to be configured to connect to any device in the system.

Device Name – This is a unique name for the individual device. Each device in the system should have a unique name. This needs to be unique so for network formation and to allow you to identify devices when performing diagnostics.

2 – Wireless Interface

Networking Mode – This option selects the way the devices will connect on the wireless network. Changing the Network Mode to the different available options will change the settings below. Each of the setting options will be covered in this chapter in detail. Options are:

- **Fixed Links** – Repeater backbone and remote sites.
- **ProMesh** – Automatic adaptable mesh.
- **Manual** – Full Manual configuration of topology.

Device Mode – This option changes depending on the selection in the Networking Mode Dropdown. These are as follows:

Fixed Links – When Networking mode is set to "Fixed Links" the options in the Device Mode drop down menu are:

- **Base** – This is the main, master, or access point unit that all radios in the network connect with.
- **Repeater** – This is the setting used when other remote radios cannot connect directly with the Base unit and must connect through one of the radios that can connect directly with the Base.
- **Remote** – These are radios that connect as slaves or clients to the Base.

NOTE: These roles are depicted in the image to the right of the settings on the Network webpage.

ProMesh – When the Networking mode is set to "ProMesh" the options in the drop-down menu are:

- **Base** – This is the main, master, or access point unit that provides the main connectivity point among all the radios in a network.
- **Mesh Node** – All other radios in the mesh network are set to Mesh Node. They can connect directly to the Base unit, or to any other Mesh Node in the network that has the best signal and connection to the Base radio.

NOTE: When the radios are set up in ProMesh mode there is no need for repeaters as any Mesh Node can connect to any other Mesh Mode or the Base directly in the wireless network. These roles also correspond to the image to the right of the settings on the Network webpage.

Manual – When "Manual" mode is selected, "Device Mode" name changes to "802.11 Mode" and the available options are:

- **Access Point** – This is basically the same setting as "Base" where the Access Point controls the behavior for the wireless links, and multiple "Clients" can connect to it.

- **Client (Station)** – This is the setting used for remote, subscriber, or Client units that connect with the Access Point.

System Address (ESSID) – When Manual is selected from the network mode drop-down menu. Above, under Identification the System Name disappears, and under Wireless Interface this setting appears. This setting takes the place of the System name which is used as the SSID (Security Set Identifier) for all radios in a wireless network. Just like the System Name setting the System Address must be exactly the same on all radios in a given network (Access Point and ALL Clients).

Radio Encryption – Sets the Encruption mode. The default is AES 256 bit, which is suitable for most applications. WPA2-PSK uses the same methods as 802.11 protocol. WPA2-PSK has additional complexity, and should only be used if there is a specific reason to use standards-based encryption method.

Encryption Passphrase – This passphrase sets the Encryption used by all devices. Radio Encryption is set to AES256 bit by default. All devices in the system must be configured with the same Encryption Passphrase.

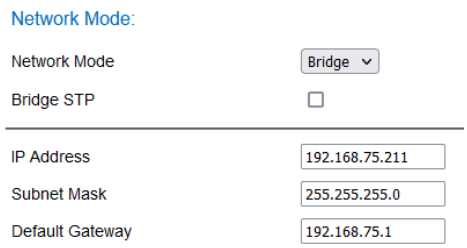
Enable Roaming – When Network Mode is set to Fixed Links, and Device Mode is set to Remote, under Device Mode an option appears to check and enable roaming, or to leave it unchecked and disabled. Selecting this option allows the Remote station to connect to and roam between any repeater or base with matching System Name. De-selecting forces the remote to only connect to the configured Upstream Device Name.

3 – Networking Mode

These Settings allows you to choose between bridged and routed networking. Bridged networking is the simplest to configure and will be the correct choice in almost all networks.

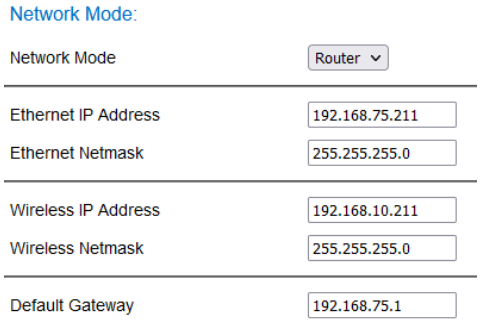
Networking Mode – There are two selections in the drop-down menu for network mode, these are:

- **Bridge** – When this mode is selected the wireless interface and the Ethernet port are bridged together and they have a single IP address assigned to both ports. All data is transparently passed between the wireless interface and the Ethernet port.



IP Settings – Bridge Mode

- **Route**r – Only IP packets are passed between the Wireless Interface and the Ethernet port, which are on separate sub-networks (they have different IP Addresses). You configure the rules for which packets are transferred on the routing configuration page.



IP Settings – Router Mode

Bridge STP - Spanning Tree Protocol (STP) is a method of removing routing loops in bridged networks. You can enable this feature and set the bridge priority if your network topology includes routing loops.

WARNING – Do not enable STP on the bridge interface unless it is configured and in use on your network. Enabling this setting will cause a flood of unwanted packets coming from the VUE looking for the root device on your network.

NOTE: The following settings will change depending on the selection of “Bridge” or “Router” from the Network Mode drop-down menu.

IP Address – There is only space for one IP address when Bridge is selected for Network Mode. This is the IP address that is assigned to the bridge and both the wireless interface and the Ethernet port will use this same IP Address. You will need to assign an IP address in the same range as the rest of the devices on your network.

There are two (2) IP address settings available when Router is selected for the Network Mode. One is for the Ethernet Port and the other is for the Wireless Interface. The Ethernet port will need to have an IP address assigned in the same range as the rest of the devices on your network, and the Wireless Interface will need to have an IP address assigned that is in a separate range as the rest of the network, and in the same range as the rest of the wireless interfaces connected together. So in review, ALL wireless interfaces for all radios connected together will need to have IP addresses assigned in the same range.

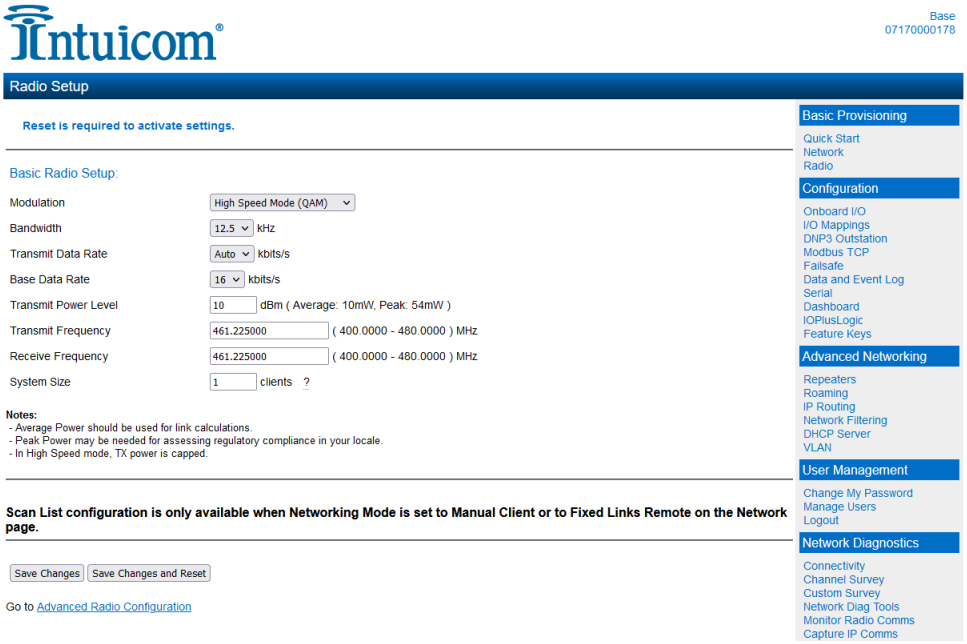
Subnet Mask – When the Network Mode is set to Bridge this setting will have to match the subnet mask being used on your network.
When the Network Mode is set to Router, the Ethernet port will need to have a Subnet Mask set to the same setting as the rest of your network, and the Wireless Interface will need to have the same Subnet Mask set on all radios connected together.

Default Gateway – When Network Mode is set to Bridge, the radios will need to have the same Default Gateway set as the rest of the devices in your network. When the Network Mode is set to Router, there is no setting available for the Default Gateway associated with the wireless links.

Save Changes and Reset – Once the changes are complete on the Network Configuration webpage a reboot is required to commit the changes. Click “Save Changes and Reset” to complete and commit the changes.

C – Radio

These settings allow you to configure the operation of the radio for unusual situations. Some of the options on this page also appear on the QuickStart Page. The options that only appear on this page are underlined in the following for clarity.



Radio Setup Webpage

1 – Basic Radio Setup

Modulation – From the drop-down, select the modulation format. The available selections are.

- **Legacy Speed Mode** – Provides compatibility with existing networks using Frequency Shift Keying modulation (FSK).
- **High Speed Mode** – provides the best throughput and sensitivity using more advanced Quadrature Amplitude Modulation (QAM).

NOTE: All devices in the system need to be set to have the same modulation format.

Bandwidth – Select the bandwidth according to your license. Larger bandwidth setting allows higher data throughput.

NOTE: All devices in the system need to be set to the same bandwidth.

Transmit Data Rate – Select the required data rate. Available data rates depend on the Modulation and Bandwidth settings you have made. You can trade off radio throughput against sensitivity. Select Auto Data rate to allow the radio to find the best rate for the path.

Base Data Rate – This setting controls the slowest speed that any radio will operate at. If no radio will operate at a lower speed, then radio timing parameters can be reduced, so setting this to a higer value improves system throughput. The default Base Rate is the second slowest rate, corresponding to 4QAM modulation.

NOTE: All devices in the system need to be set to have the same Base Data Rate.

Transmit Power Level – This selects the transmitter power level. The transmit power level is displayed in dBm. The options here will be limited by the capabilities of your radio model, and by any restrictions for the locale selection you made during Locale configuration. Normally you will select the highest available power level.
The average power (Effective Power) and peak envelop power (PEP) levels are shown beside the selection, and can differ from the selected value.

NOTE – A: If you are using high gain antennas, you may need to select a lower power level to remain inside the restrictions of your radio license, or within the requirements for unlicensed operation within your target locale.

NOTE – B: For QAM modes, The actual average power level that the radio transmits may be lower than the value you selected, and the peak envelope power level may be higher. Check your license to ensure you comply with the requirements of your regulatory body.

Transmit Frequency – This is the radio's transmit frequency, in MHz. The number will be automatically rounded to the closest available frequency based on the Frequency Step Size available for your locale.

Receive Frequency – This is the radio's receive frequency, in MHz. The number will be automatically rounded to the closest available frequency.

NOTE: For Unlicensed systems, the transmit and receive frequencies will normally be the same. Many licensed systems require transmitting and receiving on a pair of

frequencies. For these systems, you need to make sure that the Transmit frequency is the same as the receive frequency of the upstream device (Base or Repeater), and that the receive frequency matches the transmit frequency of the upstream device.

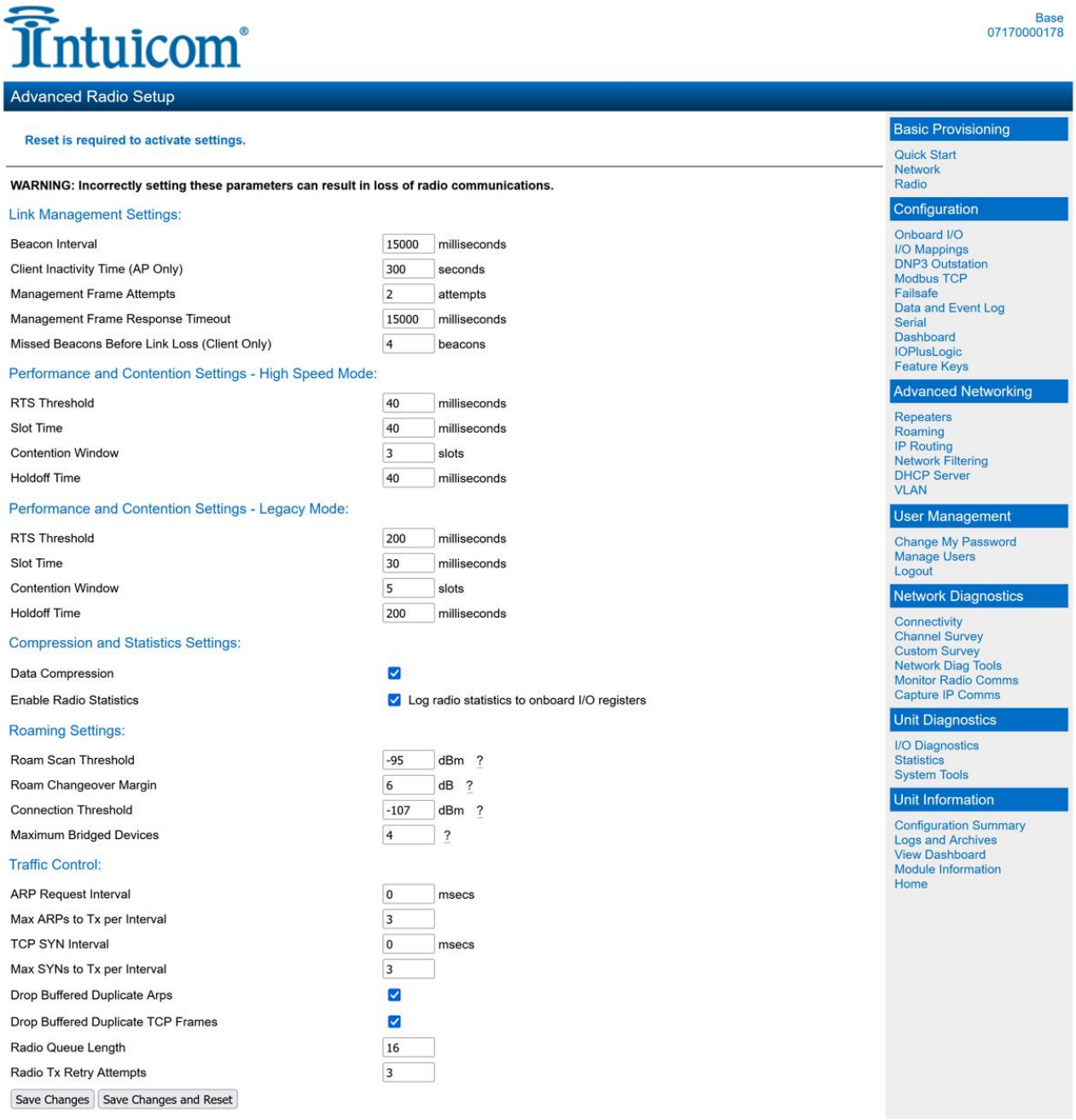
System Size – This value is used to fine-tune the delay timing parameters which deal with contention where more than one station is connecting at the same time. This should be set to approximately match the size of your system.

Save Changes and Reset – Once the changes are complete on the Network Configuration webpage a reboot is required to commit the changes. Click "Save Changes and Reset" to complete and commit the changes.

D – Advanced Radio Configuration

You reach the Advanced Radio Configuration page by clicking the link at the bottom of the Radio Setup page above.

The configuration items on this page are set correctly for the vast majority of applications. Changing items on this page could impact your radio system performance, and may stop it operating. Normally you won't need to change any of the items on this page.



Advanced Radio Setup Webpage

1 – Link Management Settings

These settings impact the maintenance and formation of links between devices. Some radio traffic is required to maintain and establish the links. Adjusting these times will affect this

Beacon Interval – This setting applies to Access Point (Manual mode), Base (ProMesh and Fixed Link modes), Mesh Node (ProMesh) and Repeater (Fixed Link) stations. These stations regularly send a special beacon message to identify themselves and allow other devices to connect to them.
You can change the interval between beacons with this setting. You may need to increase this interval if you have a very large number of devices in close proximity which are all sending beacons.
ProMesh Mesh Node stations only send beacons when they are acting as a repeater for another station.

Client Inactivity Time (AP Only) – This timeout determines how long the upstream device will maintain a link without receiving any message from the downstream device. When this time expires, the downstream device is removed from the connectivity list.

Management Frame Attempts – Management frames co-ordinate link establishment and maintenance between radio devices. This is the number of times that management frames are re-transmitted if no response is received.

Management Frame Response Timeout – The timeout waiting for a response to a management frame before re-transmitting the message.

Missed Beacons Before Link Loss (Client Only) – This timeout determines how long the downstream device will maintain a link without receiving any beacon message from the upstream device (AP). Multiply this by the Beacon Time to find the timeout.

2 – Performance and Contention Settings

These settings control the way the radio accesses the shared radio channel, and how contention for the radio channel between multiple devices is handled.

RTS Threshold – This value sets the messages size where RTS contention control is activated. RTS contention control sends a short message to reserve the radio

channel before sending the longer message. If you have a system with large messages and where remote stations cannot receive each other's messages, then setting this to a value of 100 may help reduce contention.

Slot Time – This time is the step-size in the radio random holdoff used in the channel access protocol.

Contention Window – This is the maximum number of slots in the radio random holdoff algorithm.

Holdoff Time – This is the fixed holdoff used in the radio channel access protocol.

a – Compression and Statistics Settings

Data Compression – Compresses data as it is transferred over the radio channel.

Enable Radio Statistics – Make radio statistics available in the on-board registers (30421-30490).

3 – Roaming Settings

These setting controls how the radios decide to roam between upstream devices. These settings apply to both ProMesh and Fixed Links with Roaming networking modes.

Roam Scan Threshold – The radio won't start looking for alternative upstream device until the RSSI reaches this level.

Roam Changeover Margin – This radio won't change to another upstream unless it is at least this amount better than the current connection.

Connection Threshold – This setting applies to ProMesh mode. The Mesh Node won't connect to a multi-hop path unless the path's adjusted RSSI is at least this good.

Maximum Bridged Devices – When the network topology changes due to roaming or ProMesh changes, the internal MAC routing tables throughout the netwrok need to be refreshed. This is done by the transmission of a Gratuitous ARP message. If you have a large number of host device s connected to the ethernet on one radio, you should adjust this setting.

4 – Traffic Control

Traffic Control applies intelligent filters to Ethernet network traffic reaching the radio network. Host protocols that are designed for high speed network can sometimes re-try messages before the original message has been delivered, and can sometimes send out multiple requests in a very short period. Two protocols that will typically impact radio traffic are ARP and TCP (during connection establishment).These settings limit the number of outstanding requests (ARP and TCP) that can be active at one time. This limits the traffic reaching the radio network.

Rate limiting is achieved by setting an Interval and a maximum number of messages to transmit during the interval. If there are a large number of remote devices in your system, it may be advisable to set the number and the interval both higher.

ARP Request Interval – The Interval for ARP Requests. 0 to disable ARP request rate-limit. Typical 10 sec.

Max ARPs to Tx Per Interval – The maximum number of ARP requests to transmit during the interval. Typical 20 (per 10 secs).

TCP SYN Interval – Interval for TCP SYN Requests. 0 to disable TCP SYN rate-limit. Typical 10 sec.

Max SYNs to Tx per Interval – The maximum number of TCP SYN to transmit during the interval. Typical 20 (per 10 secs).

Drop Buffered Duplicate ARPs – Check this to drop ARP messages that are duplicates of message that are already in the radio Tx Queue.

Drop Buffered Duplicate TCP Frames – Check this to drop ARP messages that are duplicates of messages that are already in the radio Tx Queue.

Radio Queue Length – The maximum number of messages that can be buffered waiting to be transmitted on the radio.

Radio Tx Retry Attempts – For Fixed data rates, the number of times to send a transmission looking for an acknowledgement. (For automatic data rate, the Tx Retry attempts are managed by the rate control algorithm)

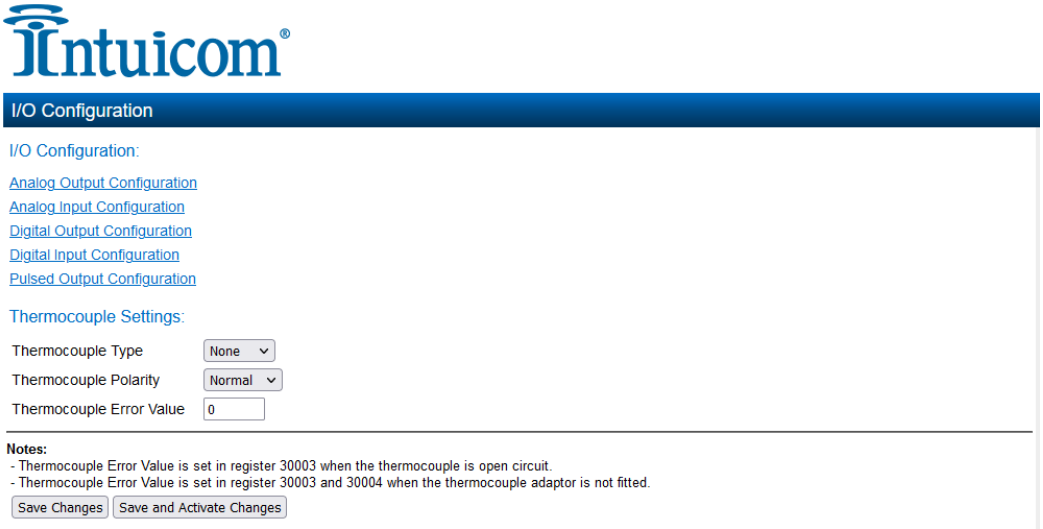
Save Changes and Reset – Once the changes are complete on the Network Configuration webpage a reboot is required to commit the changes. Click “Save Changes and Reset” to complete and commit the changes.

V – Configuration

In the column of page links on the right of the web interface, the category below "Basic Provisioning" is "Configuration". In this section the webpages under the "Configuration" header are covered.

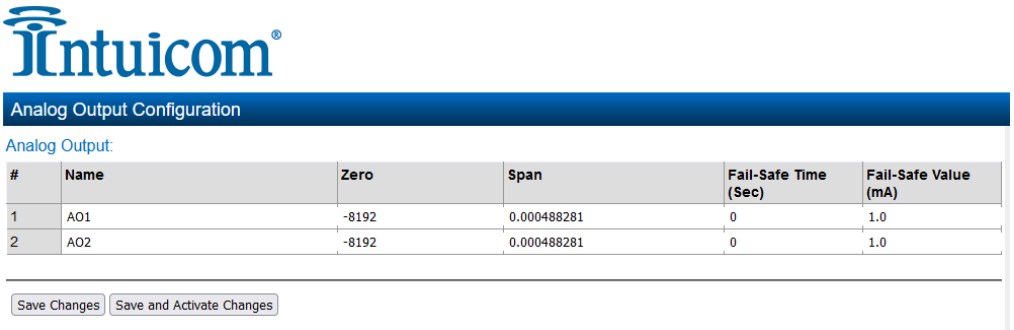
A – Onboard I/O

Click on the "Onboard I/O" link and the following webpage will load. From the I/O configuration webpage click on the I/O type you wish to configure.



I/O Configuration Webpage

1 – Analog Output Configuration



Analog Outputs Webpage

The Analog Outputs of the VUE Series have the following configuration parameters.

Name – The Outputs can be named to help with the configuration or use the default name. Limit is 30 characters including spaces.

Zero/Span – These variables will change the scale of the Analog Outputs.

Zero – Starting value of 8192 counts = -4.

Span – Number of mA per bit.

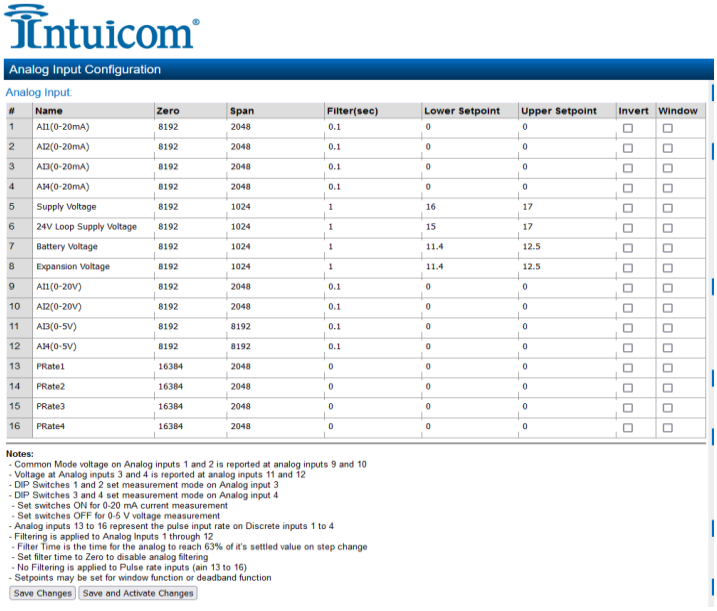
Engineering Range	Zero	Span
4-20mA	-4	$\frac{16mA}{32768}$ =.0004882815
0-20mA	-4	$\frac{20mA}{32768}$ =.0006103515

Calculating Span Values for mA range

Failsafe Time (sec) – The Fail-Safe Time is the time the output needs to count down before activating the failsafe state. Receiving an update or a COS message will reset the Fail Safe Timer back to its starting value. If the Fail-Safe Timer gets down to zero then the output will be set to the Fail-Safe state (mA).
It is recommended this Fail-Safe Time be configured for a little more than twice the update time of the input that is mapped to it, that way the output will reset if it fails to receive two update messages. Entering a zero in the Fail-Safe Time will disable.

Fail-Safe value (mA) – The value that you wish the output to be set to on activation of the failsafe timeout.

2 – Analog Input Configuration


Intuicom®

Analog Input Configuration

Analog Input:

#	Name	Zero	Span	Filter(sec)	Lower Setpoint	Upper Setpoint	Invert	Window
1	AI1(0-20mA)	8192	2048	0.1	0	0	☐	☐
2	AI2(0-20mA)	8192	2048	0.1	0	0	☐	☐
3	AI3(0-20mA)	8192	2048	0.1	0	0	☐	☐
4	AI4(0-20mA)	8192	2048	0.1	0	0	☐	☐
5	Supply Voltage	8192	1024	1	16	17	☐	☐
6	24V Loop Supply Voltage	8192	1024	1	15	17	☐	☐
7	Battery Voltage	8192	1024	1	11.4	12.5	☐	☐
8	Expansion Voltage	8192	1024	1	11.4	12.5	☐	☐
9	AI1(0-20V)	8192	2048	0.1	0	0	☐	☐
10	AI2(0-20V)	8192	2048	0.1	0	0	☐	☐
11	AI3(0-5V)	8192	8192	0.1	0	0	☐	☐
12	AI4(0-5V)	8192	8192	0.1	0	0	☐	☐
13	PRate1	16384	2048	0	0	0	☐	☐
14	PRate2	16384	2048	0	0	0	☐	☐
15	PRate3	16384	2048	0	0	0	☐	☐
16	PRate4	16384	2048	0	0	0	☐	☐

Notes:
- Common Mode voltage on Analog inputs 1 and 2 is reported at analog inputs 9 and 10
- Voltage at Analog inputs 3 and 4 is reported at analog inputs 11 and 12
- DIP Switches 1 and 2 set measurement mode on Analog input 3
- DIP Switches 3 and 4 set measurement mode on Analog input 4
- Set switches ON for 0-20 mA current measurement
- Set switches OFF for 0-5 V voltage measurement
- Analog inputs 13 to 16 represent the pulse input rate on Discrete inputs 1 to 4
- Filtering is applied to Analog Inputs 1 through 12
- Filter Time is the time for the analog to reach 63% of it's settled value on step change
- Set filter time to Zero to disable analog filtering
- No Filtering is applied to Pulse rate inputs (ain 13 to 16)
- Setpoints may be set for window function or deadband function

Save Changes | Save and Activate Changes

Analog Input Webpage

The VUE Series Analog inputs have the following configuration parameters.

Name – The inputs can be named to help with configuration or use the default, up to 30 characters including spaces.

Zero / Span – These variables will change the Scale of the Analog Inputs.

Zero – Starting Value (counts) when measured value is zero

Span – Number of counts per measured value (mA, V, Hz, etc)

Filter (sec) – The Filter time Constant is the time the analog takes to settle on a step changed of an analog value. By default, all the inputs except the Pulse Rates have a Time constant of 5 seconds. Pulsed input rates are not filtered.

Lower & Upper Setpoints – The upper and lower control point values that will be used to turn on and off the Analog Setpoint digital signals are located at register 10009 – 10020. Setpoint values are entered in the scale of the input, i.e. Analog input 1-4 will be in mA, Analog inputs 9-12 will be volts, etc.
The analogs inputs are controlled by using the setpoints and the two control options explained below. All analogs have these controlling setpoints and options.

The two main Setpoint control options are:

- **Deadband** (Default) - If the Analog Input is greater than the Upper Set point, the set-point status will be active (on, “1”). The setpoint will reset (off, “0”) when the Analog Input is less than the Lower Set Point. Note that the Upper Set Point must always be higher than the Lower Set Point.”
- **Windowed** – If the analog value is inside the upper and lower setpoints, the setpoint will be active (on, “1”), and if the analog value is outside of these setpoints the setpoint will be reset (off, “0”)

Invert –This option toggles the Setpoint control logic between the default normal and inverted state. The function does not change, only the operation is inverted, e.g. if setpoint is on in its normal state, inverting the signal will mean the setpoint will be off in the normal state.

