Reference Manual
00809-0200-4410, Rev CA
September 2020

Emerson Wireless 1410 Gateway

IEC

WirelessHART

EMERSON

NOTICE

Read this manual before working with the product. For personal and system safety, and for optimum product performance, ensure you thoroughly understand the contents before installing, using, or maintaining this product.

Within the United States, Emerson has two toll-free assistance numbers:

Global Service Center

Software and Integration Support

1-800-833-8314 (United States)

+63-2-702-1111 (International)

Customer Central

Technical support, quoting, and order-related questions.

1-800-999-9307 (7:00 am to 7:00 pm CST)

North American Response Center

Equipment service needs.

1-800-654-7768 (24 hours—includes Canada)

Outside of the United States, contact your local Emerson representative.

⚠ WARNING

Failure to follow these installation guidelines could result in death or serious injury.

Ensure only qualified personnel perform the installation.

Explosions could result in death or serious injury.

Verify that the operating environment of the device is consistent with the appropriate hazardous locations certifications.

Do not make or break connections while circuits are live unless the area is know to be non-hazardous

Potential electrostatic charging hazard. The enclosure is engineered polymer. Use care in handling and cleaning when in explosive environments to avoid an electrostatic discharge.

Electrostatic discharge can damage electronics.

Use proper personal grounding before handling electronics or making contact with leads and terminals.

Electrical shock could cause death or serious injury.

If the device is installed in a high-voltage environment and a fault condition or installation error occurs, high voltage may be present on transmitter leads and terminals.

Use extreme caution when making contact with the leads and terminals.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following conditions:

This device may not cause harmful interference. This device must accept any interference received, including interference that may cause undesired operation.

This device must be installed to ensure a minimum antenna separation distance of 8-in. (20 cm) from all persons.

The products described in this document are NOT designed for nuclear-qualified applications. Using non-nuclear qualified products in applications that require nuclear-qualified hardware or products may cause inaccurate readings.

For information on Rosemount nuclear-qualified products, contact your local Emerson Sales Representative.

Contents

1 Introduction

1.1 Product overview

The Emerson Smart Wireless Gateway 1410 (Gateway) connects *Wireless*HART® self-organizing networks with host systems and data applications. Modbus® communications over RS-485 or Ethernet provide universal integration and system interoperability. The optional OPC or EtherNet/IP™ functionality from the Gateway offers a means to connect to newer systems and applications while providing a richer set of data.

The Smart Wireless Gateway provides industry leading security, scalability, and data reliability. Layered security ensures that the network stays protected. Additional devices can be added at any time. There is no need to configure communication paths because the Gateway manages the network automatically. This feature also ensures that *Wireless*HART field devices have the most reliable path to send data.

What is included?

The box containing the Gateway will contain several items essential to the complete installation and operation of the Gateway.

- Smart Wireless Gateway
- Quick Start Guide
- Software pack, 2 disk set
- Informational side label for IP address
- Basic antenna (if no remote antenna is required)
- Terminal block (black)

If an optional remote antenna has been ordered, it will be in a separate box containing:

- Remote mount antenna
- Mounting hardware
- Lightning arrestor
- Cable (50- or 25-ft. [15,2 or 7,62 m] in length)
- Coaxial sealant tape
- Right angle SMA to N-Type adapter cable

1.2 Using this manual

This manual provides information to help install, configure, operate, and maintain the Gateway.

Introduction introduces the product and describes what components may be found in the box. It also includes details for services and support as well as return and disposal of the product.

Configuration describes how to connect to the Gateway for the first time and what settings should be configured before placing it on a live control network. It is important to note that some Gateways are used in stand-alone applications and do not reside on a network. In these cases, it is still important to configure the items outlined in this section.

Installation describes how to properly mount the Gateway and make electrical connections, including electrical wiring, grounding, and host system connections. This section also describes how to mount the optional remote antenna.

Commissioning describes the installation and setup of the optional software included with the Smart Wireless Gateway. This software will aid in secure host integration as well as wireless field device configuration.

Operation and Maintenance describes how to connect the Gateway to a host system and integrate data gathered from the field device network. It covers network architectures, security, and data mapping.

Troubleshooting provides troubleshooting tips as well as information to contact technical support over the phone or through email.

Glossary defines terms used throughout this manual or that appear in the web interface of the Smart Wireless Gateway.

Specifications and Reference Data and Product Certifications provide additional and more specific information on a variety of subjects including Product Specifications and Product Certifications.

1.3 Product recycling/disposal

Recycling of equipment and packaging should be taken into consideration and disposed of in accordance with local and national legislation/regulations.

2 Configuration

2.1 Overview

This section describes how to connect to Emerson Smart Wireless Gateway 1410 for the first time and the settings to configure before placing it on a live control network. It is important to note that some Gateways are used in stand-alone applications and do not reside on a network. In these cases, it is still important to configure the items outlined in this section.

Before the Gateway can be permanently mounted and connected to a live control network, it needs to be configured with an IP address. This is done by forming a private network between the Gateway and a PC/laptop. The following items are required to complete this section:

- Gateway
- PC/laptop
- Ethernet cable
- 24 VDC (nominal) power supply

2.2 System requirements

The following requirements apply to the PC/laptop used to configure the Gateway. Additional requirements may apply if using the Security Setup Utility or AMS™ Wireless Configurator. See Commissioning for more information.

Web browser applications

- Microsoft® Internet Explorer® 6.0 - 10.0

Ethernet

- 10/100 base-TX Ethernet communication protocol

2.3 Initial connection and configuration

2.3.1 Prepare PC/laptop

The PC/laptop will need to be configured to form a private network before communicating to the Gateway. The network settings can be found in the control panel of the PC/laptop running a Microsoft platform based operating system. To configure these settings:

Procedure

1. Find and open the **Control Panel** (generally accessed from the **Start** Menu).
2. Open **Network Connections**.
3. Select **Local Area Connection**.

4. Right click and select **Properties**.
5. Select **Internet Protocol (TCP/IP)**, then **Properties**.
6. From the *General* tab, select **Use the following IP address** button.
7. Set the *IP Address* to **192.168.1.12**, then **Tab** on the keyboard.
8. Select **OK** to close the *Internet Protocol (TCP/IP)* window.
9. Select **Close** on the *Local Area Connection* window.

Internet proxies will need to be disabled through the PC/laptop's default internet browser. Disable the proxies with the following procedure:

Procedure

1. Find and open the default internet browser.
2. Find the *Tools* menu and select **Internet Options**.
3. From the *Connections* tab, select the **LAN Settings** button.
4. Under *Proxy Server*, the boxes for *Automatically Detect Settings* and *Use a proxy server for your LAN* should be unchecked.
5. Select **OK** to close the *Local Area Network (LAN) Settings* window.
6. Select **OK** to close the *Internet Options* window.

   The PC/laptop is now set up to form a private network and to communicate with the Gateway.

Note
Connecting to the Gateway's secondary Ethernet port will require different network settings. See Table 2-1 for additional network settings.

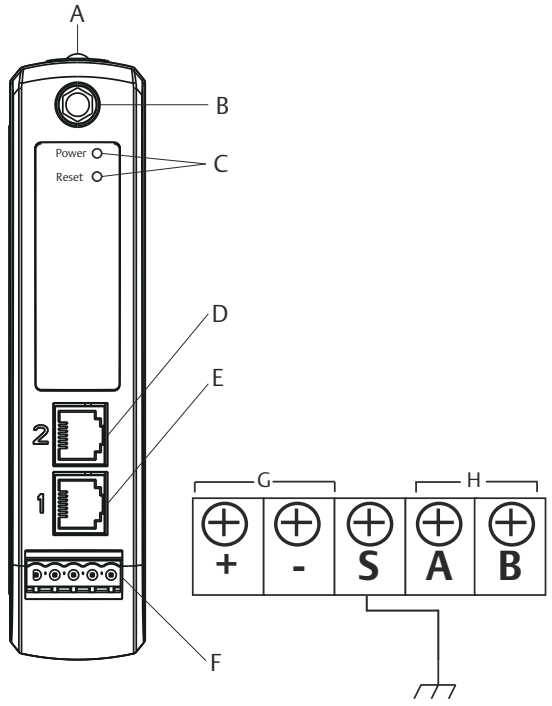
Table 2-1: Default IP Addresses

	Gateway	PC/laptop	Subnet
Ethernet 1	192.168.1.10	192.168.1.12	255.255.255.0
Ethernet 2	192.168.2.10	192.168.2.12	255.255.255.0

2.3.2 Connections and power

Physically connect the PC/laptop to the Gateway with an Ethernet cable by connecting one end to the Ethernet port on the back of the PC/laptop. Connect the other end to the Ethernet 1 port on the Gateway. Configure the gateway shows the standard terminal block diagram. Once the Gateway and PC/laptop are connected, wire a 24 VDC (nominal) power supply with a capacity of at least 250 mA to the Gateway power input terminals.

Figure 2-1: Emerson Smart Wireless Gateway 1410 Housing



A DIN rail clip

B SMA connector

C Power and reset indicator lights: During normal operation the power indicator will be green. During a reset the reset light will turn red. The reset switch should not be enabled during normal operation.

D Ethernet port 2:This secondary port must be enabled when ordering to access the device. When this port is activated, the factory IP address is 192.168.2.10. See Table 2-1.

E Ethernet port 1: Use for standard communication to the webserver or other protocols enabled on the gateway. The factory IP address is 192.168.1.10. See Table 2-1.

F 5-screw terminal block

G 24 VDC (nominal) power input

H Serial Modbus®

2.3.3 Configure the gateway

It is now possible to log into the Gateway for the first time and begin configuration for placement on a live control network. The following items need to be configured:

- Security Passwords
- Time Settings
- TCP/IP Network Settings

Use the following procedure to log in to the Gateway:

Procedure

1. Open a standard *web browser*.
2. Enter **https://192.168.1.10** in the address bar.
3. Continue though the security message.
4. Enter **admin** for User Name.
5. Enter **default** for the Password.

   The web browser will now be directed to the Gateway's default home page. There is a navigation menu located on the left hand side with four main areas.

   - Diagnostics: View status of communications, client server parameters, and more
   - Monitor: Screens created by the user to view data from field devices
   - Explorer: Basic view of values from field devices
   - Setup: Configure the Gateway for operations, security, and host system integration

Security passwords

There are four role-based user accounts for the Gateway with varying levels of access. Table 2-2 describes this access.

Table 2-2: Role Based Access User Accounts

Role	User name	Web Interface Access
Executive	exec	Read-only access
Operator	oper	Read-only access
Maintenance	maint	Configure HART® device settings Configure Modbus communications Configure Modbus register mapping Configure OPC browse tree Configure Active Advertising
Administrator	admin	Includes all maintenance privileges Configure Ethernet network settings Configure *Wireless*HART® network settings Set passwords Set time settings Set home page options Configure custom point pages Restart applications

Each of the initial passwords for the user accounts is *default*. It is recommended, for security purposes, that these passwords are changed. The administrator password should be appropriately noted when changed. If it is lost, do not return the Gateway to the factory, see Resetting to factory defaults.

To change the User Accounts Passwords:

Procedure

1. Navigate to **System Settings → Users → User accounts**.
2. Set the new password for each role based user account, and confirm.
3. Select **Submit**.

Note
It is suggested that the default security settings in **System Settings → Users → User Options** be changed to the local IT best practices or the "Normal" setting after initial login. Strong or custom settings are available for more robust passwords. For more information on this screen and others see the User Interface Terminology Guide (document number 00809-0600-4420).

Antivirus

Antivirus and other software tools are not included in the Gateway firmware. These software tools should be installed on any machine connected to the Gateway. Emerson bundles the latest software patches into our standard Gateway firmware updates. These software patches are not anti-malware or anti-virus tools in any sense of the word, but do provide the latest in security protection.

Password complexity

The browser front-end of the Gateway supports many customizable password rules (**System Settings → Users → User Options**). All of the following rules are customizable:

- Minimum overall password length
- Minimum lowercase character count
- Minimum uppercase character count
- Minimum digit count
- Minimum symbol count
- Idle session timeout time
- Maximum session lifetime to force a user to re-enter their password
- Minimum password lifetime to prevent a user from changing their password too often
- Maximum password lifetime to periodically force a user to change their password.
- Password failure limit at which point the account is locked and the user must wait for a specified period of time prior to additional attempts to enter their password
- Password failure lock to lock an account after a specified number of incorrect passwords
- Require a wait period after the specified number of incorrect passwords have been entered
- Password history depth to limit reuse of passwords

Logging

The Gateway monitors many security events automatically. A complete list of events can be viewed from the Log Settings (**System Settings** → **Gateway** → **Logging**) area in the Gateway interface. The Gateway also supports the optional use of a Syslog server. This provides significant flexibility and allows the user to determine how log messages are handled and how long logs are kept. It is possible for the user to configure the Syslog server to issue automated alerts for various messages.

Time settings

The Gateway is the timekeeper for the *Wireless*HART network, so it is imperative that the Gateway's time is accurate for timestamp data to be meaningful. Time settings can be found by navigating to **System Settings** → **Gateway** → **Time** as shown in Figure 2-2.

Gateway time settings and time stamps are stored internally as UTC time. The appropriate web browser being used displays the time as per the local browser settings.

There are three ways to set the Gateway time:

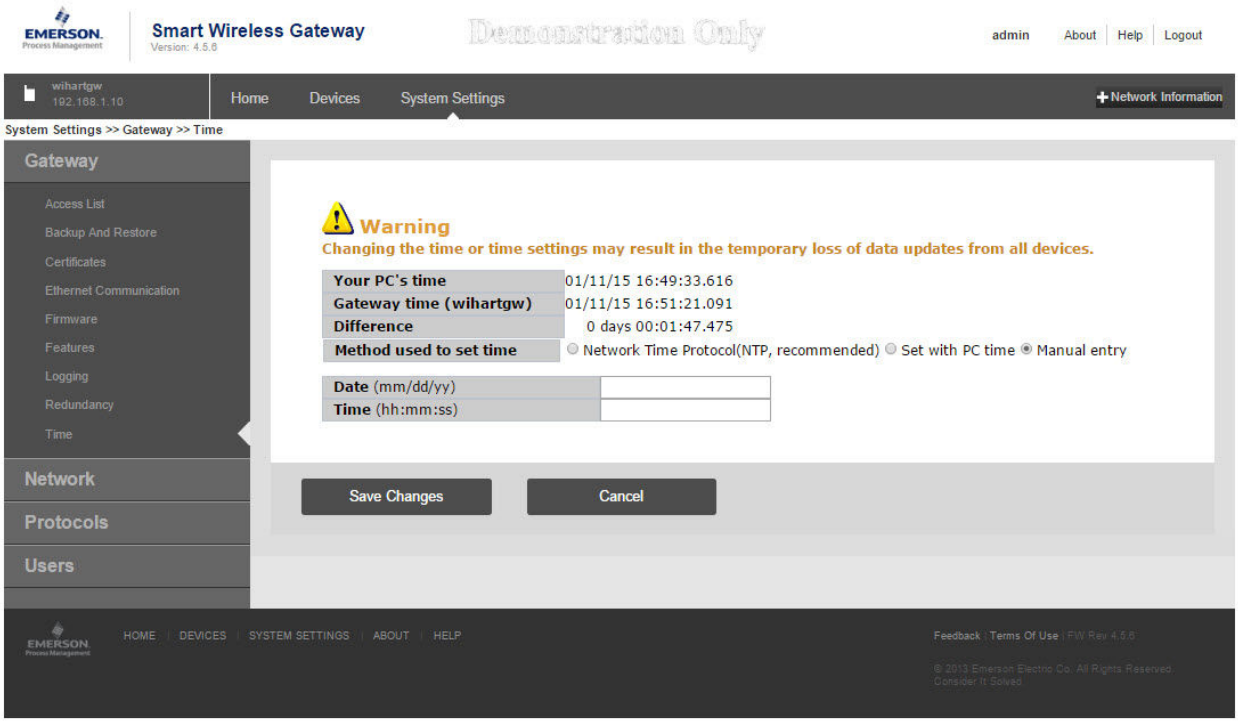
Procedure

1. Network Time Protocol (recommended). This option uses a Network Time Protocol (NTP) server to slowly adjust the Gateway's time in order to match the time of the control network. Enter the IP address for the NTP server and select the packet version (1, 2, 3, or 4).
2. Set with PC Time. This option will match the Gateway's time to that of the PC/ Laptop.
3. Manual Entry. This option allows the user to enter a specific date (MM:DD:YY) and time (HH:MM:SS).

