Weidmüller

Wireless I/O, Ethernet Modem and Gateway

WI-I/O-415-U2 / WI-MOD-415-E

User Manual

Product Notices

ATTENTION

INCORRECT TERMINATION OF SUPPLY WIRES MAY CAUSE INTERNAL DAMAGE AND WILL VOID THE WARRANTY. TO ENSURE THAT YOUR WI-IO-415-U2 WIRELESS I/O AND GATEWAY ENJOYS A LONG LIFE, CHECK THIS USER MANUAL TO VERIFY THAT ALL CONNECTIONS ARE TERMINATED CORRECTLY BEFORE TURNING ON POWER FOR THE FIRST TIME.

Safety notices

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.

CAUTION

TO COMPLY WITH FCC RF EXPOSURE REQUIREMENTS IN SECTION 1.1310 OF THE FCC RULES, ANTENNAS USED WITH THIS DEVICE MUST BE INSTALLED TO PROVIDE A SEPARATION DISTANCE OF AT LEAST 20 CM FROM ALL PERSONS TO SATISFY RF EXPOSURE COMPLIANCE.

DO NOT OPERATE THE TRANSMITTER WHEN ANYONE IS WITHIN 20 CM OF THE ANTENNA. ENSURE THAT THE ANTENNA IS CORRECTLY INSTALLED IN ORDER TO SATISFY THIS SAFETY REQUIREMENT.

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.

Example Net gain calculation for 400MHz

Manufacturer	Model number	Coax kit	Net
WEIDMULLER	WI-ANT-440MHZ-5DB OMNI NF	CC3/450	3dBgain
WEIDMULLER	WI-ANT-420MHZ-9DBDYAGINF	CC10/450	4 dBgain
WEIDMULLER	WI-ANT-420MHZ-9DBDYAGINF	CC20/450	6 dB gain

Hazardous location notices

The WI-IO-415-U2-C4-EX, WI-IO-415-U2-C3-EX, WI-MOD-415-E-C9-EX, WI-MOD-415-E-C4-EX and WI-MOD-415-E-C3-EX comply with the following standards:

- IEC 60079-0:2012/A11:2013
- IEC 60079-15:2010

The WI-IO-415-U2-C4-EX, WI-IO-415-U2-C3-EX, WI-MOD-415-E-C9-EX, WI-MOD-415-E-C4-EX, and WI-MOD-415-E-C3-EX comply 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.

The WI-IO-415-U2-C4-EX, WI-IO-415-U2-C3-EX, WI-MOD-415-E-C9-EX, WI-MOD-415-E-C4-EX, and WI-MOD-415-E-C3-EX are 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 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.

The earth/ground terminal of this equipment shall be connected to earth ground in the equipment installation.

The external power supply installed with this equipment shall be a listed, Class 2 power supply, with a rated output between 15 Vdc and 30 Vdc, and minimum 3500 mA.

General Notices

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

WEIDMULLER products use 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 noise and interference can cause product operation delays or operation failure. Like all industrial electronic products, WEIDMULLER products can 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 first consulting Weidmuller.

To avoid accidents during maintenance or adjustment of remotely controlled equipment, all equipment should be first disconnected from the WI-415 Series 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.”

The WI-415 Series modules are not suitable for use in explosive environments without additional protection.

The WI-415 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.

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 (aluminum) 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 Weidmuller 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 Weidmuller 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 t o work to prevent any potential vulnerability of their products and systems in their environment.

At Weidmuller 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.

Weidmuller strongly recommends our customers to apply the deployment practices that are outlined in the appendix to this document - "Secure hardening guidelines" on page 74.

Release notice

This is the update release of the WI-415 Series Wireless I/O and Gateway User Manual version 2.20, which applies to configuration software version 2.1.0.10 and firmware version 2.20. This user manual covers models WI-IO-415-U2-C and WI-MOD-415-C and Hazardous Location models WI-IO-415-U2-C-EX and WI-IO-415-U2-E-C-EX.

GNU General public license

Products Covered in this Manual

Freq. Band	Type	Part No.
148-174 MHz	WI-IO-415-U2-C1	7940107949
148-174 MHz (Hazloc Approved)	WI-IO-415-U2-C1-EX	7940107950
340-400 MHz	WI-IO-415-U2-C3	7940107957
340-400 MHz (Hazloc Approved)	WI-IO-415-U2-C3-EX	7940107958
400-480 MHz	WI-IO-415-U2-C4	7940107953
400-480 MHz (Hazloc Approved)	WI-IO-415-U2-C4-EX	7940107954
148-174 MHz	WI-MOD-415-E-C1	7940107951
148-174 MHz (Hazloc Approved)	WI-MOD-415-E-C1-EX	7940107952
340-400 MHz	WI-MOD-415-E-C3	7940107959
340-400 MHz (Hazloc Approved)	WI-MOD--415-E-C3-EX	7940107960
400-480 MHz	WI-MOD-415-E-C4	7940107955
400-480 MHz (Hazloc Approved)	WI-MOD-415-E-C4-EX	7940107956
928-960 MHz	WI-MOD-415-E-C9	7940107963
928-960 MHz (Hazloc Approved)	WI-MOD-415-E-C9-EX	3104830000

Table of contents

Introduction

Overview

The WEIDMULLER WI-415 Series 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 WEIDMULLER WI-415 Series is capable of providing IP-based I/O across sprawling industrial environments typical of industrial applications.

The WI-415 Series can serve as an end node or network gateway and is scalable to thousands of nodes. Gather-scatter and block mapping technology offer 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 WEIDMULLER WI-EX 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 WI-415 Series 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 page in the WI-Device Config utility, as described in “Configuration” on page 17.

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 WI-415 Series 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 WI-415 Series comes from the factory with WEIDMULLER 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 WI-415 Series device can have up to 19 expansion I/O modules (WEIDMULLER WI-EX) 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 WI-Device Config utility via Ethernet, remotely over the radio, or USB. Advanced users may configure the units by accessing the internal Web pages using a Web browser. The WI-Device Config utility is described in “Configuration” on page 17. For Web-based configuration, see “Configuring using the web configuration utility” on page 44.

Note: WI-415 Series product versions

These modules support wider temperature range, higher radio transmit power and faster radio throughput.

Module structure

The WI-415 Series 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 **Figure 1** and are described in “Register memory map” on page 68.
There are other registers within the database that can be used for system management.

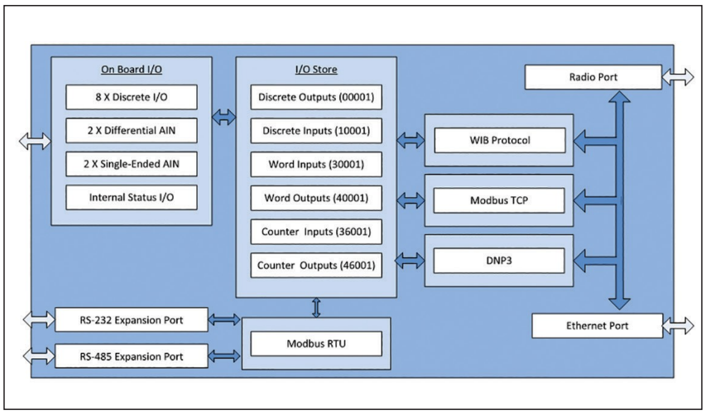


Figure 1. Module structure

The radio and Ethernet interfaces (see **Figure 1**) allow the WI-415 Series to communicate with other modules within the system using a proprietary protocol called WIB. I/O Messages from other WI-415 Series
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 WI-EX expansion I/O modules to be added to the module. Expansion I/O is dynamically added to the internal I/O of the WI-415 Series module by adding an offset to the address.

Getting started

Most applications for the WI-415 Series module require little configuration. The WI-415 Series has many sophisticated features, but if you do not require these features you can use this section to configure the units quickly.

To get started quickly:

1. Read “Installation” on page 3, which describes the power supply, antenna/coax connections, and I/O connections.
2. Power on the WI-415 Series module and set up a USB connection to your PC. For detailed steps, see “Connecting using the Configuration Utility” on page 17.
3. Install and run the WI-Device Config utility. For WI-Device Config installation instructions, see “Downloading and installing WI-Device Config” on page 17.

Installation

General

The WI-415 Series modules are housed in a 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.

Thermal

The WI-415 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 WI-415 Series 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 p and running (Network Diagnostics >> Custom Survey >> All Tx Frames).

If the device will be outside it’s 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.

WI-IO-415-U2-C and WI-MOD-415-C Power level and modulation

The charts below show the radio power relative to the maximum radio power for the WI-IO-415-U2-C and WI-MOD-415-C models. The maximum radio power depends on the radio modulation mode selected.

Refer to Table 1 below to relate power level, modulation and the power levels on the charts shown on the following pages.

Table 1

Legacy compatibility (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

Thermal Derating Charts for WI-IO-415-U2-C and WI-MOD-415-C operating from SUP inputs

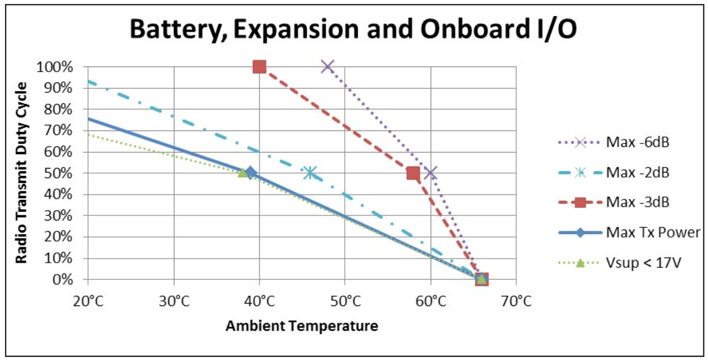


Figure 2. WI-415 Series Worst case.

The worst case occurs when you are using all features of the WI-IO-415-U2-C 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)
- WI-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.

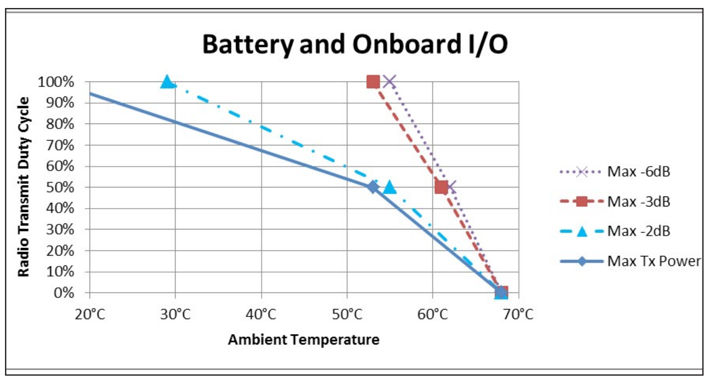


Figure 3. WI-IO-415-U2-C Battery Charging and onboard I/O.

As above, except without WI-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.

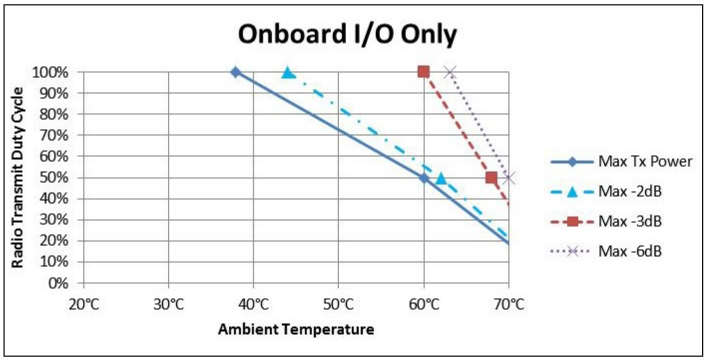


Figure 4. WI-IO-415-U2-C Onboard I/O only.

As figure 3, 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)
- WI-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.

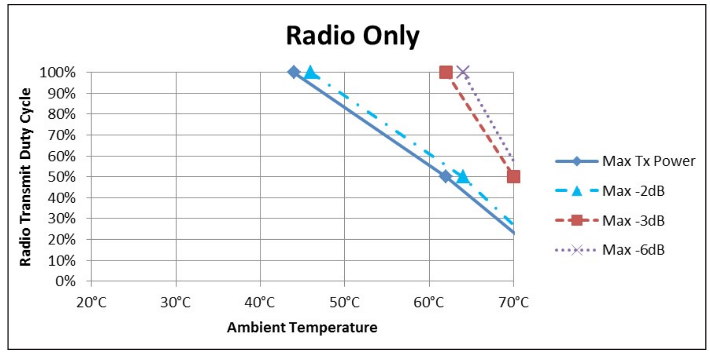


Figure 5. WI-415 Series Radio only.

Use this chart 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.

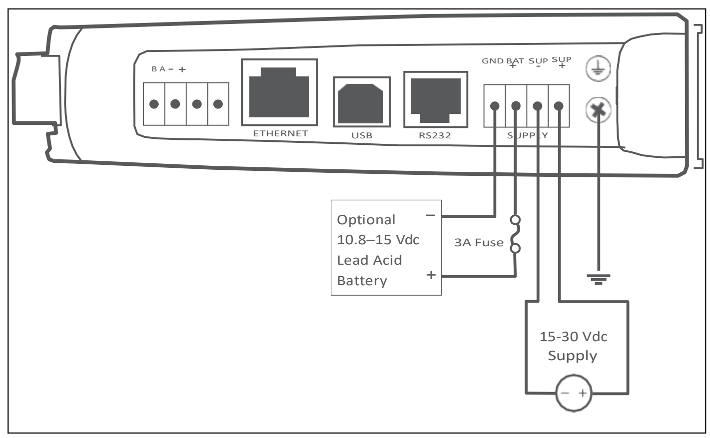


Figure 6. Supply connections

Power Supply

The WI-IO-415-U2-C and WI-MOD-415-C will operate from a 15–30 Vdc supply (nominal 24 Vdc) 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 operate from this battery if the main supply fails..

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 WI-415 Series, and to power the device's radio transmitter when it is sending data. A 24 Vdc 2.5 A power
supply such as PS-DINAC-24DC-OK 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 2** 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.

Table 2. Power supply current requirements

	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

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). **Table 3** shows the *additional* current from your power supply to support battery charging.

Table 3. Additional current 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	$I_{sup} = \frac{10.5}{V_{sup}}$

Powering expansion I/O modules

The WI-415 Series modules allow connection of WI-EX Series modules to the RS-485 port to provide expanded I/O capacity. You can use the "+" and "–" connections on the WI-415 Series to provide up to 500 mA supply for expansion I/O modules. If you have a back-up SLA battery connected to the WI-415 Series, 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.

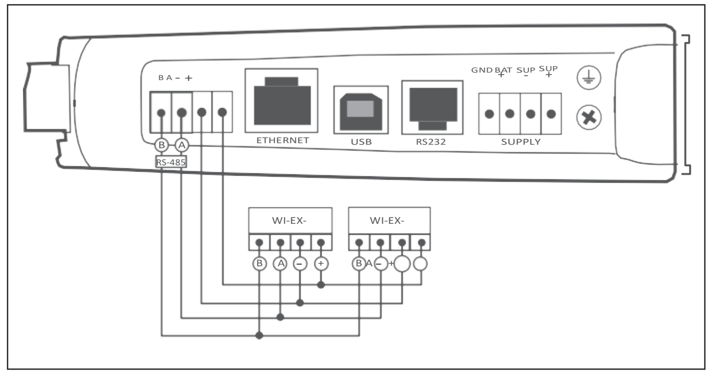


Figure 7. Expansion I/O power and RS-485

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. **Table 4** shows the *additional* current from your power supply to support expansion I/O connection.

Table 4. Additional supply current to support expansion I/O

	Expansion I/O current (I_{exp})	Current required (I_{sup}) Supply voltage		
		17 Vdc	**24 Vdc**	**30 Vdc**
Base operating current WI-EX	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	$I_{sup} = \frac{I_{exp} \times 18.4}{V_{sup}}$			

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 WI-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" on **page 3**).

Use **Table 5** 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 WI-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

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 59 for details). The values can also be mapped to a register or an analog output on another module within the network.

Table 6. Internal supply voltage registers

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	WI-EX supply voltage (0–40 V scaling).
38005–38008	Floating point registers that display the actual supply voltage, battery voltage, +24 V supply, and WI-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.

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 11** for details on how to configure these alarms.

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 WI-415 Series and WI-MOD-415 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 in^2 (2 mm^2), 14 AWG. If using the WI-415 Series with 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 8**.

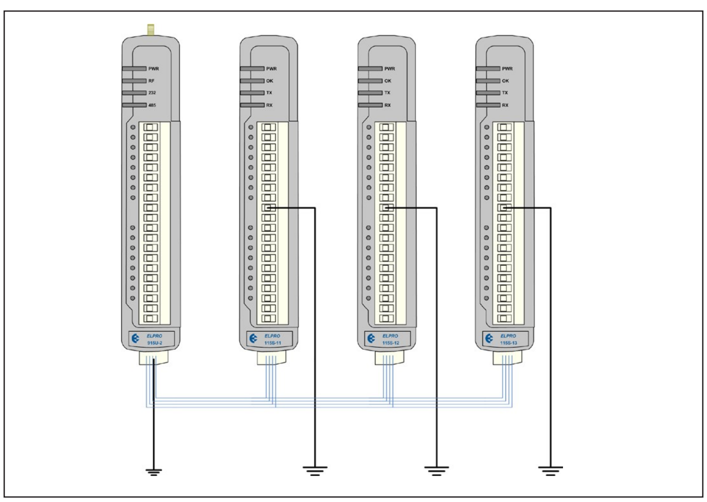


Figure 8. Grounding

Radio

The WI-415 series uses narrow band 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 WI-IO-415-U2-C and WI-MOD-415-E-C module support power levels from 10mW to 10W, and channel bandwidths of 6.25, 12.5 and 25 kHz.

The WI-IO-415-U2-C and WI-MOD-415-E-C 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 WI-IO-415-U2-C and WI-MOD-415-E-C also support FSK modulation for operation with
Legacy WI-IO-415-U2-H and WI-IO-415-U2-L models. In Legacy mode, 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 Wi-Fi applications. If you are familiar with 802.11, many of the radio networking concepts used in the 415 will also be familiar to you.

The data rates achievable with the WI-415 Series are significantly lower than those for Wi-Fi applications, so care must be taken to make the best use of the available channel bandwidth.

The WI-415 Series 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 "Radio" on page 6 for instructions on configuring the radio using the Configuration utility, and to "Configuring the locale" on **page 45** and "Quick start—basic device configuration" on **page 46** for instructions on how to configure the radio using the Web interface.

Antennas

Antennas can be either connected directly to the module's RF connector or connected via 50-ohm coaxial cable (such as RG58 Cellfoil or RG213) terminated with a male SMA coaxial connector. The higher the antenna is mounted, the greater the transmission range, but as the length of coaxial cable increases so do cable losses.

The net gain of an antenna and cable configuration is the gain of the antenna (in dBi) less the loss in the coaxial cable (in dB). Maximum net gain for the WI-415 Series will depend on the licensing regulation for the country of operation and the operating frequency.

Typical antennas gain and losses are:

Table 1. Typical antennas gains and losses

Antenna	Gain (dBi)
Dipole	2 dBi
Collinear	5 or 8 dBi
Directional (Yagi)	6–15 dBi
Cable type	**Loss (dB)**
RG58 cellfoil cable kits (3 m,10 m, 20 m)	–1 dB, –2.5 dB, –4.8 dB
RG213 per 10 m (33 ft)	–1.8 dB
LDF4-50 per 10 m (33 ft)	–0.5 dB

- The net gain of the antenna and cable configuration is determined by adding the antenna gain and the cable loss. For example, an 8 dBi antenna with 10 meters of Cellfoil (–2.5 dB) has a net gain of 5.5 dB (8 dB – 2.5 dB)

Dipole and Collinear antennas

Dipole and collinear antennas transmit the same amount of radio power in all directions, and are easy to install and use because they do not need to be aligned to the destination. The dipole antenna does not require any additional coaxial cable. However, a cable must be added if using any of the other collinear or directional antennas. In order to obtain the maximum range, collinear and dipole antennas should be mounted vertically, preferably at least one wavelength away (see **Figure 9** for distances) from a wall or mast and at least 3 ft (1 m) from the radio module.

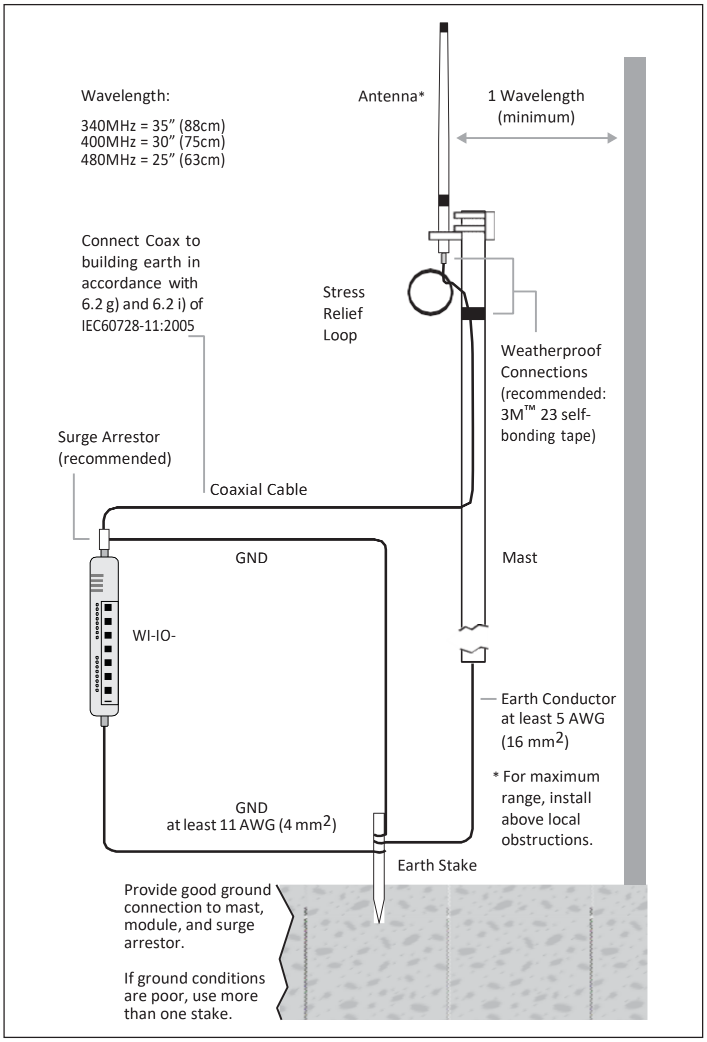


Figure 9. Antennas installation—Collinear/Dipole

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.

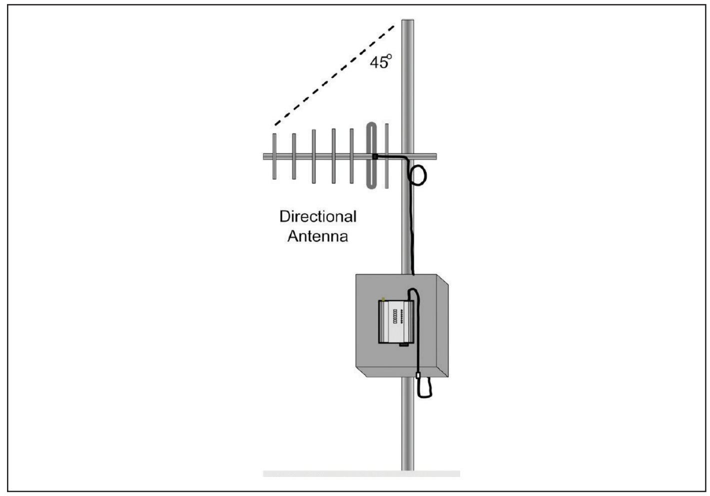


Figure 10. Directional antenna

Installation tips

Connections between the antenna and the coaxial cable should be carefully taped to prevent ingress of moisture. Moisture ingress in the coaxial cable is a common cause for problems with radio systems because it greatly increases the radio losses. We recommend that the connection be taped—first with a layer of PVC tape, next with vulcanizing tape (such as 3M™ 23 tape), and finally with another layer of PVC UV-stabilized insulating tape. The first layer of tape allows the joint to be easily inspected when troubleshooting because the vulcanizing seal can be easily removed (see **Figure 10**).

Where antennas are mounted on elevated masts, the masts should be effectively grounded to avoid lightning surges. For high lightning risk areas, approved WEIDMULLER surge suppression devices, such as the CSD-SMA-2500 or CSD-N-6000, should be fitted between the module and the antenna. If using non-WEIDMULLER 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.

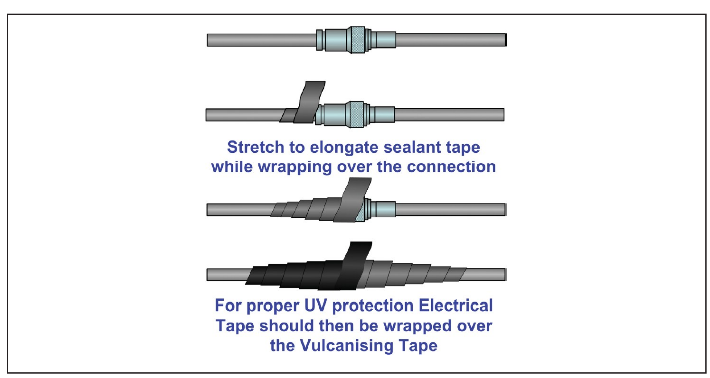


Figure 10. Vulcanizing tape

Connections

Bottom panel connections

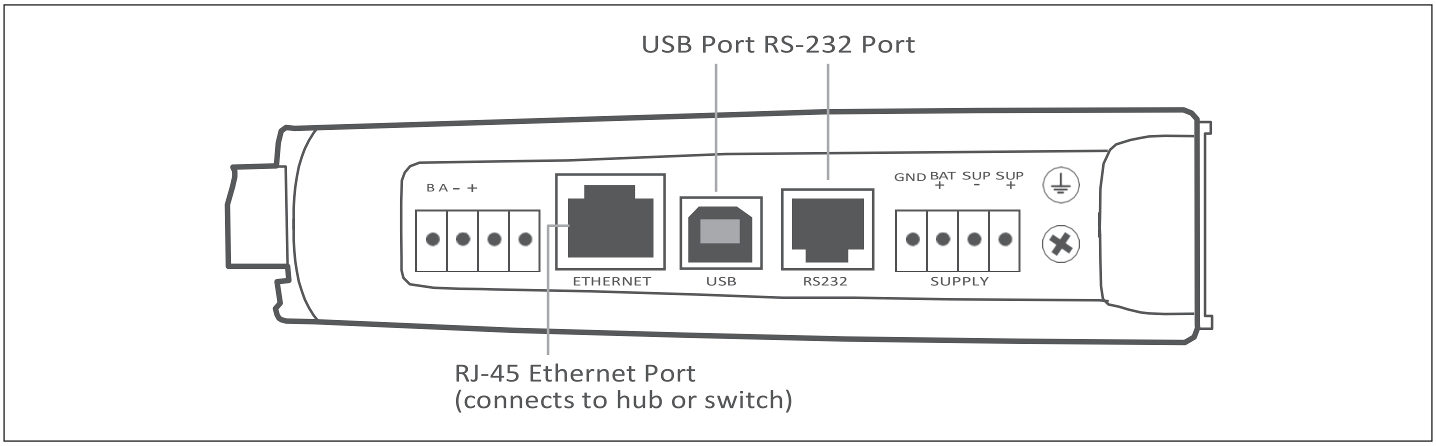


Figure 11. Bottom panel connections

Ethernet port

The WI-415 Series 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.

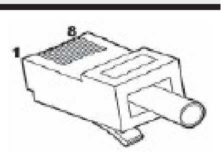
USB device port for configuration

The WI-415 Series 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.

RS-232 port

The WI-415 Series 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.

Table 2. RJ-45 connector

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	

RS-485 port with Modbus support

The WI-415 Series 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 WI-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 WI-EX expansion I/O modules, remember to enable the RS-485 termination resistor switch that is located on the end module.

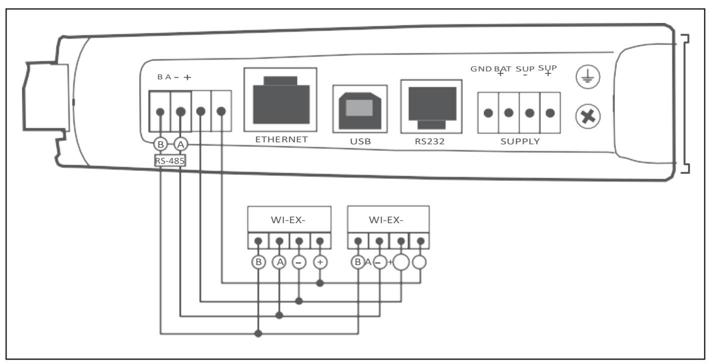


Figure 12. RS-485 connections

Side access configuration panel

A small access panel on the side of the module hides a factory boot switch, USB host port, and a small bank of DIP switches that are used for analog input voltage and current selection, external boot, and default configuration settings. Use a screw-driver to unscrew the retained screw to open the access panel.

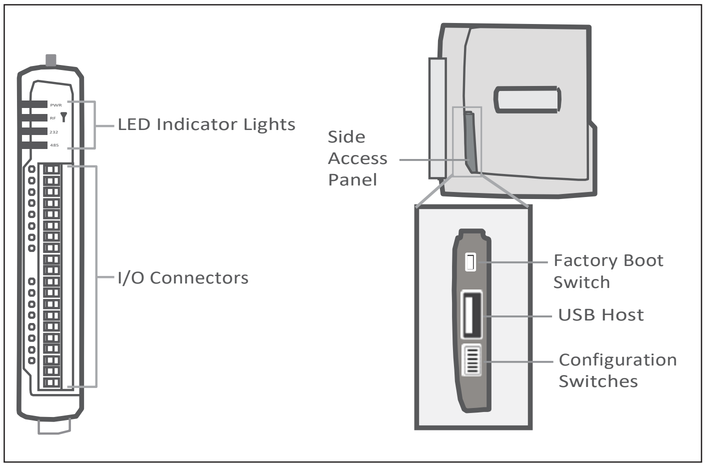


Figure 13. Access panel

Factory boot switch

The factory boot switch is used for factory setup and diagnostics. This switch should only be used if advised by WEIDMULLER technical support.

USB host port

This port is a USB host (master port) that can interface with USB storage devices for upgrading the module firmware and for uploading logged data files. For details, see “To perform a full firmware upgrade using USB flash drive” on **page 77**. Also see “Data logging” on **page 62**.

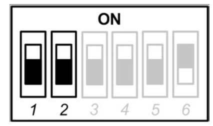
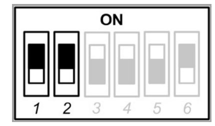
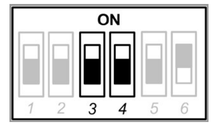
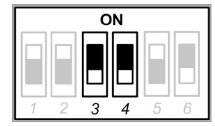
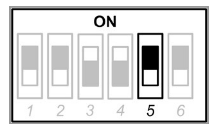
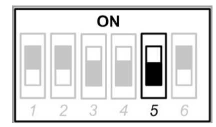
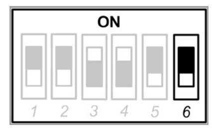
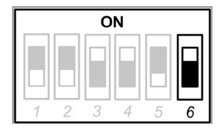
DIP switches

The DIP switches are used to select a number of functions within the module, as shown in the following table.

- **DIP switches 1 to 2**—Used for measuring current or voltage on analog input 3. Set DIP switches to “on” to measure current (0–20 mA) and “off” for voltage (0–5 Vdc).
- **DIP switches 3 to 4**—Used for measuring current or voltage on analog input 4. Set DIP switches to “on” to measure current (0–20 mA) and “off” for voltage (0–5 Vdc).
- **DIP switch 5**—Not used.
- **DIP switch 6**—When set to “on” (enabled) and the module is restarted, the module boots to a recovery mode allowing you to restore the factory default configuration. See “Restoring the factory default settings” on page 65.

⚠ **Note**: When the device is powered up with DIP switch 6 “on,” radio and I/O functionality is disabled.

Table 3. Switch functions

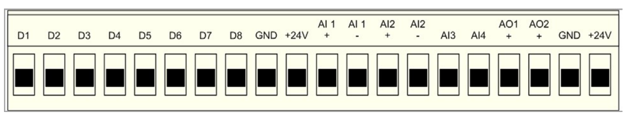
Switch	Function	Current	Voltage
DIP 1 and 2	Analog input 3		
DIP 3 and 4	Analog input 4		
Switch	**Function**	**Disabled**	**Enabled**
DIP 5	Not used		
DIP 6	Setup mode		

Front panel connections

WI-IO-415-U2 Front Panel Connections

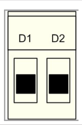
The front panel on the WI-IO-415-U2 module provides connections for the following:

- Eight digital input/output (D1–D8)
- Two 12-bit, 0.1% accuracy differential analog inputs (AI1, AI2)
- Two single-ended 12-bit, 0.1% accuracy analog inputs (AI3, AI4)
- Two 13-bit, 0.1% accuracy current sourcing outputs (AO1, AO2)
- Connection terminals for common and +24 V analog loop supply (ALS); maximum ALS current limit is 100 mA



WI-MOD-415 Front Panel Connections

The WI-MOD-415 module provides a subset of the I/O functionality of the WI-IO-415-U2. Terminals D1 and D2 are provided. Use the GND terminal on the bottom panel for common connection.



Digital or pulsed inputs

Each digital I/O channel on the WI-415 Series modules can act as either an input or an output. The input/output direction is automatically
determined by the connections and configuration of the I/O. If you have an I/O channel wired as an input but operate the channel as an output, no electrical damage will occur but the I/O system will not operate correctly. If you are operating the channel as an output and you read the corresponding input value, it will indicate the status of the output.

Marked D1–8, the digital inputs share the same terminals as the digital outputs on the WI-IO-415-U2 module. A digital input is activated by connecting the input terminal to GND or common, either by voltage- free contact, TTL level, or transistor switch. Each digital input has
an orange indication LED that will turn on when the input has been connected to a GND.

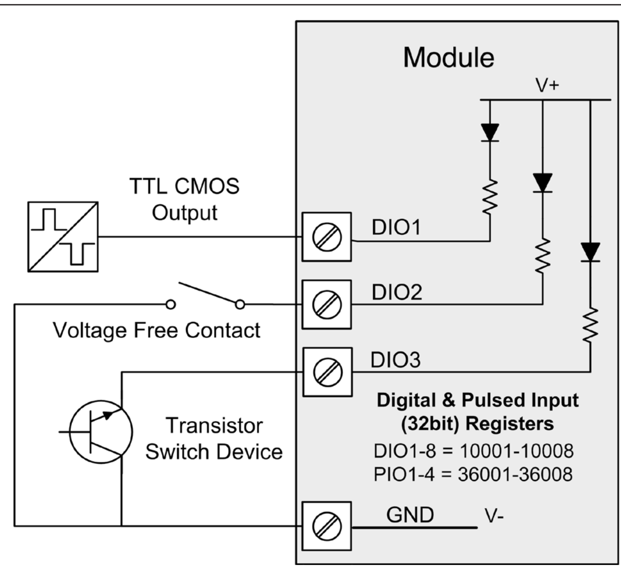


Figure 14. Digital/pulsed input wiring

Digital inputs 1–4 can be used as pulsed inputs. The maximum pulse frequency is 50 kHz for input 1 and 2, and 1 kHz for input 3 and 4. Digital/pulsed inputs are suitable for TTL signal level, NPN-transistor switch devices, or voltage-free contacts (a relay or switch with debounce capacitor).

Frequencies greater than 1 kHz you need to use a TTL logic drive or an external pull-up resistor (1 KΩ to V+). Pulsed inputs are converted to two different values internally. The first value is the pulse count, which is an indication of how many times the input has changed state over a configured time period. The second value is a pulse rate, which is an analog input derived from the pulse frequency. For example, 0 Hz = 4 mA and 1 kHz = 20 mA.