Window – This option toggles the Set point operation between the default Dead band and Windowed modes.

The Analog is a linear scale with an overall Raw range of 8192 to 49152 decimal (Total = 40960). The input Engineering range can have many different forms i.e. 0-20mA, 0-5V, or 0-1000Hz which is why the zero and span can be scaled to give the correct Raw range.

a – Calculating Span

The Span is calculated by using the formula.

Span = Intuicom Raw Range / Engineering Range

The Raw range is the number of counts between minimum and maximum analog values. Intuicom standard is minimum= 8192 and maximum value is 49152 so the Range is 40960 counts (49152-8192).

The Engineering range will be the range of engineering units – 0-20mA = 20, 0-5V = 5

Some example Span calcs are:

If the Engineering range is 0-20mA (20) the Span would be 2048 (40960/20)

If the Engineering range is 4-20mA (16) the Span would be 2048 (40960/16)

If the Engineering range is 0-5V (5) the Span would be 8192 (40960/5)

b – Calculating Zero

The zero is calculated by using the formula -

Zero = Maximum Raw Intuicom Scale – (Maximum Engineering Value x Span).

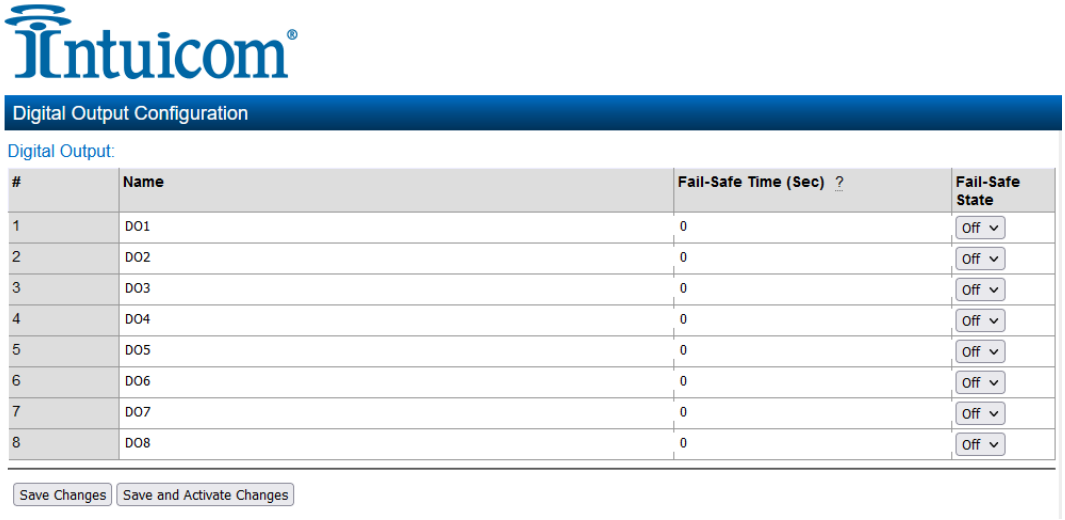
E.g. If the Engineering Range is 0-20mA the Engineering value will be 20. The span from the 0-20mA calculation above was 2048 therefore the Zero calculation will be 49152 – (20x2048) = 8192

For a 0-5V input the Engineering Value will be 5, the Span from the 0-5V calculation above was 8192 therefore the Zero calculation will be 49152 – (5x8192) = 8192

Input	Engineering Range	Raw Range (Total)	Zero	Span
AI1(4-20mA)	0-20mA	8192-49152 (40960)	8192	$\frac{40960}{20}$ =2048
AI3(0-5V)	0-5Volts	8192-49152 (40960)	8192	$\frac{40960}{20}$ =8192
Pulsed Rate1 (mA)	0-16mA	16384/49152 (32768)	16384	$\frac{40960}{16}$ =2048

Calculating Span Values for Raw Range

3 – Digital Output Configuration



Digital Output Configuration Webpage

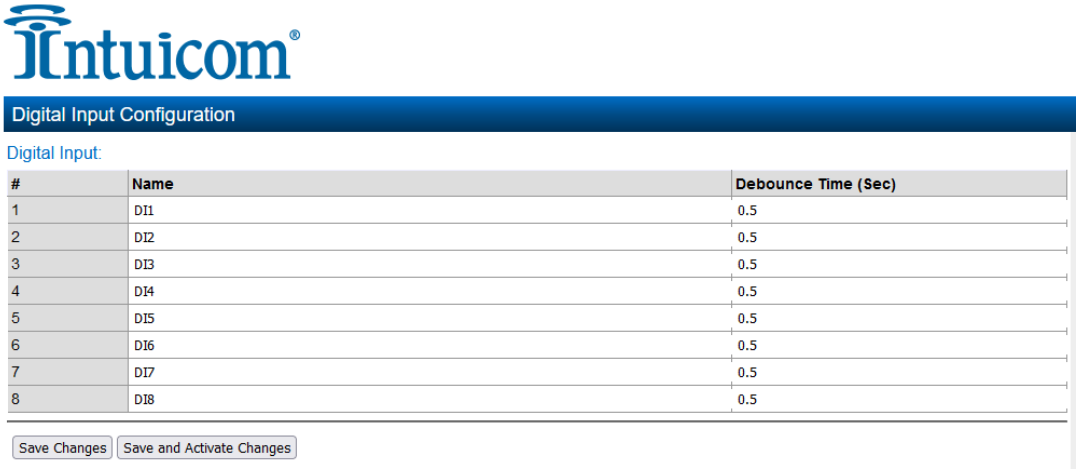
Name – The inputs can be named to help with configuration or use the default, up to 30 characters including spaces.

Failsafe Time (sec) – The Fail Safe Time is the time the output needs to count down before activating the failsafe state. Receiving an update or a COS message will reset the Fail Safe Timer back to its starting value. If the Fail Safe Timer gets down to zero then the output will be set to the Fail Safe state (ON or OFF)
It is recommended this Fail Safe Time be configured for a little more than twice the update time of the input that is mapped to it, that way the output will reset if it fails to receive two update messages.

Fail Safe State – The state that the output will go to after the 'Failsafe Time' has elapsed.
If the Failsafe state is enabled (ON) this will indicate with the LED flashing briefly OFF and the digital output will turn on.
If the Failsafe state is disabled (OFF) this will indicate with the LED flashing briefly ON and the digital output will turn off.

Save and Activate Changes – Once all the configurations are complete click "Save and Activate Changes to write the settings to the unit.

4 – Digital Input Configuration

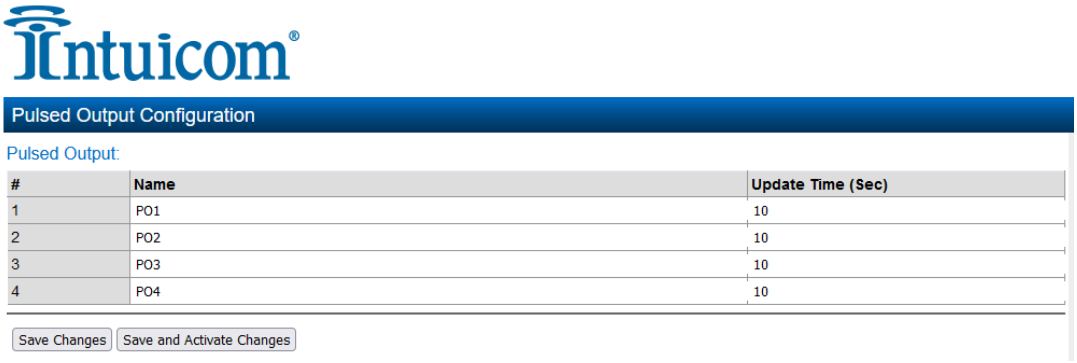


Digital Input Configuration Webpage

Name – The inputs can be named to help with configuration or use the default, up to 30 characters including spaces.

Debounce Time (sec) – Debounce is the time which an input must stay stable before the module decides that a change of state has occurred. If a digital input changes (on - off) and changes again (off - on) in less than the debounce time, then the module will ignore both changes. Default debounce time is .5 seconds.

5 – Pulsed Output Configuration



Pulsed Output Configuration Webpage

Name – The inputs can be named to help with configuration or use the default, up to 30 characters including spaces.

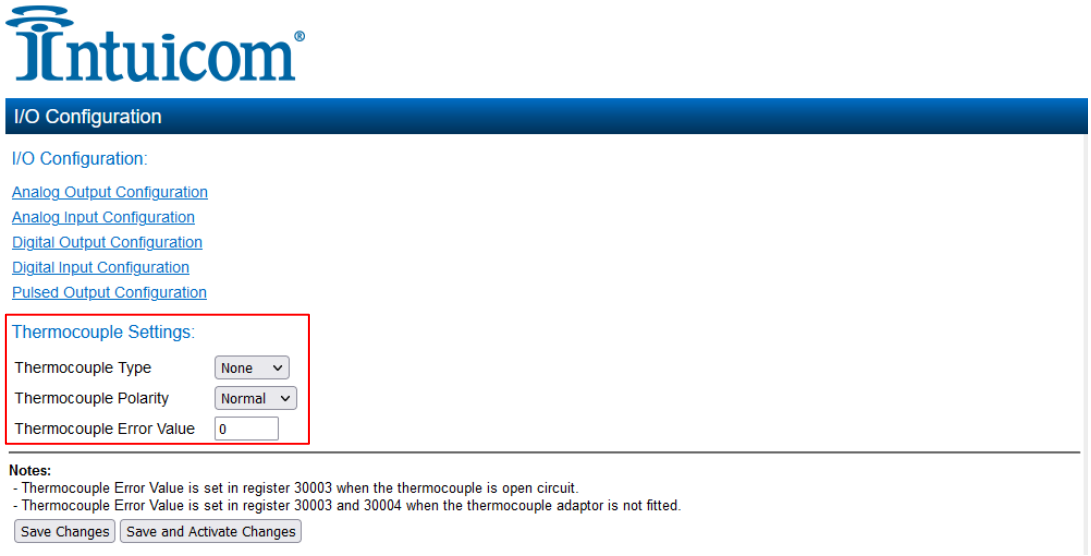
Update Time (sec) – Time that the output will be updated with the latest received value. The time is related to the update time of the pulsed input that is mapped to it. E.g. If the pulsed input update time is configured for 10 seconds the number of

pulses will be counted and send to the receiving module every 10 seconds. The receiving module will then output the pulse count over the configured update time, i.e.10 seconds

Save and Activate Changes – Once all the configurations are complete click "Save and Activate Changes to write the settings to the unit.

6 – Thermocouple Settings

On the "Onboard I/O webpage the Thermocouple Type selection and polarity are also selected.



- **Thermocouple Type** – Selects the type of Thermocouple – Type J, Type K, Type T or None.
- **Thermocouple Polarity** – Selects the Thermocoupld Polarity – Normal or Reverse.

Save and Activate Changes – Once all the configurations are complete click "Save and Activate Changes to write the settings to the unit.

B – (I/O) Mapping Configuration

Selecting "I/O Mappings" from the right hand side of the main menu will show the I/O Configuration webpage.
From here you can configure up to 200 x Read mappings, 200 x Write mappings and 200 x Gather/Scatter mappings as well as configure any Sensitivity Blocks.

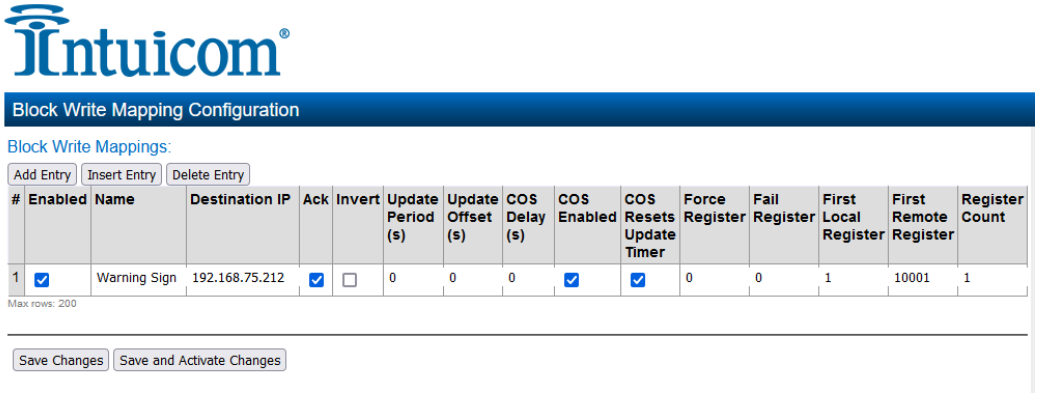
I/O Mappings Webpage

1 – Enable All Configured Mappings

To enable all configured mappings, place a checkmark in the box. See figure above.

2 – Mappings

a – Block Write Mappings



Block Write Mappings Configuration Webpage

Click Add Entry to create a new mapping.

Enabled – Write mappings can be enabled or disabled by adding or removing the checkmark from this field.

Name – Users can give each mapping a name for reference purposes.

Destination IP – This is the IP address that you wish to write the I/O to. If mapping from one VUE to another via radio connection, the destination IP address must be the radio IP address. If mapping via Ethernet port (or WAN) then the destination IP Address will be the Ethernet IP of the destination.

Ack – Selecting this box means the mapping will be acknowledged when the end device receives the message. This is an end-to-end acknowledgement, and is over and above the normal hop-by-hop frame acknowledgment between links.

Invert – This will allow the mapping to be inverted. E.g. if the digital input is on and inverted then the output will be off and visa versa. Applies to all of the I/O in the mapping and can only be used with Words and Bits, No Floating Point or Long values can be inverted.

Update Period (sec) – This is the period that the mappings are sent as an update or check signal. (Zero disabled updates)

Update Offset (sec) – Configures an offset time for the update mapping. Used to stagger the update transmissions so on start-up and every update period the module does not send all mapping at the same time. Default will be 0 however if configured a nominal offset time of around 5 seconds should be used.

COS (Change Of State) Delay – You can enter a delay period (in seconds) such that the message is delayed from sending for the configured time. Used to hold off the transmissions to allow more COS messages to be added to the mapping.

COS (Change Of State) Enabled – Can enable or disable the COS messages. If enabled the values will be sent on COS and if the value complies with any Sensitivity blocks (see Sections 0 “Sensitivity Block”). If COS is disabled, messages would only be sent on the update period.

COS Resets Update Timer – The Update Period Timer will be reset if this option is enabled and a COS is received in between updates, meaning it will not receive

another update until a further Update period has elapsed - Can help reduce the amount of radio traffic produced when multiple mappings are configured. Note: If the Turn on an I/P and at <30s past COS, check COS is sent 30s past change and old COS time is not used Turn on an I/P and at >30s past COS, check COS is only sent at the old COS time and not at 30s past the change or both.

Force Reg – Register location that when written to will force the Write Mapping to be sent. E.g., External device can initiate the transmissions. (reg 501 – 3000). Note: Do not use DIO's directly to force mappings. DIO's are continually refreshed which will trigger the mapping to be sent. If you wish to use a DIO you must map the DIO to a general I/O area (10501) and then use this register to force the mapping.

Fail Reg – Register location that indicates a failure to communicate with the configured remote Destination Address. Note: Register must be Bit register, i.e., Digital I/O or internal Bit registers (10501, 501, etc) also 'Ack' must be enabled.

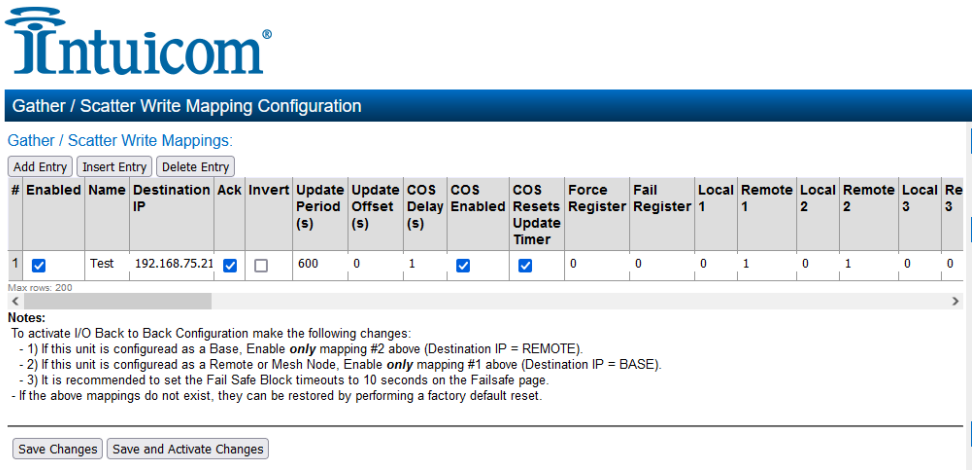
First Local Reg – Starting Local address that values will be written to.

First Remote Reg – Starting Remote address that the values will read from.

Reg Count – Total number of register values (consecutive).

Save and Activate Changes – Once all the configurations are complete click "Save and Activate Changes to write the settings to the unit.

b – Gather/Scatter Write Mappings



Gather/Scatter Write Mappings

Click Add Entry to create a new mapping.

Enabled – Write mappings can be enabled or disabled by adding or removing the checkmark from this field.

Name – Users can give each mapping a name for reference purposes.

Destination IP – This is the IP address that you wish to write the I/O to. If mapping VUE to another VUE via radio link, the destination IP address must be the radio IP address. Use the Ethernet IP of the destination if mapping via Ethernet port (or WAN).

Ack – Selecting this box will mean the mapping will be acknowledged when the end device gets the mapping. This is over and above the normal Ethernet frame acknowledgments between links.

Invert – This will allow the mapping to be inverted. E.g. if the digital input is on and inverted then the output will be off and visa versa. Applies to all the I/O in the mapping and can only be used with Words and Bits, No Floating Point or Long values.

Update Period – This is the period that the mappings are sent as an update or check signal.

Update Offset – Allows an offset to be configured for each mapping. Used to stagger the transmissions so on start-up the module does not try to send all mapping at the same time. Default will be 0 however the normal would be around 5 seconds.

COS (Change Of State) Delay – You can enter a delay period such that the message is delayed from sending for the configured time. Used to hold off the transmissions to allow more COS messages to be added to the mapping.

COS (Change Of State) Enabled – Can enable or disable the COS messaged. If disabled messages would only be sent on the update period.

COS Resets Update Timer – Enabling this timer will mean If a COS is received in between any updates it will reset the Update timer, meaning it will not receive

another update until the further Update period has passed.- used to reduce the amount of radio traffic.

Force Reg – Register location that when written to will force the Write Mapping to be sent. E.g. External device can initiate the transmissions. Note: Do not use DIO's directly to force mappings. DIO's are continually refreshed which will trigger the mapping to be sent. If you wish to use a DIO you must map the DIO to a general I/O area (10501) and then use this register to force the mapping.

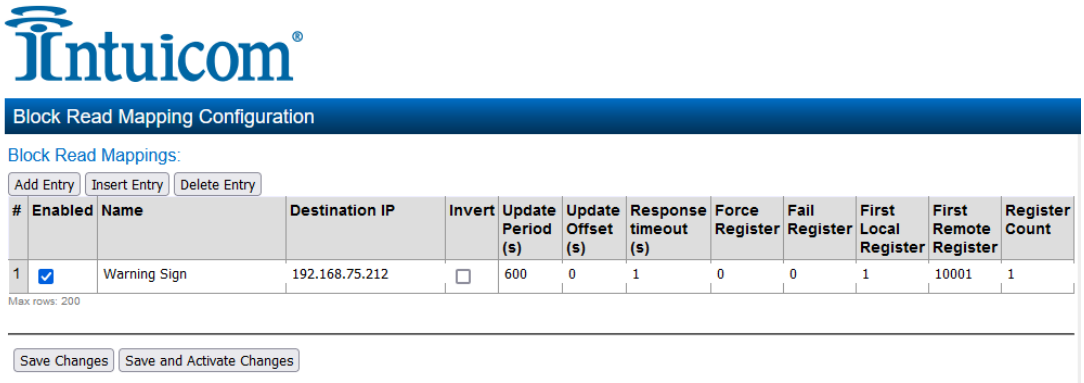
Fail Reg – Register location that indicates a failure to communicate with the configured remote Destination Address. Note: Register must be Bit register, i.e. Digital I/O or internal Bit registers (10501, 501, etc) also 'Ack' must be enabled.

Reg Count – Total number of register values (consecutive).

L1 & 12 0 L32 & R32 – Local and Remote pairs. Up to 32 scattered local I/O registers can be mapped to 32 scattered remote I/O registers.

Save and Activate Changes – Once all the configurations are complete click "Save and Activate Changes to write the settings to the unit.

c – Block Read Mappings



Block Read Mapping Configuration Webpage

Click Add Entry to create a new mapping.

Enable – Placing or removing checkmark from this box will enable or disable the mapping.

Name – This is a unique name so for reference purposes.

Destination IP – This is the IP address that you wish to write the I/O to. If mapping from one VUE to another VUE via radio, the destination IP address must be the radio IP address. If mapping via Ethernet port (or WAN) then the destination IP Address will be the Ethernet IP of the destination.

Ack – Selecting this box means the mapping will be acknowledged when the end device receives the message. This is an end-to-end acknowledgement, and is over and above the normal hop-by-hop frame acknowledgment between links.

Invert – This will allow the mapping to be inverted. E.g. if the digital input is on and inverted then the output will be off and visa versa. Applies to all of the I/O in the mapping and can only be used with Words and Bits, No Floating Point or Long values can be inverted.

Update Period (sec) – This is the period that the mappings are sent as an update or check signal. (Zero disabled updates).

Update Offset (sec) – Configures an offset time for the update mapping. Used to stagger the update transmissions so on start-up and every update period the module does not send all mapping at the same time. Default will be 0 however if configured a nominal offset time of around 5 seconds should be used.

COS (Change of State) Delay (sec) – You can enter a delay period such that the message is delayed from sending for the configured time. Used to hold off the transmissions to allow more COS messages to be added to the mapping.

COS (Change of State) Enabled – Can enable or disable the COS messages. If enabled the values will be sent on COS and if the value complies with any Sensitivity blocks (see Sections 0 “Sensitivity Block”). If COS is disabled, messages would only be sent on the update period.

COS Resets Update Timer – The Update Period Timer will be reset if this option is enabled and a COS is received in between updates, meaning it will not receive another update until a further Update period has elapsed – Can help reduce the amount of radio traffic produced when multiple mappings are configured.

NOTE: If the Turn on an I/P and at <30s past COS, check COS is sent 30s past change and old COS time is not used Turn on an I/P and at >30s past COS, check COS is only sent at the old COS time and not at 30s past the change or both.

Force Reg – Register location that when written to will force the Write Mapping to be sent. E.g. External device can initiate the transmissions. (reg 501 – 3000).

NOTE: Do not use DIO's directly to force mappings. DIO's are continually refreshed which will trigger the mapping to be sent. If you wish to use a DIO you must map the DIO to a general I/O area (10501) and then use this register to force the mapping.

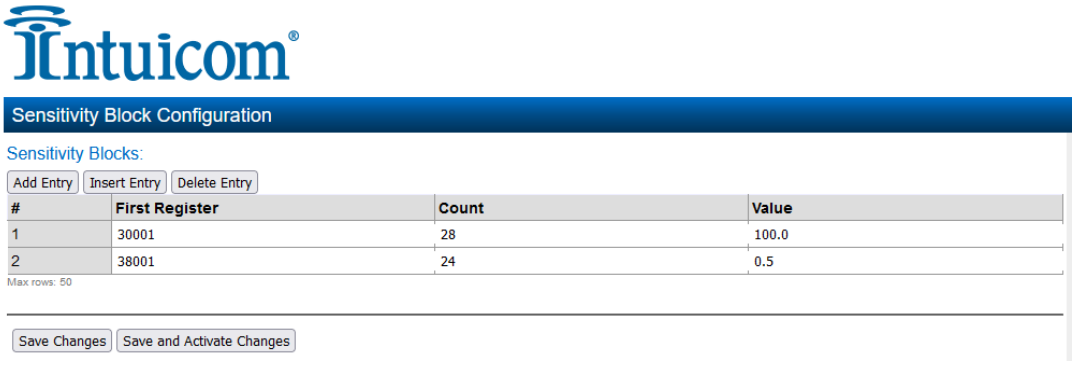
Fail Reg – Register location that indicates a failure to communicate with the configured remote Destination Address. Note: Register must be Bit register, i.e. Digital I/O or internal Bit registers (10501, 501, etc) also 'Ack' must be enabled.

First Local Reg – Starting Local address that values will be written to. First Remote Reg – Starting Remote address that the values will read from.

Reg Count – Total number of register values (consecutive)

Save and Activate Changes – Once all the configurations are complete click "Save and Activate Changes to write the settings to the unit.

d – Sensitivity Mappings



Sensitivity Block Configuration Webpage

All registers have a configurable "Sensitivity" value, which determines how much the register needs to change by before being sent as a "Change of State" (COS). All registers have a default sensitivity value of 1 except the following.

The 12 analog inputs have a sensitivity of 1000 (3.2%) and the 24 floating point values will have a default sensitivity of 0.5 units. In the case of 38001 – 38004 this will be 0.5mA, in the case of 38005-38012 it will be Volts and in 38013 – 38016 it will be Hertz. (The reason is so the module does not send every single bit change of an analog value and subsequently saturate the radio channel with unwanted change messages.
If a lower sensitivity is required then the above blocks can be adjusted and up to 48 more Sensitivity Blocks can be configured for different registers or different values.
They are configured as per the list below.

First Register – This is the starting register.

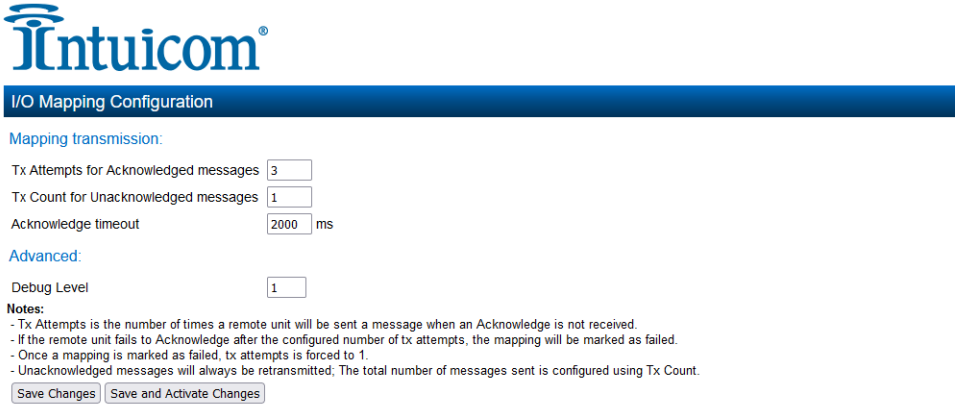
Count – Indicates the number of registers in the sensitivity block.

Value – This is the number of counts the value needs to change by to force a COS, e.g. a value of 1000 would be a change of 1000 counts in the total range (32768), which would represent about 3%.

Save and Activate Changes – Once all the configurations are complete click “Save and Activate Changes to write the settings to the unit.

e – Advanced Configuration

WIBMesh is an extremely efficient proprietary radio protocol used for radio communications. The protocol is based on the “Ad hoc On Demand Distance Vector” (AODV) routing algorithm which is a routing protocol designed for ad hoc networks. There is very little configuration for the WIBMesh as the protocol automatically routes through the mesh to the destination.



I/O Mapping Advanced Configuration Webpage

Tx Attempts for Acknowledged Messages – How many times the configured module will attempt to communicate a message to another module (message retries). After failing to communicate the module will be flagged as being in comms fail. If it tries to communicate to the remote module again, it will reduce the number of attempts down to one as it has been flagged as being in Comms fail. If communications is restored the module will go back to transmitting the number of time configured in "Tx Attempts for Acknowledged messages".

TX Count for Unacknowledged Messages – The number of times the radio transmits the same data message. It is used if the VUE has been setup as a transmit only module. It is done by not selecting the "Ack" tick box in any Block Write and Gather/Scatter Block mappings. (See "I/O Mappings" above) Being a Transmit only module there is no communication handshake between modules so transmitting the same message a number of times gives a greater reliability in communications.

Acknowledge Timeout – Time to wait for the Acknowledgement before the message is timed out. The default time is 2 Seconds but the time can be increased to 10 seconds for very long Mesh networks.