   Note
   Network Time Protocol (NTP) is recommended for the best network performance because it always adjusts time to match the network time server.

   Failure to provide regular time synchronization over a long period of time (months) can cause the Gateway network to drift off time.

Figure 2-2: Setup → Time Settings



https://192.168.1.10/themes/default/views/index.html#settings/gateway/time

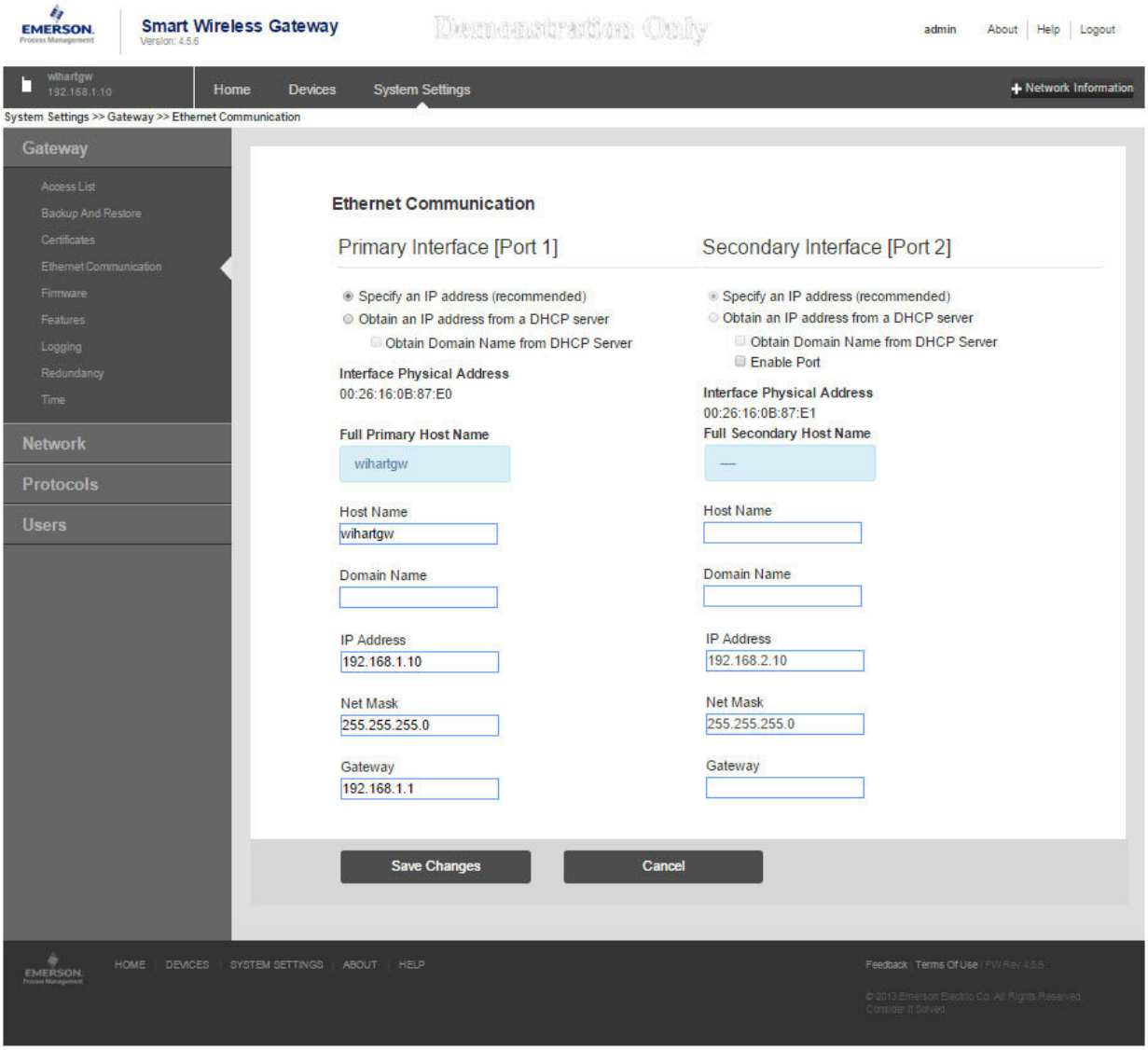
TCP/IP network settings

⚠ WARNING

Use caution when making changes to the TCP/IP network settings. If they are lost or entered incorrectly, the Gateway will require a factory reset (see Resetting to factory defaults). Contact the network administrator for information on the proper TCP/IP network settings to apply.

Prior to the Gateway being installed and connected to a live control network, it should be configured with an IP address, as well as other TCP/IP network settings. This specific page can be found in System backup.

Figure 2-3: Ethernet Settings



Request the following configuration items from the network administrator:

- Hostname
- Domain Name
- IP address
- Netmask
- Gateway

Obtaining an IP address from a DHCP server is not recommended, since the Gateway operation will be dependent on the availability of the DHCP server. For maximum Gateway availability it is best practice to specify an IP address.

To change the TCP/IP Network Settings:

Procedure

1. Navigate to **System Settings** → **Ethernet Communication**.
2. Select **Specify an IP address** (recommended).
3. Enter the following:
   - Hostname
   - Domain Name
   - IP Address
   - Netmask
   - Gateway
4. Select **Submit**.
5. When prompted, select **Restart Apps**.
6. Select **Yes** to confirm restart.
7. Close the web browser.

Note
Once the IP Address of the Gateway has been changed, communications to the web interface will be lost. Restart the web browser, then log back into the Gateway using the new IP address and other TCP/IP network settings. The PC/Laptop TCP/IP network settings may need to be changed. During a Restart Apps the wireless network will be temporarily lost.

2.3.4 System backup

The Gateway has a System Backup and Restore feature that saves all user-configured data. It is best practice that a System Backup be performed periodically throughout the installation and configuration process.

Procedure

1. Navigate to **System Settings** → **Gateway** → **Backup and Restore** → **Save**.
2. Select **Save Configuration**.
3. The Gateway collects the configuration date and when the file download pop up appears, select **Save**.
4. Enter a save location and file name.
5. Select **Save**.
6. Select **Return to form**.

Note
System backup contains user passwords and keys used for encrypting communication. Store downloaded system backups in a secure location.

2.3.5 Web page usage

It is not recommended that users stay logged on to a single page or a large number of users on multiple pages for long periods of time. This additional loading can slow the flow of data. The Gateway by default logs users out who are logged on for long periods of time with no activity.

2.3.6 Resetting to factory defaults

In the event that the user name, password, or IP address of the Gateway is lost, the Gateway can be restored to factory defaults by the procedure below.

Note
Following this procedure will cause the network to reform and all configuration parameters will be reset to factory defaults. Once the Gateway is reset, the user is strongly recommended to change the default password to maintain system security.

Procedure

1. Turn off power to the Gateway, remove connectors, and un-mount the device from the DIN rail.
2. Locate the *Reset* switch label on the back of the Gateway.
3. Break the label in the center and slide the switch up.
4. Mount and reconnect the Gateway; turn power *ON* on to the gateway.
5. Let the Gateway completely boot up (approximately 2 minutes). During this time the red *Reset* light on the front of the unit will be *ON*.
6. Turn off power to the Gateway, remove connectors and un-mount it from the rail again.
7. Return the *Reset* switch to lower position.
8. Mount and reconnect the Gateway; turn power *ON* on to the Gateway.
9. Verify the reset light is off, indicating the Reset switch is in the lower position. The Gateway will now be programmed back to factory defaults including IP addresses. The factory default IP addresses can be found in Table 2-1.

3 Installation

3.1 Overview

This section describes how to properly mount the Emerson Smart Wireless Gateway 1410 and make electrical connections, including electrical wiring, grounding, and host system connections. This section also describes how to mount the optional remote antenna.

3.1.1 General considerations

The unit itself is not designed for outdoor mounting without a suitable enclosure. The Gateway should be mounted in an approved electrical enclosure or building.

The Gateway should be mounted in a location that allows convenient access to the host system network (process control network) as well as the wireless field device network and protects the Gateway from moisture and contamination.

3.1.2 Physical description

The Gateway electronics is enclosed in a polymer housing. The front of the enclosure has connections for power, Ethernet, and serial communications. The unit is designed to be mounted on a DIN rail inside an electronic enclosure.

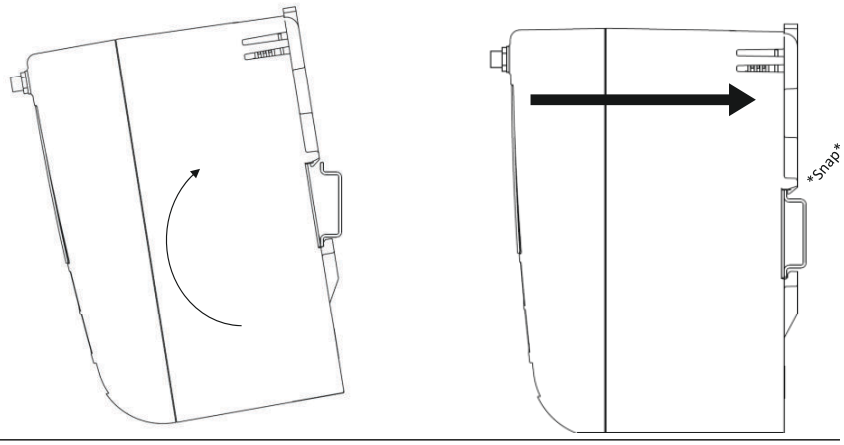
3.2 Mounting

The unit can be snapped onto a DIN TS35/7.5 or TS35/15 rail system. To clip the unit onto the DIN rail, see Figure 3-1.

Procedure

1. Tilt the unit at a slight angle allowing the lower lip of the chassis to catch the bottom of the DIN rail.
2. Apply pressure forward to snap the back of the unit securely onto the DIN rail.

Figure 3-1: Installing



To remove the unit, see Figure 3-2.

3. Place a flat or rounded object (such as a screw driver) into the DIN clip and apply a slight pressure downwards on the object.
4. Once the unit is released from the DIN rail pull backwards and down to successfully disengage.

Figure 3-2: Removing

NOTICE

When mounting the unit in an electrical enclosure or other location, comply with the appropriate local and governmental installation codes. Verify the installer, associated hardware, and installation equipment used have the proper certifications for the specific type of installation being performed. Before installation, verify if local codes require a permit and/or an inspection before energizing. When planning the installation, account for routing the antenna cable within the enclosure.

Note
Do not mount the antenna within a metal enclosure. To avoid damage to sensitive RF components, do not remove protective cap from the Gateway SMA connector until ready to install the antenna.

3.3 Remote antenna

The small black flexible basic antenna supplied with the unit is for bench testing. In most locations, a remote antenna is recommended for best range and performance. The remote antenna options provide flexibility for mounting the Gateway based on wireless connectivity, lightning protection, and current work practices.

Note
To avoid damage to sensitive RF components do not remove protective cap from the Gateway SMA connector until ready to install the antenna.

⚠ WARNING

When installing remote mount antennas for the Wireless Gateway, always use established safety procedures to avoid falling or contact with high-power electrical lines.

Install remote antenna components for the Wireless Gateway in compliance with local and national electrical codes and use best practices for lightning protection.

Before installing consult with the local area electrical inspector, electrical officer, and work area supervisor.

The Wireless Gateway remote antenna option is specifically engineered to provide installation flexibility while optimizing wireless performance and local spectrum approvals. To maintain wireless performance and avoid non-compliance with spectrum regulations, do not change the length of cable or the antenna type.

If the supplied remote mount antenna kit is not installed per these instructions, Emerson is not responsible for wireless performance or non-compliance with spectrum regulations.

The remote antenna kit includes coaxial sealant for the cable connections, for the lightning arrestor, and for the antenna.

Find a location where the remote antenna has optimal wireless performance. Ideally this will be 15- to 25-ft. (4,6 to 7,6 m) above the ground or 6-ft. (2 m) above obstructions or major infrastructure. To install the remote antenna use one of the following procedures:

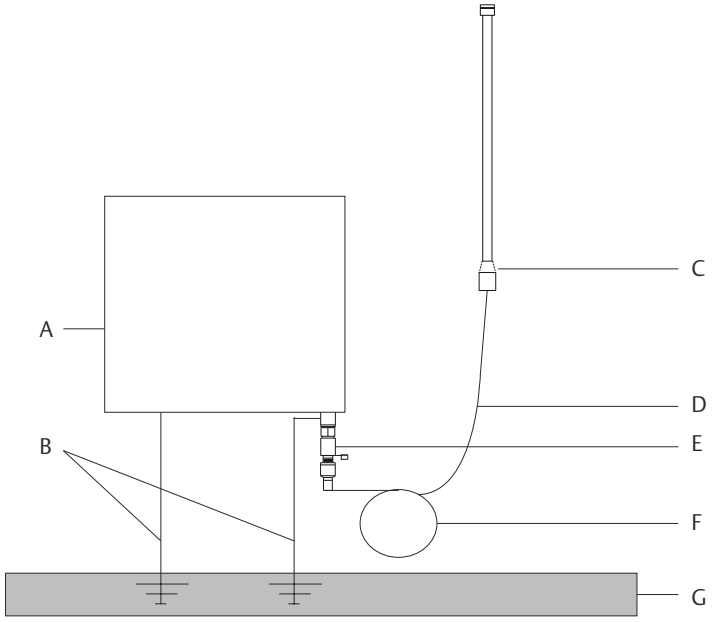
3.3.1 Installation of WL2/WN2 option

Procedure

1. Mount the antenna on a 1.5- to 2-in. pipe mast using the supplied mounting equipment.
2. Connect the lightning arrestor directly to the bottom of the user supplied enclosure.
3. Install the grounding lug, lock washer, and nut on top of the lightning arrestor.
4. Connect the antenna to the lightning arrestor using the supplied coaxial cable ensuring the drip loop is not closer than 1-ft. (0,3 m) from the lightning arrestor.
5. Use the coaxial sealant to seal each connection between the Gateway, lightning arrestor, cable, and antenna.
6. Ensure that the mounting mast, lightning arrestor, and Gateway are grounded according to local/national electrical code.

   Any spare lengths of coaxial cable should be placed in 1-ft. (0,3 m) coils.

Figure 3-3: Installation of WL2/WN2 Option



A. User supplied enclosure containing Gateway
B. Ground
C. Remote antenna
D. Cable
E. Lightning arrestor
F. Drip loop
G. Earth

Note
Weather proofing is required! The remote mount antenna kit includes coaxial sealant for the cable connections for the lightning arrestor, antenna, and Gateway. The coaxial sealant must be applied to guarantee performance of the wireless field network. See Figure 3-4 for details on how to apply weather proofing.

