

# Smart Wireless Gateway



Wireless**HART**



# Smart Wireless Gateway

## NOTICE

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

Within the United States, Emerson Process Management 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 Process Management representative.

## ⚠ WARNING

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 Process Management Sales Representative.

*PlantWeb is a registered trademark of one of the Emerson Process Management group of companies.*

*Modbus is a registered trademark of Schneider Automation, Inc.*

*All other marks are the property of their respective owners.*



---

# Table of Contents

<b>SECTION 1</b>	Safety Messages . . . . .	1-1
<b>Overview</b>	Introduction . . . . .	1-1
	Manual . . . . .	1-2
	Service Support . . . . .	1-3
	Return of Materials . . . . .	1-3
	Product Recycling/Disposal . . . . .	1-3
<b>SECTION 2</b>	Overview . . . . .	2-1
<b>Initial Connection</b>	System Requirements . . . . .	2-2
	Initial Setup . . . . .	2-2
<b>SECTION 3</b>	Overview . . . . .	3-1
<b>Mounting and</b>	Mounting . . . . .	3-2
<b>Connection</b>	Remote Antenna (optional) . . . . .	3-4
	Connecting . . . . .	3-5
<b>SECTION 4</b>	Overview . . . . .	4-1
<b>Software Setup</b>	System Requirements . . . . .	4-1
	Software Installation . . . . .	4-2
	Security Setup Utility . . . . .	4-2
	AMS Wireless Configurator . . . . .	4-4
	Licensing and Credits . . . . .	4-6
<b>SECTION 5</b>	Overview . . . . .	5-1
<b>Host Integration</b>	Network Architecture . . . . .	5-1
	Internal Firewall . . . . .	5-3
	Modbus . . . . .	5-4
<b>SECTION 6</b>		
<b>Troubleshooting</b>		
<b>SECTION 7</b>		
<b>Glossary</b>		

# Smart Wireless Gateway

---

<b>APPENDIX A</b>	Functional Specifications . . . . .	A-1
<b>Product</b>	Physical Specifications . . . . .	A-1
<b>Specifications</b>	Communication Specifications . . . . .	A-2
	Self-Organizing Network Specifications . . . . .	A-2
	System Security Specifications . . . . .	A-3
	Dimensional Drawings . . . . .	A-4
	Ordering Information . . . . .	A-6
	Accessories and Spare Parts . . . . .	A-7
<b>APPENDIX B</b>	Approved Manufacturing Locations . . . . .	B-1
<b>Product</b>	Telecommunication Compliance . . . . .	B-1
<b>Certifications</b>	FCC and IC . . . . .	B-1
	Ordinary Location Certification for FM . . . . .	B-1
	European Union Directive Information . . . . .	B-2
<b>APPENDIX C</b>	Overview . . . . .	C-1
<b>Delta V Ready</b>	Requirements . . . . .	C-1
	Mounting and Connecting . . . . .	C-1
	Setup . . . . .	C-2

# Section 1 Overview

---

<b>Safety Messages</b> .....	<b>page 1-1</b>
<b>Introduction</b> .....	<b>page 1-1</b>
<b>Manual</b> .....	<b>page 1-2</b>
<b>Service Support</b> .....	<b>page 1-3</b>
<b>Return of Materials</b> .....	<b>page 1-3</b>
<b>Product Recycling/Disposal</b> .....	<b>page 1-3</b>

---

## SAFETY MESSAGES

Instructions and procedures in this manual may require special precautions to ensure the safety of the personnel performing the operations. Information that potentially raises safety issues is indicated by a warning symbol (⚠). Please refer to these safety messages before performing an operation preceded by this symbol.

### ⚠ WARNING

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

- Make sure only qualified personnel perform the installation.

**Explosions could result in death or serious injury.**

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

**Electrical shock could cause death or serious injury.**

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

## INTRODUCTION

The Smart Wireless Gateway connects WirelessHART™ 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 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 anytime. There is no need to configure communication paths because the Gateway manages the network automatically. This feature also ensures that WirelessHART field devices have the most reliable path to send data.



# Smart Wireless Gateway

---

## What is Included?

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

- Smart Wireless Gateway
- Quick Installation Guide
- Software pack, 2 disk set
- Crossover cable, Ethernet
- Mounting hardware
- Conduit plugs, 4
- Conduit adapters (optional)

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

- Remote mount antenna
- Mounting hardware
- Lightning arrestor
- Cable (1 or 2 pieces that total 50 ft, [15,2 m] in length)
- Weatherproof tape

## MANUAL

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

### Section 1 – Overview

This section 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.

### Section 2 – Initial Connection

This section 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.

### Section 3 – Mounting and Connection

This section 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.

### Section 4 – Software Setup

This section 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.

### Section 5 – Host Integration

This section 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.

### Section 6 – Troubleshooting

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

### Section 7 – Glossary

The glossary defines terms used through out this manual or that appear in the web interface of the Smart Wireless Gateway.



## Appendices

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

## SERVICE SUPPORT

### 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 a.m. to 7:00 p.m. CST)
Asia Pacific	65 6777 8211
Europe/ Middle East/ Africa	49 8153 9390

## RETURN OF MATERIALS

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

Within the United States, call the Emerson Process Management 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.

## PRODUCT RECYCLING/DISPOSAL

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

# Smart Wireless Gateway

---

**Reference Manual**  
00809-0200-4420, Rev CA  
August 2010

## Section 2 Initial Connection

---

Overview .....	page 2-1
System Requirements .....	page 2-2
Initial Setup .....	page 2-2

---

### ⚠ WARNING

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

- Only qualified personnel should perform the installation

Explosions could result in death or serious injury.

- Verify that the operating atmosphere of the transmitter is consistent with the appropriate hazardous locations certifications

Electrical shock could cause death or serious injury.

- 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 20 cm from all persons.

### OVERVIEW

This section 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.

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 needed to complete this section:

- Gateway
- PC/Laptop
- Crossover Cable (supplied with the Gateway)
- 24 Vdc power supply

---

### NOTE

If the Gateway was ordered with the DeltaV™ Ready option, it has been configured to operate on a DeltaV control network, and the Initial Configuration Section does not need to be completed. Only setting the password is required.

---

# Smart Wireless Gateway

---

## SYSTEM REQUIREMENTS

The following requirements apply to the PC/Laptop used to configure the Gateway. Additional requirements may apply if using the optional Security Setup Utility or AMS<sup>®</sup> Wireless Configurator. See Section 4: Software Setup on page 4-1 for more information.

### Web Browser Applications

- Mozilla<sup>®</sup> Firefox<sup>®</sup> 1.5 or higher
- Microsoft Internet Explorer<sup>®</sup> 6.0 or higher

### Ethernet

- 10/100base-TX Ethernet communication protocol

## INITIAL SETUP

### 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. To configure these settings:

1. Find and open the **Control Panel**. (It is generally found from the **Start Menu**.)
2. Open **Network Connections**.
3. Select **Local Area Connection**.
4. Right click the mouse and select **Properties** from the list.
5. Select **Internet Protocol (TCP/IP)**, and choose the **Properties** button.
6. From the *General* tab, select **Use the following IP address** button.
7. Set the **IP Address** to 192.168.1.12 and press the **Tab** button.
8. A **Subnet mask** of 255.255.255.0 should fill in automatically.
9. Click **OK** to close the *Internet Protocol (TCP/IP)* window.
10. Click **Close** on the *Local Area Connection* window.

Internet proxies will need to be disabled through the PC/Laptop's default internet browser.

1. Find and open the default internet browser (typically Microsoft Internet Explorer).
2. Find the **Tools** menu and select **Internet Options**.
3. From the *Connections* tab, click 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. Click **OK** to close the *Local Area Network (LAN) Settings* window.
6. Click **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. Please see Table 2-1 for additional network settings.

---

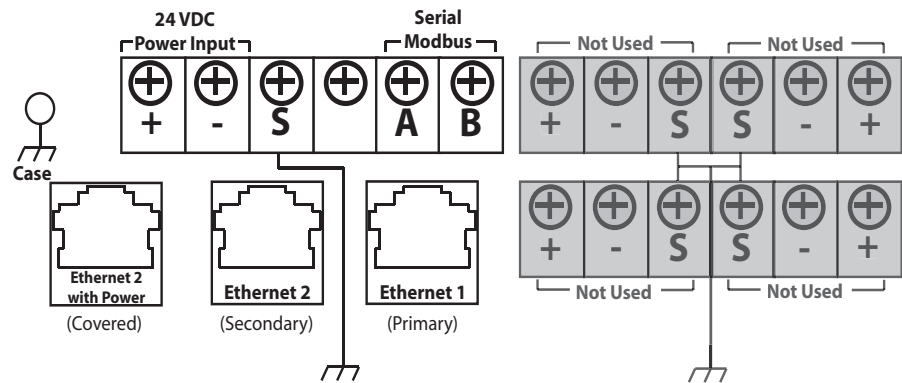
Table 2-1. Default IP Addresses

	Gateway	PC/Laptop
Ethernet 1	<b>192.168.1.10</b>	192.168.1.12
Ethernet 2	<b>192.168.2.10</b>	192.168.2.12
Ethernet 1 (DeltaV Ready)	<b>10.5.255.254</b>	10.5.255.200
Ethernet 2 (DeltaV Ready)	<b>10.9.255.254</b>	10.9.255.200

## Connections and Power

Physically connect the PC/Laptop to the Gateway with the supplied crossover 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. Figure 2-1 shows the standard terminal block diagram. Once the Gateway and PC/Laptop are connected wire a 24 Vdc power supply with a capacity of at least 250 mA to the Gateway power input terminals.

Figure 2-1. Standard Terminal Block.



### ⚠ WARNING

When making physical connections to the Gateway it is important to use the electrical conduit entries located on the bottom of the housing. Connecting through the open terminal block cover (the lower cover) may stress the connections and damage the Gateway.

# Smart Wireless Gateway

## 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:

1. Open a standard web browser (typically Microsoft Internet Explorer).
2. Enter *192.168.1.10* in the address bar
3. Acknowledge the security to proceed.
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. The table below describes this access.