All pulsed input counts are stored in non-volatile memory, so that the values are saved in the event of a power failure or a module reset.

Digital outputs (pulsed outputs)

Digital outputs are open-collector transistors, and are able to switch loads up to 30 Vdc, 200 mA. The eight digital outputs share the same terminals as the digital input. These terminals are marked D1–8.

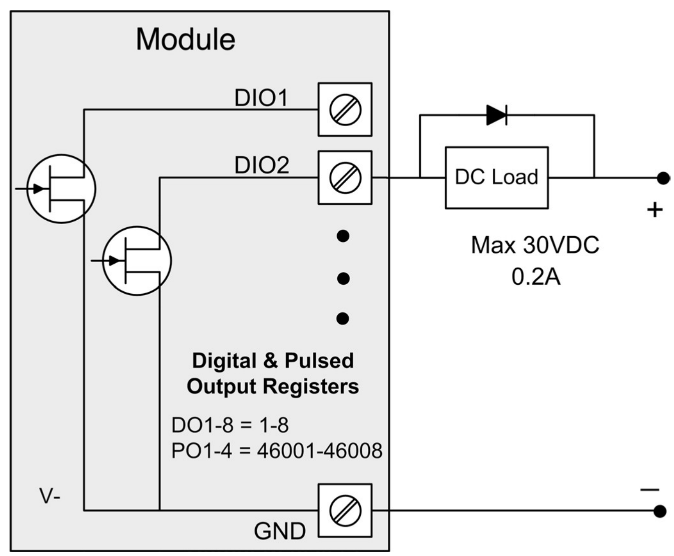


Figure 15. Digital pulsed output wiring

When active, the digital outputs provide a transistor switch to EARTH (Common). To connect a digital output, see **Figure 15**.
A bypass diode (IN4004) is required to protect against switching surges for inductive loads such as relay coils. The digital channels D1–4 on the WI-IO-415-U2 module (D1-2 on WI-MOD-415) can be used as pulse outputs with a maximum output frequency of 10 kHz.

Digital output fail-safe status

In addition to indicating the digital output status (on or off), the LEDs can also indicate a communications failure by flashing the output LED. This feature can be used by configuring a fail-safe time and status via the I/O Digital Output screen in the WI-Device Config utility.

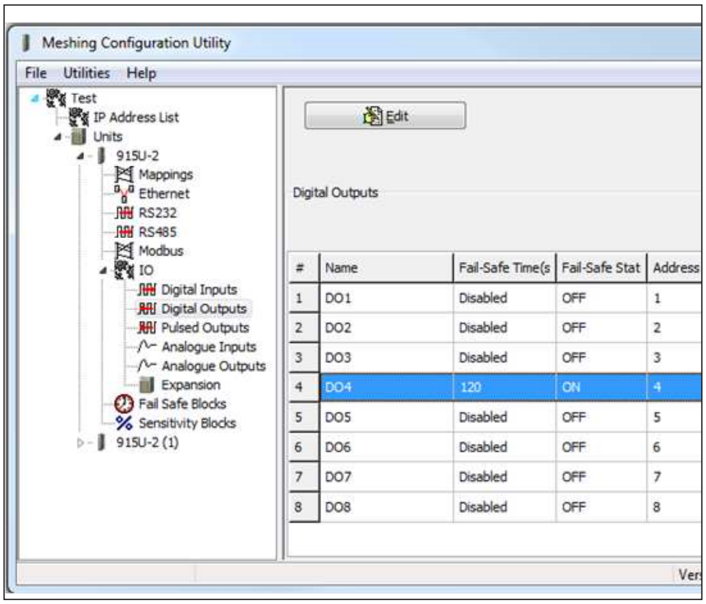


Figure 16. Digital output fail-safe times

The fail-safe time is the time the output counts down before activating a fail-safe state. Normally this would be configured for a little more than twice the update time of the mapping that is sending data to it. This is because the fail-safe timer is restarted whenever it receives an update. If you send two successive updates and fail to receive both of these messages, the timer counts down to zero and activates the fail-safe state.

If the fail-safe state is enabled (on), the LED flashes briefly off and the digital output turns on. If the fail-safe state is disabled (off), the LED flashes briefly on and the digital output turns off.

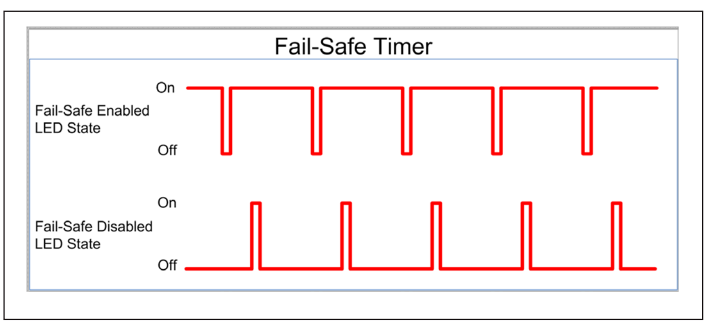


Figure 17. Fail-safe state

Analog inputs

The WI-IO-415-U2 module provides two floating differential analog inputs and two grounded single-ended analog inputs. Analog inputs 1 and 2 will automatically measure current (0–20 mA) or voltage (0–25 V), depending on what is connected to the input. Analog inputs 3 and 4 must be configured to measure current (0–20 mA) or voltage (0–5 V) via the DIP switches on the configuration panel (see "Side access configuration panel" on **page 8**).

An internal 24 V analog loop supply (ALS) provides power for any current loops with a maximum current limit of 100 mA. The LEDs have an analog diagnostic function and will indicate the status of the input. The LED comes ON when any analog signal is detected, and will go OFF when the analog signal drops to zero.

⚠ **Note**: By default, there is a one-second delay on the input because of the filter. Filter times can be changed using the Analog Input screen within the WI-Device Config utility.

The LEDs next to AI1+, AI2+ indicate the current on these inputs. The LEDs next to AI1– and AI2– indicate the voltage on the analog inputs.

Differential current inputs

Only analog input 1 and 2 can be wired as differential Inputs. Differential mode current inputs should be used when measuring a current loop, which cannot be connected to ground. This allows the input to be connected anywhere in the current loop. Common mode voltage can be up to 27 Vdc.

Figure 18 indicates how to connect loop-powered or externally powered devices to the WI-IO-415-U2 differential analog inputs. It should also be noted that the differential inputs can also be used to connect single-ended current sinking or current sourcing devices. **Figure 19** shows how to connect to these types of devices.

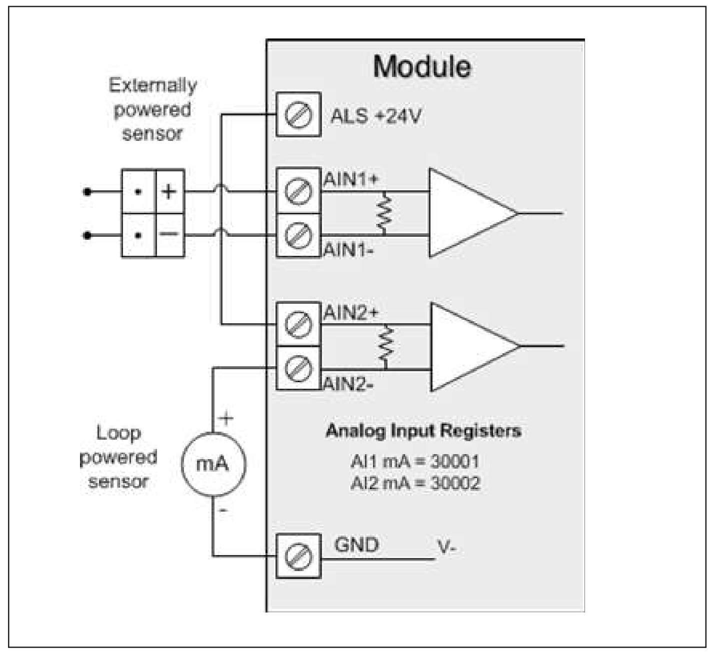


Figure 18. Differential current inputs (AI1 and AI2)

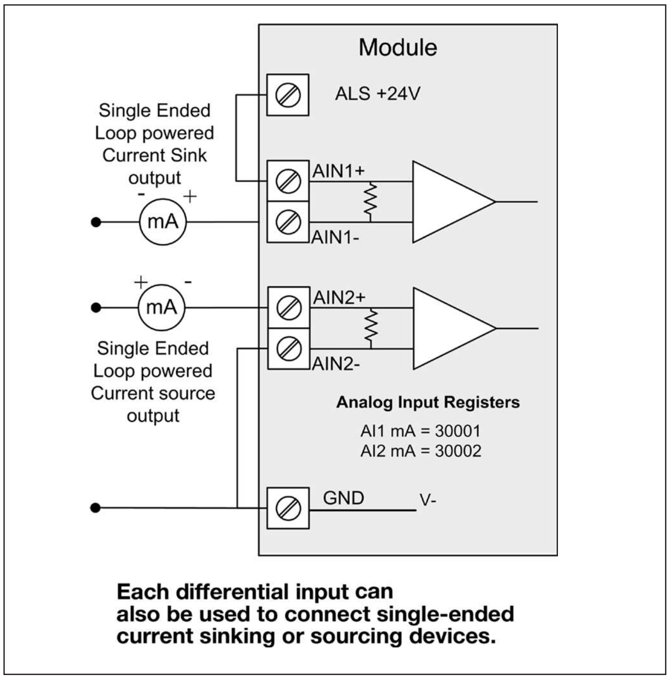


Figure 19. AI1 and AI2 single-ended current inputs

Single-ended current input mode is useful if the sensor loop is grounded to the WI-IO-415-U2 module. Devices can be powered from the 24 V analog loop supply (ALS) generated internally from the module.

The DIP switches (located in the side access panel) are used to determine if the inputs will be current or voltage. DIP switches 1 and 2 are used for analog 3, and DIP switches 3 and 4 are used for analog 4. For current, set both DIP switches to the “on” position. For voltage, set both to “off.”

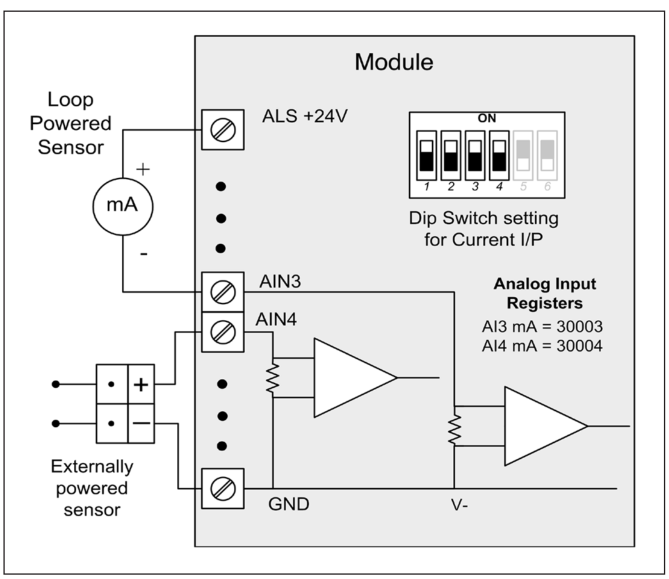


Figure 20. AI3 and AI4 Single-ended current inputs

Voltage inputs

All analog inputs can be set up to read voltage. If using analog input 1 and 2, connect the voltage source across the positive terminal of the input and ground. If using analog input 3 and 4, connect across the input terminal and GND.

⚠ **Note**: Default scaling gives 0–20 V for 0–20 mA output on analog 1 and 2. Default scaling for analog 3 and 4 gives 0–5 V for 0–20 mA output. For voltage input on analog 3 and 4, set both DIP switches to the OFF position.

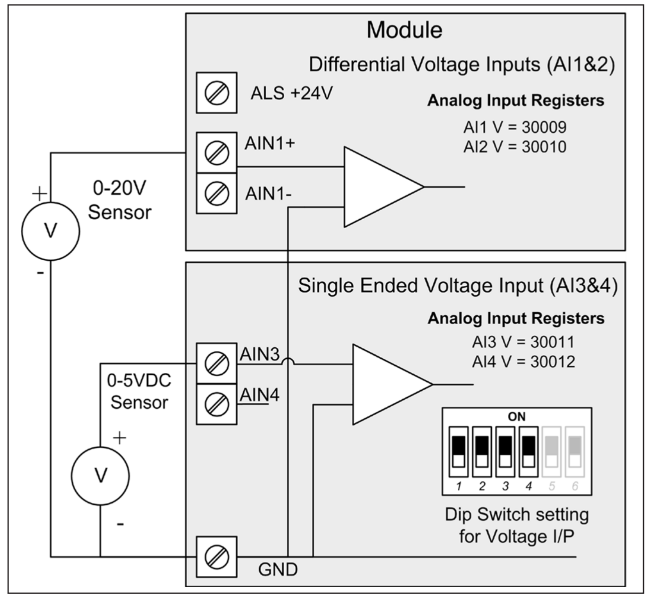


Figure 21. Single-ended voltage inputs

Analog outputs

The WI-IO-415-U2 module provides two 0–24 mA DC analog outputs for connecting to analog inputs on equipment (such as PLCs, DCS, and loggers) or connecting to instrument indicators for displaying remote analog measurements. The WI-IO-415-U2 analog outputs are a sourcing output and should be connected from the analog output terminal through the device or indicator to ground (GND). See **Figure 22** for connections. The LEDs provide level indication depending on current. The LEDs appear dimmed for 4 mA and bright for 20 mA.

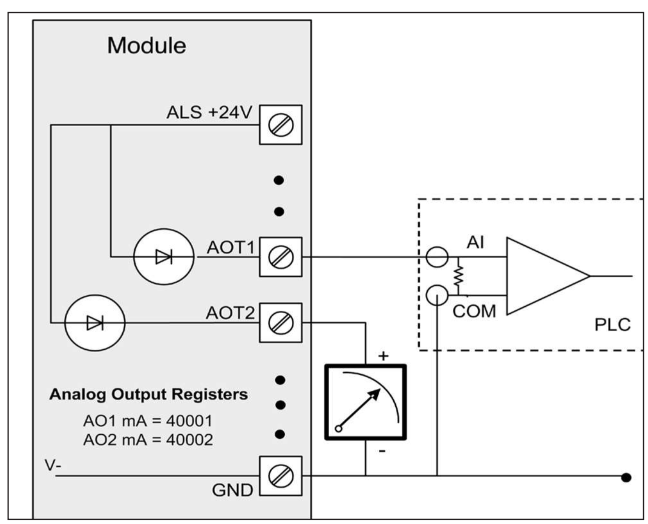


Figure 22. Analog outputs

System design

This section covers the topics you should consider when designing your system. Starting with a sound system design reduces rework and performance problems during and after commissioning.

Design for failures

All well-designed systems consider system failure. I/O systems operating on a wire link will fail eventually. Failures can be short-term, such as interference on the radio channel or power supply failure, or long-term, such as equipment failure.

The modules provide the following features for system failure:

- Outputs can reset if they do not receive a message within a configured time. If an output should receive an update or change message every 10 minutes and it has not received a message within this time, some form of failure is likely. If the output is controlling machinery, it is good design to switch off the equipment until communications are re-established.
- The modules provide a fail-safe feature for outputs. This is a configurable time value for each output. If a message has not been received for this output within the configured time, the output will assume a configured value. We suggest that this reset time be a little more than twice the update time of the input. It is possible to miss one update message because of short-term interference. However, if two successive update messages are missed, long term failure is likely and the output should be reset. For example, if the input update time is three minutes, set the output reset time to seven minutes.
- A module can provide an output that activates on communication failure to another module. This can be used to provide an external alarm indicating that there is a system fault.

Redundant Backbone

For systems redundancy is required, you can configure two WI-415 Series modules to operate as a redundant pair.

For maximum reliability you can use the dual-redundant WI-415 Series-BSR to provide a rack mounted redundant solution.

Testing and commissioning

We recommend that the system is fully bench tested before installation. It is much easier to find configuration problems on the bench when the modules are next to each other as opposed to being miles apart. When the system is configured and you are confident that it works, back up the configurations of all modules.

Networking modes

The WI-415 Series series modules support three different radio networking modes. You select different networking modes depending on your application. This simplifies your networking configuration.

Fixed Links - Use this for large systems with a fixed repeater infrastructure and remote sites connecting to the repeater backbone

ProMesh - This mode automatically assigns stations to act as repeaters as needed. Use this for smaller flexible networks where the topology can change due to moving or temporary repeater locations.

Manual - This mode allows the most flexibility in confiiguring the network topology, but also more opportunity to mis-configure the network. This option is only used in rare occasions where the other two modes can’t meet the network requirements.

ProMesh

ProMesh is the best networking mode to use when it’s not clear which sites will be repeaters. A ProMesh network consists of a Base and multiple Mesh Nodes. In a ProMesh network, any Mesh Node site can act as a repeater to provide a path for other stations to reach the Base. The ProMesh network automatically configures itself to a tree structure with the Base station at the root. When a Mesh Node cannot find a direct connection to the base, It chooses another Mesh Node to act as a repeater based on the best available path to the base.

ProMesh networking mode is typically chosen where your radio environment will be changing, either because the Mesh Nodes are expected to move, or because the physical environment is expected to change so much that the same radio paths will not remain available throughout the lifetime of the network.

⚠ **Note**: You normally configure ProMesh network for operation on a single radio frequency. Fixed Links or Manual mode networks are more commonly used where paired frequencies are required. This is because when frequencies are paired, stations can only connect to repeaters with the opposite frequency pair (transmit matches receive in both directions).

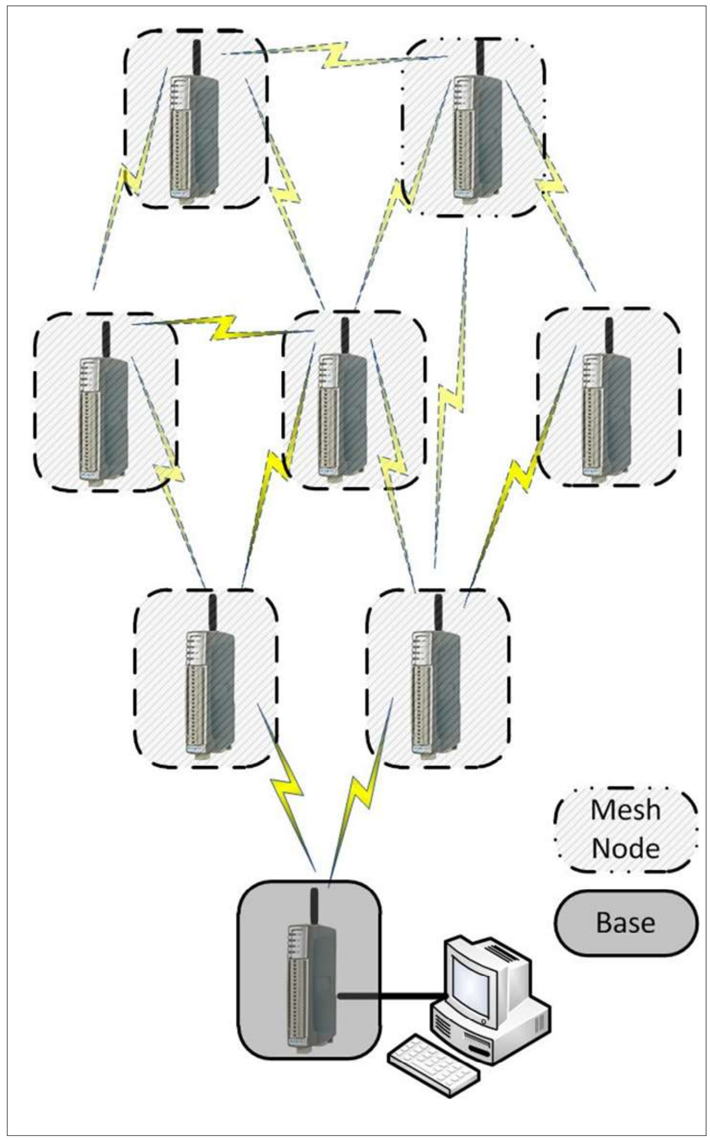


Figure 23. ProMesh network

Fixed links

- Fixed Links is the networking mode that is used in the majority of WI-415 Series applications. This mode allows you to configure a tree structured network with a base station, repeaters, and remotes.
- You use a fixed links network configuration where you will install a fixed backbone of repeater stations, with remotes connecting to one of the repeaters. You can configure the remotes to connect to a single repeater (Roaming Disabled) or to select the best repeater to use (Roaming Enabled).
- Remote stations in the Fixed Links network can be configured to scan multiple radio frequencies. This allows you to configure remotes to connect to whichever backbone network it is closest to, even when the backbone networks are operating on different frequencies.

Fixed Links networks are suitable for networks where paired frequencies are required, as it is easy to flip the transmit and receive frequencies at each repeater.

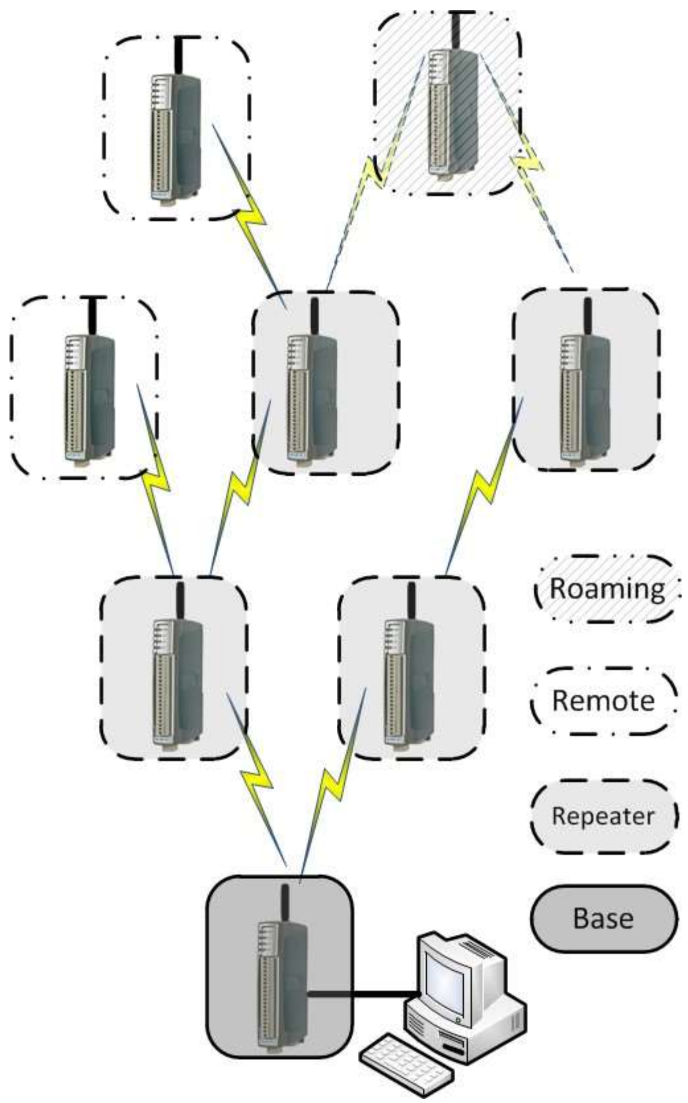


Figure 24. Fixed Links network with Roaming

Manual mode network

Manual mode networking provides the most flexibility in configuring how your network connects, but also comes with the greatest risk of configuring a network that performs poorly or not at all.

Manual mode networking uses the concept of Network Endpoints which are either Access Point or Client (802.11 networking). Each client will connect to an access point with matching SSID. Each access point can accept connections from multiple clients. Each station has a primary networking endpoint. This is the connection you define on the main Networking page. You can define additional endpoints on the Repeaters page to configure additional connections to other stations in the network.

⚠ **Note**: Behind the scenes, the Fixed Links and ProMesh network modes use the same concept of Access Point and Client to implement their networking. The main networking endpoint is always a client, which provides the upstream connection toward the base, and for repeaters and Mesh Nodes, an access point provides a second network endpoint for other devices to connect to.

Internally, all of the networking endpoints are bridged together. This allows messages to be transferred through the network, but you need to be careful of causing loops in the network. With Manual networking mode, there is nothing to stop you creating a loop, which can cause excessive network traffic as messages are sent around the loop forever.

If you create networking loops as a way to provide redundant links, you also need to enable Spanning Tree Protocol, which is designed to eliminate this type of bridged network loop by imposing a logical tree structure on the network.

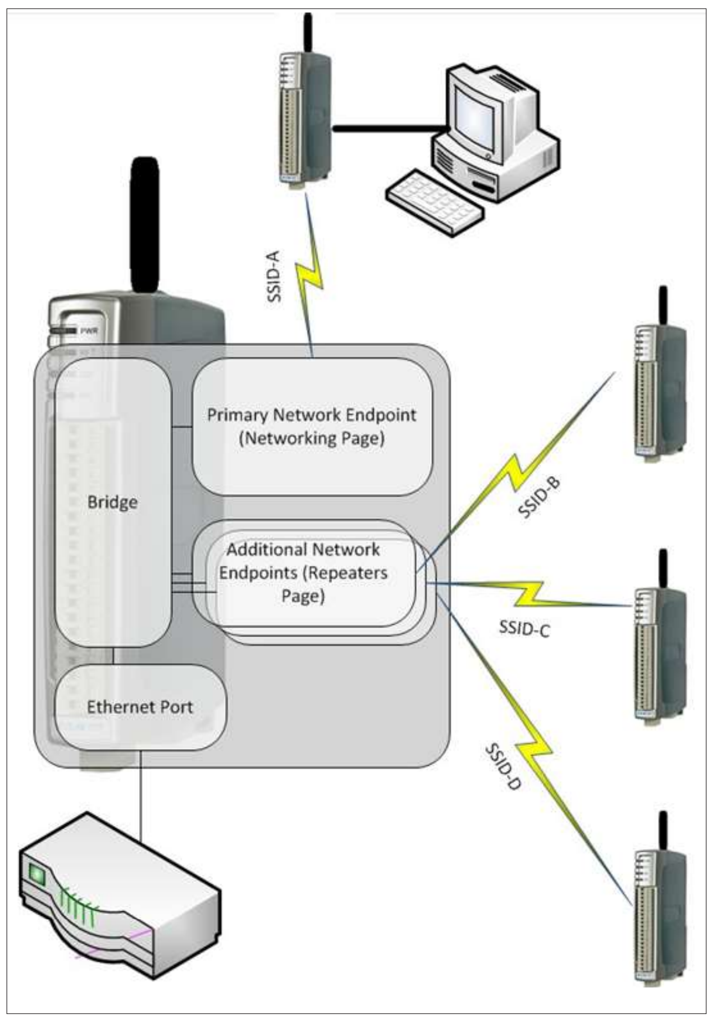


Figure 25. Manual mode networking

IP Address assignment

You should carefully plan how you are going to assign IP addresses to the devices in your system. By assigning IP addresses in a logical manner, your network setup will be easier to understand, and the amount of configuration required will be minimized.

Bridged networks

Most networks will use the Bridged networking mode. This is the default for the WI-415 Series devices. Here the local network of devices connected to the base, the remote radios, and other devices connected to the remote radios are all on the same IP subnet.

For this type of network, you should assign a separate block of IP addresses for remote WI-415 Series devices, other remote devices connected to the WI-415 Series radio network, and for any equipment on the local network at the master station. Assigning IP addresses in this way allows you to use the Easy Filter configuration to simplify network filtering. A typical installation could use the following assignment.

Sub-Network Address: 192.168.9.0 (Subnet Mask 255.255.255.0)

(The 192.168.0.xx through 192.168.255.xx addresses are assigned to private IP networks. This allows up to 254 devices on the subnetwork.)

Base Network: 192.168.9.1 – 192.168.9.50

(Use addresses in this range for all devices connected to the Base station network segment, including SCADA computer, PLCs, Managed Switches, etc.)

WI-415 Series radio network: 192.168.9.51 – 192.168.9.150

(Use these addresses for the remote WI-415 Series devices)

Other Host devices: 192.168.9.151 – 192.168.9.253

(Use these addresses for the devices connected to the Ethernet ports on the remote WI-415 Series devices)

Network traffic control in bridged networks

Bridged networks are convenient to set up because all of the devices are on a single subnet, and the bridging algorithms take care of delivering the data packets to the correct destination. One negative of bridged networking is that any broadcast traffic must be broadcast over the entire network. This isn't such a big issue with high speed Ethernet networks, but with lower speed radio networks, the level of broadcast traffic on the radio network can stop important traffic from reaching its destination. Use the Easy Filter option at your Base Station to ensure that only traffic to the desired destination IP addresses is forwarded over the radio network. Easy Filter filters out any non-IP traffic, and any IP traffic to addresses outside the configured range.

Using the example above, you should configure Easy Filter at your Base Station to cover the "WI-415 Series radio network" and the "Other Host devices", but not the "Base Network".

Figure 26. Easy filter

Routed networks

Sometimes it is necessary to configure the radio as an IP router to support desired addressing or address segmentation.

For this type of network, you need to assign different separate subnetwork addresses to each Sub-network. Normally you set the WI-415 Series Base station as an IP Router, and configure the Base Network on one subnetwork, and all remote devices on another subnetwork. Atypical installation could use the following assignment.

Base Subnetwork:

Sub-Network Address: 192.168.9.0 (Subnet Mask 255.255.255.0)

Base Network: 192.168.9.1 – 192.168.9.100

Base Station WI-415 Series Ethernet IP address:

192.168.9.101 Remote Subnetwork:

Sub-Network Address: 192.168.10.0 (Subnet Mask 255.255.255.0)

WI-415 Series radio network: 192.168.10.2 – 192.168.10.100

(Use these addresses for the remote WI-415 Series devices)

Other Host devices: 192.168.9.101 – 192.168.9.253

(Use these addresses for the devices connected to the Ethernet ports on the remote WI-415 Series devices)

Base Station WI-415 Series Radio IP address: 192.168.10.1

Note that in this configuration the remote 415 devices are still configured for Bridging. If you configure the remote 415 devices for routing, then you need to assign a separate subnetwork and separate Ethernet IP addresses for the local Ethernet network at each remote
415 device.

The PC Based Configuration Utility WI-Device Config does not support Routed network configuration. You can only configure Routed mode using the Web based configuration interface. See "Configuring using the embedded Web Configuration Utility" on **page 49**

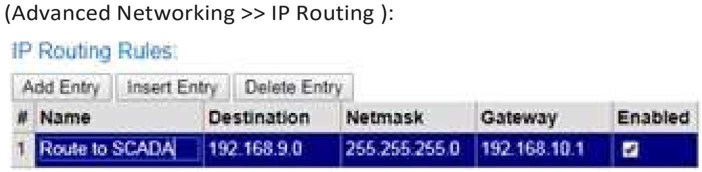
Routing rules

When you configure your Base station as an IP Router (Basic Provisioning >> Network >> Network Mode >> Router) you also configure a different IP subnet on the radio and on the Ethernet port. To allow messages to pass through the router, you need to set up routing rules to tell the remote devices (Remote WI-415 Series, Base Computer, and other remote Connected device) to use the Base station WI-415 Series as the router to reach the remote device.

Using the example above, at your Scada PC, you need to add a routing rule to use the Base Station Ethernet IP address to reach the 192.168.10.0 network:

```
> route ADD 192.168.10.0 MASK 255.255.255.0 192.168.9.101
```

And at your remote 415 units, you need to add a routing rule to use the Base Station Radio IP address to reach the 192.168.9.0 network (Advanced Networking >> IP Routing):



Note: You will need to add similar routing rules to any other devices you have connected to the Ethernet ports on the remote 415 devices which need to communicate back to the Base network.

Radio Paths and Data Rate

A critical element in system design is to ensure that the radio signals are able to reach their destination reliably. This section provides guidance on configuring your devices to deliver data reliably.

Modulation Type and Data Rate

The WI-415 Series supports two modulation types (Legacy FSK and High Speed QAM), and a total of six data encodings (two for FSK, and four for QAM modulation). The available data rates depend on the modulation type, the encoding, and the radio bandwidth. Faster data rates allow more data to be transferred in your system, but require a clearer signal to get through.

The following table shows the available data encodings and raw data rate for the available radio band-width settings.

Modulation type and encoding	Raw Data Rate		
QAM	**25kHz channel**	**12.5kHz channel**	**6.25kHz channel**
4QAM + FEC	16kbps	8kbps	4kbps
4QAM	32kbps	16kbps	8kbps
16QAM	64kbps	32kbps	16kbps
64QAM	96kbps	48kbps	24kbps
FSK			
2FSK	9.6kbps	4.8kbps	2.4kbps
4FSK	19.2kbps	9.6kbps	4.8kbps

The following table shows the available data encodings and required signal strength for reliable reception (Bit error rate 1 in 100,000). The system figure shows the maximum path loss after accounting for antenna system gains or losses. (Transmit Power minus Sensitivity)

QAM Modulation encoding	Sensitivity (BER 10^{-5})	Maximum Transmit Power	Maximum System Figure
4QAM + FEC	-116 dBm	+36dBm	152dB
4QAM	-113 dBm	+36dBM	149dB
16QAM	-104 dBm	+34dBm	138dB
64QAM	-97 dBm	+34dBm	131dB
FSK Modulation encoding			
2FSK	-110 dBm	+40 dBm	150dB
4FSK	-102 dBm	+40 dBm	142dB

When designing your radio network, you calculate the system figure to determine what data rate you are likely to achieve between two sites. You calculate the system figure by adding the transmitter power and antenna gain, and subtracting co-axial cable losses and path loss between the two sites.

Auto Rate

The WI-415 Series modules support automatic data rate selection. This is normally the best option, as the modules will set the data rate to the maximum according to the signal strength, and will then adjust the data rate if the signal strength reduces (due to changing path conditions, or degrading antenna systems), or if too many messages are corrupted during transmission (due to interference)

The default setting for the WI-415 Series modules is auto rate. This is appropriate for the majority of situations, however the automatic rate selection can struggle to find a consistent rate if there is local interference, if the system is so busy that many messages fail to be delivered, or if the two ends of the link are configured with different power levels. In these cases, you could see improved performance by setting the module transmit data rate (Radio Configuration Page)

Where you have a very remote site, you might need to use a high gain directional antenna (Yagi) to reach your repeater or base station. To stay inside the radio license requirements, you may need to reduce the transmit power to compensate for the antenna gain at that remote site. If the transmit power at each end of a link differs by more than 3dB, you should disable Auto Rate, and select the best fixed rate for that site.

Basic Rate

In addition to the Data Rate, each radio in your system.is configured with a basic rate. This is the lowest rate that any radio in the system can communicate at. The default value for the basic rate is 4QAM (for High speed mode) or 2FSK (for Legacy Mode). All radios must be configured with the same basic rate setting.

Where all of the radio paths in the system have good signal strength, you can set the basic rate to a higher value to achieve increased system throughput (Radio Configuration Page). If you have some radio paths which may require the strongest encoding (FEC) to operate, you should set the basic rate to the lowest rate (4QAM + FEC).

The basic rate is used for transmissions during link establishment, as well as for beacon messages and for broadcast transmissions. The basic rate also affects the radio channel delays (hold-off times), as the radio access protocol needs to allow for the possibility of low speed transmissions when the basic rate is lower. This means that a system with a lower basic rate will experience lower throughput, even if the actual data rates between the sites are the same.

⚠ **Note**: Radios are able to communicate with each other when the basic rate is set to different FSK or QAM encoding (without FEC), but this is not recommended, as the channel access timing is different, and this is likely to result in more message corruptions due to overlapping transmissions .

Forward Error Correction

The High Speed (QAM) modulation type provides an additional encoding mode to provide the best possible long range performance. 4QAM+FEC mode applies forward error correction to the 4QAM signal. This adds additional data bits to the transmitted message that can be used at the receiving end to recover data that was corrupted during data transmission. This mode provides a low speed option to allow operation over the longest distances.