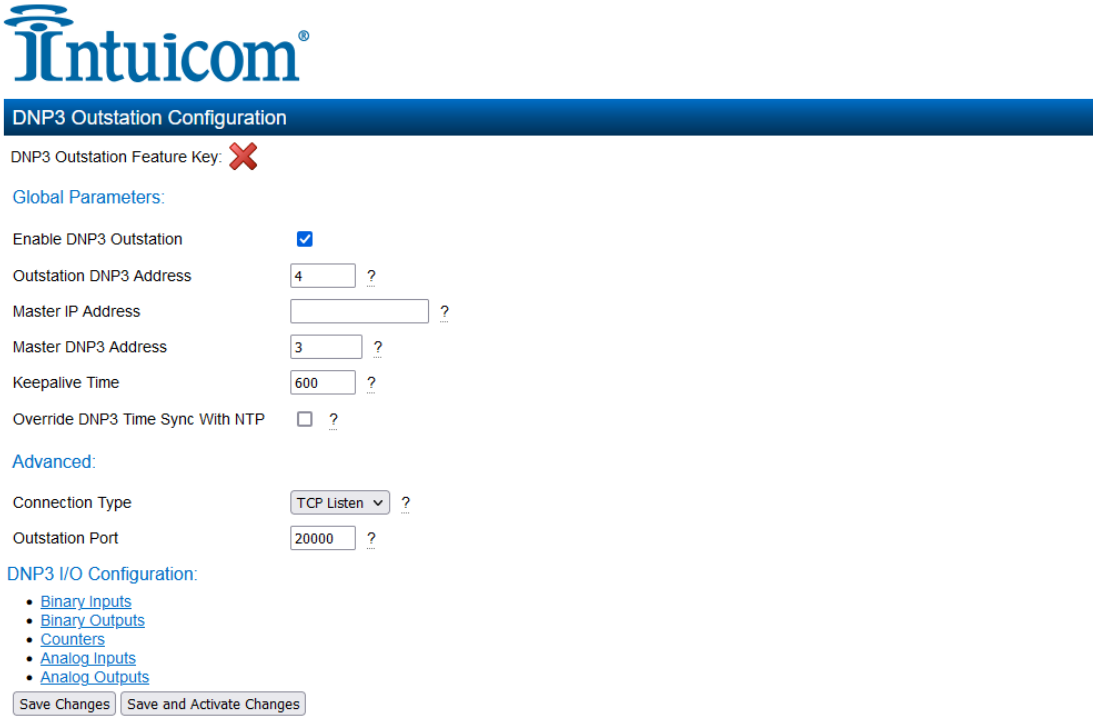
Debug Level – The level of debug information that can be shown via the serial port during normal operation and boot up. A value between 1 (only show normal operating parameters) and 8 (showing all debug messages)

Save and Activate Changes – Once all the configurations are complete click "Save and Activate Changes to write the settings to the unit.

C – DNP3 Outstation

The DNP3 protocol is widely used in many industries to provide monitoring and control of remote plants and equipment. You can enable support for DNP3 in VUE modules with the purchase of a feature license key (See License Keys page 114).

1 – Global Parameters



DNP3 Outstation Configuration Webpage

Enable DNP3 Outstation – Select this checkbox to enable the DNP3 function. Clear the checkbox to disable DNP3.

Outstation DNP3 Address – Sets DNP3 address of this VUE device. Set this address to match the address configured in the DNP3. Valid values are 1–65531.

Master IP Address – Sets the IP address of the DNP3 master station.
You do not need to set this parameter if the Connection Type is set to TCP Listen because the device will accept connections from any DNP3 master station with the address you specified in the Master DP3 Address field. If you are using TCP Listen and do not want to select a DNP3 master IP address, clear the Use checkbox to disable the Master IP Address.
The Master IP Address parameter is required if the Connection Type is set to UDP or TCP Dual.

NOTE: You also need to set the device's IP address to match the requirements of your system. For more information, see "Network settings" on page 43.

Master DNP3 Address – Sets the DNP3 address of the master station that will control the VUE device.

Keep Alive Time – Sets the keep alive time. The outstation (this device) sends a check transmission to the DNP3 master if there is no communication from the master within the keep alive time. To avoid unnecessary check transmissions, set the keep alive time to a longer period than the master poll time.

NOTE: If you are using a TCP connection, this parameter controls how long the outstation waits before it resets its TCP connection after the link is lost. If the master station drops its TCP connection through lost communications it cannot reconnect to the device until this timeout is completed. Setting the keep alive to a short time reduces the time to re-establish a connection. However, it also increases the number of check transmissions from outstations. For large networks with limited bandwidth, we recommend using the UDP connection type with a keep alive time that is longer than the master poll time.

Override DNP3 Time Sync with NTP – Placing a check mark in this box will enable the use of NTP time server for DNP3 synchronization over manually set date and time.

2 – Advanced
Connection Type – Sets the connection type to match your DNP3 master connection:

- **UDP** – Uses UDP Protocol to communicate with the master.
- **TCP Listen** – (Default) This option uses TCP protocol to communicate with the master. The device waits for a connection from the master.
- **TCP Dual** – Uses TCP protocol to communicate with the master. If the device loses connection it attempts to connect to the master at the configured IP address.

Outstation Port – Sets the TCP or UDP port number to use for the DNP3 outstation (this device). The standard port number for DNP3 is 20000. You only need to change this if your system uses a non-standard port number.

3 – DNP3 I/O Configuration

You can change the way that I/O data is reported by the VUE DNP3 outstation. By default, all the on-board I/O report as polling class 0 only (integrity poll). To enable event reporting of the I/O, you need to configure the I/O polling class. You may also want to change the dead band parameter for analog and counter inputs, and scaling for analog inputs and for analog outputs.
To configure a DNP3 I/O, click the I/O type under DNP3 in the project tree. There are five supported I/O types:

- Binary Inputs
- Binary Outputs
- Counters
- Analog Inputs
- Analog Outputs

NOTE: The VUE has a large number of registers that are not listed in the I/O configuration. By default, only physical I/O points can be accessed from the DNP3 master. You can add additional registers to the DNP3 point list by adding entries to the appropriate I/O configuration section.

When you add VUE-EX Expansion I/O modules to a VUE device configuration, the I/O of the VUE-EX device are automatically added to the DNP3 I/O list. You can add VUE-EX expansion I/O devices by clicking IO in the project tree. For more information, see “Adding an expansion I/O” on page 45 & 153 (Appendix D).

Every DNP3 I/O needs to be configured with a Register number and Poll Counting Class:

- **Register Number** – The register number relates the DNP3 I/O point to the register location within the device. You can determine the DNP3 point index of an I/O point by subtracting the base register number for that type of register. For example, the DNP3 point index for analog input #4 (register number 30004) is 30004 – 30001 = 3.

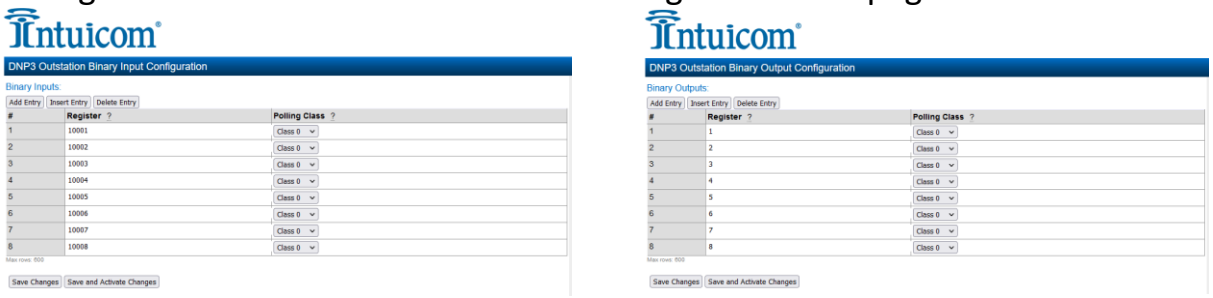
Register type	Base index
Binary Input	10001
Binary Output	1
Counters	36001
Analog Input	30001
Analog Output	40001

Register Type Base Index List

- **Polling Class** – The following options are available for polling class:
    - **No Class** – Points with this class can only be retrieved via an explicit read from the master. They are not reported in response to class polls from the master
    - **Class 0** – Points with this class have their current value reported in response to a class 0 poll from the master (integrity poll). No events are recorded for this class.
    - **Class 1, Class 2, Class 3** – Points in these classes are reported to the master station with time-stamped events in response to a corresponding poll from the master. Additionally, they have their current value reported in response to a class 0 poll in the same manner as for points configured with polling Class 0.

a – Binary Inputs and Binary Outputs

You can select which discrete input registers and output registers appear in the DNP3 point list. Discrete inputs appear in the VUE memory map in the range 10001–19999. Discrete outputs are in the VUE memory map in the range 1–9999. Use the Add, Edit, and Delete buttons to edit the list.
To configure binary inputs or binary outputs, click the option under DNP3 I/O Configuration on the DNP3 Outstation Configuration webpage.



Binary Inputs and Outputs Configuration Webpages

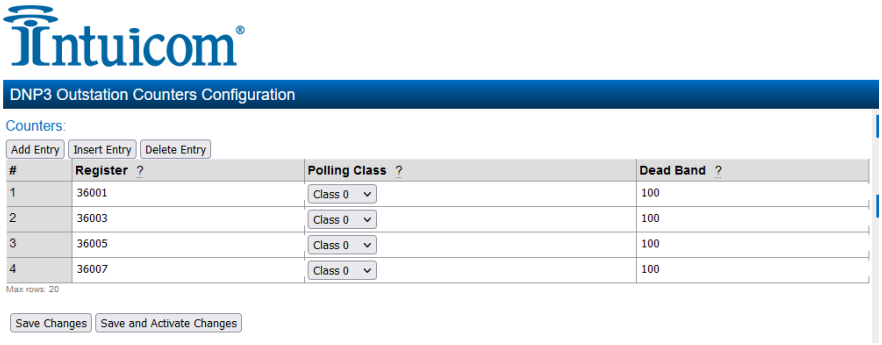
DNP3 Index – This is the number designated in the left column with the "#" symbol at the column header. This point index is used to access the I/O Data from the DNP3 master device.

Register – The I/O point register for the VUE unit. See "Register Number" on the previous page for more information.

Polling Class – See page 81 above for more information.

b – Counter Inputs

Counter inputs appear in the VUE address map in the range 36001–37999. Configure counter inputs in the DNP3 point list the same as you would digital inputs and digital outputs. For counters, you need to specify a dead band parameter in addition to a register number and polling class.
To configure counter inputs, click the Counters link on the DNP3 Outstation Configuration webpage.



DNP3 Counters Configuration Webpage

DNP3 Index – This is the number designated in the left column with the "#" symbol at the column header. This point index is used to access the I/O Data from the DNP3 master device.

Counter Register – The I/O point register in the VUE radio.

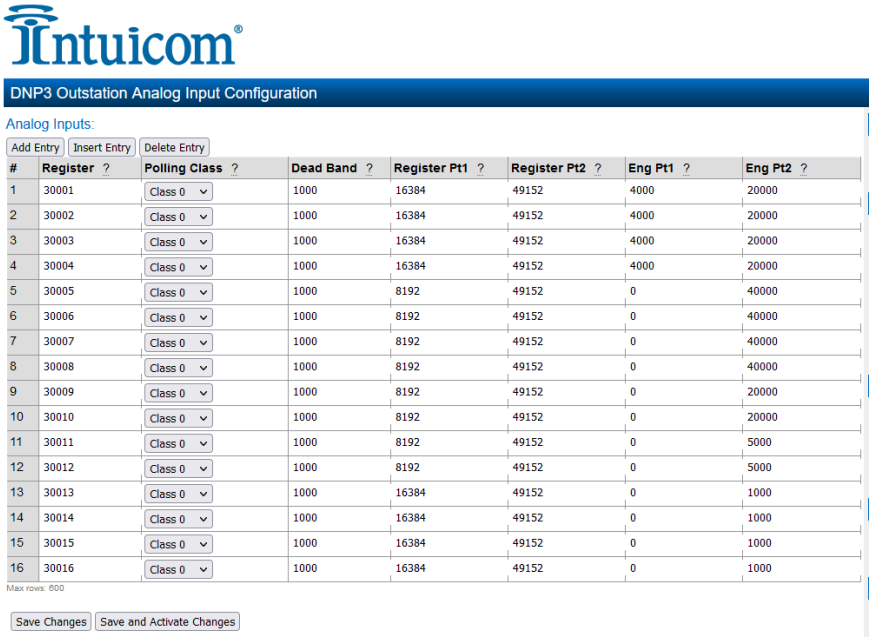
Polling Class – See page 81 above for more information.

Dead Band – The dead-band value limits the number of DNP3 event reports generated by the counter input when the counter is configured in polling class 1, 2, or 3. Once the counter generates a change event, no additional events are

generated until the counter value has changed by more than the dead-band value.

c – Analog Inputs

The configuration for analog inputs defines how change events are reported (dead band) and how the value is scaled when it is reported. The dead-band value limits the number of event reports generated by the analog input when the input is configured in polling class 1, 2, or 3. Once the analog input generates a change event, no additional events are generated until the register value has changed by more than the dead-band value.



#	Register ?	Polling Class ?	Dead Band ?	Register Pt1 ?	Register Pt2 ?	Eng Pt1 ?	Eng Pt2 ?
1	30001	Class 0	1000	16384	49152	4000	20000
2	30002	Class 0	1000	16384	49152	4000	20000
3	30003	Class 0	1000	16384	49152	4000	20000
4	30004	Class 0	1000	16384	49152	4000	20000
5	30005	Class 0	1000	8192	49152	0	40000
6	30006	Class 0	1000	8192	49152	0	40000
7	30007	Class 0	1000	8192	49152	0	40000
8	30008	Class 0	1000	8192	49152	0	40000
9	30009	Class 0	1000	8192	49152	0	20000
10	30010	Class 0	1000	8192	49152	0	20000
11	30011	Class 0	1000	8192	49152	0	5000
12	30012	Class 0	1000	8192	49152	0	5000
13	30013	Class 0	1000	16384	49152	0	1000
14	30014	Class 0	1000	16384	49152	0	1000
15	30015	Class 0	1000	16384	49152	0	1000
16	30016	Class 0	1000	16384	49152	0	1000

DNP3 Analog Inputs Configuration Webpage

Register – The I/O point register in the VUE device. For detailed description see page.

Polling Class – See page 81 for a description of the polling classes.

Dead Band – The dead-band value for the analog input, expressed as a desired change in the measured value. Changes to this field are reflected in the Dead Band field described above. You can edit either of these fields to set the dead band.

Register Pt1 – The register value for the first reference point. Default scaling on 4–20 mA analog inputs sets this to 16384 for 4 mA input current, and 49152 for 20 mA input current.

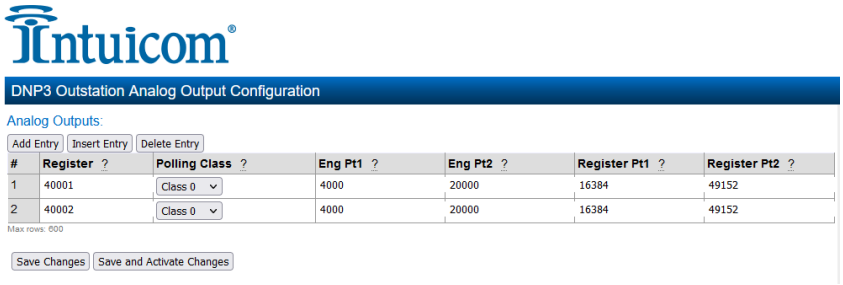
Register Pt2 – The register value for the second reference point.

Engineering Pt1 – The desired DNP3 value for the first reference point. Default scaling results in voltages being reported in mV, and currents being reported in microamps.

Engineering Pt2 – The desired DNP3 value for the second reference point.

d – Analog Outputs

The configuration for analog outputs defines any additional scaling that must be applied to the DNP3 value to set the correct register value. You can select default scaling to suit most applications, or configure custom scaling for the analog output if you need the value scaled to particular engineering units.
Physical analog outputs generate 4 mA for a register value of 16384, and 20 mA for a register value of 49152. The default scaling allows the DNP3 values to be sent as a µA value. For example, a DNP3 value of 4000 results in 4 mA; a DNP3 value of 20000 results in 20 mA output current.



DNP3 Analog Output Configuration Webpage

Register – The I/O point register in the VUE device. For a detailed description, see “Registers” on page 81

Poling Class – See page 81 for a description of the different polling classes

Engineering Pt1 – The DNP3 value for the first reference point. When this value is written by the DNP3 master, the VUE register receives the value in Register Low.

Engineering Pt2 – The DNP3 value for the second reference point. When this value is written by the DNP3 master, the VUE register receives the value in Register High.

Register Pt1 – The register value set in the VUE for the first reference point. The VUE memory register receives this value when the DNP3 master writes the value listed in Engineering Low.

Register Pt2 – The register value for the second reference point, corresponding to the DNP3 value in Engineering High.

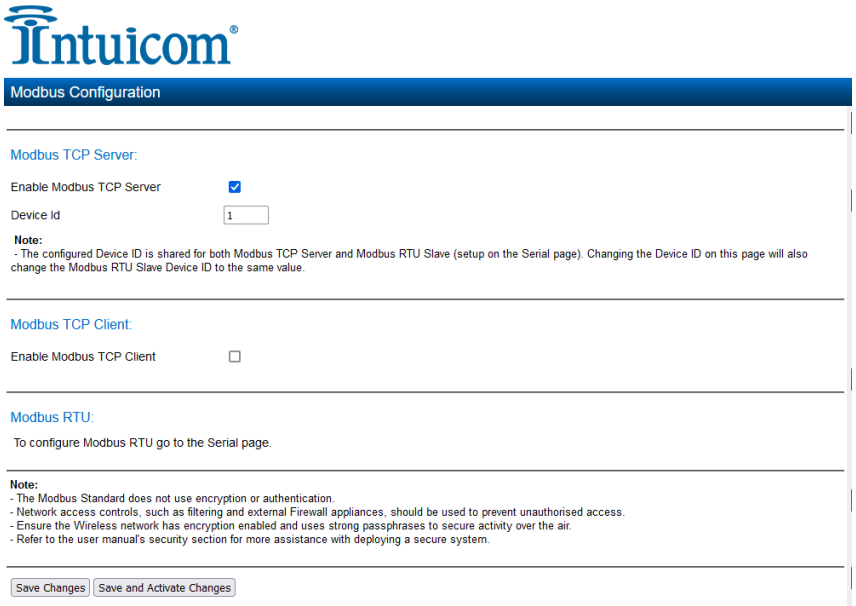
Save Changes – As each of the web pages for the DNP3 configuration are completed clicking "Save Changes" will save the settings until the full configuration is complete.

Save and Activate Changes – Once all the DNP3 configuration webpages are complete, click the "Save and Activate Changes" button to commit the changes to the VUE memory and activate them.

4 – Modbus TCP

The Modbus Configuration Webpage allows the VUE to be set up as:

- Modbus TCP Server
- Modbus TCP Client
- Modbus RTU



Modbus Configuration Webpage

Modbus TCP Server – Allows the VUE to accept connections from one or more Modbus TCP clients via Ethernet or RTU masters via the RS-485 or RS-232 serial interfaces. All Modbus transactions routed to the on-board Modbus TCP server/RTU slave are directed to/from the on-board general purpose I/O registers. The Modbus TCP server is shared with the Modbus TCP to RTU converter, so that the Modbus device ID is used to determine if a Modbus transaction is to be routed to the on-board Modbus TCP server or to a Modbus RTU device connected to the serial port. Care should be taken to ensure that all serially connected Modbus devices use different device IDs (for example, Modbus slave address), and the device ID is different than the onboard device ID. Up to 32 separate connections to the Modbus TCP server are supported.

Device ID - The device ID for the modules own Modbus server/ slave. This is the ID that any external Modbus client or Modbus master would require to allow it to read values from the internal Modbus registers (for example, if a DCS or SCADA computer needs to poll the VUE via TCP or serial connection).

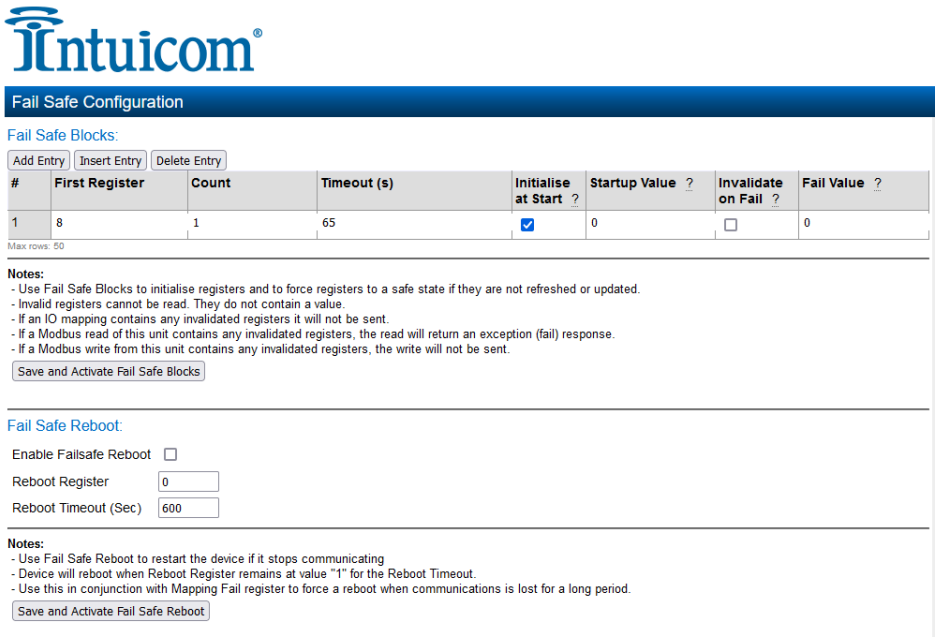
Modbus TCP Client – Allows you to configure the Modbus client mappings to communicate with remote TCP devices. Modbus TCP client functionality allows connections to a maximum of 24 different Modbus TCP servers, and up to 100 mappings can be configured.

Modbus RTU – Allows you to configure Modbus RTU mappings to communicate with remote serial Modbus devices. Configuration is completed on the Serial Webpage.

Save and Activate Changes – Once all the configurations are complete click “Save and Activate Changes” to write the settings to the unit.

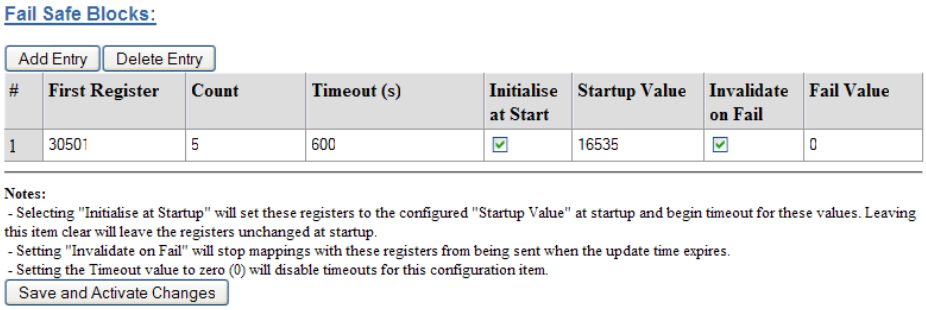
5 – Fail Safe Configuration

Fail Safe Block configuration allows registers to be set to a pre-configured value on start-up as well as configuring the outputs to reset to a predefined value after a timeout period has elapsed, when the real value comes in it will update as normal. Also if the value is lost because of a communication problem it can be configured to set the output to a failsafe value after the pre-configured time.



Fail Safe Configuration Webpage

a – Fail Safe Blocks



Fail Safe Blocks

In the screen shot above, register 30501 is an analog value that has been mapped from another module, it has an update interval of 1 minute.
On start-up this module will write a value of 16535 into register 30501 and then start counting down from the “Timeout” value (in this case 600 seconds).
If after 600 seconds, the module still has not received an update from the other module, register 30501 will be set to the “Fail Value” (in this case 0).
If the “Invalidate on Fail” were ticked, the value would be set to a null or invalidated value (~).
If this register was mapped to some other location the mapping would be inhibited until the” Invalid” value was updated with a real value.
The maximum number of Fail-Safe blocks you can have is 50.

First Register – This is the starting register

Count – Indicates the number of registers in the Fail Safe block.

Timeout – This is the starting timeout value in seconds. (setting value to 0 will disable the Timeouts).

Initialize at Start Up – Indicates that on start-up the Fail Safe Block registers will be set to the Start-up value.

Start Up Value – This is the value that the Fail Safe block registers will be set to on Start-up if the "Initialize at Start-up" is ticked.

Invalidate on Fail – If ticked will set the registers back to an Invalid state when failed. (See "Invalid Register State" above).

Fail Value – The value the register will be set to when the timeout has counted down. **NOTE:** "Invalidate on Fail" will override this value.

Save and Activate Changes – Once all the configurations are complete click "Save and Activate Changes" to write the settings to the unit.

b – Fail Safe Reboot

Failes Safe Reboot can be used to reboot the VUE if the radio stops communicating.

Enable Failsafe Reboot – To enable Failsafe Reboot place the check mark in the box.

Reboot Register – Enter a 1 into the register field, if the value remains at 1 for the Reboot Timeout period the device will reboot.

Reboot Timeout – The amount of time in seconds that communications can be down before the radio reboots itself.

NOTE: Use this in conjunction with Mapping Fail to force a reboot when communications fail for an extended period of time.

6 – Data and Event Logging Configuration

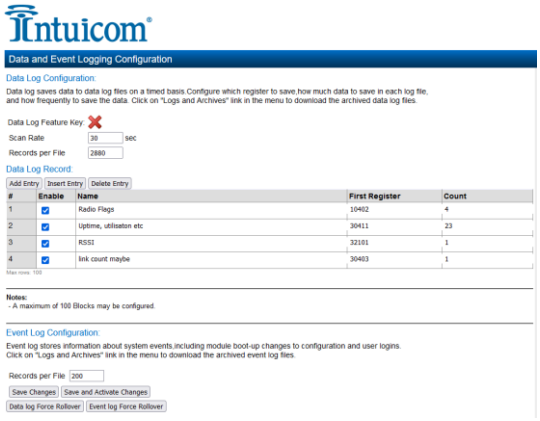
The data logging feature allows you to record the status of I/O registers on a regular basis. Data is saved to non-volatile memory, and can be retrieved at a later time. You can enable data logging on VUE modules with the purchase of a feature key license.

Data is logged to an internal data file in ".csv" format. Each row of the file is a single record, consisting of a timestamp and values of all of the configured log items at that time. When the file reaches a configured maximum number of rows, the file is "rolled," that is, the file is compressed and archived and a new log file is created.

The amount of memory available for storing logged data depends on the device type. The available data logging memory is indicated in the log files. When the memory is full, the oldest data log file is deleted.

The VUE series supports up to 500KByte of data log memory in compressed files.

NOTE: You need to be logged in as Administrator to configure data and event logging.



Data and Event Logging Configuration Webpage

Scan Rate – Enter the rate that you want data to be recorded (fastest rate is every 5 seconds).

Records Per File – Enter the maximum number of records you want in a file (up to 3,000 records per file). When the maximum is reached, the file is archived and a new data log file is created.

Data Log Record – Each entry in this table specifies a block of registers to be included in the log. To add an entry, click Add Entry and fill in the Name, First Register, and Count information. Select the Enable checkbox to enable data logging for the block. You can configure up to 100 register blocks. Use Delete to remove an entry that you no longer want. For and example see the table below.

Enable – When this checkbox is selected, data logging is enabled for this block of registers. When it is cleared, a placeholder symbol "-" is stored to the log file.

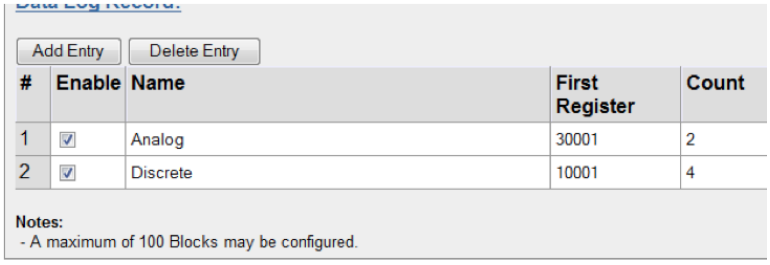
Name – Name to appear in the column heading within the log file to identify data for this entry. If no name is entered, the register number is used as the column heading.

First Register – Address of the first register to be logged.

Count – Number of registers to be logged.

Event Log Configuration – These settings apply only to modules that have the VUE – AT (Audit Trail) feature key enabled. Event Logging is discussed in a separate document.

The configuration example below The Data Log Record will log six registers in each log record. The Table Below shows an example of the logged data for this configuration.


Add Entry | Delete Entry

#	Enable	Name	First Register	Count
1	☑	Analog	30001	2
2	☑	Discrete	10001	4

Notes:
- A maximum of 100 Blocks may be configured.

Data Log Record – Example Configuration

Time stamp	Analog 01	Analog 02	Discrete 01	Discrete 02	Discrete 03	Discrete 04
2018-04-08 03:43:47	10476	33921	0	0	0	1
2018-04-08 03:43:47	10623	33923	1	1	0	1
2018-04-08 03:43:47	13923	33918	0	1	1	1
2018-04-08 03:44:02	10451	33922	0	1	1	0
2018-04-08 03:44:07	10773	33927	0	1	0	0

Data Log Example

Viewing Current Data – To view the latest logged data, click Logs and Archives on the home page of the Web-based configuration utility. The latest data is shown in a ".csv" format on the screen.