Table 2-2. Role Based Access User Accounts

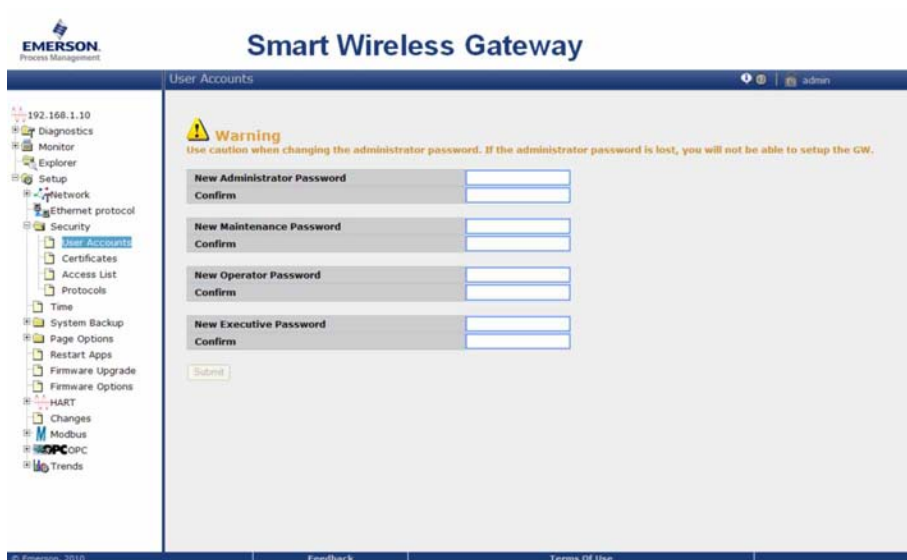
Role	User Name	Web Interface Access
Executive	exec	Read-only access
Operator	oper	Read-only access
Maintenance	maint	Configure HART <sup>®</sup> device settings Configure Modbus communications Configure Modbus register mapping Configure OPC browse tree Configure custom trends
Administrator	admin	Includes all maintenance privileges Configure Ethernet network settings Configure WirelessHART 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, please contact Emerson Process Management for technical support.

To change the User Accounts Passwords:

1. Navigate to **Setup>Security>User accounts**.
2. Set the new password for each role based user account, and confirm.
3. Click **Submit**.

Figure 2-2. User Accounts



## Time Settings

The Gateway is the timekeeper for the WirelessHART 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 **Setup>Time**.

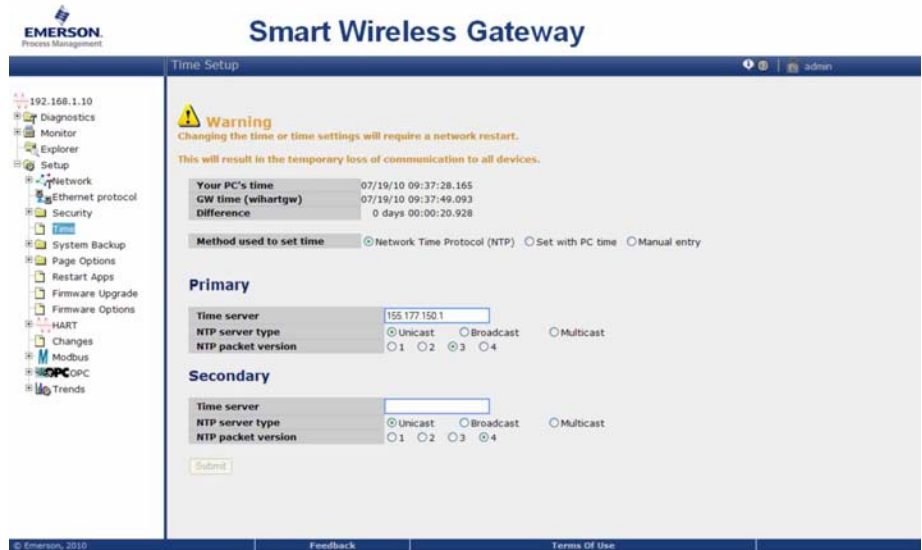
There are three ways to set the Gateway time:

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.

Figure 2-3. Time Settings



## TCP/IP Network Settings

### **⚠ WARNING**

Use caution when making changes to the TCP/IP network settings. If they are lost or improperly configured, it may be impossible to log into the Gateway. 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.

Request the following configuration items from the network administrator:

- Specify an IP address, or use a DHCP server
- Hostname
- Domain Name
- IP address
- Netmask
- Gateway

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



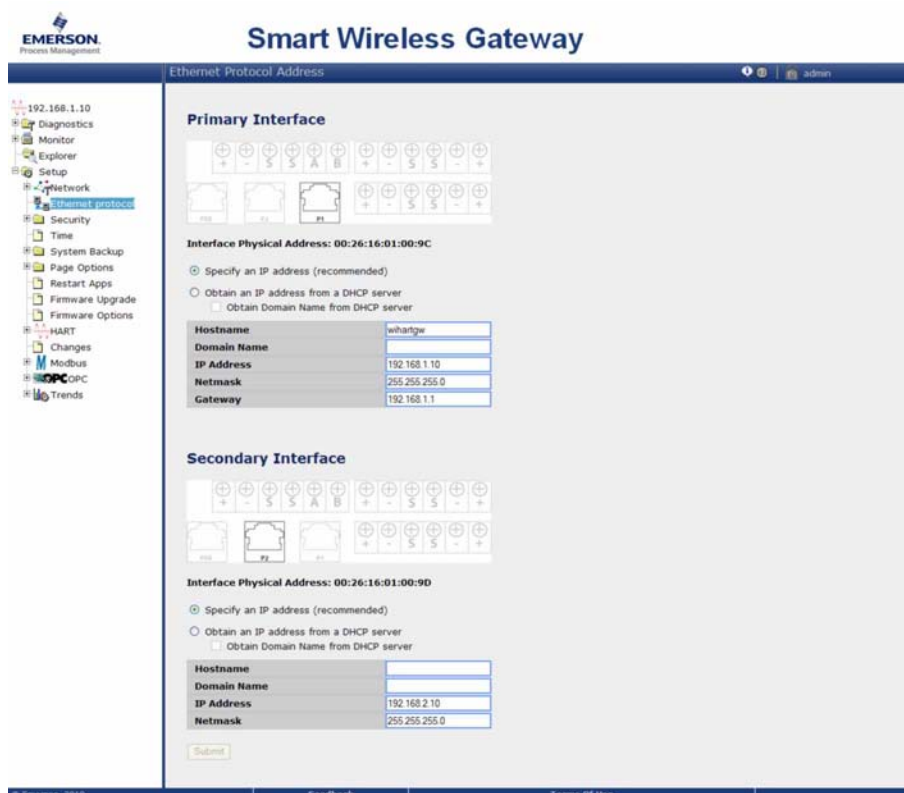
To change the TCP/IP Network Settings:

1. Navigate to **Setup>Internet protocol**.
2. Select **Specify an IP address** (recommended).
3. Enter the following:
  - Hostname
  - Domain Name
  - IP Address
  - Netmask
  - Gateway
4. Click **Submit**.
5. When prompted, click **Restart apps**.
6. Click **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. The web browser should be restarted, and 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.

Figure 2-4. Ethernet Settings



# Smart Wireless Gateway

---

## 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.

1. Navigate to **Setup>System Backup>Save**.
2. Click **Save Configuration**.
3. The Gateway collects configuration data and when the file download pop up appears, click **Save**.
4. Enter a save location and file name.
5. Enter **Save**.
6. Click **Return to form**.

---

### NOTE

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

---

# Section 3 Mounting and Connection

---

Overview .....	page 3-1
Mounting .....	page 3-2
Remote Antenna (optional) .....	page 3-4
Connecting .....	page 3-5

---

**⚠ WARNING**

Explosions could result in death or serious injury:

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

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.

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

- Make sure only qualified personnel perform the installation.

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.

## OVERVIEW

This section 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.

## General Considerations

The Smart Wireless Gateway may be mounted in any General Purpose location. Be sure the covers are secured tightly to prevent exposure of any electronics to moisture and contamination.

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.

# Smart Wireless Gateway

## Physical Description

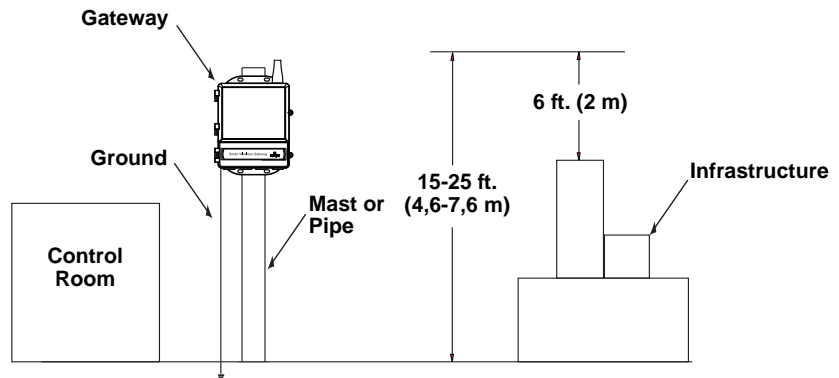
For dimensional drawing information refer to Appendix A: Product Specifications. The cast aluminum housing encloses the electronics circuitry of the Gateway. The front of the enclosure has an upper cover and a junction box cover. The upper cover provides access to the electronics and radio. The junction box cover provides access to the terminal block.

To open either cover, use a ¼-in. bladed screwdriver to remove the appropriate screw on the unhinged side of the enclosure.

## MOUNTING

Find a location where the Gateway has optimal wireless performance. Ideally this will be 15-25 ft. (4,6 - 7,6 m) above the ground or 6 ft. (2 m) above obstructions or major infrastructure. Figure 3-1 show an example gateway installation.

Figure 3-1. Gateway Installation



## Pipe Mount

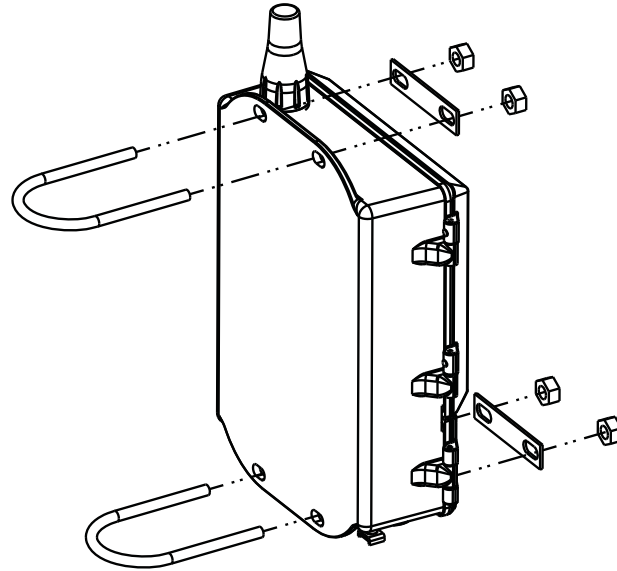
The following hardware and tools are needed to mount the Gateway to a 2-in. pipe:

- Two 5/16-in. u-bolts (supplied with Gateway)
- 2-in. mounting pipe
- ½-in. socket-head wrench

Mount the Gateway using the following procedure:

1. Insert one u-bolt around the pipe, through the top mounting holes of the Gateway enclosure, and through the washer plate.
2. Use a ½-in. socket-head wrench to fasten the nuts to the u-bolt.
3. Repeat for the second u-bolt and the lower mounting holes.