⚠ **Note**: The default basic rate setting is 4QAM *without* FEC. If you think your system will need this mode, then you need to select the 4QAM+FEC data rate as your Basic Rate setting for all radios in your system.

Transmit Power Setting.

You should set your transmit power according to your radio license. If you have configured the radio for an unlicensed / class licensed locale then your power level setting will be limited to the maximum allowed for your locale. In either case, you need to account for the gain of your antenna system to ensure you are not exceeding the allowed radiated power level.

Most radio licenses are based on average transmit power, however some specify peak power levels. For Legacy FSK transmission, the average and peak power are the same, but for High Speed QAM transmission, the average and peak powers are different. The power setting that you make sets the target average power, but at some target power levels the radio is limited by it's peak power capability. Check the peak and average power available in QAM modes according to the table below. The highlighted cells show where the average power has been limited to less than the requested value by the radio peak power capability

	Peak Power (Watts)			Average Power (Watts)		
Power Setting	**4QAM (incFEC)**	**16QAM**	**64QAM**	**4QAM (incFEC)**	**16QAM 64QAM**	**2FSK 4FSK**
40dBm (10W)	13.2W	12.1W	13.5W	4W	2.5W	10W
39dBm (8W)	13.2W	12.1W	13.5W	4W	2.5W	8W
38dBm (6.3W)	13.2W	12.1W	13.5W	4W	2.5W	6.3W
37dBm (5W)	13.2W	12.1W	13.5W	4W	2.5W	5W
36dBm (4W)	13.2W	12.1W	13.5W	4W	2.5W	4W
35dBm (3.2W)	10.5W	12.1W	13.5W	3.2W	2.5W	3.2W
34dBm (2.5W)	8.3W	12.1W	13.5W	2.5W	2.5W	2.5W
33dBm (2W)	6.6W	9.55W	10.8W	2W	2W	2W

Configuration

The WI-415 Series modules can be configured using the Windows®-based Mesh and I/O Gateway Configuration Utility (WI-Device Config), or via the embedded Web-based management utility. The following section shows how to connect to the device using the Windows®-based Configuration Utility. To access the embedded webpages, refer to the section "Configuring using the embedded Web Configuration Utility" on **page 49**.

Connecting using the Configuration Utility

On first connection, you must connect to the device through its USB port. Once you have configured the device for the first time, you can enable access through the Ethernet port and remotely through the Wireless port

Note: Before enabling the Ethernet Port or Wireless port for Configuration access, read the section "Recommended secure hardening guidelines" at the end of this manual.

Downloading and installing WI-Device Configuration utility

The WI-Device Configuration utility is provided as a executable installation file from the download section of the WEIDMULLER website. Configuration of the WI-415 modules can be performed via USB or Ethernet connection, and all appropriate USB drivers are installed during installation. If you have a problem installing the drivers, you can install them manually using Windows Device Manager. To install the WI-Device Configuration utility:

- Go to the WEIDMULLER website: www.Weidmuller.com
- Select Products > Wireless Connectivity Solutions > Downloads > WI-Device Configuration Utility.
- Download and open the file "INST_CFG_CWI-Config<version>.exe." This runs the Installation Wizard.
- Follow the on-screen instructions to install the software (see **Figure 2**7.

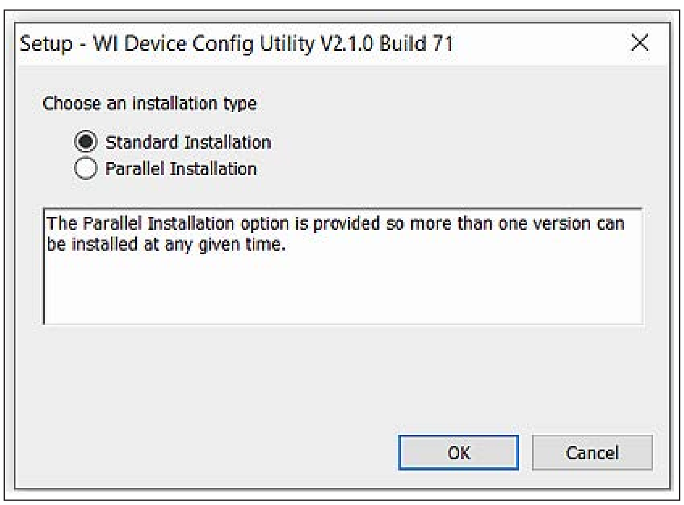


Figure 27.

Selecting "Standard Installation" replaces any existing installation of WI-Device Config with the version you are installing. Select "Parallel Installation" if you want to keep a version of WI-Device Config that you have installed previously in addition to the new version.

Connecting to the device's USB port

The USB port is located on the bottom side of the module. (Refer **Figure 11** "Bottom Panel Connections"). To connect, you need an USB cable (USB-A to USB-B) for connecting from your computer to the module's USB-B port .

If you have installed the Windows®-based Configuration Utility, then USB drivers should have been installed at the same time.

You will need to know the credentials (username and password) configured for the device. If the module is new out-of-the-box you can use the default credentials. Otherwise, you will need to use the values set previously. If you have lost the password, you can clear the device to restore all settings back to the default values.
For instructions, see "Restoring the factory default settings" on **page 68**.

1. Power on the device, and wait for the device to finish booting and for the "PWR" LED to go solid green (about 1 minute).

   ⚠ **Note**: When the module is new from the factory, the Power LED will go solid RED. Once the radio Locale is set, the OK LED will go green after boot.

2. Start the Configuration Application
3. Plug in the USB cable and wait for your computer to recognize the new USB device. The new device will identify as a "WI-415 Series".
4. Once the device is recognized, you will have an additional Network Adapter in your device manager list "Weidmuller WI-IO-415-U2 USB Ethernet/ RNDIS Interface"

Select an option from the Communications panel, such as "Program Unit". You will be presented with a connection dialog.

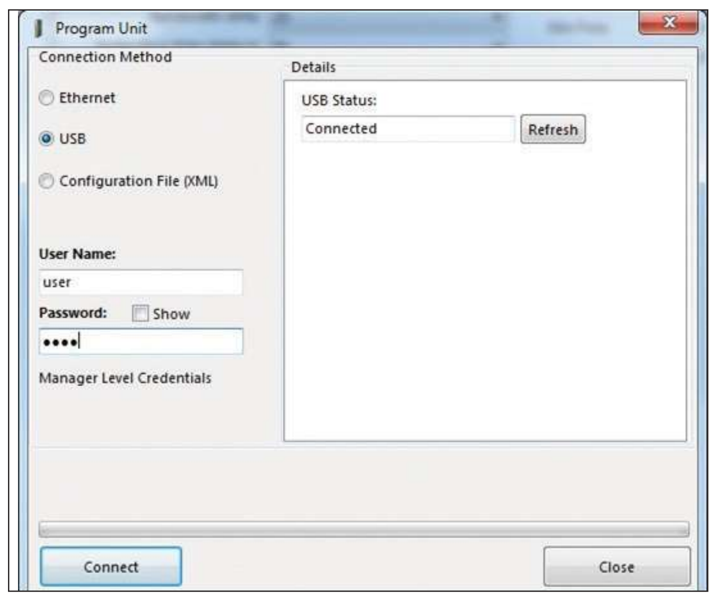


Figure 28.

Select option "USB" and click Refresh to update.

Once the USB Status shows "Connected", enter your User Name and Password, and click OK.

Connecting to the Device's Ethernet port

Note: Before connecting to the Ethernet port for the first time, you need to enable Remote Configuration Access. This can only be done using the USB connection (See above).

The Ethernet port is located on the bottom side of the module. (Refer **Figure 11** "Bottom panel connections"). To connect, you need an Ethernet cable for connecting to the module's Ethernet port.

You also need to know the device's IP Address and the username / password configured for the device. The module's default Ethernet settings are as follows:

- IP Address: 192.168.0.1XX
  (shown on the printed label on the side of the module)
- Subnet Mask: 255.255.255.0
- User Name: user
- Password: user

If the module is new out-of-the-box you can use the default credentials. Otherwise, you will need to use the values set previously. If you have lost the password, you can clear the device to set the username and password back to the default values. For instructions, see "Restoring the factory default settings" on **page 68**.

Once you have the device's IP address and password:

1. Power on the device, and wait for the device to finish booting and for the "PWR" LED to go solid green (about 1 minute).
2. Start the Configuration Application
3. Connect an Ethernet cable between the module's Ethernet port and the PC.
4. Configure your PC networking settings to be on the same network as the device. For instructions on how to do this, see "Configuring PC networking settings" on **page 68**.

Configuring your System using WI-Config Utility

Once you have installed and started the configuration utility, you can begin to configure your system. Begin by selecting the "Units" tree node, and clicking "Add a new Unit". Select the type of device you will be adding, and click "OK

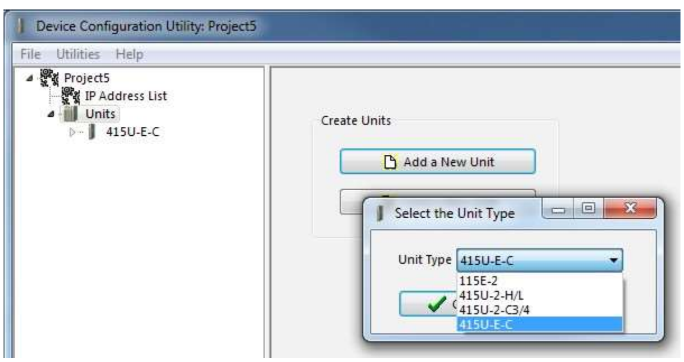


Figure 30.

Configure how the device connects

Once you have added the device, you will see the device's main configuration page. This page will allow you to set up the device to communicate with the rest of the network

The first device you add should be configured as a base station. You should add and configure each of the system base stations into your project first, followed by the repeaters, then remotes.

Note: A system is made up of base stations, repeaters, and remote sites. The base stations are connected to your wired backbone. Remote sites are your field locations. Repeaters forward signals for remotes that can't reach the base directly.

Once you have added your site, configure each item as described below.

Select an option from the Communications panel, such as "Program Unit". You will be presented with a connection dialog.

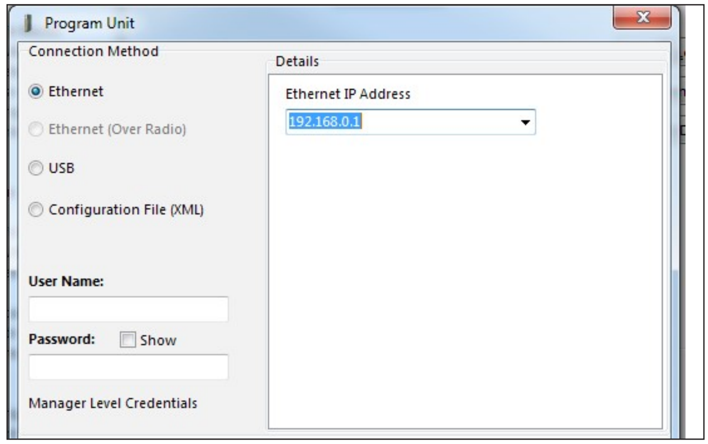


Figure 29.

Select option "Ethernet" and enter the Device's IP Address. Enter your User Name and Password, and click OK.

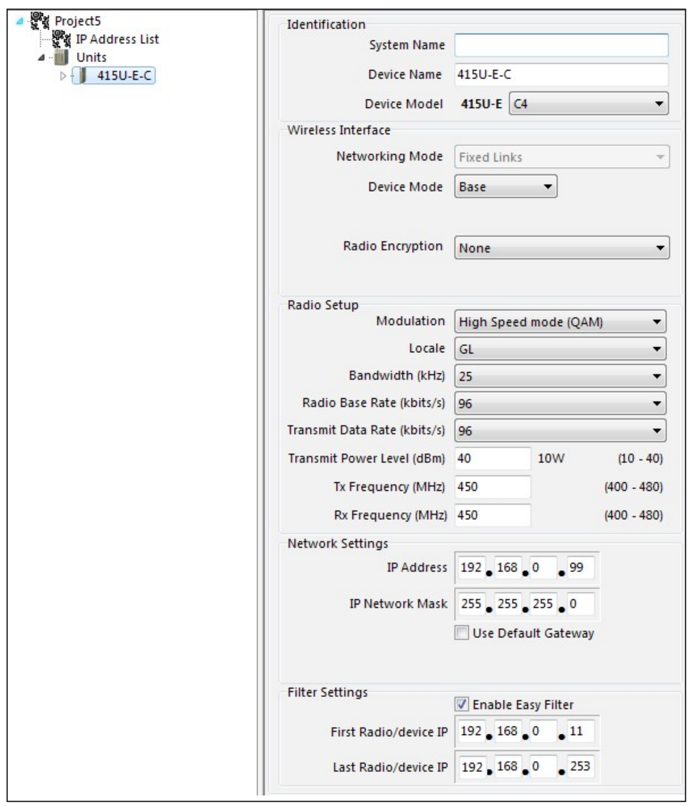


Figure 31.

Identification

System name: All devices in a system are configured with a common system name. This is used by roaming remotes, and in ProMesh mode as a common network ID for all devices to connect.

Device name: Each device in the system should be configured with a unique device name. This name is used to identify devices in diagnostic display (Connectivity) and is used in Fixed Link mode as the device ID for other devices to connect to.

Device model: Select the device model to match the product label.

Wireless Interface

Networking Mode: Select "Fixed Links" or "ProMesh". Fixed Links mode should be used in larger systems where established repeaters are installed to provide a communications backbone for remote sites. ProMesh mode is suited to systems where connections are ad-hoc, and any device may be required to act as a repeater station.

- **Fixed links** Mode implements a fixed repeater configuration where field devices (Remote) are configured to connect directly or via intermediate sites (Repeater) to a central station (Base).
- **ProMesh mode** implements automatic repeater configuration, where devices (Mesh Node) automatically choose and maintain the best path back to a central station (Base). All devices in the network use a common System Name.

Device mode: This option is available when the Networking mode is set to "Fixed Links". A Fixed Link network consists of a central station (Base) accessing a fixed arrangement of repeater stations (Repeater) and remote stations (Remote). All devices ultimately connect to the central station (Base). Repeaters and remotes can either connect directly to the base, or connect using additional repeater stations to extend the radio range.

Enable roaming: This option is available when the Device Mode is "Remote". Check this box if you want the remote to be able to roam between repeaters and base stations with the same system ID.

Upstream device name: When the Device Mode is "Repeater" or "Remote", you need to select the Upstream device. When the connection is direct to the base, this is the Device Name of the base station. When the connection is via repeaters, this is the name of the repeater station that is used to reach the base station. If this is a remote site with roaming enabled, then the Upstream device is only used to configure the radio settings, and the remote will be able to roam between base and repeaters with matching radio settings.

ProMesh mode: This option is available when the Networking Mode is set to ProMesh. A ProMesh network consists of a single central station (Base), and one or more remote sites (Mesh Nodes) which can each operate as a repeater for other stations.

The Mesh Nodes select the best path to the Base depending on the number of hops to the base, and based on signal strength of the hops in the path. Once connected, the Mesh Nodes monitor the path quality and will swap to use a better path if one comes available.

All devices in a ProMesh network share the same configured "System Name".

Radio encryption: Select the radio encryption type. "AES 256 bit" provides 256 bit AES encryption suitable for all applications. "WPA2-PSK" provides 128 bit AES with key rolling. This is the same encryption as used in 802.11 protocol. This method has additional overheads that slow down device connection. . "AES 256 bit" is the best option unless there is a specific reason to use the standards based encryption.

⚠ **Note**: Selecting Encryption "None" makes your network vulnerable to attack. Without encryption there is no protection from attackers with access to the same type of hardware.

Encryption passphrase: This is the secret key for your network encryption. All devices in the network need the same passphrase to communicate.

Note: For best security, this passphrase must be long (at least 20 characters) and should not include text that could be guessed such as names, dates, etc.

Note: Always keep this passphrase private, and ensure that the system configuration is updated with a new passphrase if this key becomes compromised.

Radio setup

Modulation: Select the Modulation required for WI-IO-415-U2-C and WI-415 Series- E-C models. This should be set to QAM mode unless you need to connect to Legacy WI-IO-415-U2-H/L devices in your network. All devices in the system must be set to the same modulation.

Locale: Select the desired licensing. For most applications, you should select "GL" for licensed operation, or "ISM" for unlicensed operation in the 433MHz ISM band. Some countries support additional unlicensed or class licensed bands. If you know that one of these locales applies to your location, then you can select the appropriate locale. Once you select the locale, other settings will be limited to be within the allowed settings for that band.

For more information on the device Locale refer to the section "Configuring the Locale" on p.47

⚠ WARNING

USE OF UNLICENSED BANDS IS LIMITED TO THE LISTED PHYSICAL LOCALES ONLY. ENSURE YOU SELECT A LOCALE THAT IS ALLOWED BY THE RADIO REGULATORY AUTHORITY IN YOUR TARGET LOCATION.

⚠ WARNING

WHEN YOU SELECT "LICENSED" LOCALE, YOU MUST HAVE A RADIO LICENSE FROM THE RADIO REGULATORY AUTHORITY IN YOUR LOCATION. THIS LICENSE WILL BE FOR A SINGLE FREQUENCY OR A RANGE OF FREQUENCIES. ENSURE THE RADIO IS CONFIGURED FOR A PROPERLY LICENSED FREQUENCY (REFER FOLLOWING SECTION) BEFORE TRANSMITTING.

If you intend to use the device in Licensed operating mode, select the "Licensed" Locale. This gives access to the full radio band available to the module.

Bandwidth: Select the bandwidth according to your license. If you have a choice, a larger bandwidth will allow higher data rates but will occupy more of the radio spectrum.

Transmit power level: Select the desired power level. You can reduce the power level to compensate for higher gain antennas to stay inside any regulatory limits that apply to your radio license or to you location.

Radio base rate: This is the lowest speed that the radio communicate at. This should normally be set to the lowest available setting. All radios that will communicate with each other must have the same Base Rate. By setting this to a higher rate, system throughput can be increased.

Transmit data rate: This is the data rate for this radio to transmit at. Different radios in the system can transmit at different rates. Slower rates improve the signal over marginal radio paths.

Tx/Rx Frequency: This is the frequency that the radio operates at. This will be set according to your radio license.

⚠ **Note**: When you connect a device to a Base or a Repeater by selecting "Upstream Device", the Modulation, Locale, Bandwidth, Radio Base Rate, and Tx/Rx Frequency are copied from the upstream device, so you normally only need to set these values at the system base station.

Caution: When selecting the Locale, frequency, bandwidth and power, make sure that you have approval from your regulatory authority to operate the radio with these settings. You will normally need a license to be issued for bands other than the ISM band.

Network settings

IP Address/Network mask: Set the IP address of the device. This will normally be an address on the same subnet that is connected to the Ethernet port on your Base station.

Note: The WI-415 Series devices are configured for Bridged networking, where the radio and Ethernet ports share a common IP address. To operate the WI-415 Series devices in a routed network, you need to configure using the device web interface. Refer to section "Configuring devices using the embedded Web Configuration Utility" for detail.

Use default gateway: Select this if you need to provide a default route out of the local subnet. Once selected, configure the IP address of the gateway device.

Filter settings

Enable easy filter: Select this option at the Base to automatically filter traffic that is not destined for devices connected to the radio network. The filter will only allow IP traffic with an address within the specified range.

Communications

Remote access: Check this to enable remote configuration access to the device from the radio or Ethernet ports. If this is not checked, you can only configure the device from the USB port.

Program unit: Program the device configuration into a module (or save to disk as an XML file for webpage upload to a device).

Load unit: Load the device configuration from a module (or load from disk as an XML file previously loaded from device webpage)

- **Ethernet**— Program the module using the local Ethernet interface displayed in the list. Select IP Address or enter a new address.
- **USB**—Program the module using a USB interface. You will need to plug in the USB cable and then click Refresh.
- **Configuration file (XML)**—Program (or load) the module configuration to (or from) an XML file.
- **User name**—Select the username to access this device. The default configuration for the manager login is "user."
- **Password**—Enter the password you configured for this module. The factory default password is "user."

Monitor Comms: Displays a diagnostic tool that allows you to monitor IP traffic received and transmitted by the device's Ethernet and Radio ports.

IO Diagnostics: Allows you to view the internal registers for the selected module unit

Networking

Click **Networking** in the project tree to configure Ethernet and routing parameters. These parameters are described in detail in this section.

⚠ **Note**: The default networking mode for the WI-415 Series uses bridged networking. This connects the radio and Ethernet ports to the same logical sub-net. The WI-415 Series device has a single IP address common to the radio and Ethernet ports.

IP routing

The IP routing rules table determines which IP address an outgoing message will be routed through. When the table contains enabled routing rules, the most explicit and exclusive subnet match is used to determine the route for an outgoing message. If there is no match, the WI-415 Series checks for a subnet match against its hard-wired default gateway (configured on the main device configuration page), assuming that the default gateway is configured and accessible. In some cases, such as routed networks with more than two routers, it is not practical to have only one default gateway. If more than one next-hop router is required, the WI-415 Series allows for the configuration of up to 100 routing rules. A routing rule specifies a destination network (or host) IP address and the corresponding next-hop router (gateway) to which messages for the specified destination will be forwarded. The gateway will then deliver the data to the required destination, or forward it on to another router that will.

⚠ **Note**: IP routing is an advanced user function. If you are not familiar with IP routing and your network consists of multiple sub-networks connected by routers, request assistance from an IT expert.

To display the IP routing rules table, click **Routing** under **Networking**. After configuring routing rules, click the **Program Unit** button on the module's Unit Details screen for the changes to take effect.

The example in **Figure 32** shows an IP routing rule that maps messages to any IP address starting with 10.0.0.0 to the gateway with the IP address 192.168.0.254. If that does not match, it attempts to use the local Ethernet interface.

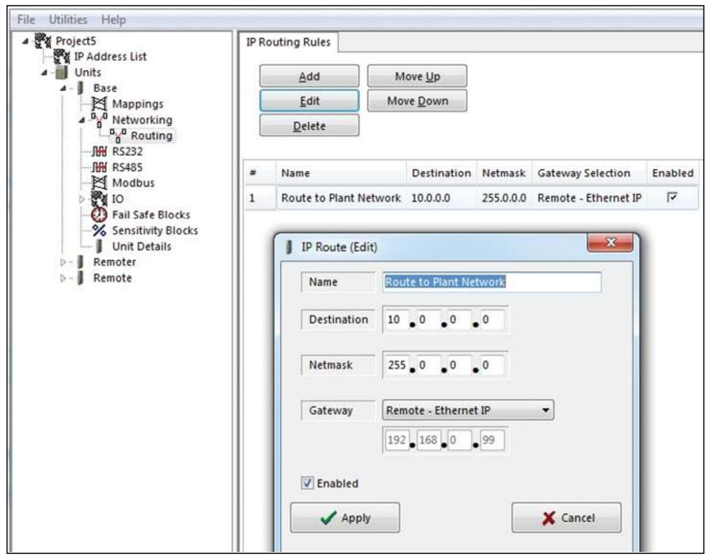


Figure 32. IP routing rules

- **Add**— Adds a new IP routing rule
- **Edit**— Edit the currently highlighted routing rule
- **Delete** —Remove a selected IP routing rule.
- **Move up / Move Down**— Moves a selected IP routing rule within the list
- **Name**— Name describing the routing rule (maximum 32 characters)
- **Destination**— Destination network or host IP address. You can specify an entire network by entering the IP range 192.168.0.0 with a netmask of 255.255.255.0, or you can specify an individual host IP address by setting the netmask to 255.255.255.255
- **Netmask**— Subnet mask for the destination network
- **Gateway**— Specifies the IP address of the next-hop router for the specified destination subnet
- **Enabled**— elect this checkbox to enable the routing rule. Clear this checkbox to disable the routing rule without deleting it

Mappings

Mappings are used to send I/O values between modules using the WIB I/O transfer protocol. The I/O is sent to a remote module via the Ethernet connection on the device. To display the current mappings for a module, open the module in the project tree and click Mappings (see **Figure 33**).

Mappings are sent on the following triggers:

- **Change of state (COS)**—This method monitors the state of the input that is being mapped. When the state changes, it triggers a transmission. This is the primary method of sending input values to a destination. As soon as the input change occurs the value is immediately sent to the destination. Digital mappings are triggered when the input changes from on to off, or from off to on. Analog mappings are triggered when the input changes by a predefined value, referred to as "sensitivity." The sensitivity value is set by configuring a sensitivity block for the particular input or a range of inputs. See "Sensitivity blocks" on **page 29** for more information.
- **Updates**—This method sends a message at a pre-configured time regardless of the input value or state. For details, see the Update Time field described in "Adding or editing mapping parameters" on **page 22**.
- **Mapping force**—This method makes use of the Force Mapping Transmit Register configuration on the Advanced page. It allows a mapping to be triggered when a separate register is written to a non-zero value. The register is written back to zero once the mapping has triggered.

There are three types of mappings—write, gather scatter, and read. Each type has advantages and disadvantages. The appropriate mapping to use will depend on the data and requirements of the system.

- **Write mapping**—A write mapping allows multiple sequential values to be sent in one message. If you are mapping analog values, the maximum I/O count is 64. However, if you are mapping digitals it can be as many as 1024 because the digitals values are packed into 16-bit words for transmission. The mapping is sent on a change-of-state of any of the values being monitored, and also on an update period.
- **Gather scatter mapping**—A gather scatter mapping is essentially the same as write mapping, but instead of sequential register it allows different I/O types to be sent in a single message. All I/O types, including digital, analog, long (32-bit registers) and floating point values, can be sent in a single message. A gather scatter mapping has a maximum I/O count of 32 values of any data type (digital, analog, longs, or floats).
- **Read mapping**—Read mappings are similar to write mappings in that they allow multiple sequential values to be sent. However, instead of writing the values to another module, the data is requested from the remote module, which responds with the requested data. This type of mapping is suited to a polling system where the receiving station initiates when it wants to communicate, for example, by sending a read request when it requires the information or by sending a request on a timed basis.

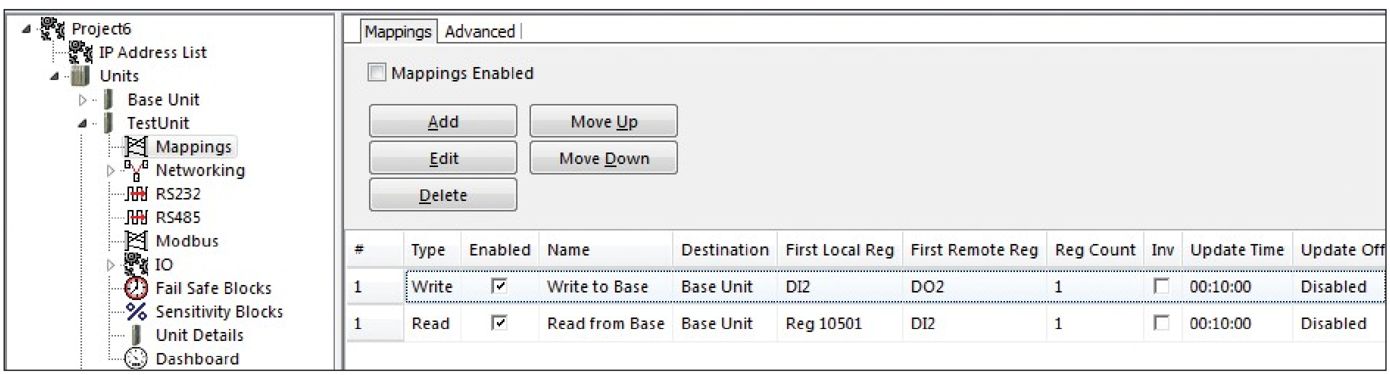
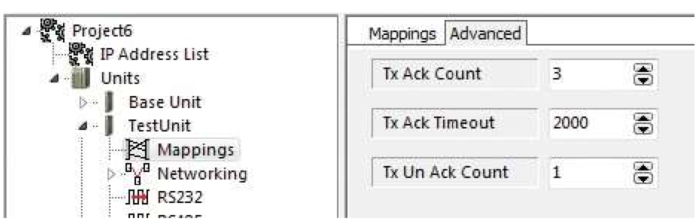


Figure 33. Mappings

WIB configuration options (Advanced Tab)

The following options are available on the "Advanced" tab of the Mappings screen (see **Figure 3342**) allow you to fine-tune the operation of the WIB protocol. The default values are appropriate for almost all systems and should not need to be changed.



Tx Ack Count— Total number of attempts to be made to transmit a mapping with its Acknowledge checkbox selected if no acknowledgment message is received. In most cases, the default value of three transmissions is recommended

Tx Ack Timeout— Time to wait before deeming a mapping message as "unacknowledged" if the Acknowledge checkbox is selected in the mapping. The default value is two seconds

Tx UnAck Count— Number of times to send an IO mapping if the Acknowledge checkbox is cleared in the mapping. The default is once only.

Figure 34. WIB Protocol configuration

Adding or editing mapping parameters

To add a new mapping for a module or to edit existing mapping parameters, open the module in the project tree, click **Mappings**, and then click **Add** (or **Edit**). **Figure 35** provides an example of a gather scatter mapping.

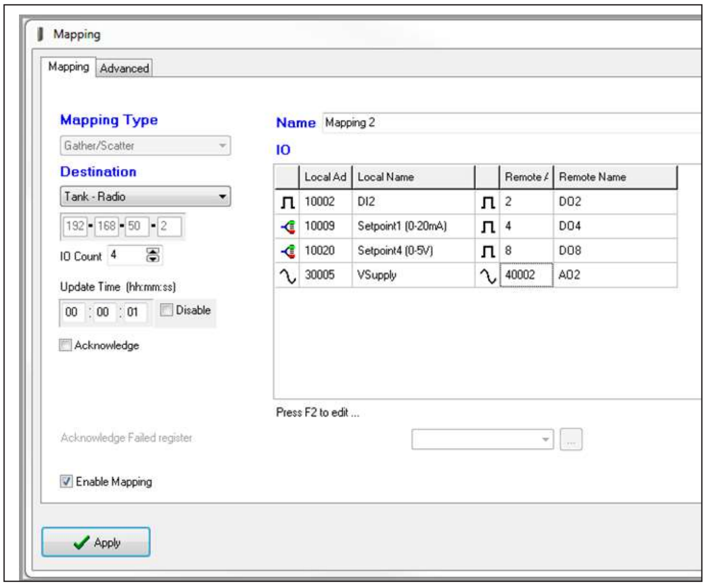


Figure 35. Gather scatter mapping

Name—You can give each mapping a name for reference purposes.

Destination—Provides two standard choices, as well as an Ethernet IP address for each module in the project tree

This Unit—This option refers to the module that you are currently configuring. When this option is selected, the IP address changes to the local host loopback address of 127.0.0.1.

Remote device Name—When you select the name of a device in the system, the mapping will be sent to the device. Ensure that the IP addresses of the sending module and receiving module are able to communicate to each other.

IP Address—This option allows any IP address to be entered in the configuration. It is for advanced users only because the remote name and address location will not show up in the I/O list. Knowledge of the remote module's I/O location and address is required for it to function correctly. Generally this option is only used when a module that is not in the project is loaded or is being mapped to.

I/O Table—Allows you to map each I/O to an output.

Click the **Local Name** field to see a drop-down list of all available I/O, or click the **Local Address** field to view a tabbed I/O selection screen that will allow you to select an I/O point (input) that you want to map.

Select a destination I/O location. Click **Remote Name** for a drop-down list of destination I/O names or **Remote Address** to open a drop-down list of destination I/O locations.

⚠**Note**: You must select an actual destination unit before you can select a remote name. You can select remote address for IP address.

I/O Count—Allows you to add more I/O points to the mapping. If you are using a write or a read mapping, WI-Config will automatically select consecutive registers that are shaded and cannot be edited. When using a gather scatter mapping, WI-Config will add mapping entries which you must then edit by selecting the sending and destination I/O points.

Acknowledge—Select this checkbox to allow the mapping to be acknowledged when the end device receives the message. This is an end-to-end acknowledgment, and is in addition to the normal hop-by-hop frame acknowledgment between links.

⚠**Note**: Enabling this option will increase the amount of radio communications and care should be taken in larger systems.

Update Time—Configures how often the mapping update messages (check signals) are sent. These messages are in addition to the normal change-of-state updates that occur when an input changes.

The default update time is 10 minutes, but you can increase the update time to a maximum of over two weeks, or decrease it to a minimum of one second. Updates can also be disabled by entering a time of zero or selecting the checkbox. Note that the updates are only a check signal, and care should be taken when configuring the update values with short update times (less than 5 seconds) because this will greatly increase the amount of radio traffic.

Response Time—(Read mappings only.) The countdown time before the module registers a communications failure for the configured read mapping. When the timeout is complete, the fail register is activated.

Fail Register—Allows you to configure a register location that will indicate a communication failure for the configured remote destination address.

⚠ **Note**: The Acknowledge checkbox must be selected for fail registers to work. Also, the fail register can only be a digital output or internal bit registers (10501, 501, and so on).

Enable Mapping—Select the checkbox to enable this mapping.

Advanced Options

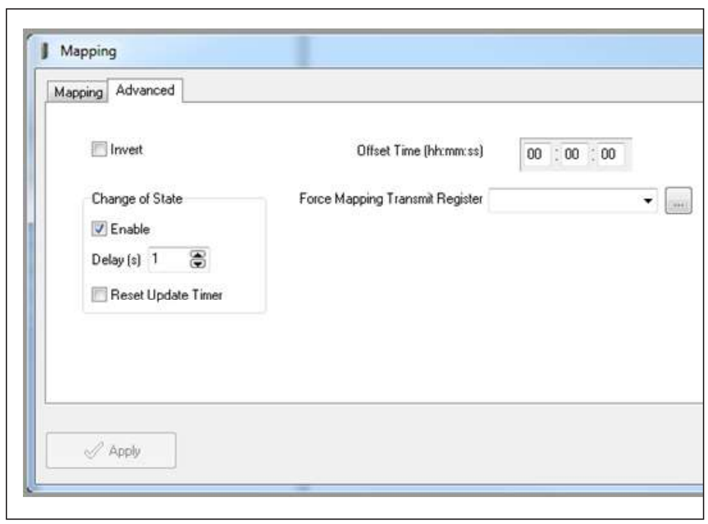


Figure 36. Mapping—advanced tab

Invert—Select this checkbox to allow the mapping to be inverted. For example, if the digital input is "on" and the mapping is inverted, the output will be "off," or if an analog input is 4 mA and the mapping is inverted the output will be 20 mA. The invert applies to all I/O in the mapping. Floating point and long values are not inverted.

Offset Time— Configures an offset time for the update mapping. The offset is used to stagger the update transmissions at startup and at every update period so that the module does not send all mappings at the same time. The default is 0. To stagger transmissions to a predetermined schedule, set a different offset time value for each mapping, and clear the "Reset Update

Timer" flag and the "Change of State Enable" flag for these mappings

Change of State

Enable— When the Enable checkbox is selected, the values are sent to their configured destination when a change-of-state (COS) occurs and the value complies with any sensitivity blocks. If COS is disabled, messages will only be sent on the update period

Delay— Allows you to set the time period during which the message is delayed from being sent. The purpose is to reduce the amount of radio traffic by holding off the transmission to allow more I/O COS to the mapping

Reset Update Timer— If this option is selected, the Update Time period will reset when a COS occurs between configured updates. This means that the next update will not be sent until a further update period has elapsed. You can use this option to reduce the amount of radio traffic produced when multiple mappings are configured

Force Mapping Transmit—Allows you to configure an I/O location that will force the mapping to be sent when the I/O location is written to. External devices, such as Modbus Master/Clients, can initiate the transmission of a mapping by writing to an internal register that then forces the transmission to occur. For more information and examples, see "Startup or force configuration".