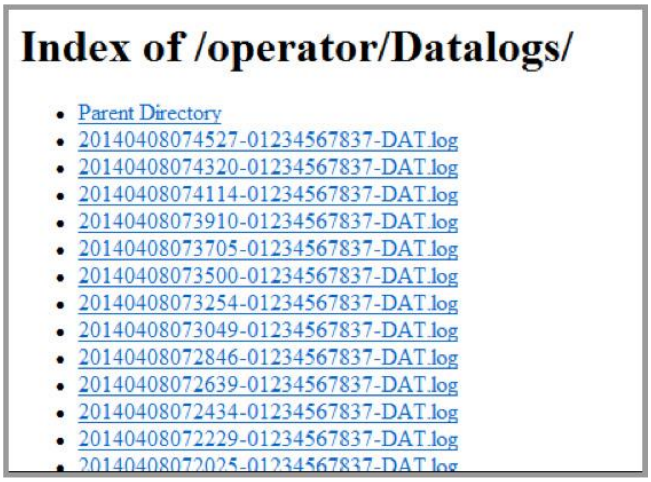
a – Retrieving Logged Data

The module supports remote retrieval of files via HTTP, as well as local retrieval of files via USB flash drive.

To Retrieve Logged Data Files via HTTP.

1) Click “Logs and Archives” on the Home Webpage.

2) Click the link “Click to download data log files.” This displays a listing of all of the stored data log files. Files are named with the time and date created and the module serial number, in the format yyyymmddhhmmss-nnnnnnnnnnn-DAT.log.



Data Log Listing

3) Right click the that you want to retrieve.

4) Click “Save Target as” to save the file to your local computer.

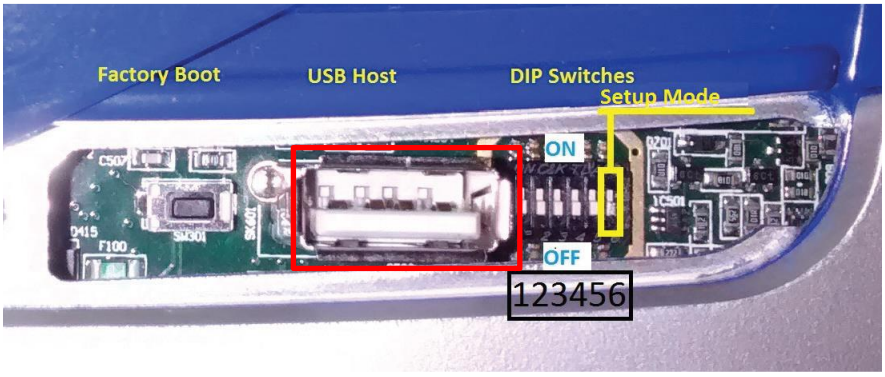
To Retrieve Logged Data Files using a USB drive.

1) Make sure that the USB drive is formatted for a FAT file system. This is the normal file system on USB drives.

2) Create a directory named “logs” (all lowercase) on the USB drive.

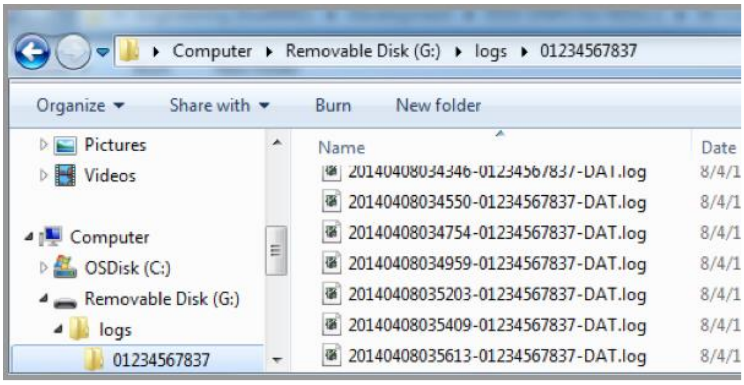
3) Using a small screwdriver, open the hatch on the side of the module.

4) Plug the USB drive into the USB Host port (see figure below). Within 10 seconds, the module should recognize the USB drive and the OK LED should flash red-green. If the module does not recognize the USB drive, check to make sure that the drive is formatted with FAT file system and that it contains a directory named “logs”. When the USB drive is recognized, the module copies the data log files to the USB drive. Once all files are copied, the OK LED turns solid green. The data log files are not deleted from the module when they are copied to USB drive. If the module encounters an error or if the USB drive does not have sufficient space to fit all of the files, the OK LED turns solid red to indicate a failure. Remove the USB drive and try another one until the files are successfully transferred and the OK LED turns green.



USB Port – Outlined in Red

5) Remove the USB drive from the module USB port. The log files are contained in a directory under the “logs” directory. This subdirectory is named with the module device name, or the module serial number if no device name was configured for the module. The device name is configured on the Module Information configuration page. The following example shows the contents of a USB drive after retrieving log files from a module. In this example, the module serial number is 01234567837.
You can leave the files on the USB drive. The next time you plug in the USB drive, only the new files are retrieved from the module. You can also use the same USB drive to retrieve data from multiple modules. The data for each module is stored in a separate directory.
If you configure your modules with a device name, the data is stored in a directory with that name. Take care that each module has a unique device name. Data from modules with the same device name will be stored in the same directory.



Log File Directory on USB drive

Retrieving Stored Log File Data

The log files are stored in comma-separated-value (.csv) format. To increase storage space, each log file is compressed using the Tar-Gzip method when it is stored to internal flash memory. The log files can be opened and the compressed .csv files recovered using an archive manager, such as 7-Zip, that can operate with Tar-Gzip (.tgz) files.

D – Serial

The VUE has an RS-232, and an RS-485 port for serial communications. These ports may be used to connect external Modbus RTU devices via the Modbus TCP to RTU Gateway and or VUE-EX serial expansion I/O modules. They may also be used to achieve serial to serial communications between VUE radios.

1 – RS-232 Serial Port Configuration

RS-232 Port Type – Settings available in the drop-down menu for RS232 port type are:

- **None** – Turns the port off when it is not in use.
- **Modbus RTU Master** – Sets the port as a master for a Modbus RTU network.
- **Expansion I/O** – Sets the port for communication with a VUE-EX module.
- **Modbus RTU Slave** – Sets the port to run as a slave on a Modbus RTU network.
- **Serial Gateway** – Sets the port to communicate with serial devices.
- **Modbus TCP/RTU Converter** – Sets the port to communicate with a Modbus RTU slave on a Modbus TCP network.

Every one of the available port type selections will need to have the following settings configured. These settings allow the serial port to communicate with the device connected to it. These setting must match the serial port settings on the connected device. These settings are:

- **Data Rate** – Also known as the baud rate, in Kbps – must be set the same as the device connected to the serial port.
- **Data Format** – Also known as the data bit, parity, and stop bit – Also must be set to match the device connected to the serial port.
- **Flow Control** – Options are None, and CTS/RTS – Again must be set to match the device connected to the serial port.

2 – RS-232 Additional Settings

When you change the port type setting the RS-232 additional settings title line changes and below provides you with the settings that are necessary for the port type selected.

Modbus RTU Master – When this port type is selected the header changes to "RS-232 Modbus Settings" and the settings below are:
Scan Rate – This is the time interval, in milli-seconds, that the RTU Master will wait between polling the RTU slaves. Default is set to 1000 msec.
Response Timeout – This is the time in milli-seconds that the RTU master will wait for a response before indicating a coms failure on the register. Default is set to 1000 msec.

RS-232 Modbus Master Mappings

When the port type is set to "Modbus RTU Master" a additional header appears with the title "RS-232 Modbus Master Mappings" These are the mappings for the Modbus slave devices directly connected to the master radios RS-232 port.


RS-232 Modbus Master Mappings:

Add Entry | Insert Entry | Delete Entry

#	Local Register	IO Count	Function Code	Destination Register	Device Id	Comm Fail Register
1	10001	1	16: Write Registers	1	1	0

Max rows: 100

RS-232 Modbus Master Mappings Configuration

Local Register – When the Function Code Modbus command is “Read” the Local Register field will be the destination register (output location) on the local device. When the Function Code command is “Write” the Local Register field will be the originating register (input location) on the local device. These are your Analog and Digital input/outputs that you enter into this field.

I/O Count – The number of consecutive I/O values in the mapping.

Function Code – The Function Code Modbus command determines if the command will be “Read” or “Write” and what type of register will be used. When entering a mapping, you need to select “Read” or “Write” from the drop-down list in the Command Type field, and then select one of the four radio buttons representing the register types. Selecting the register type will change the Destination (slave) register address range to a suitable range.

Destination Register – The register location on the RTU slave device. The register selection offered will be appropriate for the Modbus command selected in the Command field.

Device ID – The unit address (device ID) of the Modbus TCP server or Modbus RTU slave. Each device must have a unique ID.

Comm Fail Register – The Comms Fail indication register can be a physical output, such as DIO #1–8 (Reg 1-8), which will turn on a digital output when in fail. It can also be configured as an internal holding register (Reg 30501), which will show the fail indication as well as any Modbus error codes. This is useful for diagnosing communication problems. For Modbus error code descriptions, see “Modbus error codes” on page 155 (Appendix E).

RS-232 Expansion I/O

When port type of “Expansion I/O” is selected the only setting available is the Maximum Device ID to Poll.

Maximum Device ID to Poll - This is the maximum number of slave addresses that the Modbus Client will scan or poll for. Default is 3. If adding more that 3 VUE-EX expansion I/O modules this number will need to be increased.

RS-232 Modbus Slave Settings
When port type is set to "Modbus RTU Slave" the only setting available is the Modbus Slave ID.

Modbus Slave Device ID – The configured Device ID is shared for both Modbus RTU Slave and Modbus TCP Server (setup on the Modbus TCP page). Changing the Device ID on this page will also change the Modbus TCP Server Device ID to the same value.

Serial Gateway
When RS-232 port type is set to Serial Gateway, the options under for RS-232 Serial Gateway for "Serial Gateway Mode are as follows:

- **TCP Server** – This configures the VUE in listen mode where it will receive connections from clients that try to connect with the radio's serial port using a TCP connection initiated to the units IP Address and TCP Port number.
- **TCP Client** – This configures the radio so it will try and connect with a TCP server by IP Address and TCP Port number.
- **UDP Multicast** – This configures the VUE radios to connect with multiple radios over the serial port. All radios that will communicate via serial to serial connection must have the same multicast IP Address and port number.
- **UDP Point to Point** – This setting configures two VUE radios to communicate serial to serial with each other. The IP Address of the Base radio must be entered into the Remote radios "Remote Device IP Address" field. Additionally, the Remote radio's IP Address must be entered into the Base radio's "Remote Device IP Address field, and port numbers must match on both radios for serial to serial communication to take place.

TCP Server
Additional settings under "RS-232 Serial Gateway" below the "Serial Gateway Mode" drop down are:

Character Timeout (msec) – The amount of time the TCP Server radio will wait for the next character in the message. Upon expiration a new synchronization packet will be sent over the connection.

Packet Size (bytes) – This specifies the size of the packets in bytes used to transmit messages to and from the TCP Server. Smaller packet sizes will decrease throughput, and increase link reliability.

Listen Port – This is the TCP Port that the Server and Client will use for data transmission.

TCP Client
Additional settings under "RS-232 Serial Gateway" below the "Serial Gateway Mode" drop down are:

Character Timeout (msec) – The amount of time the TCP Server radio will wait for the next character in the message. Upon expiration a new synchronization packet will be sent over the connection. This setting must match on both client and server.

Packet Size (bytes) – This specifies the size of the packets in bytes used to transmit messages to and from the TCP Server. Smaller packet sizes will decrease throughput, and increase link reliability. This must match on the client and the server for data transmission to take place.
Listen Port – This is the TCP Port that the Server and Client will use for data transmission. This setting must match on both client and server for a TCP/IP connection to be made.

Remote Device IP Address – This is the IP Address of the TCP server that the TCP client is to connect with.

UDP Multicast
Additional settings under "RS-232 Serial Gateway" below the "Serial Gateway Mode" drop down are:

Character Timeout (msec) – The amount of time the TCP Server radio will wait for the next character in the message. Upon expiration a new synchronization packet will be sent over the connection. This setting must match on all radios in the UDP Multicast Group.

Packet Size (bytes) – This specifies the size of the packets in bytes used to transmit messages to and from the TCP Server. Smaller packet sizes will decrease

throughput, and increase link reliability. Again, this setting must match on all radios in the UDP Multicast Group.

Multicast Group Port – The port setting must be the same for all radios in the Multicast group for connections to be made.

Multicast Group IP Address – This setting must be the same for all radios in the Multicast group, and it must be set in the Multicast range (224.0.1.0 to 238.255.255.255).

WARNING – Multicast addressing is not like TCP/IP Addressing – for multicast communications to take place all devices in a multicast group must have the exact same multicast address and port number. If you set them different and make them unique address per radio, no communications will occur.

UDP Point to Point
Additional settings under "RS-232 Serial Gateway" below the "Serial Gateway Mode" drop down are:

Character Timeout (msec) – The amount of time the TCP Server radio will wait for the next character in the message. Upon expiration a new synchronization packet will be sent over the connection. This setting must match on both radios in the Point-to-Point connection.

Packet Size (bytes) – This specifies the size of the packets in bytes used to transmit messages to and from the TCP Server. Smaller packet sizes will decrease throughput, and increase link reliability. Again, this setting must match on both radios in the Point-to-Point connection.

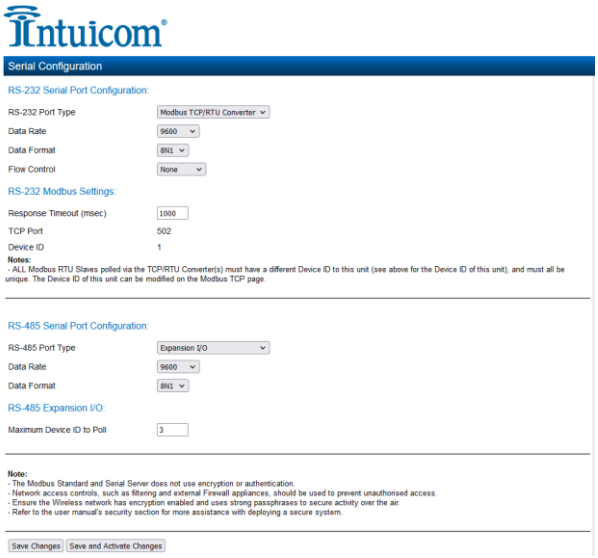
Remote Device Port – This is the UDP port that both radios will use to form the connection, and it must be set the same on both radios.

Remote Device IP Address – This setting is the IP Address configured on the remote radio. Both radios must have the IP Address entered in this field for their remote counterpart for communications to occur.

a – Modbus TCP to RTU Gateway

The Modbus TCP to RTU Gateway allows an Ethernet Modbus/TCP Client (Master) to communicate with a serial Modbus RTU Slave. The VUE makes this possible by internally performing the necessary protocol conversion. The conversion is always performed by the VUE, which is directly connected to the Modbus serial device (i.e. only this module needs to have Modbus TCP to RTU Gateway enabled – Port type set to Modbus TCP/RTU Converter).

The example below demonstrates how a Modbus/TCP Client (Master) can connect to one or more Modbus RTU (i.e. serial) Slaves. In this example the remote VUE is configured with the "RS232 Modbus/TCP to RTU Gateway" enabled

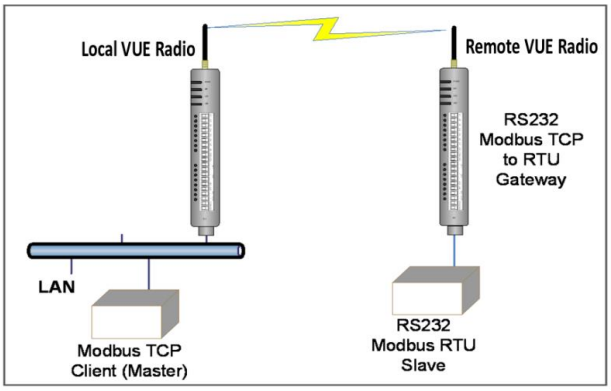


TCP to RTU Serial Port Configuration

Once enabled, the gateway converts the Modbus/TCP queries received from the Master into Modbus RTU queries and forwards these over the RS232 port to the Slave.

When the serial response to the query arrives from the Slave, it is converted to a Modbus/TCP response and forwarded via the network to the Modbus/TCP Master. If no response was received serially by the VUE within the configured Response Timeout, the VUE will initiate a number of retries specified by the configured Maximum Request Retries.

The Modbus TCP to RTU Gateway may be configured to operate on either the RS-232 or RS-485 port.



Modbus TCP to RTU

Response Timeout (msec) – Enter the serial response timeout in milliseconds – a serial retry will be sent if a response is not received within this timeout.

TCP Port – Enter the TCP port number used by the VUE to establish coms to the device connected to the serial port. This same port number must also be entered on the Modbus TCP Master radio.

Device ID – Enter a unique device ID for the Modbus RTU slave connected to the VUE.

b – RS-485 Serial Port Configuration

RS-485 Port Type – By default the port type is set to Expansion I/O. Settings available in the drop-down menu for RS232 port type are:

- **None** – Turns the port off when it is not in use.
- **Modbus RTU Master** – Sets the port as a master for a Modbus RTU network.
- **Expansion I/O** – Sets the port for communication with a VUE-EX module.
- **Modbus RTU Slave** – Sets the port to run as a slave on a Modbus RTU network.
- **Serial Gateway** – Sets the port to communicate with serial devices.
- **Modbus TCP/RTU Converter** – Sets the port to communicate with a Modbus RTU slave on a Modbus TCP network.

Every one of the available port type selections will need to have the following settings configured. These settings allow the serial port to communicate with the

device connected to it. These setting must match the serial port settings on the connected device. These settings are:

- **Data Rate** – Also known as the baud rate, in Kbps – must be set the same as the device connected to the serial port.
- **Data Format** – Also known as the data bit, parity, and stop bit – Also must be set to match the device connected to the serial port.
- **Flow Control** – Options are None, and CTS/RTS – Again must be set to match the device connected to the serial port.

c – RS-485 Additional Settings

When you change the port type setting the RS-485 additional settings title line changes and below provides you with the settings that are necessary for the port type selected.

Modbus RTU Master – When this port type is selected the header changes to "RS-485 Modbus Settings" and the settings below are:

Scan Rate – This is the time interval, in milli-seconds, that the RTU Master will wait between polling the RTU slaves. Default is set to 1000 msec.

Response Timeout – This is the time in milli-seconds that the RTU master will wait for a response before indicating a coms failure on the register. Default is set to 1000 msec.

RS-485 Modbus Master Mappings

When the port type is set to "Modbus RTU Master" a additional header appears with the title "RS-485 Modbus Master Mappings" These are the mappings for the Modbus slave devices directly connected to the master radios RS-485 port.

RS-485 Modbus Master Mappings Configuration

Local Register – When the Function Code Modbus command is "Read" the Local Register field will be the destination register (output location) on the local device.

When the Function Code command is “Write” the Local Register field will be the originating register (input location) on the local device. These are your Analog and Digital input/outputs that you enter into this field.

I/O Count – The number of consecutive I/O values in the mapping.

Function Code – The Function Code Modbus command determines if the command will be “Read” or “Write” and what type of register will be used. When entering a mapping, you need to select “Read” or “Write” from the drop-down list in the Command Type field, and then select one of the four radio buttons representing the register types. Selecting the register type will change the Destination (slave) register address range to a suitable range.

Destination Register – The register location on the RTU slave device. The register selection offered will be appropriate for the Modbus command selected in the Command field.

Device ID – The unit address (device ID) of the Modbus TCP server or Modbus RTU slave. Each device must have a unique ID.

Comm Fail Register – The Comms Fail indication register can be a physical output, such as DIO #1–8 (Reg 1-8), which will turn on a digital output when in fail. It can also be configured as an internal holding register (Reg 30501), which will show the fail indication as well as any Modbus error codes. This is useful for diagnosing communication problems. For Modbus error code descriptions, see “Modbus error codes” on page 155 (Appendix E).

RS-485 Expansion I/O

When port type of “Expansion I/O” is selected the only setting available is the Maximum Device ID to Poll.

Maximum Device ID to Poll - This is the maximum number of slave addresses that the Modbus Client will scan or poll for. Default is 3. If adding more that 3 VUE-EX expansion I/O modules this number will need to be increased.

RS-485 Modbus Slave Settings

When port type is set to “Modbus RTU Slave” the only setting available is the Modbus Slave ID.

Modbus Slave Device ID – The configured Device ID is shared for both Modbus RTU Slave and Modbus TCP Server (setup on the Modbus TCP page). Changing the Device ID on this page will also change the Modbus TCP Server Device ID to the same value.

Serial Gateway
When RS-232 port type is set to Serial Gateway, the options under for RS-232 Serial Gateway for "Serial Gateway Mode are as follows:

- **TCP Server** – This configures the VUE in listen mode where it will receive connections from clients that try to connect with the radio's serial port using a TCP connection initiated to the units IP Address and TCP Port number.
- **TCP Client** – This configures the radio so it will try and connect with a TCP server by IP Address and TCP Port number.
- **UDP Multicast** – This configures the VUE radios to connect with multiple radios over the serial port. All radios that will communicate via serial to serial connection must have the same multicast IP Address and port number.
- **UDP Point to Point** – This setting configures two VUE radios to communicate serial to serial with each other. The IP Address of the Base radio must be entered into the Remote radios "Remote Device IP Address" field. Additionally, the Remote radio's IP Address must be entered into the Base radio's "Remote Device IP Address field, and port numbers must match on both radios for serial to serial communication to take place.

TCP Server
Additional settings under "RS-232 Serial Gateway" below the "Serial Gateway Mode" drop down are:

Character Timeout (msec) – The amount of time the TCP Server radio will wait for the next character in the message. Upon expiration a new synchronization packet will be sent over the connection.

Packet Size (bytes) – This specifies the size of the packets in bytes used to transmit messages to and from the TCP Server. Smaller packet sizes will decrease throughput, and increase link reliability.

Listen Port – This is the TCP Port that the Server and Client will use for data transmission.

TCP Client
Additional settings under “RS-232 Serial Gateway” below the “Serial Gateway Mode” drop down are:

Character Timeout (msec) – The amount of time the TCP Server radio will wait for the next character in the message. Upon expiration a new synchronization packet will be sent over the connection. This setting must match on both client and server.

Packet Size (bytes) – This specifies the size of the packets in bytes used to transmit messages to and from the TCP Server. Smaller packet sizes will decrease throughput, and increase link reliability. This must match on the client and the server for data transmission to take place.

Listen Port – This is the TCP Port that the Server and Client will use for data transmission. This setting must match on both client and server for a TCP/IP connection to be made.

Remote Device IP Address – This is the IP Address of the TCP server that the TCP client is to connect with.

UDP Multicast
Additional settings under “RS-232 Serial Gateway” below the “Serial Gateway Mode” drop down are:

Character Timeout (msec) – The amount of time the TCP Server radio will wait for the next character in the message. Upon expiration a new synchronization packet will be sent over the connection. This setting must match on all radios in the UDP Multicast Group.

Packet Size (bytes) – This specifies the size of the packets in bytes used to transmit messages to and from the TCP Server. Smaller packet sizes will decrease throughput, and increase link reliability. Again, this setting must match on all radios in the UDP Multicast Group.

Multicast Group Port – The port setting must be the same for all radios in the Multicast group for connections to be made.

Multicast Group IP Address – This setting must be the same for all radios in the Multicast group, and it must be set in the Multicast range (224.0.1.0 to 238.255.255.255).

WARNING – Multicast addressing is not like TCP/IP Addressing – for multicast communications to take place all devices in a multicast group must have the exact same multicast address and port number. If you set them different and make them unique address per radio, no communications will occur.

UDP Point to Point

Additional settings under "RS-232 Serial Gateway" below the "Serial Gateway Mode" drop down are:

Character Timeout (msec) – The amount of time the TCP Server radio will wait for the next character in the message. Upon expiration a new synchronization packet will be sent over the connection. This setting must match on both radios in the Point-to-Point connection.

Packet Size (bytes) – This specifies the size of the packets in bytes used to transmit messages to and from the TCP Server. Smaller packet sizes will decrease throughput, and increase link reliability. Again, this setting must match on both radios in the Point-to-Point connection.

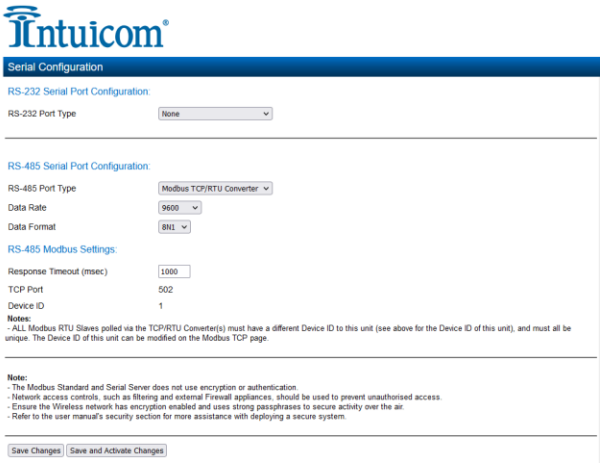
Remote Device Port – This is the UDP port that both radios will use to form the connection, and it must be set the same on both radios.

Remote Device IP Address – This setting is the IP Address configured on the remote radio. Both radios must have the IP Address entered in this field for their remote counterpart for communications to occur.

Modbus TCP to RTU Gateway

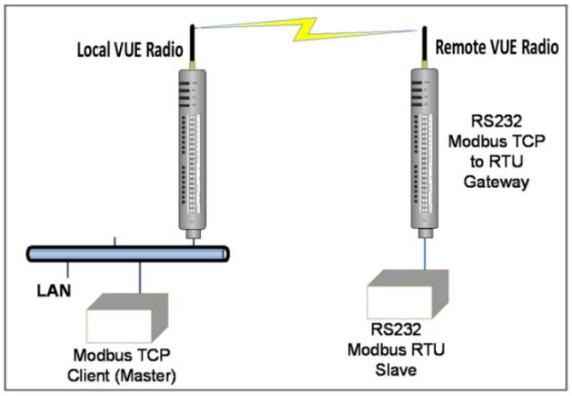
The Modbus TCP to RTU Gateway allows an Ethernet Modbus/TCP Client (Master) to communicate with a serial Modbus RTU Slave. The VUE makes this possible by internally performing the necessary protocol conversion. The conversion is always performed by the VUE, which is directly connected to the Modbus serial device

(i.e. only this module needs to have Modbus TCP to RTU Gateway enabled – Port type set to Modbus TCP/RTU Converter).
The example below demonstrates how a Modbus/TCP Client (Master) can connect to one or more Modbus RTU (i.e. serial) Slaves. In this example the remote VUE is configured with the "RS232 Modbus/TCP to RTU Gateway" enabled



TCP to RTU Serial Port Configuration

Once enabled, the gateway converts the Modbus/TCP queries received from the Master into Modbus RTU queries and forwards these over the RS232 port to the Slave.
When the serial response to the query arrives from the Slave, it is converted to a Modbus/TCP response and forwarded via the network to the Modbus/TCP Master. If no response was received serially by the VUE within the configured Response Timeout, the VUE will initiate a number of retries specified by the configured Maximum Request Retries.
The Modbus TCP to RTU Gateway may be configured to operate on either the RS-232 or RS-485 port.



Modbus TCP to RTU

Response Timeout (msec) – Enter the serial response timeout in milliseconds – a serial retry will be sent if a response is not received within this timeout.

TCP Port – Enter the TCP port number used by the VUE to establish coms to the device connected to the serial port. This same port number must also be entered on the Modbus TCP Master radio.

Device ID – Enter a unique device ID for the Modbus RTU slave connected to the VUE.

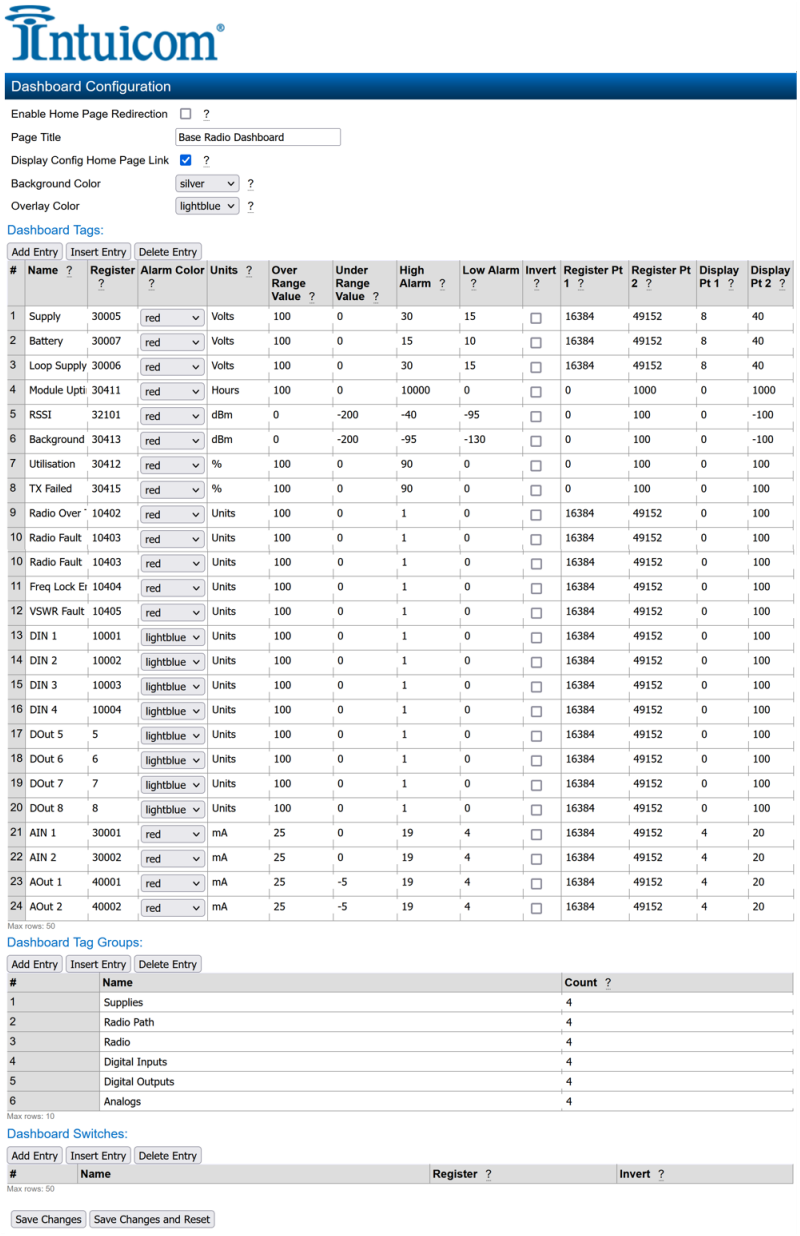
Save Changes and Reset – Once the changes are complete on the Network Configuration webpage a reboot is required to commit the changes. Click “Save Changes and Reset” to complete and commit the changes.

