Reference Manual
00809-0100-4420, Rev BA
August 2007

1420 Wireless Gateway

Product Discontinued. Click here for the new WirelessHART document.

EMERSON
Process Management

1420 Wireless Gateway

Physical Device Revision 1.0

Web Server Revision 3.0.10

Network Revision 1.0

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:

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 Rosemount representative.

⚠CAUTION

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 Rosemount Sales Representative.

Cover Photo: 1420_wrong_cover.tif

Table of Contents

Section 1 Introduction

BASIC FUNCTIONALITY AND GENERAL CONSIDERATIONS

The 1420 Wireless Gateway enables wireless, self-organizing devices to communicate with each other, and manages security and connectivity. The gateway is the entry point for wireless device data that is then converted to a format that is compatible with other systems. System integration is possible with Modbus, OPC, TCP/IP via Ethernet or serial connections. The 1420 Wireless Gateway enables users to monitor points that were previously out of reach.

The 1420 Wireless Gateway provides industry leading security, scalability, and functionality. Users can customize security levels to meet plant standards via a web-based interface. This interface also allows monitoring of points, simple trending, customized measuring point lists, basic configuration, and security management. The 1420 Wireless Gateway allows easy network expansion; simply set the Network ID and Join Key on the new device and it will become a part of the existing network.

SYSTEM REQUIREMENTS

In order to properly install and operate the 1420 Wireless Gateway, the Information System computer must meet or exceed the following criteria. For the initial configuration, a PC/Laptop must have an ethernet card and a web browser.

Operating System:

- Windows 2000, service pack 4
- Windows Server 2003
- Windows XP (Home or Professional), service pack 1 or higher

If the operating system requirement is not met, the setup will display a message and stop.

Applications:

- Internet Explorer 6.0 or higher
- Mozilla Firefox 1.5 or higher
- Sun Microsystems™ Java™ Runtime 1.4.1 (or newer)

If the user manual is being installed, the following application is also required:

- Adobe® Acrobat® 5.0 (or newer)

If the Network Assistant or OPC Proxy Setup utilities are being installed, the following application is also required:

- .NET Framework 2.0

If any of the above requirements are not met, the setup disc will install the following:

- Internet Explorer 6.0 service pack 1
- Sun Microsystems™ Java™ Runtime 1.5.0_10
- Adobe® Acrobat Reader® 8.0
- .NET Framework 2.0

Hard disk space:

- Maximum installation (including all upgrades performed by the setup disc): 250 mb

Typical installation (all features, but none of the above installed): 35 mb

Hardware:

Ethernet port

GUIDE TO THE 1420 WIRELESS GATEWAY

Common Terms and Definitions

The following terms and definitions are intended to define how the terms are used in this document. They may vary slightly from their common usage outside this document. See “Glossary” on page Glossary-1 for more terms and definitions.

Term	Definition
Connectivity	Refers to the connection between devices, specifically Path Statistics and Link Reliability in the devices.
Device	Refers to a wireless temperature or pressure transmitter.
Gateway	Refers to the 1420 Wireless Gateway. The interface between a network of devices and an information system. In this case, HART protocol in the devices and Modbus, Serial RS485, and Ethernet outputs.
Information System	This term will be used to describe any information system (computer network), Host System, or Control System. Typical systems include Distributed Control Systems (DCS), programmable logic controllers (PLC), data historians and asset management systems.
Private Network/LAN	A local connection between a 1420 Wireless Gateway and a PC/Laptop. This network is used for commissioning and configuration of the gateway.

Parts

The 1420 Wireless Gateway comes packaged with one Crossover Cable, four metal conduit entry plugs, and one Installation CD. If any of these are missing, please contact Rosemount Customer Central.

Conduit Entries

There are four ½” NPT Conduit entries. Any unused entries should be sealed using the metal plugs provided with the 1420 Wireless Gateway.

Upper Cover

The region of the 1420 Wireless Gateway behind the upper cover houses the gateway’s electronics, including the processor and the RS485 communication board. This area should not need to be opened at any time during installation or operation.

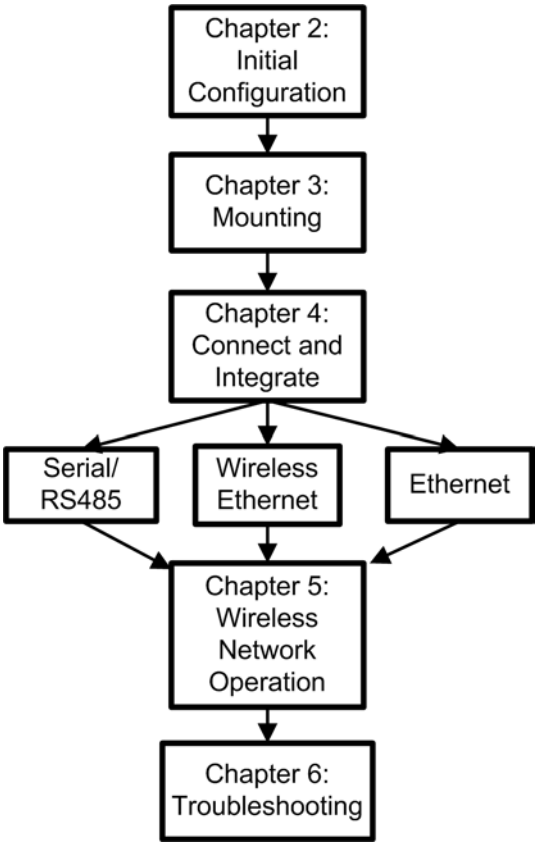
Lower Cover

The lower cover of the 1420 Wireless Gateway houses the junction box. The junction box houses the terminal block, which has connections for the power supply, Modbus output, Ethernet output, redundant Ethernet output and a Power Over Ethernet (POE) connection.

WARNING
Using the POE receptacle with a standard Ethernet or non-Rosemount wireless radio may result in equipment damage.

GUIDE TO THE 1420 WIRELESS GATEWAY MANUAL

This manual will guide you through the Initial Configuration, Mounting, Data Connection, Wireless Network Operation, and Troubleshooting of the 1420 Wireless Gateway. It also includes several Appendices for additional information including Reference Data, Approvals Information and Modbus Integer Scaling. At the end of the manual is a glossary of terms for your convenience.



Section 2: Initial Configuration

This chapter will describe how to connect directly to the 1420 Wireless Gateway for initial configuration using a PC/Laptop and the Crossover Cable. This process will prepare the 1420 Wireless Gateway to function properly when connected to the Information System.

Section 3: Mounting

This chapter will describe how to properly mount the 1420 Wireless Gateway. It will provide information for installing the gateway indoors versus outdoors, on a pipe or a bracket, and information about connecting an antenna.

Section 4: Data Integration

This chapter will describe how to establish a connection from the 1420 Wireless Gateway to the Information System and how to integrate the data collected by the gateway into the Information System. It will focus on the three primary interfacing methods: Serial/RS485, Ethernet, and Wireless Ethernet.

Section 5: Wireless Network Operation

This chapter will describe how to operate the wireless network after it is installed. Specifically it will cover fortification techniques and username/password management.

Section 6: Troubleshooting

This chapter will describe common problems and their solutions in three primary subjects: Physical Connections, Wireless Device Connectivity, and Application Integration Troubleshooting.

Glossary and Appendices

Included in this manual is a glossary of terms and definitions. The appendices will provide additional and more specific information on a variety of subjects.

WARNING
You will see warnings like this throughout the manual. They will refer to specific hazards regarding safety of personnel and equipment.

BEST PRACTICES
You will see callouts like this throughout the manual. They will refer to best practices involved in installing, configuring and maintaining your wireless network.

HINT/TIP
You will see callouts like this throughout the manual. They will refer to hints and tips involved in installing, configuring and maintaining your wireless network.

SECURITY
You will see callouts like this throughout the manual. They will refer to specific important details about ways to secure your wireless network.

Section 2 Initial Configuration

⚠WARNING

Explosions could result in death or serious injury:

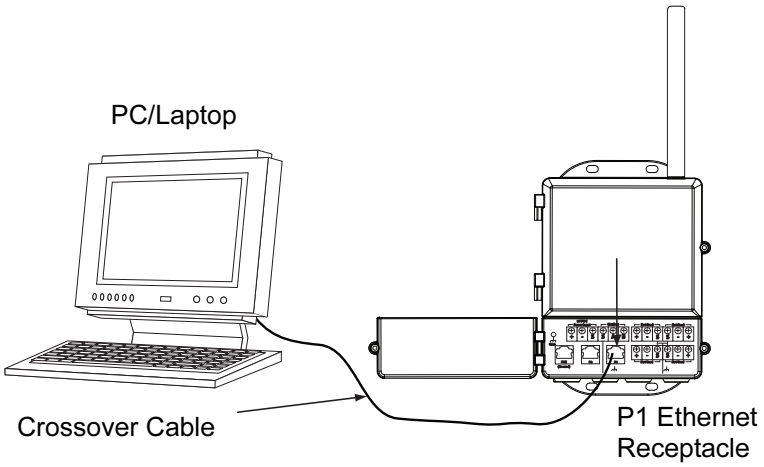
- In an Explosion-Proof and Flame-Proof environment, do not open the 1420 Wireless Gateway electronic housing in an explosive atmosphere.

COMMISSIONING

To configure the 1420 Wireless Gateway, a local connection between a PC/laptop and the 1420 Wireless Gateway must first be established. This can be done with the crossover cable and a PC/laptop dedicated to the 1420 Wireless Gateway, or a PC/laptop used for another purpose can be temporarily configured for the task.

HINT/TIP
If a PC/laptop from another network is used, carefully record the current IP address and other settings so the PC/laptop can be returned to its original network when configuration of the 1420 Wireless Gateway is finished.

If using a PC/laptop attached to another network, shut down the PC/laptop and remove it from the network before proceeding to set up the 1420 Wireless Gateway local connection.



Configure from the CD

The simplest way to configure the PC/laptop for use with the 1420 Wireless Gateway is to use the Network Assistant installed from the CD included with the 1420 Wireless Gateway.

Configuration of the gateway is done through its web interface. To access the device, you must create a private LAN with a subnet of 192.168.1.XX. The gateway will appear on this LAN at the IP address 192.168.1.10.

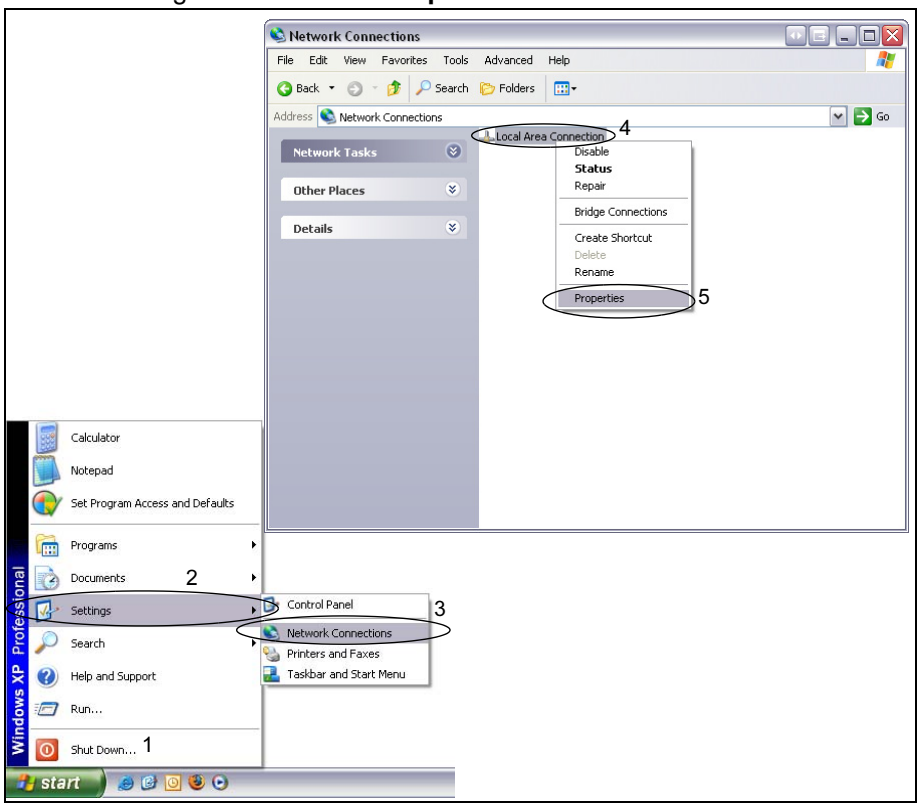
1. Using the supplied cross-over Ethernet cable, attach your PC to the 1420 Wireless Gateway's P1 receptacle.
2. Launch the Network Assistant on your PC/laptop by double-clicking on its desktop icon or by selecting it from the start menu.
3. If prompted, select the network adapter that you connected to the 1420 Wireless Gateway.
4. Click on the **Direct** button to establish a direct connection to the 1420.

When you are ready to remove the PC from the 1420 first open the Network Assistant and select **Normal** to return the settings of the PC/laptop to their original values. To check the connection, proceed to step 5 below.

Configure Manually

The PC/laptop address and host settings can also be changed manually using the following procedure for Internet Explorer on Windows XP. The procedure for other operating systems and web browsers may vary slightly:

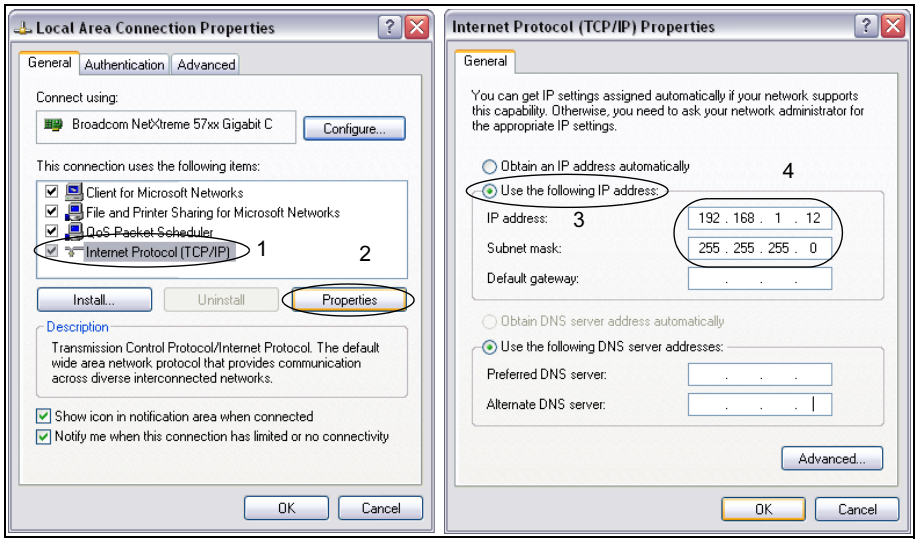
1. On the PC/laptop, install the Java Plug-in found on the CD provided with the 1420. The Plug-in can also be found at http://java.com/
2. Under Network Connections:
   a. Select **Local Area Connection**
   b. Right click to select **Properties**.



c. Select **Internet Protocol (TCP/IP)**, then click the **Properties** button

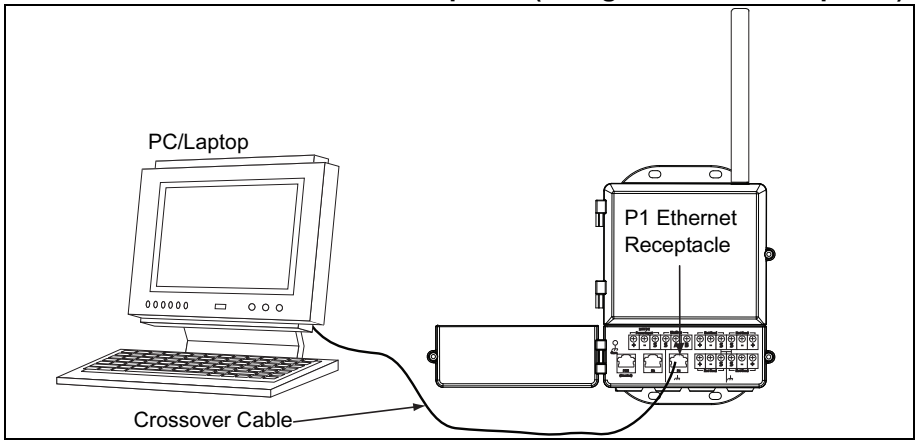
d. Select the **Use the following IP address** button and set the IP address to **192.168.1.12**

e. Set the **Subnet Mask** to **255.255.255.0**



f. Select **OK** for each of the settings windows that have opened.