⚠ **Note**: Digital inputs 1–8 cannot be used as a force trigger because the digital inputs are continually being scanned by the internal processor and each time a scan occurs it would force the mapping to be sent. If a digital input is required to be used as the trigger, map the digital input to a general purpose bit storage register (501, 10501, and so on), and then use this general purpose register to trigger the force mapping.

Startup or force configuration

When a module is first powered on, it transmits update messages to remote modules based on how the input mappings are configured. The module's outputs will remain in the default "off" condition until the module receives an update or change-of-state message from the remote modules—unless a fail-safe block has been configured for the output, in which case it will default to the value configured in the fail-safe block. For more information, see "Fail-safe blocks" on **page 28**.

To ensure that the module outputs are updated with the latest remote input status when the module is first powered on, you can configure the module to transmit a special startup or force message that will write a value into an internal register at the remote module (or modules). The remote module can then use this register to force any mappings that it has configured for the destination. To configure a force register, see the previous section, "Adding or editing mapping parameters" on **page 22**.

When the force register is activated, any mapping configured with this force register will immediately send an update message to the destination so that its outputs can be set to the latest value. It may be necessary to configure a startup or force message for each remote module that sends values back to the module's outputs.

Example

In the example shown in **Figure 3738**, site A needs to be configured so that on power-up it writes to a register at Site B. Site B then uses this register to trigger an update of any mappings it has that communicate back to Site A. If the system has multiple remote sites that require startup or force configuration, Site A needs to have configured a startup or force mapping for each remote site. If there were multiple remotes in this example, all mappings from the remote sites that are sent to Site A would use the force register configured for 501.

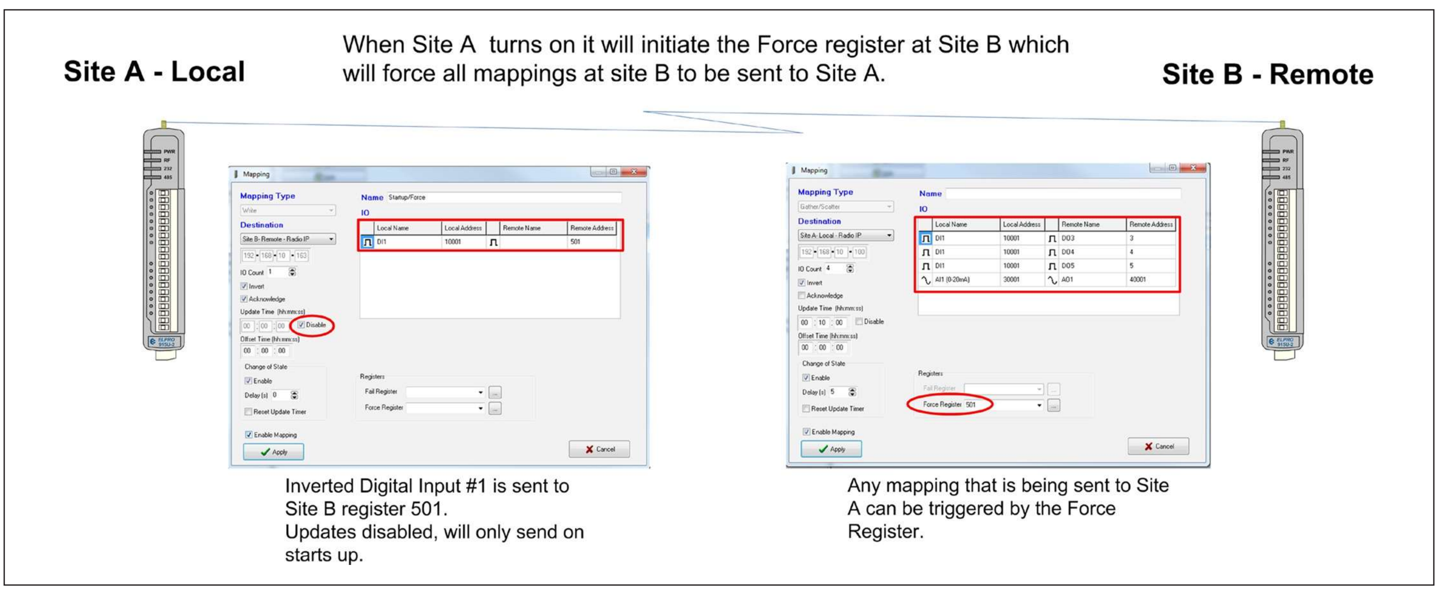


Figure 37. Startup or force configuration

Address map

The I/O data store provides storage for all I/O data, both local data and data received from the system. The I/O store provides four register types—two bit registers, two word registers, two long-word registers, and two floating point registers. In addition, each register type supports both inputs and outputs, making a total of eight register address ranges that are used for physical I/O and gateway storage. These files are mapped into the address range as described in the following table. The addressing uses standard Modbus protocol formatting and is also common to the WEIDMULLER protocol.

Address map

Type	Size	Address
Discrete outputs	6000 (bits)	00001
Discrete inputs	6000 (bits)	10001
Word (unsigned) inputs (16-bit)	6000 (words)	30001
Word (unsigned) outputs (16-bit)	6000 (words)	40001
Long inputs (32-bit)	20 (longwords)	36001
Float inputs (32-bit)	20 (floats)	38001
Long outputs (32-bit)	20 (longwords)	46001
Float outputs (32-bit)	20 (floats)	48001

Common I/O registers for the WI-IO-415-U2

The following table shows the basic on-board I/O registers available in a standard WI-IO-415-U2 module with no expansion I/O connected to it. For a detailed I/O map showing the full register range, see Register memory map **page 71**.

Table 4. Address map—inputs / outputs

Address	Input / output description
0001–0008	Local DIO1–DIO8, as outputs
10001–10008	Local DIO1–DIO8, as inputs
10009–10020	Set point status from analog inputs 1 through 12: AI1, 2, 3, 4 current mode Internal supplies AI1, 2, 3, 4 voltage mode
30001–30004	Local AI1–AI4 (current mode): AI1 and AI2, 4–20 mA diff AI3 and AI4, 4–20 mA sink
30005	Local supply voltage (0–40 V default scaling)
30006	Local 24 V loop voltage (0–40V default scaling)
30007	Local battery voltage (0–40 V default scaling)
30008	WI-EX expansion I/O supply voltage (0–40 V default scaling)
30009–30012	Local AI1–AI4 (voltage mode): AI1 and AI2, 0–20 V AI3 and AI4, 0–5 V
30013–30016	Local pulse input rates PI1–PI4
36001–36008	Local pulsed input counts (PI1 most significant word is 36001 and least significant word is 36002)
38001–38032	Local analog inputs as floating point values (mA, volts, or Hz)
40001–40002	Local AO1–AO2
48001–48002	Local AO1–AO2 as floating point values (mA)

Common I/O Registers for the WI-MOD-415

The WI-MOD-415 is is a reduced I/O version of the WI-IO-415-U2. The following registers are supported.

Address	Input / output description
0001-0002	Local DIO1-DIO2 as outputs
10001-10002	Local DIO1-DIO2 as inputs
10013-10015	Setpoint status from internal supplies
30005	Local supply voltage (0-40 V default scaling)
30007	Local battery voltage (0-40 V default scaling)
30008	WI-EX expansion I/O supply voltage (0-40 V default scaling)
30013-30014	Local pulse input rates PI1 -PI2
36001-36002	Local pulsed input counts (PI1 most significant word is 36001 and least significant word is 36002)

I/O configuration

Each I/O has characteristics that can be tailored to applications. To configure individual I/O settings for a module, click **I/O** in the project tree to display the configurable parameters. These parameters are described in detail in this section.

Digital inputs

To configure digital inputs, click **Digital Inputs** under **IO** in the project tree. Select a digital input from the list on the right, and click **Edit** (see **Figure 38**). This displays the IO Edit screen (**Figure 3940**) where you can change settings.

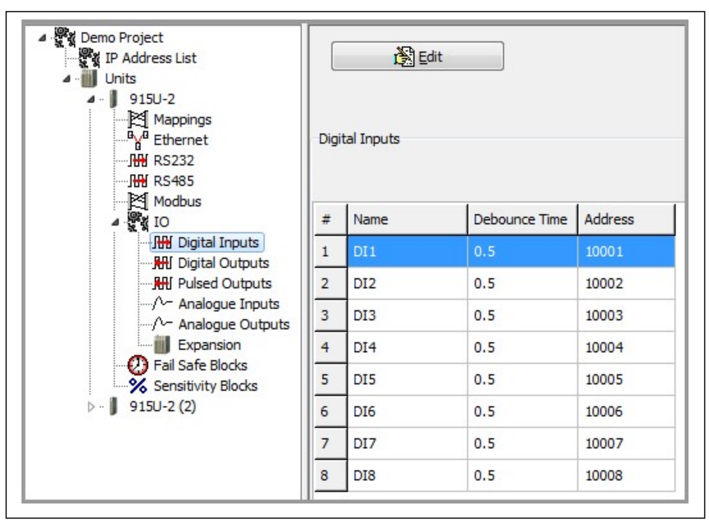


Figure 38. IO—digital inputs

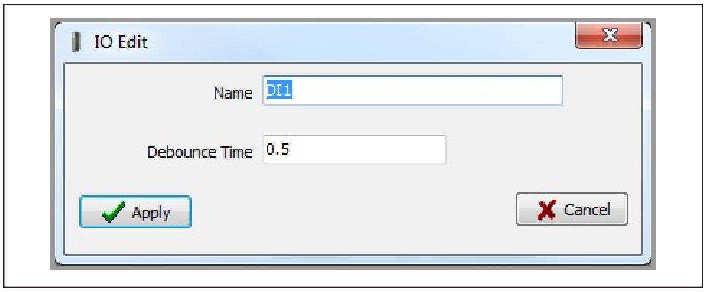


Figure 39. I/O edit (digital inputs)

You can configure following parameters for WI-415 Series digital inputs.

Name
: Enter a name for the digital input or leave the default name. The name can be up to 30 characters, including spaces.

Debounce time (sec)
: Debounce is the period of time that an input must remain stable before the module determines that a change of state has occurred. If a digital input changes from on to off and from off to on in less than the debounce time, the module will ignore both changes. The default debounce time is 0.5 seconds.

Digital outputs

To configure digital outputs, click **Digital Outputs** under **IO** in the project tree. Select a digital output from the list on the right and click **Edit**. This displays the IO Edit screen (**Figure 4041**) where you can change settings.

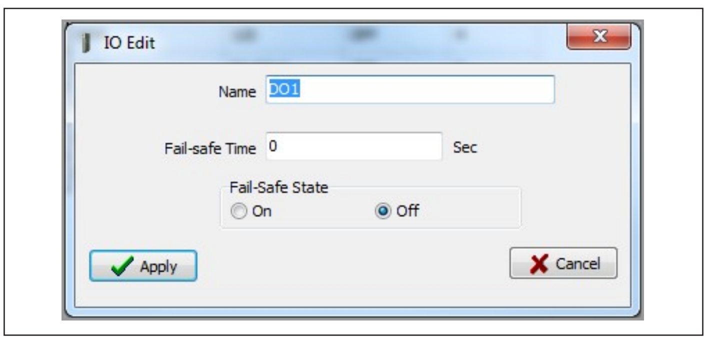


Figure 40. IO edit (digital output)

You can configure the following parameters for WI-415 Series digital outputs.

Name
: Enter a name for the digital output or leave the default name. The name can be up to 30 characters, including spaces.

Fail-safe Time (sec)
: Sets the time the output needs to count down before activating the fail-safe state. Receiving an update or a COS message will reset the fail-safe timer to its starting value. If the fail-safe timer goes down to zero, the output will be set to the fail-safe state (on or off).

: It is recommend the 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 in succession.

Fail-safe State
: Sets the state that the output will assume after the fail-safe time has elapsed. When the fail-safe state is set to On, the LED flashes briefly off, and the digital output turns on. When the fail-safe state is set to Off, the LED flashing briefly on, and the digital output turns off.

Pulsed outputs

To configure pulsed outputs, click **Pulsed Outputs** under **IO** in the project tree. Select a pulsed output from the list on the right, and click **Edit**. This displays the IO Edit screen (**Figure 41**) where you can change settings.

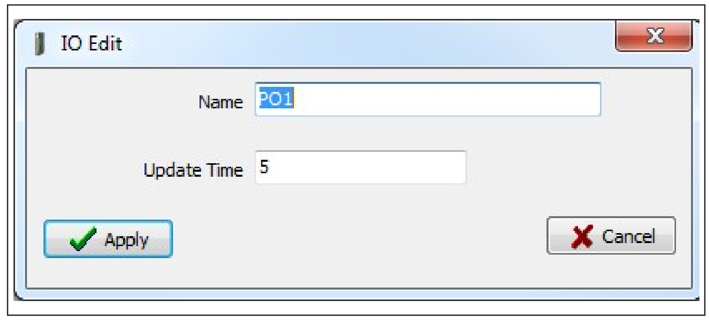


Figure 41. IO edit (pulsed output)

You can configure the following parameters for WI-415 Series pulsed outputs.

Name
: Enter a name for the pulsed output or leave the default name. The name can be 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. For example, if the pulsed input update time at the remote unit is configured for 10 seconds, the number of pulses will be counted and sent to the receiving module every 10 seconds. The receiving module will then output the pulse count over the configured update time (10 seconds).

Analog inputs

Analog inputs each support an associated set-point. Each analog input can also be scaled to convert the analog values to a range suitable for other equipment. Analog inputs can also be used as voltage inputs by selecting DIP switches on the WI-415 Series modules (see “DIP switches” on **page 9**).

To configure analog inputs, click **Analog Inputs** under **IO** in the project tree. Select an analog input from the list on the right, and click **Edit** (see **Figure 42**). This displays the IO Edit screen (**Figure** 43) where you can change settings.

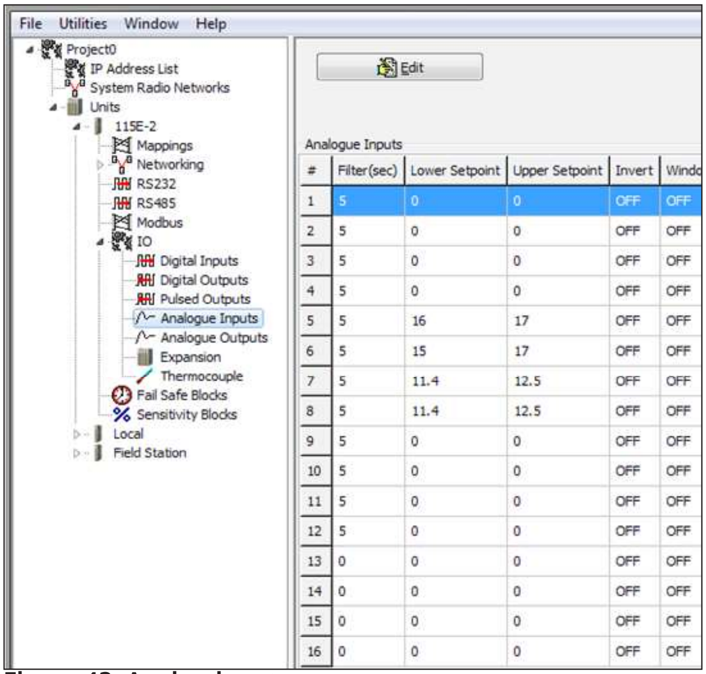


Figure 42. Analog inputs

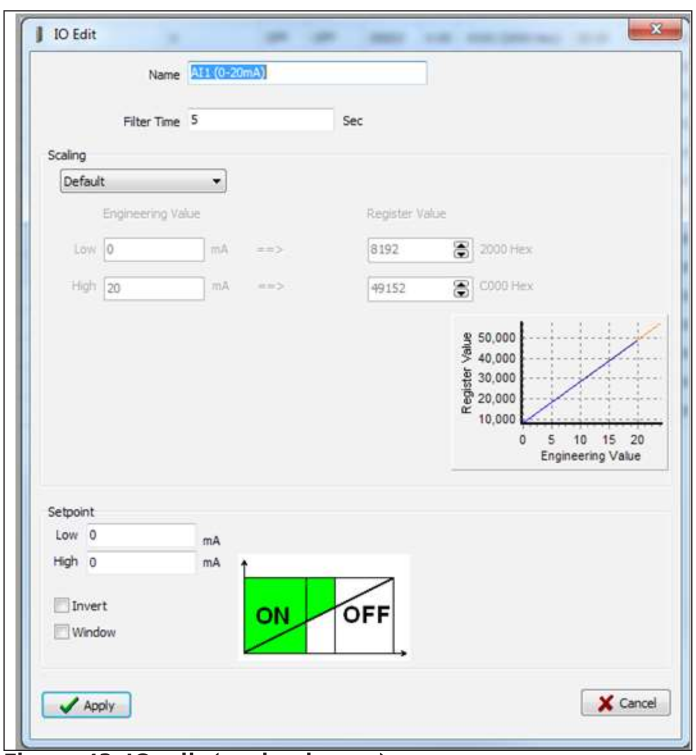


Figure 43. IO edit (analog inputs)

You can configure the following parameters for WI-415 Series analog inputs, including the supply voltage analogs available on both the WI-IO-415-U2 and WI-MOD-415 models.

Name — Enter a name for the analog input or leave the default name. The name can be up to 30 characters, including spaces.

Filter Time (sec) — Period of time (in seconds) needed by the analog input to settle on a step change of an analog value.
By default, all inputs except the pulse rates have a time constant of five seconds. Pulsed input rates are not filtered.

Scaling — You can scale analog inputs to suit data requirements of other systems. When sending analog inputs to outputs on other WI-415 Series devices, select Default. Other scaling options provide support for systems that need data ranges of 8-bit, 12-bit, and 16-bit (signed and unsigned). Use the Custom setting to configure other scaling for systems that cannot be accommodated with any of the other options.

The graph shows how the scaling affects the relationship between the measured value (Engineering Value) and the corresponding scaled 16-bit Register Value.

Lower and Upper Set Points — These set points are the upper and lower control point values that will be used to turn on and off the analog set point digital signals located at register 10009–10020.

⚠ **Note**: Set point values are entered in the scale of the input. For example, analog input 1–4 should be in mA, analog inputs 9–12 should be volts, and so on.

To control the set points, use the Invert and Window control options described below. All set points have these controlling options.

Invert — Selecting this option inverts the set point control logic. The function does not change—only the operation is inverted. For example, if the set point is “on” in its normal state, inverting the signal causes the set point to be “off” in the normal state. By default, the checkbox is cleared and the set point logic is not inverted.

Window — Selecting this checkbox sets the set point operation to Window mode. Clearing this checkbox sets the set point operation to default mode.

Window mode—In this mode, if the analog value is inside the upper and lower set points, the set point will be active (on, “1”), and if the analog value is outside of these set points, the set point will be reset (off, “0”).

Default mode—In this mode, the set point operates in default mode. If the analog input is greater than the upper set point, the set point status is active (on, or “1”). When the analog input is less than the lower set point, the set point is reset (off, or “0”). When the analog value is between the upper and lower set points, the previous value is maintained.

⚠ **Note**: The upper set point must always be higher than the lower set point.

Analog outputs

To configure analog outputs, click **Analog Outputs** under **IO** in the project tree. Select an analog output from the list on the right, and click **Edit** (see **Figure 44**). This displays the IO Edit screen (**Figure 45**) where you can change settings.

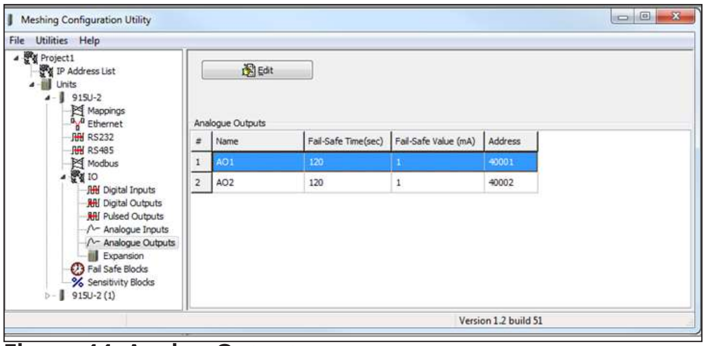


Figure 44. Analog Outputs

Figure 45. Analog outputs

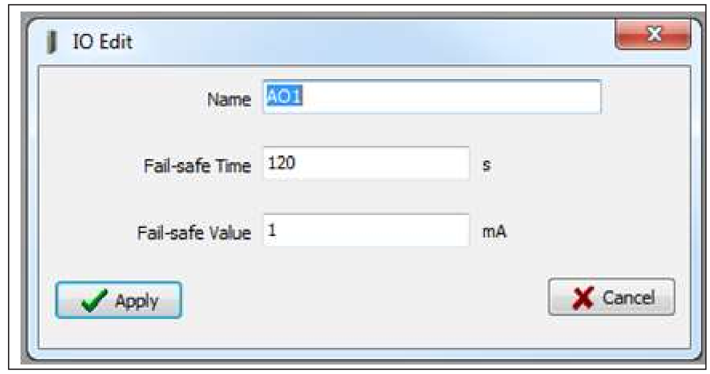


Figure 45. IO edit (analog outputs)

Adding expansion I/O modules

You can connect additional WI-EX serial expansion I/O modules to the WI-415 Series module if more I/O is required. The RS-485 serial port on the WI-415 Series is configured by default to communicate with WI-EX expansion modules using the Modbus protocol. The default serial parameters of the RS-485 port on the WI-415 Series are 9600 baud, no parity, 8 data bits, 1 stop bit, which match the default settings of the WI-EX serial expansion modules. You can change these parameters to increase poll speeds in larger systems, but the serial module's parameters must match that of the WI-415 Series RS-485 port.

If more than three serial expansion I/O modules are added to the WI-415 Series module, you will need to adjust the Maximum Connections setting for RS-485 or RS-232. To display these configuration screens, select the module in the project tree and click **RS-485** or **RS-232**.

⚠ **Note**: Reducing the Maximum Connections setting will slightly improve the serial scan time. However, you need to make sure that the slave addresses fall within the Maximum Connections. If the Slave address is above the Maximum Connections, it will not be polled.

When you connect the serial expansion module, before powering on, set the expansion module address using the rotary switches on the bottom of the module. Assign addresses sequentially, starting at address 1. Make a note of the module address. This address will be used as an offset to locate the I/O within the WI-415 Series. Also make sure that the termination switch is "on" (down) for the last module in the RS-485 loop.

⚠ **Note**: Failure to terminate the RS-485 correctly will result in modules not operating correctly.

WI-EX Expansion I/O Memory map

The I/O data on the WI-EX module is read into memory locations according to their Modbus address. The maximum supported Modbus address is 19. Each WI-EX module has an offset that applies to the location of its registers. This offset is equal to the units Modbus address (selected on the rotary switch on the end of the WI-EX expansion I/O module), multiplied by 20.

If the modules Modbus address is 15, the offset value will be 15 X 20 = 300.

For example, if connecting a WI-EX-11 (16 x DIO) with address #15:

- Digital input 1 will be at register location 10301
- Digital Output 1 will be at register location 301

If using a WI-EX-12 (8 x DIO and 8 AIN) with address 16:

- Digital input 1 will be at register location 10321
- Analog input 1 will be at register location 30321

For a detailed address map of the serial expansion I/O modules, see **page 71**.

When adding expansion I/O modules to the WI-415 Series, there are two inbuilt registers indicating the communication status of the expansion I/O module:

- **Communication fail**—Located at register location 10019 + offset value. This register indicates "1" when the module is in failure.
- **Communication oK**—Located at register location 10020 + offset value. This register indicates "1" when the module is communicating properly.

Adding an expansion I/O to WI-Config

In WI-Config to add a WI-EX expansion I/O to the WI-Config utility, open the module in the project tree and click **Expansion**, and then click **Add** (see **Figure 46**).

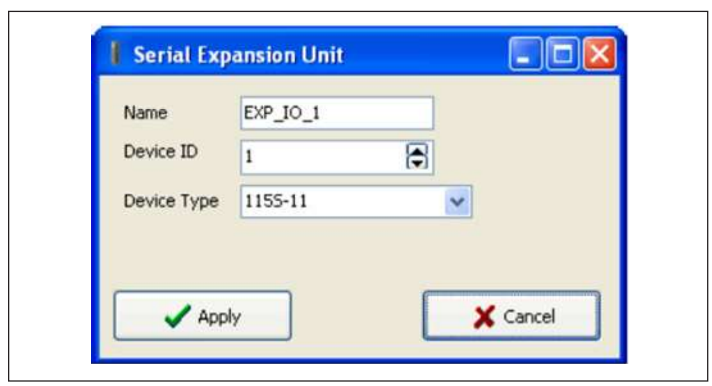


Figure 46. Serial expansion unit

Name	Enter a name for the WI-EX expansion I/O module, or leave the default name. The name can be up to 30 characters, including spaces.
Device ID	Select the address of the expansion I/O module. The address is found on the rotary switch on the bottom of the WI-EX expansion I/O module.

Device type Select the module type from the drop down list.

Fail-safe blocks

To configure fail-safe blocks for a module, open the module in the project tree and click **Fail-safe Blocks**. The Fail-safe Block configuration screen (**Figure 47**) allows you to set registers to a pre-configured value on startup and configure the outputs to reset to a predefined value after a timeout period has elapsed. When the actual value is received, the register is automatically updated with this value. If the value is lost because of a communication problem, the register can be configured to set the register to a fail-safe value after the pre-configured time. You can have a maximum of 50 fail-safe blocks.

In the example shown in **Figure 47**, register 40501 holds an analog value that has been mapped from another module and is updated every 60 seconds. The fail-safe block is configured so that on startup the module will write a value of 16384 into register 40501, and then start counting down the fail timeout period (in this case, 600 seconds), which is a little over two times the update period from the sending module. If the module has not received an update from the other module after 600 seconds, register 40501 will be set to the fail value (in this case, Invalid). If the "Invalidate" option is selected, the value will be set to a null or invalidated value (~). If this register happens to be mapped to another module and the state is "Invalid," the mapping will be inhibited until the invalid value is updated with an actual value.

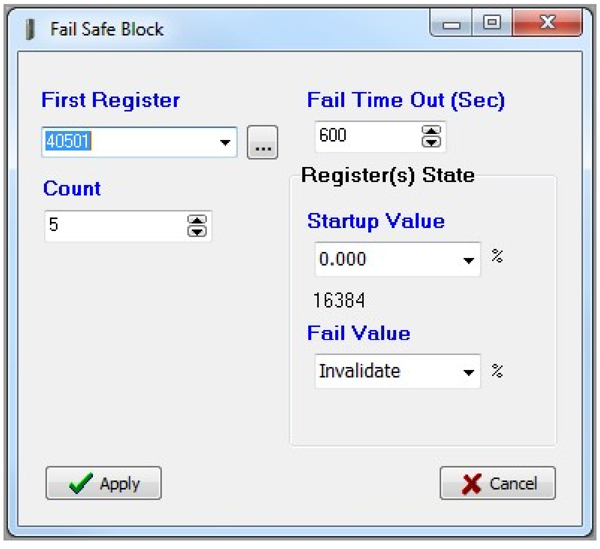


Figure 47. Fail-safe block analog

In the example shown in **Figure 4849**, digital outputs 1–8 will be initialized on startup (turned on) and then start the fail timeout countdown from 60 seconds after which time the outputs will be set to the fail value (off) unless the output is updated.

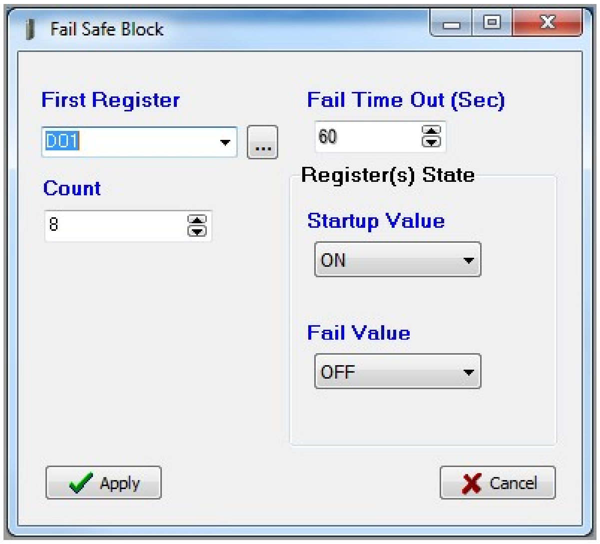


Figure 48. Fail-safe block digital

First Register	Starting register to which the fail-safe block applies.
Fail Timeout	Time period before the fail-safe state will be activated. Set this value to zero to disable the fail timeout (the startup value will still be set).
Count	Number of outputs to which the fail-safe block applies.
Startup Value	Value the registers are set to when the module is powered on. Select “Invalid” or a desired value. For digital registers, the value can be either ON or OFF. For analog registers, select “Enter Value” and enter the desired value. The value is set as a milli-amp value or as a percentage. The actual register value is displayed below the value setting.
Fail Value	Value that the registers are set to if an update is not received before the fail timeout period expires. Select “Invalid” or a desired value. For digital registers, the value can be either ON or OFF. For analog registers, select “Enter Value” to enter a value. The value is set as a milli-amp value or as a percentage. The actual register value is displayed below the percentage setting.
Apply	Saves the settings.

⚠ **Note**: Don’t use the failsafe for physical outputs. For Physical outputs, use the fail safe feature attached to the output.

Invalid register state

All registers within the module can have different states, depending on the type of register and the type of value it holds. A typical analog range is between 0 and 65535, and a digital can be 0 or 1. Registers that are not associated with a physical I/O can also be in the “invalid” state, which means that the register has not been written to and holds a non-value or null value. If you use I/O diagnostics to read the registers, an invalid register will read “~“ as shown in **Figure 49**. For information on I/O diagnostics, see “IO diagnostics” on page 59.

⚠ **Note**: Any mapping with an invalid register will be inhibited from sending. This is to ensure that the data sent to the destination is valid and not the default values the module has on startup. See “Fail-safe blocks” on **page 28** for information on configuring registers with a valid value at startup.

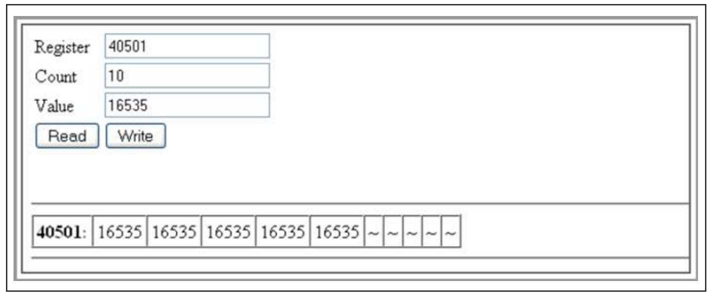


Figure 49. Invalid register state

Sensitivity blocks

All I/O registers have a configurable sensitivity value that determines how much the register needs to change before a change-of-state” (COS) message is sent. All registers except the following have a default sensitivity value of 1:

- The 12 analog inputs have a sensitivity of 1000 counts, or approximately 3% (1000 counts from a total range of 32768 = 3.05%).
- The 24 floating point values have a default sensitivity of 0.5 units.
- Inputs 38001–38004 will be 0.5 mA, inputs 38005–38012 will be in volts, and inputs 38013–38016 will be in hertz.

A sensitivity value is needed for analog inputs in order to prevent the module from sending every single-bit change of an analog value, and subsequently saturating the radio channel with unwanted COS messages. If a lower sensitivity is required, you can adjust the sensitivity block. However, take care not reduce the sensitivity to the point where radio messages are so frequent (due to a sensitivity change) that it saturates the radio network. There is a fine line between adjusting system parameters to receive up-to-date data and overloading the radio communications. A total of 50 sensitivity blocks can be configured for different registers or different values.

To change sensitivity blocks for a module, click **Sensitivity Blocks** in the project tree (see **Figure 50**). The screen lists existing sensitivity blocks for this module. To add a new sensitivity block, click **Add**. To edit an existing sensitivity block, select it in list on the right, and click **Edit**. This displays the IO Edit screen (see **Figure 51**) where you can change settings. To delete a sensitivity block, select it in the list and click **Delete**.

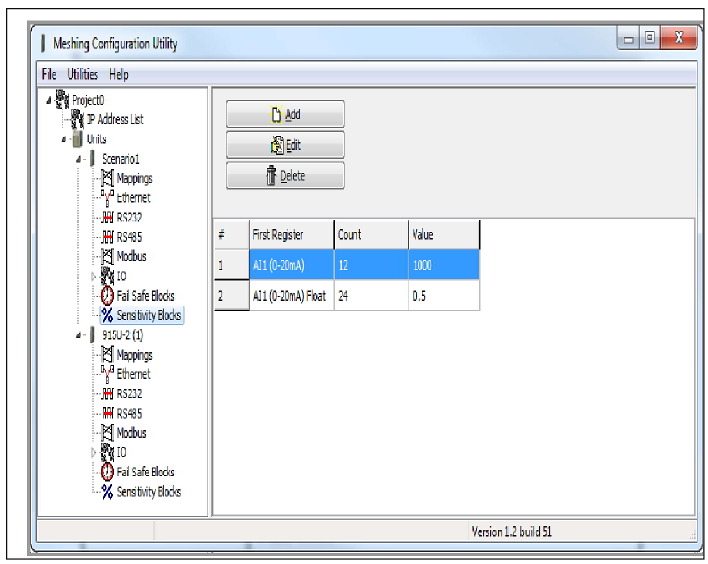


Figure 50. Sensitivity block

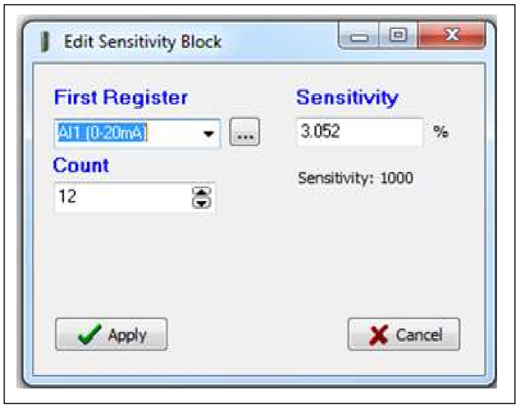


Figure 51. Editing sensitivity block

First Register	Select the starting register for the sensitivity block.
Count	Select the number of consecutive registers to which the sensitivity applies.
Sensitivity	Select the amount that the register needs to change before a COS trigger occurs.

Dashboard configuration

The 451U-2 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" tree node under the device that you want to configure.

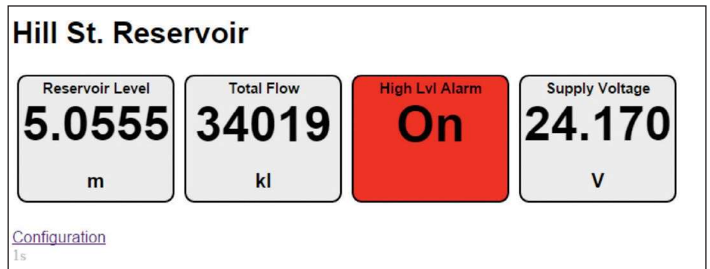


Figure 52. Example dashboard display

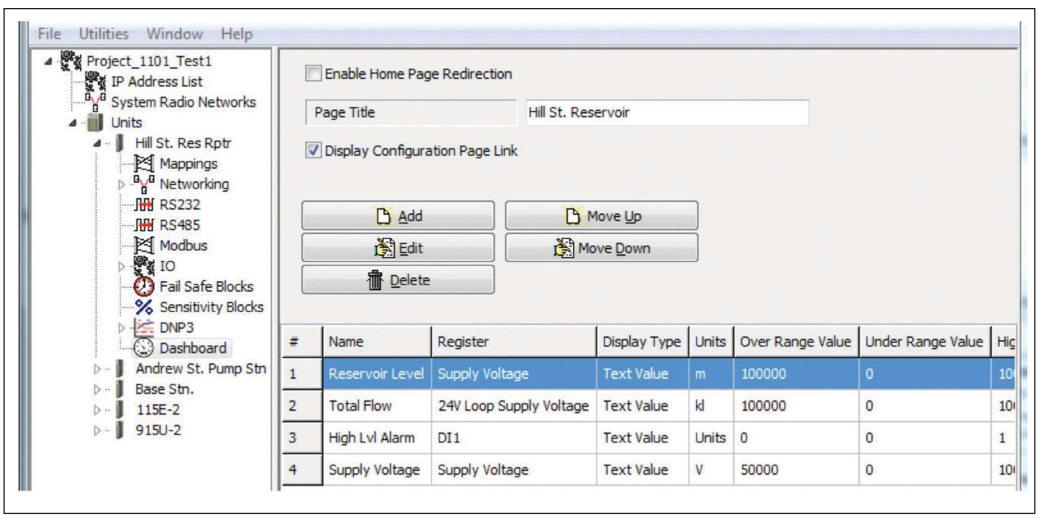


Figure 53. Dashboard configuration

You 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).	**Display Configuration 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:///operator/main.asp
Page Title:	This is the title that will be displayed at the top of the dashboard view	**Add" and "Delete" buttons:**	These let you add and delete table rows. Each row corresponds to an item on the dashboard display.
		"Move Up" and "Move Down" buttons:	These let you adjust the order items are displayed on the dashboard. Items are displayed on the dashboard in the same order as they are listed in the table

"Edit" Button: This lets you edit the settings for the currently selected table row. This activates the Edit dialog box.