E – Dashboard

The VUE provides a dashboard feature to allow users to remotely access a view of the status of the device's I/O and registers. Any authorized user can access the device's dashboard remotely using a Web-browser. You configure which registers will be displayed on the dashboard, and how they will be displayed.

To access the dashboard, use a Web-browser to browse to the device's IP address. The dashboard display updates automatically.

To configure the dashboard display, select the "Dashboard" link under the "Configuration" header, in the right column of links on the web interface.



Dashboard Configuration Webpage

1 – Dashboard Configuration

The following list is an overview of the available Dashboard settings. You will need to configure these items for the entire dashboard page.

Enable Home Page Redirection – Checking this button makes future access to the device's IP address directly to the dashboard. This simplifies access to the dashboard for users that are unfamiliar with the product. If this button is left unchecked, accessing the device will take users to the device's home page. (From the home-page, you can still access the dashboard by clicking a link to view the dashboard).

Page Title – This is the title that will be displayed at the top of the dashboard view.

Display Configuration Home Page Link – If this is selected, the dashboard view provides a link labeled "Configuration". This provides a link to the device's regular home page. If you don't want your users to have easy access to the device's home page, then un-check this button.

NOTE: You can still access the home page by typing in full address to your browser bar: http://<Device_IPAddress>/operator/main.asp

Background Color – Changes the background color to one of the selections in the drop-down menu.

Overlay Color – Changes the overlay color to one of the selections in the drop-down menu.

Add Entry – Depressing this button adds an additional line for configuration in the Dashboard Tags table.

Insert Entry – Depressing this button inserts and entry into the Dashboard Tags table, and allows you to move entries up and down in the table.

Delete Entry – Deletes an entry from the Dashboard Tags table.

NOTE: To Edit a Row highlight it and click into the field you want to change and edit the entry.

Name – The item name displayed on the dashboard display.

Register – This is the register that will be displayed on the dashboard. Use the drop-down to select from named registers, or use the button to display a full dialog to select any device register.

Alarm Color – Allows you to select the color of the Alarm display.

Units – (Analog Registers Only) If the test to display for units.

Over/Under Range Value – If displayed value moves beyond these values, the dashboard item displays in red. For Digital registers, set these both to 0 to disable. Set High alarm to 1 to alarm with ON state, and set Low alarm to 1 to alarm with OFF state.

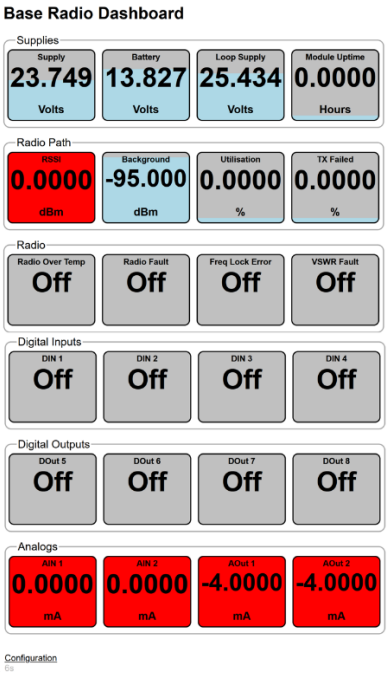
Invert – For digital registers, use this to invert the state, so that ON displays when the input is off, and vice-versa.

Register/Display Point 1/2 – For Analog registers, these four values set the display scaling. You configure two points which define what value will be displayed as the register value changes. Refer to section “Internal I/O” and “Analog Inputs” for more detail on how the measured value is represented in the registers.

Dashboard Tag Groups

Dashboard Tag Groups are used to configured the number of alarms and name of the display lines on the webpage. On the webpage above (page 106), the first 4 alarms in the table are power supply or voltage alarms – They are given the name Supplies and the number of displays on line 1 of the Dashboard webpage is 4, which correspond to the first 4 entries in the table.

The next four entries in the table are for “Radio Path” displays, so the name is set to “Radio Paths” and the count is set to 4. The next four lines in the table will now be displayed on the Dashboard second line down with the title “Radio Paths”.



Dashboard Webpage – First Row 4 Supplies Alarms

If you only had 3 Supply alerts in the first three entries of the table, and 5 Radio Path Alarms, you could set the count to 3 and 5 respectively, and those would then display row 1 with three alerts, and row 2 with five.

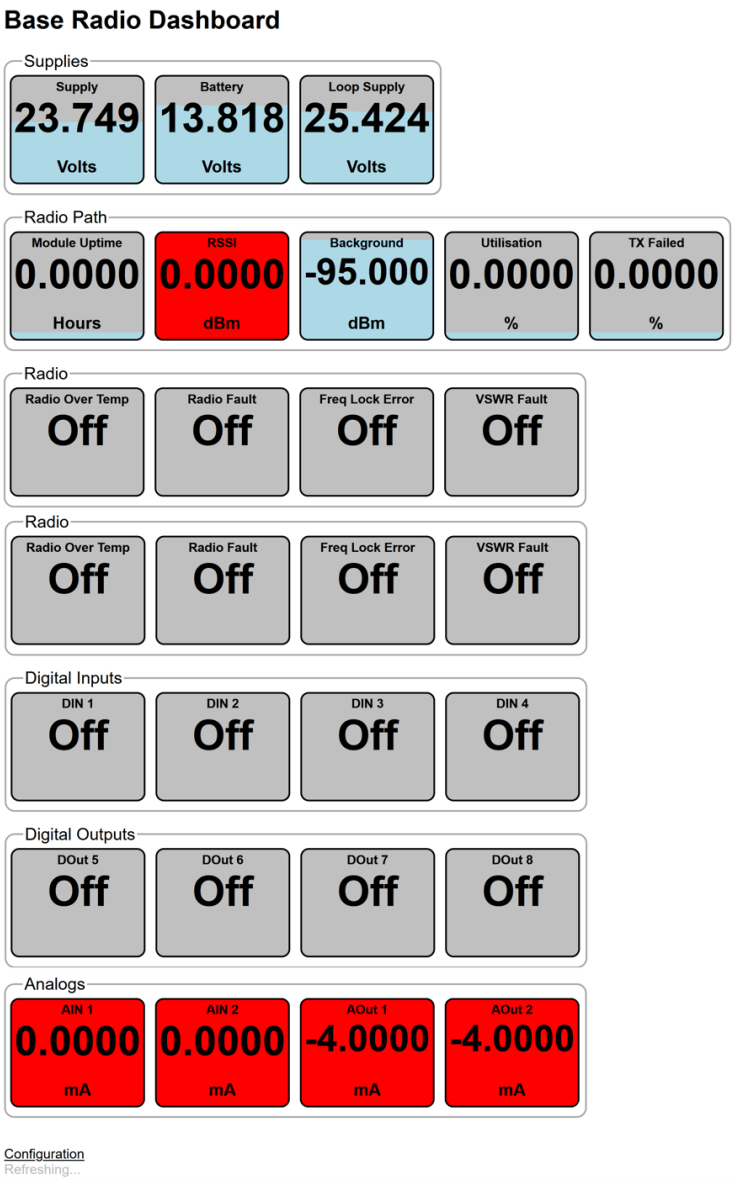
Dashboard Tag Groups:

Add Entry | Insert Entry | Delete Entry

#	Name	Count ?
1	Supplies	3
2	Radio Path	5
3	Radio	4
4	Digital Inputs	4
5	Digital Outputs	4
6	Analogs	4

Max rows: 10

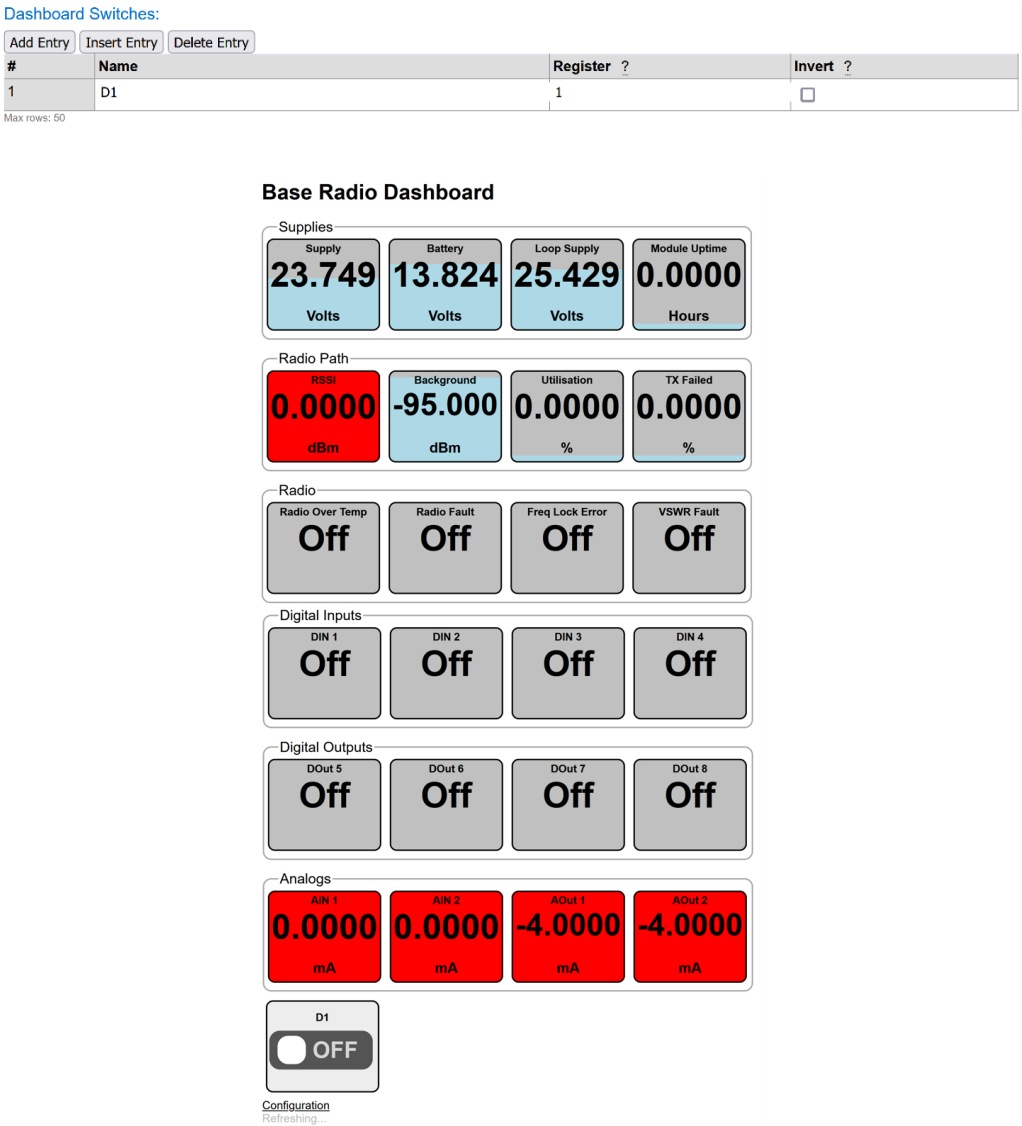
Dashboard Tag Groups – 1 set to 3 count and 2 set to 5 count



Dashboard Display after changing Dashboard Tag Counts

Dashboard Switches

The VUE also has the capability of adding switches to the Dashboard Webpage that will allow you to turn the Digital Input/Outputs on and off by clicking on the switch on the web page. Below and entry has been added for Registry 1 so a switch will now display at the bottom of the Dashboard giving users the capacity to manually turn D1 off and on. For D2 you would use Registry number 2, D3 Registry number 3 and so on.

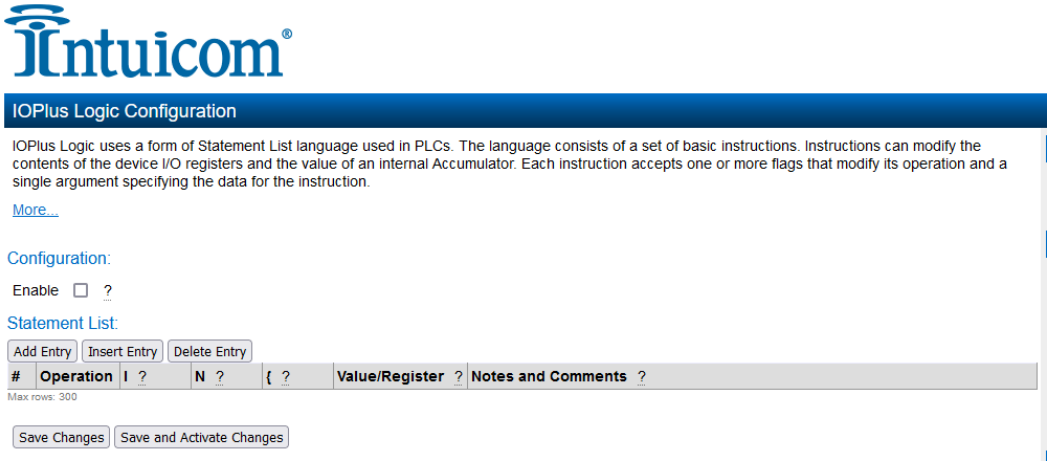


Dashboard with D1 Input/Output Switch Added

Save Changes and Reset – Once the changes are complete on the Network Configuration webpage a reboot is required to commit the changes. Click “Save Changes and Reset” to complete and commit the changes.

F – I/O Plus Logic

The IOPlus Logic Configuration webpage allows users to configure "Statement List language" used in Programmable Logic Controllers. Detailed instructions on how to configure this webpage can be found by clicking on the "More…" link below the opening paragraph.

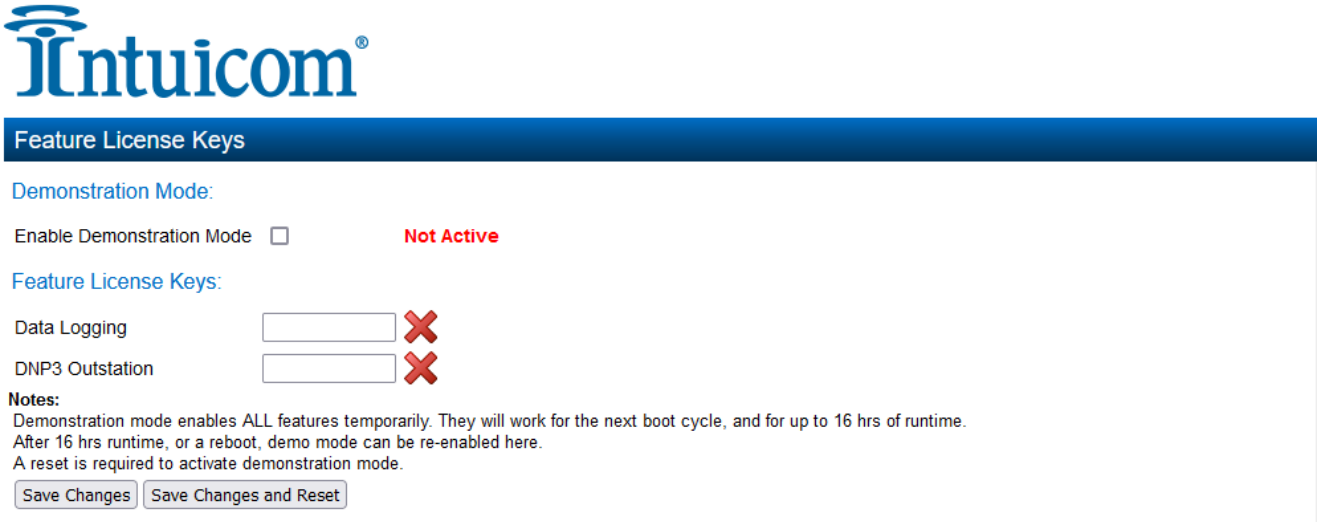


IOPlus Logic Configuration Webpage

G – Feature Keys

The Features License Keys webpage provides the ability to enter License Keys to unlock additional features available on the VUE. These features are:

- Demonstration Mode
- Data Logging
- DNP3 Outstation



Features Key Webpage

VI – Advanced Networking

This section describes the Advanced features of the VUE available for setting up complex networks. This allows you to make changes away from the default networking setup. You might need to make changes in this section if you need to support an unusual application, or if you need to interoperate with equipment from other manufacturers. If you're setting up a network of VUE devices, you normally won't need to change any of the settings in this section. To access these options, select "Full Configuration" on the right side menu to show the full configuration menu, and select from the items under the "Advanced Networking" section.

A – Repeaters

Repeaters setting allows you to configure arbitrary radio networks between different devices. Repeaters configuration is only available to devices configured as Access Point (Manual mode). The Repeaters configuration is managed automatically in ProMesh mode and in Fixed Link mode.
The VUE networking architecture allows an arbitrary set of Virtual Client and Virtual Access Point devices to be configured to provide arbitrarily complex networks. Use the "Add Entry", button to add a row to the repeaters table. Once this is complete, select the following:

Connection Mode – Select the desired connection mode This is either "Client/Station (Uplink)". or "Access Point (Downlink)". This creates a virtual network endpoint, which you can use to connect to another Endpoint with matching SSID.

SSID – This is the SSID of the Access Point you want to connect to. If you're connecting to a Fixed links network, this is the device name of the Repeater or Base that you want to connect to. For Roaming in a fixed links network, and for ProMesh connection, this is the System Name.

Encryption – This is set to match the encryption used in the remote endpoint you want to connect to.

Passphrase – This is set to match the encryption passphrase in the remote endpoint you want to connect to.

B – Roaming

Advanced roaming configuration is accessed by clicking on the "Roaming" link under advanced Networking. For the majority of mesh deployments with fixed nodes, these settings will not be needed.

Enable Mesh Path Roaming – By selecting this option Mesh Nodes can change path through the wireless network depending on best available signal strength. They can roam between repeaters and base nodes with the same system name.

Enable Mesh Node – By Selecting this This device behaves as a Mesh Node – i.e. Access Point functionality will be dynamically turned on only as needed

Primary SSID – This is the System Name entered on the Network webpage, and Mesh Nodes configured with the same SSID will connect to it or other Mesh Nodes as repeaters.

Secondary SSID – Adding additional SSIDs will allow Mesh Nodes to connect with devices in other ProMesh networks that have better Signal Strength. Up to a maximum of 10 alternate SSIDs can be configured.

NOTE: The Primary SSID will have top priority and the secondary SSIDs priority are set by the order in which they are entered into the Roaming Table.

C – IP Routing

If your system is divided into multiple IP Subnetworks, then you might need to configure IP Routing rules to allow IP data from the VUE to reach its destination IP address.
If your Base station or Access Point is configured for Routed Network mode, you will need to add routing rules or to set the Gateway IP to allow messages from your VUE to get out from the radio network onto the Ethernet network.
Use the "Add Entry", "Insert Entry" and "Delete Entry" buttons to manipulate the rows in the routing rules table so that you have one row for each routing rule.
The order of routing rules in the table is not important. They are always applied in order from most specific to least specific. Nevertheless, to help with understanding the routing rules, you should order the table in this way.
Once your table entry is complete, set the following:

Name – Create a descriptive name for the rule to remind you of the purpose of this rule at a later date.

Destination – This is the destination network IP address. Combined with the Netmask in the following field, this determines which destination IP addresses the rule applies to.

Netmask – This is the IP Network mask for the destination network IP address.

Gateway – This is the IP address of the gateway device that is used to reach the destination IP network. All packets that are destined for an IP address on the Destination network will be forwarded to this Gateway address for delivery to the destination network.

Enabled – You can enable or disable routing rules. Check this box to activate the rule.

D – Network Filtering

This configuration screen allows you to set up rules that stop unwanted traffic from entering your network. The filter applies to traffic coming from the Ethernet port which would otherwise be automatically sent over the radio network. This can be useful to reduce radio message traffic when a device is connected to a busy Ethernet network where the majority of traffic is not destined for the radio network.

NOTE: It is possible to configure filtering that stops your PC from accessing the device's web pages. If you are unable to access the device from the Ethernet port after configuring Filtering rules, you can either: Access the device from the USB connection; or restore the device's default network settings. For instructions, see "Restoring the factory default connection settings" on page 138.

Easy IP Filtering allows you to quickly configure filtering for a network that will only use IP protocols. If your network only uses IP protocols and IP Addresses in a single range, then use this method to configure your filtering.

Only allow IPv4 and ARP – Select this option if all of the devices on your network use IP protocol communications (TCP/IP or UDP protocols). This will automatically block all non-IP protocols from reaching the radio network.

Enable Easy IP Filtering – Select this option if all your devices' IP addresses are within a single range of addresses. By setting the first and last IP addresses, only IP messages within this range will be able to reach the radio network.

First Radio/Device IP – Select the lowest IP address of the devices on the radio network.

Last Radio/Device IP – Select the highest IP address of the devices on the network.

NOTE: Easy IP Filtering is a simple method to set up IP Filter rules. The IP Filter Rules table is disabled if you select Easy IP Filtering.

For more complex networks, where Easy IP Filtering does not provide the necessary functionality, you may need to set up multiple filtering rules to fully manage the network traffic.

IP Whitelist or Blacklist – Set this to "Whitelist" if you want to allow messages that meet the IP Filter Rules. Set this to "Blacklist" if you want to exclude messages that meet the IP Filtering Rules.

NOTE: If you set this to Blacklist, and you haven't selected "Only allow IPv4 and ARP" above, then the filter will block the specified messages, but any non-IP protocol messages will pass through the filter.

IP Filter Rules – These rules apply by checking the source address and destination IP addresses and ports of the message. A rule will match a message if the IP address is within the defined range, and the Port number is within the defined range.
Use the "Add Entry", "Insert Entry" and "Delete Entry" buttons to manipulate the rows in the table. For each row in the table, enter the parameters:

Enable – Check this to enable the rule. To temporarily disable a rule you can clear this checkbox.

IP Address Min/Max – These are the first and last IP addresses that this rule applies to.

Port Min/Max – This is the range of IP Port numbers (TCP or UDP Ports) that the rule applies to.

Protocol – You can set this to allow only one protocol type (TCP, UDP or ICMP) or all three protocol types.

NOTE: When you select any of these protocols, ARP messages for the corresponding IP address range are also allowed by default. For ICMP type messages, the port range values are ignored.

MAC Filtering Rules – These rules apply by checking the source MAC of the message. A rule will match a message if the source MAC matches the configured value.

NOTE: Messages that match any of the MAC filter rules are immediately passed (whitelist) or dropped (blacklist), and are not checked by the IP Filter Rules. Messages that do not match any filter rules in the whitelist are also immediately dropped. Messages that do not match any rules in a blacklist are passed and subsequently checked by the IP Filter Rules.

Enable – Check this to enable the rule. To temporarily disable a rule, you can clear this checkbox.

MAC Address – This is the MAC address that this rule applies to.

E – DHCP Server

You can configure one device in your network to act as a DHCP server for other devices in the network. This lets you automatically assign IP addresses to devices that join the network. This is most useful when you want to access the network with a device such as tablet or PC to connect to the devices in the network at their fixed network addresses.

NOTE: You must ensure there is only one DHCP server on your local bridged network. When your Base site is configured as a Bridge (Default), this includes DHCP servers connected to the Ethernet network that is connected to your Base station. When your Base site is configured as a Router, the DHCP server will only operate on the radio network.

Enable – Check this box to enable the DHCP server functionality.

IP Range Min/Max – This sets the range of IP Addresses that are assigned to devices that connect to the network. Make sure that this address range does not overlap any

existing fixed address assignments you have made on your network. Normally this range will be part of the same IP network address range as the other devices on your network.

Gateway IP Address – If the connected devices need a default gateway, you can enter this IP address here. Otherwise, leave this blank.

Primary/Secondary DNS Server – If the connected devices will be using DNS (Domain Name Service) to register or lookup device names, enter the IP addresses of the primary (and secondary) DNS Servers here. Otherwise, leave these blank.

Lease Time – This the amount of time that connected devices are allocated an IP address. Once the lease time expires, the IP address becomes available for allocation to other DHCP client devices.

NOTE: The lease time in conjunction with the IP range limits the number of devices that can be assigned DHCP addresses within a particular period. If all of the available IP addresses are allocated to devices then new devices won't be able to join the network until some of the existing leases expire.

F – VLAN

VLAN (Virtual Local Area Network) provides a method of segregating a single bridged network into multiple virtual networks that are logically separated. This allows segregation and prioritization of traffic in your network.

NOTE: VLAN is an advanced networking technique. You should only need to configure VLAN functionality if you have to interoperate with a network that already uses VLAN.

The following configuration items are available for VLAN.

1 – VLAN Mode

VLAN Passthrough – To disable VLAN functionality select this setting from the drop-down menu.

VLAN Aware – To enable VLAN, select this setting from the drop-down menu. When you select mode "VLAN Aware", the IP Address and Subnet Mask settings on

the main Quick Start page are ignored. The settings for Management IP/Netmask on this page are used instead.

NOTE: It is possible to configure a VLAN setup that stops your PC from accessing the device's web pages. If you are unable to access the device from the Ethernet port after configuring VLAN rules, you can either: Access the device from the USB connection; or restore the device's default network settings. For instructions, see "Restoring the factory default connection settings" on Page 138.

2 – Add VLAN Group
Click this button to add another VLAN Group. You can add multiple VLAN groups, with each group corresponding to a separate VLAN network. The first VLAN that you add is the Management VLAN, which provides access to the device Configuration on the new VLAN using the same IP Address as configured on the Quick Start page.

Name – You can add a descriptive name for each VLAN group. By default the first VLAN is named "Management VLAN".

VLAN ID – This is the 16-bit number that uniquely identifies the VLAN. Each configured VLAN Group should have a separate VLAN ID.

VLAN Priority – This is the QoS priority given to messages on this VLAN when sending over the radio channel. The radio channel takes this setting into account when prioritizing access to the radio for multiple separate VLANs.

Bridge STP/Priority – These settings enable Spanning Tree Protocol on this VLAN. Spanning Tree Protocol is required where there are bridging loops which would otherwise allow packets to circulate continuously on the network.

3 – Interface Membership for VLAN
This allows you to set which interfaces are part of the VLAN. The VUE has two interfaces which can join the VLAN; The Ethernet Interface and the Wireless Interface.

NOTE: The USB interface is reserved for local access to the device and cannot be connected to a VLAN.

Interface – Select the desired interface(s) to be connected to the VLAN. Use the "Add Entry" button to add an additional interface. (You need to select at least one interface for the VLAN to be reachable at the device)

Type – This specifies how data packets will be treated when they are received on this interface (Ingress) or are transmitted on the interface (Egress).

Type	Ingress behavior	Egress behavior
Tagged	Packet is only accepted if it's VLAN ID matches the configured ID for this VLAN.	Packet is transmitted as a VLAN packet with the configured VLAN ID
Untagged	All non-VLAN packets are received into the VLAN.	Packet is transmitted as a non-VLAN packet.

VLAN – Tagged and Untagged

VII – User Management

The User Management section of the webpages has the options to allow users that are logged in to change their password. Additionally, there is a link to a webpage that provides an interface for the Administrator to Manage Users. Last, there is a link to logout of the radio. Each of these functions are presented in more detail below.

A – Change My Password

You can change your password by clicking Change Password on the menu and entering the new password in both password fields. Click Save and Activate Changes to change your password. Passwords must be at least eight characters.

B – Manage Users

Users with Admin privileges can click User Management on the menu to configure access to the module (see figure below). An Admin can add new users, change user passwords, or retire (deactivate) user access. The Admin assigns each user a "role" which limits the functions available to them according their operational needs. There are three user roles:

- **Operator** – Can view information on the device, but cannot change configuration.
- **Manager** – Can view information and change the device configuration, but cannot modify the list of users allowed to access the device.
- **Admin** – Has all of the permissions of a Manager, plus the ability to modify the user list, user passwords, and access levels. (All users can change their own passwords.)