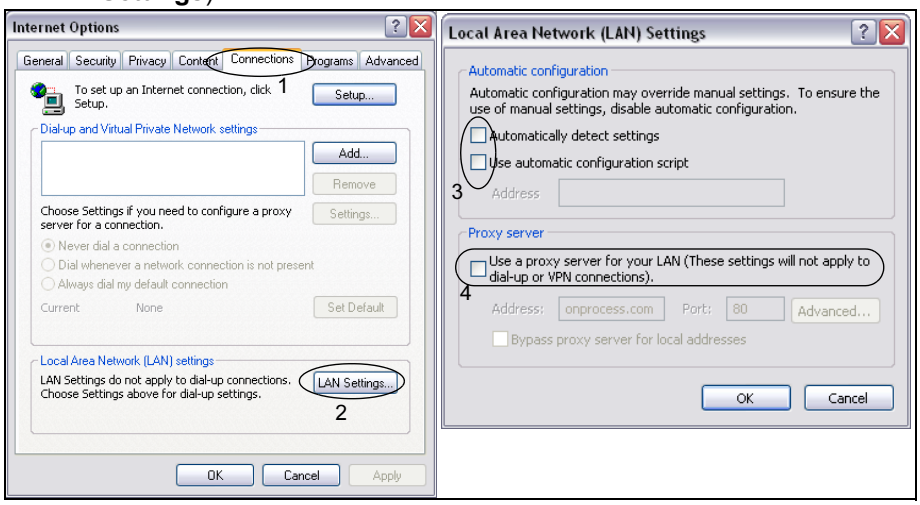
3. Using the supplied crossover Ethernet cable, attach your PC/laptop to the 1420's **P1 Ethernet Receptacle (far right Ethernet receptacle)**.



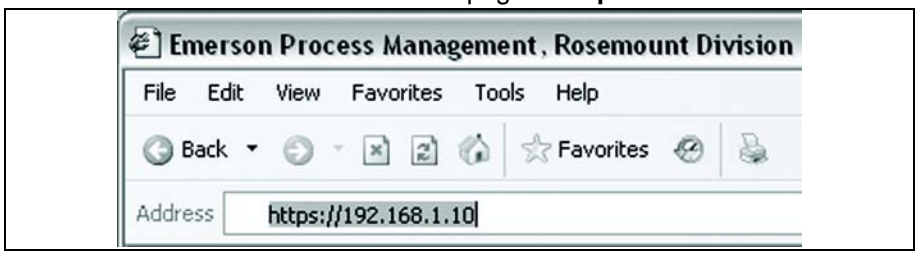
WARNING
Do not connect to the P3 Power Over Ethernet (POE) port. This port supplies power and could potentially damage the PC/laptop.

4. Open a standard web browser (Internet Explorer, Mozilla Firefox or similar).

5. Uncheck proxies (**Tools>Internet Options>Connections>LAN Settings**)



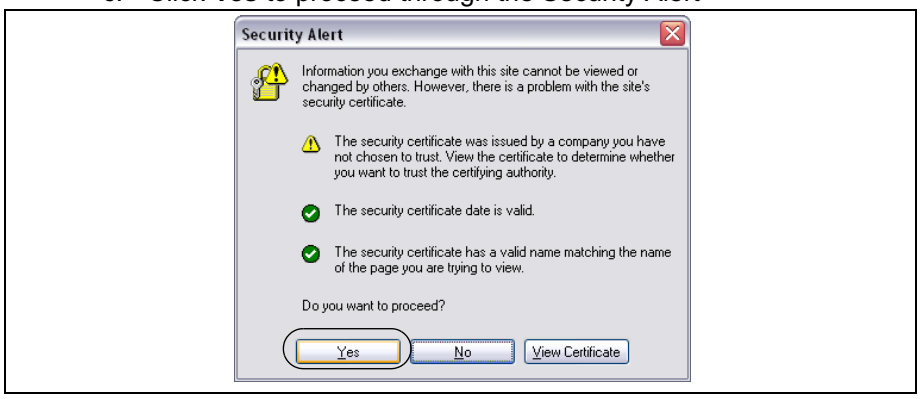
6. Access the 1420's default web page at **https://192.168.1.10**



   a. Log on as User: **admin**

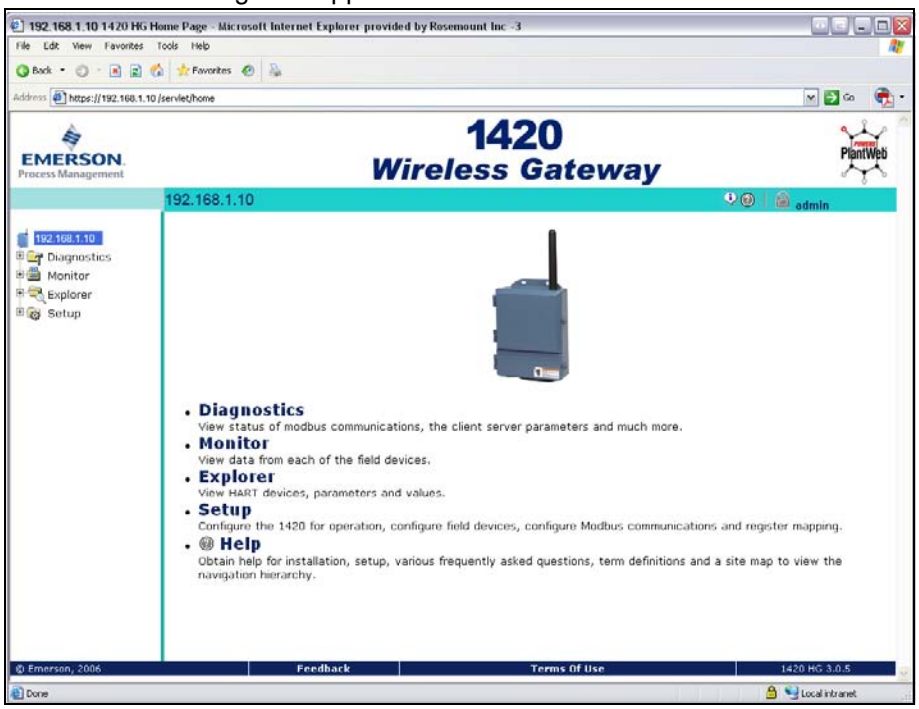
   b. Password: **default**

c. Click **Yes** to proceed through the Security Alert



To prevent future security warnings, navigate to **Setup>Security>Certificates**, then click the **Import 1420 certificate into web browser** button.

The 1420 Home Page will appear as shown below.



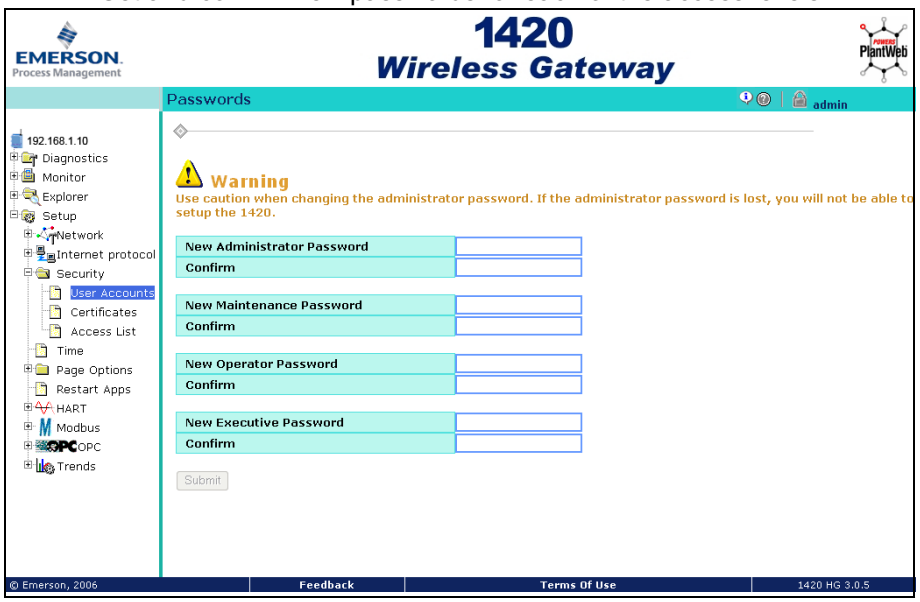
CONFIGURATION

Basic Security Configuration

Click **Setup>Security>User Accounts** to change the passwords. These passwords allow for varying levels of application access. The administrator can modify any system or field device setting. In contrast, the operator is only able to modify some parameters. Use caution when changing the administrator password. If the administrator password is lost, you will not be able to set up the 1420. The 1420 is shipped with the following default passwords:

To configure the basic security of the 1420 Wireless Gateway, perform the following steps.

1. Navigate to **Setup>Security>User Accounts**
2. Set and confirm new passwords for each of the access levels



3. Click **Submit**

Table 2-1. Default Passwords

ID	PASSWORD
Executive (exec)	default
Operator (oper)	default
Maintenance (maint)	default
Administrator (admin)	default

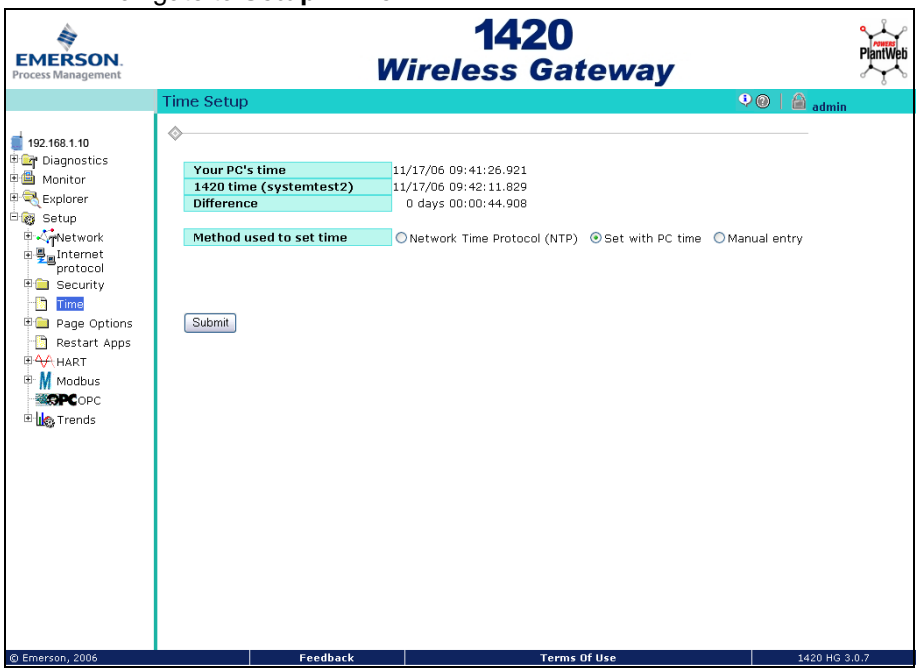
Table 2-2. Access Table

Role	HTML Access
Executive (exec)	With the exception of factory settings (Setup/factory.html), can get any page (Read-Only access).
Operator (oper)	No additional privileges
Maintenance (maint)	• Can set device tags • Can configure Modbus communications • Can configure Modbus register map
Administrator (admin)	• Can configure network settings (address, default). • Can set passwords • Can set time settings • Can set home page options • Can restart applications

BEST PRACTICES
It is recommended that passwords be changed for security purposes. Consult your Network Administrator for guidelines on setting passwords.

Time Configuration

1. Navigate to **Setup>Time**



2. Select method and click **Submit**

Ethernet Network Configuration:

Once a local connection with the 1420 Wireless Gateway is established, configuration can be performed using the Gateway's User Interface. The settings can be modified to ensure best performance when the 1420 Wireless Gateway is permanently installed and integrated into the Information System.

If the gateway is connected to a LAN or if more than one gateway will be used on a private network, the unit will need to be given a new IP address and a new hostname. A new entry will need to be added to your host file with the new IP address and Host name using the Network Assistant or the manual procedure described above.

Address

If you will be attaching the 1420 Wireless Gateway to an internal Intranet, you may select to have the device obtain an IP address via DHCP or be statically assigned an IP address (Figure 2-1). Contact your network administrator if you are not sure which selection is appropriate.

BEST PRACTICES
The 1420 should be assigned a static IP address.

1. Determine 1420 Ethernet Port for connecting to Ethernet Network

NOTE
If using a wired connection, use Port 1 (P1)

IT/Process Control Network Administrator or Technician can provide the following:

a. 1420 fixed IP Address or DHCP Host Name

b. Netmask (Subnet Mask)

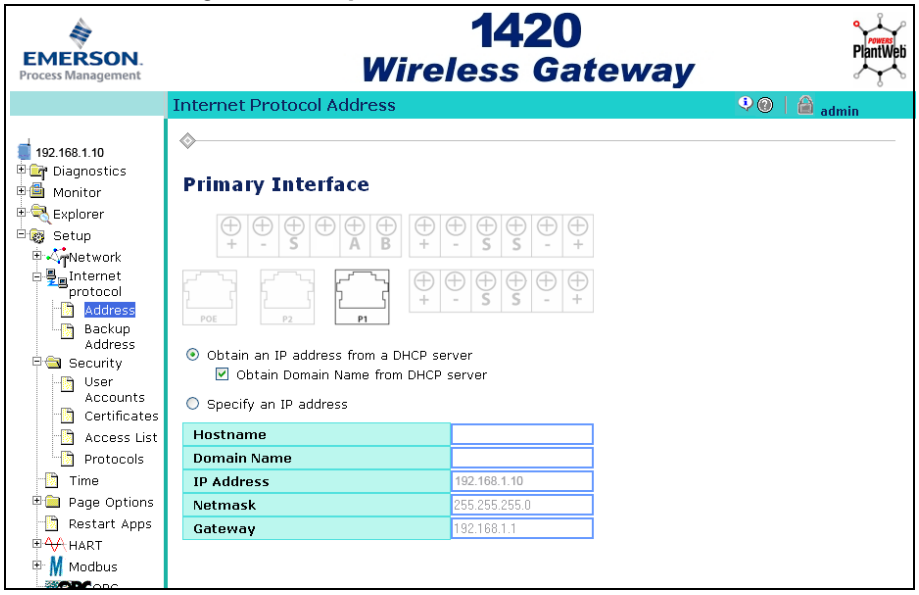
c. Gateway

BEST PRACTICES
Keep these values in a secure location not accessible by unauthorized personnel.

2. Configure 1420 Ethernet IP settings

   a. Access the 1420 with **Administrator** access

   b. Navigate to **Setup>Internet Protocol>Address**

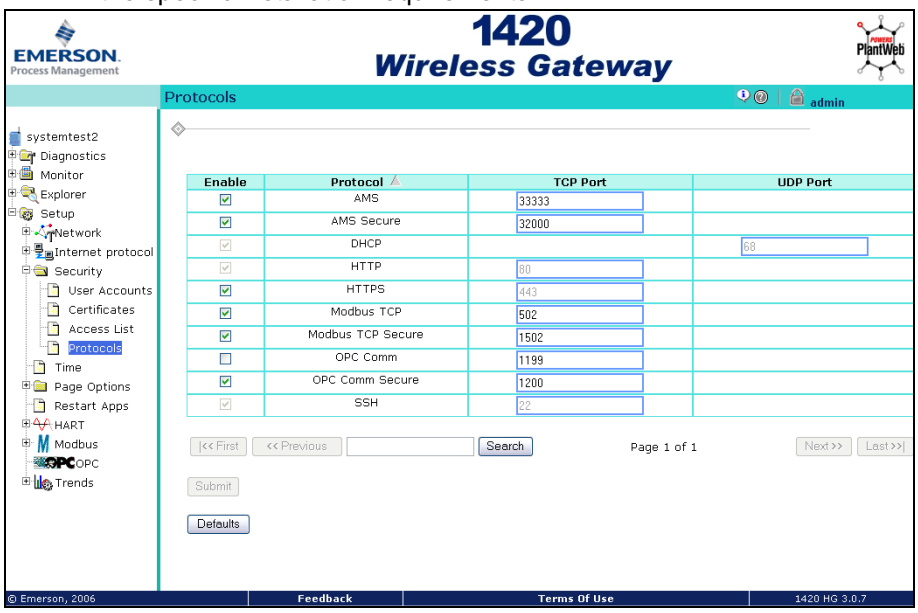


   c. Enter configuration information determined above

3. To complete configuration without a firewall, click **Submit** and proceed with 1420 Restart when prompted.

To configure the 1420 for an Ethernet Network with a firewall, perform the following steps:

1. Navigate to **Setup>Security>Protocol**
2. Click to enable or disable security in the various protocols
   The ports listed are the 1420 defaults. They may be changed to suit the specific installation requirements.