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.

Display Type: Currently the "Text Value" option is only supported. Future firmware releases may support graphical display of analog values

Units: (Analog registers only) Enter the text to display for units.

Over/Under Range Value: (Analog registers only) If the displayed value moves beyond these thresholds, the text "Ovr" or "Und" is displayed instead of the displayed value.

High / Low Alarm: If the 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

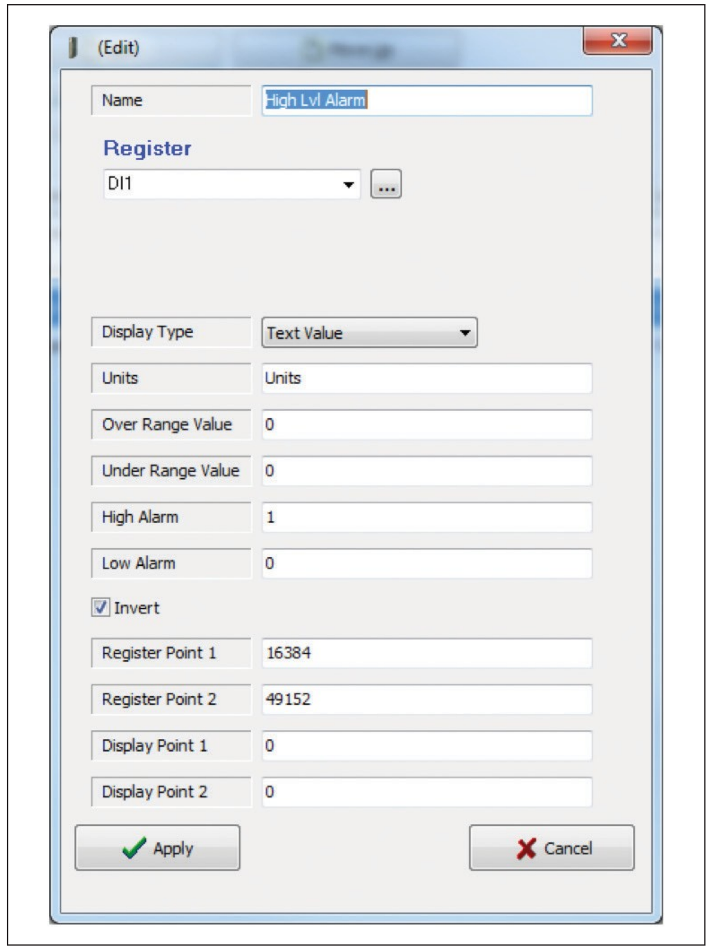


Figure 54. Edit window

Serial configuration

The WI-415 Series module has an RS-232 and an RS-485 port for serial communications. These ports are used to connect WEIDMULLER WI-EX-11, WI-EX-12, and WI-EX-13 serial expansion I/O modules. The ports can also be used to connect external Modbus RTU master or slave devices. The port operating mode and the normal serial parameters, baud rate, data format, flow control, and so on, all need to be selected from the drop-down lists, depending on the type of device connected and how it will operate.

⚠ **Note**: An error is displayed if the operating mode selection is incompatible with the configuration. For example, you will see an error if Modbus mode is not selected when Modbus mappings are configured.

Each serial port can be configured to operate in one of the following operating modes:

- **Modbus RTU Master**—This mode should be configured when the port is operating as a Modbus master, for example, when Modbus RTU slave devices are connected directly to the serial port.
- **Modbus RTU Slave**—This operating mode should be used when the port is being used as a Modbus RTU slave, for example, when a Modbus master (such as DCS, or SCADA) is connected to the serial port.
- **Expansion I/O**—This operating mode should be selected when WEIDMULLER serial expansion modules are connected to the module.

Modbus RTU master

To configure a module serial port as a Modbus RTU master, click the serial port (**RS-485** or **RS-232**) in the project tree, and then select **Modbus RTU Master** from the **Operating Mode** drop down menu (see **Figure 55)**.

The Modbus RTU master should be configured if the WI-415 Series is acting as a Modbus RTU master and polling Modbus slave devices via the selected serial port. It also allows Ethernet Modbus/TCP clients connected to the WI-415 Series Ethernet port to communicate with Modbus RTU slave devices connected to the configured serial port. The WI-415 Series makes this possible by internally performing the necessary protocol conversion. The conversion is performed by the WI-415 Series that is directly connected to the Modbus serial device (only this module needs to have Modbus TCP to RTU gateway enabled).

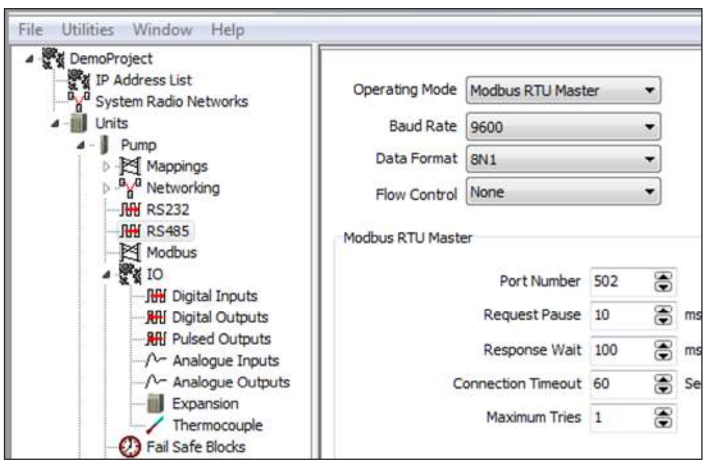


Figure 55. Modbus TCP/RTU

When a serial port is configured as a Modbus RTU master there are a number of parameters (such as baud rate, data format and flow control) that you can adjust, depending on the devices connected.

Request Pause	Delay between serial requests, in milliseconds.
Response Wait	Serial response timeout period, in milliseconds. A serial retry is sent if a response is not received within this timeout period.
Connection Timeout	TCP connection timeout period, in seconds. If no Modbus/TCP data is received within this timeout period, the TCP connection will be dropped. Set this field to zero for no timeout.
Maximum Tries	Maximum number of request retries that are performed on the serial port.

Serial expansion I/O

To change serial port parameters for expansion I/O, click the serial port (**RS-485** or **RS-232**) in the project tree, and then click **Expansion I/O** in the **Operating Mode** drop down menu (see **Figure 56**).

By default the RS-485 port is automatically enabled for expansion I/O. This is to allow you to connect serial expansion I/O modules with minimal or no module configuration. When you add an WEIDMULLER Expansion I/O module (such as an WI-EX-11, WI-EX-12, or WI-EX-13)
to the RS-485 port of the WI-415 Series, the I/O is automatically available from within the I/O store of the WI-415 Series. See **page 71** for location addresses, or refer to the WI-EX Expansion I/O User Manual.

The default data rate and data format are standard 9600, N81 with no flow control, which matches the default serial baud rate and data format of the WI-EX serial expansion module. You can adjust serial parameters for compatibility or faster serial performance. If you change the baud rate or data format, the serial port parameters on the expansion I/O module also need to be changed. To do this use the Modbus Serial I/O Module option from the WI-Config Utilities menu.

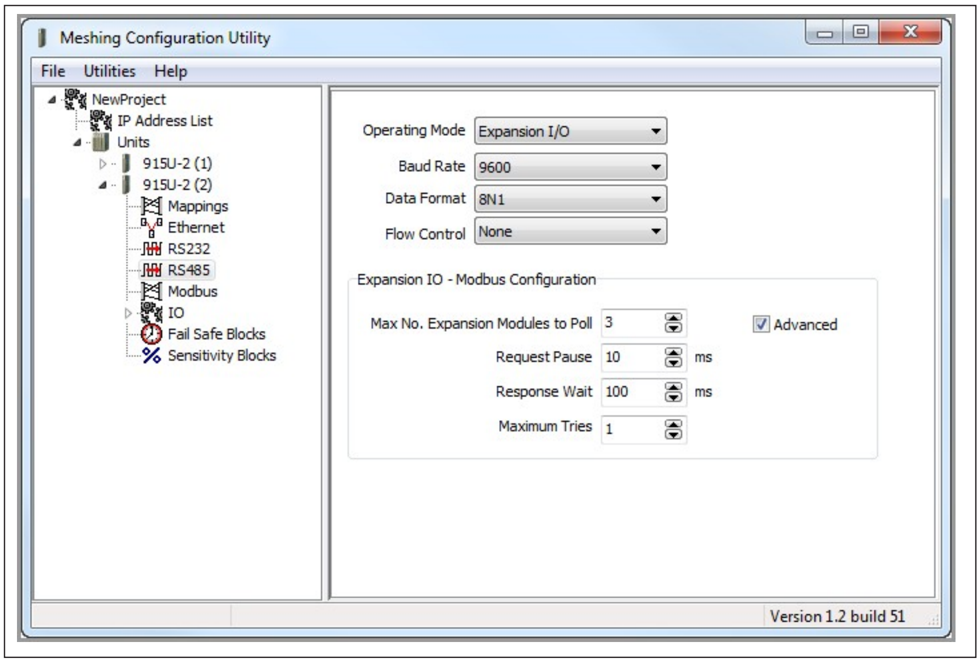


Figure 56. Expansion I/O

Maximum No. Expansion Modules to Poll	Maximum number of slave addresses that the WI-415 Series will scan or poll. Default is 3. If adding more than 3 x WI-EX expansion I/O module or the address used are greater than 3, this number will need to be increased to match the largest address.
Advanced	Selecting the Advanced check-box displays the Request Pause, Response Wait, and Maximum Time fields. If a WI-EX module is directly connected to the WI-415 Series, it will operate correctly using the default settings. You may need to change the default settings if the WI-EX is located remotely from the host module.
Request Pause	Delay between serial requests, in milliseconds
Response Wait	Serial response timeout, in milliseconds. A serial retry is sent if a response is not received within this timeout period.
Maximum Tries	Maximum number of request retries performed on the serial port. This should be set to 1 (no re-tries) for directly connected expansion I/O.

Serial Modbus RTU slave

When a serial port is configured as a Modbus RTU slave, the only parameters that need to be configured are data rate, data format, and flow control. To configure these parameters, click the serial port (**RS-485** or **RS-232**) in the module project tree, and then click **Modbus RTU Slave** in the **Operating Mode** drop down menu. The Modbus slave device ID is configured by clicking Modbus in the project tree (see the next section).

Modbus configuration

The WI-415 Series provides Modbus TCP client/server and Modbus RTU master/slave functionality for I/O transfer. Modbus TCP client, Modbus RTU master, and Modbus TCP server/RTU slave can all be supported simultaneously. When combined with the built-in Modbus TCP-to-RTU converter, the WI-415 Series can transfer I/O to and from almost any combination of Modbus TCP or RTU devices.

The WI-415 Series has predefined data areas for inputs and outputs and the different I/O types (bits, words, long, floats, and so on), which
include the onboard input/outputs and are shared for both client and server. For a full list of the available I/O and address locations see .

To change Modbus configuration parameters, click **Modbus** in the project tree. The Modbus configuration screen (**Figure 57**) is arranged in tabs. The main tabs are:

- **Modbus TCP Server and RTU Slave**—Used for configuring Modbus TCP Server or RTU Slave parameters.
- **Modbus TCP Client and RTU Master**—Used for any Modbus TCP Client and Modbus RTU Master Configuration parameters.

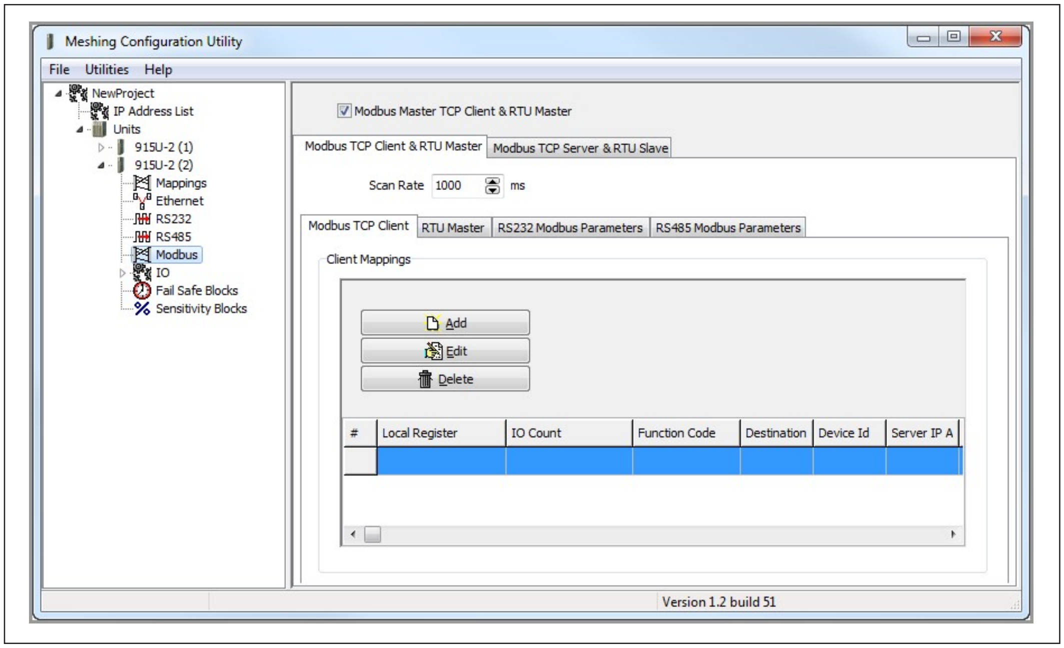


Figure 57. Modbus configuration

Modbus Master TCP Client and RTU Master	Used to enable the Modbus master TCP client and RTU master. When this is disabled the screen appears as in **Figure 58**.
Scan Rate	Allows you to adjust the Modbus polling scan rate. The scan rate is the delay between the completion of one request and the initiation of the next request.

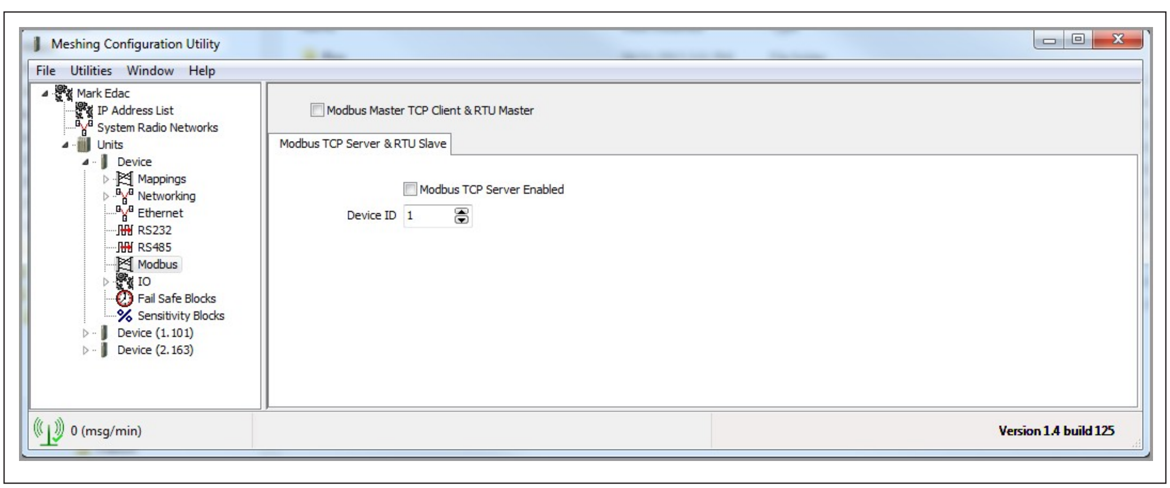


Figure 58. Modbus master TCP client and RTU master disabled

Modbus TCP server and RTU slave tab

Click this tab in the Modbus configuration screen to change parameters for the Modbus TCP server or RTU slave (see **Figure 59**).

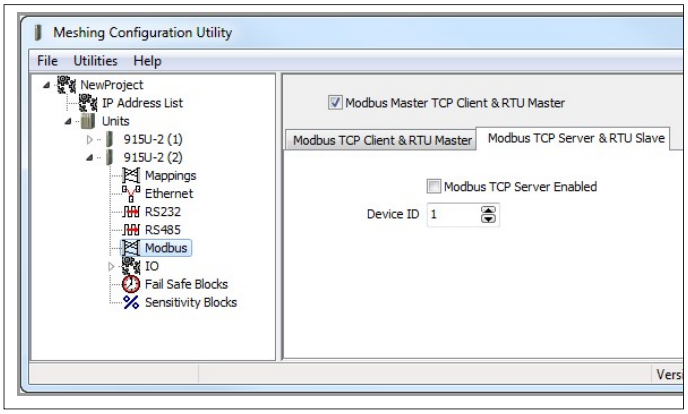


Figure 59. Modbus TCP server and RTU slave tab

Modbus TCP Server enabled	Allows the WI-415 Series 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 WI-415 Series via TCP or serial connection).

Modbus TCP client and RTU master tab

Click this tab in the Modbus configuration screen to set the Modbus client scan rate, which is common to both the Modbus TCP client and Modbus RTU master (see **Figure 60**). The default rate is 1000 msec. Each mapping is configured with a response timeout, which is the period of time that the master will wait for a response before indicating the failure on the Comms Fail Register.

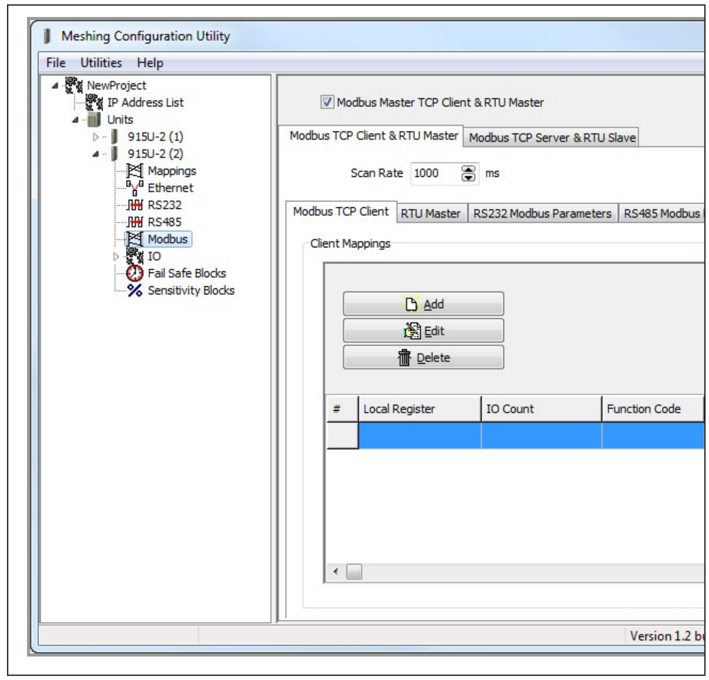


Figure 60. Modbus TCP client and RTU master tab

The Modbus TCP Client and RTU Master tab contains the following subtabs.

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. For more information, see "Adding mapping parameters" on **page 36**.
RTU Master	Allows you to configure Modbus RTU mappings to communicate with remote serial Modbus devices. For more information, see "Adding mapping parameters" on **page 36**.
RS-232 Modbus Parameters	Shows the configuration parameters for RS-232 ports. See "RS-232/RS-485 Modbus parameters" on **page 38**.
RS-485 Modbus Parameters	Shows the configuration parameters for RS-485 ports. See "RS-232/RS-485 Modbus parameters" on **page 38**.

All Modbus mappings are directed to and from the onboard I/O registers, depending on configuration (see the following section).

Adding mapping parameters

Before adding or modifying a module's TCP or RTU mappings, make sure that the Modbus Master TCP Client and RTU Master checkbox is selected at the top of the Modbus configuration screen (see **Figure 60**). Click the Modbus TCP Client or the RTU Master subtab, depending on the connected device. Then, click **Add** to add a new mapping, **Edit** to edit a selected mapping, or **Delete** to delete a selected mapping. Clicking Add or Edit displays the screen in **Figure 61**, where you can specify mapping parameters.

Both Modbus TCP client and RTU master mappings have similar parameters, the only difference will be the slave communication path. For example, Modbus TCP client mappings will use a network address and port while RTU master mappings will use a serial port.

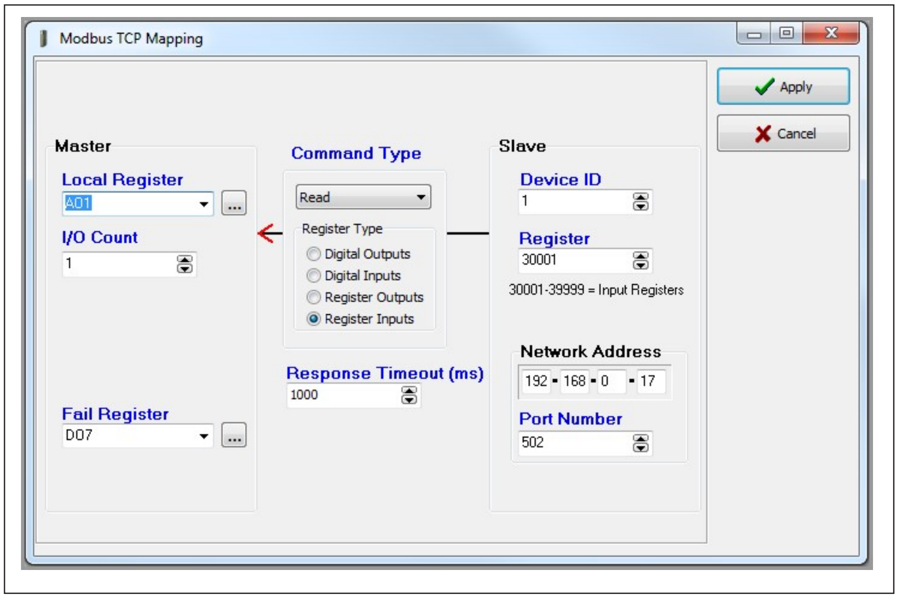


Figure 61. Modbus TCP client mapping

Local Register (Master)	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.
I/O Count	The number of consecutive I/O values in the mapping.
Function Code (Command Type)	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 (Slave)	The register location on the TCP server/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.
Server IP Address **Network Address**	(TCP client only.) The IP address of the Modbus TCP server.
Server Port (TCP Client only)	The server port of the slave device, Modbus TCP will usually be the standard port address of 502.
Serial Port (Modbus RTU only)	This is the serial port used to connect to the device. Select the port from the drop-down list.
Response Time	The amount of time the TCP client or Modbus master waits for a response from a TCP server or an RTU slave device before registering a Communications Fail.
Fail Reg	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 73**.

Modbus TCP mapping examples

In the example in **Figure 62**, the first mapping (#1) shows the Modbus client (master) is configured to read analog values from a device connected on the LAN. The mappings function code is “Read” and is reading a count of four values (analogs) from the Ethernet address 192,168.0.17, device ID #10, starting at address 30001, and then writing these values into its own local registers, starting at 40501. The server port is 502, which is a standard Modbus TCP port address. If the mapping fails to communicate to the TCP server, it will write a value of “1” into local register 508, indicating a communications failure.

#	Local Register	IO Count	Function Code	Destination	Device Id	Server IP Address	Server Port	Response Timeout	Comm Fail Register
1	10501	1	Read	1	1	192.168.0.17	502	1000	DO8
2	AO1	1	Read	30001	1	192.168.0.17	502	1000	DO7
3	10502	1	Read	10001	1	192.168.0.17	502	1000	DO6
4	AO2	1	Read	40001	1	192.168.0.17	502	1000	DO5
5	10503	1	Read	10001	1	192.168.10.101	502	1000	DO4
6	10504	1	Read	10001	2	192.168.10.101	503	1000	DO3

Figure 62. Modbus TCP mapping table

The second mapping (#2) shows something similar, but instead of analog values, the values are digital. The Function code is “Read” from IP address 192.168.0.17 and device ID #10. It will read eight values starting from address 10001, and write them to the local address, starting at 501. Again, it is using the same server port of 502. If the mapping fails to communicate to the TCP server, it will write a value of “1” into local register 507, indicating that mapping failed to communicate.

The third mapping (#3) is similar to the second mapping, but instead of reading from the local Ethernet subnet (LAN) it is reading from an IP address on the radio network (another WI-415 Series module). The Function code is “Read” from IP address 192.168.10.101 and device ID #1. It will read four values, starting from address 10001, and write them to the local address, starting at 509. A Comms Fail register is configured at local register 506.

The fourth mapping (#4) is configured to write the values from the local analog input #1 and #2 across to a TCP server at IP address 192.168.0.17. It will write the values into the destination address 40001 and 40002 at device ID of 10. It is using the TCP server port 502 and is configured with a response time of 1000 msec. If it fails to communicate, it will turn on local register 505.

Modbus RTU master

Modbus RTU functionality allows connections to Modbus RTU slave devices via the RS-232 or RS-485 ports. Up to 100 mappings can be configured. All Modbus mappings are directed to or from the onboard I/O registers depending on the configuration (described below). The Modbus RTU master polls the slave devices via the serial port configured in the mappings.

Modbus RTU (serial) devices can also be polled if connected to remote WI-415 Series serial ports. To enable this feature the remote WI-IO-415-U2 serial port must be set to “Modbus RTU Master” mode and the TCP mappings must reflect the correct server IP address and port number of the remote WI-415 Series. Polling TCP servers or RTU slaves over the radio network will greatly increase radio communications and is not recommended for busy systems.

Example

The Modbus RTU mapping is very similar to the Modbus TCP mapping except that the destination is a serial interface instead of an Ethernet address and port.

In the example in **Figure 63**, the first mapping (#1) shows a read mapping from a serial device connected on the RS-485 port with a device ID of 5. It is reading one I/O point, starting at remote address 30001, and writing the value into the local address 40501. It is configured with a response timeout of 1000 msec, and local register 508 will indicate a failure to communicate with this device.

#	Local Register	IO Count	Function Code	Destination	Device Id	Serial Port	Response Timeout	Comm Fail Register
1	40501	1	Read	30001	5	RS485	1000	508
2	501	16	Read	10001	5	RS485	1000	507
3	VBatt	1	Write	40001	6	RS232	1000	506

Figure 63. Modbus RTU example

The second mapping (#2) shows a read mapping from a serial device connected on the RS-485 port with a device ID of 5. It is reading 16 I/O points, starting at remote address 10001, and writing the value into the local address 501. It is configured with a response timeout of 1000 msec, and local register 507 will indicate a failure to communicate with this device.

The third mapping (#3) is a write mapping that will write the local battery voltage (Reg 30007) to register 40001 on a serial device connected on the RS-232 with a device ID of 6. Again, the response timeout is 1000 msec, and it has a communications fail register of 506.

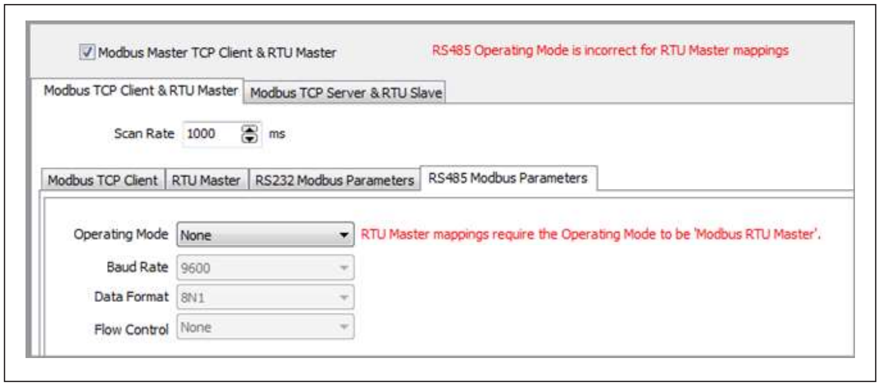


Figure 64. Operating mode error

⚠ **Note**: WI-Config will indicate whether the serial port "Operating Mode" is not set, or set to the wrong mode. To change the mode, click the RS-232 or RS-485 Modbus Parameter tab.

RS-232/RS-485 Modbus parameters

The RS-232 and RS-485 Modbus Parameters tabs show the configuration parameters for the RS-232 and RS-485 ports. These parameters are the same as the serial parameters described in "Serial configuration" on **page 32**. These parameters are displayed under the Modbus tab for convenience.

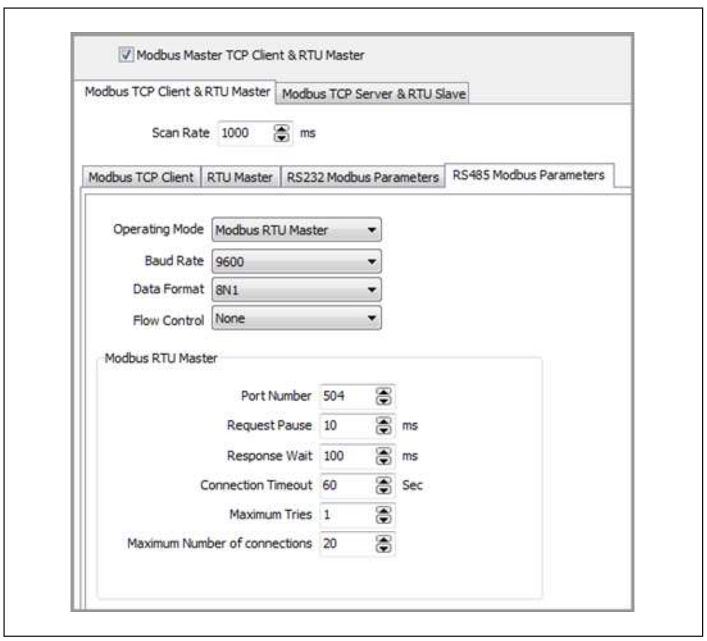


Figure 65. Modbus parameters

DNP3 protocol configuration

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 WI-415 Series modules with the purchase of a feature license key (see “Feature license keys” on page 5161).

This chapter describes how to use the WI-Config utility to configure DNP3 settings once you have enabled the DNP3 feature in the WI-415 Series.

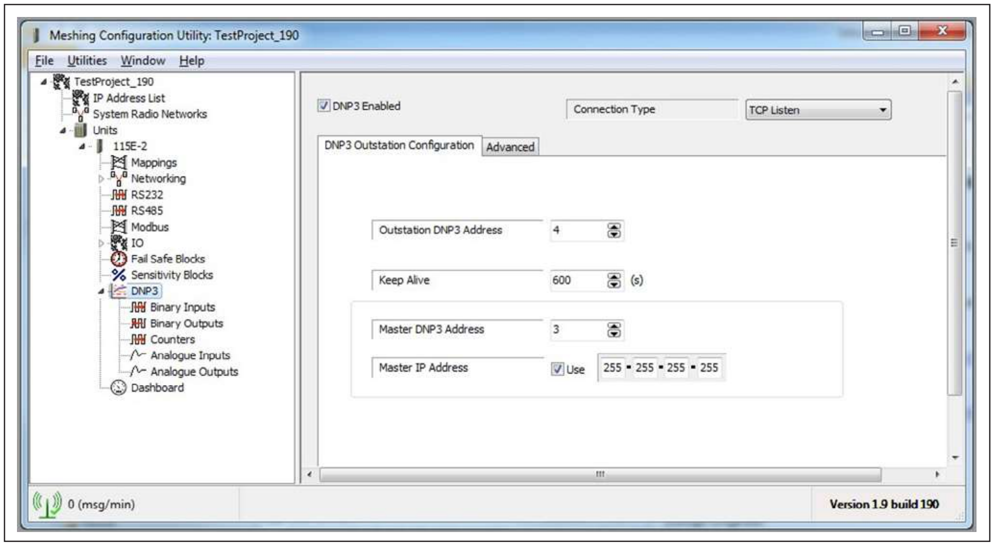


Figure 66. DNP3 address configuration

DNP3 Enabled	Select this checkbox to enable the DNP3 function. Clear the checkbox to disable DNP3.	Master DNP3 Address	Sets the DNP3 address of the master station that will control the WI-415 device.
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.	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 devices IP address to match the requirements of your system. For more information, see “Network settings” on page 20.
Outstation DNP3 Address	Sets DNP3 address of this WI-415 device. Set this address to match the address configured in the DNP3. Valid values are 1–65531.	Outstation DNP3 Address	Sets DNP3 address of this WI-415 device. Set this address to match the address configured in the DNP3. Valid values are 1–65531.
Keep Alive	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.	**Default Address Configuration**	The following are the factory default DNP3 settings for the WI-415. You may find that you can use these default settings for simple applications without further configuration. • Device IP Address—192.168.0.1xx (xx is the last two digits of the serial number). • Master IP Address—Any (the device accepts connections from any IP address) • Connection Mode—TCP Listen (the master initiates the connection) • DNP3 TCP Port— 20000 • Device DNP3 Addr—4 (outstation) • Master DNP3 Addr—3 For most systems, you will only need to enable the DNP3 outstation function and set the outstation DNP3 address and connection type. To access DNP3 configuration, click DNP3 in the WI-Config project tree to display the screen in “DNP3 address configuration”.

Advanced port settings

DNP3 protocol typically uses TCP and UDP port number 20000 for all communications. You may need configure nonstandard port numbers to match the requirements of your system.

To configure DNP3 ports, click DNP3 in the project tree and then click the Advanced tab.

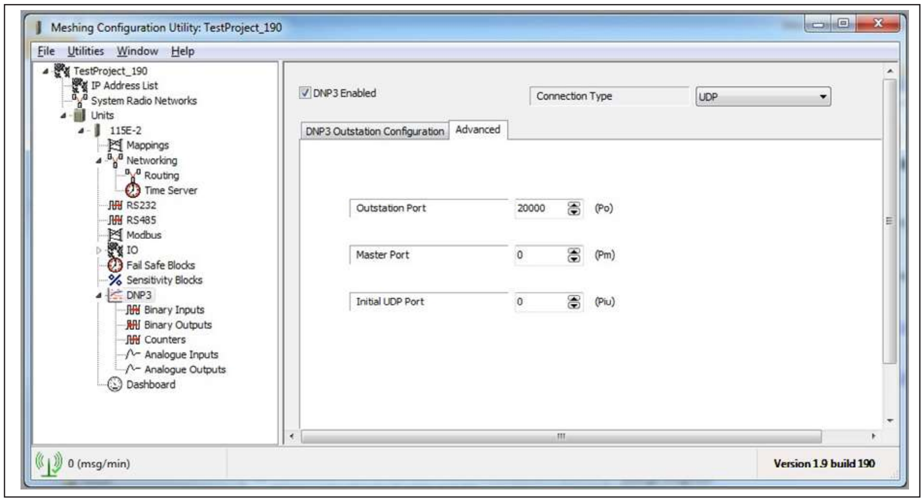


Figure 67. DNP3 advanced port settings

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.
Master Port	Sets the TCP or UDP port number of the master station. If the Connection Type is set to UDP or TCP Dual, you need to set this value to the port number that the DNP3 master uses to receive incoming connections. This parameter is not available if the Connection Type is set to TCP Listen.
Initial UDP Port	Sets the UDP port that the remote station uses to send UDP messages to the master station before there is a connection from the master station. This parameter is only available when the Connection Type is set to UDP.