Figure 3-2. Pipe Mount



### **Bracket Mount (alternate)**

The following hardware and tools are needed to mount the Gateway to a support bracket:

- Four  $15/16$ -in. bolts
- Mounting support bracket
- $3/8$ -in. drill
- $1/2$ -in. socket-head wrench

Mount the Gateway using the following procedure:

1. Drill four  $3/8$ -in. (9,525 mm) holes spaced 3.06-in. (77 mm) apart horizontally and 11.15-in. (283 mm) apart vertically in the support bracket, corresponding with the holes on the Gateway enclosure.
2. Using a  $1/2$ -in. socket-head wrench, attach the Gateway to the support bracket with four  $15/16$ -in. bolts.

# Smart Wireless Gateway

## REMOTE ANTENNA (OPTIONAL)

The Remote Mount Antenna options provide flexibility for mounting the Gateway based on wireless connectivity, lightning protection, and current work practices.

### **WARNING**

When installing Remote Mount Antennas for the Smart Wireless Gateway, always use established safety procedures to avoid falling or contact with high-power electrical lines.

Install Remote Antenna components for the Smart 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 Smart Wireless Gateway Remote Antenna options are 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 Process Management is not responsible for wireless performance or non-compliance with spectrum regulations.

All Remote Mount Antenna kits include weatherproof tape for the cable connections as well as mounting kits for the lightning arrestor and antenna. See Table 3-1 for specifications for each remote antenna kit option.

Table 3-1. Remote Antenna options

Kit Option	Antenna	Cable 1	Cable 2	Lightning Arrestor
WL2	½ Wavelength Dipole Omni-Directional +6 dB gain	50 ft. (15,2 m) LMR-400	N/A	Head mount, jack to plug Gas discharge tube 0.5 dB insertion loss
WL3	½ Wavelength Dipole Omni-Directional +6 dB gain	30 ft. (6,1 m) LMR-400	20 ft. (6,1 m) LMR-400	In-line, jack to jack Gas discharge tube 0.1 dB insertion loss
WL4	½ Wavelength Dipole Omni-Directional +6 dB gain	40 ft. (12,2 m) LMR-400	10 ft. (3,0 m) LMR-400	In-line, jack to jack Gas discharge tube 0.1 dB insertion loss

Find a location where the remote antenna has optimal wireless performance. Ideally this will be 15-25 ft. (4,6 - 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:

#### WL2 option

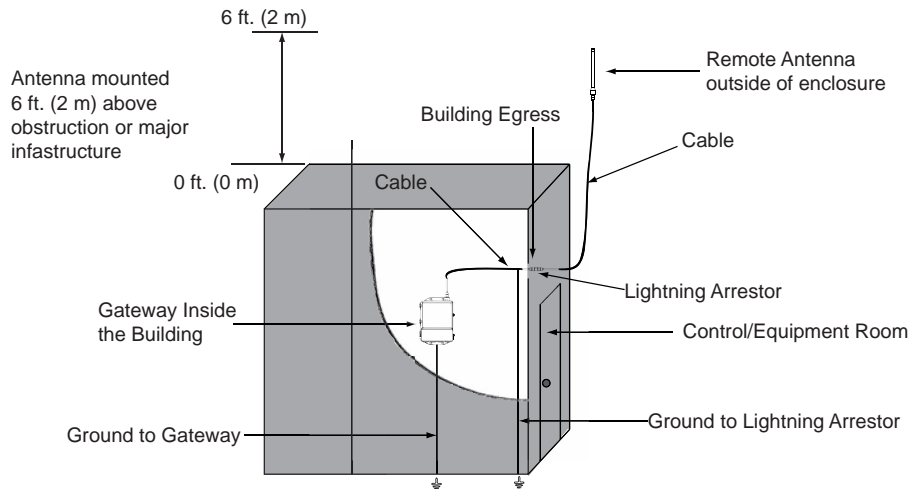
1. Mount the antenna on a 2-in. pipe mast using the supplied mounting equipment.
2. Connect the lightning arrestor directly to the top of the Gateway.
3. Connect the antenna to the lightning arrestor using the LMR-400 coaxial cable.
4. Use the weatherproofing tape to seal each connection between the Gateway, lightning arrestor, cable, and antenna.

### WL3 / WL4 option

1. Mount the antenna on a 2-in. pipe mast using the supplied mounting equipment.
2. Mount the lightning arrestor using the supplied mounting equipment. Minimize the distance between the arrestor and the egress into the building for optimal lightning protection.
3. Connect the Gateway, lightning arrestor, and antenna using the LMR-400 coaxial cables.
4. Use the weatherproofing tape to seal each connection between the Gateway, lightning arrestor, cables, and antenna.

Any spare lengths of coaxial cable should be placed in 12-in. (0,3 m) coils. Also ensure that the mounting mast and lightning arrestor are grounded according to local/national electrical code. See the following mounting example:

Figure 3-3. Remote Antenna Installation



### NOTE

Be sure to apply weatherproof tape to all remote antenna connections. The tape provided is self fusing silicon tape which must be stretched during application in order to form a proper seal. This tape is intended for single use, do not reuse.

## CONNECTING

All connections to the Gateway can be made at the terminal block, which is located in the lower junction box section of the enclosure. The terminal block label is located on the inside of the lower cover. See Figure 3-4 for the standard terminal block label and Figure 3-5 for the fiber optic terminal block label.

The junction box portion of the enclosure has four conduit entries for power and communications wiring. Do not run communication wiring in conduit or open trays with power wiring, or near heavy electrical equipment.

# Smart Wireless Gateway

Install the included conduit plugs in any unused conduit openings. For NEMA 4X and IP65 requirements, use thread seal (PTFE) tape or paste on male threads to provide a watertight seal.

## Grounding

The Gateway enclosure case 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. Ground the Gateway by connecting the external grounding lug to earth ground. The connection should be  $1 \Omega$  or less. The external ground lug is located below the Gateway enclosure and is identified by the following symbol:

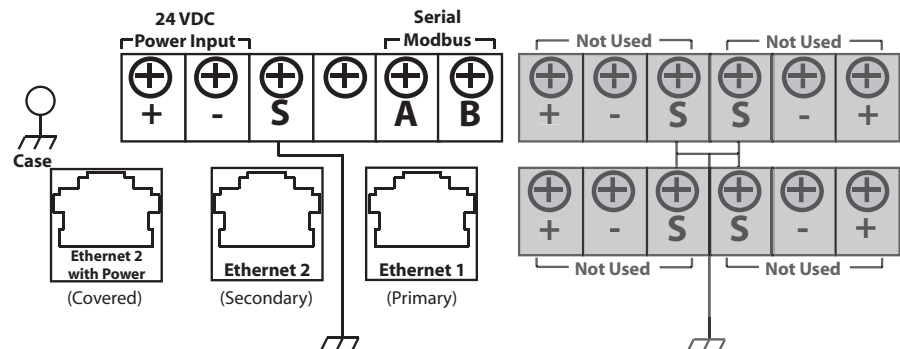


## Ethernet

The Gateway is equipped with two 10/100 Based-TX Ethernet communications ports (see Figure 3-4). These connections can be used to access the Gateway's web interface and to communicate Modbus TCP and OPC 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.

Figure 3-4. Terminal Block Diagram



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).

### NOTE

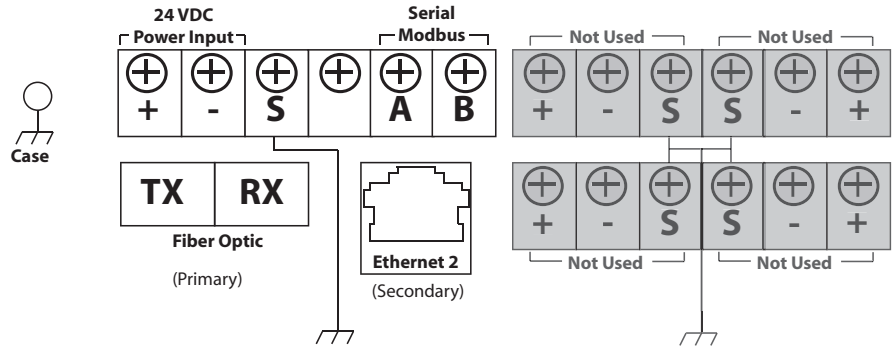
Unless dual Ethernet ports were specified at the time of order, the secondary Ethernet port (Ethernet 2) will not be active.

## Fiber Optic Connection (optional)

The Gateway may be ordered with an optional fiber optic connection (Figure 3-5). This interface can use the same communications protocols as the Ethernet interface. The fiber optic connection is the primary interface and Ethernet 2 is the secondary interface.



Figure 3-5. Fiber Optic Terminal Block Diagram



The fiber optic connection uses SC type connectors with a push-pull latching mechanism for quick connection and removal. It requires 1300 nm wavelength multi-mode cable. The maximum cable length should not exceed 2.48 miles (4,0 km).

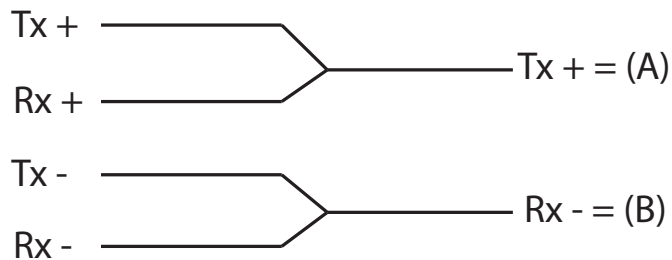
**RS-485**

The Gateway may be ordered with an optional RS-485 (serial) connection (Figure 3-4). It is referenced by the A and B Serial Modbus terminals. 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 + (positive, transmit) wire to terminal A and the Rx - (negative, receive) 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