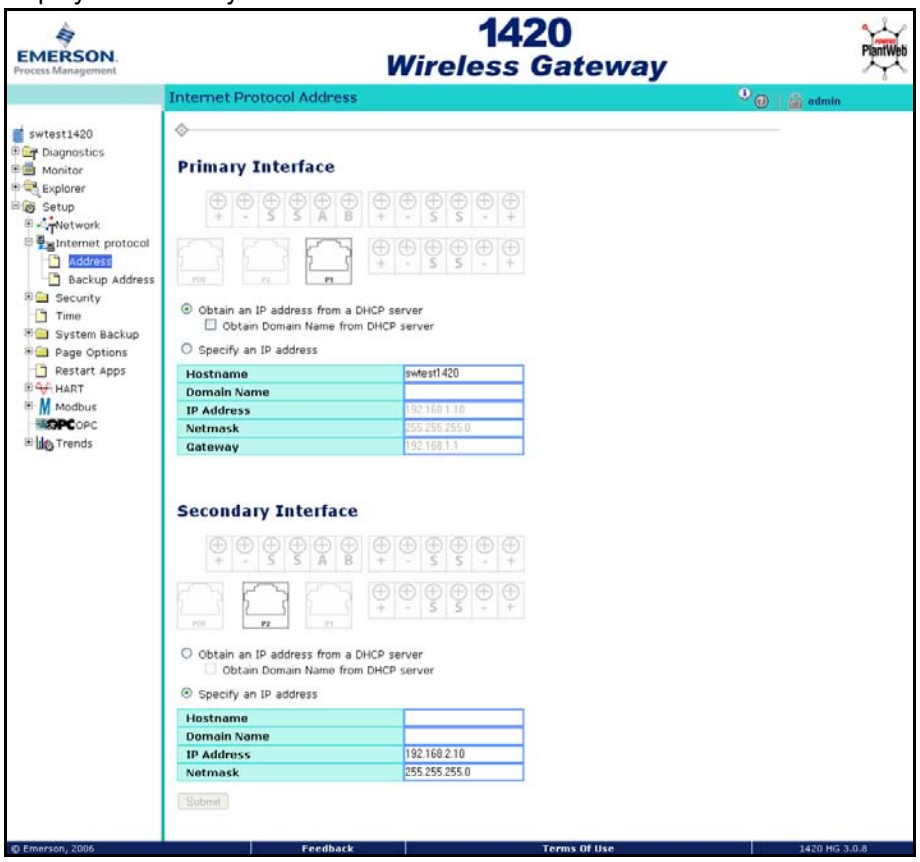
3. Click **Submit** and proceed with 1420 Restart when prompted

Redundant Ethernet Configuration

BEST PRACTICES
To protect against accidental misconfiguration of IP addresses, best practice is to change the IP address for Ethernet Receptacles P1 and P2 one at a time. If P1 is misconfigured, it can be reconfigured from P2.

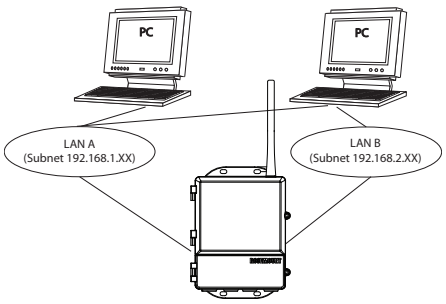
.

If the 1420 Wireless Gateway has been ordered with a redundant network interface, the network setup page (**Setup>Internet Protocol>Address**) will display a secondary interface as shown below.



The second network interface allows the 1420 to be accessed with two separate network addresses. The redundant interfaces provide the 1420 with a degree of fault tolerance to network failures. The network topology shown in Figure 2-1 is supported.

Figure 2-1. Redundant Ethernet Network Topology

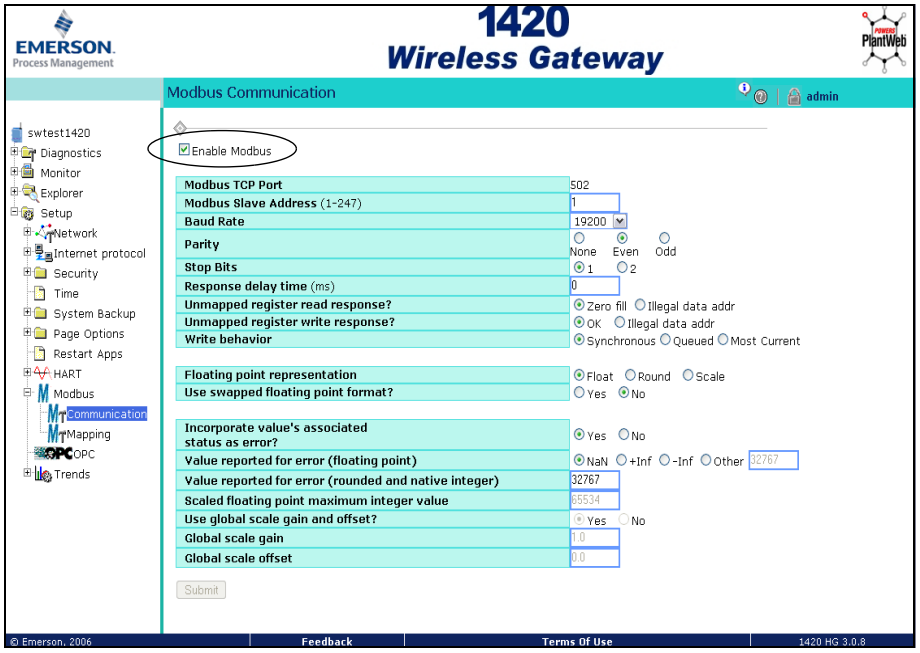


NOTE
The subnet numbers listed in the diagram are an example. Any valid network subnets are acceptable.

If you will be using the redundant ethernet feature, you may select to have the device obtain an IP address via DHCP or be statically assigned an IP for the secondary interface. Contact your network administrator if you are not sure which selection is appropriate.

Serial Connection Configuration:

1. Configure 1420 Serial Communication Settings
   a. Access the 1420 Web Interface with **Administrator** access
   b. Navigate to **Setup>Modbus>Communication**
   c. Click **Enable Modbus**



   d. Configure the 1420 Modbus Communication settings to match the Host Modbus settings

HINT/TIP
Modbus communications will fail if they are not configured identically on the Host and the 1420.

   e. Click **Submit** and proceed with restart

2. When configuration is completed, disconnect the PC/laptop from the 1420 and return the PC/laptop to its previous network settings.

RETURN PC/LAPTOP TO ORIGINAL SETTINGS

When initial configuration of the 1420 Wireless Gateway is complete, you may disconnect the PC/Laptop from the Gateway and return it to its original network settings. The 1420 Wireless Gateway should now be prepared for integration into the Information System.

Section 3 Mounting

OVERVIEW

This chapter will describe how to properly mount the 1420 Wireless Gateway.

Safety Messages

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

Warnings

⚠WARNING

Explosions could result in death or serious injury:

- Do not remove the transmitter from its mounting enclosure in explosive atmospheres when the circuit is live.
- Verify that the operating atmosphere of the transmitter is consistent with the appropriate hazardous locations certifications.

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.

General Considerations

The 1420 Wireless Gateway may be mounted in any General Purpose location. Be sure the covers are secured tightly to prevent exposure of the electronics to moisture and contamination.

The gateway should be mounted in a location that allows convenient access to the Information System, preferably at least three feet (1 meter) above any structures in the canopy (for example, above the roof of the control room). If this is not possible, place it near the closest wired integration point.

If outdoor mounting is not an option, connect the gateway to a remote omnidirectional antenna using a cable no longer than 50 feet (15 meters).

Consider the location of the wireless devices that will be routed through the 1420 Wireless Gateway as well to ensure robust network connectivity. Additional devices may be required to maintain optimal connectivity.

The 1420 Wireless Gateway is capable of handling networks of up to 100 transmitters. The closest transmitters should be at a maximum of 100 feet away from the 1420.

The gateway can be mounted to a support bracket on a wall or to a pipe.

MOUNTING CONSIDERATIONS

For highest signal quality, mount the 1420 Wireless Gateway outdoors. In this case, a minimum rating of Class I Div 2 or Zone 2 is required. Install the gateway at least three feet (1 m) above other structures.

If outdoor mounting is not an option, connect the gateway to a remote omnidirectional antenna using a cable no longer than 50 ft. (15 m).

Install the gateway first. Doing so allows you to check for proper operation of each device as it's added to the network and begins communicating with the gateway.

PHYSICAL INSTALLATION

For dimensional drawing information refer to Appendix A: Reference Data on page A-4.

The cast aluminum housing encloses the electronics and circuitry of the gateway. The front of the enclosure has two covers; an upper cover and a lower cover.

The upper cover provides access to the electronics assembly which includes the microprocessor. Normally the upper cover does not need to be opened. The lower cover provides access to the junction box which contains the terminals for the power supply, and Ethernet and Serial Modbus connections.

Mounting Procedure

Mounting the Gateway to a Support Bracket

The following hardware and tools are needed:

- Four 15/16 inch bolts
- Mounting support bracket
- 3/8 inch drill
- 1/2 inch wrench

Mount the gateway by doing the following:

1. Drill four 3/8 inch (9.525 mm) holes in the support bracket, corresponding with the holes on the 1420 housing.
2. Using a 1/2 inch socket-head wrench, attach the module to the support bracket with four 15/16 inch bolts.

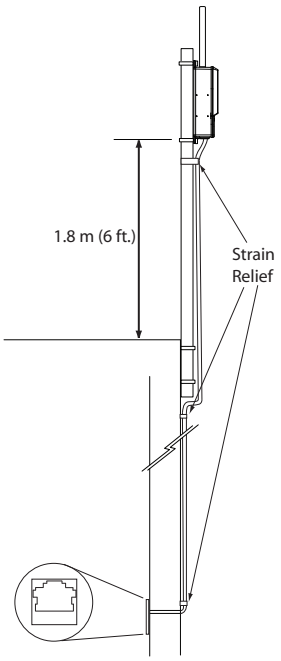
Mounting the Gateway to a Pipe

The following hardware tools are needed:

- Two 5/16 inch U-bolts
- 1/2 inch wrench

Mount the gateway by doing the following:

1. Insert one U-bolt around the pipe and through the top mounting holes of the pipe mount and the module and another U-bolt through the bottom mounting holes of the pipe mount and the module.
2. Using a 1/2 inch socket-head wrench, fasten nuts to the U-bolts.



Wiring the Module

Module wiring is done in the terminal block. For access to the terminal block, open the lower junction box cover. The terminal block label is located on the inside of the module junction box cover and is also found in Figure 3-1 on page 3-4.

Grounding the Module

If mounting the 1420 Wireless Gateway in the field, ground the module with a connection of 1 Ω or less leading from the external grounding lug to earth ground. If mounting the module in the control room, a cabinet ground is sufficient. In either location, follow local or plant electrical codes.

At the bottom of the junction box in 1/2 inch NPT conduit entries are four plastic plugs that were placed there at the factory. Four metal plugs were shipped with the module and are used to seal any unused ports.

The module 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.

The internal Ground Connection located with the supply terminals is the Internal Ground Connection screw. This screw is identified by the following symbol:

NOTE
Grounding the module case via threaded conduit connection may not provide sufficient ground.

Module Input Power Connection

The module is designed to be powered by 24 V dc power. Use a power supply suitable for 185°F with sufficient capacity to power the module. The 1420 Wireless Gateway requires 500 mA of current. The positive and negative power terminals are found on the left side of the terminal block. A case ground is also found on the left hand side of the compartment.

The wiring should include an external power shut-off switch or an external circuit breaker. This device should be located near the module.

BEST PRACTICES
Use an uninterruptible power supply (UPS) to ensure that the network is still functional should there be a loss of power.

Figure 3-1. Terminal Wiring Diagram with Secondary Ethernet and POE Connection

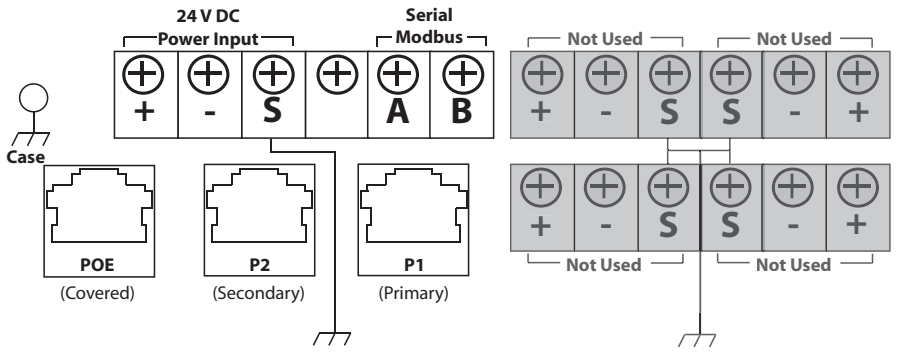
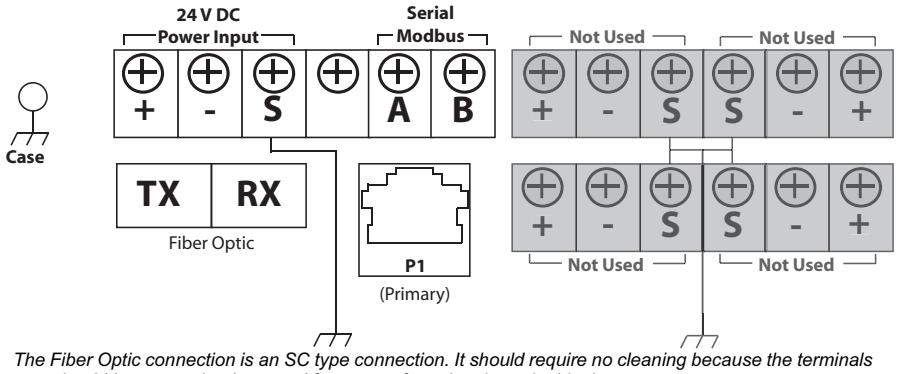


Figure 3-2. Terminal Wiring Diagram with Fiber Optic Connection



The Fiber Optic connection is an SC type connection. It should require no cleaning because the terminals should have remained covered from manufacturing through shipping.

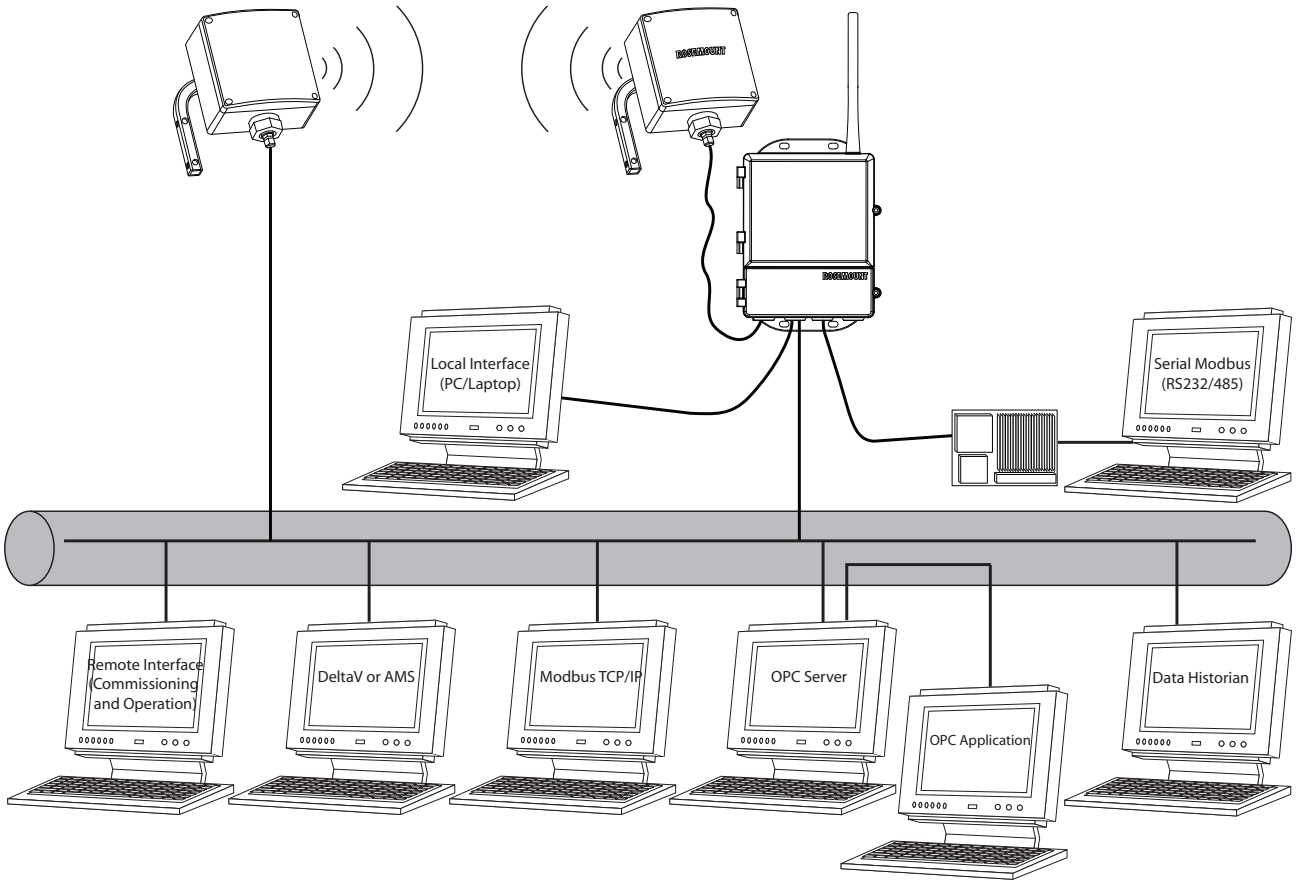
ATTACHING A REMOTE ANTENNA

A remote mount antenna is available (consult factory). It attaches to the 1420 Wireless Gateway via the antenna adapter on the top of the housing. This antenna is omnidirectional and includes a **50 foot long cable** to allow for it to be mounted in an optimal location, even if the 1420 Wireless Gateway cannot.