Figure 3-4: Applying Coaxial Sealant to Cable Connections

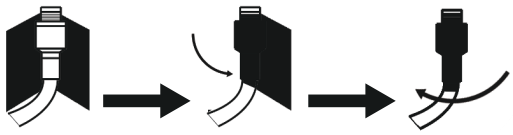


Table 3-1: Remote Antenna Kit Options

Kit option	Antenna	Cable 1	Lightning arrestor
WL2	1/2 Wavelength Dipole Omni-Directional +6 dB Gain	50 ft. (15,2 m) LMR-400	Head mount, jack to plug Gas discharge tube 0.5 dB insertion loss
WN2	1/2 Wavelength Dipole Omni-Directional +8 dB Gain	25 ft. (7,6 m) LMR-400	Head mount, jack to plug Gas discharge tube 0.5 dB insertion loss

3.4 Connections

3.4.1 Grounding

The DIN rail should always be grounded in accordance with national and local electrical codes. The most effective grounding method is a direct connection to earth ground with minimal impedance. Grounding to the Gateway is accomplished through the DIN rail clip on the back of the Gateway.

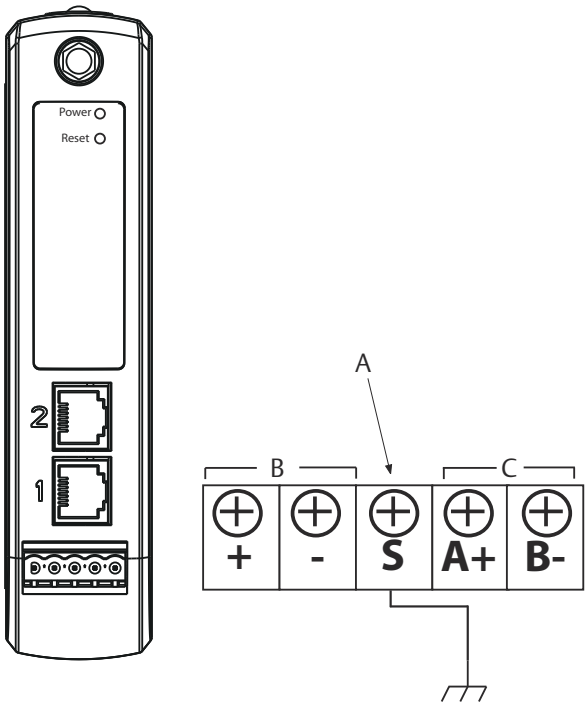
3.4.2 Ethernet

The Gateway is equipped with two 10/100 base-TX Ethernet communications ports (see Figure 3-5). These connections can be used to access the Gateway's web interface and to communicate Modbus® TCP, OPC, and EtherNet/IP™ protocols.

The primary Ethernet port (Ethernet 1) is used to connect to the host system or other application systems. The secondary Ethernet port (Ethernet 2) can be used as a back up connection or a maintenance port for local access to the Gateway.

Note
Unless dual Ethernet ports were specified at the time of order, the secondary Ethernet port (Ethernet 2) will not be active.

Figure 3-5: Emerson Smart Wireless Gateway 1410 Terminal Block



A 5-screw terminal block

B 24 VDC (nominal) power input

C Serial Modbus®

Ethernet connections should use Cat5e shielded cable to connect to an Ethernet hub, switch, or router. The maximum cable length should not exceed 328-ft. (100 m).

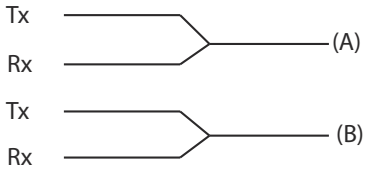
3.4.3 RS-485

The Gateway can be ordered with an optional RS-485 (serial) connection (Figure 3-6). Modbus terminals are labeled A and B on the wiring diagram. This connection is used to communicate Modbus RTU on an RS-485 data bus.

Use 18 AWG single twisted shielded pair wiring to connect the Gateway to the RS-485 data bus. The total bus length should not exceed 4000-ft. (1220 m). Connect the Tx - (negative, receive) wire to terminal A and the Rx + (positive, transmit) wire to terminal B. The wiring shield should be trimmed close and insulated from touching the Gateway enclosure or other terminations.

If the existing data bus uses a 4-wire Full Duplex configuration, see Figure 3-6 to convert to a 2-wire Half Duplex configuration.

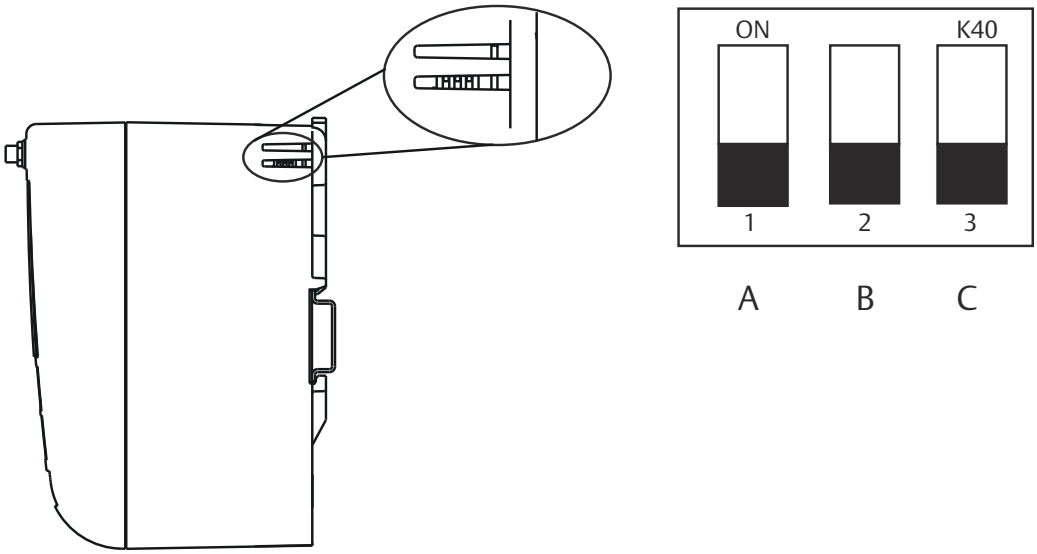
Figure 3-6: Convert from Full to Half Duplex



3.4.4 Terminating resistors

Three DIP switches are provided to enable various terminating resistors to the RS-485 data bus. The switches are found inside the electronics housing, located behind an access slot on the upper right side. The switches number bottom to top 1 through 3 and the upward position is ON.

Figure 3-7: RS-485 Resistor DIP Switches



(1)

A 470 Ω pull-up resistor

B 120 Ω terminating resistor

C 470 Ω pull-down resistor

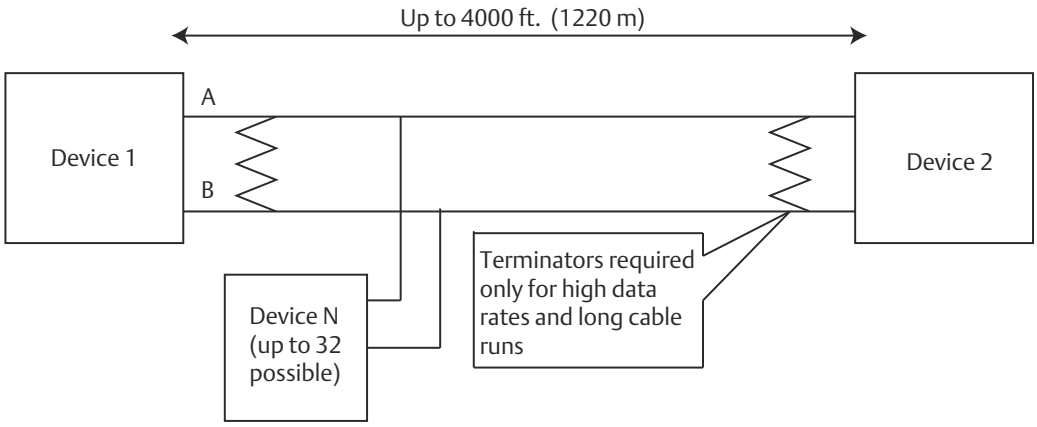
Switches 1 and 3 are connected to pull-up and pull down resistors. Switch 1 is for the Tx (A) line and Switch 3 is for the Rx (B) line. These 470 ohm resistors are used to prevent noise from being interpreted as valid communications during periods when no actual communications are occurring. Only one set of pull-up and pull-down resistors should be active on the RS-485 data bus at time.

Switch 2 is connected to a 120 ohm terminating resistor. This resistor is used to dampen signal reflections on long cable runs. RS-485 specifications indicate that the data bus

(1) Use a sharp non metal tool to switch between resistor options.

should be terminated at both ends (Figure 3-8). However termination should only be used with high data rates (above 115 kbps) and long cable runs.

Figure 3-8: Typical Half Duplex (2-wire) Network



A	Tx line
B	Rx line

3.4.5 Power

The Gateway is designed to be powered by 24 VDC (nominal) Class 2 supply and requires 250 mA of current. The positive and negative connections are depicted on the diagram shown in Figure 3-6.

The wiring should include an external power shut-off switch or circuit breaker located near the Gateway.

Note
Using an uninterruptible power supply is recommended to ensure availability should there be a loss of power.

4 Commissioning

4.1 Overview

This section discusses the installation and setup of the optional software included with the Emerson Smart Wireless Gateway 1410. This software is not required for the wireless field network to operate; however, it will aid in secure host integration as well as wireless field device configuration. The following table describes what items are installed and on which disk they can be found.

Table 4-1: Software Applications

Name	Description	Location
Security Setup Utility	This utility allows the setup of SSL enabled communications between the Gateway and host system.	Disk 1
AMS™ Wireless Configurator	This application allows complete configuration of wireless field devices and provides added security through drag and drop provisioning.	Disk 2
Network Configuration	This application configures AMS Wireless Configurator to interface to a Wireless Network or a HART® Modem.	Disk 2

Additional system components may be installed depending on the current configuration of the system.

4.2 System requirements

Table 4-2: PC Hardware

Minimum requirements	Recommended requirements
Intel® Core 2 Duo, 2.0 GHz	Intel Core 2 Quad, 2.0 GHz or greater
1 GB Memory	3 GB Memory or Greater
1.5 GB free hard disk space	2 GB or more of free hard disk space

Note
Additional hard disk space is required for SNAP-ON™ applications. The minimum monitor requirements are 1024 × 768 resolution and 16-bit color.

Table 4-3: Supported Operating Systems

Operating system	Version
Microsoft® Windows™ XP	Professional, Service Pack 3
Windows Server 2003	Standard, Service Pack 2
Windows Server 2003 R2	Standard, Service Pack 2
Windows Server 2008	Standard, Service Pack 2

Table 4-3: Supported Operating Systems *(continued)*

Operating system	Version
Windows Server 2008 R2	Standard, Service Pack 1
Windows 7	Professional, Service Pack 1
Windows 7	Enterprise, Service Pack 1
Windows 8	Enterprise, Service Pack 1
Windows Server 2008	Standard, Service Pack 2
Windows 10	Enterprise, Service Pack 1

Note
Only 32-bit versions of the operating systems are supported for AMS Wireless Configurator.

4.3 Software installation

The software can be found on the 2 disk pack, included with the Gateway. Depending on the PC system configuration, installation may take 30-35 minutes. Installing disk one followed by disk two is recommended. The Security Setup Utility is located on Disk 1. To install the software:

Procedure

1. Exit/close all Windows programs, including any running in the background, such as virus scan software.
2. Insert Disk 1 into the CD/DVD drive of the PC.
3. Follow the prompts.

   AMS Wireless Configurator is located on Disk 2. To install the software:

4. Exit/close all Windows programs, including any running in the background, such as virus scan software.
5. Insert Disk 2 into the CD/DVD drive of the PC.
6. Select **Install** from the menu when the AMS Wireless Configurator setup begins.
7. Follow the prompts.
8. Allow AMS Wireless Configurator to reboot PC.
9. Do not remove the disk from the CD/DVD drive.
10. Installation will resume automatically after login.
11. Follow the prompts.

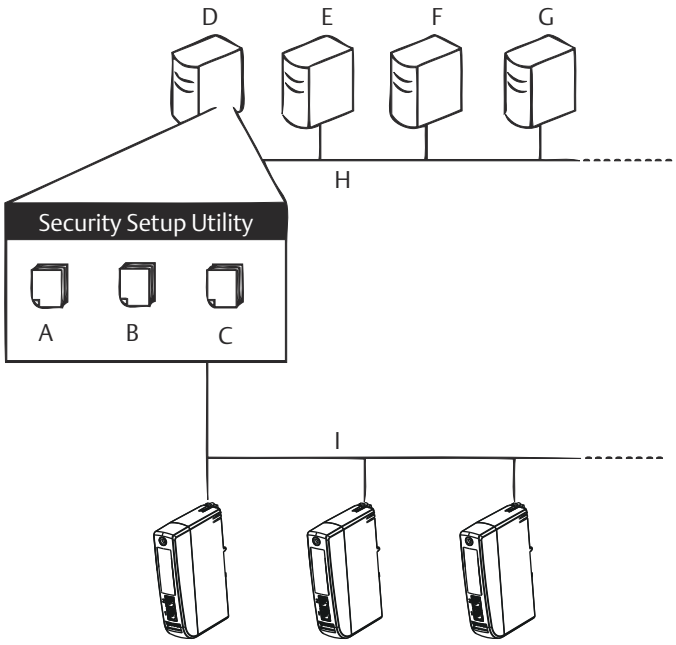
Note
If the autorun function is disabled on the PC, or installation does not begin automatically, double click **D:\SETUP.EXE**(where D is the CD/DVD drive on the PC) and select **OK**.

4.4 Security Setup Utility

The Gateway provides significant flexibility by offering many different interface options. Users should be aware that with this flexibility comes certain risks. Opening the non-secure versions of an industrial protocol can expose significant information, some of it sensitive, about the wireless network. For this reason, Emerson encourages end users to use Emerson's Security Setup Utility to secure the industrial protocols. Users running non-secure versions of the industrial protocols are encouraged to make sure the Gateway is running on a secure network and following security best practices.

The Security Setup Utility enables secure communications between the Gateway and host system, asset management software, data historians, or other applications. This is done by encrypting the standard data protocols (AMS Wireless Configurator, Modbus® TCP, and OPC) used by the Gateway and making them available through various proxies within the Security Setup Utility. These proxies can function as a data server for other applications on the control network. The Security Setup Utility can support multiple Gateways at once and each proxy can support multiple client application connects. Figure 4-1 shows a typical system architecture using the Security Setup Utility.

Figure 4-1: Typical Host System Architecture Using Security Setup



A AMS proxy
B Modbus proxy
C OPC proxy
D Data server
E Engineering station
F Asset management
G Historian
H Control network
I Encrypted data

Note
OPC communications requires the use of the Security Setup Utility regardless of whether encryption is required.

4.4.1 Setup

In the Security Setup Utility add a new proxy for each Gateway based on the communication protocol that is being used. For example, add an OPC proxy for each Gateway that is communicating OPC.

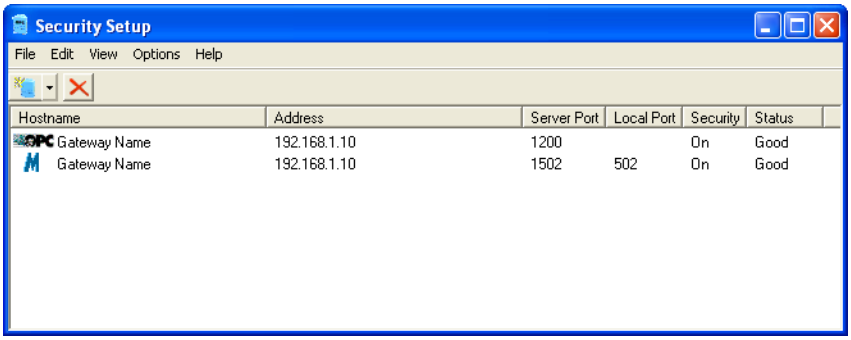
Use the following procedure to add a new proxy in the Security Setup Utility:

Procedure

1. Open the **Security Setup** Utility.
2. Select **EDIT** → **NEW**, then select the type of new proxy to be added.
3. Right click on the new proxy entry and select **Properties**.
4. Enter the target Gateway's **Hostname** and **IP Address**.
5. Select **OK**.
6. Select **FILE** → **SAVE**.
7. When prompted for authentication, enter the admin password for the target Gateway.
8. Select **OK**.
9. Repeat Step 2-Step 8 to added additional proxies.
10. Select **FILE** → **EXIT** to close the *Security Setup* Utility.