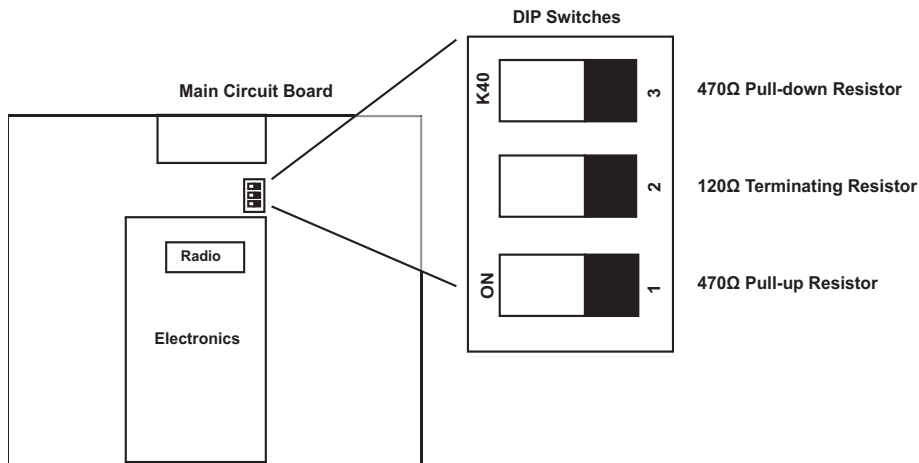


# Smart Wireless Gateway

## 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 near the top center of the main circuit board (Figure 3-7).

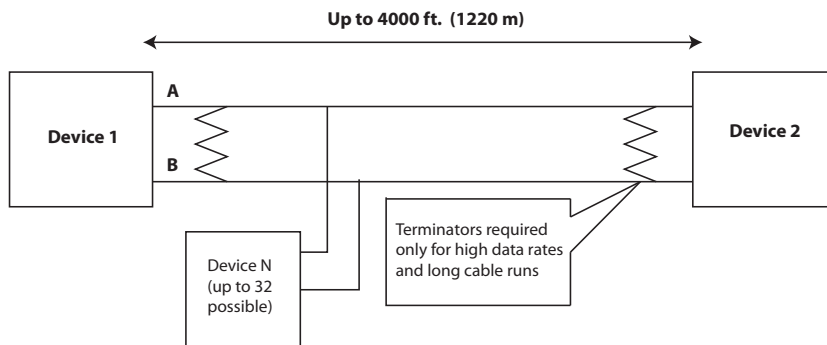
Figure 3-7. RS-485 Resistor DIP Switches



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 Ω 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 Ω terminating resistor. This resistor is used to dampen signal reflections on long cable runs. RS-485 specifications indicate that the data bus 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



## **Power**

The Gateway is designed to be powered by 24 Vdc (nominal) and requires 250 mA of current. The positive and negative connections are found on the left side of the terminal block (Figure 3-4). An additional case ground is found on the left side of the junction box enclosure.

Connect supply power to the positive + and negative – power terminals found on the left side of the terminal block (Figure 3-4). An additional internal case ground can be found on the left side of the enclosure. The wiring should include an external power shut-off switch or circuit breaker that is located near the Gateway.

---

### **NOTE**

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

---



# Section 4 Software Setup

---

<b>Overview</b> .....	<b>page 4-1</b>
<b>System Requirements</b> .....	<b>page 4-1</b>
<b>Software Installation</b> .....	<b>page 4-2</b>
<b>Security Setup Utility</b> .....	<b>page 4-2</b>
<b>AMS Wireless Configurator</b> .....	<b>page 4-4</b>
<b>Licensing and Credits</b> .....	<b>page 4-6</b>

---

## OVERVIEW

This section discusses the installation and setup of the optional software included with the Smart Wireless Gateway. 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
Reference Manual	An electronic copy of this document	Disk 1
User Interface Terminology Guide	This guide describes all the screens in the Gateway web interface and all the items/terms used on those pages.	Disk 1
Security Setup Utility	This utility allows the setup of SSL enable 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.

## 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 x 768 resolution and 16-bit color.*

# Smart Wireless Gateway

Table 4-3. Supported Operating Systems

Operating System	Version
Windows XP	Professional, Service Pack 2 or 3
Windows Server 2003	Standard, Service Pack 2
Windows Vista	Business, Service Pack 1 or 2
Windows Server 2008	Standard, Service Pack 1 or 2

*Note: Only 32-bit versions of the operating systems area supported.*

## 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 both disks in order is recommended. The Security Setup Utility is located on Disk 1. To install the software:

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:

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

---

### NOTE:

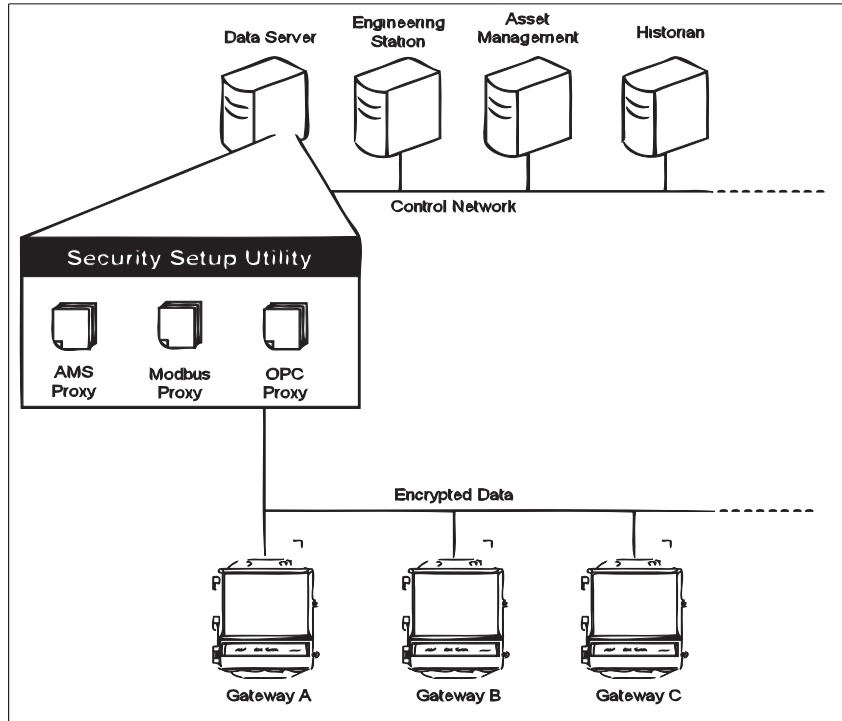
If the autorun function is disabled on the PC, or installation does not begin automatically, double click D:\SETUP.EXE (where D is the CD/DVD drive on the PC) and click OK.

---

## SECURITY SETUP UTILITY

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, 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



**NOTE:**

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

## Setup

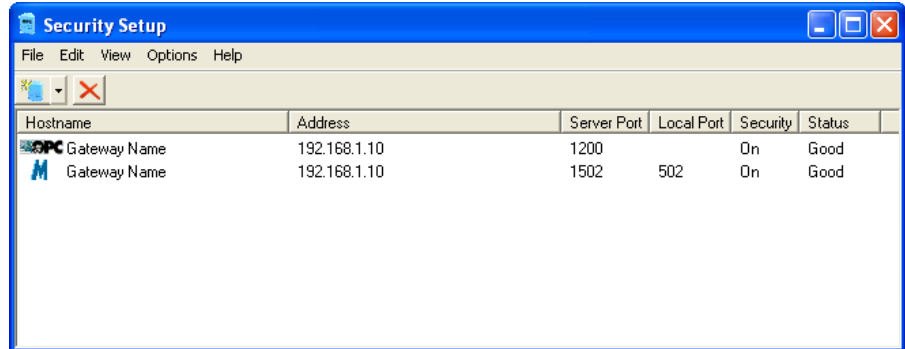
In the Security Setup Utility add a new proxy for each Gateway based on the communication protocol is being used. For example, add an OPC proxy for each Gateway that is communicating OPC.

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

1. Open the **Security Setup Utility**.
2. Click **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. Click **OK**.
6. Click **FILE>SAVE**.
7. When prompted for authentication, enter the admin **password** for the target Gateway.
8. Click **OK**.
9. Repeat steps 2-8 to added additional proxies.
10. Click **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



## 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 WirelessHART, 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**.

## 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:

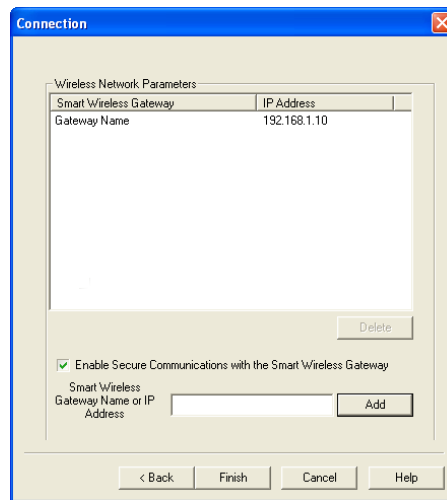
Do not have the Security Setup Utility running at the same time as the Network Configuration application or else a configuration error might occur.



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

1. Open the **Network Configuration** application.
2. Click **Add...**
3. Select **Wireless Network** and click **Install...**
4. Click **Next**.
5. Enter a **name** for the wireless network and click **Next**.
6. Enter the **HostName** or **IP Address** for the Gateway and click **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. Click **Finish** to close the configuration window.
10. Click **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:

1. Open the **Network Configuration** application.
2. Click **Add...**
3. Select **HART modem** and click **Install...**
4. Click **Next**.
5. Enter a **name** for the HART modem and click **Next**.
6. Select the Hart master type (default is AMS will be Primary HART master) and click **Next**.
7. Select the **COM port** for the HART modem and click **Next**.
8. Check the box to **Check to support Multi Drop devices**.
9. Check the box to **Include WirelessHART Adapter**.
10. Click **Finish** to close the configuration window.
11. Click **Close** to exit the Network Configuration application.

# Smart Wireless Gateway

---

## **LICENSING AND CREDITS**

The latest licensing agreements are include 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)"

# Section 5 Host Integration

---

Overview .....	page 5-1
Network Architecture .....	page 5-1
Internal Firewall .....	page 5-3
Modbus .....	page 5-4

---

## OVERVIEW

This section 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.