CONNECTING THE GATEWAY

This section will describe how to connect the 1420 to a Serial Modbus (RS485) system, an Ethernet system or a Wireless Ethernet system. Some applications may require multiple connection types - for example, to support both a DCS and a data historian. The 1420 is able to support such applications.

Figure 3-3. 1420 Connection Options



Considerations for the Protocols

Ethernet

When installing an Ethernet connection, cabling will need to be run from the 1420 Wireless Gateway to an access point on the Ethernet Network. Be sure to consider the length of the cable and the availability of an access point.

Wireless Ethernet

When installing a Wireless Ethernet connection, a stable connection will need to be available between the 1420 and the Ethernet Network. Be sure to consider the constraints of such a connection.

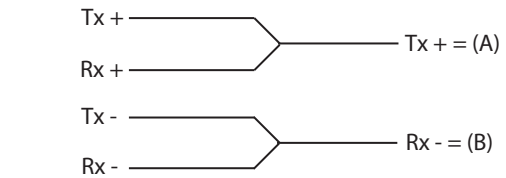
Serial Modbus

When installing a Serial Modbus connection, cabling will need to be run from the 1420 Wireless Gateway to the Modbus PLC or DCS. Be sure to consider the length and location of this cable. Key information required by the administrator will be the number of Modbus registers required for integration. A good estimate for the number of registers is three registers for each data point so that the process variable and device status indicators can be remotely monitored.

BEST PRACTICES
Typically, twisted shielded pair cable is used to wire the Serial connection. Standard practice is to ground the shield on the Serial Host side and leave the shield floating on the 1420 side. Be sure to insulate the 1420 shield to avoid grounding issues.

HINT/TIP
In most systems, A = Tx + and B = Rx -. In some systems, this is reversed. For 4-wire systems, see Figure 3-4.

Figure 3-4. Typical Full Duplex (4-wire) to Half Duplex (2-wire) Conversion Diagram



Confirm wiring configuration with host system documentation.

NOTE:
Do not open the 1420 electronics housing in an explosive atmosphere.

Ethernet

The 1420 Wireless Gateway is equipped with two 10/100 Base-T Ethernet interface receptacles on the left side of the terminal block (Figure 3-1 on page 3-4). When installing the gateway, you may connect the 1420 Wireless Gateway to an existing Ethernet Hub, Switch or Router.

The primary Ethernet port (P1) is used to connect to the Information System, specifically a Remote Interface Machine, an OPC Proxy Machine (and an OPC Application Machine), or a Modbus TCP Application Machine. This can be done over a non-encrypted Ethernet connection or over an encrypted Ethernet connection using the Security Setup application.

SECURITY
The most secure option is to connect over an encrypted Ethernet connection using the Security Setup application.

The second Ethernet port (P2) on the 1420 Wireless Gateway terminal block is an optional factory-configured redundant Ethernet port. (ordering option Output Code 2)

Wireless Ethernet

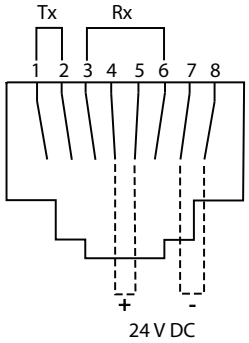
The 1420 Wireless Gateway is capable of communicating to the Information System via a Wireless Ethernet connection. This allows for greater flexibility in placement of the gateway with the same functionality as a standard Ethernet connection.

To install a wireless ethernet connection, simply mount the 1420 Wireless Gateway, then mount the wireless antenna. Remove the cap from the Power Over Ethernet (POE) receptacle and connect the antenna cable to the POE receptacle (Figure 3-1 on page 3-4).

WARNING
Connecting a standard wireless radio to the POE receptacle may result in damage to equipment.

HINT/TIP
To use a standard wireless radio, confirm that the radio is compatible with the 1420 Wireless Gateway's POE specifications, or use an externally powered radio connected to the P1 Ethernet port.

Figure 3-5. POE Specifications



The POE Port is 24 VDC, ± 4; 500 mA.

Compare to the standard wireless radio specifications and confirm that the radio is compatible with the POE Port before connecting.

When installing the gateway, you may connect the 1420 Wireless Gateway to an existing Ethernet Hub, Switch or Router. This connection is used to communicate with the Information System, specifically a Remote Interface Machine, an OPC Proxy Machine (and an OPC Application Machine), or a Modbus TCP Application Machine. This can be done over a non-encrypted Ethernet connection or over an encrypted Ethernet connection using the Security Setup application.

SECURITY
The most secure option is to connect over an encrypted Ethernet connection using the Security Setup application.

Modbus

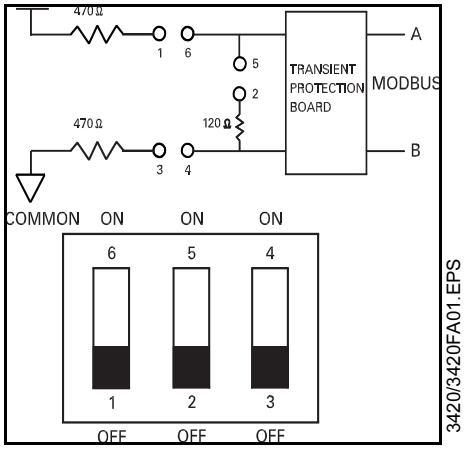
The Modbus interface terminals are located in the upper-middle of the wiring block next to the power input (Figure 3-1 on page 3-4). The Modbus interface is polarity sensitive. Connect the negative to the right-most Modbus terminal (B) and the positive to the center Modbus terminal (A). The left-most terminal is for the cable shield, if it is required.

Modbus Termination Setup

Modbus RTU is transmitted on an RS485 physical layer. Three dip-switches are provided to enable the RS485 circuitry with a network terminator. The switches are found inside the electronics housing on the RS485 communication board located in the top center of the housing. Switch 2 places a 120 ohm terminator on the bus. This would be used to match cable impedance if needed to dampen reflections on long cable runs. Its use will depend on the baud rate and cable length of the Modbus network.

Switches 1 and 3 are connected to pull-up and pull-down resisters on the Modbus network. These resisters are used to prevent noise from being interpreted as valid communications during periods when no communications are occurring on the network. Only one set is required on an RS485 network.

Figure 3-6. Modbus Setup

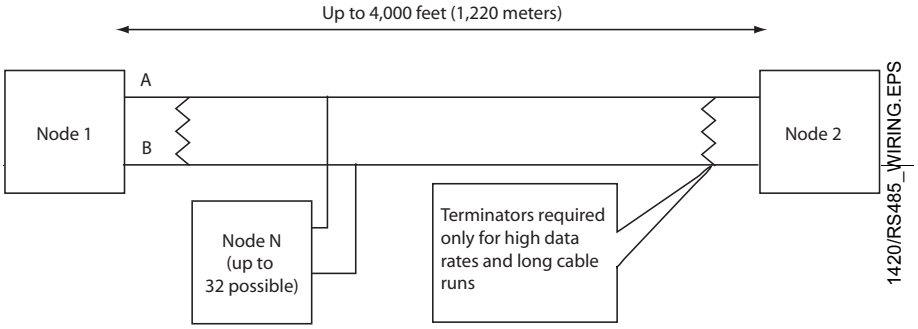


RS485 Serial Interface

The RS485 standard describes a balanced transmission line operating in a shared or multi-drop model. As many as 32 driver/receiver pairs can share a single network.

Figure 3-7 shows a typical two-wire multi-drop network such as used with the 1420 Wireless Gateway. The RS485 specifications indicate that the transmission line should be terminated at both ends of the network. However termination should only be used with high data rates above 115kbps and long cable runs so it should not be necessary with the transmission rates used by the 1420 Wireless Gateway.

Figure 3-7. Typical two-wire multi-drop network.



Section 4 Data Integration

⚠WARNING

Explosions could result in death or serious injury:

- In an Explosion-Proof and Flame-Proof environment, do not open the 1420 Wireless Gateway electronic housing in an explosive atmosphere.
- Cover must be fully engaged to meet Explosion-Proof requirements.

DATA INTEGRATION

The 1420 Wireless Gateway is capable of integrating data from wireless measurement devices into a number of information systems. This chapter will describe how to integrate the data using the three available output protocols: Ethernet (TCP/IP), Wireless Ethernet (TCP/IP) and Serial/RS485.

ETHERNET

The 1420 Wireless Gateway integrates data to the information system via a wired Ethernet connection.

Begin by installing the software on the Information System.

Software Installation

To prepare the Information System to communicate with the 1420 Wireless Gateway, insert the Setup Assistant & Support Files CD that came with the 1420 Wireless Gateway. Follow the directions in the installation windows to install the desired components.

The data application administrator can determine where to install the required software.

At the **Setup Type** screen, select **Complete** or **Custom** depending on your specific needs. Custom setup allows you to choose whether to install the following options:

1420 User Interface	When this feature is selected, setup will install any additional software required to use this PC as a user interface for the 1420. This may include installing Microsoft Internet Explorer and Sun Microsystems Java Runtime.
1420 Reference Manual	When this feature is selected, setup will install an electronic copy of the 1420 Wireless Gateway Reference Manual (this manual) on the PC. This may include installing Adobe Acrobat Reader.
Network Assistant	When this feature is selected, setup will install Network Assistant, a program that automates network configuration changes to support 1420 configuration.
Security Setup	When this feature is selected, setup will install a security application that encrypts communications between the 1420 and AMS, Modbus, OPC, etc.

Once you have selected the desired options, continue with installation by clicking **Next**. Other selectable optional features include a desktop icon for the network assistant, and Security Setup.

Security

If the 1420 Wireless Gateway will be connected through a firewall, run the Security Setup application to allow the gateway to communicate with the Information System. The application requires the IP address of the 1420 Wireless Gateway and the firewall port through which the gateway will communicate with the network.

Verify Connectivity

Verify that the 1420 Wireless Gateway is connected to the Information System and that the data is propagating through correctly. Verification will vary depending on the type of information system being used. Refer to the respective documentation for verification instructions.

Add Wireless Devices

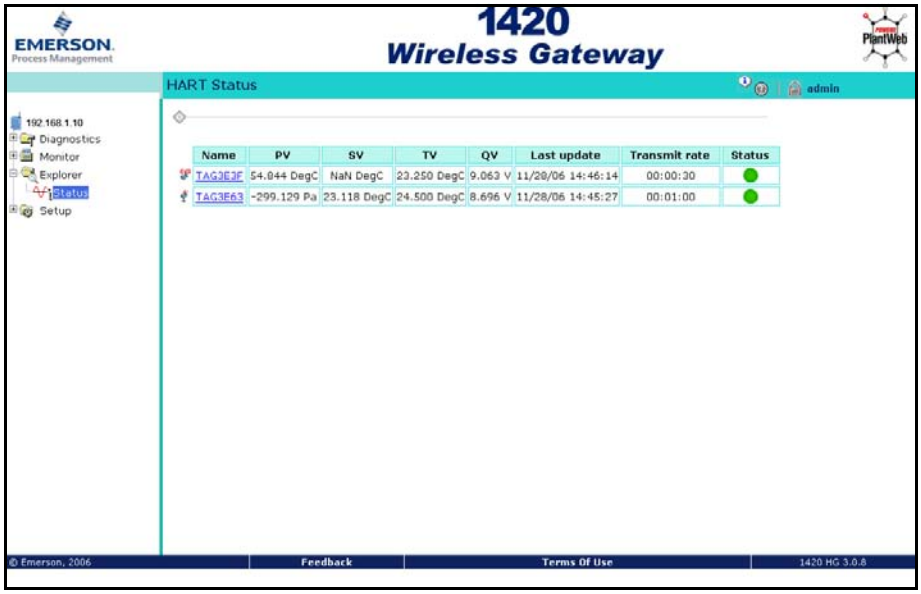
This is done by powering the 1420 Wireless Gateway first, then powering the wireless measurement devices in order of proximity beginning with the devices closest to the gateway. If the Network ID and Join Keys are properly entered, the gateway will automatically detect and organize the devices in the network. Device configuration and installation information is covered in the device manuals: Rosemount 648 Wireless Temperature Transmitter, 00809-0100-4648 and Rosemount 3051S Wireless Pressure Transmitter, 00809-0100-4802.

NOTE
This may take up to several hours depending on the update rate, number of devices and network paths. As devices are added, they will appear in the web interface at the **Explorer>Status** page.

The **Diagnostics>Network>Overview** pages display the following information about the network.

Data Type	Description
Wireless Device Count	**Total count of wireless devices, regardless of state**
Live	**Devices that are connected and reporting data values**
Late	**Devices that are connected and have missed one or two scheduled data values**
Stale	**Devices that are connected and are no longer reporting data values**
Joining	**Devices that are joining the network**
Unreachable	**Devices that are no longer on the network**
Unknown	**Device whose state is not known, not communicating to the gateway**
Conventional HART devices	**Non-wireless HART devices connected to a wireless device router (WDR)**
Devices with unknown tags	**Devices whose tags have not been read yet**
Devices with undefined tags	**Devices with blank or uninitialized tags**
Devices with duplicate tags	**Devices with duplicate tags**
Devices with invalid tags	**Devices with tags containing invalid characters (a period or comma)**
Devices with duplicated IDs	**Devices with duplicate device IDs**

Figure 4-1. Explorer Status



Map Application Data on the Gateway

Modbus

In the user interface, click **Setup>Modbus** to configure the Modbus Interface. This page is automatically redirected to **Setup>Modbus>Communication**. To enable Modbus, check the **Enable Modbus** box at the top of the page.

Communication

Click **Setup>Modbus>Communication (Figure 4-7)** to configure the Modbus Communication settings. The options on this page allow you to configure the Modbus communication settings. These settings should correspond to settings of the Modbus Master. Be sure to check the **Enable Modbus** checkbox at the top of the page.

The measured values can be represented as either a single register integer number, a scaled integer or a two-register (standard or swapped) floating point number. One common difference in Modbus Masters is the representation of a floating point number. The default used by the 1420 is a Standard Floating Point but this configuration page also allows you to use Swapped Floating Point which reverses the order in which the data in the floating point registers is sent. For more on scaled integers, see Appendix E: Integer Scaling on page E-1.

The **Response delay time** entry allows you to have the 1420 Wireless Gateway wait for a specified amount of time before it outputs its response to the master request. Some master devices may not be able to immediately receive the response due to receiver setup time. This setting accommodates those master devices.

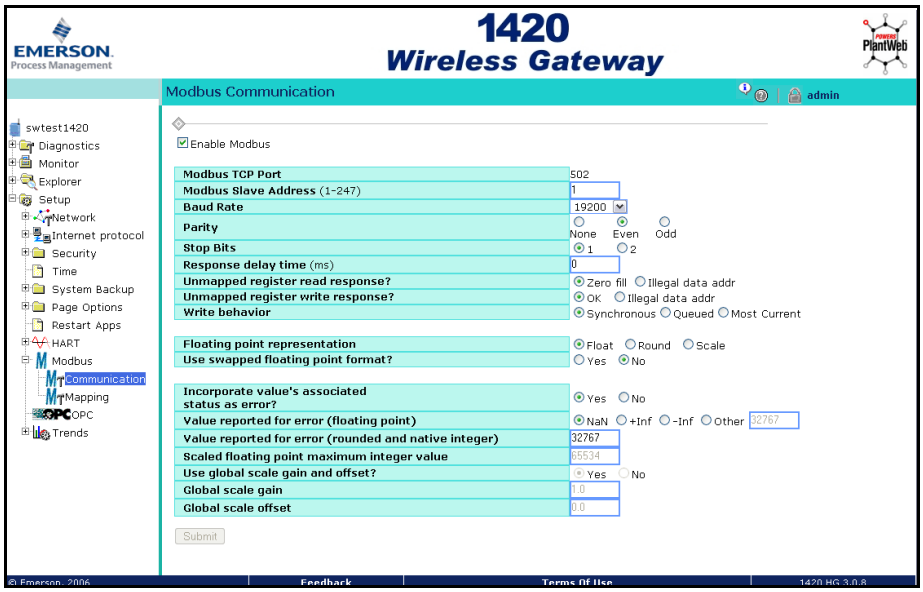
The unmapped register response setting allows the selection of the value entered into a register if no tag is assigned to it.

The Scaled Floating Point option allows the user to return values as a scaled integer rather than the direct integer. Using Gain and Offset, the values can show positive values, negative values or both.

For more on integer scaling, see Appendix E: Integer Scaling on page E-1.

For more information on Modbus, refer to the information system's documentation or http://www.modbus.org/specs.php.