    During this process the Gateway will exchange security certificates (digital signatures) with the proxy.

Figure 4-2: Security Setup Utility



4.5 AMS Wireless Configurator

AMS Wireless Configurator helps deploy and configure wireless field devices. It provides an integrated operating environment that leverages the full capabilities of *Wireless*HART®,

including embedded data trending, charting, and graphical display capabilities provided by enhanced EDDL technology.

- Display and modify device configuration
- View device diagnostics
- View process variables
- Provision a wireless device using the drag-and-drop operation so it can join a Gateway's self-organizing network
- Enhance AMS Wireless Configurator functionality with the AMS Wireless SNAP-ON Application
- Restrict access to AMS Wireless Configurator functions through the use of security permissions

See the release notes for information specific to the current release of AMS Wireless Configurator. To display the release notes, select **START** → **PROGRAMS** → **AMS WIRELESS CONFIGURATOR** → **HELP**.

4.5.1 Setup

AMS Wireless Configurator supports connectivity to a Wireless Network and a HART Modem. Both of these interfaces must be configured through the Network Configuration application. To run this application, select **START** → **PROGRAMS** → **AMS DEVICE MANAGER** → **NETWORK CONFIGURATION**.

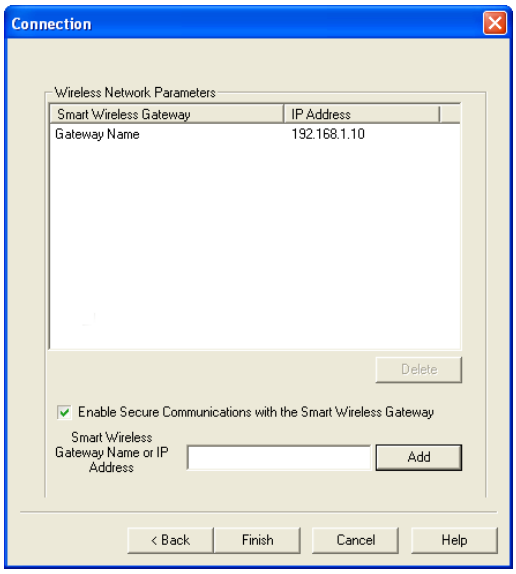
Note
Do not have the Security Setup Utility running at the same time as the Network Configuration application or else a configuration error might occur.

Use the following procedure to configure a wireless network for AMS Wireless Configurator:

Procedure

1. Open the **Network Configuration** application.
2. Select **Add...**
3. Select **Wireless Network** and select **Install...**
4. Select **Next**.
5. Enter a name for the wireless network and select **Next**.
6. Enter the *HostName* or *IP Address* for the Gateway and select **Add**.
7. Repeat Step 6 if multiple Gateways need to be added.
8. Check the box to *Enable Secure Communications* with the Smart Wireless Gateway.
9. Select **Finish** to close the configuration window.
10. Select **Close** to exit the Network Configuration application.

Figure 4-3: Wireless Network in the Network Configuration



Use the following procedure to configure a HART modem for AMS Wireless Configurator:

11. Open the **Network Configuration** application.
12. Select **Add...** This is shown in Figure 4-3.
13. Select **HART modem** and select **Install...**
14. Select **Next**.
15. Enter a name for the HART modem and select **Next**.
16. Select the *HART master type*(default is that AMS Wireless Configurator will be the Primary HART master) and select **Next**.
17. Select the **COM port** for the HART modem and select **Next**.
18. Check the box to *Check* to support Multi Drop *devices*.
19. Check the box to *Include WirelessHART* Adapter.
20. Select **Finish** to close the configuration window.
21. Select **Close** to exit the Network Configuration application.

4.6 Licensing and credits

The latest licensing agreements are included on each disk of the software pack.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes software written by Eric Young (eay@cryptsoft.com).

5 Operation and Maintenance

5.1 Overview

This section describes how to connect the Emerson Smart Wireless Gateway 1410 to a host system and integrate data gathered from the field device network. It covers network architectures, security, and data mapping.

In accordance with Emerson *Wireless*HART® security guidelines, the Gateway should be connected to the host system via a LAN (Local Area Network) and not a WAN (Wide Area Network)

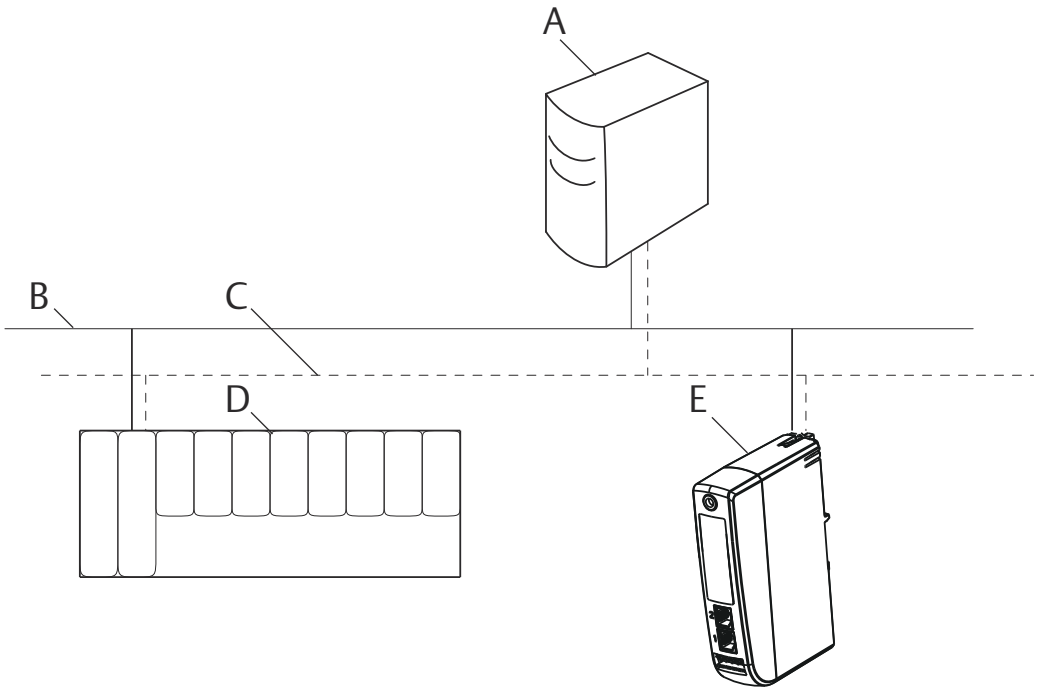
5.2 Network architecture

Physical connection types are important when determining the network architecture and what protocols can be used for integration. Ethernet is the primary physical connection type and RS485 is available an optional connection type. The following network architecture diagrams will help when integrating data from the Gateway into the host system.

Ethernet

An Ethernet connection supports Modbus® TCP, OPC, AMS™ Wireless Configurator, EtherNet/IP™, and HART® TCP protocols. Using this connection type, the Gateway is wired directly to a control network (see Figure 5-1) using a network switch, router, or hub. Often there are two networks for redundancy purposes.

Figure 5-1: Ethernet Architecture

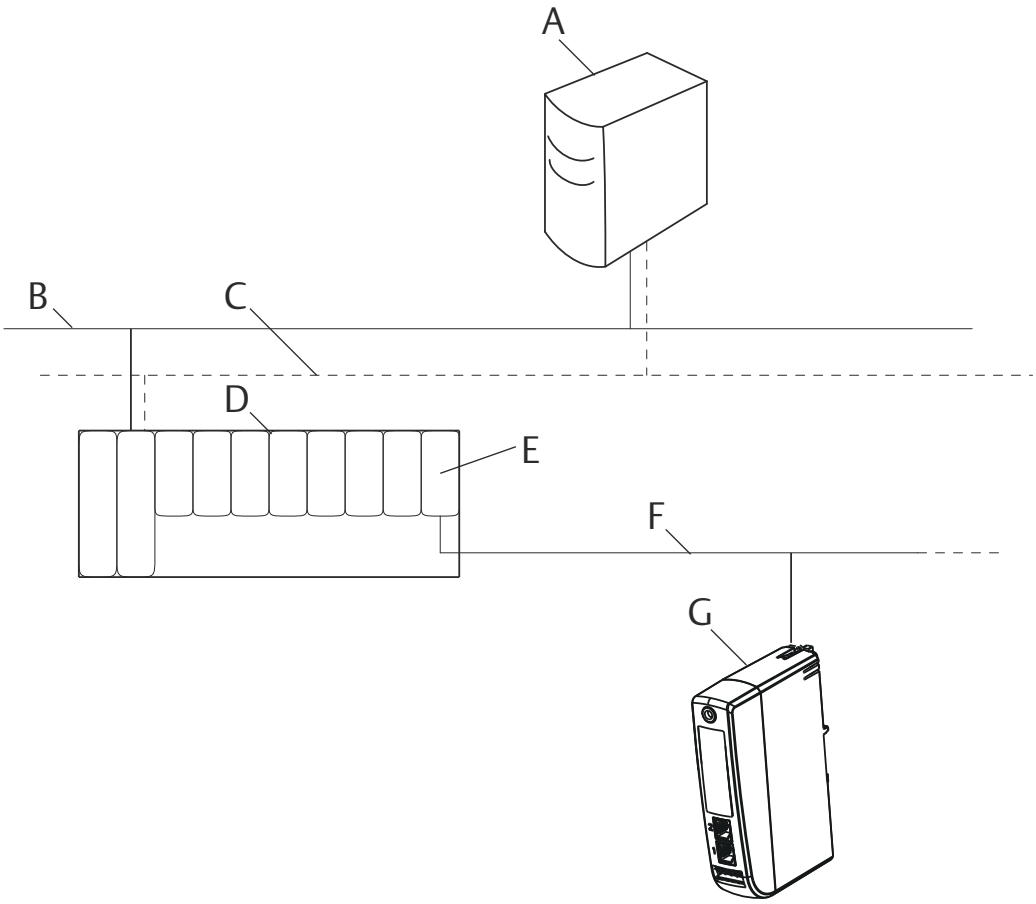


A	Engineering station
B	Primary control network
C	Secondary control network
D	Controller and I/O
E	Smart Wireless Gateway

RS485 (serial)

An RS485 connection supports Modbus RTU protocol. Using this connection type, the Gateway is wired to an RS485 bus which typically leads to a serial I/O card or Modbus I/O card (see Figure 5-2). Up to 31 Gateways can be connected to a single I/O card in this manner.

Figure 5-2: RS485 Architecture



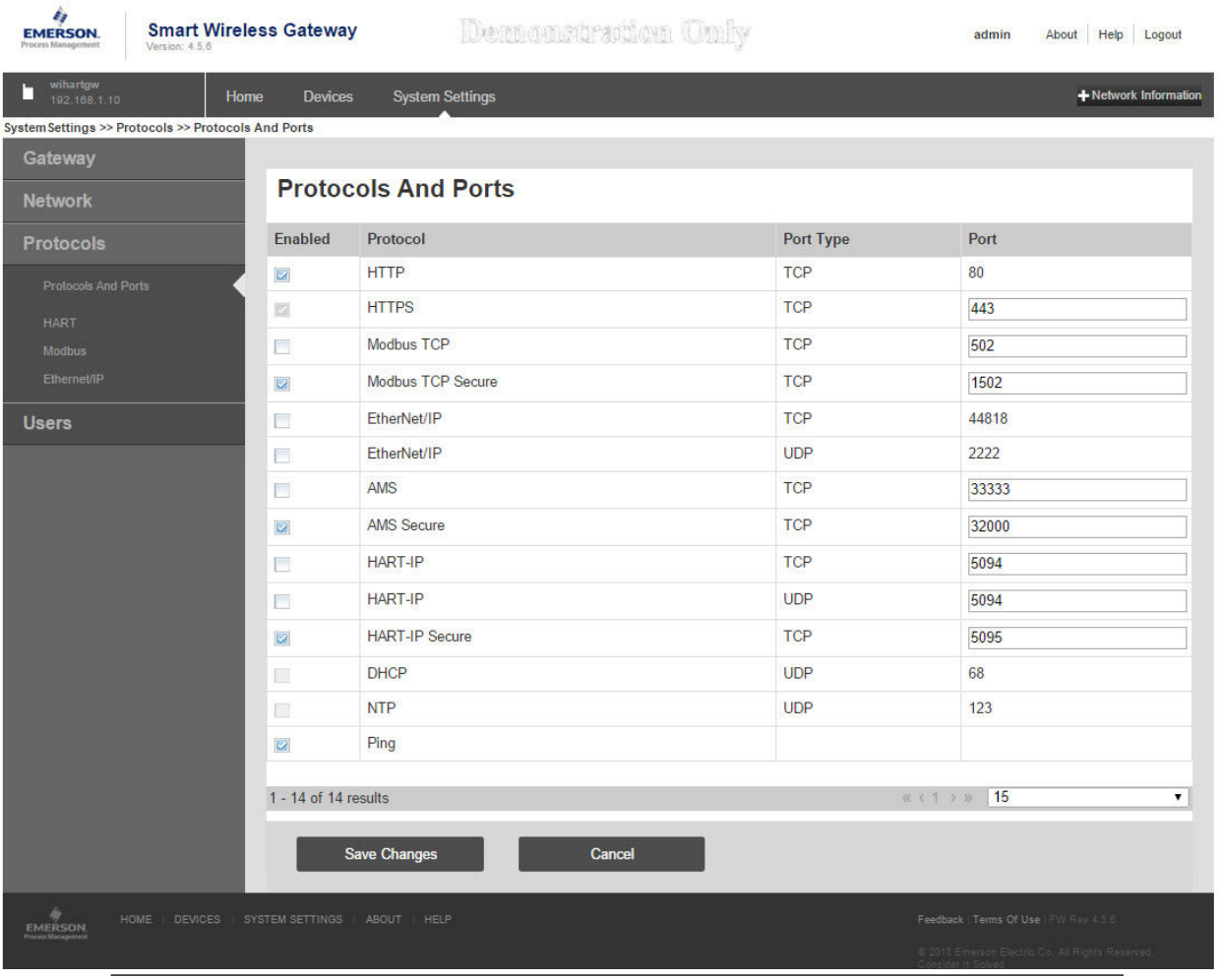
A	Engineering station
B	Primary control network
C	Secondary control network
D	Controller and I/O
E	Serial I/O card
F	RS485 bus
G	Smart Wireless Gateway

5.3 Internal firewall

The Gateway supports an internal firewall that inspects both incoming and outgoing data packets. TCP ports for communication protocols are user configurable, including user specified port numbers and the ability to disable ports.

The Gateway's internal firewall settings can be found by navigating to **System Settings** → **Protocols** → **Protocols And Ports**.