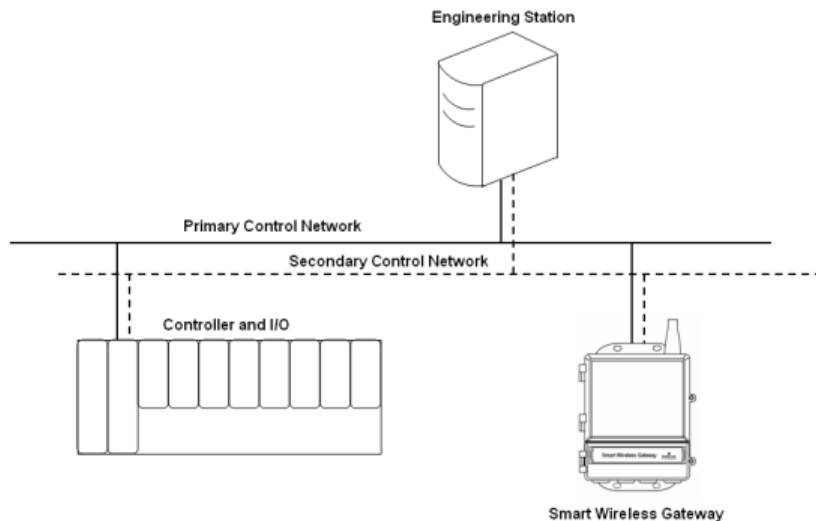
## NETWORK ARCHITECTURE

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. Fiber Optic and RS485 are available as optional connection types. 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, 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

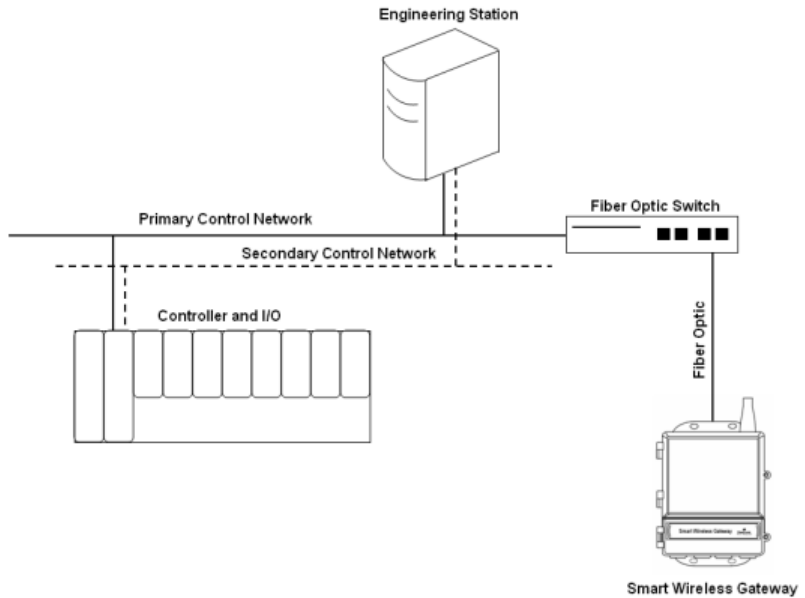


# Smart Wireless Gateway

## Fiber Optic (Optional)

A Fiber Optic connection supports Modbus TCP, OPC, AMS, and HART TCP protocols. Using this connection type, the Gateway is wired to a fiber optic switch (see Figure 5-2). Please note that a redundant fiber optic connection is not available.

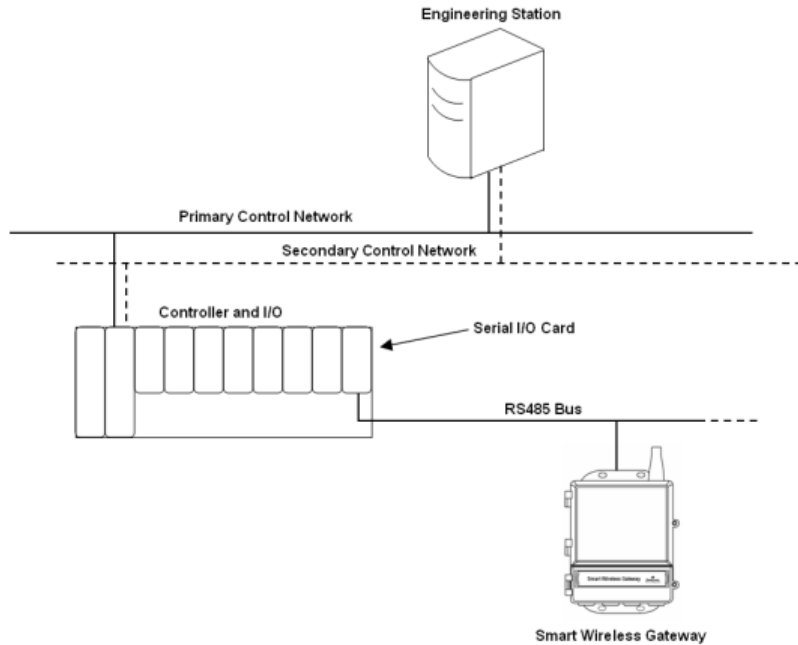
Figure 5-2. Fiber Optic Architecture



## 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 5-3). Up to 31 Gateways can be connected to a single I/O card in this manner.

Figure 5-3. RS485 Architecture



## 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 **Setup>Security>Protocols**.

Figure 5-4. Security Protocols page (internal firewall)

The screenshot shows the 'Protocols' configuration page in the Smart Wireless Gateway web interface. The page has a sidebar on the left with navigation options like 'Monitor', 'Setup', 'Network', 'Security', etc. The main content area displays a table of protocols with columns for 'Enable', 'Protocol', 'TCP Port', and 'UDP Port'. The 'Enable' column contains checkboxes, and the 'TCP Port' and 'UDP Port' columns contain input fields. The 'UDP Port' field for HART-IP is set to '5094 - 5126'. At the bottom of the table, there are navigation buttons: '<< First', '<< Previous', 'Search', 'Page 1 of 1', 'Next >>', and 'Last >>'. A 'Submit' button is also present.

Enable	Protocol	TCP Port	UDP Port
<input checked="" type="checkbox"/>	AMS	33333	
<input type="checkbox"/>	AMS Secure	32000	
<input type="checkbox"/>	DHCP		0
<input type="checkbox"/>	HART-IP	5094	5094 - 5126
<input checked="" type="checkbox"/>	HART-IP Secure	5095	
<input checked="" type="checkbox"/>	HTTP	80	
<input type="checkbox"/>	HTTPS	443	
<input type="checkbox"/>	Modbus TCP	502	
<input checked="" type="checkbox"/>	Modbus TCP Secure	1502	
<input type="checkbox"/>	NTP		123
<input type="checkbox"/>	OPC Comm	1199	
<input checked="" type="checkbox"/>	OPC Comm Secure	1200	
<input checked="" type="checkbox"/>	Ping		

# Smart Wireless Gateway

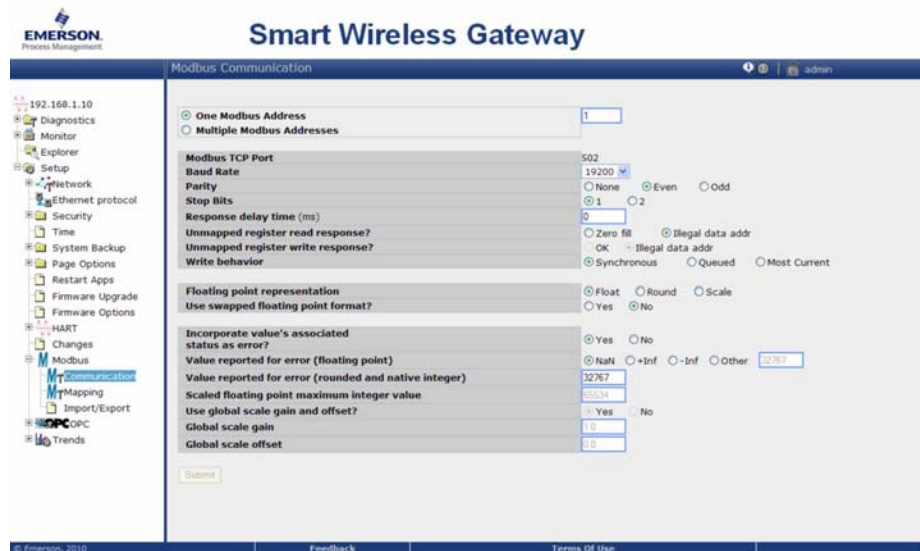
## MODBUS

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).

## Communication Settings

It is important that the Modbus communication settings in the Gateway match the setting in the Modbus master or client. Please refer to host system documentation for more information on how to configure these settings. The Modbus communication settings can be found by navigating to Setup>Modbus>Communications.

Figure 5-5. 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 valued 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.

# Smart Wireless Gateway

## 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 **Setup>Modbus>Mapping**.

Figure 5-6. Modbus Register Map Page



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

1. Click **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. Click **Submit**.
5. When changes have been accepted, click **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 manual entered. The following table gives a list of standard device parameter which may be considered for Modbus register mapping.



Table 5-1. Device parameters available via Modbus

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. Please refer to the device's documentation for more information on for 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.

# Smart Wireless Gateway

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
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

# Section 6 Troubleshooting

This section provides basic troubleshooting tips for the 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:

Specialist-Wireless.EPM-RTC@Emerson.com

Initial Connection	
Web browser returns page not found	<ol style="list-style-type: none"> <li>1. Use the supplied crossover cable to connect the Gateway and PC/Laptop</li> <li>2. Verify the Gateway is properly powered, 24 Vdc and 250 mA. Open the upper cover and verify if any indicator lights are on.</li> <li>3. Verify which Ethernet port is being used on the Gateway.</li> <li>4. 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).</li> <li>5. 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).</li> <li>6. Disable internet browser proxy settings.</li> </ol>
Can not find Gateway after changing IP address	<ol style="list-style-type: none"> <li>1. 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).</li> </ol>
Can not find Gateway using Secondary Ethernet Port	<ol style="list-style-type: none"> <li>1. Verify which Ethernet port is being used on the Gateway.</li> <li>2. Verify the IP address for the Gateway (default primary port is 192.168.1.10, default secondary port is 192.168.2.10).</li> <li>3. 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).</li> </ol>
Can not log into the Gateway	<ol style="list-style-type: none"> <li>1. Verify the user name and password. The administrator user name is admin and the default password is default. See Table 2-1.</li> </ol>

# Smart Wireless Gateway

AMS Wireless Configurator	
Gateway does not appear in AMS Wireless Configurator	<ol style="list-style-type: none"> <li>1. Verify the Security Setup Utility is installed on the same PC as AMS Wireless Configurator.</li> <li>2. Setup a wireless network interface using the Network Configuration application. See Section 4 Software Setup.</li> <li>3. Verify if the wireless network interface is configured for Secure Gateway Communications.</li> <li>4. Verify secure/unsecure AMS protocol settings in the Gateway. Log on to the Gateway and navigate to SETUP &gt; SECURITY &gt; PROTOCOLS.</li> <li>5. Restart AMS data server. Right click on AMS server icon in the Windows system tray (lower right corner) and select stop server.</li> </ol>
Wireless devices do not appear under the Gateway	<ol style="list-style-type: none"> <li>1. Verify wireless devices are connected to the Gateway. Log on to the Gateway and navigate to EXPLORER.</li> <li>2. Right click on wireless network and select rebuild hierarchy.</li> </ol>
Wireless device appears with red HART symbol	<ol style="list-style-type: none"> <li>1. Install latest device support files from AMS. Go to <a href="http://www.emersonprocess.com">www.emersonprocess.com</a> &gt; BRANDS &gt; AMS SUITE &gt; AMS DEVICE MANAGER &gt; DEVICE DESCRIPTION (DDs).</li> </ol>
Device configuration items are grayed out	<ol style="list-style-type: none"> <li>1. Verify whether current or historical information is being displayed. This setting is displayed at the bottom of each device configuration screen. Configuration requires the Current setting.</li> <li>2. For security purposes a configuration timeout is applied to sessions that have been idle for more than 30 minutes. Log back into AMS Wireless Configurator.</li> </ol>