Figure 4-2. Modbus Communication



Modbus Register Map

The Modbus Register Map page is located at **Setup>Modbus>Mapping (Figure 4-8)**. On this page, Modbus Registers can be mapped to the measurement points. Please note that the registers in Table 4-3 are predefined.

To create a new entry, click the **New Entry** button. This will activate a row of text fields in the Modbus Register table. Begin by filling in the **Register Number**, then choose or type the Point Name. Be sure to click **Submit** to implement the changes.

Figure 4-3. Modbus Mapping

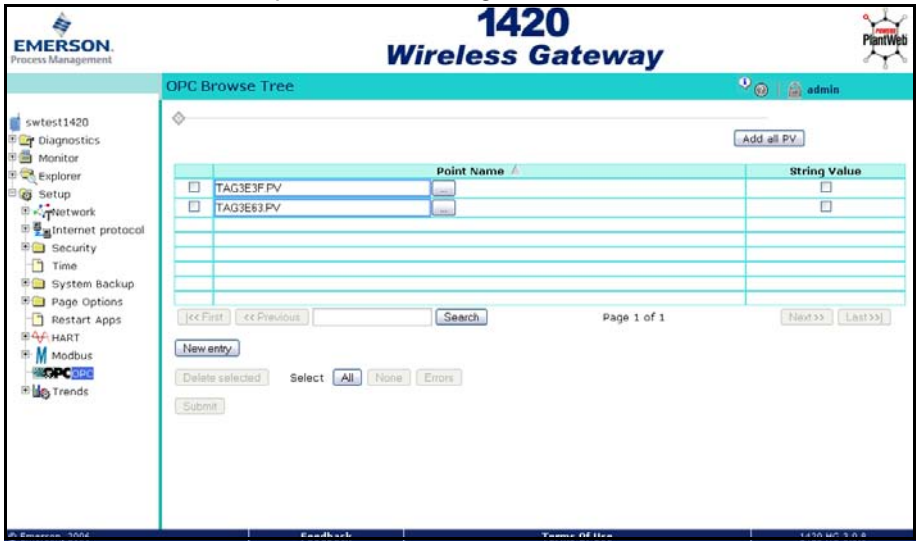
Table 4-1. Predefined Diagnostic Registers

Description	Register
Current Year (1)	49001
Current Month (1)	49002
Current Day (1)	49003
Current Hour (1)	49004
Current Minute (1)	49005
Current Second (1)	49006
Messages Received	49007
Corrupt Messages Received	49008
Messages Sent with Exception (error responses)	49009
Messages Sent Count	49010
Valid Messages Ignored (when in listen only mode)	49011

(1) Time is reported in GMT.

OPC

In the user interface, click **Setup>OPC** to configure the OPC Settings. To choose a new Point Name, click **New Entry**. This will open a text field in the point name table. Type the name of the point in the field or use the chooser to the right (pops up a new window) to select the name of the point. Click **Submit** to save and implement the changes.



Map Application Data on the Information System

Refer to your Information System's documentation for specific instructions regarding mapping application data using the TCP/IP protocol.

WIRELESS ETHERNET

The 1420 Wireless Gateway integrates data to the information system via a wired Ethernet connection.

Begin by installing the software on the Information System.

Software Installation

To prepare the Information System to communicate with the 1420 Wireless Gateway, insert the Setup Assistant & Support Files CD that came with the 1420 Wireless Gateway. Follow the directions in the installation windows to install the desired components.

The data application administrator can determine where to install the required software.

At the **Setup Type** screen, select **Complete** or **Custom** depending on your specific needs. Custom setup allows you to choose whether to install the following options:

1420 User Interface	When this feature is selected, setup will install any additional software required to use this PC as a user interface for the 1420. This may include installing Microsoft Internet Explorer and Sun Microsystems Java Runtime.
1420 Reference Manual	When this feature is selected, setup will install an electronic copy of the 1420 Wireless Gateway Reference Manual (this manual) on the PC. This may include installing Adobe Acrobat Reader.
Network Assistant	When this feature is selected, setup will install Network Assistant, a program that automates network configuration changes to support 1420 configuration.
OPC Client Runtime	When this feature is selected, setup will install software that will allow OPC clients running on this PC to access the 1420.
OPC Proxy Setup	When this feature is selected, setup will install the OPC Proxy Setup program to configure which 1420s will be accessed by OPC clients running on this PC
Security Setup	When this feature is selected, setup will install a security application that encrypts communications between the 1420 and AMS, Modbus, OPC, etc.

Once you have selected the desired options, continue with installation by clicking **Next**. Other selectable optional features include a desktop icon for the network assistant, a desktop icon for OPC Proxy Setup, and whether to start the OPC deviceCOM server automatically.

Security

If the 1420 Wireless Gateway will be connected through a firewall, run the Security Setup application to allow the gateway to communicate with the Information System. The application requires the IP address of the 1420 Wireless Gateway and the firewall port through which the gateway will communicate with the network.

Verify Connectivity

Verify that the 1420 Wireless Gateway is connected to the Information System and that the data is propagating through correctly. Verification will vary depending on the type of information system being used. Refer to the respective documentation for verification instructions.

Add Wireless Devices

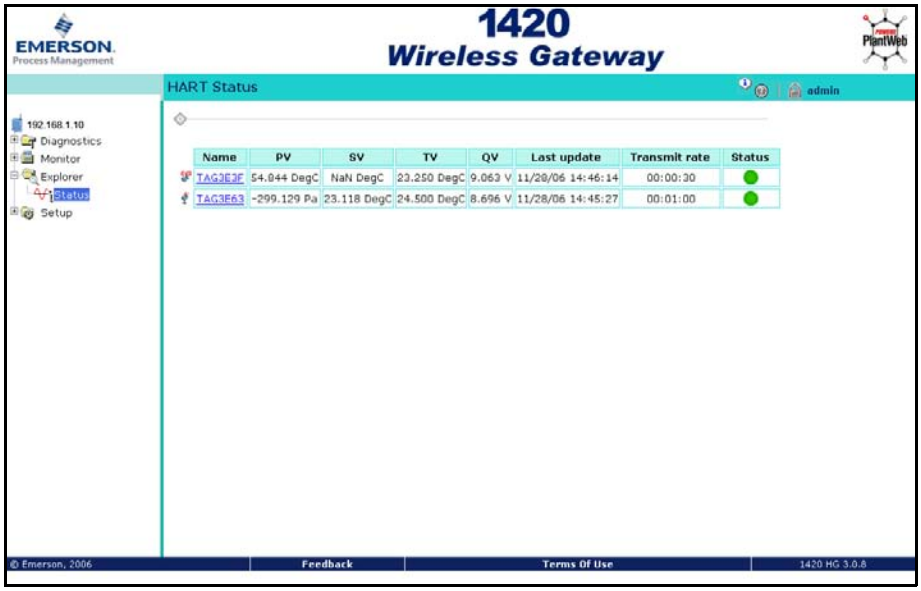
This is done by powering the 1420 Wireless Gateway first, then powering the wireless measurement devices in order of proximity beginning with the devices closest to the gateway. If the Network ID and Join Keys are properly entered, the gateway will automatically detect and organize the devices in the network. Device configuration and installation information is covered in the device manuals: Rosemount 648 Wireless Temperature Transmitter, 00809-0100-4648 and Rosemount 3051S Wireless Pressure Transmitter, 00809-0100-4802.

NOTE
This may take up to several hours depending on the update rate, number of devices and network paths. As devices are added, they will appear in the web interface at the **Explorer>Status** page.

The **Diagnostics>Network>Overview** pages display the following information about the network.

Data Type	Description
Wireless Device Count	**Total count of wireless devices, regardless of state**
Live	**Devices that are connected and reporting data values**
Late	**Devices that are connected and have missed one or two scheduled data values**
Stale	**Devices that are connected and are no longer reporting data values**
Joining	**Devices that are joining the network**
Unreachable	**Devices that are no longer on the network**
Unknown	**Device whose state is not known, not communicating to the gateway**
Conventional HART devices	**Non-wireless HART devices connected to a wireless device router (WDR)**
Devices with unknown tags	**Devices whose tags have not been read yet**
Devices with undefined tags	**Devices with blank or uninitialized tags**
Devices with duplicate tags	**Devices with duplicate tags**
Devices with invalid tags	**Devices with tags containing invalid characters (a period or comma)**
Devices with duplicated IDs	**Devices with duplicate device IDs**

Figure 4-4. Explorer Status



Map Application Data on the Gateway

Modbus

In the user interface, click **Setup>Modbus** to configure the Modbus Interface. This page is automatically redirected to **Setup>Modbus>Communication**. To enable Modbus, check the **Enable Modbus** box at the top of the page.

Communication

Click **Setup>Modbus>Communication (Figure 4-7)** to configure the Modbus Communication settings. The options on this page allow you to configure the Modbus communication settings. These settings should correspond to settings of the Modbus Master. Be sure to check the **Enable Modbus** checkbox at the top of the page.

The measured values can be represented as either a single register integer number, a scaled integer or a two-register (standard or swapped) floating point number. One common difference in Modbus Masters is the representation of a floating point number. The default used by the 1420 is a Standard Floating Point but this configuration page also allows you to use Swapped Floating Point which reverses the order in which the data in the floating point registers is sent. For more on scaled integers, see Appendix E: Integer Scaling on page E-1.

The **Response delay time** entry allows you to have the 1420 Wireless Gateway wait for a specified amount of time before it outputs its response to the master request. Some master devices may not be able to immediately receive the response due to receiver setup time. This setting accommodates those master devices.

The unmapped register response setting allows the selection of the value entered into a register if no tag is assigned to it.

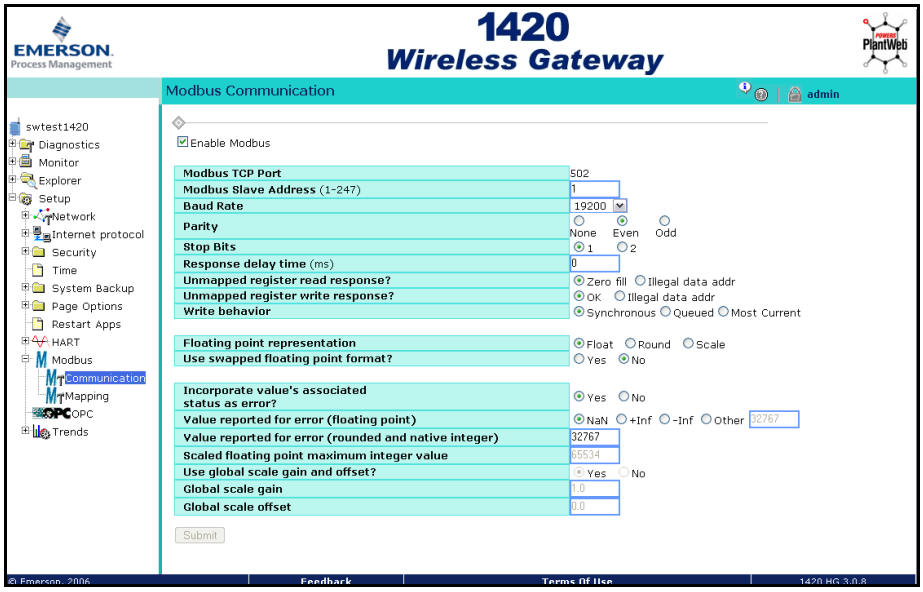
As an option you may elect to have a specified value replace the actual reading from the field device in the event of an error. This will allow a host to recognize an error condition without the need to read a separate set of registers containing the status indicators.

The Scaled Floating Point option allows the user to return values as a scaled integer rather than the direct integer. Using Gain and Offset, the values can show positive values, negative values or both.

For more on integer scaling, see Appendix E: Integer Scaling on page E-1.

For more information on Modbus, refer to the information system's documentation or http://www.modbus.org/specs.php.

Figure 4-5. Modbus Communication



Modbus Register Map

The Modbus Register Map page is located at **Setup>Modbus>Mapping (Figure 4-8)**. On this page, Modbus Registers can be mapped to the measurement points. Please note that the registers in Table 4-3 are predefined.

To create a new entry, click the **New Entry** button. This will activate a row of text fields in the Modbus Register table. Begin by filling in the **Register Number**, then choose or type the Point Name. Be sure to click **Submit** to implement the changes.

Figure 4-6. Modbus Mapping

Table 4-2. Predefined Diagnostic Registers

Description	Register
Current Year (1)	49001
Current Month (1)	49002
Current Day (1)	49003
Current Hour (1)	49004
Current Minute (1)	49005
Current Second (1)	49006
Messages Received	49007
Corrupt Messages Received	49008
Messages Sent with Exception (error responses)	49009
Messages Sent Count	49010
Valid Messages Ignored (when in listen only mode)	49011

(1) Time is reported in GMT.

OPC

In the user interface, click **Setup>OPC** to configure the OPC Settings. This page is automatically redirected to **Setup>OPC>Settings**. To incorporate the value's associated status as OPC quality, click the **Yes** radio button, then click **Submit**.

Click **Setup>OPC>Browse Tree** to map the application data through the gateway. Use this page to choose the **Point Name** and whether to enable the **String Value**.

To choose a new Point Name, click **New Entry**. This will open a text field in the point name table. Type the name of the point in the field or use the chooser to the right (pops up a new window) to select the name of the point. Click **Submit** to save and implement the changes.

Map Application Data on the Information System

Refer to your Information System's documentation for specific instructions regarding mapping application data using the TCP/IP protocol.

SERIAL MODBUS/RS485

The 1420 Wireless Gateway supports Modbus RTU over the RS485 serial port.

Begin by adding the wireless devices. This is done by powering the 1420 Wireless Gateway first, then powering the wireless measurement devices in order of proximity beginning with the devices closest to the gateway. If the Network ID and Join Keys are properly entered, the gateway will automatically detect and organize the devices in the network. Device configuration and installation information is covered in the device manuals: Rosemount 648 Wireless Temperature Transmitter, 00809-0100-4648 and Rosemount 3051S Wireless Pressure Transmitter, 00809-0100-4802.

NOTE
This may take up to several hours depending on the update rate, number of devices and network paths. As devices are added, they will appear in the web interface at the **Explorer>Status** page.

The **Diagnostics>Network>Overview** pages display the following information about the network.

Data Type	Description
Wireless Device Count	**Total count of wireless devices, regardless of state**
Live	**Devices that are connected and reporting data values**
Late	**Devices that are connected and have missed one or two scheduled data values**
Stale	**Devices that are connected and are no longer reporting data values**
Joining	**Devices that are joining the network**
Unreachable	**Devices that are no longer on the network**
Unknown	**Device whose state is not known, not communicating to the gateway**
Conventional HART devices	**Non-wireless HART devices connected to a wireless device router (WDR)**
Devices with unknown tags	**Devices whose tags have not been read yet**
Devices with undefined tags	**Devices with blank or uninitialized tags**
Devices with duplicate tags	**Devices with duplicate tags**
Devices with invalid tags	**Devices with tags containing invalid characters (a period or comma)**
Devices with duplicated IDs	**Devices with duplicate device IDs**

In the user interface, click **Setup>Modbus** to configure the Modbus Interface. This page is automatically redirected to **Setup>Modbus>Communication**. To enable Modbus, check the **Enable Modbus** box at the top of the page.

Communication

Click **Setup>Modbus>Communication (Figure 4-7)** to configure the Modbus Communication settings. The options on this page allow you to configure the Modbus communication settings. These settings should correspond to settings of the Modbus Master. Be sure to check the **Enable Modbus** checkbox at the top of the page.

The measured values can be represented as either a single register integer number, a scaled integer or a two-register (standard or swapped) floating point number. One common difference in Modbus Masters is the representation of a floating point number. The default used by the 1420 is a Standard Floating Point but this configuration page also allows you to use Swapped Floating Point which reverses the order in which the data in the floating point registers is sent. For more on scaled integers, see Appendix E: Integer Scaling on page E-1.

The **Response delay time** entry allows you to have the 1420 Wireless Gateway wait for a specified amount of time before it outputs its response to the master request. Some master devices may not be able to immediately receive the response due to receiver setup time. This setting accommodates those master devices.

The unmapped register response setting allows the selection of the value entered into a register if no tag is assigned to it.