Figure 5-3: Security Protocols Page (Internal Firewall)



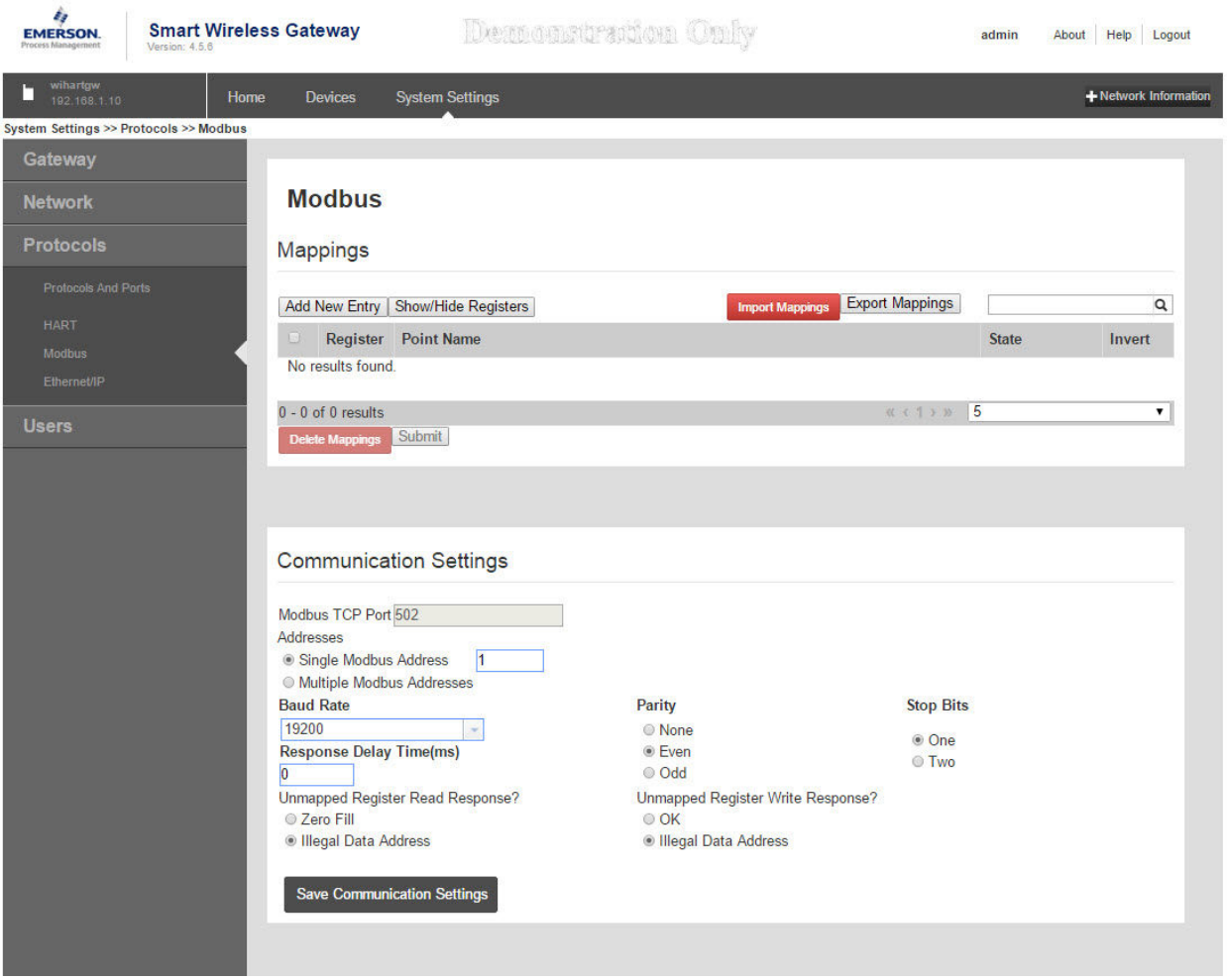
5.4 Modbus

The Gateway supports both Modbus RTU over the RS-485 serial port and Modbus TCP over Ethernet. It functions as a sub device on the Modbus network and must be polled by a Modbus master or client (host system).

5.4.1 Communication settings

It is import that the Modbus communication settings in the Gateway match the settings in the Modbus master or client. Refer to host system documentation for more information on how to configure these settings. The Modbus communication settings can be found by navigating to **System Settings → Protocols → Modbus**.

Figure 5-4: Modbus Communications Page



One Modbus Address: When this option is selected, this address is used by the Gateway for Modbus RTU communications.

Multiple Modbus Addresses: When this option is selected, a new column for address will appear on the Modbus mapping page.

Modbus TCP Port: This is the TCP/IP port the Gateway uses for Modbus TCP (Ethernet). To change TCP/IP port settings, see the Internal Firewall section for more details.

Baud Rate: The data rate or speed of serial communications. This setting is only required for Modbus RTU.

Parity: This setting determines parity (none, even, or odd) to use for error checking purposes. This setting is only required for Modbus RTU.

Stop Bits: This setting determines the number (1 or 2) of stop bits to use when ending a message. This setting is only required for Modbus RTU.

Response delay time (ms): This setting determines how long (ms) the Gateway waits before responding to a Modbus request. This setting is only required for Modbus RTU.

Unmapped register read response?: This is the value returned by the Gateway if the Modbus master requests a register with no data assigned to it (empty register). It is recommended this be set to zero fill to prevent errors.

Floating point representation: This setting determines if the Gateway uses floating point values or integer values. There are three options for this setting.

- Float: This option uses 32-bit floating point values.
- Round: This option rounds the data value to the nearest whole number.
- Scaled: This option uses scaled integers to offset negative values or increase decimal point resolution. The equation for scaled integers is:

y = Ax - (B - 32768)

Where:

y = Scaled integer returned by the Gateway

A = Gain for scaled integer value

x = Measured value from wireless field device

B = Offset for scaled integer value

Use swapped floating point format?: This setting switches which register is sent first for a floating point value. This setting is only used for floating point values.

Incorporate value's associated status as error?: This setting will cause the Gateway to report a predetermined value when a communications or critical diagnostic error is received from the wireless field device. The value is user configurable depending on which floating point representation is chosen. See Value reported for error below.

Value reported for error (floating point): This setting determines what value is reported if the wireless field device reports a failure or stops communicating to the Gateway. This setting is used for floating point values. The choices are NaN (not a number), +Inf (positive infinity), -Inf (negative infinity), or Other (user specified).

Value reported for error (rounded and native integer): This setting determines what value is reported if the wireless field device reports a failure or stops communicating to the Gateway. This setting is used for rounded or scaled integers. The choice is a user specified value between -32768 and 65535.

Scaled floating point maximum integer value: This determines the maximum integer value for the purpose scaling integers. 999-65534

Use global scale gain and offset?: This setting determines if a global gain and offset is applied for scaled integers or if each value has a unique gain and offset. Unique gain and offsets are found on the Modbus Mapping page.

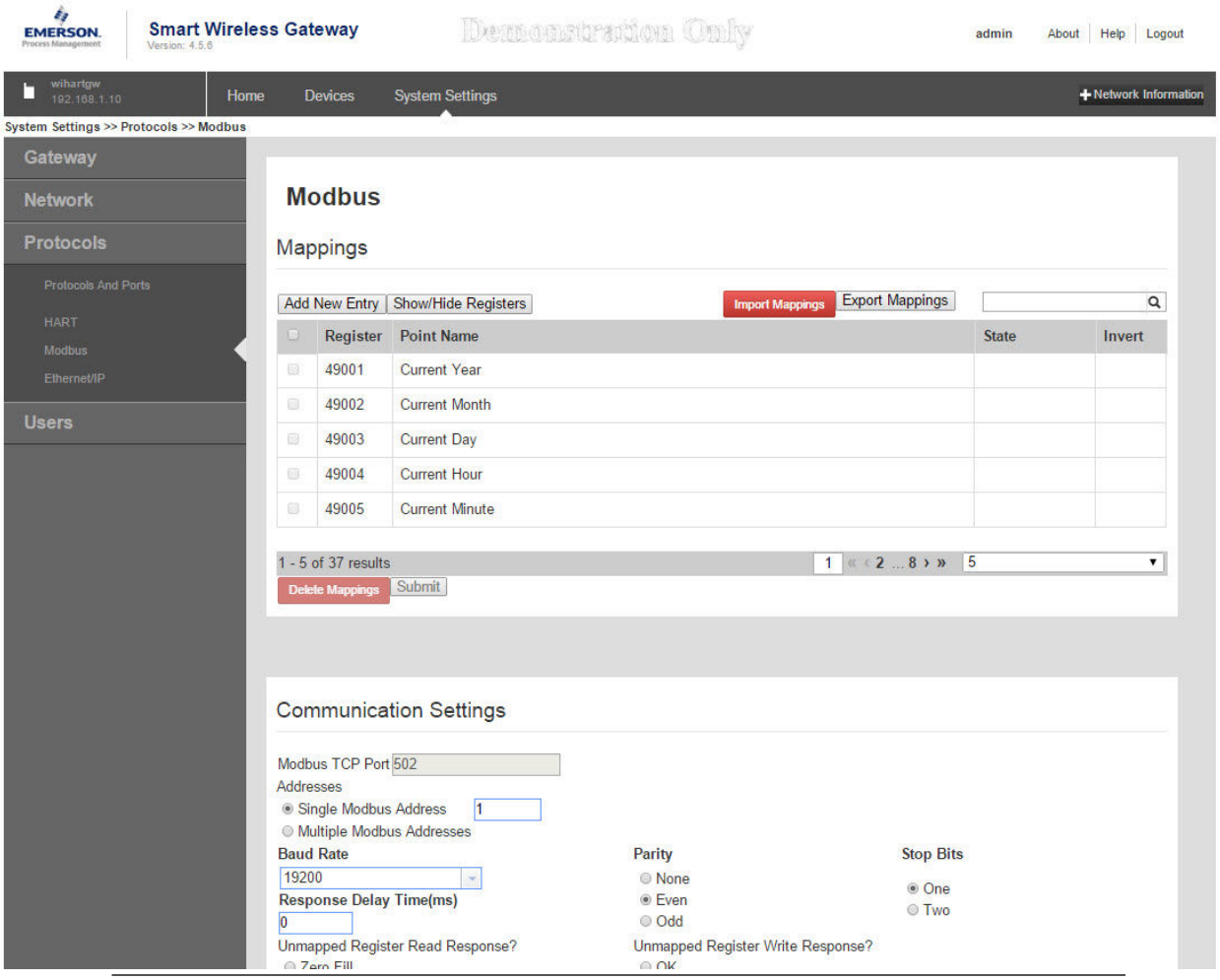
Global scale gain: This value is multiplied to the data values for the purpose of scaling integers. If global scaling is not selected, a gain value will be available for each separate data value on the Modbus Mapping page.

Global scale offset: This value is added to the data values for the purpose of scaling integers. If global scaling is not selected, an offset value will be available for each separate data value on the Modbus Mapping page.

5.4.2 Register mapping

Register Mapping is the process of assigning data points from wireless field devices to Modbus registers. These registers can then be read by a Modbus master or client. Modbus register mapping can be found by navigating to **System Settings** → **Protocols** → **Modbus**.

Figure 5-5: Modbus Register Map Page



To add a new data point to the Modbus register map:

Procedure

1. Select **New entry**.
2. Complete all of the table entries for the new data point (note that the entry columns may vary based on the Modbus communications settings).

3. Repeat for each new data point.
4. Select **Submit**.
5. When changes have been accepted, select **Return to form**.

Address: This is the Modbus RTU address used by the Gateway for this data point. It is possible to group data points assigning them the same address (i.e. all data points from the same process unit can have the same address). This column only appears if Multiple Modbus Addresses is selected on the Modbus Communications page.

Register: This is the Modbus register number used for this data value. Modbus registers hold two bytes (16 bits) of information; therefore 32-bit floats and integers require two Modbus registers. Each data point needs a unique Modbus register number, unless they are assigned different addresses. Register numbers 0-19999 are reserved for Boolean (bit, coil, binary, etc...) values. Register numbers 20000+ are reserved for floating point or integer values.

Point Name: This is a two-part name for the data point. The first part is the HART Tag of the wireless field device which is producing the data. The second part is the parameter of the wireless field device.

Point Name is entered as <HART Tag.PARAMETER>. Point Name can be entered using the list of values (...) or manually entered. The following table gives a list of standard device parameters which may be considered for Modbus register mapping.

Table 5-1: Device parameters available

Parameter	Description	Data type
PV	Primary Variable	32-bit float
SV	Secondary Variable	32-bit float
TV	Tertiary Variable	32-bit float
QV	Quaternary Variable	32-bit float
RELIABILITY	A measure of connectivity to the Gateway	32-bit float
ONLINE	Wireless communications status	Boolean
PV_HEALTHY	Health status for PV	Boolean
SV_HEALTHY	Health status for SV	Boolean
TV_HEALTHY	Health status for TV	Boolean
QV_HEALTHY	Health status for QV	Boolean

PV, SV, TV, and QV (dynamic variables) will vary by device type. Refer to the device's documentation for more information on what value is represented by each dynamic variable.

RELIABILITY and ONLINE relate to wireless communications. RELIABILITY is the percentage of messages received from the wireless field device. ONLINE is a true/false indication of whether the device is communicating on the wireless network.

_HEALTHY parameters are a true/false indication of the health of a particular variable (= dynamic variable – PV, SV, etc...). These parameters incorporate critical diagnostics from the wireless field device as well as communication status.

Note
The **_HEALTHY parameters are a great indication of the health and communications status of the data values.

State (state value): The value of a data point which drives a Modbus output of 1. For example, if a data point is reported as either True or False, a state value of True will report a 1 for True and 0 for False. A state of False will report a 0 for True and a 1 for False. State is only required for register numbers 0-19999 (Boolean, bit, coil, binary, etc...).

Invert: This check box will invert the Modbus output from a 1 to a 0 or a 0 to a 1. Invert is only used for Boolean values using register numbers 0-19999.

Gain: This value is multiplied to the data value for the purpose of scaling integers. Gain is only required if scaled is chosen on the Modbus communications page and globe gain and offset is not chosen.

Offset: This value is added to the data value for the purpose of scaling integers. Offset is only required if scaled is chosen on the Modbus communications page and globe gain and offset is not chosen.

Predefined Modbus registers

In addition to user configurable parameters, the Gateway also supports a list of predefined Modbus registers with diagnostics and test parameters. The following table is a list of the predefined Modbus registers.

Table 5-2: Predefined Modbus Registers

Description	Register	Data type
Current Year (1)	49001	32-bit int
Current Month (1)	49002	32-bit int
Current Day (1)	49003	32-bit int
Current Hour (1)	49004	32-bit int
Current Minute (1)	49005	32-bit int
Current Second (1)	49006	32-bit int
Messages Received	49007	32-bit int
Corrupt Messages Received	49008	32-bit int
Messages Sent With Exception	49009	32-bit int
Messages Sent Count	49010	32-bit int
Valid Messages Ignored	49011	32-bit int
Constant Float 12345.0	49012	32 float
SYSTEM_DIAG.HART_DEVICES	49014	32-bit int
SYSTEM_DIAG.ADDITIONAL_STATUS_0	49015	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_1	49016	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_2	49017	8-bit unsigned int

Table 5-2: Predefined Modbus Registers *(continued)*

Description	Register	Data type
SYSTEM_DIAG.ADDITIONAL_STATUS_3	49018	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_4	49019	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_5	49020	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_6	49021	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_7	49022	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_8	49023	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_9	49024	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_10	49025	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_11	49026	8-bit unsigned int
SYSTEM_DIAG.ADDITIONAL_STATUS_12	49027	8-bit unsigned int
SYSTEM_DIAG.UNREACHABLE	49028	32-bit int
SYSTEM_DIAG.UPTIME	49029	32-bit int
SYSTEM_DIAG.TEST_BOOLEAN	49031	Boolean
SYSTEM_DIAG.TEST_BYTE	49032	8-bit int
SYSTEM_DIAG.TEST_UNSIGNED_BYTE	49033	8-bit unsigned int
SYSTEM_DIAG.TEST_SHORT	49034	16-bit int
SYSTEM_DIAG.TEST_UNSIGNED_SHORT	49035	16 -bit unsigned int
SYSTEM_DIAG.TEST_INT	49036	32-bit int
SYSTEM_DIAG.TEST_UNSIGNED_INT	49038	32-bit unsigned int
SYSTEM_DIAG.TEST_FLOAT	49040	32-bit float

5.5 EtherNet/IP

5.5.1 Communication settings

It is important that the EtherNet/IP communication settings in the Gateway match the setting in the EtherNet/IP master or client. Refer to the host system documentation for more information on how to configure these settings, or to the reference manual for the EtherNet/IP (document number 00809-0500-4420). The EtherNet/IP communication settings can be found by navigating to:

System Settings → Protocols → Ethernet/IP

Note
EtherNet/IP can be integrated with any approved EtherNet/IP ODVA member. Other protocols such as HART-IP™ are still functional within the Gateway. Consult the Product Data Sheet (document number 00813-0200-4420) for ordering options.