NOTE: You cannot delete individual users from the system, but can deactivate user access by "retiring" the user. If you need to delete all user information from the module and restore the factory default user settings, see "Restoring the factory default settings" on page 138.
The radio comes from the factory with two default users.

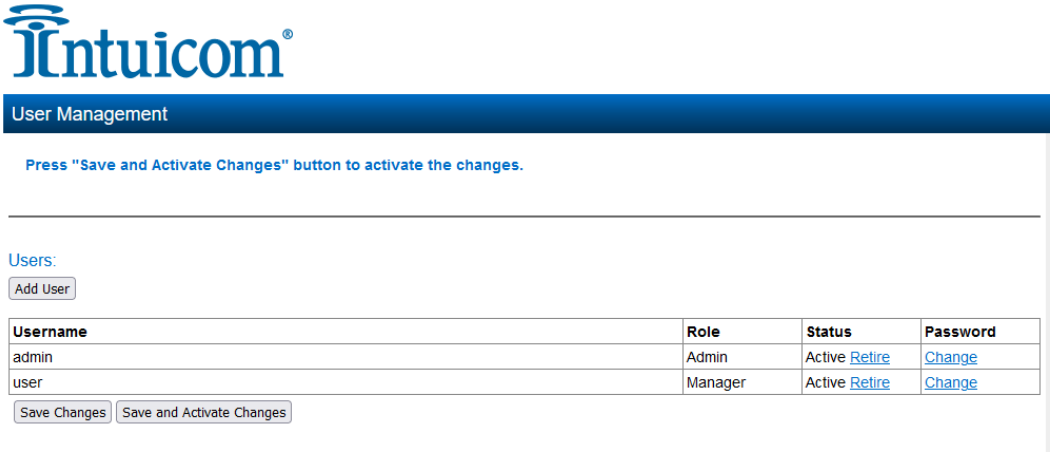
Default user name	Default password	Role
admin	admin	Admin
user	user	Manager

Users

Access to menu items is restricted by the user's role, as shown in the following table. If you click a menu item and do not have sufficient access privileges, you are prompted to enter a username and password with the necessary access privileges.

Menu item	Operator	Manager	Admin
Network	—	Yes	Yes
IP Routing	—	Yes	Yes
I/O Mappings	—	Yes	Yes
Fail safe configuration	—	Yes	Yes
Serial	—	Yes	Yes
I/O Configuration	—	Yes	Yes
Modbus	—	Yes	Yes
Module information	—	Yes	Yes
System tools	—	Yes	Yes
Feature keys	—	Yes	Yes
Data and event log	—	Yes	Yes
Change password	Yes	Yes	Yes
User management	—	—	Yes
I/O Diagnostics	Yes	Yes	Yes
Connectivity	Yes	Yes	Yes
Logs and archives	Yes	Yes	Yes
Home	Yes	Yes	Yes

Access Privileges



User Management

1 – To add a user

1) Click “User Management” on the left column of menus.
2) Click “Add User”.
3) Enter a username and password, and confirm the password. Passwords must be at least eight characters.
4) Select a role for the user.
5) Click “Create” to add the user.
6) To add additional users, repeat steps 2 through 5.
7) When you have finished adding users, click “Save and Activate”.

2 – To retire a user

1) Click “User Management” on the left column of menus.
2) Click “Add User”.
3) In the Status Column for the user click “Retire”.
4) Click “OK” to confirm. The user’s status changes from “Active” to “Retired”.
5) Click “Save and Activate Changes”. This disables access to the radio by the retired user.

3 – To change a user password

1) Click “User Management” on the left column of menus.
2) In the Password column for the user, click “Change”.
3) Enter a new password for the user and confirm the new password.
4) Click “Apply”
5) Click “Save and Activate Changes”.

Recovery after lost admin password – If you lose the password for your admin account, you need to restore the device to factory default settings to restore the default Admin password. Refer to “Restoring the factory default settings” on page 138.

C – Logout

Click on this link will log you out of the radio and bring up the browser username and password window.

VIII – Network Diagnostics

The VUE series radios include a Network Diagnostics menu that provides users with the tools necessary to check available channels, wireless connections, network performance, and radio communications. In this section we will cover all the webpages under the Network Diagnostics header.

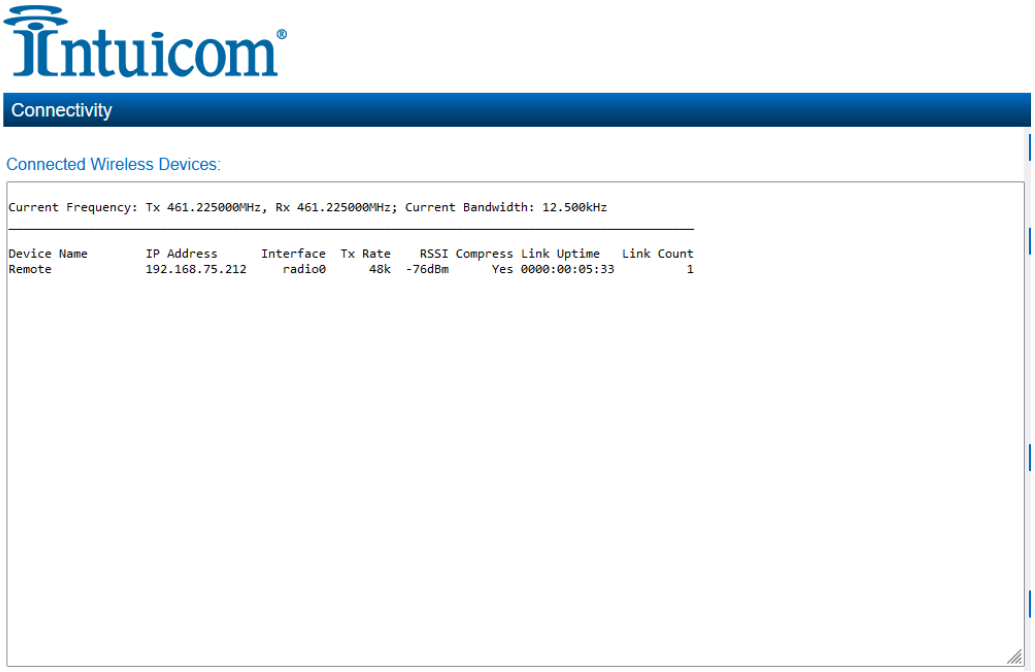
A – Connectivity

The Connectivity webpage provides the ability to see devices that are connected wirelessly to the radio. Parameters are:

1 – Connected Wireless Devices

The Connected Wireless Devices window shows the status of the remote radios connected to the local radio where you are logged in and viewing the webpage.

- **Device Name** – This is the name that is configured in the remote device
- **IP Address** – This is the IP address of the remote radio.
- **Interface** – The remote radio interface connected to your local radio.
- **Tx Rate** – The data rate running on the wireless link.
- **RSSI** – Receive Signal Strength Indicator, in dBm.
- **Compression** – Indicates if compression is on (yes) off (no).
- **Link Uptime** – Indicates the amount of time the link has been up.
- **Link Count** – How many links the remote radio has to the local.



Connected Wireless Devices

2 – Available Access Points

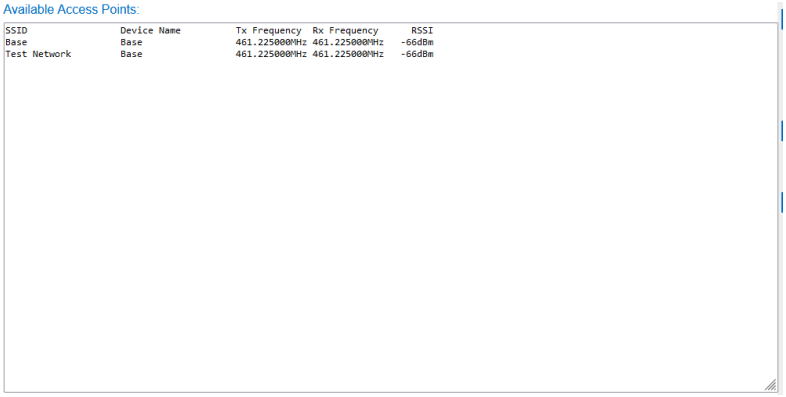
The Available Access Points window will only display information on a remote or client radio. The window provides information such as.

SSID – Security Set Identifier that must be exact so both radios will connect.

Device Name – This is the name configured into the Access Point.

Tx and Rx Frequencies – Displays the frequency in MHz that the Access Point is using for communications.

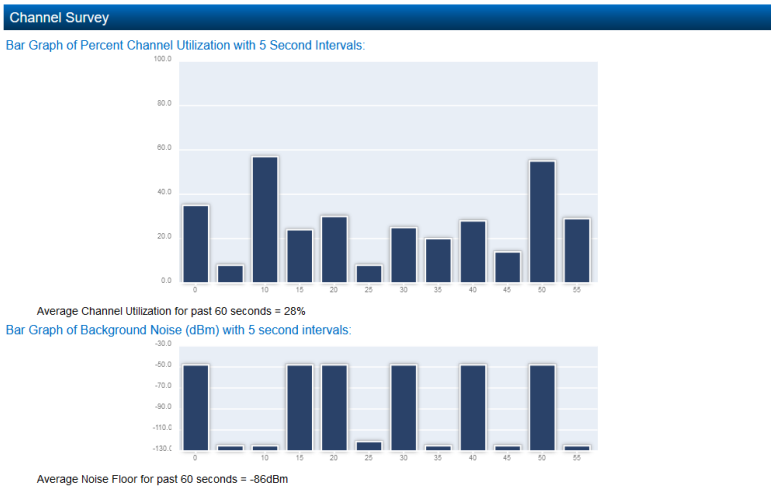
RSSI – Receive Signal Strength Indicator – Shows the Signal Strength is dB that the radio is picking up from the Access Point.



Available Access Points

B – Channel Suvey

The Channel Survey webpage provides bar graphs of the channel utilization, and the noise floor for time increments of 5 seconds, 1 minute, and 1 hour.



Channel Utilization and Noise Floor – 5 Second Chart

C – Custom Survey

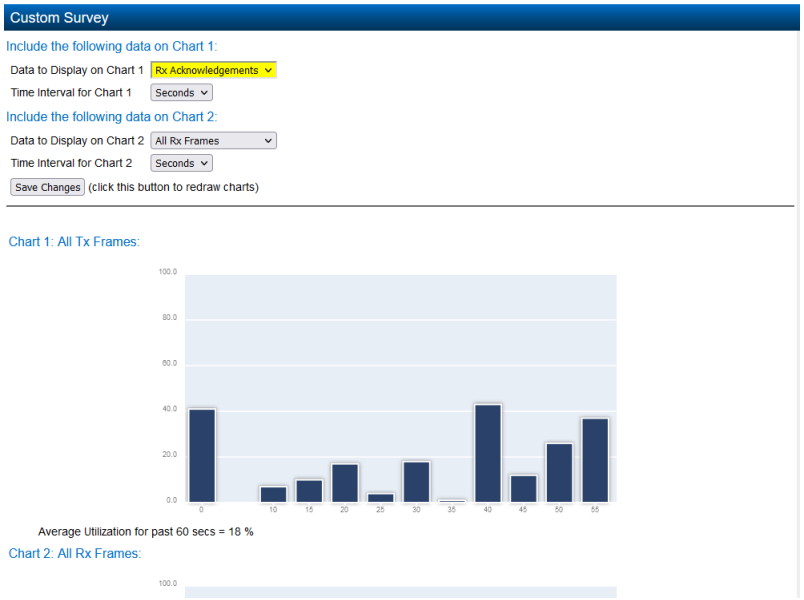
The Custom Survey webpage allows the user to run custom scans on spectrum the radio is using and different data can be displayed on the chart as well as different time frames. The different selection of data to display on the charts are as follows.

1) All Tx and Rx Frames
2) All Tx Frames
3) All Rx Frames
4) All Tx First Attempts
5) All Tx Retries
6) All Tx Acknowledgements
7) Radio Holdoff
8) Rx to this Radio
9) Rx to all other Radios
10) Rx Acknowledgements
11) Rx Errors

Time intervals available for selection are.

1) Seconds
2) Minutes
3) Hours

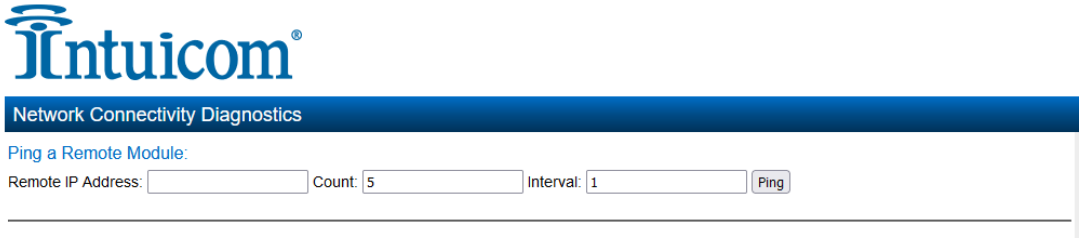
Two charts can be set up with different data for comparison.



Custom Survey

D – Network Connectivity Diagnostics

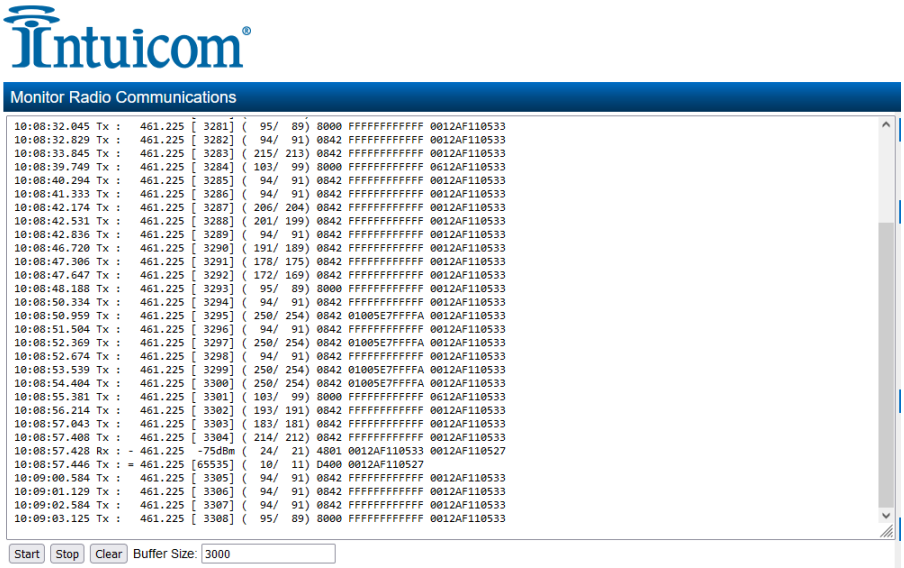
This webpage provides a ping tool so users can ping remote radios from the unit they are logged into.



Ping Tool – Network Connectivity Webpage

E – Monitor Radio Communications

This feature gives you a detailed view of the radio messages. You can view the low level radio transmissions, the radio signal strength, and indication of corrupted radio messages.



Monitor Radio Comms Webpage – Communications Display

Use the “Start” and “Stop” buttons to start and stop the communications log. “Clear” clears the logged data. Buffer Size sets the amount of data to log. Check the table below for a detailed description of the fields in the log data.

Position	Name	Description
1-13	Time Stamp	Message timestamp according to the radio’s time. Format is hh:mm:ss.sss, providing millisecond. This should be close to the host time.
15-18	Direction	Tx indicates Transmitted Message. Rx indicates Received Message.
20	Flag	More information about the message: 1-9: Transmission Counter (re-tries)

		* : Received Acknowledgement to transmitted message (from this station) - : Received message (to this station) =: Transmitted Acknowledgement to received message (to this station) B: Bit-Error test frame
22-29	Frequency	Radio Frequency (in MHz).
30-36	Seq (Tx)	For transmitted messages, the sequence number of the message. [65535] indicates internally generated message ACK or CTS.
	RSSI (Rx)	For received messages, the RSSI (signal strength) of the message in dBm
38-48	Length	The message length in bytes. first number is the MAC message length. Second number is the on-air length.
50-53	Frame Control	The frame Control field according to 802.11 protocol. Some common values are shown here. 8000 - Beacon frame from AP D400 - ACK (message acknowledge) 0000 - Association Request 1000 - Association Response 4000 - Probe Request 5000 - Probe Response 0803 - Data Frame (UnEncrypted) B400 - RTS (Channel Request) C400 - CTS (Channel Grant) A000 - Disassociation B000 - Authenticaiton (WPA only) C000 - Deauthentication
	CRC Error	ERROR! is displayed in positions 50-55 for a corrupted received frame. If the messge Header is received, the Length will indicate the message length. Otherwise, it shows zero.
55-66	Destination	Address1 field from 802.11 protocol This is the destination MAC address for the message. FFFFFFFFFFFF for broadcast messages.
68-79	Source	source MAC address for the message (blank for acknowledgements).

Examples

In the examples below, the monitoring site has MAC address ending 1124AF, the remote station has MAC addres ending 1123FF.

Message Retry: Monitoring site sends encrypted data (0843) with re-transmission (0847) and remote acknowledgement (D400).

```
5:47:05.336 Tx: 1 433.000 [18112] (163/158) 0843 0612AF1123FF 0012AF1124AF
5:47:05.486 Tx: 2 433.000 [18112] (163/158) 0847 0612AF1123FF 0012AF1124AF
5:47:05.499 Rx: * 433.000 -38dBm ( 10/ 11) D400 0012AF1124AF
```

Probe and Connect: Remote site sends probe request. Local site sends probe response Remote waits, then sends association request, with association response from the local site.

```
0:03:38.574 Rx: 433.000 -41dBm (107/ 99) 4000 FFFFFFFFFFFF 0612AF1123FF
0:03:38.672 Tx: 1 433.000 [ 20] ( 93/ 91) 5000 0612AF1123FF 0012AF1124AF
0:03:38.684 Rx: * 433.000 -40dBm ( 10/ 11) D400 0012AF1124AF
0:03:44.165 Tx: 433.000 [ 21] ( 99/ 93) 8000 FFFFFFFFFFFF 0012AF1124AF
0:03:58.631 Rx: - 433.000 -41dBm ( 80/ 78) 0000 0012AF1124AF 0612AF1123FF
0:03:58.642 Tx: = 433.000 [65535] ( 10/ 11) D400 0612AF1123FF
0:03:58.659 Tx: 1 433.000 [ 22] ( 71/ 69) 1000 0612AF1123FF 0012AF1124AF
0:03:58.671 Rx: * 433.000 -41dBm ( 10/ 11) D400 0012AF1124AF
```

Received Data with Channel Allocation: Remote site sends RTS (B408), with CTS response (C400) from monitoring site. Then sends encrypted data (0843) to monitoring site, with acknowledgement from monitoring site (D400).

```
1:18:21.162 Rx: R 433.000 -41dBm ( 16/ 16) B408 0612AF1124AF 0012AF1123FF
1:18:21.178 Tx: C 433.000 -76dBm ( 10/ 11) C400 0012AF1123FF
1:18:21.235 Rx: - 433.000 -76dBm ( 93/ 91) 0843 0612AF1124AF 0012AF1123FF
1:18:21.251 Tx: = 433.000 [65535] ( 10/ 11) D400 0012AF1124AF
```

Beacon Tx: Monitoring site sends a beacon transmission (8000)

```
5:47:06.380 Tx: 433.000 [18113] ( 99/ 93) 8000 FFFFFFFFFFFF 0012AF1124AF
```

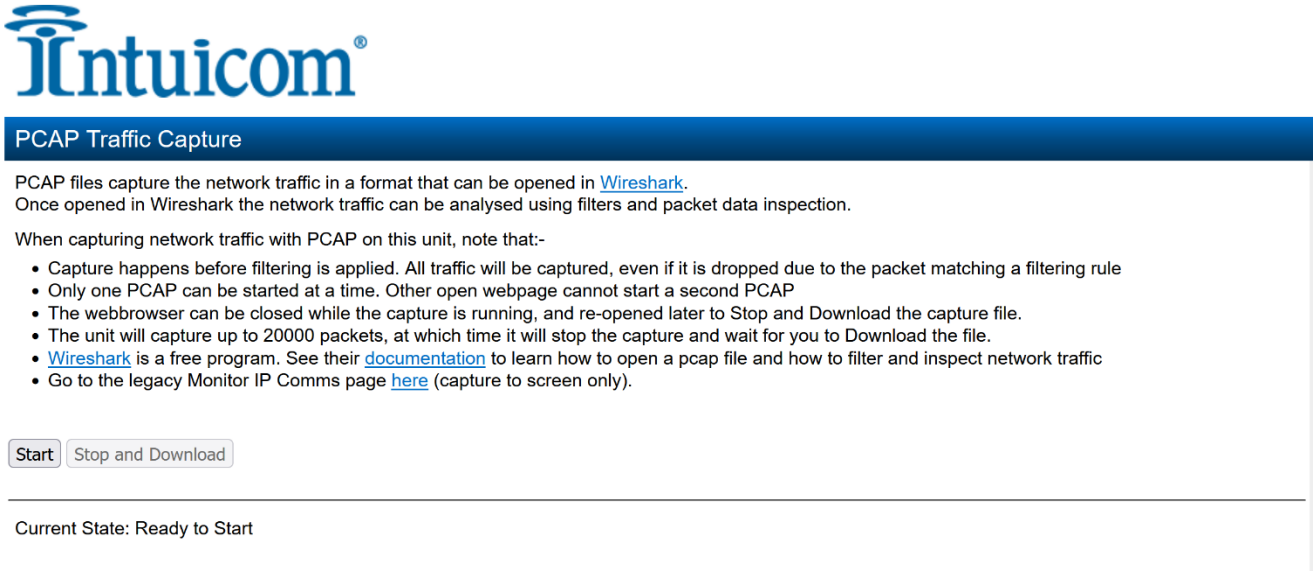
Remote to Remote: Remote site sends encrypted data (0843) to a more distant remote site,with acknowledgement from the distant remote site (D400).

```
5:44:58.332 Rx: 433.000 -41dBm ( 73/ 68) 0843 0012AF110DC3 0612AF1123FF
5:44:58.344 Rx: 433.000 -73dBm ( 10/ 11) D400 0612AF1123FF
```

NOTE: The first byte of the displayed MAC address might not match the device's radio MAC address. For ProMesh and FixedLinks modes, the first three bytes of the uplink (towards the base station) will be 0612AF. The downlink will be 0012AF. INTUCOM OUI is 0012AF. The last three bytes of the MAC address will uniquely identify the station.

F – Capture IP Comms

The VUE Series radios can save network communications data for downloading an analyzing using the WireShark™ protocol analyzer. You can download WireShark from https://www.wireshark.org/download.html
Click "Capture IP Comms" under Network Diagnostics on the right-side menu. To start the capture, click "Start".



Capture IP Coms – WireShark™ Webpage

Once the capture is active, the screen displays the capture status, and the size of the capture file. Capture will stop automatically when the file reaches a maximum size (20,000 packets), and the state will change to “Stopped”. You can click on the “Stop and Download” button at any time to download the current capture file.

NOTE: When the device is configured for bridged mode (default), all of the network traffic on both the ethernet port and the radio is captured, including ethernet packets that are blocked by the filter configuration. When the device is configured for Routed mode, only radio traffic is captured.

IX – Unit Diagnostics

This section describes the unit diagnostic tools and information available from the radios Web-based configuration utility. The three webpages under Unit Diagnostics are I/O Diagnostics, Statistics, and System Tools.

A – I/O Diagnostics

Click “IO Diagnostics” from the home page of the Web-based configuration utility to read and write I/O store registers within the radio.
To read a register location, enter an address location (for example, 10001 for digital inputs), enter a count (number of consecutive registers), and then click Read (see figure on the next page). The returned address location and the returned values appears at the bottom of the page.
To write to outputs, enter the address location, count, and value, and then click Write. You will see the o00utputs change to the value you entered. For example, write to Register 1 with a count of 8 and a value of 1 will turn all the local digital outputs on. Write to Register 40001 with a count of 2 and a value of 49152 will set the two local physical analog outputs to 20 mA.

NOTE: If the symbol “~“ appears beside the register value when reading a register, it indicates that the register has been initialized to the “Invalid” state through the fail-safe configuration. I/O Mapping messages that include an invalid register are disabled until all of the source data is valid.

NOTE: If the symbol “*“ appears beside the register value when reading a register, it indicates that the register has been set to its failsafe value through the fail-safe configuration. It can still be sent via a regular mapping. This flag is available through the DNP3 protocol when reading the DNP3 Data Quality flags.

A mapping will only be sent when all registers have a value (no “~” symbols). To set an initial value for registers upon startup, use the Fail-safe Block Configuration menu in the Web-based configuration utility. If there is a mapping configured and any one of the source register values has the value “~“ the mapping will not be sent.
Using the I/O Diagnostics page, you can check the register locations for the “~“ and “*” symbols and even write values if required. If you see the value “3” when reading the status of the DIO on the module it indicates that the DIO is being used as an output in the “on” state.

I/O Diagnostics

Settings available are:

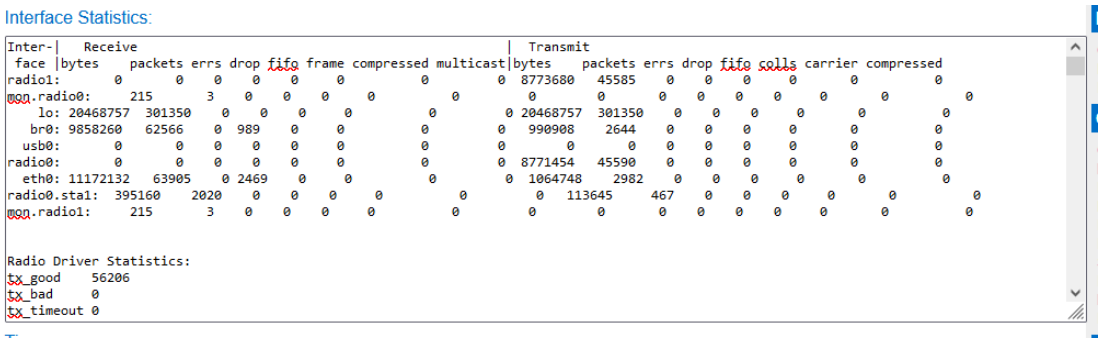
- **Register** – Register address location.
- **Count** – Number of consecutive registers, starting from register location specified in the Register field.
- **Value** – Value to be written.
- **Read** – To read a register location, enter an address location (for example, 10001 for digital inputs), enter a count (number of consecutive registers), and then click “Read”.
- **Write** – To write to outputs, enter the address location, count, and value, and then click “Write”.

B – Statistics

The Statistics webpage provides a large array of statistical information on the performance of the VUE. A description of each is given below.

1 – Interface Statistics

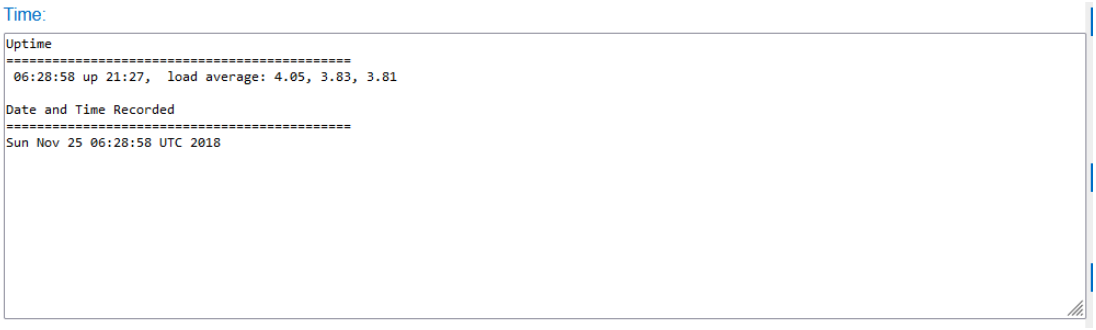
Interface statistics contains data on all the interfaces in the VUE and the transmit and receive detailed statistics for the traffic passing in and out of those interfaces.



Interface Statistics

2 – Time

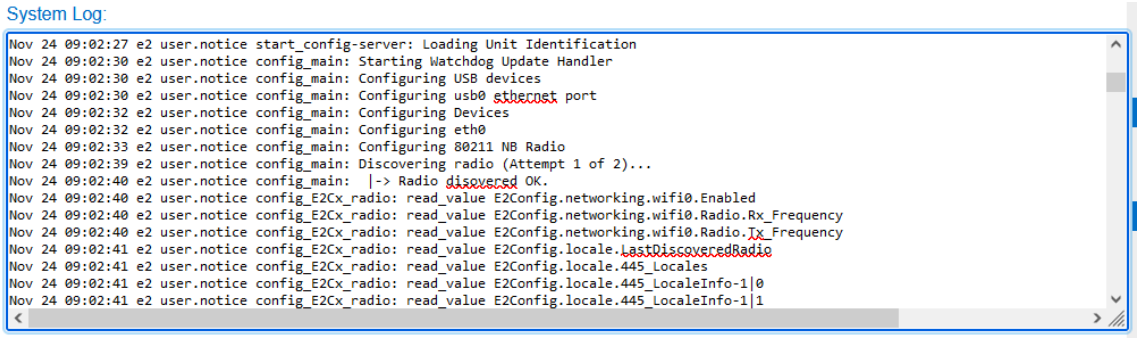
Shows relevant time statistics such as up time and the date and time set on the unit.