Wireless Field Devices	
Wireless device does not appear on the network	<ol style="list-style-type: none"> <li>1. Verify the device has power.</li> <li>2. Verify the device is within effect communications range.</li> <li>3. Verify the proper Network ID has been entered into the device</li> </ol>
Wireless device appears in the join failure list	<ol style="list-style-type: none"> <li>1. Re-enter the Network ID and Join Key into the device.</li> </ol>
Wireless device appears with service denied	<ol style="list-style-type: none"> <li>1. Verify the total number of devices on the network (100 max).</li> <li>2. Go to SETUP &gt; NETWORK &gt; BANDWIDTH and click analyze bandwidth (Note: any changes will require the network to reform)</li> <li>3. Reduce the update rate for the device.</li> </ol>

Modbus Communications	
Can not communicate using Modbus RTU	<ol style="list-style-type: none"> <li>1. Verify the use of RS-485</li> <li>2. Verify wiring connections. See Section 3 Mounting and Connections.</li> <li>3. Verify if termination is required.</li> <li>4. Verify that Modbus serial communications setting in the Gateway match the Modbus Host settings. Log on to the Gateway and navigate to SETUP &gt; MODBUS &gt; COMMUNICATIONS.</li> <li>5. Verify the Modbus address for the Gateway</li> <li>6. Verify Modbus register mapping in the Gateway. Log on to the Gateway and navigate to SETUP &gt; MODBUS &gt; MAPPING.</li> </ol>
Can not communicate using Modbus TCP	<ol style="list-style-type: none"> <li>1. Verify secure / unsecure Modbus protocol settings in the Gateway. Log on to the Gateway and navigate to SETUP &gt; SECURITY &gt; PROTOCOLS.</li> <li>2. Verify the Modbus TCP communications settings in the Gateway. Log on to the Gateway and navigate to SETUP &gt; MODBUS &gt; COMMUNICATIONS.</li> <li>3. Verify Modbus register mapping in the Gateway. Log on to the Gateway and navigate to SETUP &gt; MODBUS &gt; MAPPING.</li> </ol>
Can not communicate using secure Modbus TCP	<ol style="list-style-type: none"> <li>1. Verify the Security Setup Utility has been installed.</li> <li>2. Configure a Secure Modbus Proxy for the Gateway. See Section 4 Software Setup.</li> <li>3. Verify secure / unsecure Modbus protocol settings in the Gateway. Log on to the Gateway and navigate to SETUP &gt; SECURITY &gt; PROTOCOLS.</li> <li>4. Verify the Modbus TCP communications settings in the Gateway. Log on to the Gateway and navigate to SETUP &gt; MODBUS &gt; COMMUNICATIONS.</li> <li>5. Verify Modbus register mapping in the Gateway. Log on to the Gateway and navigate to SETUP &gt; MODBUS &gt; MAPPING.</li> </ol>

<b>OPC Communications</b>	
OPC application can not find a Gateway OPC server	<ol style="list-style-type: none"><li>1. Verify the Security Setup Utility has been installed on the same PC as the OPC application.</li><li>2. Configure an OPC proxy for the Gateway. See Section 4 Software Setup.</li></ol>
Gateway OPC server does not show any Gateways	<ol style="list-style-type: none"><li>1. Configure an OPC proxy for the Gateway. See Section 4 Software Setup.</li></ol>
Gateway OPC server does not show any data tags	<ol style="list-style-type: none"><li>1. Configure the Gateway OPC Browse Tree. Log on to the Gateway and navigate to SETUP &gt; OPC &gt; OPC BROWSE TREE.</li><li>2. Verify the connection status for the OPC proxy in the Security Setup Utility.</li><li>3. Verify if the OPC proxy is configured for secure or unsecure communications.</li><li>4. Verify secure / unsecure OPC protocol settings in the Gateway. Log on to the Gateway and navigate to SETUP &gt; SECURITY &gt; PROTOCOLS.</li><li>5. Verify network firewall and port settings.</li></ol>



## Section 7 Glossary

This glossary defines terms used through out this manual or that appear in the web interface of the Smart Wireless Gateway.

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 devices 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 hexadecimal 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 WirelessHART 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 WirelessHART 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.
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.

# Smart Wireless Gateway

---

Term	Definition
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 devices transmits measurement and status data to the Gateway. Same as Burst Rate.
Wireless Field Device(s)	WirelessHART field devices that are a part of the wireless field network.
Wireless Field Network	WirelessHART 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.



# Appendix A Product Specifications

---

Functional Specifications .....	page A-1
Physical Specifications .....	page A-1
Communication Specifications .....	page A-2
Self-Organizing Network Specifications .....	page A-2
System Security Specifications .....	page A-3
Dimensional Drawings .....	page A-4
Ordering Information .....	page A-6
Accessories and Spare Parts .....	page A-7

---

## FUNCTIONAL SPECIFICATIONS

### Input Power

19.2-28.8 VDC

150 milliamps for continuous operation. 250 milliamps required to power the Smart Wireless Gateway.

### Environmental

Operating Temperature Range:

-40 to 158 °F (-40 to 70 °C)

Operating Humidity Range:

10-90% relative humidity

### EMC Performance

Complies with EN61326-1:2006.

### Antenna Options

Integrated Omnidirectional Antenna

Optional remote mount Omnidirectional Antenna

## PHYSICAL SPECIFICATIONS

### Weight

10 lbs. (4,54 kg)

### Material of Construction

#### Housing

Low-copper aluminum, NEMA 4X

#### Paint

Polyurethane

#### Cover Gasket

Silicone Rubber

#### Antenna

PBT/PC integrated Omnidirectional Antenna

### Certifications

Class I Division 2 (U.S.)

Equivalent Worldwide



# Smart Wireless Gateway

---

## COMMUNICATION SPECIFICATIONS

### 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)

### Ethernet

10/100base-TX Ethernet communication port  
Protocols: Modbus TCP, OPC, HART-IP, https (for Web Interface)  
Wiring: Cat5E shielded cable. Wiring distance 328 ft. (100 m).

### Fiber Optic Ethernet (optional)

100BaseFx optical Ethernet communication port  
Wavelength: 1300 nm center  
Multimode  
SC connectors  
Protocols: Modbus, TCP, OPC, HART-IP, https (for Web Interface)  
Wiring: 50/125 um or 62.5/125 um fiber, 2.48 miles (4.0 km) maximum distance.

### Modbus

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

### OPC

OPC server supports OPC DA v2, v3

## SELF-ORGANIZING NETWORK SPECIFICATIONS

### Protocol

WirelessHART, 2.4 - 2.5 GHz DSSS.  
Maximum Network Size  
100 devices @ 8 sec.  
50 devices @ 4 sec.

### Supported Device Update Rates

4 sec. to 60 min.