Figure 5-6: EtherNet/IP Communications Page

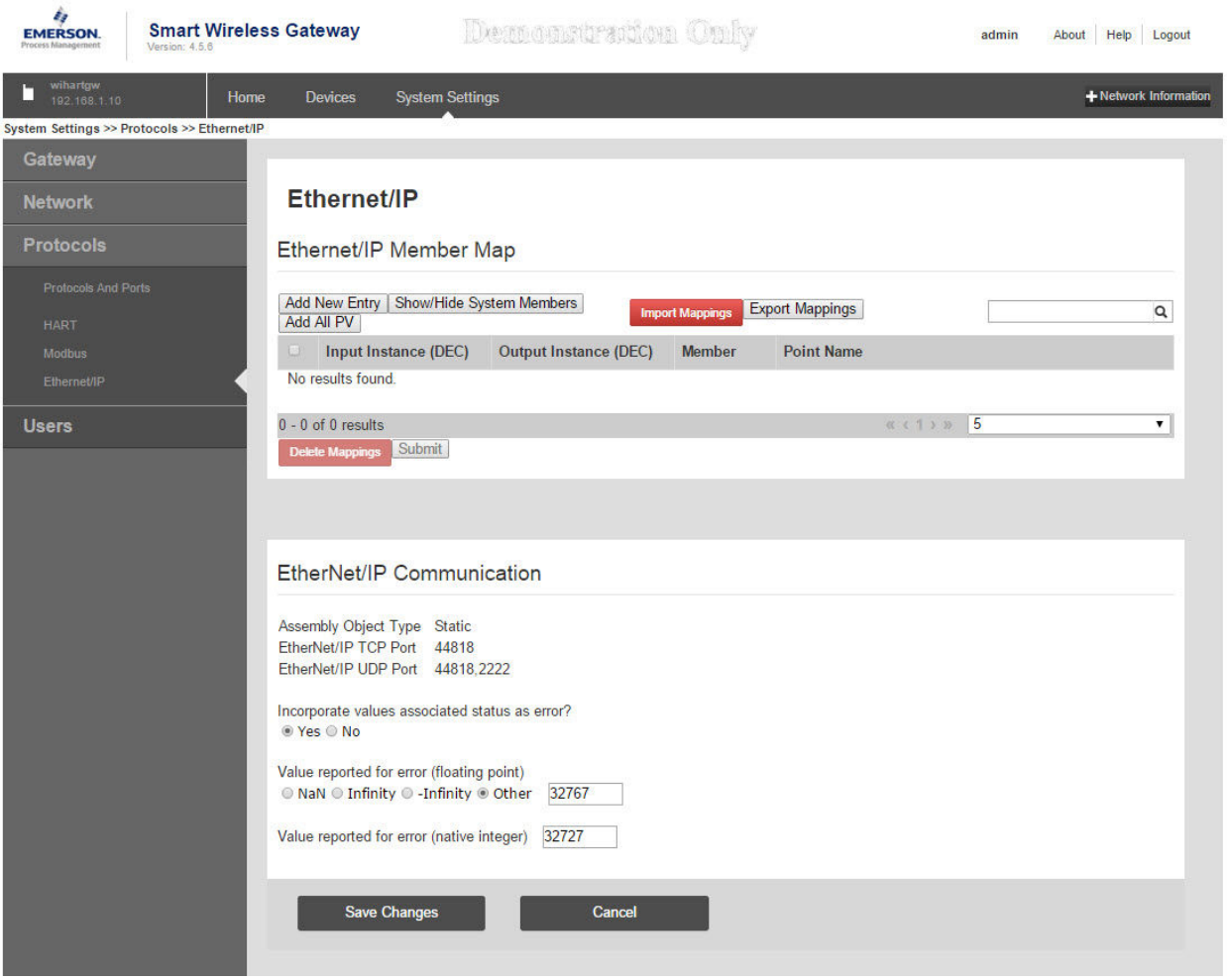


Table 5-3: System Settings → Protocols → Ethernet/IP

Terms	Description
Assembly Object Type	EtherNet/IP use Static assembly object.
EtherNet/IP TCP Port	The TCP Port used to access EtherNet/IP TCP data directly from the Gateway.
EtherNet/IP UDP Ports	The UDP Ports used to access EtherNet/IP UDP data directly from the Gateway.
Incorporate value's associated status as error?	If the HART variable status indicates a critical failure or if there is a loss of communications, it will be reported through the EtherNet/IP member.
Value reported for error (floating point)	Chooses what value is reported if the value's associated status indicates a critical failure. Only used if the Gateway is using float representation

Table 5-3: System Settings → Protocols → Ethernet/IP *(continued)*

Terms	Description
NaN	Not a number is reported if the value's associated status indicates a critical failure.
+Inf	Positive infinity is reported if the value's associated status indicates a critical failure.
-Inf	Negative infinity is reported if the value's associated status indicates a critical failure.
Other	User defined value is reported if the value's associated status indicates a critical failure.
Value reported for error (native integer)	User defined value is reported if the value's associated status indicates a critical failure. Only used if the Gateway is using integer representation.
Unmapped parameter read response	This is the value returned by the Gateway if the EtherNet/IP master requests a register with no data assigned to it (empty register). It is recommended this be set to zero fill to prevent errors.
Parameter mapping	Register Mapping is the process of assigning data points from wireless field devices to EtherNet/IP registers. These registers can then be read by a EtherNet/IP master or client. EtherNet/IP register mapping can be found by navigating to **System Settings → Protocols → Ethernet/IP**.

Figure 5-7: EtherNet/IP Register Map Page

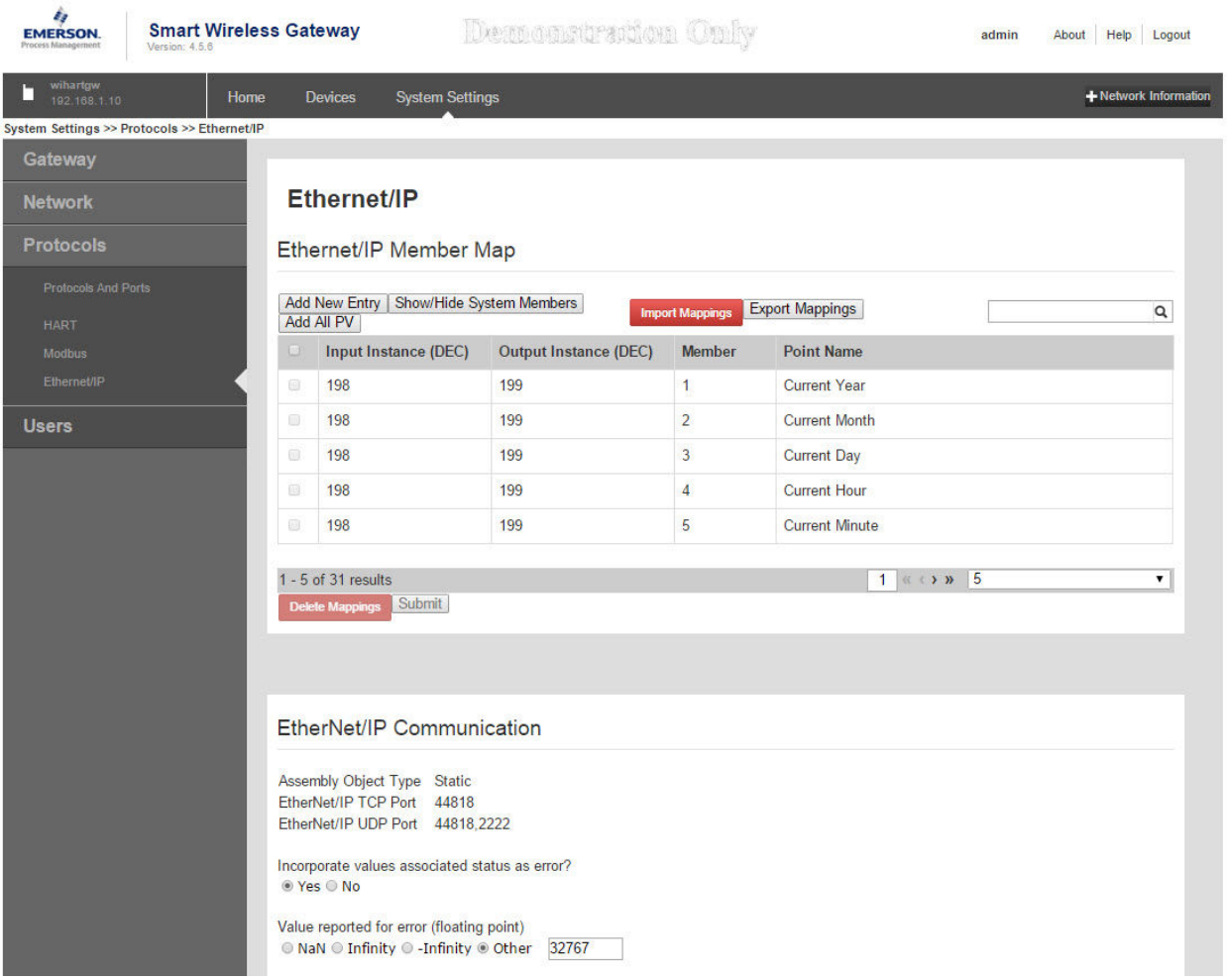


Table 5-4: Summary of Terms Used for EtherNet/IP Mapping Page

Terms	Description
Input Instance	EtherNet/IP Input Static Assembly Instance - 496 bytes
Output Instance	EtherNet/IP Output Static Assembly Instance - 496 bytes
Member	EtherNet/IP Instance Member in which data will get produced or consumed
Point Name	Assigned data point in the format HARTtag.parameter
New entry	Creates a new entry in this table
<<First	Navigates to the first page of this table
<<Previous	Navigates to the previous page of this table
Search	Finds the next occurrence of the characters entered into this field
Next>>	Navigates to the next page of this table

Table 5-4: Summary of Terms Used for EtherNet/IP Mapping Page *(continued)*

Terms	Description
Last>>	Navigates to the last page of this table
Terms	Description
Delete Selected	Removes the selected entry from this table
Select All	Selects all table entries
Select None	Deselects all table entries
Select Errors	Selects all table entries that have an error message
Submit	Accepts all changes (highlighted in yellow)

To add a new data point to the EtherNet/IP register map:

Procedure

1. Select **New** entry.
2. Complete all of the table entries for the new data point (note that the entry columns may vary based on the EtherNet/IP communications settings).
3. Repeat for each new data point.
4. Select **Submit**.
5. When changes have been accepted, select **Return to form**.

   See Table 5-1 for options of parameters that can be mapped.

6 Troubleshooting

6.1 Service support

This section provides basic troubleshooting tips for the Emerson Smart Wireless Field Network. To receive technical support by phone:

Global Service Center

Software and Integration support

United States-1 800 833 8314

International-63 2 702 1111

Customer Central

Technical support, quoting, and order-related questions

United States-1 800 999 9307 (7:00 am to 7:00 pm CST)

Asia Pacific-65 6777 8211

Europe/Middle East/Africa-49 (8153) 9390

Or email the wireless specialists at: Specialists-Wireless.EPM-RTC@EmersonProcess.com

6.2 Initial connection: Web browser returns "page not found"

Possible cause: Incorrect IP address

Recommended actions

1. Connect the Gateway and PC/laptop.
2. Verify the Gateway is properly powered, 24 VDC (nominal) and 250 mA.
3. Verify the IP address for the Gateway (default primary port is 192.168.1.10, default secondary port is 192.168.2.10 or for DeltaV™ Ready Gateway's default primary port is 10.5.255.254, default secondary port is 10.9.255.254).
4. Verify the IP address of the PC/laptop is in the same subnet range as the Gateway (i.e. If the Gateway IP is 155.177.0.xxx, then the PC/Lap IP address should be 155.177.0.yyy).

Possible cause: Internet proxy settings

Recommended actions

1. Connect the Gateway and PC/laptop.
2. Verify the Gateway is properly powered, 24 VDC (nominal) and 250 mA.
3. Disable Internet browser proxy settings.

6.3 Initial connection: Cannot find Gateway after changing IP address

Possible cause: Incorrect IP address

Recommended actions

1. Verify the IP address of the PC/laptop is in the same subnet range as the Gateway (i.e. If Gateway IP address is 155.177.0.xxx, then PC/laptop IP address should be 155.177.0.yyy).
2. Consider resetting the gateway to factory defaults.

6.4 Initial connection: Cannot find Gateway using secondary Ethernet port

Possible cause: Incorrect IP address

Recommended actions

1. Verify which Ethernet port is being used on the Gateway.
2. Verify the Gateway IP address (default primary port is 192.168.1.10, default secondary port is 192.168.2.10).
3. Verify the IP address of the PC/laptop is in the same subnet range as the Gateway (i.e. If Gateway IP address is 155.177.0.xxx, then PC/laptop IP address should be 155.177.0.yyy).
4. Verify this option was ordered with the Gateway.

6.5 Initial connection: Cannot log into the Gateway

Possible cause: Incorrect credentials

Recommended actions

1. Verify the user name and password (administrator user name is "admin", default password is "default").
2. If unable to connect, consider resetting the Gateway.

6.6 AMS Wireless Configurator: Gateway does not appear in AMS Wireless Configurator

Possible cause: Wireless network interface configuration

Recommended actions

1. Verify the Security Setup Utility is installed on the same PC as AMS Wireless Configurator.
2. Setup a wireless network interface using the Network Configuration application.
3. Verify the wireless network interface is configured for secure Gateway communications.
4. Verify secure/unsecure AMS Wireless Configurator protocol settings in the Gateway.
   a) Log on to the Gateway.
   b) Navigate to **SETUP** → **SECURITY** → **PROTOCOLS**.
5. Restart AMS Wireless Configurator data server.
   a) Right click on ***AMS Wireless Configurator*** server icon in the Windows system tray (lower right corner).
   b) Select **Stop server**.

6.7 AMS Wireless Configurator: Wireless devices do not appear under the Gateway

Possible cause: Devices not connected

Recommended actions

1. Log on to the Gateway and navigate to **EXPLORER**.
2. Right click on wireless network and select **Rebuild hierarchy**.

6.8 AMS Wireless Configurator: Wireless device appears with red HART® symbol

Possible cause: Non-current device support files

Recommended actions

1. Navigate to Emerson's AMS Device Manager product page.
2. Install latest device support files from AMS Wireless Configurator.

6.9 AMS Wireless Configurator: Device configuration items are grayed out

Possible cause: Session timeout

Recommended actions

1. Verify whether current or historical information is being displayed (setting is displayed at the bottom of each device configuration screen). Configuration requires the **Current** setting.
2. Log back into AMS Wireless Configurator.