Time Statistics

3 – System Log

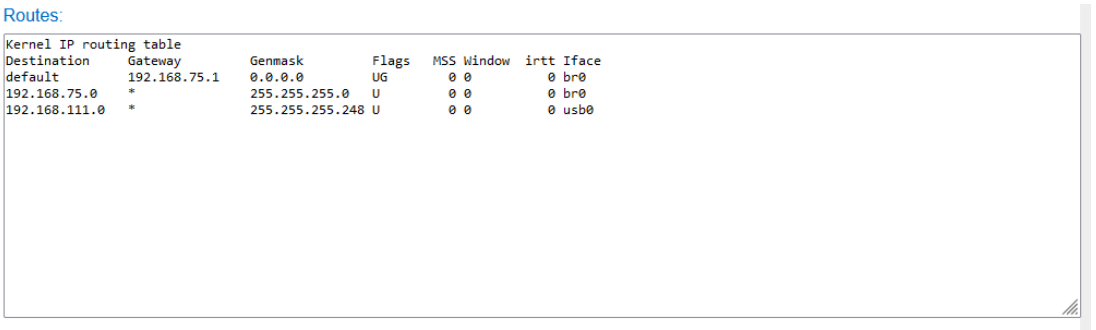
The system log contains message about the system performance and events that are relevant to the latest configuration.



System Log Statistics

4 – Routes

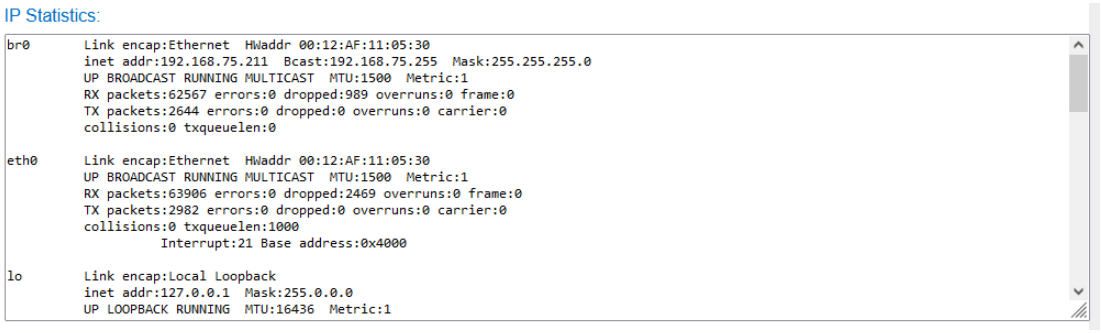
This window displays the IP routes the system is using for communication, both dynamic and static.



Routes Statistics

5 – IP Statistics

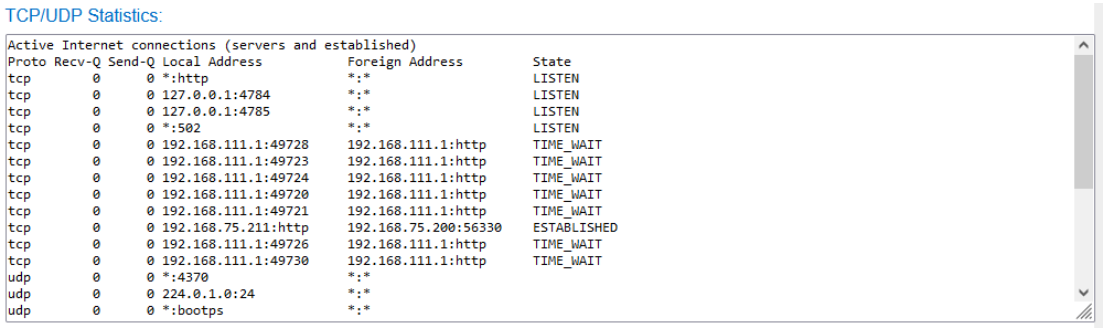
This window contains detailed IP traffic statistics for each interface in the VUE.



IP Statistics

6 – TCP/UDP Statistics

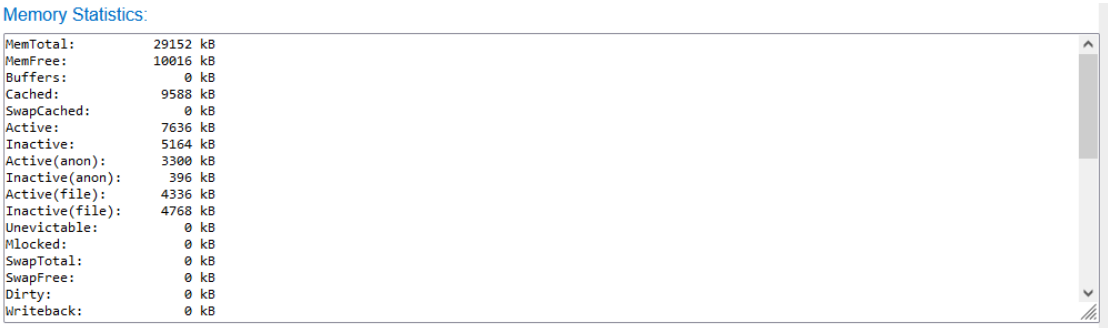
This window contains detailed TCP and UDP statistics for the VUE.



TCP/UDP Statistics

7 – Memory Statistics

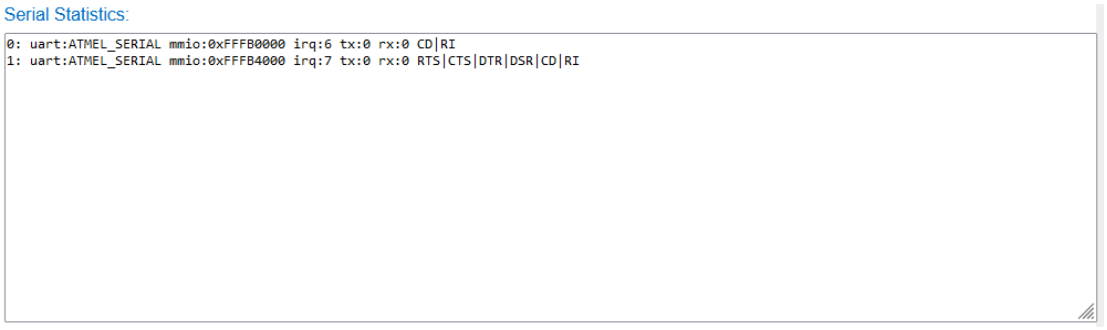
The Memory Statistics window displays detailed information on memory utilization and performance.



Memory Statistics

8 – Serial Statistics

The last window on the Statistics webpage contains information about the serial interfaces on the VUE.



Serial Statistics

B – System Tools

The System Tools webpage provides links to perform administrative tasks such as, clearing the system log, reading or writing configuration file, performing firmware upgrades and setting the date and time.

System Tools Webpage

System Log – Logs system instructions and other information to the screen. The log screen can then be saved to a file that may be used by Intuicom technical support to diagnose problems.

Clear System Log – Clears the log screen.

Read Configuration File – Reads the module configuration for saving to a file. For details, see the section below “Configuration Export”

Write Configuration File – Loads a previously saved configuration file into the module.

Firmware Upgrade – Upgrades the module firmware. For details, see "Patch file firmware upgrade" below.

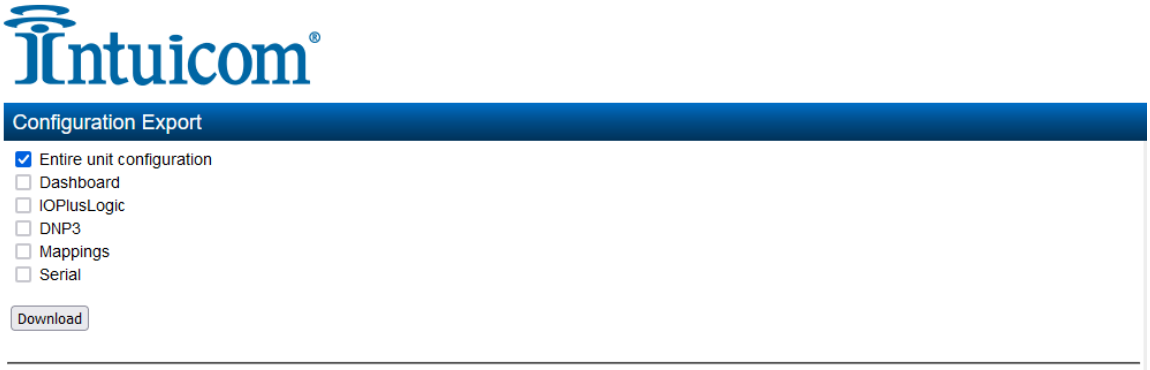
Set Date and Time – Allows you to set the date and time for the device.

Reset – Resets the module.

Clear Configuration and Reset – Resets the module and restores its factory default configuration.

1 – Configuration Export

You can export the module configuration to a file for upload to another unit. Select "Read Configuration File" from the system tools page. You can then select to export the full device configuration, or particular elements of the device configuration. If you want to save the device configuration as a backup, select "Entire unit Configuration". If you want to save some elements of the configuration for use in a future project, then you can just select the elements that you need to save.

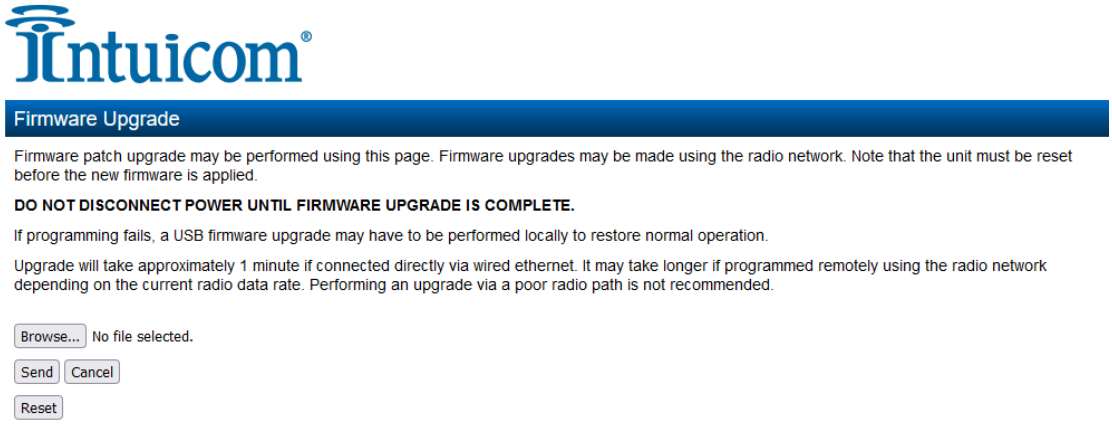


Configuration Export

2 – Patch File Firmware Upgrade

To upgrade the module firmware locally using a firmware patch file, click System Tools on the menu, and then click Firmware Upgrade and browse for the saved firmware patch file. When you locate the file, click Send to upload the file to the module. A status message appears. If the upgrade was successful, click Reset. If it was not successful, repeat the process. (The module must verify that the file is valid before you can initiate a reset.)

NOTE: All existing configuration parameters will be saved. However, if any new parameters are added to the firmware, the default values will be used.



Firmware Upgrade

3 – Setting the Date and Time

This feature is associated with data logging. The module needs access to the current date and time to make effective use of data logging if this feature is enabled on the module.

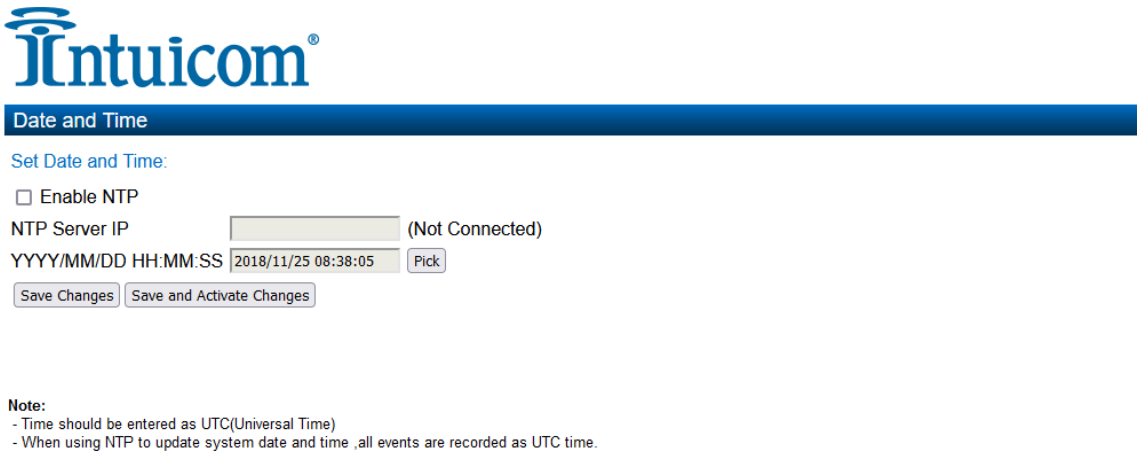
To configure the date and time, click System Tools on the menu, and then click Set Date and Time. This displays the page in the figure below. There are two ways you can set the date and time on this page:

- **Manually** – Enter the date and time.
- **Enable Network Time Protocol (NTP)** – This method requires access to a date and time (NTP) server.

If you set the date and time manually, keep in mind that the date and time function does not support time zones or daylight savings time. Normally you should set the time to UTC (Universal Time). You can set the time to your local time, but you will need to remember to change the time if your location uses daylight savings. When the time is set manually, the module uses an internal real-time-clock to keep time during loss of power. This real time clock has power to run for at least twelve hours (typical 3-5 days). If the duration of the power loss is too long, the time at power restoration will be the time that power was lost.

To use the NTP feature, you need network access to an NTP server. You can use a public server, or set up your own server. Most modern operation systems (such as Microsoft® Windows and Linux) can be configured to operate as an NTP server. If

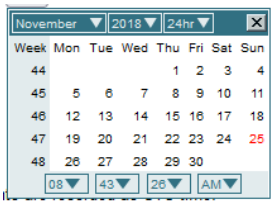
the NTP server is on a different sub-network, you may need to configure routing rules to allow the device to reach the NTP server. Use the "Ping" command on the Network Diagnostics page to check if you have connectivity to the NTP Server IP address.



Date and Time Webpage

Enable NTP – Select this checkbox to automatically set the time and date in the device from an external NTP server. You will also need to enter the IP address of the NTP server in the NTP Server IP field.

NTP Server IP – Enter the IP address of the NTP server if you selected the checkbox to Enable NTP.



YYYY/MM/DD HH:MM:SS – Use this field to set the time manually if there is no access to an NTP server. Click "Pick" to display a date and time selection pop-up. Select the day, month, year and hour, minute and second, and click "Pick" again to set the time and close the pop-up. To set the time more precisely, try selecting a time a little in the future and waiting until that time to click "Pick".

Save Changes and Activate – After configuring the settings, click "Save changes and activate"

For manual time, clicking this button sets the clock with the new time.
For NTP time, after a short delay the message next to the NTP Server IP field updates to show whether the module successfully connected to the NTP server. If

the message is “Not Connected,” check that the NTP server is configured correctly, and use the Ping command on the Network Diagnostics page to check that the module can reach the NTP server. After connecting to the NTP server, the displayed time changes to match the NTP server. This is normally UTC time.

X – Unit Information

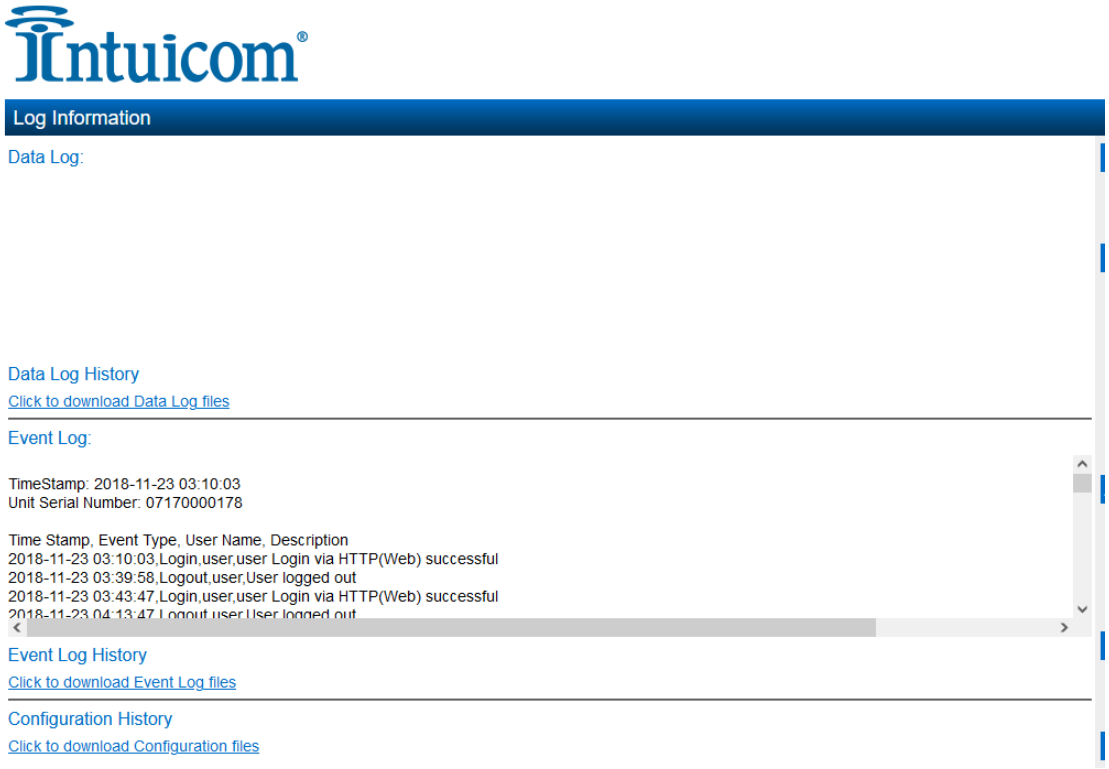
The last header in the right column of links is Unit Information. The links below this header provide the user with detailed information about the VUE.

A – Configuration Summary

This webpage provides an overview of the unit configuration. Starts with the Home Page at the top and runs down through all the settings that are programmed into the VUE. The Configuration Summary also includes the statistic windows at the end or the page.

B – Logs and Archives

This webpage provides access to Data, Event, and Configuration History logs. These logs can be downloaded from this page for review.

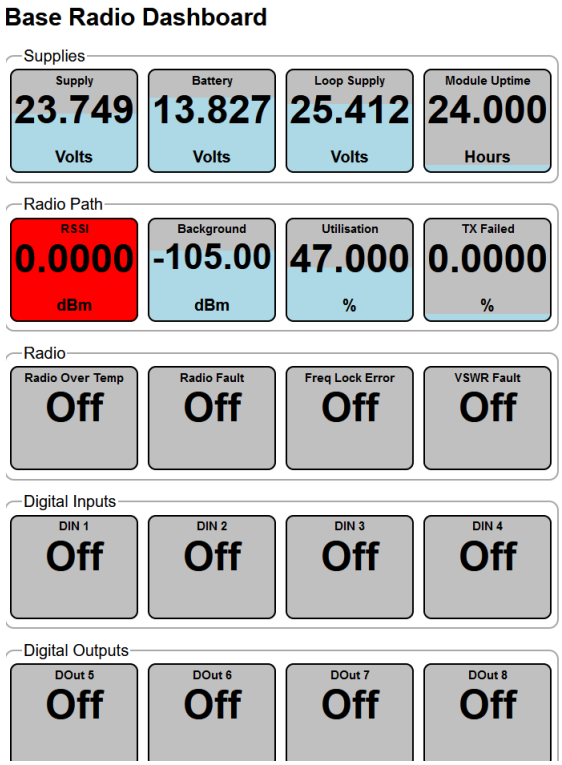


Logs and Archives Webpage

C – View Dashboard

The VUE Dashboard page provides a quick overview of the module performance in real time. This includes all aspects of unit operation such as:

1) Power Supplies
2) Radio Path
3) Radio
4) Digital Inputs
5) Digital Outputs
6) Analog Inputs and Outputs



VUE Dashboard

D – Module Information

Click “Module Information” from the menu to change the following information for the module. With the exception of the password, the information entered here is displayed on the module’s home configuration Web page.

Device Name – Allows you to label the module.

Owner – Module owner name.

Contact – Contact details.

Description – Description of the module.

Config Version – The date and time when the module was last programmed.

E – Home

The last link in the right column is the link to the Home webpage. This is the page that is displayed when you first log into the unit. It contains the following information.

- Dipswitch settings and Ethernet MAC Address
- Module Information (covered in the previous section on page 143 above)
- Unit Information such as model, licenses, firmware versions and more.

Appendix A - Specifications

VUE Specifications

Item	Specification	
Input/Output	**VUE-4-IO**	**VUE-1-IO**
Discrete Input	8 Digital I/O (1–4 Configurable as Pulsed Input or Output) On-State Voltage: < 2.1 Vdc Wetting Current: 3.3 mA Max I/P Pulse Rate: DI 1/2: 50 kHz; DI 3/4: 1 kHz Min I/P Pulse Width: DI 1/2: 10 µsec; PI 3/4: 0.2 msec	2 Digital I/O (Configurable as Pulsed Input or Output) On-State Voltage: < 2.1 Vdc Wetting Current: 3.3 mA Max I/P Pulse Rate: 50 kHz Min I/P Pulse Width: 10 µsec
Discrete Output	8 Digital I/O (1–4 Configurable as Pulsed Input or Output) On-State Voltage: DO Max, < 0.5 V Maximum Current: 200 mA Max O/P Pulse Rate: PO Max Rate, 1 kHz	2 Digital I/O (Configurable as Pulsed Input or Output) On-State Voltage: DO Max, < 0.5 V Maximum Current: 200 mA Max O/P Pulse Rate: PO Max Rate, 1 kHz
Analog Inputs	4 AI (2 Differential, 2 Single Ended) Current Range: 0–24 mA Voltage Input Range: AI 1/2: 0–20 V, AI 3/4: 0–5 V Accuracy (Voltage and Current): 0.1% full scale	N/A
Analog Output	2 AO (Sourcing) Current Range: 0–24 mA Accuracy (Current): 0.1% (20 µA)	N/A
Radio		
Operating Frequency Range	400-480 MHz	148-174 MHz
Transmit Power	Adjustable 10mW to 10Watts	Adjustable 10mW to 5Watts
Receive Sensitivity	-116 dBm (BER 1e-5 - 4QAM modulation with FEC)	
Bandwidth	6.25kHz, 12.kHz, 25kHz (Configurable).	
Emission Designator	5K75F1D (6.25kHz); 11K5F1D (12.5kHz) ; 23K0F1D (25KHZ)	
Modulation	2FSK, 4FSK, 4QAM, 16QAM, 64QAM	
Data Rates	2400, 4800, 9600, 19,200 baud (FSK); 4k, 8k, 16k, 24k, 32k, 48k, 64k, 96k baud (QAM)	
Ethernet Ports		
Ethernet Port	10/100base®; RJ-45 Connector, IEEE 802.3	
Link Activity	Link, 100Base via LED	
Serial Ports		
RS-232 Port	EIA-562 (RJ-45 Connector)	
RS-485 Port	2-Pin Terminal Block, Non-isolated	
Data Rate (Bps)	1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 76800, 115200, 230400 bps	
Serial Settings	7 / 8 Data Bits; Stop/Start/Parity (Configurable)	
Protocols & Configuration		
Protocols Supported	TCP/IP, UDP, HTTP, FTP, TFTP, Telnet, Modbus RTU Master/Slave, Modbus-TCP Client/Server, WIB I/O	
User Configuration	All User Configurable Parameters via HTTP	
Configurable Parameters	Unit details, I/O mappings and parameters. For configuration details, see in this manual. Modbus TCP/ RTU Gateway. Embedded Modbus Master/Slave for I/O Transfer.	
Security	Data Encryption: 256-bit AES, WPA2-PSK	
LED Diagnostics		
LED Indication	Power/OK; LAN Link/Activity; RS-232; RS-485; Digital I/O; Analog I/O Status; Signal strength	
Reported Diagnostics	Connectivity Information/Statistics, System Log File	
Compliance		
EMC	FCC Part 15, EN 301 489-5, EN 301 489-3, CISPR22	
Hazardous Area (VUE Series)	UL Class 1, Division 2; ATEX; IECEx nA IIC	
Safety	EN 62368 (RoHS Compliant, UL Listed)	
Radio	FCC Part 90, AS/NZS 4295, EN 300 113, EN 300 220	
General		
Size	5.91" x 7.09" x 1.38" (180 mm x 150 mm x 40 mm)	
Housing	IP20 Rated Aluminum	
Mounting	DIN Rail	
Terminal Blocks	Removable; Max Conductor 12 AWG 0.1 in2 (2.5 mm²)	
Temperature Rating	–40 to +158 °F (–40 to +70 °C)	
Humidity Rating	0–99% RH Non-condensing	
Weight	1.5 lb (0.7 kg)	
Power Supply		
Nominal Supply	15 to 30 Vdc; Under/Over Voltage Protection	
Battery Supply	10.8 to 15 Vdc	
Average Current Draw	220 mA @ 12 V (Idle), 110 mA @ 24 V (Idle)	

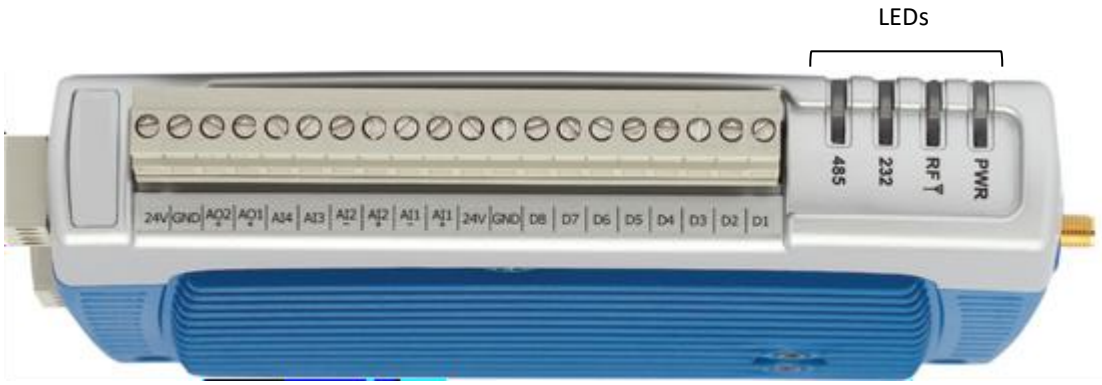
Appendix B – LED Function

Front panel LEDs

When the module is initially connected to power, it performs internal setup and diagnostics checks to determine if it is operating correctly. These checks take approximately 80 seconds. The following table shows how the LEDs appear when the module is operating correctly.

LED	Condition	Meaning
PWR	Green	System OK
PWR	Red	System boot (initial or system fault)
PWR	Orange	Start of system boot
PWR	Fast Flash	System boot, stage 1
PWR	Slow Flash	System boot, stage 2
RF	Green	RF Link established
RF	Flash Off from Green	Radio Receive
RF	Flash Green from Off	Radio Receive (Good Signal)
RF	Flash Red from Off	Radio Receive (Weak Signal)
RF	Orange Flash	Radio transmit
232	Green	Transmitting RS-232 data
232	Red	Receiving RS-232 data
232	Orange	Transmitting and receiving RS-232 data
485	Green	Transmitting RS-485 data
485	Red	Receiving RS-485 data

Front Panel LEDs



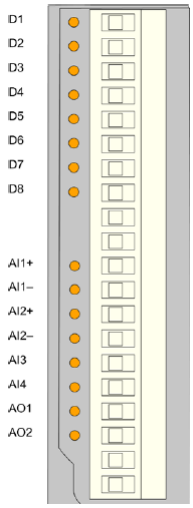
LED	Condition	Meaning
▼■■■■	Green	Strong signal suitable for 64QAM/4FSK
▼■■■	Green	Good signal suitable for 16QAM/4FSK
▼■■	Green	Weak signal suitable for 4QAM/2FSK
▼■	Yellow	Very weak signal suitable for 4QAMFEC/2FSK
RPT	Green	Device is active as a Repeater
ETH	Solid Yellow	Ethernet LINK
ETH	Flash Yellow	Ethernet activity

Additional VUE LEDs

LED Boot Sequence

Upon reset, the PWR LED appears solid red for about 2 seconds (system boot), followed by 12 seconds of Orange (start of system boot process). The PWR LED then fast flashes between red and green for 30 seconds (stage 1 of system boot process) followed by a slow flashes for 50 seconds (stage 2 of system boot process). At the end of the boot sequence the PWR should appear solid green. The time periods are approximate, and depend on the hardware and firmware revisions.