### Network Size/Latency

100 Devices: less than 10 sec.  
50 Devices: less than 5 sec.

### Data Reliability

>99%

## **SYSTEM SECURITY SPECIFICATIONS**

### **Ethernet**

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

### **Smart 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.

### **Self-Organizing Network**

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

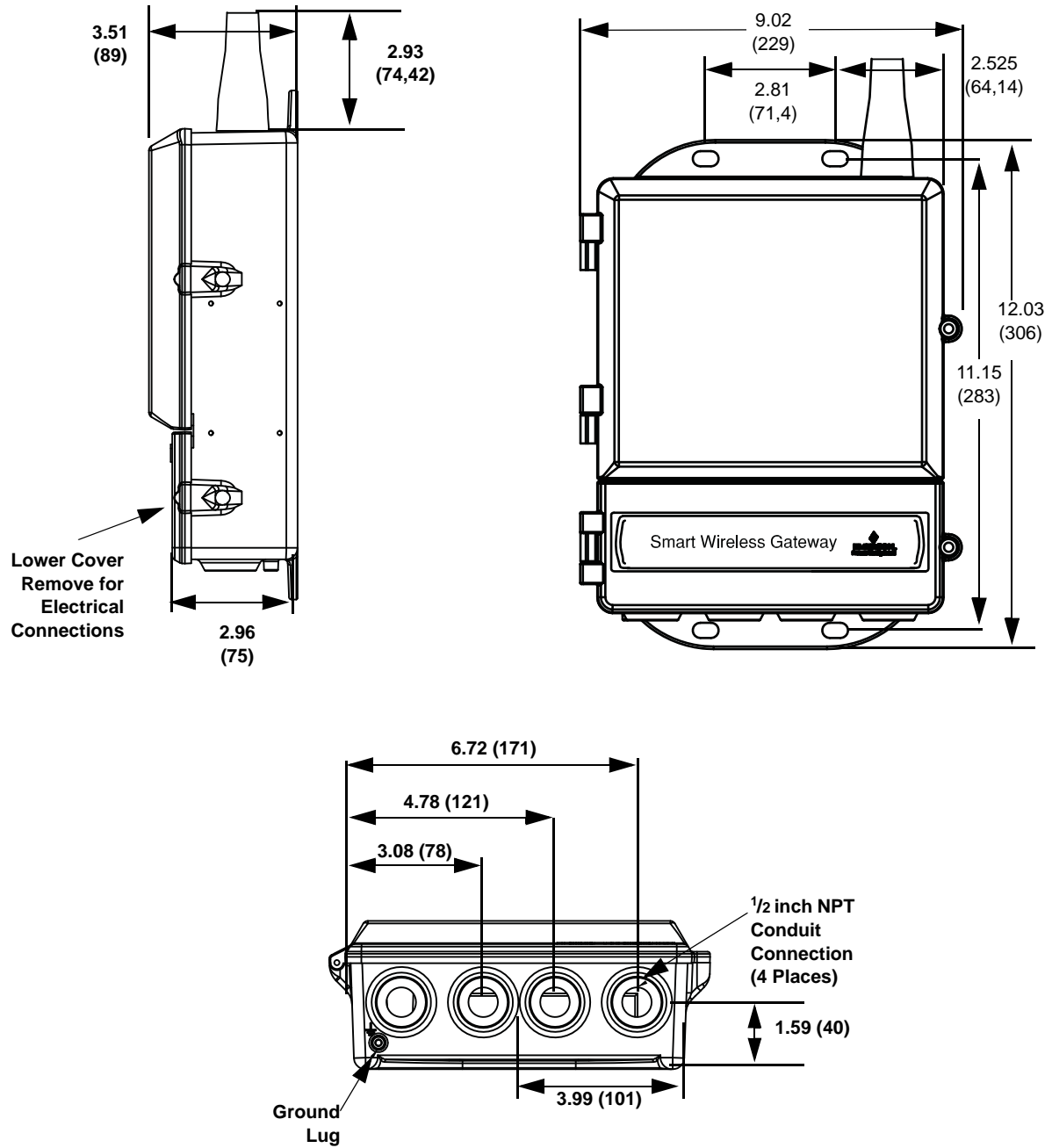
### **Internal Firewall**

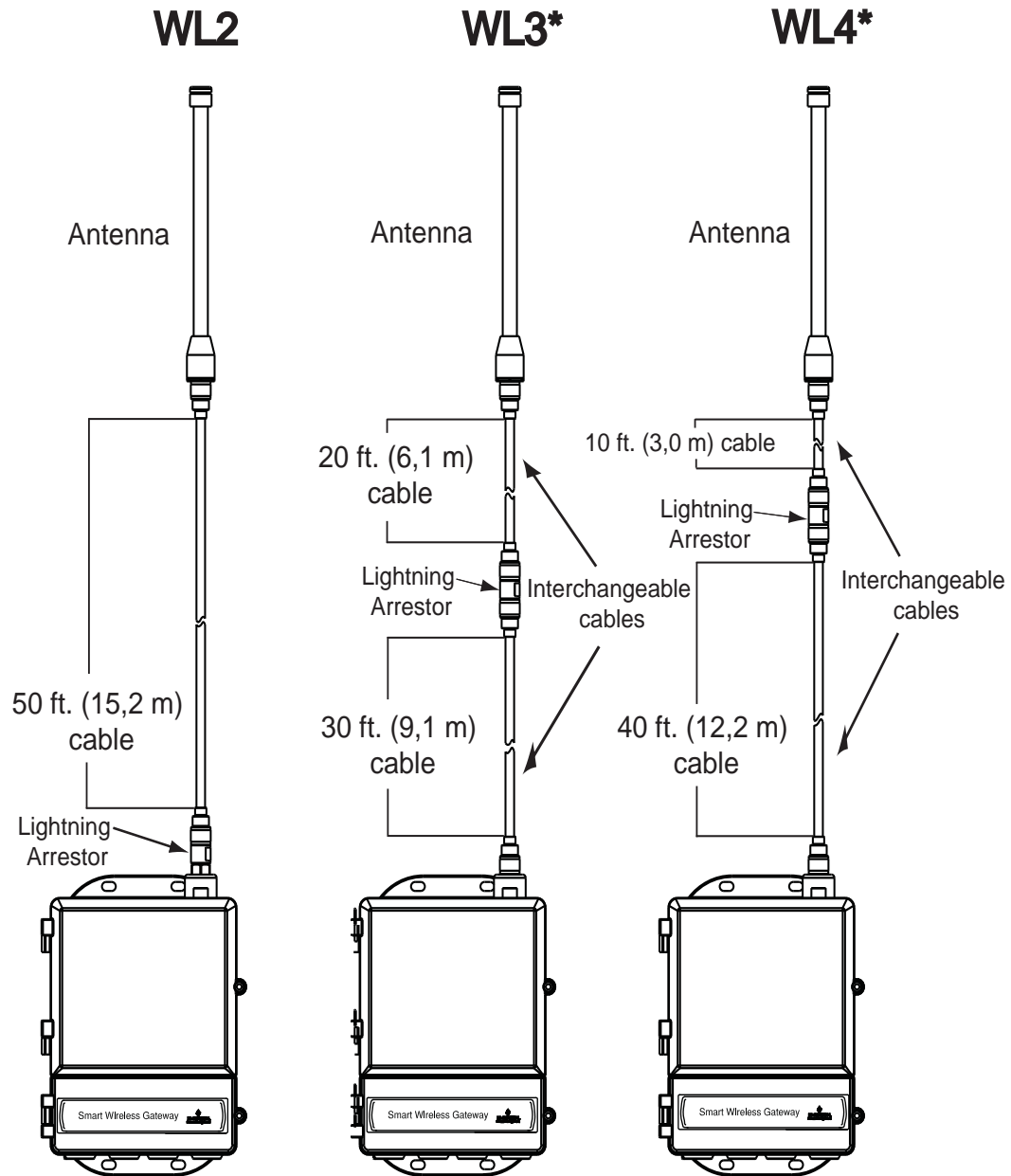
User Configurable TCP ports for communications protocols, including Enable/Disable and user specified port numbers. Inspects both incoming and outgoing packets.

# Smart Wireless Gateway

## DIMENSIONAL DRAWINGS

Figure A-1. Smart Wireless Gateway (Dimensions are in inches (millimeters))





**Remote Omni-Antenna Kit**

The Remote Omni-Antenna kit includes sealant tape for remote antenna connection, as well as mounting brackets for the antenna, Lightning Arrestor, and the Smart Wireless Gateway.

**Lightning protection is included on all the options. WL3 and WL4 provide lightning protection along with the ability to have the gateway mounted indoors, the antenna mounted outdoors, and the lightning arrestor mounted at the building egress.**

**\*Note that the coaxial cables on the remote antenna options WL3 and WL4 are interchangeable for installation convenience.**

# Smart Wireless Gateway

## ORDERING INFORMATION

Table A-1. Rosemount 1420 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	
1420	Smart Wireless Gateway	
<b>Power Input</b>		
<b>Standard</b>		<b>Standard</b>
A	24 VDC	★
<b>Ethernet Communications - Physical Connection</b>		
<b>Standard</b>		<b>Standard</b>
1 <sup>(1)(2)</sup>	Ethernet	★
2 <sup>(3)(4)</sup>	Dual Ethernet	★
<b>Expanded</b>		
3 <sup>(5)(6)</sup>	Fiber Optic Ethernet	
<b>Wireless Update Rate, Operating Frequency, and Protocol</b>		
<b>Standard</b>		<b>Standard</b>
A3	User Configurable Update Rate, 2.4 GHz DSSS, WirelessHART	★
<b>Serial Communication</b>		
<b>Standard</b>		<b>Standard</b>
N	None	★
A <sup>(7)</sup>	Modbus RTU via RS485	★
<b>Ethernet Communication - Data Protocols</b>		
<b>Standard</b>		<b>Standard</b>
2	Webserver, Modbus TCP/IP, AMS Ready	★
4	Webserver, Modbus TCP/IP, AMS Ready, OPC	★
5 <sup>(8)</sup>	DeltaV Ready	★
6 <sup>(8)</sup>	Ovation Ready	★
7 <sup>(9)</sup>	HART-IP	★

### Options (Include with selected model number)

<b>Product Certifications</b>		
<b>Standard</b>		<b>Standard</b>
N5	FM Division 2, Non-incendive	★
N6	CSA Division 2, Non-incendive	★
N1	ATEX Type n	★
ND	ATEX Dust	★
N7	IECEX Type n	★
NF	IECEX Dust	★
KD	FM & CSA Division 2, Non-incendive and ATEX Type n	★
N3	China Type n	★
N4	TIIS Type n	★
<b>Adapters</b>		
<b>Standard</b>		<b>Standard</b>
J1	CM 20 Conduit Adapters	★
J2	PG 13.5 Conduit Adapters	★
J3	3/4 NPT Conduit Adapters	★
<b>Antenna Options<sup>(10)</sup></b>		
<b>Standard</b>		<b>Standard</b>
WL2	Remote Omni-Antenna Kit, 50 ft. (15.2 m) cable, Lightning Arrestor	★
WL3	Remote Omni-Antenna Kit, 20 ft. (6.1 m) and 30 ft. (9.1 m) cables, Lightning Arrestor	★
WL4	Remote Omni-antenna Kit, 10 ft. (3.0 m) and 40 ft. (12.2 m) cables, Lightning Arrestor	★
<b>Typical Model Number: 1420 A 2 A3 A 2 N5</b>		

- (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) 1300nm Multimode Optical fiber connection with separate SC connectors for Rx and Tx.
- (6) Includes features of Option 1.
- (7) Convertible to RS232 via adaptor, not included with Gateway.
- (8) Includes Webserver, Modbus TCP, AMS Ready, and OPC.
- (9) Includes Webserver, Modbus TCP, and AMS Ready.
- (10) The WL2 - WL4 options require minor assembly.

**ACCESSORIES AND SPARE PARTS**

Table A-2. 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-3. Spare Parts

Item Description	Part Number
Spare Kit, WL2 Replacement <sup>(1)</sup> , Remote Antenna, 50 ft. (15,2 m) Cable, and Lightning Arrestor	01420-1615-0302
Spare Kit, WL3 Replacement <sup>(1)</sup> , Remote Antenna, 20/30 ft. (6,1/9,1 m) Cables, and Lightning Arrestor	01420-1615-0303
Spare Kit, WL4 Replacement <sup>(1)</sup> , Remote Antenna, 10/40 ft. (3,0/12,2 m) Cables, and Lightning Arrestor	01420-1615-0304

(1) Can not upgrade from integral to remote antenna.





# Appendix B Product Certifications

---

Approved Manufacturing Locations . . . . .	page B-1
Telecommunication Compliance . . . . .	page B-1
FCC and IC . . . . .	page B-1
Ordinary Location Certification for FM . . . . .	page B-1
European Union Directive Information . . . . .	page B-2

---

## APPROVED MANUFACTURING LOCATIONS

Rosemount Inc. – Chanhassen, Minnesota, USA  
Emerson Process Management GmbH & Co. - Karlstein, Germany  
Emerson Process Management Asia Pacific Private Limited - Singapore  
Beijing Rosemount Far East Instrument Co., Limited - Beijing, China

## 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.

## 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.

## ORDINARY LOCATION CERTIFICATION FOR FM

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

### North American Certifications

N5 FM Division 2, Non-Incendive  
Certificate Number: 3028321  
Nonincendive for Class I, Division 2, Groups A, B, C, and D.  
Suitable for Class II, III, Division 2,  
Groups E, F, and G; Indoors/outdoor locations;  
Type 4X  
Temperature Code: T4 (-40 °C < T<sub>a</sub> < 60 °C)

### Canadian Standards Association (CSA)

N6 CSA Division 2, Non-Incendive  
Certificate Number: 1849337  
Suitable for Class I, Division 2, Groups A, B, C, and D.  
Install per Rosemount drawing 01420-1011.  
Temperature Code: T4 (-40 °C < T<sub>a</sub> < 60 °C)  
CSA Enclosure Type 4X

# Smart Wireless Gateway

---

## EUROPEAN UNION DIRECTIVE INFORMATION

The EC declaration of conformity for all applicable European directives for this product can be found on the Rosemount website at [www.rosemount.com](http://www.rosemount.com). A hard copy may be obtained by contacting your local sales representative.

### *ATEX Directive (94/9/EC)*

Emerson Process Management complies with the ATEX Directive.

### *Electro Magnetic Compatibility (EMC) (2004/108/EC)*

Emerson Process Management complies with the EMC Directive.

### *Radio and Telecommunications Terminal Equipment Directive (R&TTE)(1999/5/EC)*

Emerson Process Management complies with the R&TTE Directive



## European Certification

### N1 ATEX Type n

Certificate Number: Baseefa 07ATEX0056X

ATEX Marking: Ⓢ II 3 G

Ex nA nL IIC T4 (-40 °C < T<sub>a</sub> < 60 °C)

#### **Special condition for safe use (X):**

The surface resistivity of the antenna is greater than one gigaohm. To avoid electrostatic charge build-up, it must not be rubbed or cleaned with solvents or a dry cloth.