   For security purposes, a configuration timeout is applied to sessions that have been idle for more than 30 minutes.

6.10 Wireless field devices: Wireless device does not appear on the network

Recommended actions

1. Verify the device has power.
2. Verify the device is within effect communications range.
3. Verify the proper network ID has been entered into the device.

6.11 Wireless field devices: Wireless device appears in the join failure list

Recommended actions

Re-enter the network ID and join key into the device.

6.12 Wireless field devices: Wireless device appears with service denied

Possible cause: Update rate setting

Recommended actions

1. Verify the total number of devices on the network (25 maximum).
2. Go to **SETUP** → **NETWORK** → **BANDWIDTH** and click **Analyze bandwidth**.

   Any changes will require the network to reform.
3. Reduce the update rate for the device.

6.13 Modbus communications: Cannot communicate using Modbus® RTU

Recommended actions

1. Verify the use of RS-485.
2. Verify wiring connections.
3. Verify if termination or a pull up is required.
   a) Verify that Modbus serial communications settings in the Gateway match the Modbus Host settings.
   b) Log on to the Gateway and navigate to **SETUP** → **MODBUS** → **COMMUNICATIONS**.
4. Verify the Modbus address for the Gateway.
5. Verify Modbus register mapping in the Gateway.
   a) Log on to the Gateway and navigate to **SETUP** → **MODBUS** → **MAPPING**.

6.14 Modbus communications: Cannot communicate using Modbus® TCP

Possible cause: Incorrect settings

Recommended actions

1. Verify secure/unsecure Modbus protocol settings in the Gateway.
   a) Log on to the Gateway.
   b) Navigate to **SETUP** → **SECURITY** → **PROTOCOLS**.
2. Verify the Modbus TCP communications settings in the Gateway.
   a) Log on to the Gateway.
   b) Navigate to **SETUP** → **MODBUS** → **COMMUNICATIONS**.
3. Verify Modbus register mapping in the Gateway.
   a) Log on to the Gateway.
   b) Navigate to **SETUP** → **MODBUS** → **MAPPING**.

6.15 Modbus communications: Cannot communicate using secure Modbus® TCP

Recommended actions

1. Verify the Security Setup Utility has been installed.
2. Configure a secure Modbus proxy for the Gateway (see Security setup utility).
3. Verify secure/unsecure Modbus protocol settings in the Gateway
   a) Log on to the Gateway.
   b) Navigate to **SETUP** → **SECURITY** → **PROTOCOLS**.
4. Verify the Modbus TCP communications settings in the Gateway.
   a) Log on to the Gateway.
   b) Navigate to **SETUP** → **MODBUS** → **COMMUNICATIONS**.
5. Verify Modbus register mapping in the Gateway.
   a) Log on to the Gateway.
   b) Navigate to **SETUP** → **MODBUS** → **MAPPING**.

6.16 OPC communications: OPC application cannot find a Gateway OPC server

Possible cause: Incorrect Security Setup Utility installation

Recommended actions

1. Verify the Security Setup Utility has been installed on the same PC as the OPC application.
2. Configure an OPC proxy for the Gateway (see Security setup utility).

6.17 OPC communications: Gateway OPC server does not show any Gateways

Possible cause: Proxy not configured

Recommended actions

Configure an OPC proxy for the Gateway (see Security setup utility).

6.18 OPC communications: Gateway OPC server does not show any data tags

Possible cause: Configuration or settings

Recommended actions

1. Configure the Gateway OPC Browse Tree.
   a) Log on to the Gateway.
   b) Navigate to **SETUP** → **OPC** → **OPC BROWSE TREE**.
2. Verify the connection status for the OPC proxy in the Security Setup Utility.
3. Check to ensure the OPC proxy is configured for secure or unsecure communications.
4. Verify secure/unsecure OPC protocol settings in the Gateway.
   a) Log on to the Gateway.
   b) Navigate to **SETUP** → **SECURITY** → **PROTOCOLS**.
5. Verify network firewall and port settings.

6.19 EtherNet/IP™: Gateway is not publishing the parameters

Possible cause: System integration

Recommended actions

1. Verify connection is established with EtherNet/IP.
   a) Navigate to **SETUP** → **SECURITY** → **PROTOCOLS**.
2. To connect to an Allen-Bradley® system, reference the Integration Manual.

6.20 Return of materials

To expedite the return process outside of North America, contact your Emerson representative.

Within the United States, call the Emerson Response Center toll-free number 1 800 654 7768. The center, which is available 24 hours a day, will assist you with any needed information or materials.

The center will ask for product model and serial numbers, and will provide a Return Material Authorization (RMA) number. The center will also ask for the process material to which the product was last exposed.

⚠ WARNING

Individuals who handle products exposed to a hazardous substance can avoid injury if they are informed of, and understand, the hazard. If the product being returned was exposed to a hazardous substance as defined by OSHA, a copy of the required Material Safety Data Sheet (MSDS) for each hazardous substance identified must be included with the returned goods.

7 Glossary

This glossary defines terms used throughout this manual or those appearing in the Emerson Smart Wireless Gateway web interface.

Term	Definition
Access Control List	A list of all devices that are approved to join the network. Each device will also have a unique join key. Also referred to as a white list.
Active Advertising	An operational state of the network manager that causes the entire wireless field network to send messages looking for new or unreachable devices to join the network.
Baud Rate	Communication speed for Modbus® RTU.
Burst Rate	The interval in which a wireless field device transmits measurement and status data to the Gateway. Same as Update Rate.
Certificate	A digital signature used to authenticate a client/server while using encrypted communications.
Connectivity	Typically refers to a combination of communication statistics and link reliability of a wireless field device. May also refer to the connection between the Gateway and the Host System.
Device ID	A hexidecimal number that provides unique device identification.
DHCP	Dynamic Host Configuration Protocol: Used to automatically configure the TCP/IP parameters of a device.
Domain	A unique designator on the internet comprised of symbols separated by dots such as: this.domain.com
Gateway	Refers to the Smart Wireless Gateway.
HART Tag	The device's electronic tag that the Gateway uses for all host integration mapping. Refers to the HART® long tag (32 characters, used for HART 6 or 7 devices) or the HART message (32 characters, only used for HART 5 wired devices connected via a *Wireless*HART® adapter).
Host Name	A unique designator in a domain associated with the IP address of a device such as: device.this.domain.com. In that example the hostname is device.
HTML	Hyper Text Markup Language: The file format used to define pages viewed with a web browser.
HTTP	Hyper Text Transfer Protocol: The protocol that defines how a web server sends and receives data to and from a web browser.
HTTPS	HTTP over an encrypted Secure Sockets Layer (SSL).
Join Failure	When a wireless field device fails to join the *Wireless*HART network. Most join failures are due to security reasons (missing or incorrect join key, not on access control list, etc.).
Join Key	Hexadecimal security code that allows wireless field devices to join the wireless field network. This code must be identical in the device and the Gateway.

Term	Definition
Latency	The time from when a message leaves a wireless field device until it reaches the Gateway.
Netmask	A string of 1's and 0's that mask out or hide the network portion of an IP address leaving only the host component.
Network I.D.	Numeric code that associates wireless field devices to the Gateway. This code must be identical in the device and the gateway.
Network Manager	Operational function within the Smart Wireless Gateway that automatically handles all device connections and scheduling of wireless data.
NTP	Network Time Protocol. Used to keep the system time synchronized with a network time server.
Path	A wireless connection between two devices in a wireless network. Also referred to as a hop.
Path Stability	A measure of connectivity between two devices in the wireless network. Calculated as the ratio of the number of received messages over the number of expected messages.
Primary Interface	Ethernet 1 or Fiber Optic port that is used for primary host communications.
Private Network/LAN	A local connection between a Smart Wireless Gateway and a PC/laptop. This network is used for commissioning and configuration of the Gateway.
Reliability	A measure of connectivity between the Gateway and a wireless field device. Calculated as the ratio of the number of received messages over the number of expected messages. Takes into account all paths.
RSSI	Received signal strength indication (dBm) for the wireless field device.
Secondary Interface	Ethernet 2 port that is used for backup connection or a maintenance port for local access.
Security Setup Utility	A software application that enables secure communications between the Gateway and host system, asset management software, data historians, or other applications.
Self-Organizing Network	Mesh network technology in which a network manager automatically handles all device connections and scheduling of wireless data.
Service Denied	The device has been denied bandwidth and can not publish its regular updates.
TCP/IP	Transmission Control Protocol/Internet Protocol. The protocol that specifies how data is transmitted over Ethernet.
Update Rate	The interval in which a wireless field device transmits measurement and status data to the Gateway. Same as Burst Rate.
Wireless Field Device(s)	*Wireless*HART field devices that are a part of the wireless field network.
Wireless Field Network	*Wireless*HART network, consisting of Smart Wireless Gateway and multiple wireless field devices.
Wireless Plant Network	Industrial WiFi network, used to integrate the Wireless Field Network into the control network.

A Specifications and Reference Data

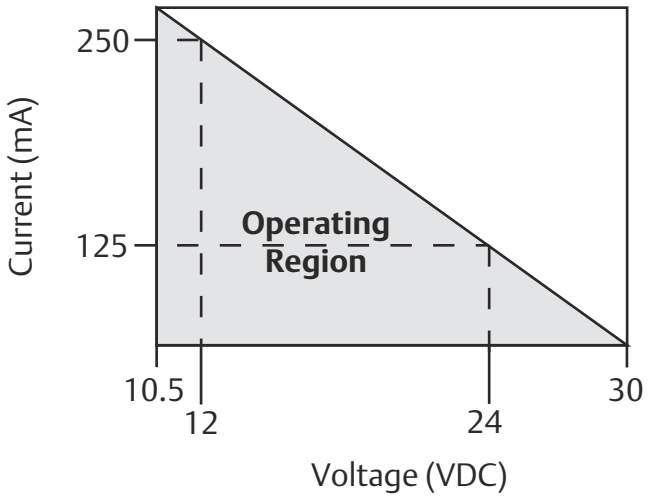
A.1 Functional specifications

A.1.1 Input voltage

10.5-30 VDC Class 2 power supply

A.1.2 Current draw

Operating current draw is based on 3.0 Watt power consumption.



A.1.3 Radio frequency power output from antenna

Maximum of 10 mW (10 dBm) EIRP for WL or WX antenna types

Maximum of 40 mW (16 dBm) EIRP for WN2 high gain option

A.1.4 Environmental

Operating Temperature range: -40 to 167 °F (-40 to 75 °C)

Operating Humidity range: 0-100% relative humidity

A.1.5 EMC performance

Meets all industrial environment requirements of EN61326 and NAMUR NE-21. Maximum deviation <1% span during EMC disturbance.(2)

(2) *During surge event, device may exceed maximum EMC deviation limit or reset; however, device will self-recover and return to normal operation within specified start-up time.*

A.1.6 Antenna options

Optional remote mount omnidirectional antenna

A.1.7 Antenna

2 dBi rubber dipole with SMA connector

SMA connection is female

A.2 Physical specifications

A.2.1 Weight

0.70 lb. (0,318 kg)

A.2.2 Material of construction

Housing

Polymer

A.2.3 Rail mount

Top hat rail EN 50022: 35 mm × 7.5 mm and 35 mm × 15 mm

A.3 Communication specifications

A.3.1 Isolated RS485

2-wire communication link for Modbus® RTU multidrop connections

Baud rate: 57600, 38400, 19200, or 9600

Protocol: Modbus RTU

Wiring: Single twisted shielded pair, 18 AWG. Wiring distance is approximately 4000-ft. (1,524 m)

A.3.2 Ethernet

10/100base-TX Ethernet communication port

Protocols: Modbus TCP, OPC, EtherNet/IP, HART-IP™, https (for Web Interface)

Wiring: Cat5e shielded cable, Wiring distance 328-ft. (100 m)

A.3.3 Modbus

Supports Modbus RTU and Modbus TCP with 32-bit floating point values, integers, and scaled integers. Modbus Registers are user-specified.

A.3.4 OPC

OPC server supports OPC DA v2, v3

A.3.5 EtherNet/IP

Supports EtherNet/IP™ protocol with 32 bit Floating Point values and Integers. EtherNet/IP Assembly Input-Output instances are user configurable. EtherNet/IP specifications are managed and distributed by ODVA. For details on capabilities, see the Smart Wireless Gateway to Allen-Bradley® Integration Manual (document number 00809-0500-4420) on Emerson.com/Rosemount.com.

A.4 Self-organizing network specifications

A.4.1 Protocol

IEC 62591(*Wireless*HART®), 2.4 - 2.5 GHz DSSS.

A.4.2 Maximum network size

25 wireless devices @ 2 seconds or greater

12 wireless devices @ 1 seconds

A.4.3 Supported device update rates

1, 2, 4, 8, 16, 32 seconds or 1 - 60 minutes or greater depending on the device

A.4.4 Network size/latency

25 Devices/ less than 5 sec.

A.4.5 Data reliability

Greater than 99%

A.5 System security specifications

A.5.1 Ethernet

Secure Sockets Layer (SSL) enabled (default) TCP/IP communications

A.5.2 Wireless Gateway access

Role-based Access Control (RBAC) including Administrator, Maintenance, Operator, and Executive. Administrator has complete control of the Gateway and connections to host systems and the self-organizing network.

A.5.3 Self-organizing network

AES-128 Encrypted *Wireless*HART, including individual session keys. Drag and Drop device provisioning, including unique join keys and white listing.

A.5.4 Internal firewall

User Configurable TCP ports for communications protocols, including Enable/Disable and user specified port numbers. Inspects both incoming and outgoing packets.

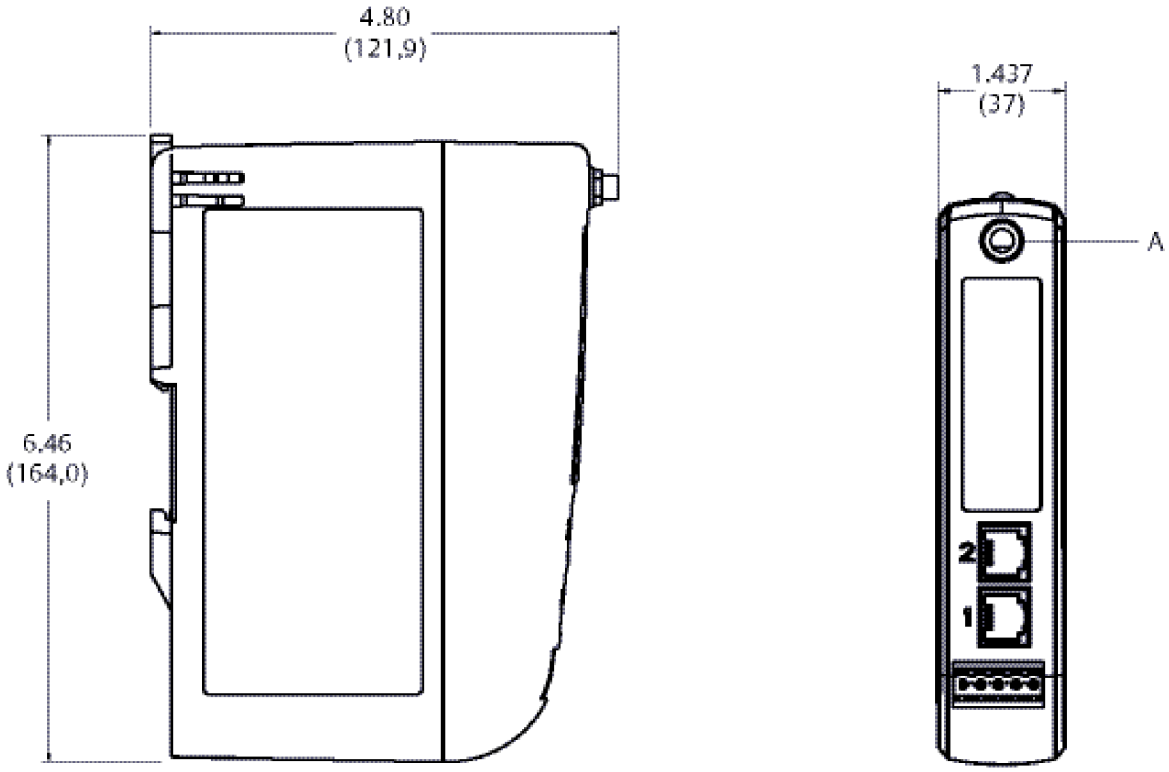
A.5.5 Third party certification

Wurldtech: Achilles Level 1 certified for network resiliency

National Institute of Standards and Technology (NIST): Advanced Encryption Standard (AES) Algorithm conforming to Federal Information Processing Standard Publication 197 (FIPS-197).