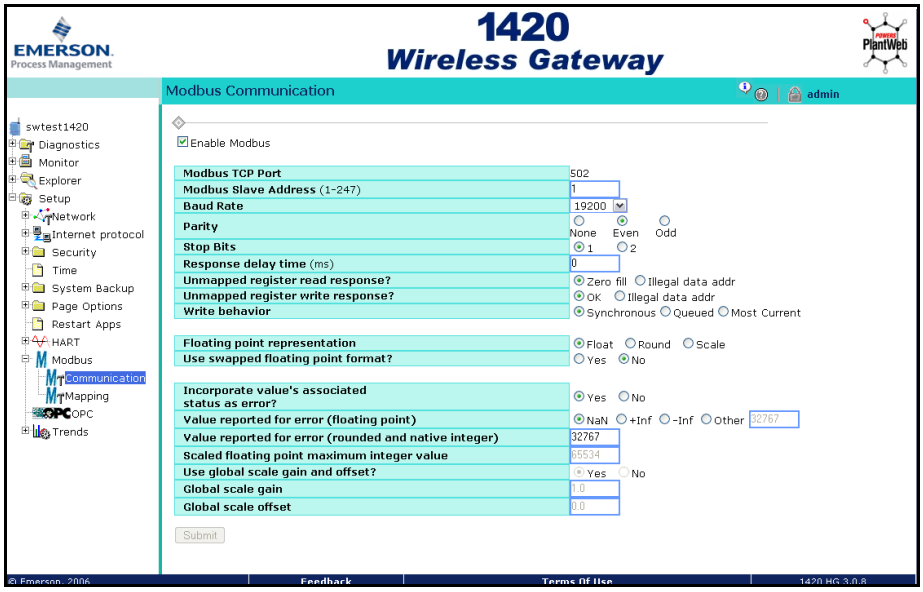
As an option you may elect to have a specified value replace the actual reading from the field device in the event of an error. This will allow a host to recognize an error condition without the need to read a separate set of registers containing the status indicators.

The Scaled Floating Point option allows the user to return values as a scaled integer rather than the direct integer. Using Gain and Offset, the values can show positive values, negative values or both.

For more on integer scaling, see Appendix E: Integer Scaling on page E-1.

For more information on Modbus, refer to the information system's documentation or http://www.modbus.org/specs.php.

Figure 4-7. Modbus Communication



Modbus Register Map

The Modbus Register Map page is located at **Setup>Modbus>Mapping (Figure 4-8)**. On this page, Modbus Registers can be mapped to the measurement points. Please note that the registers in Table 4-3 are predefined.

To create a new entry, click the **New Entry** button. This will activate a row of text fields in the Modbus Register table. Begin by filling in the **Register Number**, then choose or type the Point Name. Be sure to click **Submit** to implement the changes.

Figure 4-8. Modbus Mapping

Table 4-3. Predefined Diagnostic Registers

Description	Register
Current Year (1)	49001
Current Month (1)	49002
Current Day (1)	49003
Current Hour (1)	49004
Current Minute (1)	49005
Current Second (1)	49006
Messages Received	49007
Corrupt Messages Received	49008
Messages Sent with Exception (error responses)	49009
Messages Sent Count	49010
Valid Messages Ignored (when in listen only mode)	49011

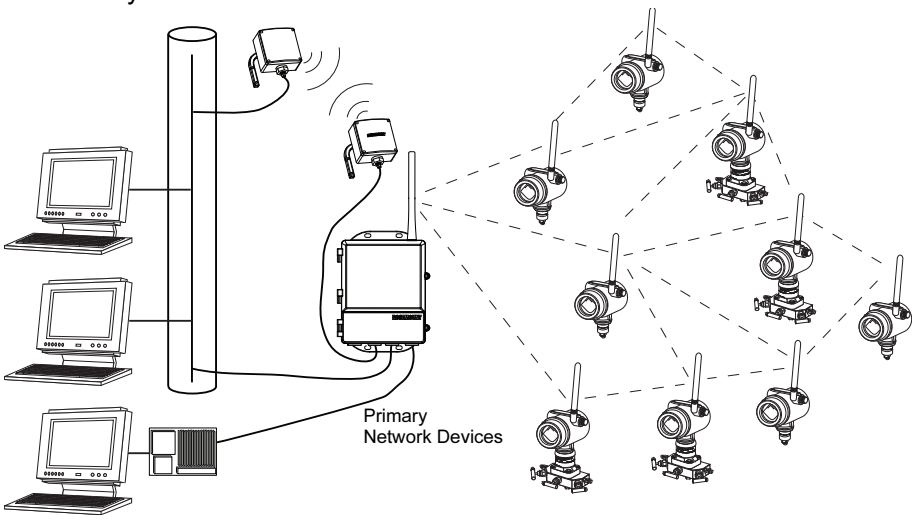
(1) Time is reported in GMT.

Section 5 Wireless Network Operation

OVERVIEW

This chapter will discuss ways to ensure good performance and security in the wireless network. Once the network is up and running, two simple steps will help ensure that the network is robust and reliable for the long term. These two steps are fortifying the network and identifying “pinch points.” Network expansion is also an easy process that not only broadens the reach of the network, but also increases robustness and reliability.

The second half of this chapter will lay out guidelines to increase and ensure the security of the network.



NETWORK FORTIFICATION

Verify Connections

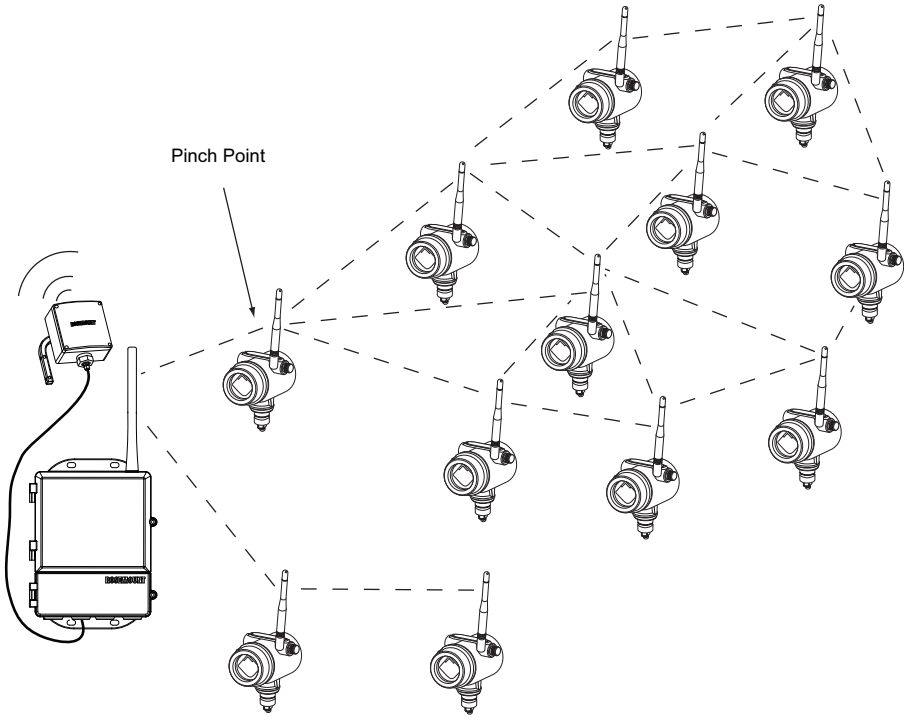
A fortified network allows the devices to communicate with the gateway in the most optimal configuration. First, verify that each device has joined the network and is communicating properly by checking the **Explorer>Status** page. If a communication link can’t be made, an additional device can be added to bridge the connection to the network.

A good connection should exhibit the following characteristics:

- Data Reliability > 99%
- Data Latency < 3 times update rate
- Battery Life > desired life span at fastest update rate
- Primary Network Connections
- Path Stabilities
- Radio Signal Strength Indication (RSSI) in the gateway diagnostics is good. This check is listed last because it can be misleading on its own (weak signals can still get through if the path is stable), but it can help identify a problem when it arises.

Identify Pinch Points

Next, identify “pinch points.” If messages from several devices must all pass through a single device at any point on their way to the gateway, the network becomes “pinched.” This pinch point then becomes a single point where failure can compromise the network’s long-term reliability.

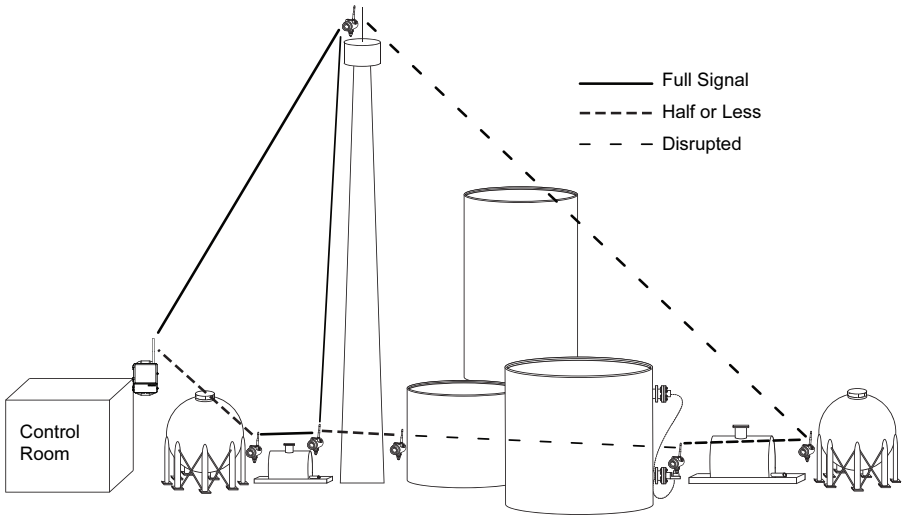


This doesn’t happen often because of the redundant communication paths in most self-organizing networks. The solution is simply to add additional devices near the pinch point to provide more communication paths. In general, for every ten devices, there should be a minimum of two connections to unique wireless devices.

HINT/TIP
Identification of pinch points should be performed 24 hours after all the devices have joined the network. This will allow the network to stabilize and optimize itself.

Impenetrables

A typical plant includes plenty of potential impenetrables, such as buildings, dense piping, concrete walls and long distances. The diagram below shows how impenetrables affect signal strength. There are three layers: floor, canopy, and emergent. Each layer has different potential impenetrables that can affect the network.



In this example, the floor layer - from ground to about 15-20 feet (5-6 m) - has very dense infrastructure that reduces signal range by 50% or more. This attenuation depends on the frequency of the radios, as well as the actual density of the environment.

Fortunately, the many potential measurement points in the floor layer mean there are likely to be many wireless devices. These devices provide many alternative communication paths around these impenetrables.

The canopy is the layer above the motors and pipe racks and below third floor stair decks. It's relatively open usually, but signals may be disrupted by tall structures.

The third layer is occupied by emergent structures such as distillation columns or exhaust towers that extend above the canopy. Emergent structures usually have minimal effect on radio signals unless they're part of a larger structure. Extensive testing has also shown that devices mounted in this layer can communicate with devices as far as approximately 160 feet (50 m) below in the canopy.

At any layer, increasing distance can also weaken signals. In general, if impenetrables disrupt direct transmission between wireless devices, simply add additional devices to provide alternate communication paths around the disruptions.

Expanding the Network

When it comes to self-organizing networks, bigger is better. In fact, the more wireless devices in the network, the easier it is to expand. That's because there are so many available paths for the additional communications to follow. The network simply senses that a device has joined the network, and routing algorithms in the devices and gateway automatically find the best route to the destination.

The existing network functions as a large antenna for any new device that is added to the periphery of the network, and a myriad of connections are available to devices added to the interior of the network. The only limitation is the amount of traffic that can be handled by each gateway and by the devices that provide the last “hop” to it. A high density of devices near the primary device level may cause pinch points.

This capability makes not only large-scale additions easy, but also allows the addition of single points to meet short-term needs. You can even install a temporary device to test whether a permanent installation would add value, or to do short-term monitoring for diagnostic purposes.

SECURITY FEATURES

The 1420 Wireless Gateway is shipped with the following usernames and passwords:

Table 5-1. Default Passwords

ID	PASSWORD
Executive (exec)	default
Operator (oper)	default
Maintenance (maint)	default
Administrator (admin)	default

Table 5-2. Access Table

Role	HTML Access	Explorer view Access
Executive (exec)	With the exception of factory settings (Setup/factory.html), can get any page (Read-Only access).	Read-only access.
Operator (oper)	No additional privileges	Same values as executive, but with read-write access.
Maintenance (maint)	• Can set device tags • Can configure Modbus communications • Can configure Modbus register map	All parameters (Read-Write).
Administrator (admin)	• Can configure network settings (address, default). • Can set passwords • Can set time settings • Can set home page options • Can restart applications	No additional privileges

These passwords should be changed periodically once the network is installed. Consult your local IT personnel or your network administrator for guidance when changing passwords.

WARNING
Use caution when changing the administrator password. If the administrator password is lost, you will not be able to operate the 1420 Wireless Gateway from the administrator role.

Network ID and Join Key

The Network ID and Join key work together to ensure that your network communicates only with itself. These two codes must be identical in the gateway and devices in order for them to communicate. The 1420 Wireless Gateway is capable of generating a random join key, or you may create your own custom Join Key using hexadecimal characters.

Encryption Key Rotation

Another security option in the 1420 Wireless Gateway is Encryption Key Rotation. To enable and configure Encryption Key Rotation, click **Setup>Mesh**.

TRENDS

Setting Up Trends

Setting up trends is a two part process. First the global Trend Settings need to be configured. This is done on the **Setup>Trends>Settings** page. On this page you will configure the Maximum series displayed, the Maximum initial samples, the Retained data duration (how long the gateway stores point data for trending), and the View port interval (how much time appears on the graph). When finished, click **Submit** to put the changes into effect.

New Trend

To begin collecting a trend, click **Setup>Trends>Collections**. Start by clicking the **New Trend** button. This will open a new page where the Name, Collection interval and Data retention period are entered. Next, click the **New Entry** button to select a Point Name. Select the point name from the list, then add a label if desired. This can help identify the measurement separate from just the HART Point Name. Repeat the above steps to add more measurement points to the trend. Click **Submit** to complete the trend setup.

Edit an Existing Trend

To edit an existing trend, click **Setup>Trends>Collections**. If there are any active trends, they will appear here. Click the Edit button to edit the trend settings, add or remove measurement points, or change a measurement point's Label. Click **Submit** when you are finished editing.

Delete a Trend

To delete a trend, click **Setup>Trends>Collections**. Click the **Delete** button next to the trend you wish to delete. A confirmation window will pop up. Click **OK** to delete the trend or cancel to return to the Trend Collections page. Click **Return to form** to return to the Trend Collections page.

Monitoring Trends

Trends may be monitored in one of two formats, an on-screen graph, or a generated report in Comma Separated Variable (CSV), Excel or XML format.

Graph

To view the graph of a trend, click **Monitor>Trend>Graph**. This will show the available trend graphs. Click the name of the trend you wish to view. The graph may be customized by zoom level, viewing mode, etc. These settings may be adjusted using the menus at the top of the graph page.

Report

To view a report of a trend, click **Monitor>Trend>Report**. Choose the trend to report, then select Local Time or Server Time, the Start and End times, and CSV, Excel, or XML format. To finish, click **Generate Report**.

Section 6 Troubleshooting

Select the Help menu in the top right of the web browser to view information on product installation, setup and configuration, diagnostics, and monitoring. In addition, field device, and specific 1420 Wireless Gateway facts are available.

To find the appropriate phone support contact, see the Rosemount Support web page at: **http://www.rosemount.com/support/support.html**

or email the tech specialists at:
Specialist-Wireless.EPM-RTC@EmersonProcess.com

Contact your local representative for additional service support, see Service Support on page 1-1.

Table 6-1. Connectivity To 1420

Cannot Connect Laptop/PC to 1420 Wireless Gateway Using Cross-Over Cable	
Verify cable connecting the Laptop/PC and the 1420 is an Ethernet Cross-Over Cable	Compare the order of the wires as seen through the clear plastic connectors on both ends of the cable. If the order on both ends is identical, the cable is a standard cable and not a Cross-Over cable. If the order is different on both ends, as seen in the colors of the wires, then the cable is a Cross-Over cable.
Verify the IP Address of the Laptop/PC is configured to communicate with the 1420	See Commissioning on page 2-1.
Verify Internet Explorer proxy settings are disabled	See Commissioning on page 2-1.
Verify that you are using the complete 1420 IP Address with secure https header when navigating with Internet Explorer	Complete IP Address: https://192.168.1.10 Incomplete IP Addresses: 192.168.1.10 -or- http://192.168.1.10
Verify that you are using the correct IP Address when connecting to the 1420	The 1420 administrator may have changed the IP Address as a security best practice. The primary, secondary and Power Over Ethernet ports have unique IP Addresses. Try the secondary port if the primary port IP Address is unknown. If the IP Addresses for both the primary and secondary ports are unknown, contact Rosemount Customer Central. Do not try connecting a laptop/PC to the Power Over Ethernet port because the powered connection could damage the laptop/PC.

Cannot Connect Laptop/PC to the 1420 Through Ethernet	
Verify the cables connecting the Ethernet to the Laptop/PC and 1420 are standard Ethernet cables	Compare the order of the wires as seen through the clear plastic connectors on both ends of the cable. If the order on both ends is identical, the cable is a standard Ethernet cable and not a Cross-Over cable. If the order is different on both ends, as seen in the colors of the wires, then the cable is a Cross-Over cable.
Verify the IP Address of the Laptop/PC is configured to communicate with the Ethernet	The Laptop/PC and 1420 will need unique IP Addresses. Contact the Ethernet network administrator for more information on connecting the Laptop/PC to the Ethernet. Also see Ethernet on page 4-1.