I/O configuration

You can change the way that I/O data is reported by the WI-415 Series 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 WI-415 Series 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 WI-EX Expansion I/O modules to a WI-415 Series device configuration, the I/O of the WI-EX device are automatically added to the DNP3 I/O list. You can add WI-EX expansion I/O devices by clicking IO in the WI-Config project tree. For more information, see “Adding an expansion I/O to WI-Config” on page 27.

Every DNP3 I/O needs to be configured with a polling class and register number:

- **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.
- **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

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 WI-415 Series memory map in the range 10001–19999. Discrete outputs are in the WI-415 Series 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 in the project tree.

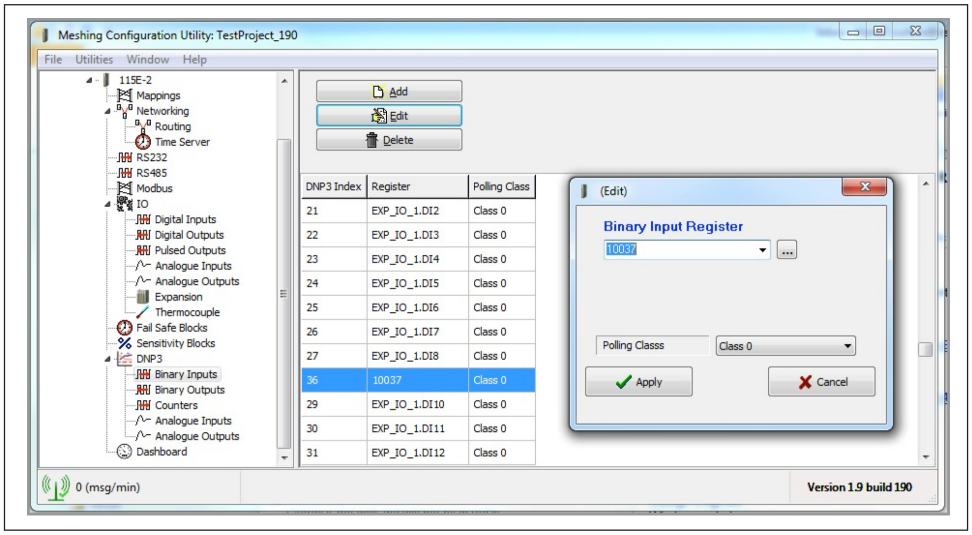


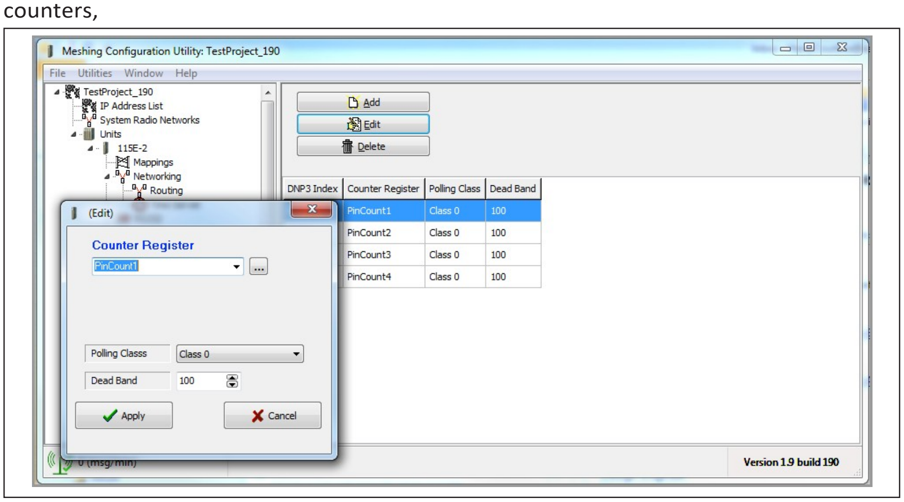
Figure 68. Binary inputs and binary outputs

DNP3 Index	This is the DNP3 point index used to access the I/O data from the DNP3 master device.
Register	The I/O point register in the WI-415 Series device. For a detailed description, see "I/O configuration" on **page 40**. Select the register by name from the drop-down menu in the Edit dialog box, or click the ... button to list all registers by number.
Polling Class	See "I/O configuration" on **page 40**.

Counter inputs

Counter inputs appear in the WI-415 Series 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 option under **DNP3** in the project tree



.

Figure 69. DNP3 counters

DNP3 Index	This is the DNP3 point index used to access the I/O data from the DNP3 master device.
Counter Register	The I/O point register in the WI-415 Series device. For a detailed description, see "I/O configuration" on **page 40**. Select the register by name from the drop-down menu in the Edit dialog box, or click the ... button to list all registers by number.
Polling Class	See "I/O configuration" on **page 40**.
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.

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.

To configure how a DNP3 variable is scaled, you can select from a list of commonly used scaling values or configure your own custom scaling by entering two reference points. A graph provides feedback on the configured scaling and the configured dead band (see **Figure 70**).

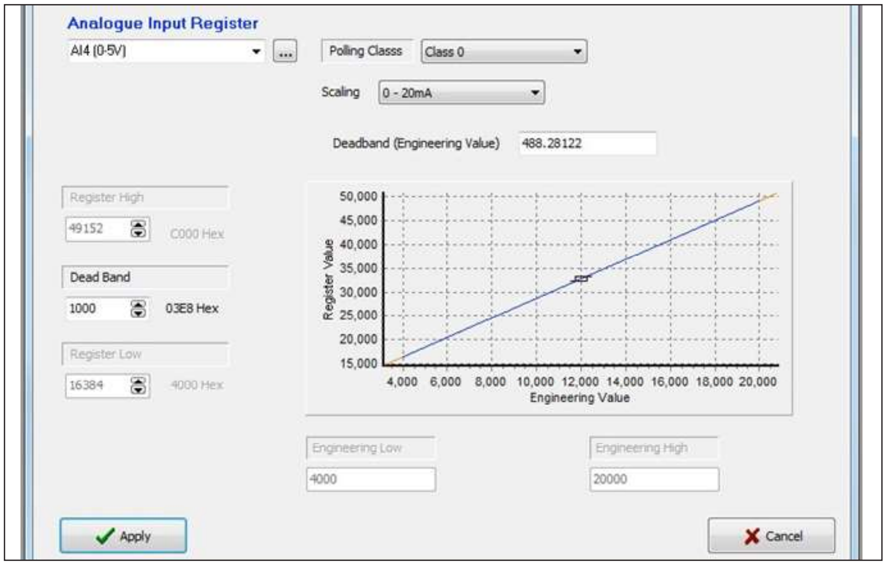


Figure 70. DNP3 analog inputs

Analog Input Register — The I/O point register in the WI-415 Series device. For a detailed description, see "I/O configuration" on **page 40**. Select the register by name from the drop-down menu in the Edit dialog box, or click the [...] button to list all registers by number.

Polling Class — See "I/O configuration" on **page 40**.

Scaling — Select automatic scaling to match the available input types or select custom scaling if you want to report data in your system engineering values.

0–20 mA—Use this scaling to report the value from a 0–20 mA analog input such as analog inputs 1–4 in current mode. The value is reported in microamps (20 mA reports in DNP3 as 20,000 µA).

0–5 V—Use this scaling to report the value from a 0–5 V analog input such as analog inputs 3 and 4 when used in voltage mode. The value is reported in millivolts (5 V reports in DNP3 as 5,000 mV).

0–20 V—Use this scaling to report the value from a 0–20 V analog input such as analog inputs 1 and 2 used in voltage mode. The value is reported in millivolts (5 V reports in DNP3 as 5,000 mV).

0–40 V—Use this scaling to report a value from a supply voltage input, such as battery voltage or supply voltage. The value is reported in millivolts (24 V reports in DNP3 as 24,000 mV)

⚠ **Note**: When reading this value as a DNP3 integer value, it will not measure voltages above 32.768 V since the integer value is limited to a maximum of 32768.

0–100 Hz—Use this scaling for pulse rate inputs configured for full-scaled to 100 Hz.

No Scaling—Use this option when you want DNP3 to report the raw register value without any scaling.

Custom—Use this option to apply custom scaling. Select the scaling option closest to the desired scaling, then select Custom, and enter values for Register High, Register Low, Engineering High, and Engineering Low fields described below.

⚠ **Note**: If you change the device's analog input scaling using the I/O option in the project tree, it will affect the scaling of DNP3 analog input points. The DNP3 values are derived by applying this scaling to the register values after they are scaled by the device's analog scaling. For more information on analog input scaling, see "Analog inputs" on **page 26**.

Dead Band — The dead-band value for the analog input, expressed as a desired change in the register value. 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.

Dead Band (Engineering Value) — 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 Low — 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 High — The register value for the second reference point.

Engineering Low — 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 High — The desired DNP3 value for the second reference point.

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. A graph provides feedback to show the configured scaling (**see Figure 71**). 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.

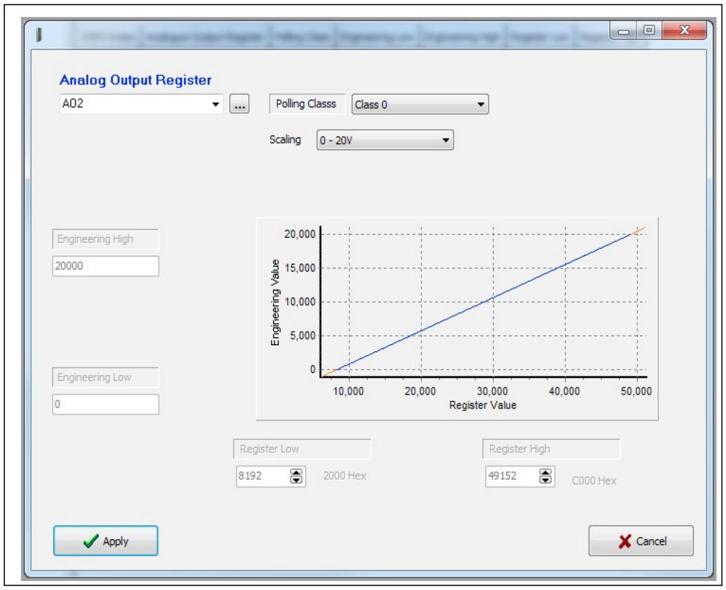


Figure 71. DNP3 analog outputs

Analog Output Register	The I/O point register in the 415U device. For a detailed description, see “I/O configuration” on page 40. Select the register by name from the drop-down menu in the Edit dialog box or click the ... button to list all registers by number.
Polling Class	See “I/O configuration” on page 40.
Scaling	Select automatic scaling to match the available output types, or select custom scaling if you want to report data in your system engineering values. **0–20 mA**—Use this scaling to send the value from a 0–20 mA analog output such as analog outputs 1 and 2. The value is set in microamps. Set the DNP3 register to 20,000 in order to set the output to 20 mA (or 20,000 µA). **0–5 V**—Use this scaling to report the value from a 0–5 V analog input such as analog Inputs on 115S-13 configured for 0–5 V mode. **No Scaling**—Use this option when you want to write the raw register value from the DNP3 master without any scaling. **Custom**—Use this option to apply custom scaling. Select the scaling option closest to the desired scaling, then select Custom, and enter values for the Register High, Register Low, Engineering High, and Engineering Low fields described below.
Engineering Low	The DNP3 value for the first reference point. When this value is written by the DNP3 master, the 415U register receives the value in Register Low.
Engineering High	The DNP3 value for the second reference point. When this value is written by the DNP3 master, the 415U register receives the value in Register High.
Register Low	The register value set in the 415U for the first reference point. The 415U memory register receives this value when the DNP3 master writes the value listed in Engineering Low.
Register High	The register value for the second reference point, corresponding to the DNP3 value in Engineering High.

Configuring using the web configuration utility

Connecting to the embedded web configuration

An alternative to the WI-Config configuration application is to access the device embedded configuration webpages directly using a web browser such as Internet Explorer® or Chrome.

On first connection, you must connect to the device through its USB port. Once you have configured the device for the first time, you can enable access through the Ethernet port and remotely through the Wireless port.

⚠ **Note**: Before enabling the Ethernet Port or Wireless port for Configuration access, read the section “Secure hardening guidelines” on **page 79**.

Connecting to the device’s USB port

The USB port is located on the bottom side of the module. (Refer **Figure 11** “Bottom panel connections”). To connect, you need an USB cable (USB-A to USB-B) for connecting from your computer to the module’s USB-B port .

If you plan to use the web-based management, and this is the first time you have used your computer to connect to an WEIDMULLER device through the USB port, then you will need to download the
USB driver file from the product’s internet website. This is available from the same location that you downloaded this user manual. The filename is “Inst_Weidmuller_USB_Driver_1.21.0.0”.

You will also need to know the credentials (username and password) configured for the device. If the module is new out-of-the-box you can use the default credentials. Otherwise, you will need to use the values set previously. If you have lost the password, you can clear the device to set the username and password back to the default values. For instructions, see “Restoring the factory default settings” on **page 68**.

1. Install the USB driver by double-clicking the file “Inst_Weidmuller_ USB_Driver_1.21.0.0” which you downloaded from the Weidmuller website.
2. Power on the device, and wait for the device to finish booting and for the “PWR” LED to go on solid (about 1 minute).

   ⚠ **Note**: From the factory, the PWR LED will turn solid RED at the end of the boot sequence. Once you have set the device Locale, the PWR LED will come on GREEN.
3. Plug in the USB cable and wait for your computer to recognize the new USB device. The new device will identify as a “WI-415 Series”.
4. Once the driver is installed, you will have an additional Network Adapter in your device manager list “Weidmuller WI-IO-415-U2 USB Ethernet/ RNDIS Interface”
5. Open your web browser (recommended Internet Explorer version 10 or later) and type “http://192.168.111.1” into the browser bar. The device’s USB address is always the same. The module responds with a username and password box.
6. Type the username and password. The default username is “user” and the default password is “user”.

This connects you to the home page of the Web-based configuration utility (see **Figure 69**). This utility allows you to manage wireless connection links between all modules in the system through a standard browser, such as Microsoft® Internet Explorer®.

Connecting to the Device’s Ethernet port

The Ethernet port is located on the bottom side of the module. (Refer **Figure 11** “Bottom Panel Connections”). To connect, you need an Ethernet cable for connecting to the module’s Ethernet port. You also need to know the device’s IP Address and the username / password configured for the device.

The module’s default settings are as follows:

IP Address: 192.168.0.1XX
(shown on the printed label on the side of the module)

- Subnet Mask: 255.255.255.0
- User Name: user
- Password: user

If the module is not new out-of-the-box and does not have the default settings, you may need to restore these settings. If you have lost the current device settings, you can set the IP address and password back to the default values. For instructions, see “Restoring the factory default settings” on **page 68**.

Once you have the device’s IP address and password:

1. Connect an Ethernet cable between the module’s Ethernet port and the PC.
2. Configure your PC networking settings to be on the same network as the device. For instructions on how to do this, see “Configuring PC networking settings” on **page 68**.
3. Open your web browser (recommended Internet Explorer version 10 or later) and type “http://” followed by the IP address of the module and press Enter.
   The module responds with a username and password box.
   If the module does not respond, the PC networking setting may be incorrect. For more information, see “Configuring PC networking settings” on **page 68**.
4. Type the username and password. The default username is “user” and the default password is “user”.

This connects you to the home page of the Web-based configuration utility (see Figure 1). This utility allows you to manage wireless connection links between all modules in the system through a standard browser, such as Microsoft® Internet Explorer®.

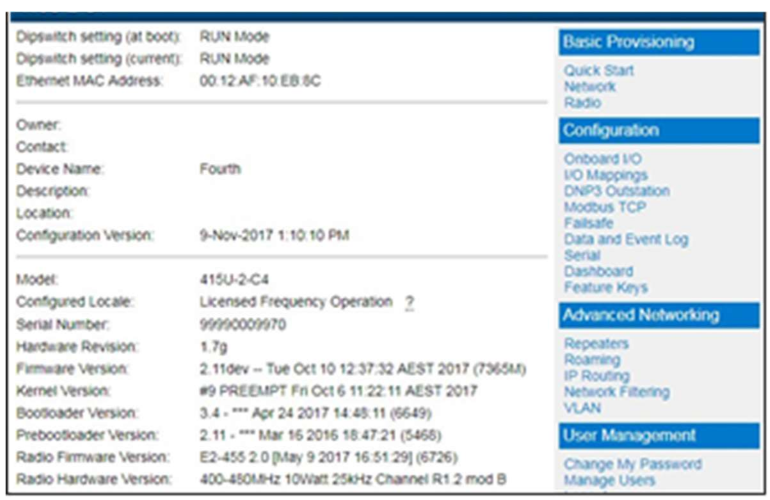


Figure 72. Device home page

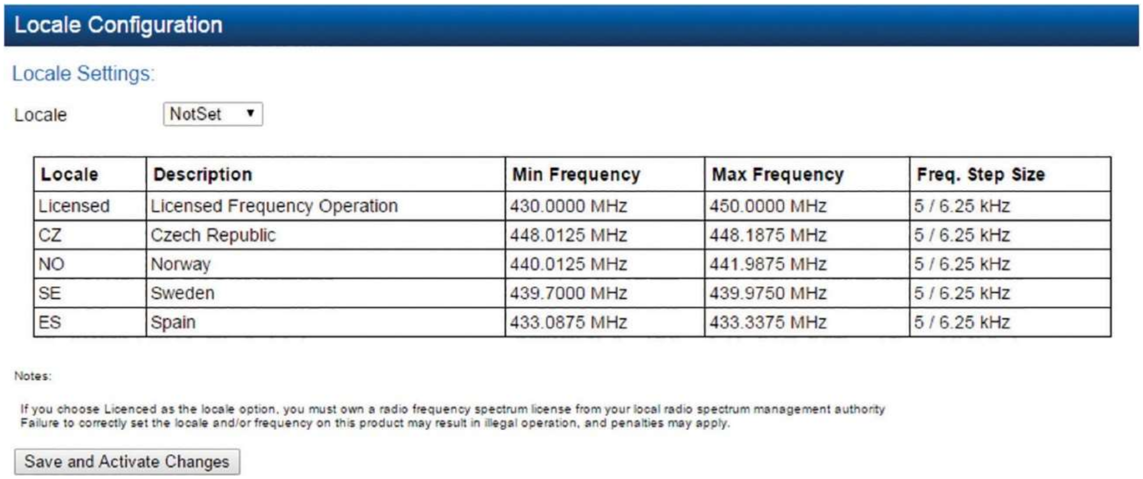
Configuring the locale

When the WI-415 Series module is shipped from the factory, the radio is not configured. At power-up, the OK LED will glow RED to indicate that the device is not configured. The radio will not send any transmissions until the initial provisioning has 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.

The Locale only needs to be set when the device is first configured from the factory. The Quick Start screen is available at any time to change the device's radio configuration.

Connect to the device using USB connection. See "Connecting to the device's USB port" on page 44 for instructions to connect to the module.



Locale	Description	Min Frequency	Max Frequency	Freq. Step Size
Licensed	Licensed Frequency Operation	430.0000 MHz	450.0000 MHz	5 / 6.25 kHz
CZ	Czech Republic	448.0125 MHz	448.1875 MHz	5 / 6.25 kHz
NO	Norway	440.0125 MHz	441.9875 MHz	5 / 6.25 kHz
SE	Sweden	439.7000 MHz	439.9750 MHz	5 / 6.25 kHz
ES	Spain	433.0875 MHz	433.3375 MHz	5 / 6.25 kHz

Figure 73. Locale configuration

The available options for the device's operating locale on this screen will depend on the exact radio device you have chosen. Different devices support radio operation on different unlicensed bands. Refer to the appendix for a list of supported Locales for each radio type.

If you intend to use the device in unlicensed operating mode, select the appropriate Locale name from the table (e.g. one of CZ, NO, SE, ES in the example above).

⚠ WARNING

USE OF UNLICENSED BANDS IS LIMITED TO THE LISTED PHYSICAL LOCALES ONLY. ENSURE YOU SELECT A LOCALE THAT IS ALLOWED BY THE RADIO REGULATORY AUTHORITY IN YOUR TARGET LOCATION.

If you intend to use the device in Licensed operating mode, select the "Licensed" Locale. This gives access to the full radio band available to the module.

⚠ WARNING

WHEN YOU SELECT "LICENSED" LOCALE, YOU MUST HAVE A RADIO LICENSE FROM THE RADIO REGULATORY AUTHORITY IN YOUR LOCATION. THIS LICENSE WILL BE FOR A SINGLE FREQUENCY OR A RANGE OF FREQUENCIES. ENSURE THE RADIO IS CONFIGURED FOR A PROPERLY LICENSED FREQUENCY (REFER FOLLOWING SECTION) BEFORE TRANSMITTING.

⚠ **Note**: Once the Locale is set this screen will not be displayed again. To set the device to a new locale, you must perform a Factory Default Configuration (Available under the System Tools menu item).

Once you have completed the Locale configuration, press the "Save and Activate Changes" button to progress to the next stage. You will be taken to the Quick Start page. You need to configure the items on the quick-start page before the radio will operate.

Quick start—basic device configuration

This page allows you to configure everything required to setup basic radio communication with the device. You can return to this configuration page at any time by selecting “Quick Start” from the device’s main menu.

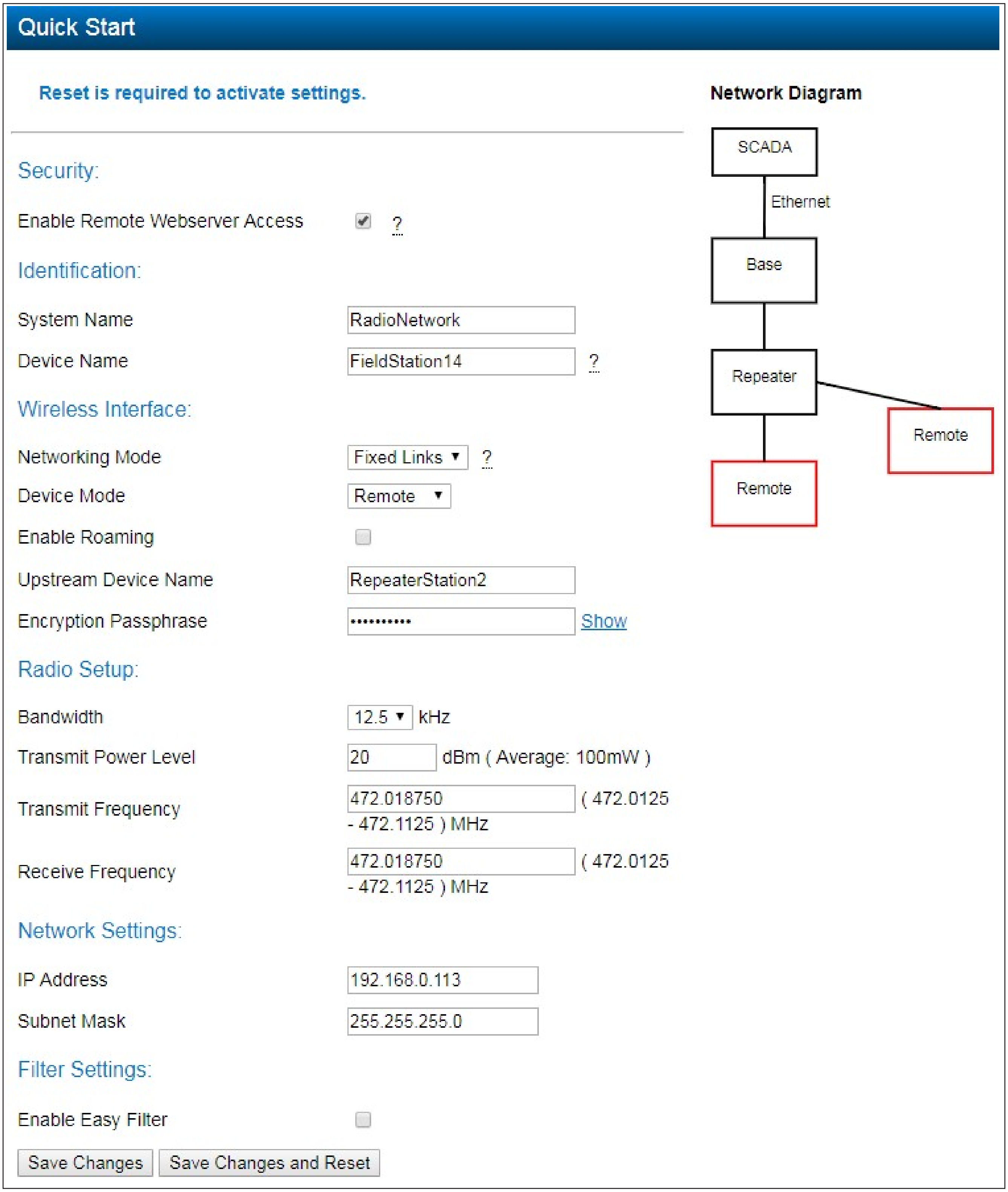
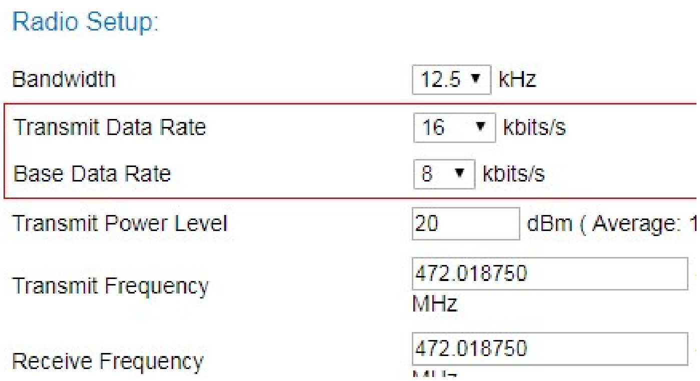


Figure 74. Quick start configuration

These items configure the device’s networking setup. Values that you enter here determine how devices will connect and communicate through the network.

Quick Start Additional Items

If you make changes to configuration items on other configuration pages, these may appear on the Quick Start page surrounded b y 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 Configuration page. These are shown on the Quick Start page as a reminder that they are not set to default values.



Security

Enable Remote Webserver Access	Check this box to enable 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: Read the security sections in this manual before enabling remote access.

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.

Wireless Interface

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 adaptable mesh Manual - Full Manual configuration of topology ⚠ Note: Configuring Manual networking mode requires understanding of 802.11 networking concepts. For the majority of applications, you will select one of the other operating modes
Device Name: (Fixed Links)	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.
Promesh Mode	ProMesh devices are either a Base or a MeshNode. These correspond to the roles in the image on the right of the screen
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 (Fixed Links)	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 .
Upstream Device Name: (Fixed Links)	This option configures networking when the Device Mode is set to "Repeater" or to "Remote". This selects how the device will connect to the network. The Upstream device name is the name of the device closer to the Base. For devices that will connect directly to the Base, the upstream device name is the name for the Base station. For devices that connect to a repeater, the upstream device name is the name for that repeater station.
802.11 Mode: (Manual)	(Manual Device Mode Only) This option configures additional networking when the device mode is set to "Manual". Select "Access Point" for a central 802.11 Access Point, or "Client (Station)" for a remote.
System Address: (Manual)	This option configures additional networking when the device mode is set to "Manual". Client stations will attempt to connect to an Access Point with matching ESSID/System Address.

Radio Setup

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

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.
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
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.

Network settings

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

IP Address — This is the IP address you use to access the WI-415 Series device. This IP address is part of the same sub-net as the Ethernet network.

⚠ **Note**: The WI-415 Series 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.

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.

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 WI-415 Series 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.

IP filter settings

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

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.

Default Back-To-Back gather scatter mapping

The WI-IO-415-U2 and WI-MOD-415 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 WI-EX-12 and WI-EX-13 expansion modules to your Base and Remote sites to increase the number of I/O. When you do this, you must configure the WI-EX-12 with address 01 and the WI-EX-13 with address 02. You set the address using the rotary switches on the bottom panel of the WI-EX module. Refer to section "Adding expansion I/O modules" on page 23 for instructions on how to connect WI-EX modules.

Note: You don't need to connect the WI-EX modules. You can use only the base and remote modules, or just connect one WI-EX-12 module at one end, and one WI-EX-13 at the other end.

Table 5.

Input point (Local)	Output point (Remote)
WI-IO-415-U2	**WI-IO-415-U2**
DI1 – DI4	DO5-DO8
AI1 – AI2 (4-20mA)	AO1-AO2
WI-MOD-415	**WI-MOD-415**
DI1	DO2
Expansion WI-EX-12	**Expansion WI-EX-13**
DI1 – DI6	DO1 – DO6
AI1 – AI8	AO1 – AO8
Expansion WI-EX-13	**Expansion WI-EX-12**
DI7 – DI8	DO7 – DO8

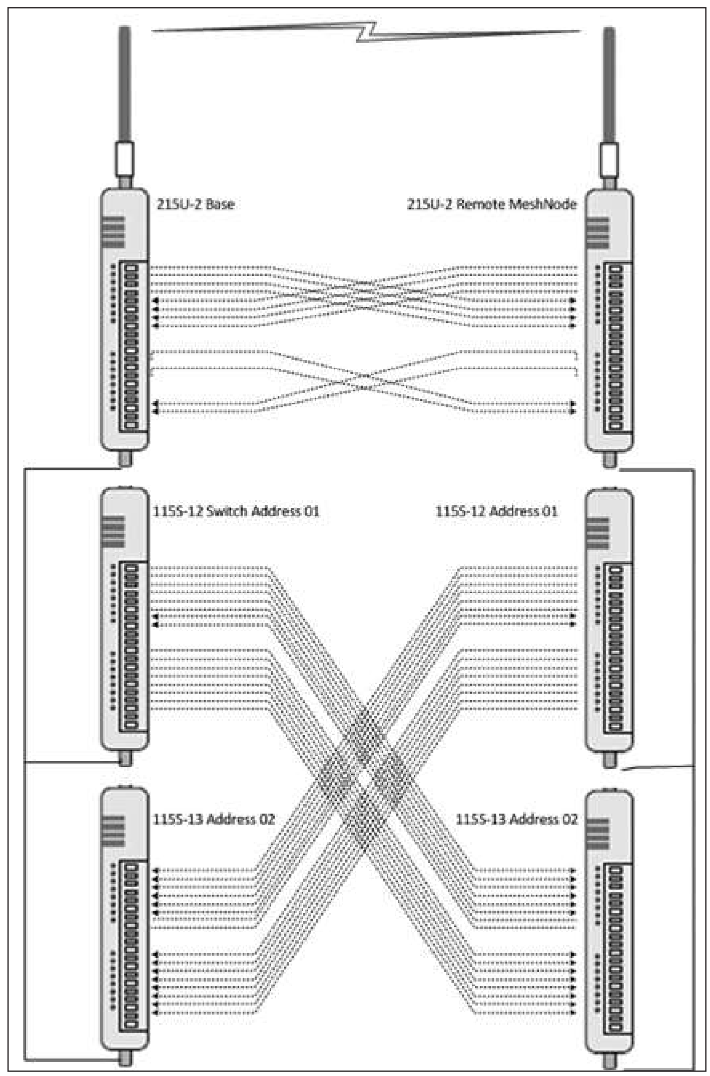


Figure 75. Back to Back mappings - WI-IO-415-U2

Module information web page

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.
Location	Physical location of the module.
Config Version	The date and time when the module was last programmed.

System tools

Click **System Tools** on the menu to perform administrative tasks, such as clearing the system log, reading or writing the module configuration, or performing firmware upgrades.

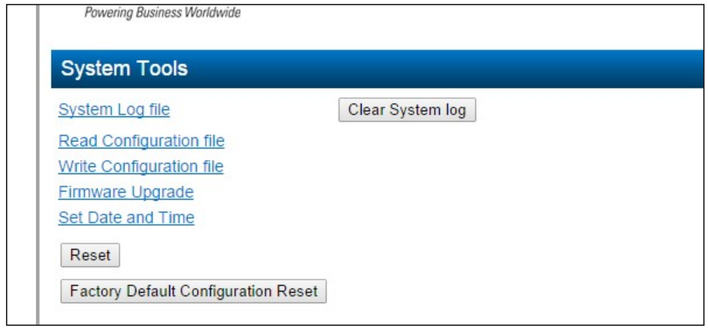


Figure 76. System tools

System Log File	Logs system instructions and other information to the screen. The log screen can then be saved to a file that may be used by WEIDMULLER 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.
Factory Default Configuration Reset	Resets the module and restores its factory default configuration.

Configuration Export

You can export the module configuration to a file for upload to another unit, or for loading into the PC based configuration utility WI-Config. 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.

Select the items you want to save, and click "Download". The configuration file will download to your web-browser, where you can save the file for future use.

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.

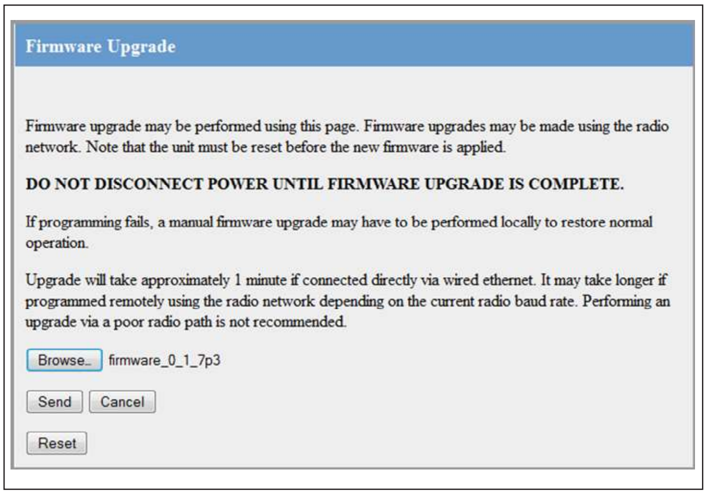


Figure 77. Firmware upgrade

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 (see "Data logging" on **page 62**).

To configure the date and time, click **System Tools** on the menu, and then click **Set Date and Time**. This displays the page in **Figure 7878**. 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) to retrieve the time and date from a remote time server. This method requires network access to an 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.

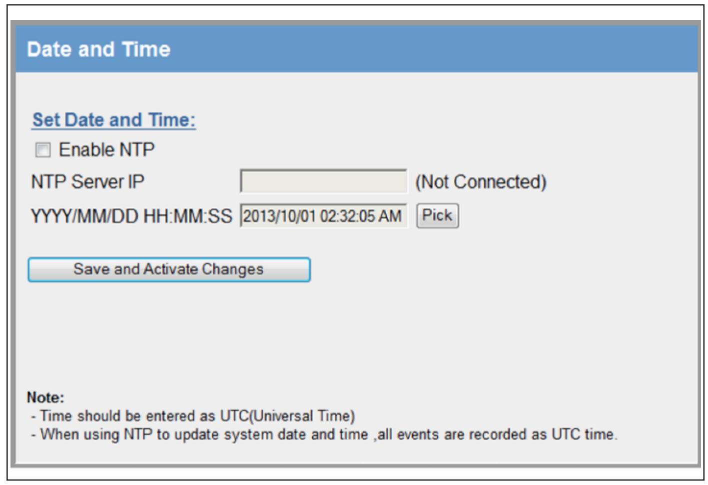


Figure 78. Date and time

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.
YYY/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 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.