The Apparatus is not capable of withstanding the 500V insulation test required by Clause 9.4 of EN 60079-15: 2005. This must be taken into account when installing the apparatus.

### ND ATEX Dust

Certificate Number: Baseefa 07ATEX0057

ATEX Marking: Ⓢ II 3 D

Ex tD A 22 IP66 T135 (-40 °C < T<sub>a</sub> < 60 °C)

Maximum working voltage = 28 V

**N7** IECEx Type n  
Certificate Number: IECEx BAS 07.0012X  
Ex nA nL IIC T4 (-40 °C ≤ T<sub>a</sub> ≤ 60 °C)  
Maximum working voltage = 28 V

**Special condition for safe use (X):**

The surface resistivity of the antenna is greater than one gigaohm. To avoid electrostatic charge build-up, it must not be rubbed or cleaned with solvents or a dry cloth.

The Apparatus is not capable of withstanding the 500V insulation test required by Clause 9.4 of EN 60079-15: 2005. This must be taken into account when installing the apparatus.

**NF** IECEx Dust  
Certification Number: IECEx BAS 07.0013  
Ex tD A22 IP66 T135 (-40 °C < T<sub>a</sub> < 60 °C)  
Maximum working voltage = 28 V

**Combinations of Certifications**

**KD** Combination of N5, N6, and N1.



---

# Appendix C      Delta V Ready

---

<b>Overview</b> .....	<b>page C-1</b>
<b>Requirements</b> .....	<b>page C-1</b>
<b>Mounting and Connecting</b> .....	<b>page C-1</b>
<b>Setup</b> .....	<b>page C-2</b>

---

## OVERVIEW

Native integration with DeltaV enables the Smart Wireless Gateway to be autosensed and easily commissioned for seamless integration with all DeltaV applications: Explorer, Diagnostics, and Control Studio. WirelessHART devices can be easily added to the wireless field network and then reconciled through DeltaV Explorer and assigned to analog channels through drag and drop assignment.

## REQUIREMENTS

### DeltaV:

Version 10.3 or newer.

### Smart Wireless Gateway:

DeltaV Ready option (Data Protocol option 5). Appendix A: Ordering Information

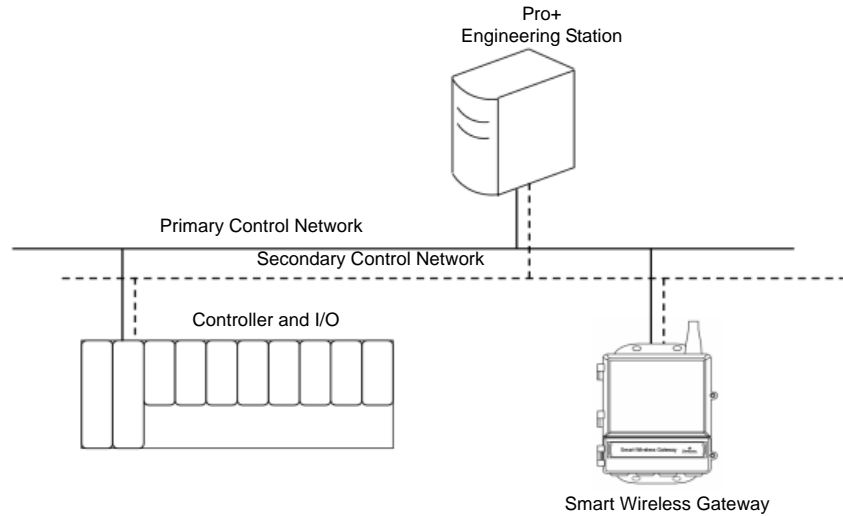
## MOUNTING AND CONNECTING

Mount the DeltaV Ready Gateway in the same manner as a standard Gateway. (Section 3: Mounting and Connection on page 3-1). The Gateway should be mounted in a location that allows convenient access to the DeltaV control network as well as the wireless field network.

Connect the Gateway's primary Ethernet port (Ethernet 1) into the DeltaV primary control network. If the dual Ethernet option (Physical Connection code 2) was order with the Gateway, connect the secondary Ethernet port (Ethernet 2) into the DeltaV secondary control network.

# Smart Wireless Gateway

Figure C-1. Delta V Control Network Architecture



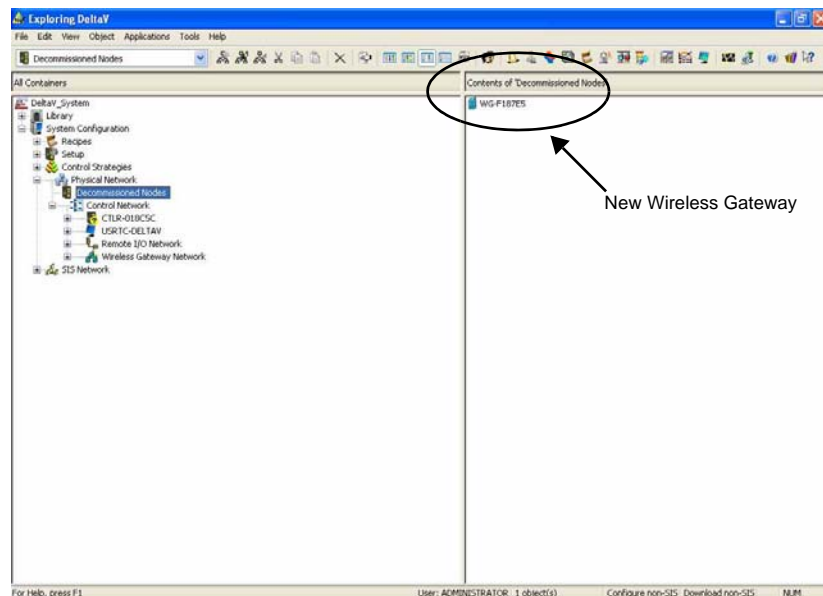
## SETUP

Out of the box the Smart Wireless Gateway is pre-configured for use on the DeltaV control network. In the DeltaV Explore application, the Gateway will automatically appear in the Decommissioned Nodes folder.

To setup a wireless network will require 3 steps:

1. Commission the Gateway
2. Assign wireless device tags
3. Assign Gateway to controller and download

Figure C-2. Decommissioned Nodes folder within Delta V Explorer

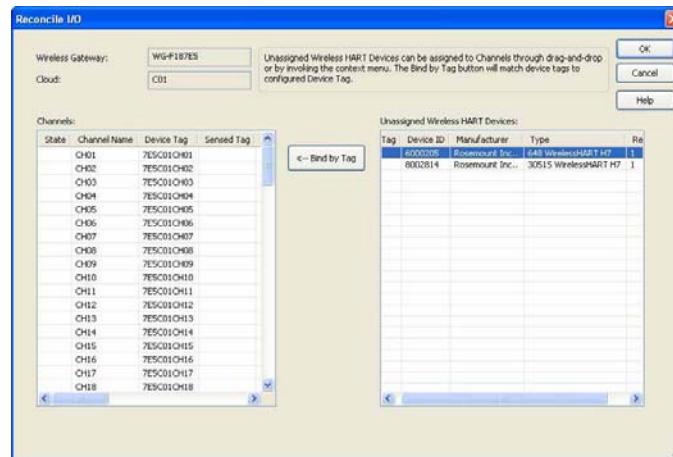


Commission the Gateway using the following procedure:

1. Click **START>PROGRAMS>DELTA V>ENGINEERING> DELTA V EXPLORE** to launch the DeltaV Explorer application.
2. Expand the folder **SYSTEM CONFIGURATION >PHYSICAL NETWORK>DECOMMISSIONED NODES**.
3. Right click on the Smart Wireless Gateway and select **Commission**.
4. Enter a name for the Gateway and click **OK**.
5. Click **YES** when prompted to Auto-Sense Wireless Gateway.

At this time the Reconcile I/O window will appear. The purpose of this screen is to assign WirelessHART devices to DeltaV I/O channel. This allows the wireless device to be referenced in other DeltaV applications like Control Studio.

Figure C-3. Assign WirelessHART devices to DeltaV I/O Channel



Assign wireless device tags using the following procedure:

1. Drag and Drop WirelessHART device from the **Unassigned Wireless HART Devices:** list to the **Channels:** list.
2. Repeat this process for each wireless device until all have been assigned.
3. Click **OK** to continue.

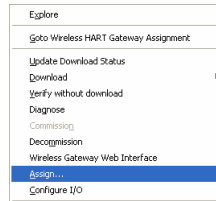
Next the Gateway will need to be assigned to a DeltaV Controller and download all. Assign and download the Gateway using the following procedure:

1. Right click on the Gateway and select **Assign...**
2. Use the browse window and select the desired controller
3. Click **OK** to close the assignment window
4. Right click on the Gateway and select **Download**
5. Follow the download dialog
6. Click **OK** to close the down load window

# Smart Wireless Gateway

---

Figure C-4. Gateway context menu (right click).



Now the Gateway and wireless devices are fully commissioned and available to use in other DeltaV applications. When new devices are added to the wireless network they will need to be assigned to DeltaV channels through the reconcile process (right click on Gateway and select configure IO).

---

**NOTE:**

Logging in to the Gateway is not possible using the default TCP/IP network setting. If the Gateway is decommissioned, use an IP address 10.5.255.254. If the Gateway is commissioned right click on the Gateway in DeltaV Explore and select Wireless Gateway Web Interface.

---





*The Emerson logo is a trade mark and service mark of Emerson Electric Co.  
Rosemount and the Rosemount logotype are registered trademarks of Rosemount Inc.  
PlantWeb is a registered trademark of one of the Emerson Process Management group of companies.  
HART is a registered trademark of the HART Communication Foundation.  
All other marks are the property of their respective owners.*

*Standard Terms and Conditions of Sale can be found at [www.rosemount.com/terms\\_of\\_sale](http://www.rosemount.com/terms_of_sale)*

©2010 Rosemount Inc. All rights reserved.

**Emerson Process Management  
Rosemount Inc.**  
8200 Market Boulevard  
Chanhassen, MN 55317 USA  
T (U.S.) 1 800 999 9307  
T (International) 952 906 8888  
F 952 949 7001

[www.rosemount.com](http://www.rosemount.com)

**Rosemount Temperature GmbH**  
Frankenstrasse 21  
63791 Karlstein  
Germany  
T 49 6188 992 0  
F 49 6188 992 112

**Emerson Process Management  
Asia Pacific Private Limited**  
1 Pandan Crescent  
Singapore 128461  
Tel (65) 777-8211  
Fax (65) 777-0947  
[Enquiries@AP.EmersonProcess.com](mailto:Enquiries@AP.EmersonProcess.com)



**EMERSON™**  
Process Management