Cannot Connect Laptop/PC to the 1420 Through Ethernet	
Verify the Internet Explorer proxy settings are disabled	See Section 2: Initial Configuration
Verify that you are using the complete 1420 IP Address with secure https header when navigating with Internet Explorer	Complete IP Address: https://192.168.1.10 Incomplete IP Addresses: 192.168.1.10 -or- http://192.168.1.10
Verify that you are using the correct IP Address when connecting to the 1420	The 1420 administrator may have changed the IP Address as a security best practice. The primary, secondary and Power Over Ethernet ports have unique IP Addresses. Try the secondary port if the primary port IP Address is unknown. If the IP Addresses for both the primary and secondary ports are unknown, contact Rosemount Customer Central. Do not try connecting a laptop/PC to the Power Over Ethernet port because the powered connection could damage the laptop/PC.
Verify that the Ethernet connection between the Laptop/PC does not require a secure connection in order to make a connection through an Ethernet firewall	Contact the Ethernet network administrator to determine if a firewall exists. If it does, then install the Security Setup on the Laptop/PC. See Section XXX on creating a secure connection between the Laptop/PC and a 1420

Cannot Connect Laptop/PC to the 1420 Through a Secure Connection	
Verify Security Setup is installed on the Laptop/PC	See Section 4: Data Integration
Verify that the Security Setup on the Laptop/PC is configured to communicate on the correct firewall port	See Ethernet network administrator or firewall administrator to determine which firewall port to use. The default is 1164.
Verify that the 1420 is configured to communicate on the correct firewall port	See Section 4: Data Integration
Verify that the Security Setup service is active	Once the Security Setup is installed, the security setup service is activated to create the actual secure connection. See Section 4: Data Integration
Verify that you are using the correct secure IP Address when connecting to the 1420 through a secure connection	The Security Setup Application will give the 1420 a unique IP Address to ensure security. Open the Security Setup session to verify the 1420 secure address. Each laptop/PC with a secure connection to the 1420 will use a unique secure address to the 1420. See Section 4: Data Integration

Cannot Receive OPC Data Into Host System	
Verify that the Security Setup service is enabled between the 1420 and the OPC Server PC	For security reasons, all OPC and MOdbus TCP data is only transferred using a secure connection. See Section 4: Data Integration
Verify that the 1420 OPC Server software is installed and activated on the OPC Server PC	See Ethernet on page 4-1.
Verify that the 1420 OPC Server software is using the correct 1420 secure IP Address	The 1420 has to use the 1420 secure IP Address created by a Secure Setup session. See Section 4: Data Integration
Verify that the OPC tags have been entered on the 1420 to enable OPC output of the 1420	See OPC on page 4-6.
Verify that the OPC data is transmitted to the OPC Server PC	Verify the data transmission using Matrikon's OPC Explorer software. This is free software for troubleshooting OPC connections. By verifying that the OPC data is coming to the OPC Server PC, the problem can be isolated to the Application OPC Client that brings the data into the OPC Application.
Verify the most recent Application OPC Client is installed on the same PC as the OPC Server PC	The easiest installation has both the OPC Server and Client software on the same machine. Make sure to use the latest revision of OPC Client software. Check with the Application developer to ensure the latest revision of the client.
Verify the OPC Client is directed to the correct OPC Server	The 1420 OPC Server software is capable of receiving data from several 1420s at the same time. The OPC Client has to be pointed to the correct 1420 through the 1420 OPC Server. See Ethernet on page 4-1.

Cannot Receive Modbus TCP Data into Host System	
Verify that the Security Setup service is enabled between the 1420 and the Modbus TCP Server	For security reasons, all OPC and Modbus TCP data is only transferred using a secure connection. See Section 4: Data Integration
Verify the Modbus TCP Data Type is correctly configured on the 1420 to match the Modbus TCP Host System	The 1420 must be configured to either Floating Values (with digits of precision), or to Rounded (integer) digits of precision. Consult the Host System administrator and specifications for verification of data type. See Ethernet on page 4-1.
Verify Modbus TCP tags have been entered on the 1420 to enable the Modbus TCP output of the 1420	See Modbus Register Map on page 4-10.
Verify Modbus registers on the Host Serial System	The Modbus registers on the 1420 and the Host Serial System must be identical in order to correctly transfer data. If the registers are mismatched, then data will not be transmitted or the wrong data will be transmitted.
Verify wireless devices are active	If wireless devices are not active, then error values will be transmitted through the Modbus registers.

Cannot Receive Serial Modbus RS232/RS485 data into Host System	
Verify the 1420 has correct serial settings that match the settings of the Host System	The 1420 needs to have the exact same settings for serial communication as the Serial Host System. Any deviation will cause communications to fail. See serial system administrator and Host System specifications for correct settings and Ethernet on page 4-1.
Verify the 1420 has the correct Serial Slave Address	The 1420 will need to be assigned a Slave Address that is unique from all other serial devices on the serial input. See serial administrator and Host System specifications for correct settings and Ethernet on page 4-1.
Verify the Host System is communicating with the correct Slave Address assigned to the 1420 on the correct serial input card	The Serial Host System will need to be configured to communicate with the 1420 on its assigned Slave Address and assigned to a serial input card. See serial system administrator and Host System specifications for correct settings and Ethernet on page 4-1.
Verify the correct Serial Modbus Type, either RS232 or RS485, is being used.	The 1420 default Modbus output is RS485. If the Host System requires RS232, then an adaptor from RS485 to RS232 will need to be installed in series between the 1420 and the serial input point. Or, in some cases, the serial input card can be configured to receive either RS232 or RS485. See Ethernet on page 4-1.
Verify all electrical terminations between the 1420 and the Serial Host	Any frayed or damaged connection between the 1420 terminal block and the serial host system can cause intermittent data transmission and errors.
Verify Modbus registers exist on the 1420	See Modbus Register Map on page 4-5.
Verify Modbus registers have been entered on the Serial Host System	The Modbus registers on the 1420 and the Serial Host System must be identical in order to correctly transfer data. If the registers are mismatched, then data will not be transmitted, or the wrong data will be transmitted.
Verify wireless devices are active	If wireless devices are not active, then error values will be transmitted through the Modbus registers.

Glossary

The following terms and definitions are intended to define how the terms are used in this document. They may vary slightly from their common usage outside this document.

Term	Definition
Broadcast	The address that a station can send to that will be received by all devices on the network.
Canopy Level	The level of the process unit between the Floor Level and the Emergent Level (from approximately 20 ft. (6 m))
Connectivity	Typically refers to a combination of path statistics and link reliability. May also refer to the operability of the connection between the Gateway and the Information System.
Data Latency	The time from when a message leaves a device until it reaches the gateway. It should be less than 1/3 the update rate. For example, with a 60 second update rate, the data latency should be less than 20 seconds.
Device(s)	Refers to a wireless pressure or temperature transmitter(s).
DHCP	Dynamic Host Configuration Protocol: Used to configure the network parameters automatically. This device contains a DHCP Client to retrieve the network configuration parameters from a DHCP server on the network.
Domain Name	A unique designator on the internet composed of symbols separated by dots such as: this.domain.com
Emergent Level	The level of a process unit above the Canopy Level (up to 160 ft. (50 m))
Floor Level	The level of a process unit from 0-20 ft. (0-6 m)
Gateway	The address of the node on the network that serves as an entrance to other networks.
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)
Information System	This term will be used to describe any information system (computer network), Host System, or Control System. Typical systems include Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), data historians and asset management systems.
IP (TCP/IP)	Internet Protocol: The protocol that specifies how data is transmitted over the internet.
Item(s)	Parameter in OPC protocol that contains a value. Similar to a Register in Modbus protocol.
Join Key	Hexadecimal code that links devices to the gateway. This code must be identical in the device and 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	The portion of the network that the device resides on.
Network I.D.	Numeric code that links devices to the gateway. This code must be identical in the device and the gateway.

Term	Definition
NTP/SNTP	Network or Simple Network Time Protocol: Used to set the system time. This device contains an NTP client for keeping the system time synchronized with a network time server.
Populate	The process of a device joining the network and sending data to the gateway.
Power Over Ethernet (POE)	A receptacle designed to provide power through the Ethernet cable. WARNING: Non-standard POE configuration.
Primary Device	A device in the closest layer, connected directly to the gateway (“one hop”)
Private Network/LAN	A local connection between a 1420 Wireless Gateway and a PC/Laptop. This network is used for commissioning and configuration of the gateway.
Register(s)	Modbus term
Self Organizing Network	The network topology utilized in the Rosemount Wireless Gateway and devices.
Tag(s)	A piece of HART data that resides in the device and functions as the “name” of a device.
TCP	Transmission Control Protocol, a core protocol of the internet protocol suite (TCP/IP)

Appendix A Reference Data

SPECIFICATIONS

Functional Specifications

Power Input Options
24 V dc
500 milliamps required to power the 1420 Wireless Gateway.

Environmental
Operating Temperature Range:
-40 to 60°C (-40 to 158°F)
Operating Humidity Range:
0-95% relative humidity (non-condensing)

Physical Specifications

Weight
10.7 lb (4.85 kg)

Material of Construction

Housing
Low-copper aluminum, NEMA 4X and IP65 IEC 529

Pollution Degree 2

Paint
Polyurethane

Cover Gasket
Rubber

Communication Specifications

RS485

2-wire communication link for Modbus multidrop connections

Baud rate: 57600, 38400, 19200, or 9600

Protocol: Modbus RTU

Wiring: Single twisted shielded pair, 18 AWG. Wiring distance is approximately 5,000 ft. (1,524 m)

Ethernet

Webserver and Modbus TCPIP

OPC with Webserver and Modbus TCPIP

HSE for AMS with Webserver and Modbus TCPIP

HSE for AMS with OPC, Webserver and Modbus TCPIP

Modbus

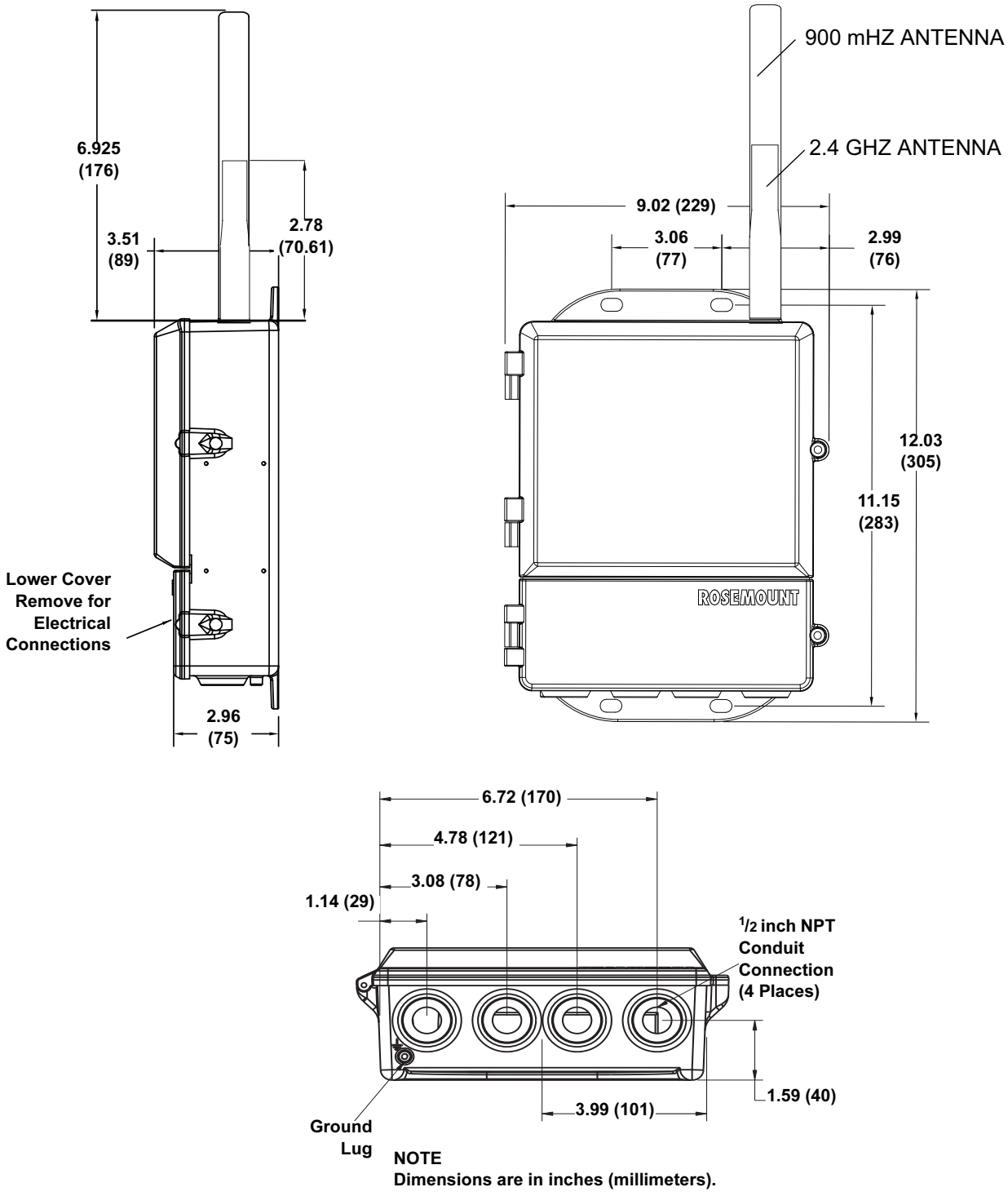
- Supports Modbus RTU and TCP/IP with 32 bit floating point values, integers, and scaled integers.
- Modbus registers are assigned to measurement inputs by the TAG of the analog input block.
- Modbus register numbers are specified by the user.
- The status of each variable is available in a 16 bit register.
- The configuration of the Modbus interface is accomplished using web pages generated by the 1420 Wireless Gateway.

NOTE

It is recommended that external power conditioners be used in any critical applications. This will allow the 1420 to be removed for maintenance and allow the fieldbus segments to continue functioning should the 1420 be unavailable.

DIMENSIONAL DRAWINGS

Figure A-1. 1420 Wireless Gateway



NOTE
Dimensions are in inches (millimeters).

ORDERING INFORMATION

Model	Product Description
1420	Wireless Gateway
Code	**Power Input**
A	24 VDC
Code	**Output**
1	RS485 + Ethernet
2	RS485 + Redundant Ethernet
3	RS485 + Fiber Optic Ethernet
Code	**Operating Frequency and Protocol**
A1	HART, Self Organizing Network - 2.4 GHz DSSS
A2	HART, Self Organizing Network - 900 MHz FHSS
Code	**RS-485 Communication**
N	No RS-485 Communication
A	Modbus RTU
Code	**Ethernet Communication**
0	Webserver and Modbus TCP/IP
1	OPC with Webserver and Modbus TCP/IP
2	AMS Ready Connectivity with Webserver and Modbus TCP/IP
4	AMS Ready Connectivity with OPC, Webserver and Modbus TCP/IP
Code	**Other Options**
	Software Configuration
C1	Custom Software Configuration
	Product Certifications
N5	FM Division 2, Dust Ignition-Proof
N6	CSA Division 2, Dust Ignition-Proof
N1	ATEX Type n
N7	IECEx Type n
NF	IECEx Dust Ignition-proof
ND	ATEX dust Ignition-proof
	Adapters
J1	CM 20 Conduit Adapter
J2	PG 13.5 Conduit Adapter
Typical Model Number: 1420 A 1 A2 1 N5	

1420 Wireless Gateway Configuration Data Sheet

Sales Order No. _____	Unit No. _____	Line No. _____
For Factory Use Only		

Configuration Information

Customer: _____ P.O. No.:_____

Model No.: _____ Line Item: _____

Self Organizing Network Parameters

☐	Generated Network Parameters				
☐	Customer Network Parameters				
	Network ID(1)				
	Join Key[1]				
	Update Rate				
	Update Rate should be between 0:10 seconds and 60:00 minutes				

(1) Valid Characters: 0-9, A-F

Network Size

☐ 50 devices or fewer ☐ 51 to 100 devices

Appendix B Approval Information

APPROVED MANUFACTURING LOCATIONS

Rosemount Inc. – Chanhassen, Minnesota, USA

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. To see which countries our devices have received certification for use in, see www.rosemount.com/smartwireless.

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.

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. 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)

EN 61326-1: 1997 with amendments A1, A2, and A3—Industrial

Radio and Telecommunications Terminal Equipment Directive (R&TTE) (1999/S/EC)

Emerson Process Management complies with the R&TTE Directive.

FM Ordinary Locations Approval

The 1420 Wireless Gateway has been evaluated and approved by FM for ordinary locations.