Feature license keys

Feature license keys allow you to upgrade the WI-415 Series module with enhanced features or to a more advanced model (for example, by enabling the Modbus option). You can purchase the feature license keys by contacting your sales representative or local distributor. To complete the purchase, you will need to provide the module serial number so that the feature license key can be generated for the module. The module serial number can be found on the home page (see **Figure 72**).

After receiving the feature key certificate, follow the instructions in "Enabling a feature license key" on this page to install the feature on the module. You can also temporarily enable all feature license options by placing the module in demonstration mode. See the following section, "Using demonstration mode."

Click **Feature Keys** in the menu to enable or demo feature license key options (**Figure 80**).

Demonstration Mode	Allows you to temporarily enable all feature license options. See the following section, "Using Demonstration Mode."
Feature License Keys	Allows you to enable advanced features after purchasing a feature license key. See "Enabling a feature license key" on this page.

Using demonstration mode

The demonstration mode option on the Feature License Keys page (**Figure 80**) temporarily allows full operation of all feature license options for 16 hours, or until the module is restarted. This allows you to try out the feature without purchasing the feature key. When the demonstration period is up, the module is restarted and demonstration mode is turned off.

To enable demonstration mode

1. Click **Feature Keys** on the menu.
2. Click to select the **Enable Demonstration Mode** checkbox.
3. Click **Save Changes and Reset**.
4. Wait for the module to complete the restart, and then click **Continue**.
After the module resets, the message "Active" appears, indicating that the demonstration mode is activated.


Certificate

Thank you for purchasing a Feature Code.

Date: 28 April 2015

Module Serial Number: 08141255150

Modbus Feature Code:

Logging Feature Code:

DNP3 Feature Code: 9e2TA7X

Feature Code Certificate

Product functionality can be enabled by providing a code that is specific to the unit and to the feature being enabled (The Feature Code). This certificate provides a record of the feature codes that have been purchased for the product with the serial number listed above.

If these codes were purchased at the time of ordering the module, these features may have already been enabled in the module. In this case the Feature Code will be documented on the module test report. If the codes were purchased subsequent to purchasing the module, refer to the user manual for instructions on how to enable the additional features.

Retain this certificate, as it may be necessary to re-enter the feature codes for this device at some stage in the future.

Figure 79. Example feature key certificate

Enabling a feature license key

Use the following procedure to enable a purchased feature license key (see "Feature license keys" on page 51

To enable a feature license key

1. Make sure that the module serial number on the feature key certificate (**"Example feature key certificate"**) matches the serial number on the label on the left side of the module.
2. Click **Feature Keys** on the menu.
3. Enter the key value from the certificate into the field next to the feature.
4. Click **Save Changes**.
If the feature license key is valid, a green checkmark appears next to the key. If the key is invalid, a red cross appears. Feature license keys are retained even if the module is returned to factory default settings.

Figure 80. Feature license keys

5. If the code is valid, activate the feature by clicking **Save Changes and Reset**.

Changing your 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.

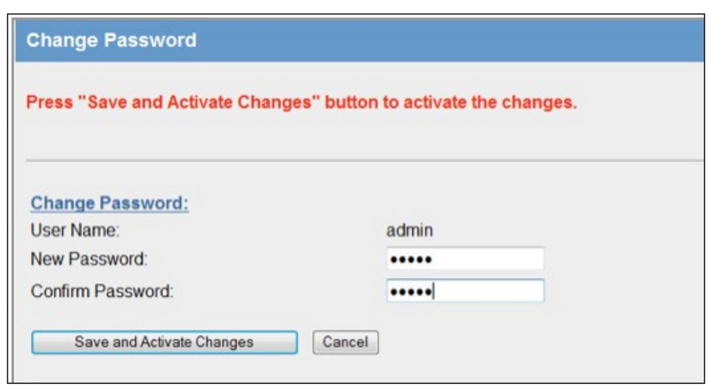


Figure 81. Change password

User management

Users with Admin privileges can click **User Management** on the menu to configure access to the module (see **Figure 82**). 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.

⚠ **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 65**68**.

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.)

The module comes from the factory with two default users.

Table 6. Users

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

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.

Table 7. 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

Figure 82. User management

To add a user

1. Click **User Management** on the menu.
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 Changes**.

To retire a user

1. Click **User Management** on the menu.
2. In the Status column for the user, click **Retire**.
3. Click **OK** to confirm.
   The user's status changes from "Active" to "Retired."
4. Click **Save and Activate Changes**.
   This disables access to the module by the retired user.

To change a user password

1. Click **User Management** on the menu.
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 67**.

Advanced network configuration

This section describes the Advanced features of the WI-415 Series 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 WI-IO-415-U2 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.

Network

This configuration repeats much of the configuration available on the Quick Start page. If a setting appears on both pages, you can set on either page. Additional items that are only on the Network Configuration page will appear on the Quick Start page if they are set away from their default values. Additional items that are not on the Quick Start page are underlined for clarity.

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.

Wireless Interface

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 adaptable mesh Manual - Full Manual configuration of topology ⚠ **Note**: Configuring Manual networking mode requires understanding of 802.11 networking concepts. For the majority of applications, you will select one of the other operating modes
Device Mode: (Fixed Links)	This selects the device operating mode when the networking mode is "Fixed Links". Base, Repeater, or Remote correspond to the roles in the image on the right of the screen. L.
ProMesh Mode	ProMesh devices are either a Base or a MeshNode. These correspond to the roles in the image on the right of the screen
<u>Radio Encryption</u>	Sets the Encryption 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 (Fixed Links)	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 .
Upstream Device Name: (Fixed Links)	This option configures networking when the Device Mode is set to "Repeater" or to "Remote". This selects how the device will connect to the network. The Upstream device name is the name of the device closer to the Base. For devices that will connect directly to the Base, the upstream device name is the name for the Base station. For devices that connect to a repeater, the upstream device name is the name for that repeater station.
802.11 Mode: (Manual)	(Manual Device Mode Only) This option configures additional networking when the device mode is set to "Manual". Select "Access Point" for a central 802.11 Access Point, or "Client (Station)" for a remote.
System Address: (Manual)	This option configures additional networking when the device mode is set to "Manual". Client stations will attempt to connect to an Access Point with matching ESSID/System Address.

Network Mode

This 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.

<u>Network Mode</u>	The WI-415 Series can act as a bridge or as a routoer between the radio and Ethernet ports. Bridge: Data packets are transparently passed between the radio and Ethernet ports using rules learned from traffic that has already passed. Router: Only IP packets are passed between the radio and Ethernet, which are on separate sub-networks. You configure the rules for which packets are transferred on the routing configuration page.
<u>Bridge STP</u>	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.

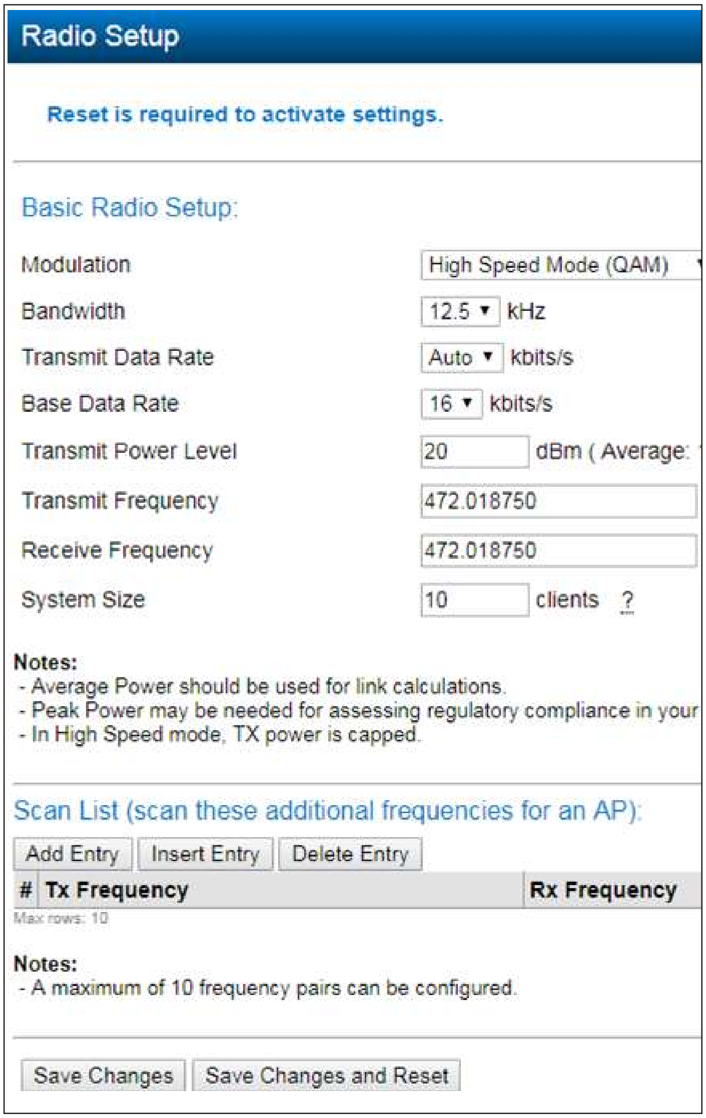
IP Address/Subnet Mask: When the network mode is set to Bridge, the Ethernet and Wireless interfaces are bridged together, and the device has a single IP Address accessible from either interface.

<u>Ethernet IP Address/Netmask</u>: When the network mode is set to Router, the Ethernet and Wireless interfaces on the device each have separate IP addresses. This sets the IP address for the Ethernet interface.

<u>Wireless IP Address/Netmask</u>: When the network mode is set to Router, the Ethernet and Wireless interfaces on the device each have separate IP addresses. This sets the IP address for the wireless interface.

Radio

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



<u>Modulation</u>

Select the Modulation format.

Legacy mode provides compatibility with existing networks of WI-IO-415-U2-H and WI-IO-415-U2-L devices using Frequency Shift Keying modulation (FSK).

High Speed mode provides 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 have 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..

<u>Base Data Rate</u>

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 higher 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**: 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

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.

<u>System Size</u>

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

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.

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.

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	his 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.

Compression and Statistics Settings

Data Compression	Compress data as it is transferred over the radio channel.
Enable Radio Statistics	Make radio statistics available in the on-board registers (30421-30490).

Roaming Settings

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

Roam Scan Thresold	The radio won't start looking for alternative upstream device until the RSSI reaches this level
Roam Changeover Margin.	The 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 network 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.

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	The Interval for TCP SYN Requests. 0 to disable TCP SYN rate-limit. Typical 10 sec
TCP SYN 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 tat 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).

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.

he WI-415 Series 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.

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 215U-2 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 215U-2 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.

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 38.

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.

IPWhitelist 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 Filter 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.

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

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 Minimum/ Maximum	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 is 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.

VLAN Configuration

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.

VLAN Mode	To disable VLAN functionality, select mode "VLAN Passthrough". To enable the VLAN, select mode "VLAN Aware". 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 39.

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.

Interface Membership for VLAN: This allows you to set which interfaces are part of the VLAN. The 215U-2 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).

Table 8.

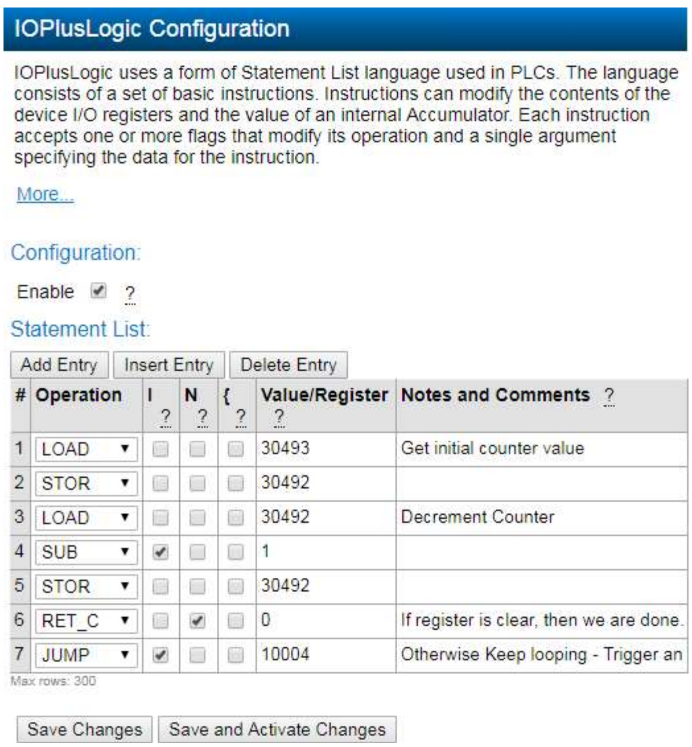
Type	Ingress behavior	Egress behavior
Tagged	Packet is only accepted if it's VLAN ID matches the configured ID for this VLAN.	Packet is transmitted as a VLAN packet with the configured VLAN ID
Untagged	All non-VLAN packets are received into the VLAN.	Packet is transmitted as a non-VLAN packet.

Logic Configuration

The WI-415 Series modules support a simple programming language to allow you to control the I/O registers on the device. This allows you to perform simple control actions, such a setting an output depending on the state of several inputs, generating a on-off “heartbeat” signal, or calculating total flow volume by accumulating a flow rate.

To configure, you enter a list of instructions for the Logic Engine to execute. Each instruction can read or write an I/O register, can perform an mathematical or logical operation, make a comparison, or perform a branch to another instruction line.

This list is executed every 250milli-seconds (four times per second).



IOPlusLogic Configuration

IOPlusLogic uses a form of Statement List language used in PLCs. The language consists of a set of basic instructions. Instructions can modify the contents of the device I/O registers and the value of an internal Accumulator. Each instruction accepts one or more flags that modify its operation and a single argument specifying the data for the instruction.

More...

Configuration:

Enable ☑ ?

Statement List:

Add Entry | Insert Entry | Delete Entry

#	Operation	I ?	N ?	{ ?	Value/Register ?	Notes and Comments ?
1	LOAD	☐	☐	☐	30493	Get initial counter value
2	STOR	☐	☐	☐	30492	
3	LOAD	☐	☐	☐	30492	Decrement Counter
4	SUB	☑	☐	☐	1	
5	STOR	☐	☐	☐	30492	
6	RET_C	☐	☑	☐	0	If register is clear, then we are done.
7	JUMP	☑	☐	☐	10004	Otherwise Keep looping - Trigger an

Max rows: 300

Save Changes | Save and Activate Changes

Figure 83. IO Plus Configuration

You configure the Logic functionality as a list of operations to perform in the table “Statement List”.

Use the “Add Entry” to append a new line to the table. Use “Insert entry” to insert an line into the table at the current position, and use “Delete Entry” to delete the current line of the table.

Toe enable the logic operation, ensure that “Enable” is checked, and click the “Save and Activate Changes” button. After making changes, you can use the “Save and Activate Changes” button to quickly test the operation.

Statement List Execution and Timing

The device executes a software process that reads and performs the actions programmed in the statement list. The statements in the list are executed by this process in the defined order until the end of the list is reached. The logic process then waits until it is time to begin the next execution cycle, and again executes the statements in the list. This execution cycle is repeated again and again while the device is operating.

The statement list can include branch instructions which cause the control flow to follow a different path, so every statement in the list will not necessarily be executed on each execution cycle. It is also possible to develop looping constructs within the statement list, so a group of instructions could be executed multiple times during one execution cycle. Care must be taken to ensure that any loops will terminate in time so that the execution of the Statement list will not exceed the maximum allowed cycle time.

The Logic engine aims to execute the full statement list once every 0.25 Sec. This is the cycle time. Each execution of the statement list has a deadline that is 1.25 seconds after the target completion time. If the execution cycle does not complete before the deadline, the execution of the remaining statements in the cycle is aborted. When this happens, the Diagnostic register is set to the value 32768. This means that you can rely on timers being no more than 1.25 second late as long as the Diagnostic register doesn’t indicate overrun. The Logic engine is designed to be capable of executing up to 1000 instructions without exceeding the deadline.

If the list does not complete in time (overrun), then the Logic engine aborts the current execution, and flags the overrun condition in the Logic engine status register (register 30491)

Register 30491 Value	Meaning
0	Logic engine is Stopped
256	Logic engine is running
32768	Logic engine has overrun

Click the “More” link on the device webpage, or refer to the appendix in this manual for a more detailed description of the available operations.

Statement List Overview

Operations

There are a number of configurable operations and each one will perform a specific task, whether it be loading a value, storing a value, applying a logical or mathematical operation or applying some other operational instruction, i.e. Jumping , setting or calling.

“I” (Immediate)

When selected the instruction will use the actual value that is entered into the “Value/Register” column. When de-selected, it will use the value as the register location to use as the argument.

When selected for JUMP and CALL instructions, the instruction uses the value entered as an offset from the current line number, rather than the absolute line number to transfer to.

“N” (Negate)

When selected this allows the argument to be negated (opposite) before it is used by the instruction. i.e.

“{“ (Delayed Calculation)

Allows you to evaluate the argument to a statement using multiple calculation steps. You can have up to 20 levels of nesting sub-blocks to perform a calculation..

Value /Register

The value or register location that will be used by the operation.

Notes and comments

Notes or comments that help to explain the logic operation and configuration

Diagnostics

This chapter describes network diagnostic tools and information available from the module's Web-based configuration utility.
To access this utility, see "Connecting to the embedded web configuration" on page 44.

IO diagnostics

Click **IO Diagnostics** from the home page of the Web-based configuration utility to read and write I/O store registers within the module.

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 84**). 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 outputs 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 it's 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 or use the WI-Config utility (see "Fail-safe blocks" on **page 28**). If there is a mapping configured and any one of the source register values has the value "~" the mapping will not be sent (see "Invalid register state" on **page 29**).

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.

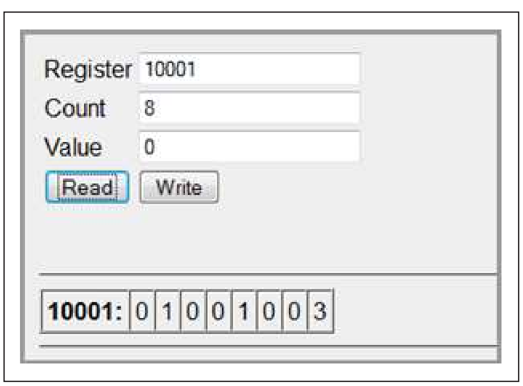


Figure 84. I/O diagnostics

Register	Register address location.
Count	Number of consecutive registers, starting from the 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**.

Watchdog error log

The module uses a various processes to control aspects of its internal functions, such as radio operation, I/O functionality, Ad hoc On-Demand Distance Vector (AODV) communications, and Modbus communications. Each process runs independently, and can interact with the other processes to provide a robust wireless I/O product.

All processes are monitored by an internal "watchdog." If a processes has a problem and stops running, the watchdog will identify the problem and restart the module. The watchdog also creates a text file showing which process had the problem. This text file is stored in a directory called "dog" off the main root IP address of the module. To display this text file in your browser, enter http://<module IP Address>/dog/,

If the watchdog directory continues to show text files, it may indicate a problem with the module or its configuration. If this happens, save the module configuration (see "System tools" on page 49) and the list of watchdog files, and then contact Weidmuller technical support.

The following table describes the different watchdog processes.

Table 9. Watchdog process

Watchdog process	
A00	Internal process monitor
A01	I/O processing application
A02	Fail-safe manager application
A03	Modbus application
A04	I/O mapping application
A06	AODV meshing protocol application
A07	Data logging application
A15	Warm restart backup

Module information registers

Certain registers in the module show modules characteristics, such as the serial number, firmware version, and so on. This information is available on the home page of the module's Web-based configuration utility. However, having the information available in registers allows a host system to read the values via Modbus, if Modbus has been activated.

- Register 30494, 30495 and 30496 = Module serial number
- Register 30497, 30498 and 30499 = Module firmware version
- Register 30500 = Firmware patch level

Expansion I/O error registers

The WI-415 Series has diagnostics registers allocated for each expansion I/O module. These registers indicate the module type, error counts,
error codes, and so on. Each expansion I/O module has the following registers.

- 30017 + Offset = Modbus error counter (number of errors the modules has had)
- 30018 + Offset = Last WI-EX status code / Modbus error code Register 30018 will display one of the following WI-EX status codes (hexadecimal code 0001–0005 and 0081). In the case of a communications fault, the register will contain the Modbus error code as listed in the section “Modbus Error Codes” on **page 78**.

Table 10. Expansion I/O error registers

Dec code	Hex code	Name	Meaning
1	0001	No Response	No response from a poll
2	0002	Corrupt/invalid	Corrupt or invalid data
3	0003	CRC Fail	CRC error check does not match the message. Indicates this a different message or possible data corruption.
4	0004	Response did not match request	The response heard was not the correct ID; possibly heard other RS-485 traffic.
5	0005	Message type did not match request	The response heard did not match the requested poll (different command response); possibly heard other RS-485 traffic.
129	0081	Problem accessing local memory	Could not access register location, possibly because the register is not initialized.
	??01-??0B	As per **page 73**	Modbus Error Codes

- 30019 + Offset = Modbus Lost Link Counter (number of Communication Errors)
- 30020 + Offset = Modbus Module Type:

  dec 257 (101 hex) indicates a WI-EX-11 dec 513 (201 hex) indicates a WI-EX-12 dec 769 (301 hex) indicates a WI-EX-13

Diagnostic registers—device statistics

Commonly used statistics for diagnostics and system monitoring can be logged to onboard I/O Registers. These registers may then be accessed via an external device using any of the supported I/O transfer protocols (WIB, MODBUS, DNP3). By default, logging of statistics to I/O registers is enabled.

When statistics logging is enabled, the statistics are logged to Analog Input Registers. These are listed in detail in “Input registers (words)” on page 68.

Statistics registers provide the following information about the upstream connection (Towards the base station). If the module is configured as a base, or configured in manual mode without any Client functionality, then these registers will be zero.

RSSI: The signal strength to the upstream device (Repeater or base station)

Connected Time: The amount of time the current upstream connection has been established (in hours)

Generation Count: The number of times the current upstream connection has been established. This value is 1 when the device first connects, then if the link is lost it increments once each time the link is re-established. Note that if both the upstream device and the local device are re-started, the Generation count will reset to 1. If only one device is re-started, then the generation count is designed to be retained.

Upstream IP Address: The address of the Upstream device (Base, Repeater or Manual Mode Access Point).

The following information about the device uptime is available for all devices:

Module Uptime: The amount of time the module has been powered on. You can compare this against the connected time to determine if the module has been losing link.

Channel and radio statistics are available for all devices, and are available averaged over the last minute, last hour, and last 60-hour periods.

Channel Utilization: This is the percentage of time the radio channel has been busy with radio transmissions from any devices within receiving range of this device.

Background Noise: This is the background noise level on the radio channel when the radio is not receiving valid data.

Retried Transmissions: This is the percentage of radio transmissions that were successful, but required at least one re-transmission before they were acknowledged. This statistic does not apply to broadcast transmissions, which are not acknowledged.

Failed Transmissions: This is the percentage of transmissions that were unsuccessful due to not receiving an acknowledgement message to any of the re-transmissions. This statistic does not apply to broadcast transmissions, which are not acknowledged.

Statistics registers also record information about downstream connections. These registers are used by all devices that have downstream connections—Base station, Repeater, and Manual Mode Access Points. For Manual Mode clients, and for Field Station devices, these registers are unused and available as general purpose storage.

RSSI List: This is a block of 255 register locations. For each downstream device, the last byte of the device’s IP address is used to determine which location to store the signal strength. For example, a downstream device with IP Address 192.168.0.199 will have its RSSI stored in I/O register offset 199. If no device is connected with the IP address, the register has the value Zero.

Monitoring communications

Monitor Network communications using WireShark™

The WI-415 Series 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 **Monitor IP Comms** under Network Diagnostics on the right side menu. To start the capture, click "Start".

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.

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.

Click "Monitor Radio Comms" on the right side menu under "Network Diagnostics"

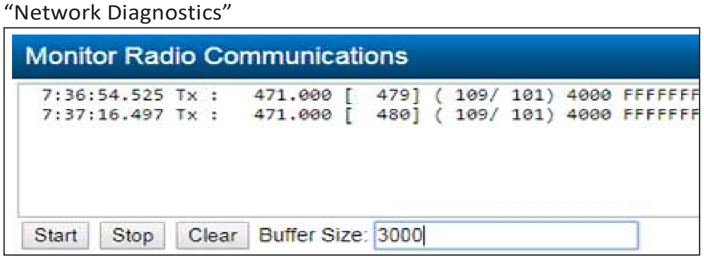


Figure 85. Radio communication monitoring

Use the "Start" and "Stop buttons to start and stop the communication s 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.

Posn	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	Dir'n	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	Freq	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 message Header is received, the Length will indicate the message length. Otherwise it shows zero.
55-66	Dest	Address1 field from 802.11 protocol This is the destination MAC address for the message. FFFFFFFFFFFF for broadcast messages
68-79	Source	Address2 field from 802.11 protocol This is the 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 address 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. WEIDMULLER OUI is 0012AF. The last three bytes of the MAC address will uniquely identify the station.

Data logging

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 WI-415 Series modules with the purchase of a feature key license (see "Feature license keys" on **page 51**).

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 WI-415 Series supports up to 500KByte of data log memory in compressed files.

Configuring data logging

To configure data logging, you need to specify how frequently the data is to be stored, what data is to be stored, and the maximum number of records stored in each log file. Click **Data and Event Log** on the home page of the Web-based configuration utility to configure these settings (see **Figure 86**).

⚠ **Note**: You need Administrator or Manager privileges to configure data and event logging.

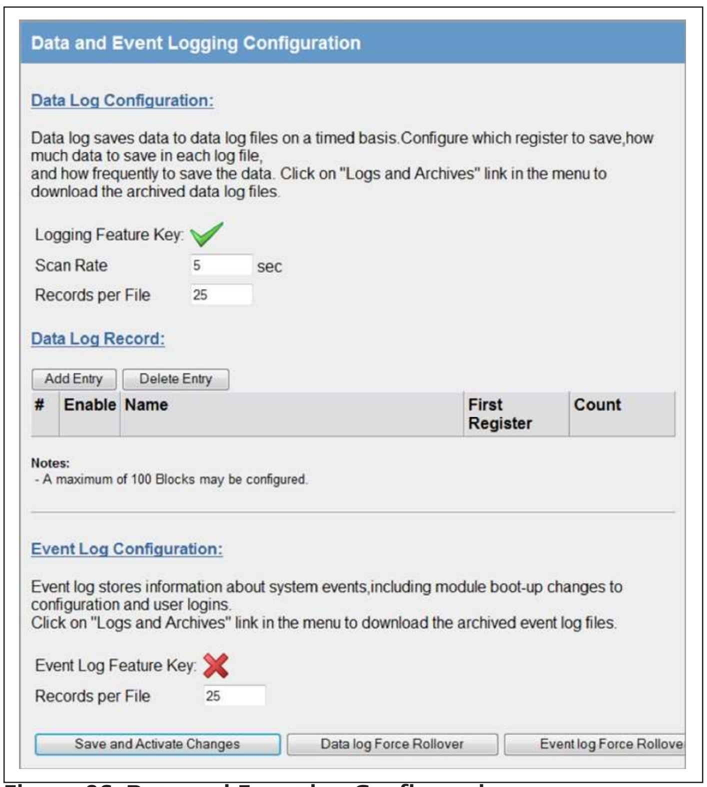


Figure 86. Data and Event log Configuration

Data log configuration

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 a configuration example, see **Figure 87** and **Table 11**.

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 915U-AT (Audit Trail) feature key enabled. Event Logging is discussed in a separate document.

The configuration example in see **Figure 87** will log six registers in each log record. **Table 111** shows an example of the logged data for this configuration.

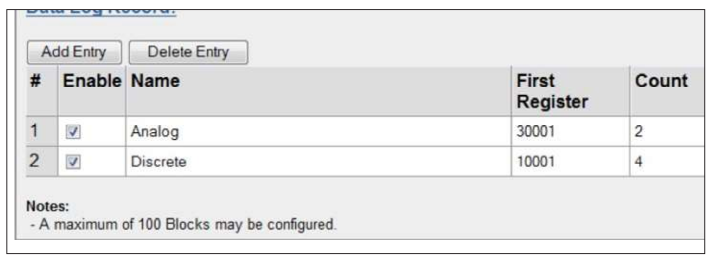


Figure 87. Data log record

Table 11. Data log example

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

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.

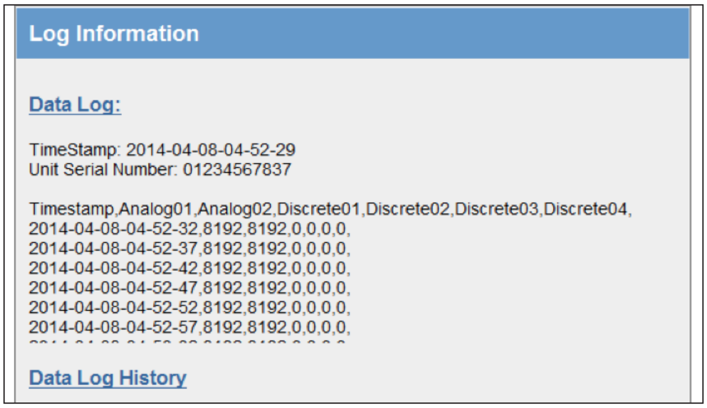


Figure 88. Log information

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 page of the Web-based configuration utility.
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.

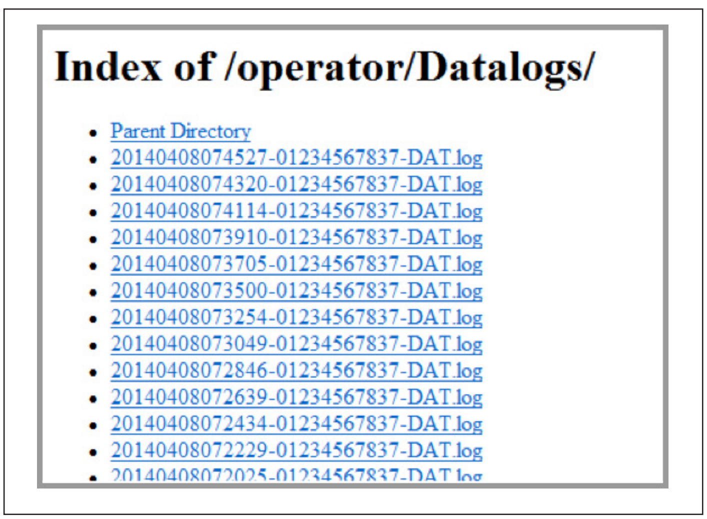


Figure 89. Data log listing

3. Right-click the file 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 900**). 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.

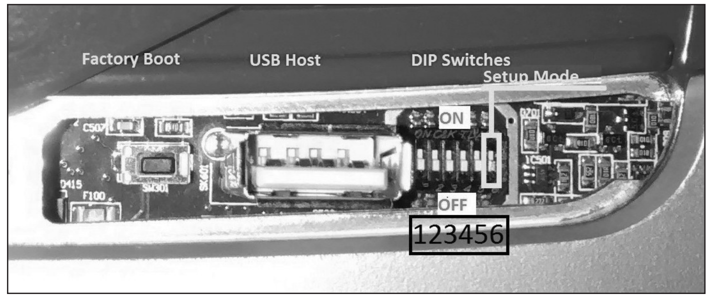


Figure 90. USB port

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.

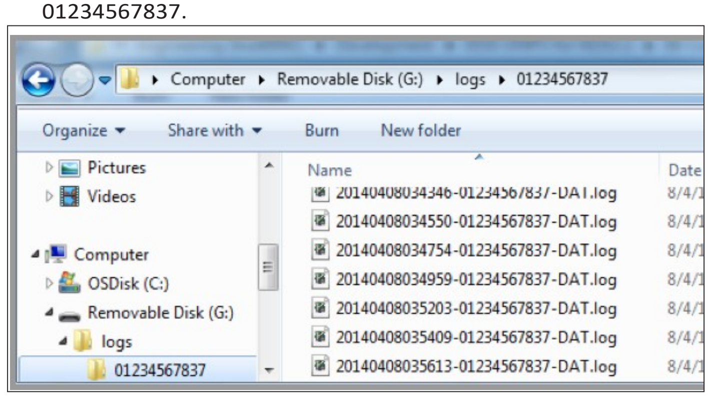


Figure 91. Log file directory on USB drive

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.

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.

Specifications

Table 12. WI-415 Series specifications

Item	Specification (Subject to change)	
Input/output	**WI-IO-415-U2-C**	**WI-MOD-415-E-C**
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 (-C4 Models)	360-400 MHz (-C3 Models)
Transmit Power	Adjustable. 10mW to 10Watt .	Adjustable 10mW to 2Watt (-EX models)
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 and 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 Indication/Diagnostics		
LED Indication	Power/OK; LAN Link/Activity; RS-232; RS-485; Digital I/O; Analog I/O Status (WI-IO-415-U2); Signal strength (WI-MOD-415)	
Reported Diagnostics	Connectivity Information/Statistics, System Log File	
Compliance		
EMC	FCC Part 15, EN 301 489-5, EN 301 489-3, CISPR22	
Hazardous Area (WI-IO-415-U2-C-EX and WI-MOD-415-E-C-EX)	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 in^2 (2.5 mm^2)	
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)	

Troubleshooting

Restoring the factory default settings

Use this procedure to temporarily restore the module's factory default settings.

1. Open the side configuration panel on the module, and set DIP switch #6 to "on."

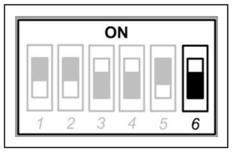


Figure 92. DIP switch #6 in ON position

2. Power cycle the module.
   When the WI-415 Series is powered on with DIP switch #6 set to "on," the module goes into Setup mode and temporarily loads its factory-default settings. In Setup mode, wireless operation is disabled. The previous configuration remains stored in non-volatile memory and will only change if a configuration parameter is modified and the change is saved.

⚠ **Important**: Remember to set DIP switch #6 to "off" and power cycle the module to return to normal operation after you have completed configuration. Otherwise, the module will continue to boot into the default IP address.

Configuring PC networking settings

Use this procedure to configure the PC networking settings needed in order to connect the PC to the module for configuration purposes.

1. On the PC, open the **Control Panel**, and then click **Network Settings**.
   The following description is for Windows XP. Other Windows operating systems have similar settings.
2. Open **Properties** of Local Area Connection.
3. Select **Internet Protocol (TCP/IP)** and click **Properties**.

Figure 93. Local area connection properties

4. On the **General** tab, enter IP address 192.168.0.1 and subnet mask 255.255.255.0, and then click **OK**.

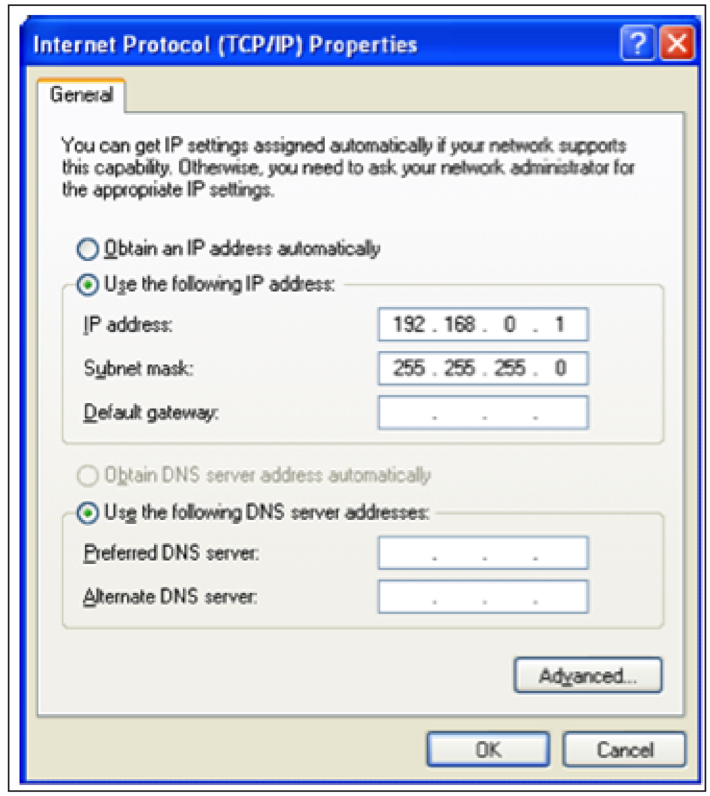


Figure 94. TCP/IP properties

5. Verify the Ethernet connection to the module by using the "ping" command:
   1. From the Windows **Start** menu, choose **Run**, and then type: **command**
      A command prompt DOS window appears.
   2. Type "ping 192.168.0.1XX", where "XX" is the last two digits of the serial number shown on the printed label on the side of the module.