Input and Output LEDs



LED indicator	Condition	Meaning
D 1–8	Orange	Digital input is on
D 1–8	Flashing Orange -(Long On)	Update failure (fail-safe state is on)
D 1–8	Flashing Orange -(Long Off)	Update failure (fail-safe state is off)
AI 1 and 2 +	Orange	Analog input current indication
AI 1 and 2 –	Orange	Analog input voltage indication
AI 3 and 4	Orange	Analog input current or voltage indication
AO1 and 2	Orange	Analog output current indication

LED Indicator Status

Digital Inputs – LEDs display the status of each of the eight DIOs when used as inputs. If the LED is on, it indicates that the input is on.

Digital Outputs – When the DIOs are used as outputs, the LEDs display the status of each of the digital outputs. If an LED is on, it indicates that the output is on. The LEDs also indicate if the output is in a fail-safe state by flashing at different rates. If an LED is mostly on (long on) it indicates that the fail-safe state is on. If an LED is mostly off (long off) it indicates that the fail-safe state is off.

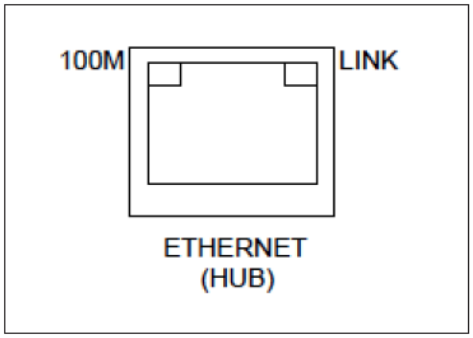
Analog Inputs – There are two LEDs for each differential analog input. The first LED (+) is used to indicate that the analog input is reading a current (mA). The second LED (–) indicates that the input is reading voltage. Each of the analog input LEDs will come ON when a signal is present at the analog input. (greater than 0.5mA for current, greater than 0.5V for voltage).
For each of the single-ended analog channels, the LED indicates will come ON when a signal is present at the analog input. (greater than 0.5mA for current, greater than 0.5V for voltage).

Analog Outputs – Each analog output has an LED in series that indicates the output current by increasing or decreasing the intensity of the LED. For example, at 4 mA the LED appears dimmed, and at 20 mA, the LED appears bright.

Ethernet LEDs
On the end plate, the Ethernet socket incorporates two LEDs that indicate the Ethernet status.

100M – Green LED indicates presence of a 100-Mbps Ethernet connection. With a 10-Mbps connection, the LED is off.

LINK – Orange indicates an Ethernet connection. The LED briefly flashes with activity on the VUE, The front panel ETH LED provides additional indication of the Ethernet status.



Ethernet Port

Appendix C – Register Memory Map

Digital Output Registers (coils)

Address range	Description
0001 – 0008	Local DIO1–DIO8 as digital outputs
0009 – 0020	Spare
0021 – 0400	Space for locally attached 115s expansion I/O modules. Twenty register per module address, maximum number of modules is 19.
0401 – 6000	General purpose bit storage used for: Staging area for data concentrator; Fieldbus mappings storage; Force mapping registers
6001 – 10000	Not Available

Digital Output Registers (bits)

Address range	Description
10001 – 10008	Local DIO1–DIO8 as digital inputs
10009 – 10020	Set point status from analog inputs 1 through 12
10021 – 10400	Space for locally attached 115s expansion I/O modules. Twenty register per module address, Maximum number of modules is 19.
10401	Reserved - Used for repeater status indication
10402-10405	Radio hard fault status flags
10402	Radio power amplifier over temperature
10403	Radio general hardware fault
10404	Radio frequency lock error
10405	Antenna VSWR fault
10406 – 16000	General purpose bit storage used for: Staging area for data concentrator; Fieldbus mappings storage;
16001 – 20000	Not Available

Digital Output Registers (word)

Address range	Description	
30001 – 30004	Local AI1–AI4 (analog inputs, current mode) AI1 and AI2: 4–20 mA differential AI3 and AI4: 4–20 mA sink	
30005	Local supply voltage 0–40 V scales to 0-20mA	
30006	Local 24 V loop voltage 0–40 V scales to 0-20mA	
30007	Local battery voltage 0–40 V scales to 0-20mA	
30008	115S supply voltage 0–40 V scales to 0-20mA	
30009 – 30010	Local AI1, AI2, Voltage Mode. 0-24V Scales to 0-24mA.	
30011 – 30012	Local AI3, AI4, Voltage Mode. 0-5V Scales to 0-20mA	
30013 – 30016	Local pulse input rates: PI1–PI4	
30018 – 30020	Spare	
30021 - 30400	Space for locally attached 115s expansion I/O modules. Twenty registers per module address, maximum number of modules is 19.	
30401	RSSI: When configured as a Remote, MeshNode, Repeater, or Manual Client, the RSSI of the connected upstream device in (negative)dBm	
30402	Connected Time: When configured as a Remote, MeshNode, Repeater, or Manual Client, the time (in hours) that the connection to the upstream device has been made.	
30403	Generation Count: When configured as a Remote, MeshNode, Repeater, or Manual Client, the generation count of the connection to the upstream device. This is the number of times the connection has been lost and re-established	
30404 – 30405	Upstream IP Address: When configured as a Remote, MeshNode, Repeater, or Manual Client, the IP Address of the upstream device.	
	Most Significant Byte	High byte of Register 30404
	Second Byte	Low byte of Register 30404
	Third Byte	High byte of register 30405
	Least Significant Byte	Low byte of register 30405
30406	Current Radio Channel for frequency agility	
30407 – 30408	Radio Transmit Frequency (in Hz). 32-bit. Most significant word at lower (odd) address.	

Address range	Description
30409 – 30410	Radio Receive Frequency (in Hz). 32-bit. Most significant word at lower (odd) address. (As for Transmit Frequency)
30411	Module uptime: The time (in hours) that this module has been up and running
30412	Channel Utilization % (average of last 60 seconds)
30413	Background Noise (average of last 60 seconds)
30414	Tx retry % (average of last 60 seconds): The percentage of total transmissions that required at least one retry
30415	Tx failed % (average of last 60 seconds): The percentage of total transmissions that failed to get an acknowledgement after all retries exhausted.
30416 – 30419	Channel Utilization, Background noise, Tx Retry % and Tx Failed % (average of the last 60 minutes)
30420 – 30423	Channel Utilization, Background noise, Tx Retry % and Tx Failed % (average of the last 60 hours)
30424	Radio Power Amplifier Temperature. Actual temperature is reading - 100 °C. (-40 °C reads as 60, 25 °C reads as 125, 70 °C reads as 170 etc).
30425	Radio primay connection data rate (Upstream data rate).
30426 – 30490	Spare - General purpose word storage used for: Staging area for data concentrator; Fieldbus mappings storage;
30491	Logic Engine Execution State:. 0 -> Stopped. 256 -> Running; 32768 -> Overrun
30494 – 30500	Internal information registers: serial number, firmware version and patch level
30494	First four digits of serial number (Encodes Manufacture Month & Year
30495	Next three digits of serial number (Encodes Manufactured Firmware version)
30496	Remaining four digits of the serial number
30497	First part of Current Firmware version
30498	Second part of Current Firmware version
30499	Third part of Current firmware version
30500	Patch Level of current firmware version
30501 – 32000	General purpose word storage used for: Staging area for data concentrator; Fieldbus mappings storage;
32001 - 32255	RSSI List: When configured as an Base, Repeater, or Manual AP. The RSSI of each connected downstream is added to an I/O register according to the last byte of that device's IP Address. For example, a downstream device with IP Address 192.168.0.199 will have its RSSI stored in I/O register 32000 + 199 = 32199. If no device is connected with that IP address, the corresponding register has the value Zero.
32256 – 36000	General purpose word storage used for: Staging area for data concentrator; Fieldbus mappings storage;
36001 - 36008	Local pulsed inputs 1–4, big endian format Most significant word at lower/odd address
36009 – 36040	Spare space for 32-bit register values
36041 – 38000	Not Available
38001 - 38032	Local analog inputs as floating point values. ModScan format (sign + exponent + most significant 7 bits of significant at even/higher addressed location; lower 16 bits of significant at lower/odd addressed location) (example: Analog input 1 at 12.3 mA gives registers 38001=CCCD, 38002=4144)
38033 – 38040	Spare space for floating point values
38041 – 40000	Not Available

Output Registers (holding registers)

Address range	Description
40001 – 40002	Local AO1 and AO2:analog outputs
40003 – 40020	Spare
40021 – 40400	Space for locally attached 115s expansion I/O modules. Twenty registers per module address, maximum number of modules is 19.
40401 – 46000	General purpose word storage area used for: Staging area for data concentrator; Fieldbus mappings storage
46001 – 46008	Local pulsed outputs 1–4. Big endian format. Most significant word at lower/odd address
46009 – 46040	Spare 32-bit registers
46041 – 48000	Not Available
48001 – 48004	Local analog outputs as floating point values. ModScan format (sign + exponent + most significant 7 bits of significant at even/higher addressed location) Lower 16 bits of significant at lower/odd addressed location (example: Analog output 1 at 12.3 mA gives registers 48001=CCCD, 48002=4144)
48005 – 48040	Spare space for floating point values
48041 Onwards	Not available

Physical I/O Registers

I/O	Input	Output
Digital I/O 1	10001	1
Digital I/O 2	10002	2
Digital I/O 3	10003	3
Digital I/O 4	10004	4
Digital I/O 5	10005	5
Digital I/O 6	10006	6
Digital I/O 7	10007	7
Digital I/O 8	10008	8
Analog Input 1 (mA)	30001	—
Analog Input 2 (mA)	30002	—
Analog Input 3 (mA)	30003	—
Analog Input 4 (mA)	30004	—
Input 5 – Local V Supply	30005	—
Input 6 – Local +24 V Analog Loop	30006	—
Input 7 – Local V Battery	30007	—
Input 8 – Local V Expansion I/O	30008	—
Analog Input 1 (Volts)	30009	—
Analog Input 2 (Volts)	30010	—
Analog Input 3 (Volts)	30011	—
Analog 6 Set point	10014	—
Analog 7 Set point	10015	—
Analog 8 Set point	10016	—
Analog 9 Set point	10017	—
Analog 10 Set point	10018	—
Analog 11 Set point	10019	—
Analog 12 Set point	10020	—
Analog Output 1	—	40001
Analog Output 2	—	40002
Pulsed Input 1 Count	36001-36002	—
Pulsed Input 2 Count	36003-36004	—
Pulsed Input 3 Count	36005-36006	—
Pulsed Input 4 Count	36007-36008	—
Pulsed Input 1 Rate	30013	—
Pulsed Input 2 Rate	30014	—
Pulsed Input 3 Rate	30015	—
Pulsed Input 4 Rate	30016	—
Pulsed Output 1 Count	—	46001-46002
Pulsed Output 2 Count	—	46003-46004
Pulsed Output 3 Count	—	46005-46006
Pulsed Output 4 Count	—	46007-46008
Analog Input 1 Floating Point (mA)	38001-38002	—
Analog Input 2 Floating Point (mA)	38003-38004	—
Analog Input 3 Floating Point (mA)	38005-38006	—
Analog Input 4 Floating Point (mA)	38007-38008	—

I/O	Input	Output
Input 5 – Local V Supply Floating Point	38009-38010	—
Input 6 – Local +24 V Analog Loop Floating Point	38011-38012	—
Input 7 – Local V Battery Floating Point	38013-38014	—
Input 8 – Local V Expansion I/O Floating Point	38015-38016	—
Analog Input 1 Floating Point (Volts)	38017-38018	—
Analog Input 2 Floating Point (Volts)	38019-38020	—
Analog Input 3 Floating Point (Volts)	38021-38022	—
Analog Input 4 Floating Point (Volts)	38023-38024	—
Pulse Rate 1 Floating Point	38025-38026	—
Pulse Rate 2 Floating Point	38027-38028	—
Pulse Rate 3 Floating Point	38029-38030	—
Pulse Rate 4 Floating Point	38031-38032	—
Analog O/P Floating Point	—	48001
Analog O/P Floating Point	—	48002
Analog O/P Floating Point	—	48003
Analog O/P Floating Point	—	48004

Appendix D – Expansion I/O Registers

Adding expansion I/O modules to the VUE will automatically add the I/O from the VUE-EX modules to the internal VUE I/O store. To calculate the register location in the I/O store, find the address of the I/O point in the tables in this appendix, and then add the offset. The offset is the Modbus address, multiplied by 20.

Examples

- Digital input #1 on a VUE-EX with address 5 would be: (5x20) +10001 = 10101
- Digital output #2 on a VUE-EX with address 6 would be: (6x20) +2 = 122
- Analog input #3 on a VUE-EX with address 3 would be: (3x20) +30003 = 30063.
- Analog output #8 on a VUE-EX with address # 7 would be: (7x20) + 40007 = 40147

I/O Store for VUE-EX-11 Expansion I/O Modules

I/O Store	Description
0001 + Offset 0016 + Offset	DIO Outputs 1-16
10001 + Offset 10016 + Offset	DIO Inputs 1-16
10019 + Offset	Modbus Comms Fail indication for VUE-EX Module
10020 + Offset	Modbus Comms Fail indication (inverse) for this VUE-EX module
30001 + Offset 30004 + Offset	VUE-EX-11 pulsed input rate 1-4
30005 + Offset 30012 + Offset	VUE-EX-11 pulsed input count
30017 + Offset	Modbus Error counter for VUE-EX Module
30018 + Offset	Modbus Last Error code for this VUE-EX module
30019 + Offset	Modbus Lost Link counter for this VUE-EX
30020 + Offset	Module type (0x0101)=257/error status
40009 + Offset 40016 + Offset	Pulsed output target 1-8 (1 register per pulsed output)

I/O Store for VUE-EX-12

I/O Store	Description
0001 + Offset 0008 + Offset	DIO Outputs 1-8
10001 + Offset 10008 + Offset	DIO Inputs 1-8
10019 + Offset	Modbus Error indication for VUE-EX Module
10020 + Offset	Detected indication for this VUE-EX module
30001 + Offset 30008 + Offset	Inputs AIN 1 – AIN 8
30017 + Offset	Modbus Error counter for VUE-EX Module
30018 + Offset	Modbus Last Error code for this VUE-EX module
30019 + Offset	Modbus Lost Link counter for this VUE-EX

30020 + Offset	Module type (0x0201)=513/error status
40009 + Offset 40016 + Offset	Pulsed output target 1-8 (1 register per pulsed output)

I/O Store for VUE-EX-113

I/O Store	Description
0001 + Offset 0008 + Offset	DIO Outputs 1-8
10001 + Offset 10008 + Offset	DIO Inputs 1-
10019 + Offset	Modbus Error indication for VUE-EX Module
10020 + Offset	Detected indication for this VUE-EX module
30017 + Offset	Modbus Error counter for VUE-EX Module
30018 + Offset	Modbus Last Error code for this VUE-EX module
30019 + Offset	Modbus Lost Link counter for this VUE-EX
30020 + Offset	Module type (0x0301)=769/error status
40001 + Offset 40008 + Offset	Analog output 1-8
40009 + Offset 40016	Pulsed output target 1-8 (1 register per pulsed output)

Appendix E – Modbus Error Codes

The following are Modbus error response codes that the Master will generate and write to a general purpose analog register (30501, 40501, and so on) in the event of a poll fail.

Dec code	Hex code	Name	Meaning
65281	FF01	Illegal Function	The function code received in the query is not an allowable action for the server (or slave). This may be because the function code is only applicable to newer devices, and was not implemented in the unit selected. It might also indicate that the server (or slave) is in the wrong state to process a request of this type.
65282	FF02	Illegal Data Address	The data address received in the query is not an allowable address for the server (or slave). More specifically, the combination of reference number and transfer length is invalid. For a controller with 100 registers, the PDU addresses the first register as 0, and the last one as 99. If a request is submitted with a starting register address of 96 and a quantity of 4 registers, this request will successfully operate on registers 96, 97, 98, 99. If a request is submitted with a starting register address of 96 and a quantity of 5, this request will fail with Exception Code 0x02 "Illegal Data Address."
65283	FF03	Illegal Data Value	A value contained in the query data field is not an allowable value for server (or slave). This indicates a fault in the structure of the remainder of a complex request. For example, it may indicate that the implied length is incorrect. It does not mean that a data item submitted for storage in a register has a value outside the expectation of the application program. The Modbus protocol is unaware of the significance of any particular value of any particular register.
65384	FF04	Slave Device Failure	An unrecoverable error occurred while the server (or slave) was attempting to perform the requested action.
65285	FF05	Acknowledge	Specialized use in conjunction with programming commands. The server (or slave) has accepted the request and is processing it, but significant time will be required to complete this task. This response is returned to prevent a timeout error from occurring in the client (or master).
65286	FF06	Slave Device Busy	Specialized use in conjunction with programming commands. The server (or slave) is engaged in processing a long–duration program command. The client (or master) should retransmit the message later when the server (or slave) is free.
65288	FF08	Memory Parity Error	Specialized use in conjunction with function codes 20 and 21 and reference type 6, to indicate that the extended file area failed to pass a consistency check.
65290	FF0A	Gateway Path Unavailable	Specialized use in conjunction with gateways. Indicates that the gateway was unable to allocate an internal communication path from the input port to the output port for processing the request. Typically indicates that the gateway is mis-configured or overloaded.
65291	FF0B	Gateway Device Failed to Respond	Specialized use in conjunction with gateways. Indicates that no response was obtained from the target device. Typically indicates that the device is not present on the network.
65024	FE00	Invalid Responsefrom Slave	Command type or slave address did not match request (probably another unit).
64512	FC00	Server Offline	Could not connect to the Modbus TCP server.
63488	F800	Invalid Local Memory Address	Local address is invalid in the command. The memory location does not exist or is not initialized.
65535	FFFF	No Response to the Poll	There was no response to the poll message.

Appendix F – Secure Hardening Guidelines

Introduction

The VUE has been designed with Cybersecurity as an important consideration. A number of Cybersecurity features are available in the product. By implementing these according to the recommendations in this appendix you will minimize the Cybersecurity risk for your system. This section "secure configuration" or "hardening" guidelines provide information to the users to securely deploy and maintain their product to adequately minimize the cybersecurity risks to their system. Intuicom is committed to minimizing the Cybersecurity risk in its products and deploys cybersecurity best practices and latest cybersecurity technologies in its products and solutions; making them more secure, reliable and competitive for our customers.

Category	Description
Asset identification and Inventory	Keeping track of all the devices in the system is a prerequisite for effective management of Cybersecurity of a system. Ensure you maintain an inventory of all the components in your system in a manner in which you uniquely identify each component. To facilitate this the VUE supports the following identification information - manufacturer, type, serial number, f/w version number, and location. If you are using the Configuration Utility, you can access the device identification information from the "Unit Details" tree node. You can also access the device identification information from the main device web-page. You can add your own device specific information in the Module Information screen available from the right hand side menu.
Restrict physical access	The VUE supports Industrial Control Protocols which don't offer cryptographic protections at protocol level. Additionally, the device incorporates USB port that can interface with USB storage devices for upgrading the module firmware. These features expose the device to Cybersecurity risk. Physical security is an important layer of defense in such cases. The VUE is designed with the consideration that it would be deployed and operated in a physically secure location. • Physical access to cabinets and/or enclosures hosting VUE devices and the associated system should be restricted, monitored and logged at all times. • Physical access to the communication lines should be restricted to prevent any attempts of wiretapping, sabotage. It's a best practice to use metal conduits for the communication lines running between cabinets. • An attacker with unauthorized physical access to the device could cause serious disruption of the device functionality. A combination of physical access controls to the location should be used, such as locks, card readers, and/or guards etc. • Although the VUE will not accept firmware images that are not cryptographically signed, it is still best practice to restrict any unknown/un-authorized USB drives from being connected to the VUE.
Restrict logical access to equipment	It is extremely important to securely configure the logical access mechanisms provided in in the VUE to safeguard the device from unauthorized access. The provides administrative, operational, configuration roles for device users. Intuicom recommends that the available access control mechanisms be used properly to ensure that access to the system is restricted to legitimate users only and to ensure that these users are restricted to only the privilege levels necessary to complete their job roles/functions. • Ensure default credentials are changed upon first login. The VUE should not be commissioned for production with Default credentials; it's a serious Cybersecurity flaw as the default credentials are published in the manuals. • No password sharing – Make sure each user gets his/her own password vs. sharing the passwords. Security monitoring features of VUE are created with the view of each user having his/her own unique password. Security controls will be weakened as soon as the users start sharing a password. • Use the provided roles (Admin, Manager, Operator) to ensure users only gain access as necessary for the business /operational need. Grant the users' privileges as per their job requirements; follow principle of least privilege (minimal authority level required) and least access (minimize unnecessary access to system resources). • Perform periodic account maintenance (remove unused accounts).

<table>
<tr><td></td><td>

Change passwords and other system access credentials regularly (recommend every 90 days).
Ensure that user access is revised when there is a change in personnel's security status, access levels, job role or when a user leaves the organization or group.

You can find a description of the user management functions in the section "User Management "

Passwords must be at least 8 characters, and should not consist of easily guessed words or dates.

When distributing credentials (username and password) to users, you should make sure that this information is not compromised during distribution. The following methods are recommended:

In person or by Phone
By physical post
By email – Zip and encrypt the credential file, and provide the password to unzip the credentials in a separate email or by phone.

Access to the device is through HTTP Digest Authentication. Note that this secures the password exchange from eavesdropping, but communication via HTTP protocol is not secured from eavesdropping
</td></tr>
<tr><td>Conduct regular Cybersecurity risk analyses of the organization/system.</td><td>Intuicom has worked with third-party security firms to perform system audits, both as part of a specific customer's deployment and within Intuicom's own development cycle process. Intuicom can provide guidance and support to your organization's effort to perform regular cybersecurity audits or assessments.</td></tr>
<tr><td>Restrict network access</td><td>
Protect your SSID - To avoid outsiders easily accessing your radio network, avoid publicizing System address (SSID). On Network configuration page user need to change the default SSID to make it more difficult to guess.

In the event that a device is lost or stolen, ensure that the encryption key used to secure communications on the radio network is changed.

The VUE uses the following IP protocol ports which may need to be configured in your network firewall:
<table>
<tr><td>Modbus protocol:</td><td>TCP port 502 (Default, Configurable)</td></tr>
<tr><td>Intuicom WIB Protocol:</td><td>UDP port 4370</td></tr>
<tr><td>Serial transfer protocol:</td><td>TCP, UDP port 24 (Default, Configurable)</td></tr>
<tr><td>DNP3 Protocol:</td><td>TCP, UDP port 20000 (Default Configurable)</td></tr>
<tr><td>Remote Configuration:</td><td>TCP port 80 (HTTP)</td></tr>
<tr><td>Remote Dashboard:</td><td>TCP port 80 (HTTP)</td></tr>
</table>
Each of these protocols are disabled by default. They must be enabled on the corresponding configuration page before they are enabled on the network ports. HTTP access is always open on the USB port (IP Address 192.168.111.1).

You can view a list of open ports on the Statistics Page under "TCP/UDP Statistics". This section lists all open ports. You should configure your device to whitelist remote devices which will have access to the device. By whitelisting only the IP addresses that should have access to the device functions, you can reduce the chance of unintended operation. This is particularly important for MODBUS and WIB protocols which can remotely control the device's outputs. Configure your IP Whitelist on the "Network Filtering" page. Disable the "Easy IP Filtering" option and add specific IP Filter rules for each remote device that needs to access the device.

You can prioritize data according to its purpose by using the VLAN functionality under "Advanced Networking >> VLAN". Each VLAN group can be assigned a separate priority, in the range 1 to 7. Messages sent over the higher priority VLAN groups will be transmitted first on the radio channel.
</td></tr>
<tr><td>Logging and event management</td><td>
Best practices

Intuicom recommends that that all remote interactive sessions are logged, including all administrative and maintenance activities.
Ensure that logs are backed up; retain the backups for a minimum of 3 months or as per organization's security policy.
Perform log review at a minimum every 15 days.
You can access and download the device log files remotely from a web-browser on your PC if you have remote access enabled. You can also automatically load log files by plugging a Flash memory stick into the USB-A port on the side of the module. For more detail, refer to the section "Retrieving Logged Data".

This exercise should be conducted in conformance with established technical and regulatory frameworks such as IEC 62443 and NERC-CIP.
</td></tr>
</table>

Plan for business continuity/cybersecurity disaster recovery	It's a Cybersecurity best practice for organizations to plan for business continuity. Establish an OT business continuity plan, periodically review and, where possible, exercise the established continuity plans. Make sure offsite backups include: • Backup of the latest firmware. Make it a part of SOP to update the backup copy as soon as the latest f/w is updated on Backup of the most current configurations. • Documentation of the most current User List. • Save the current configurations of the device.

References

[R1] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015.

https://ics-cert.us-cert.gov/Standards-and-References

[R2] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009.

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

Appendix G – Firmware Upgrade

For firmware upgrades contact Intuicom Support.

Appendix H – Intuicom Support

Intuicom, Inc.
4909 Nautilus Court, Ste 111
Boulder, CO 80301 USA
(303) 449-4330
support@intuicom.com

Appendix I - Warranty

LIMITED WARRANTY TO END-USERS

Intuicom, Inc.
4909 Nautilus Court North, Suite 111 BOULDER,
CO 80301

A. Standard Limited Warranty for Software Products. For Products that include a software license, INTUICOM makes a limited warranty to the End User that the software will perform substantially in accordance with the accompanying written materials and that the transfer media on which the Product is provided will be free from defects in materials or workmanship under normal use and service for a period of ninety (90) days from the date of delivery (the "Limited Warranty") pursuant to the software license included with the Product. The software license specifically disclaims all other warranties relating to the Products, including any and all other warranties with respect to the performance of the Products.

B. Hardware and Other Equipment Manufactured By Intuicom. Hardware products manufactured by INTUICOM include a limited warranty for defects in materials or workmanship under normal use and service for a period of one (1) year from the date of delivery. Intuicom, at its sole discretion, will repair or replace hardware covered under this limited warranty. Cables, antennas or other accessories manufactured by INTUICOM include a limited warranty for defects in materials or workmanship under normal use and service for a period of ninety (90) days from the date of delivery. Repairs not covered under this limited warranty will be billed as set forth in INTUICOM's current Hardware Service Policy and Instructions.

C. Hardware Manufactured By Others. INTUICOM makes no warranties whatsoever with respect to Hardware manufactured by third parties. Customers shall look only to the original manufacturer of the Hardware, pursuant to the terms of any manufacturer warranty for any alleged defects and indemnifies and holds INTUICOM harmless from and against any claims by any party related directly or indirectly to any defects in the Hardware, and functional failure, improper operation, failure to operate according to specifications or any other matter related to the Hardware. INTUICOM shall not be liable or responsible for the failure of the Manufacturer to perform under or honor any warranty with respect to the Hardware. Customer acknowledges and agrees that Customer shall have the risk of any loss, damage or functional failure related to the HARDWARE and shall have the responsibility for maintaining the proper operation of the HARDWARE and complying with all maintenance guidelines and specifications from the Manufacturer and all other conditions to receiving warranty coverage from the Manufacturer.

D. No Other Warranty. EXCEPT FOR THE EXPRESS STANDARD LIMITED WARRANTY REFERENCED ABOVE, INTUICOM GRANTS NO OTHER WARRANTIES, EXPRESS OR IMPLIED, REGARDING THE PRODUCTS, THEIR FITNESS FOR ANY PURPOSE, THEIR QUALITY, THEIR MERCHANTABILITY OR OTHERWISE. INTUICOM DOES NOT MAKE BY VIRTUE OF THIS AGREEMENT OR ANY PRODUCT ORDER, AND HEREBY EXPRESSLY DISCLAIMS, ANY OTHER REPRESENTATION OR WARRANTY OF ANY KIND WITH RESPECT TO THE PRODUCTS.

E. Limitation of Liability. IN NO EVENT WILL INTUICOM BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, BUSINESS INTERUPTION, CATESTROHPIC, PUNITIVE OR OTHER DAMAGES WHICH MAY BE CLAIMED TO ARISE IN CONECTION WITH ITS PRODUCTS, REGARDLESS OF THE LEGAL THEORY BEHIND SUCH CLAIMS, WHETHER IN TORT, CONTRACT OR UNDER ANY APPLICABLE STATUTORY OR REGULATORY LAWS, RULES, REGULATIONS, EXECUTIVE OR ADMINISTRATIVE ORDERS OR DECLARATIONS OR OTHERWISE, EVEN IF INTUICOM HAS BEEN ADVISED OR OTHERWISE HAS KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES AND TAKES NO ACTION TO PREVENT OR MINIMIZE SUCH DAMAGES. IN THE EVENT THAT REGARLDESS OF THE WARRANTY DISCLAIMERS AND HOLD HARMLESS PROVISIONS INCLUDED ABOVE INTUICOM IS SOMEHOW HELD LIABLE OR RESPONSIBLE FOR ANY DAMAGE OR INJURY, INTUICOM'S LIABILITY FOR ANY DAMAGES SHALL NOT EXCEED THE PROFIT REALIZED BY INTUICOM ON THE SALE OR PROVISION OF THE HARDWARE TO THE CUSTOMER.