A.6 Dimensional drawings

Figure A-1: Smart Wireless Gateway

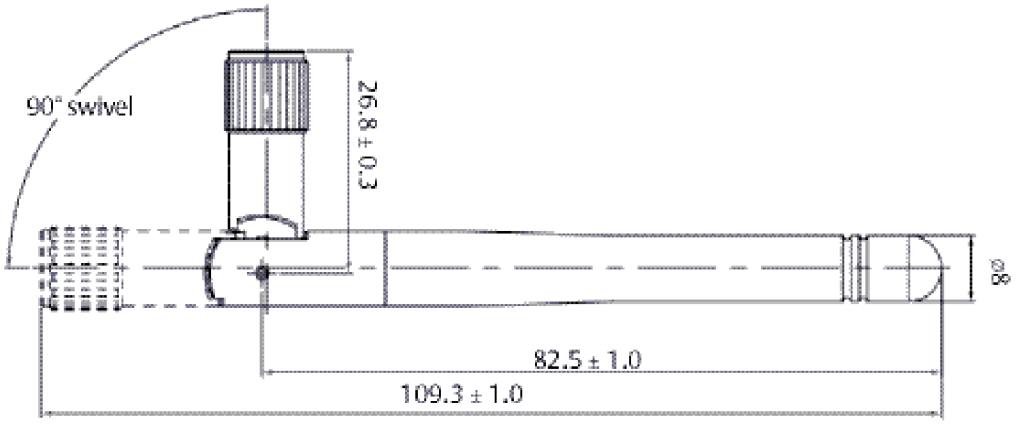


A RF connector on 1410 is an SMA female. Matching RF cable to antenna should be a SMA male.

Note
Allow extra space in front of unit for wiring, antenna connector and antenna cable service loop.

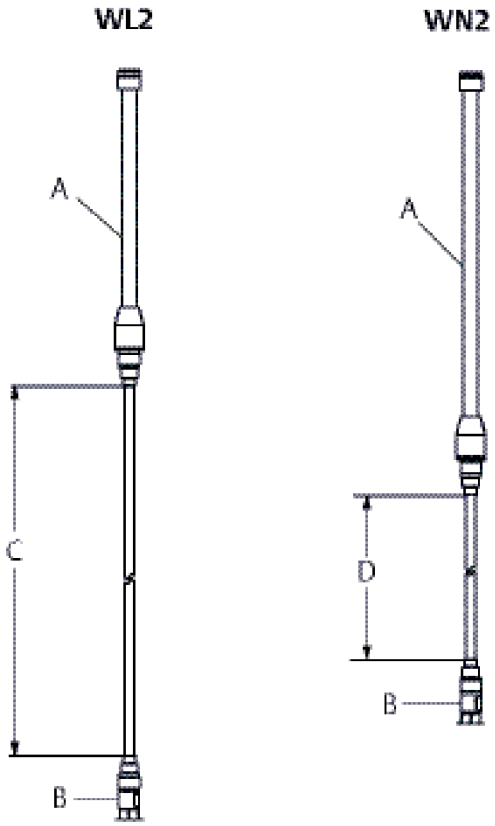
Dimensions are in inches (millimeters).

Figure A-2: WX2 Basic Antenna Dimensions



Dimensions are in millimeters.

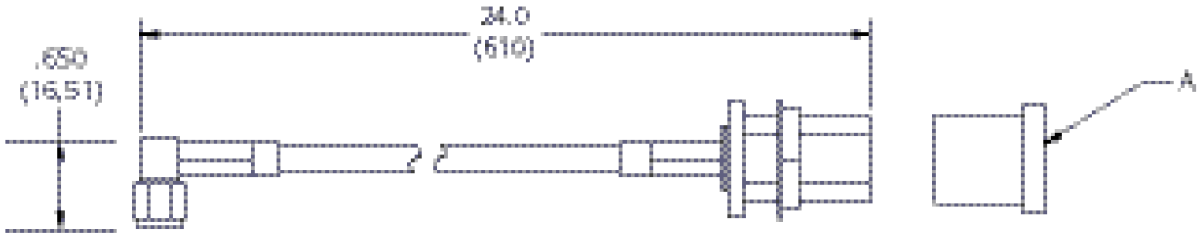
Figure A-3: Remote Omni-Antenna Kit



The remote omni-antenna kit includes sealant tape for remote antenna connection, SMA to N-type adapter cable, mounting brackets for the antenna, and lightning arrester.

A	Antenna
B	Lightning arrestor
C	50-ft. (15,2 m) cable
D	25-ft. (7,6 m) cable

Figure A-4: SMA to N-Type Adapter Cable



A	End cap

Dimensions are in inches (millimeters).

A.7 Ordering information

Table A-1: Smart Wireless Gateway Ordering Information

The Standard offering represents the most common options. The starred options (★) should be selected for best delivery. The Expanded offering is subject to additional delivery lead time.

Model	Product Description	
1410	Smart Wireless Gateway, 2.4 GHz DSSS, WirelessHART, Webserver, AMS™ Ready, HART-IP	
Wireless Configuration		
A	25 Device network (10.5-30 VDC)	★
Ethernet Communications - Physical Connection		
1(1) (2)	Single Ethernet connection	★
2(3) (4)	Dual Ethernet connection	★
Serial Communication		
N	None	★
A(5)	Modbus RTU via RS-485	★
Ethernet Communication - Data Protocols(6)		
D1	Modbus TCP/IP	★
D2	OPC	★
D3	EtherNet/IP	★
D4	Modbus TCP/IP, OPC	★
D5	EtherNet/IP, Modbus TCP/IP	★
D6	EtherNet/IP, OPC	★
E2	Ovation™ Ready	★
E3(7)	Webserver Only	★
Antenna Options(8)		
WX2	Basic antenna	★
WL2	SMA-to-N-Type adapter cable, and remote antenna kit	★
WN2(9)	SMA-to-N-Type adapter cable, and High-Gain remote antenna kit	★
Product Certifications		
NA	No Approvals	★
N5	FM Division 2, Non-incendive	★
N6	CSA Division 2 (Suitable for Canada and the United States)	★

(1) Single active 10/100 baseT Ethernet port with RJ45 connector.
(2) Additional ports disabled.
(3) Dual active 10/100 baseT Ethernet ports with RJ45 connectors.
(4) Multiple active ports have separate IP addresses, firewall isolation, and no packet forwarding.
(5) Convertible to RS232 via adapter, not included with Gateway.

(6) Selection of Dual Ethernet option code 2 is recommended.
(7) Requires (A) Modbus RTU via RS-485 Communication protocol.
(8) The WL2 and WN2 options require minor assembly.
(9) Not available in all countries.

Table A-2: Options

(include with selected model number)

Model	Product Description	
Host Integration(1)		
H6	Allen-Bradley	★
H9	Other	★
Oil and Gas Options		
G	Oil and gas monitor page	★
Typical Model Number: 1410 A 2 D5 WX2 NA		

(1) Support documentation included in the package.

A.8 Accessories and spare parts

Table A-3: Accessories

Item Description	Part Number
AMS Wireless SNAP-ON™, 1 Gateway license	01420-1644-0001
AMS Wireless SNAP-ON, 5 Gateway licenses	01420-1644-0002
AMS Wireless SNAP-ON, 10 Gateway licenses	01420-1644-0003
AMS Wireless SNAP-ON, 5-10 upgrade licenses	01420-1644-0004
Serial port HART modem and cables only	03095-5105-0001
USB port HART modem and cables only	03095-5105-0002

Table A-4: Spare Parts

Item Description(1)	Part Number
Spare kit, WL2 replacement(2), Remote antenna, 50-ft. (15,2 m) cable, and lightning arrestor	01420-1615-0302
Spare kit, WN2 replacement(2), High Gain, Remote antenna, 25-ft. (7.6 m) cable, and lightning arrestor	01420-1615-0402

(1) Does not include SMA to N-type adapter.
(2) Can not upgrade from integral to remote antenna.Replacement Kits must be matched to original antenna type to maintain telecommunication approvals. I.e. WN2 cannot replace a WL2.

B Product Certifications

B.1 European Directive Information

A copy of the EC Declaration of Conformity can be found at the end of the Quick Start Guide. The most recent revision of the EC Declaration of Conformity can be found at www.Emerson.com/Rosemount.

B.2 Telecommunication Compliance

All wireless devices require certification to ensure that they adhere to regulations regarding the use of the RF spectrum. Nearly every country requires this type of product certification. Emerson is working with governmental agencies around the world to supply fully compliant products and remove the risk of violating country directives or laws governing wireless device usage.

B.3 FCC and IC

This device complies with Part 15 of the FCC Rules. Operation is subject to the following conditions: This device may not cause harmful interference. This device must accept any interference received, including interference that may cause undesired operation. This device must be installed to ensure a minimum antenna separation distance of 20 cm from all persons.

B.4 Ordinary Location Certification

As standard, the transmitter has been examined and tested to determine that the design meets the basic electrical, mechanical, and fire protection requirements by a nationally recognized test laboratory (NRTL) as accredited by the Federal Occupational Safety and Health Administration (OSHA).

B.5 Installing Equipment in North America

The US National Electrical Code (NEC) and the Canadian Electrical Code (CEC) permit the use of Division marked equipment in Zones and Zone marked equipment in Divisions. The markings must be suitable for the area classification, gas, and temperature class. This information is clearly defined in the respective codes.

B.5.1 USA

N5 U.S.A. Division 2

Certificate 30349590 (FM)

Standards FM Class 3600 – 2011,

FM Class 3611 – 2004,
FM Class 3616 – 2011,
FM Class 3810 – 2005;

Markings NI CL 1, DIV 2, GP A, B, C, D T4; Suitable for use in CL II, III, DIV 2, GP F, G T4; T4(-40 °C ≤ T_a ≤ 60 °C)

Special Conditions for Safe Use(X)

1. When installed as Division 2 equipment, the Model 1410 Smart Wireless Gateway shall be mounted within a tool-secured enclosure which meets the requirements of ANSI/ISA 61010-1 and be capable of accepting the applicable wiring methods per the NEC.

B.5.2 Canada

N6 Canada Division 2

Certificate	2646342 (CSA)
Standards	CAN/CSA C22.2 No. 0-10, CSA C22.2 No. 213-M1987 (R2013), CSA C22.2 No. 61010-1 - 2012, ANSI/ISA-12.12.01 - 2012, UL61010-1, 3rd Edition
Markings	Suitable for CL I, DIV 2, GP A, B, C, D; T4 (-40 °C ≤ T_a ≤ 70 °C)

Note

- Shall be powered by a class 2 power supply.
- Suitable for dry indoor locations only.
- Equipment must be installed in a suitable tool accessible enclosure subject to the end use application.
- Using the Emerson 1410D and the Smart Wireless Field Link 781 in a hazardous location requires barriers between the two units.

B.5.3 Europe

N1 ATEX Type n

Certificate	Baseefa14ATEX0125X
Standards	EN 60079-0: 2012, EN 60079-15: 2010
Markings	Ⓔx II 3 G Ex nA IIC T4 Gc, T4(-40 °C ≤ T_a ≤ +75 °C), V_{MAX} = 30 Vdc

Special Conditions for Safe Use(X)

1. The equipment must be installed in an area of not more than Pollution Degree 2 as defined in IEC 60664-1, and in an enclosure that provides a degree of protection of at least IP54 and meets the relevant requirements of EN 60079-0 and EN 60079-15.
2. External connections to the equipment must not be inserted or removed unless either the area in which the equipment is installed is known to be non-hazardous, or the circuits connected have been de-energised.
3. The equipment is not capable of withstanding the 500 V electrical strength test as defined in clause 6.5.1 of EN 60079-15: 2010. This must be taken into account during installation.
4. When fitted, the surface resistivity of the remote antenna is greater than 1 GΩ. To avoid electrostatic charge build up, it must not be rubbed with a dry cloth or cleaned with solvents.

B.5.4 International

N7 IECEx Type n

Certificate	IECEx BAS 14.0067X
Standards	IEC 60079-0: 2011, IEC 60079-15: 2010
Markings	Ex nA IIC T4 Gc, T4(-40 °C ≤ T_a ≤ +75 °C), V_{MAX} = 30 Vdc

Special Conditions for Safe Use(X)

1. The equipment must be installed in an area of not more than Pollution Degree 2 as defined in IEC 60664-1, and in an enclosure that provides a degree of protection of at least IP54 and meets the relevant requirements of EN 60079-0 and EN 60079-15.
2. External connections to the equipment must not be inserted or removed unless either the area in which the equipment is installed is known to be nonhazardous, or the circuits connected have been de-energised.
3. The equipment is not capable of withstanding the 500 V electrical strength test as defined in clause 6.5.1 of EN 60059-15: 2010. This must be taken into account during installation.
4. When fitted, the surface resistivity of the remote antenna is greater than 1 GΩ. To avoid electrostatic charge build-up, it must not be rubbed with a dry cloth or cleaned with solvents.

Note
Currently not available for Emerson 1410D option.

00809-0200-4410
Rev. CA
2020

Emerson Automation Solutions
6021 Innovation Blvd.
Shakopee, MN 55379, USA
+1 800 999 9307 or +1 952 906 8888
+1 952 949 7001
RFQ.RMD-RCC@Emerson.com

North America Regional Office
Emerson Automation Solutions
8200 Market Blvd.
Chanhassen, MN 55317, USA
+1 800 999 9307 or +1 952 906 8888
+1 952 949 7001
RMT-NA.RCCRFQ@Emerson.com

Latin America Regional Office
Emerson Automation Solutions
1300 Concord Terrace, Suite 400
Sunrise, FL 33323, USA
+1 954 846 5030
+1 954 846 5121
RFQ.RMD-RCC@Emerson.com

Europe Regional Office
Emerson Automation Solutions Europe
GmbH
Neuhofstrasse 19a P.O. Box 1046
CH 6340 Baar
Switzerland
+41 (0) 41 768 6111
+41 (0) 41 768 6300
RFQ.RMD-RCC@Emerson.com

Asia Pacific Regional Office
Emerson Automation Solutions
1 Pandan Crescent
Singapore 128461
+65 6777 8211
+65 6777 0947
Enquiries@AP.Emerson.com

Middle East and Africa Regional Office
Emerson Automation Solutions
Emerson FZE P.O. Box 17033
Jebel Ali Free Zone - South 2
Dubai, United Arab Emirates
+971 4 8118100
+971 4 8865465
RFQ.RMTMEA@Emerson.com

Linkedin.com/company/Emerson-Automation-Solutions
Twitter.com/Rosemount_News
Facebook.com/Rosemount
Youtube.com/user/RosemountMeasurement

EMERSON™