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.

Table 13. Front panel LEDs

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

Additional WI-MOD-415 LEDs

LED	Condition	Meaning
Ƴ ■■■■	Green	Strong signal suitable for 64QAM/4FSK
Ƴ ■■■	Green	Good signal suitable for 16QAM/4FSK
Ƴ ■■	Green	Weak signal suitable for 4QAM/2FSK
Ƴ ■	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

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.

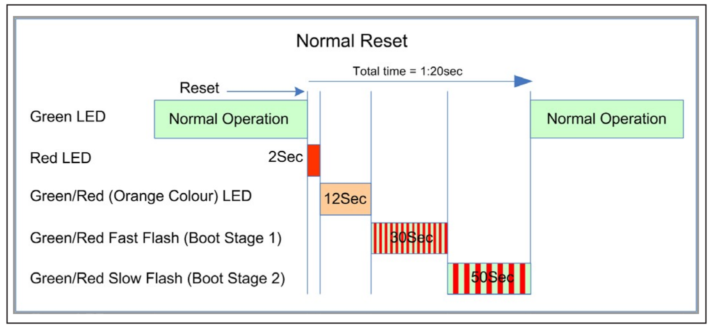
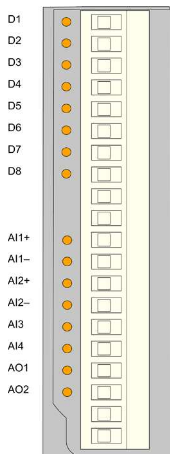


Figure 95. Boot sequence

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

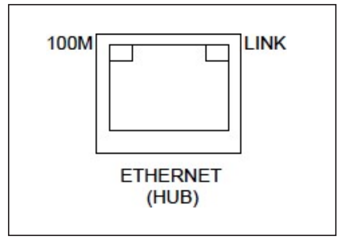


Figure 96. Ethernet socket

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 shown on the Digital Output Configuration page (in WI-Config utility) is on. If an LED is mostly off (long off) it indicates that the fail-safe state shown on the Digital Output Configuration page (in the WI-Config utility) is off. See “Fail-safe blocks” on **page 28** for details.

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 WI-MOD-415, The front panel ETH LED provides additional indication of the Ethernet status. See **page 66**.

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 WI-EX 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 input 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 WI-EX 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

Input registers (words)

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	WI-EX 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 WI-EX 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 WI-EX 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

Expansion I/O registers

Adding expansion I/O modules to the WI-415 Series will automatically add the I/O from the WI-EX modules to the internal WI-415 Series 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 an WI-EX-11 with address 5 would be: (5x20) +10001 = 10101
- Digital output #2 on an WI-EX-11 with address 6 would be: (6x20) +2 = 122
- Analog input #3 on an WI-EX-12 with address 3 would be: (3x20) +30003 = 30063.
- Analog output #8 on an WI-EX-13 with address # 7 would be: (7x20) + 40007 = 40147

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 this WI-EX module
10020 + Offset	Modbus Comms Fail indication (inverse) for this WI-EX module
30001 + Offset 30004 + Offset	WI-EX-11 pulsed input rate 1–4
30005 + Offset 30012+Offset	WI-EX-11 pulsed input count
30017 + Offset	Modbus Error counter for this WI-EX module
30018 + Offset	Modbus Last Error code for this WI-EX module (see "Expansion I/O error registers" on page 60.)
30019 + Offset	Modbus Lost Link counter for this WI-EX module
30020 + Offset	Module type (0x0101) = 257 / error status
40009 + Offset	Pulsed output target 1–8 (1 register per pulsed output)

I/O store for WI-EX-12 expansion I/O modules

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 WI-EX module
10020 + Offset	Detected indication for this WI-EX module
30001 + Offset 30008 + Offset	Inputs AIN 1–AIN 8
30017 + Offset	Modbus Error counter for this WI-EX module
30018 + Offset	Modbus Last Error code for this WI-EX module (see "Expansion I/O error registers" on **page 60**)
30019 + Offset	Modbus Lost Link counter for this WI-EX module
30020 + Offset	Module type (0x0201) = 513 / error status
40009 + Offset 40016+Offset	Pulsed output target 1–8 (1 register per output)

I/O store for WI-EX-13 expansion I/O modules

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 WI-EX module
10020 + Offset	Detected indication for this WI-EX module
30017 + Offset	Modbus Error counter for this WI-EX module
30018 + Offset	Modbus Last Error code for this WI-EX module (see "Expansion I/O error registers" on **page 60**)
30019 + Offset	Modbus Lost Link counter for this WI-EX module
30020 + Offset	Module type (0x0301) = 769 / error status
40001 + Offset 40008 + Offset	Analog output 1–8
40009 + Offset 40016+Offset	Pulsed output target 1–8 (one register per pulsed output)

Device models and locales

Device model	Lower frequency	Upper frequency	Max power		Bandwidth	Duty cycle limit	Description
Available locales							
WI-IO-415-U2-C3, WI-MOD-415-E-C3	340.0000	400.0000	40dBm	10W			
GL	340.0000	400.0000	40dBm	10W	6.25 kHz		Licensed (not USA)
			40dBm	10W	12.5 kHz		
			40dBm	10W	25 kHz		
WI-IO-415-U2-C4, WI-MOD-415-E-C4	400.0000	480.0000	40dBm	10W			
GL	400.0000	480.0000	40dBm	10W	6.25 kHz		Licensed Worldwide (Excluding USA)
					12.5 kHz		
					25 kHz		
US1	421.0000	454.0000	40dBm	10W	6.25 kHz		Licensed USA FCC Part 90 - Band 1
					12.5kHz		
US2	456.0000	462.5375	40dBm	10W	6.25 kHz		Licensed USA FCC Part 90 - Band 2
					12.5kHz		
US3	462.7375	467.5375	40dBm	10W	6.25 kHz		Licensed USA FCC Part 90 - Band 3
					12.5kHz		
US4	467.7375	480.0000	40dBm	10W	6.25 kHz		Licensed USA FCC Part 90 - Band 4
					12.5kHz		
HK	409.7500	409.9875	27dBm	500mW	12.5 kHz		Hong Kong
					25 kHz		
ISM-1	433.0500	434.0400	10dBm	10mW	12.5 kHz	10%	Region 1 ISM - Band 1
					25 kHz	10%	
ISM-2	434.0400	434.7900	10dBm	10mW	12.5 kHz		Region 1 ISM - Band 2
					25 kHz		
ISM-AUNZ	433.0500	434.7900	14dBm	25mW	12.5 kHz		Australia and NZ - ISM
					25 kHz		
ISM-ZA	433.0500	434.7900	20dBm	100mW	12.5 kHz		South Africa - ISM
					25 kHz		
ISM-ES	433.0750	433.3500	27dBm	500mW	12.5 kHz		Spain - ISM
					25 khz		
SE	439.6875	439.9875	27dBm	500mW	12.5 kHz		Sweden
					25 kHz		
CZ1	448.0700	448.0700	27dBm	500mW	12.5 kHz	10%	Czech Republic Freq 1
CZ2	448.1700	448.1700	27dBm	500mW	12.5 kHz	10%	Czech Republic Freq 2
NZ	458.5400	458.6100	27dBm	500mW	12.5 kHz		New Zealand GURL
					25 kHz		
UK1	458.5000	458.8250	27dBm	500mW	12.5 kHz		United Kingdom GURL Band 1
					25 kHz		
UK2	458.8375	458.9000	27dBm	500mW	12.5 kHz		United Kingdom GURL Band 2
					25 kHz		
UK3	458.9000	458.9500	27dBm	500mW	12.5 kHz		United Kingdom GURL Band 3
					25 kHz		
ZA	464.5000	464.5875	20dBm	100mW	12.5 kHz		South Africa RFSR GG34172
					25 kHz		
AU	472.0125	472.1125	20dBm	100mW	12.5 kHz		Australia LIPD Class License
					25 kHz		

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 thistype.
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.

Secure hardening guidelines

Introduction

The WI-415 Series 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.

Weidmuller 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. Weidmuller also offers Cybersecurity Best Practices whitepapers to its customers that can be referenced at www.Weidmuller.com/cybersecurity

Category	Description
Asset identification and Inventory	Keeping track of all the devices in the system is a pre-requisite 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 WI-415 Series 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 WI-415 Series 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 WI-415 Series 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 WI-415 Series 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 WI-415 Series 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 WI-415 Series.

Category	Description
Restrict logical access to equipment	It is extremely important to securely configure the logical access mechanisms provided in in the WI-415 Series to safeguard the device from unauthorized access. The WI-415 Series provides administrative, operational, configuration roles for device users. Eaton 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 WI-415 Series 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 WI-415 Series 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). • 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 “ on page 58 of this manual 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
Conduct regular Cybersecurity risk analyses of the organization /	Eaton has worked with third-party security firms to perform system audits, both as part of a specific customer’s deployment and within Eaton’s own development cycle process. Eaton can provide guidance and support to your

Category	Description
Restrict network access	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 WI-415 Series uses the following IP protocol ports which may need to be configured in your network firewall: Modbus protocol: TCP port 502 (Default, Configurable) WIB Protocol: UDP port 4370 Serial transfer protocol: TCP, UDP port 24 (Default, Configurable) DNP3 Protocol: TCP, UDP port 20000 (Default, Configurable) Remote configuration: TCP port 80 (HTTP) Remote dashboard: TCP port 80 (HTTP) 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.
Logging and event management	**Best practices** • Eaton 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” on **page 65** of this manual. This exercise should be conducted in conformance with established technical and regulatory frameworks such as IEC 62443 and NERC-CIP.
Plan for business continuity/ cybersecurity disaster recovery	t’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] Cybersecurity Considerations for Electrical Distribution

[R2] Cybersecurity Best Practices Checklist Reminder

[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015.

[R4] National Institute of Technology (NIST) Interagency “Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41”, October 2009.

Full firmware upgrade

You can upgrade the firmware using a USB flash drive containing the firmware files. A full USB upgrade is necessary if a patch file is not available or the existing firmware is a much older version and would require multiple patch files to upgrade to the latest version.

Note: The feature keys and configuration are not changed or erased during a full upgrade.

The following procedure provides instructions for performing a full USB firmware upgrade on a WI-415 Series.

Requirements

- USB flash drive
- Firmware files (contact WEIDMULLER technical support for these files)
- PC for transferring files

To prepare the USB flash drive

Not all USB flash drives are configured correctly for use as a firmware upgrade drive. Use the following procedure to check the configuration of the USB drive and re-configure the drive if necessary.

1. Plug USB drive into the USB port on the PC and wait until Windows recognizes the drive and completes the driver installation.
2. Open the Windows Start menu, choose Run, and then enter “CMD” to open a command prompt. Then, type “diskpart” at the command prompt. This opens the Diskpart utility.

```
C:\>diskpart
Microsoft DiskPart version 6.1.7601 Copyright
(C) 1999-2008 Microsoft Corporation.
On computer: TEST_COMPUTER
```

3. Type command “list disk” to list available disks, and identify the USB drive based on the size.
   In the following example, the USB drive is a 1911 MB (2 GB) drive, which corresponds to Disk 1.

```
DISKPART> list disk
Disk ### Status Size Free DynGpt
----------------------------------------
Disk 0Online232 GB0 B
Disk 1Online 1911 MB0 B
```

4. When you have identified the USB disk, enter the “select Disk X” command to select this disk.

WARNING

THE COMMANDS THAT FOLLOW THIS STEP CAN DESTROY THE CONTENTS OF THE SELECTED DISK, MAKE SURE THAT YOU HAVE SELECTED THE CORRECT DRIVE BEFORE CONTINUING. SELECTING THE WRONG DRIVE COULD FORMAT YOUR PC’S HARD DRIVE.

```
DISKPART> select Disk 1
Disk 1 is now the selected disk.
```

5. Enter the command “list partition” to check how the USB drive is partitioned.

   This command indicates whether the drive is correctly configured for use as a firmware upgrade drive on the WI-415 Series.

   - If the drive contains only one partition and the “Offset” value is non-zero, as shown in the example below, you can proceed to format the drive and use it “as is” for firmware upgrade. Skip to step 7 for instructions on how to format the drive using the Diskpart utility.

```
DISKPART> list partition
  Partition ###  Type        Size     Offset
  -------------  ----        ----     ------
  Partition      1Primary    1910 MB  64 KB
```

   - If the “Offset” is zero or if there is more than one partition, as shown in the examples below, go to steps 6 and 7 below to re-configure the drive.

```
Partition ###  Type        Size      Offset
-------------  ----        ----      ------
Partition      1Primary    1911 MB   0 KB
Partition ###  Type        Size      Offset
-------------  ----        ----      ------
Partition      1Primary    100 MB    64 KB
Partition      2Primary    1810 MB   101 KB
```

6. Enter the command “clean” to delete all partitions on the disk, and then enter “list disk” to check that all memory is now free. In the example below, the asterisk (*) indicates that Disk 1 is the selected disk.

```
DISKPART> clean
DiskPart succeeded in cleaning the disk.
DISKPART> list disk
  Disk ###  Status   Size    Free     DynGpt
  --------  ------   ----    ------   ------
   *        Disk 0   Online  1911 MB  1910 KB
```

7. Enter the command “create partition primary” to create a partition on the USB drive. Then, enter the “list partition” command and note that there is only one partition, and that the offset is non-zero.

```
DISKPART> create partition primary
DiskPart succeeded in creating the
specified partition
  Partition ###   Type       Size     Offset
  -------------   ----       ----     ------
  Partition       1Primary   1910 MB  64 KB
```

8. Finally, format the drive using the Diskpart command line. The file system format should be selected as FAT32 using the option “fs=fat32”. You can select any convenient label. In the example below the label “FW_UPGRADE” was used.

```
DISKPART> format fs=fat32 label=FW_
UPGRADE
100 percent completed
DiskPart successfully formatted the
volume.
```

Alternatively, you can format the drive from within the Windows GUI environment using the following procedure.

To format the USB flash drive

1. Plug the USB flash drive in to the USB port on the PC.
2. Right-click the drive and select **Format** from the menu.

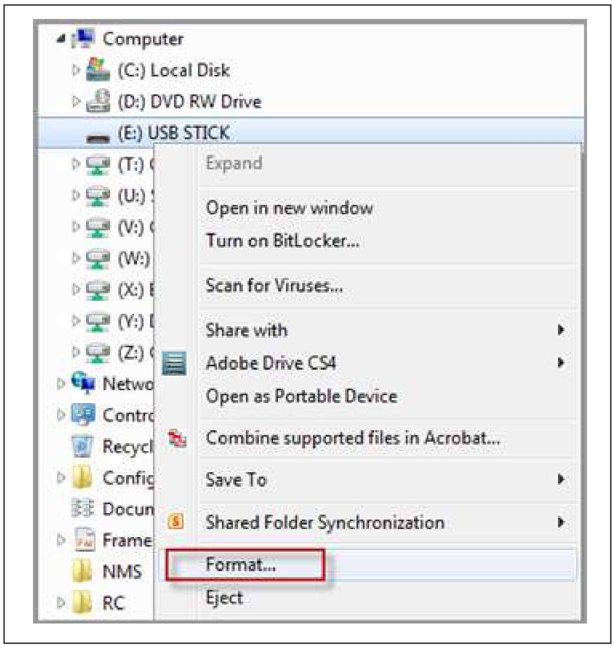


Figure 97. Formatting USB flash drive

3. Make sure that **Quick Format** is not selected, and then click **Start**.

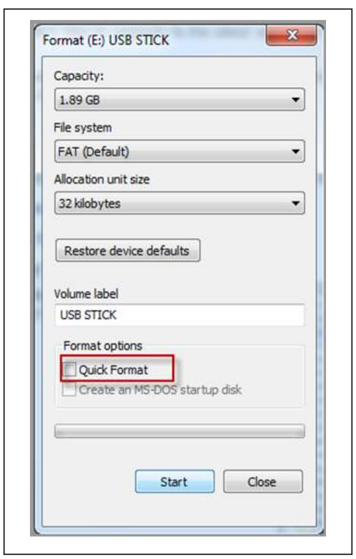


Figure 98. Quick format

4. When formatting is complete, copy the supplied firmware files to the USB flash drive root directory.

The files should look similar to the following figure.

Figure 99. Firmware files

5. Remove the USB flash drive from the PC.

To perform a full firmware upgrade using USB flash drive

1. Connect to the module's Web-based configuration utility and make a note of the current firmware version, which appears on the home Web page.

   This will enable you to compare versions to confirm that the upgrade procedure has been performed successfully.

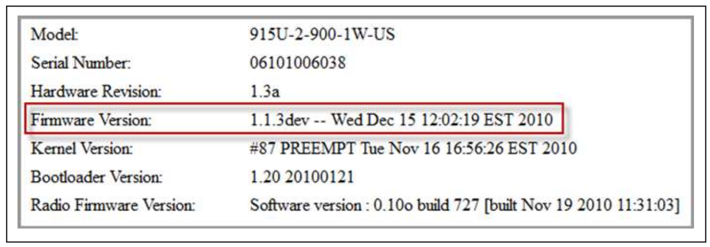


Figure 100. Firmware version

2. Power off the WI-415 Seriesif it is currently powered on.
3. Remove the cover from the small access panel on side of module to reveal a USB port and switches.

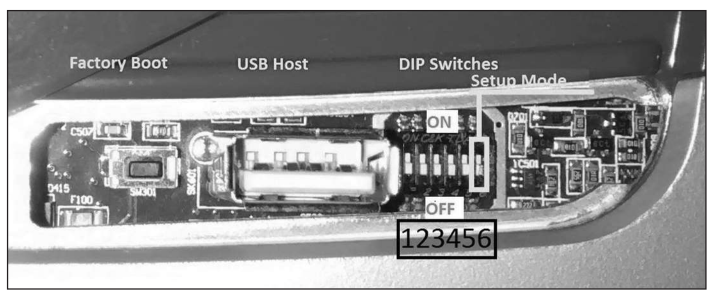


Figure 101. Module USB port and switches

4. Plug USB stick into USB port and power on the WI-415 Series module.
5. The PWR LED will flash, as indicated in .

⚠**Note**: Do not remove the flash drive or interrupt power to the module while the upgrade is in progress. If the upgrade process is interrupted, the module may become unserviceable and will need to be returned to Weidmuller for repair.

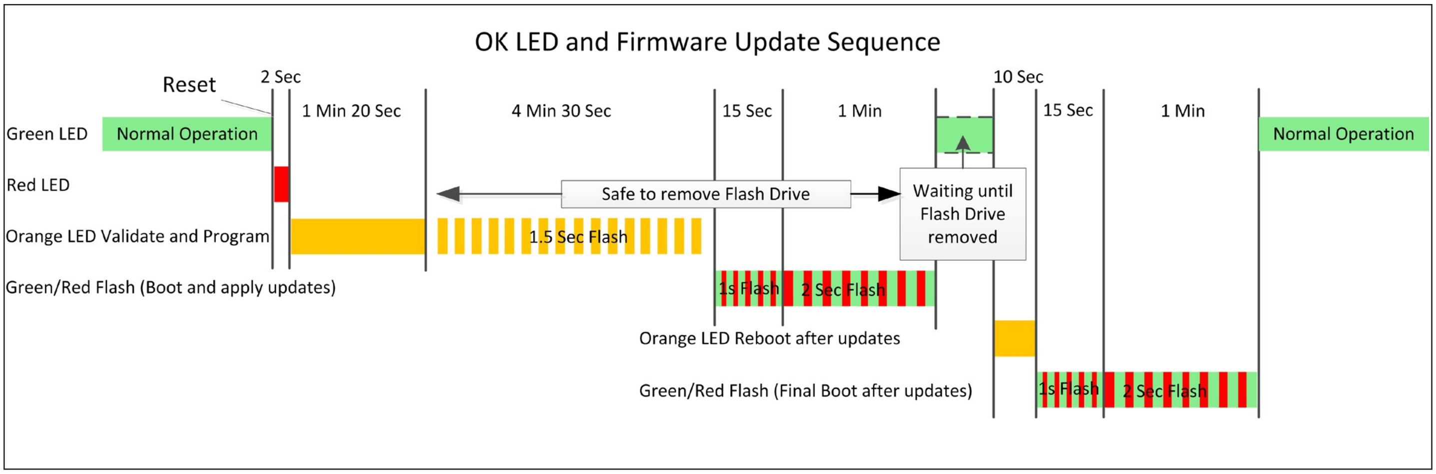


Figure 102. Firmware upgrade LED indicators

6. When the upgrade is complete, remove the USB flash drive from the module's USB port and replace the access panel cover.

IO Plus Logic Command Reference

Instruction	I	N	{	Description	Argument
LOAD				**Load the Accumulator**	
LOAD				Load a value from memory to the accumulator. 32-bit counter: MSW at the high (Even) address. Float: Loads the integer part only (0-65535)	Memory Register to load from
LOAD	I			Load an immediate value to the accumulator	The actual value to load to accumulator
LOAD		N		Invert and Load to accumulator Discrete: ON gives "0"; OFF gives "1". Other types: bitwise invert e.g. 0xFACE gives 0x0531	Memory Register to load from
LOAD			{	Calculate Memory Register to Load from within the { }. The accumulator value is loaded from the location that has been calculated when the "}" statement is reached.	Initial value for the Memory Register calculation
STORE				**Store the accumulator to memory**	
STOR				Save value from the accumulator to memory	Register location to save to
STOR		N		Invert accumulator and save. When storing to a bit Register, a non-zero value is stored as off, and zero is stored as on.	Register location to save to
STOR			{	Calculate Memory Register to Store to within the following instructions { }. The current accumulator value is saved to the location that has been calculated when the "}" statement is reached.	Initial value of Register calculation
Delayed Calculation			**{**	**Calculate the Second Argument of a statement** Use this feature when you need multiple steps to calculate the second argument of a statement.	
			{	Check the "{" Column to begin calculation of the argument to a statement. This works for LOAD, STOR and for all of the Logic and Math operations, as well as for the Test/Comparison operations.	Initial value to load for the calculation
}				Complete and execute a delayed Calculation. This matches the opening brace flag "{" in the LOAD, STORE, Arithmetic, Logical, and Comparison commands. It completes the calculation of the argument value and executes the original command.	Argument Ignored
SET/ RESET				**Set or Clear a bit**	
SET				Set memory register to "1" if accumulator is non-zero. Unchanged if accumulator is zero.	Memory location to set
SET		N		Set memory register to "1" if accumulator is zero.	Memory location to set
RES				Clear memory register if accumulator is non-zero. Unchanged if accumulator is zero.	Memory location to clear
RES		N		Clear memory register if accumulator is zero.	Memory location to clear
LOGIC/MATH				**Bitwise Logical and Arithmetic operations**	
AND OR XOR ADD SUB MUL DIV				Perform Logical / Arithmetic operation between Accumulator and memory. Result is saved in the accumulator. AND, OR, XOR – Bitwise Operation ADD – 16-bit addition with overflow SUB – 16-Bit subtraction with overflow MUL – Multiplication (mod 65536) DIV – Division (x / 0 = 0)	Register index of the value to use for the second operand
AND ... DIV	I			Perform Logical / Arithmetic operation between Accumulator and Immediate value	Immediate value to use for the second operand
AND ... DIV		N		Negate the argument (Bitwise invert) before performing the operation.	Applies to Register, Immediate and delayed calculation.
AND ... DIV			{	Perform Logical / Arithmetic operation between Accumulator and the result of the following calculation within the { }	Initial memory location or immediate value (I) for calculation of second operand.
TEST				**Compare two values**	

Instruction	I	N	{	Description	Argument
GT GE EQ NE LE LT				Perform Comparison operation between Accumulator and memory. Accumulator gets "1" if comparison true. "0" if false. GT – Greater Than GE – Greater or Equal EQ – Equal To NE – Not Equal LE – Less or equal LT – Less Than	Register index of the value to use for the second operand of the comparison
GT ... LT	I			Perform Comparison operation between Accumulator and Immediate value. Accumulatorgets "1" if comparison true. "0" if false.	Immediate value to use for the second operand of the comparison
GT ... LT		N		Negate the argument (two's compliment) before performing the comparison	Applies to Register, Immediate and delayed calculation forms.
GT ... LT			{	Perform Comparison operation between Accumulator and the result of the following calculation within the { }	Initial memory location or immediate value (I) for calculation of second operand.
JUMP				**Transfer Control to a new location**	
JMP				Jump to instruction	Line number to jump to
JMP	I			Jump forward or backward from the current location the number of lines specified	0-9999: Jump Forward 10000+: Jump backward
JMP_C				Conditional Jump if accumulator is non-zero	Line number to jump to if accumulator is non-zero
JMP_C		N		Conditional Jump if accumulator is zero	Line number to jump to if accumulator is zero.
JMP_C	I			Conditional Jump forward or backward from the current location the number of lines specified	0-9999: Jump Forward 10000+: Jump backward
CALL/ RETURN				**Call a subroutine and Return**	
CALL				Call a subroutine. A subroutine will execute the listed statements until a "RET" statement is reached, where control returns to the line following the CALL statement.	Line number of first instruction of the subroutine to call
CALL	I			Call a subroutine forward or backward from the current location, offset from current location	0-9999: call Forward 10000+: call backward
CALL_C				Conditional Call if accumulator is non-zero. (otherwise continue to next line)	Line number to call if accumulator is non-zero
CALL_C		N		Conditional Call if accumulator is zero	Line number to call if accumulator Is zero.
CALL_C	I			Conditional Call a subroutine forward or backward from the current location, offset from current location	0-9999: Jump Forward 10000+: Jump backward
RET				Return from subroutine. Returns to the instruction following the last executed CALL instruction.	Argument Ignored
RET_C				Return to calling address if accumulator is non-zero	Argument Ignored
RET_C		N		Return to calling address if accumulator is zero	Argument Ignored

GNU General public license

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms And Conditions For Copying, Distribution And Modification

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.
   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)
      These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

      Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.
      In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.
3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   b. Accompany it with a written offer, valid for at least three

years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Glossary

Term	Definition
ACK	Acknowledgment.
Access Point	An access point connects wireless network stations (or clients) to other stations within the wireless network and also can serve as the point of interconnection between the wireless network and a wired network. Each access point can serve multiple users within a defined network area. Also known as a base station.
Antenna Gain	Antennas do not increase the transmission power, but instead focus the signal. Rather than transmitting in every direction (including the sky and ground), antenna focus the signal either more horizontally or in one particular direction. This gain is measured in decibels.
AODV	Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks and other wireless ad hoc networks. In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time.
AWG	American wire gauge (AWG), also known as the Brown and Sharpe wire gauge, is a standardized wire gauge system used predominantly in the United States and Canada for the diameters of round, solid, nonferrous, electrically conducting wire.
Bandwidth	The maximum data transfer speed available to a user through a network.
COS	Change of state. For a digital input, a COS 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 called sensitivity.
CSA	The Canadian Standards Association (CSA), is a not-for-profit standards organization that develops standards in 57 areas. The CSA registered mark shows that a product has been independently tested and certified to meet recognized standards for safety or performance.
DCS	A Distributed Control System (DCS) is a computerized control system used to control the production line in industry. The entire system of controllers is connected by networks for communication and monitoring.
DHCP	Dynamic Host Configuration Protocol is a utility that enables a server to dynamically assign IP addresses from a predefined list and limit their time of use so that they can be reassigned. Without DHCP, an IT manager would need to manually enter in all the IP addresses of all the computers on the network. When DHCP is used, whenever a computer logs onto the network, an IP address is automatically assigned to it.
DIO	Digital input/output.
DIN Rail	A DIN rail is a metal rail of a standard type widely used for mounting circuit breakers and industrial control equipment inside equipment racks.
DNP3	Communication protocol used in industrial control systems. Commonly used in Water supply and Electrical distribution.
DNS	Domain name service (DNS) is a program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers. The program works behind the scenes to facilitate surfing the Web with alpha versus numeric addresses. A DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. Every website has its own specific IP address on the Internet.
Encryption Key	An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read. Encryption keys should be kept secret.
EIRP	Equivalent isotropically radiated power (EIRP) or, alternatively, effective isotropically radiated power is the amount of power that a theoretical isotropic antenna (which evenly distributes power in all directions) would emit to produce the peak power density observed in the direction of maximum antenna gain. EIRP can take into account the losses in transmission line and connectors and includes the gain of the antenna. The EIRP is often stated in terms of decibels over a reference power emitted by an isotropic radiator with an equivalent signal strength. The EIRP allows comparisons between different emitters regardless of type, size or form.
FEC	Forward Erro Correction. This is a method of reducing the errors in a message by adding aditional data which is used to detect and correct errors. The extra data reduces the effective data rate, but improves the sensitivity for long and dificult radio paths.
FSK	Frequency Shift Keying. This method of radio modulation encodes data using shifts in radio frequency. 2FSK uses two frequency levels to encode one bit of data for each symbol. 4FSK uses four frequency levels to encode two bits of data for each symbol.
Hub	A multiport device used to connect PCs to a network via Ethernet cabling or via 802.11. Wired hubs can have numerous ports and can transmit data at speeds ranging from 10 Mbps to multi-Gigabyte speeds per second. A hub transmits packets it receives to all the connected ports. A small wired hub may only connect four computers; a large hub can connect 48 or more.
Hz	Hertz. The international unit for measuring frequency, equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 535–1605 kHz, the FM broadcast radio frequency band is 88–108 MHz, and wireless 802.11b/g LANs operate at 2.4 GHz.
IEEE	Institute of Electrical and Electronics Engineers, New York, www.ieee.org. A membership organization that includes engineers, scientists and students in electronics and allied fields. It has more than 300,000 members and is involved with setting standards for computers and communications.
I/O	Input/Output. The term used to describe any operation, program, or device that transfers data to or from a computer.
IP	Internet Protocol (IP) is a set of rules used to send and receive messages across local networks and the Internet.
IP Address	A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.
ISM	The industrial, scientific and medical (ISM) radio bands are portions of the radio spectrum reserved internationally for industrial, scientific, and medical purposes other than telecommunications.
LAN	Local Area Network (LAN) is a system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files, and drives.
LQI	Link quality indicator (LQI) is used in wireless networks to indicate how good the communications link is. LQI is a computed value, based on how clearly the signal is received by the radio. Interference, low signal strength, and radio transmitter or receiver faults can all contribute to poor LQI.

Term	Definition
MAC Address	Media Access Control (MAC) address is a unique code assigned to most forms of networking hardware. The address is permanently assigned to the hardware, so limiting a wireless network's access to hardware (such as wireless cards) is a security feature employed by closed wireless networks. But an experienced hacker armed with the proper tools can still figure out an authorized MAC address, masquerade as a legitimate address, and access a closed network. Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.
Modbus	Modbus is a serial communications protocol for use with its programmable logic controllers (PLCs).
PLC	A programmable logic controller (PLC) is a digital computer used for automation of electromechanical processes, such as control of machinery on factory assembly lines, amusement rides, or light fixtures.
Proxy Server	Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data.
QAM	Quadrature Amplitude Modulation. This method of radio modulation encodes data by varying the phase and amplitude of the radio signal. This allows more data to be encoded into each symbol at the expense of reduced sensitivity.
Receive Sensitivity	The minimum signal strength required to pick up a signal. Higher bandwidth connections usually have less receive sensitivity than lower bandwidth connections.
RJ-45	Standard connectors used in Ethernet networks. RJ-45 connectors are similar to standard RJ-11 telephone connectors, but RJ-45 connectors can have up to eight wires, whereas telephone connectors have four.
Router	A device that forwards data from one WLAN or wired local area network to another.
RSSI	Received signal strength indicator (RSSI) is a measurement of the power present in a received radio signal. In a radio system, RSSI is the relative received signal strength in a wireless environment, in arbitrary units. RSSI is an indication of the power level being received by the antenna. Therefore, the higher the RSSI number (or less negative in some devices), the stronger the signal.
RTU	A remote terminal unit (RTU) is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.
SCADA	SCADA (supervisory control and data acquisition) is a type of industrial control system (ICS). Industrial control systems are computer controlled systems that monitor and control industrial processes that exist in the physical world. SCADA systems historically distinguish themselves from other ICS systems by being large scale processes that can include multiple sites, and large distances.
Server	A computer that provides its resources to other computers and devices on a network. These include print servers, Internet servers and data servers. A server can also be combined with a hub or router.
SMA	SMA (SubMiniature version A) connectors are semi-precision coaxial RF connectors for coaxial cable with a screw type coupling mechanism. The connector has a 50 Ω impedance. It is designed for use from DC to 18 GHz.
Sub Network or Subnet	Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect together through a router.
Switch	A type of hub that efficiently controls the way multiple devices use the same network so that each can operate at optimal performance. A switch acts as a networks traffic cop: rather than transmitting all the packets it receives to all ports as a hub does, a switch transmits packets to only the receiving port.
TCP	Transmission Control Protocol (TCP) isprotocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet. For example, when a Web page is downloaded from a Web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as single message.
TCP/IP	The underlying technology behind the Internet and communications between computers in a network. The first part, TCP, is the transport part, which matches the size of the messages on either end and guarantees that the correct message has been received. The IP part is the user's computer address on a network. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup or permanently assigned. All TCP/IP messages contain the address of the destination network as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide.
Transmit Power	The power at which the wireless devices transmits, usually expressed in mW or dBm.
TTL	Transistor–transistor logic (TTL) is a class of digital circuits built from bipolar junction transistors and resistors. It is called TTL logic because both the logic gating function (AND) and the amplifying function are performed by transistors.
WAN	Wide area network (WAN) is a communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. Also used to distinguish between phone-based data networks and Wi-Fi. Phone networks are considered WANs and Wi-Fi networks are considered Wireless Local Area Networks (WLANs).
WEP	Wired Equivalent Privacy (WEP) is a basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. WEP is available in 40-bit (also called 64-bit), or in 108-bit (also called 128-bit) encryption modes. As 108-bit encryption provides a longer algorithm that takes longer to decode, it can provide better security than basic 40-bit (64-bit) encryption.
Wi-Fi	Wireless Fidelity. An interoperability certification for wireless local area network (LAN) products based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard.

Weidmuller - your partner in Industrial Connectivity

As experienced experts we support our customers and partners around the world with products, solutions and services in the industrial environment of power, signal and data. We are at home in their industries and markets and know the technological challenges of tomorrow. We are therefore continuously developing innovative, sustainable and useful solutions for their individual needs.
Together we set standards in Industrial Connectivity.

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold
phone +49 5231 14-0
fax +49 5231 14-292083
https://www.weidmueller.com

Weidmuller, SA de CV
Blvd. Hermanos Serdán 698, Col.
San Rafael Oriente
Puebla, Puebla, Mexico
C.P. 72029
Telephone: 01 222 2686267
Facsimile: 01 222 2686219 Email:
clientes@weidmueller.com Website:
www.weidmuller.com.mx

Weidmuller, Inc
821 Southlake Blvd.
Richmond, Virginia 23236
Telephone: (800) 849-9343
Facsimile: (804) 379-2593
Email: customerservice@weidmuller.com
Website: www.weidmuller.com

Weidmuller, Ltd
10 Spy Court
Markham, Ontario L3R 5H6
Telephone: (800) 268-4080 Facsimile:
(877) 300-5635
Email:orders_can@weidmueller.com
Website: www.weidmuller.ca