CE EMC Marking

Compliance with European Union EMC

HAZARDOUS LOCATION CERTIFICATIONS

North American Certifications

N5 FM Division 2
Certificate Number: See Certificate
Nonincendive for Class I, Division 2, Groups A,B,C, and D;
Dust Ignitionproof for Class II,III, Division 1,
Groups E,F, and G; Indoor/outdoor locations;
NEMA Type 4X
Temperature Code: T4 (-40°C < T_a < 60°C)

Canadian Standards Association (CSA)

N6 CSA Division 2 & Dust Ignitionproof
Certificate Number: See Certificate
Suitable for Class I, Division 2, Groups A,B,C,D;
Dust Ignitionproof for Class II, Groups E,F, and G;
Suitable for Class III Hazardous Locations.
Install per Rosemount drawing 01420-1011.
Temperature Code: T4 (-40°C < T_a < 60°C)
CSA Enclosure Type 4X

EUROPEAN CERTIFICATION

N1 CENELEC Type n (ATEX)
See note below
Certificate Number: See Certificate
ATEX Marking: Ex II 3 G
EEx nA nL IIC T4 (-40°C < T_a < 60°C)

ND ATEX Dust Ignition-proof Approval
Certificate Number: See Certificate
EX tD A22 IP66 TI35 (-40°C < T_a < 60°C)
EE nA Nl IIC T4 (-40°C < T_a < 60°C) Ex I 3D

IECEx Certification

N7 IECEx Type n
See note below
Certificate Number: See Certificate
Ex nC IIC T4 (-40°C < T_a <= +60°C)
Rated Voltage: 28V

NF IECEx Dust Ignition-proof Approval
Certificate Number: See Certificate
EX tD A22 IP66 TI35 (-40°C < T_a < 60°C)
Vmax = 28V

Conditions of Installing N1 and N7

The apparatus is not capable of withstanding the 500V insulation test required by Clause 9.4 of EN 60079-15: Soo5. This must be taken into account when installing the apparatus.

CE ⓘ

Table 1.

Country	Restriction
Bulgaria	General authorization required for outdoor use and public service
France	Outdoor use limited to 10mW e.i.r.p.
Italy	If used outside of own premises, general authorization is required.
Norway	May be restricted in the geographical area within a radius of 20 km from the center of Ny-Alesund.
Romania	Use on a secondary basis. Individual license required.

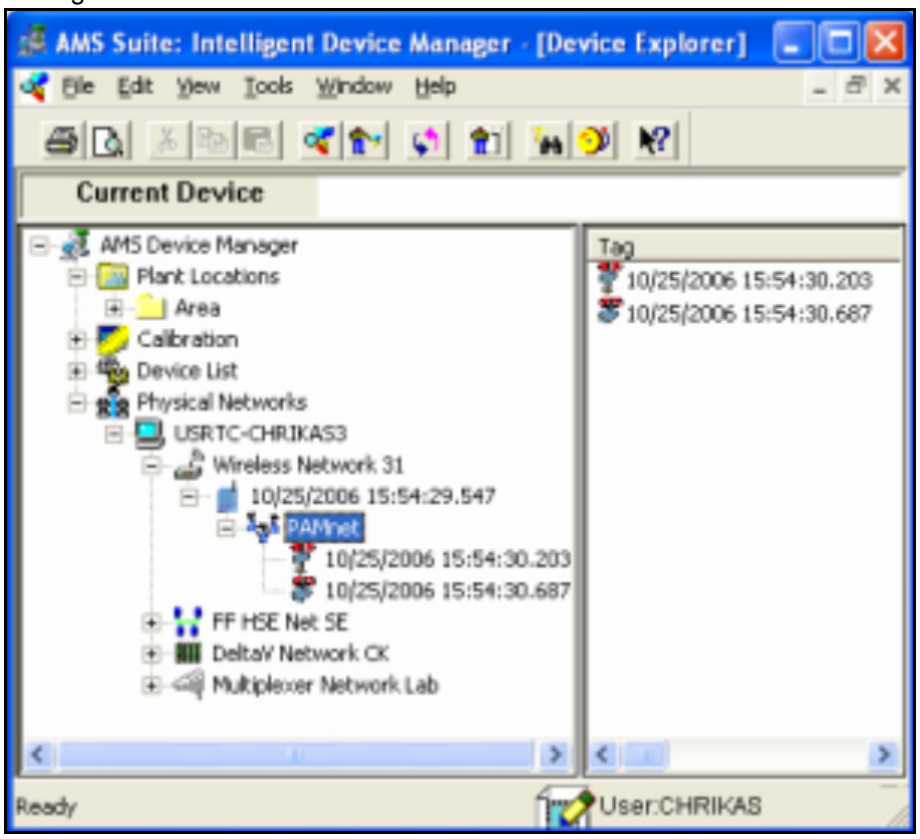
Radio Power Label - see Figure 3 - indicates output power configuration of the radio. Devices with this label are configured for output power less than 10 mW e.i.r.p. At time of purchase the customer must specify ultimate country of installation and operation.

Appendix C Using AMS™ Suite: Intelligent Device Manager with the 1420 Wireless Gateway

BENEFITS

AMS Suite provides a comprehensive and integrated family of predictive and proactive maintenance applications including a common interface to device diagnostics. AMS Suite: Intelligent Device Manager provides support for more than 141 FOUNDATION™ fieldbus devices from 33 manufacturers, and 267 HART® devices from 39 manufacturers. Its comprehensive set of analysis and reporting tools presents a single application for predictive diagnostics, documentation, calibration management, and device configuration.

When used in conjunction with the 1420 Wireless Gateway, Intelligent Device Manager provides a powerful tool for complete management of a plant's valuable instrument assets. Besides providing a user-friendly interface for configuring, diagnosing, and calibrating a plant's wireless HART devices, Intelligent Device Manager provides a complete historical Audit Trail of all events associated with these activities. The Alert Monitor within AMS Device Manager quickly alerts the user of diagnostic conditions associated with the wireless HART devices. Calibration management of these devices is easily handled by the Calibration Assistant SNAP-ON™ available with AMS Device Manager.



1420 Wireless Gateway displayed in AMS Device Manager

CONNECTING THE 1420 WIRELESS GATEWAY TO AMS DEVICE MANAGER

The 1420 Wireless Gateway is connected to the AMS Device Manager PC through an Ethernet card. AMS Device Manager supports up to 16 1420's in one wireless network.

Establishing a connection between Intelligent Device Manager and a 1420 is easy. The following steps are required:

1. Stop AMS Device Manager if it is running.
2. **Select Start>Programs>AMS Device Manager>Network Configuration** from the Windows task bar.
3. Click **Add**.
4. Select **Wireless Network** from the list of networks in the **Select Network Component Type** dialog box.
5. Click **Install**.
6. Enter a name for the wireless network. This will be the name that will appear at the top of the wireless network hierarchy in AMS Device Manager.
7. Click **NEXT**.
8. Enter the name or IP address of a gateway and click **Add**.
9. If prompted, enter the username and password you use to log in to the 1420 Setup Utility. Click **OK**.
10. If prompted, enter information to allow secure (SSL) communications between the 1420 and AMS Device Manager. Click **OK**.
11. Click **FINISH**.
12. Click **Close**.

When AMS Device Manager is restarted, the wireless network will show up in both Device Explorer and Device Connection View. Right click the wireless network icon and select Rebuild and Identify Hierarchy. Next, right click the wireless network icon and select Scan | New Devices. Unlike wired devices, AMS Device Manager scans wireless devices concurrently to offset some of the expected latencies in a wireless network. When the scan is complete, you can expand the interface by clicking the plus sign next to each icon and navigating down the hierarchy.

USING THE WIRELESS INTERFACE IN AMS DEVICE MANAGER

A wireless network is represented by its icon, which is at the top of the network hierarchy in Device Connection View or Device Explorer. The second level of the hierarchy displays the wireless gateways. A gateway is a HART device; its icon is provided by the manufacturer. Below the gateway icons are mesh network icons. A mesh network is a collection of wireless devices that work together to pass messages between each other and a wireless gateway.

Below the mesh network icons are icons for wireless HART devices (WHDs).

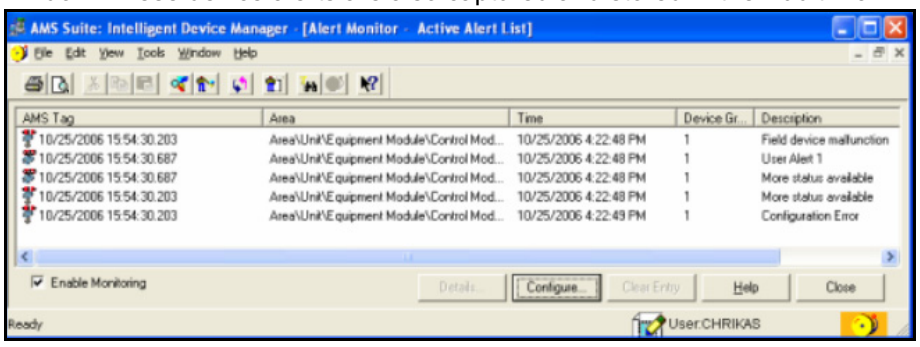
The icons within the wireless network have context menus from which you can perform various AMS Device Manager and device functions. See the AMS Device Manager Books Online for detailed information.

The 1420 Web Browser is easily launched in Device Connection View or Device Explorer View by right clicking on the 1420 icon and selecting "Launch Setup" from the context menu. When the Web Browser is launched, enter the User Name and Password.

USING AMS DEVICE MANAGER'S ALERT MONITOR WITH THE 1420

The Alert Monitor in AMS Device Manager provides a powerful means to monitor device alerts reported from the wireless HART devices. When an alert is reported from a wireless device added to the Device Monitor List, the bell icon in the AMS Device Manager status bar is lit and the alert shows up in the Alert Monitor window. By right clicking a specific alert, a status screen is displayed identifying the specific alert conditions. By clicking on the alert and then clicking Details, additional information about the specific alert can be obtained. See the AMS Device Manager Books Online for details about using Alert Monitor.

When the alert condition is corrected, it disappears from the Alert Monitor window. These device alerts are also captured and stored in the Audit Trail.



AMS Alert Monitor displays alerts as they happen

In order for device alerts to be reported to the Alert Monitor from the 1420, some setup is required. The following steps must be performed for a device to have its alerts show up in Alert Monitor:

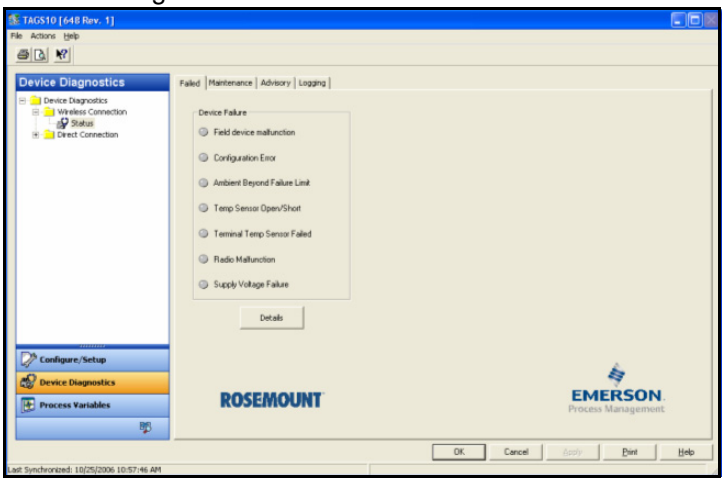
1. Add the device to the AMS Device Manager Plant Database by "dragging" the device shown under the 1420 to an Equipment Module folder in the Plant Database.
2. Add the device to the Device Monitor List by doing the following:

   a. Click CONFIGURE on the Alert Monitor window.

   b. Click ADD on the Device Monitor List window.

   c. Select the device(s) to be added and click OK.

   d. Click OK again.



Detailed status information can be called up from AMS Alert Monitor

Appendix D Modbus Configuration in Honeywell® TDC APM/HPM

Refer to the Honeywell Manual OP01-501 APM/HPM Serial Interface Options for information on Modbus Configuration.

The 1420 Wireless Gateway can address registers up to 65535. TDC requires that you use specific register ranges to read floating point numbers. The Honeywell manual contains the following information:

> *"Floating point format data for the address range 20001 to 29999 is returned in standard IEEE floating point format except that the low and high words are swapped. This format is appropriate for the Modicon 984 Programmable Logic Controller (PLC)."*

This requires setting the swapped floating point option in the 1420 Wireless Gateway on the Modbus Setup Page.

Appendix E Integer Scaling

INTEGER SCALING

If you read process variables from integer registers, the 1420 ordinarily returns a rounded integer, such as 2712 to represent 2711.97 grams per minute, or 1 to indicate a density of 1.2534 grams per cubic centimeter.

Integer scaling causes the 1420 to return integers, accurate to one part in 65536, representing the measured value of the process variable, such as 50000 to represent a mass flow rate of 50 grams per second. Scaled integers amplify and linearize small changes in critical process variables.

You can implement integer scaling for the following purposes:

- To offset negative values such as subzero temperatures or reverse flow rates, so they can be read as positive integers.
- To increase output resolution of values such as density, temperature, pressure, or low flow rates.

NOTE
Integer scaling is typically used in legacy systems. Floating point representation is usually used when the Information System supports it.

CONFIGURING SCALED INTEGERS

If you configure integer scaling for more than one process variable, the same maximum integer applies to all scaled process variables. Each scaled process variable can have its own offset and scale factor.

To determine a scaled integer proportional to the measured value of a process variable, the 1420 uses a variation of the linear equation. The equation represents a linear correction of the measured value:

$$y = Ax - (B - 32768)$$

Where:

y = Scaled integer returned by the1420

A = Gain for scaled integer values

x = Measured value of the process variable

B = Offset for scaled integer values

To configure integer scaling of process variables, follow these steps:

1. Select a maximum integer and write its value in the appropriate field on the **Setup>Modbus>Communications** page. If you are using global scale factors and offsets enter these on the same page. Otherwise:
2. Derive a gain for each desired process variable and write the values to the appropriate I/O point.
3. Derive an offset for each desired process variable and write the values to the appropriate I/O point.

Step 1: Determine Maximum Integer

A scaled integer is the value of y in the equation presented above. The maximum integer is the highest integer proportional to a measured value of a process variable. The default maximum integer is 65534.

KEY TO USING MAXIMUM INTEGERS
If integer scaling applies to more than one process variable, all scales must share the same maximum integer, but may have different offsets and scale factors.

You can program a maximum integer below the default maximum integer. The maximum integer selected may be determined by the Modbus host's capabilities. For example, the Honeywell control system allows transmission of integer values from 0 to 9999 or from 0 to 4096.

The overflow integer is defined as the maximum integer plus 1. Therefore, if the maximum integer is 1000, the overflow integer is 1001. If the default maximum integer is used (65534), the default overflow integer is 65535.

The 1420 returns the overflow integer if the measured value of a process variable derives an integer higher than the maximum integer. The transmitter also returns the overflow integer if any of the following alarm conditions exists:

- Sensor failure
- Input overrange
- Density outside sensor limits
- Temperature outside sensor limits
- Transmitter electronics failure

Step 2: Determine the Gain (Slope)

The scale factor is the value of A in the equation above. The scale factor equals the linear slope of the integers, which are proportional to measured values of the process variable. The scale factor therefore is a ratio that compares the change in the measured value to the proportional change in value of the scaled integers.

Step 3: Determine Offset

The offset for scaled integers is the value of B in the equation above. The intercept, or the offset minus 32768, equals the value of the process variable that is represented by a scaled integer value of 0. The offset enables scaled integers, which always have positive values, to represent negative values such as a subzero temperature or a reverse flow rate.

Since B (the offset) always has a value from 0 to 65534, the1420 uses the following equation to derive a positive or negative intercept:

Intercept = Offset - 32768

- The maximum negative intercept is -32768, where the offset = 0.
- The intercept is 0, where the offset = 32768
- The maximum positive intercept is 32767, where the offset = 65535

So, although you write the offset as an integer from 0 to 65535, the process variable can have a value less than, equal to, or greater than 0.

USING INTEGER SCALING TO DEFINE RANGE LIMITS

The maximum integer, offsets, and scale factors establish programmable limits on process variables. Establish an integer scale for programmable limits on process variables according to either of the two methods described below.

Method 1

Follow these steps while referring to Example 1 and Example 2.

1. Use the following equations to set up scaled integer limits corresponding to lower and upper range values of the process variable.

$$\text{Offset} = (\text{Gain} \times x_1) \quad y_2 + 32768$$

$$\text{Gain} = \frac{y_2 - y_1}{x_2 - x_1}$$

Where:

x_1 = Lower range value

x_2 = Upper range value

y_1 = Maximum integer

y_2 = An integer (usually 0) with lower than the maximum integer

2. Write the integer value of y (the maximum integer) to the appropriate configuration entry field.
3. Write the integer value of A (the gain) to the appropriate configuration entry field.
4. Write the integer value of B (the offset) to the appropriate configuration entry field.

Example 1 The 1420 FIM is connected to a Honeywell TDC3000 control system using a PLC Gateway. The control system engineer sets up an analog input point to bring in volume flow, which enables use of flow limit alarms in the control system. On the control system, an analog input point has limits of 0 to 4095, with any input greater than 4095 indicating a “bad” process variable. The lower range limit is -100 barrels/day. The upper range limit is 300 barrels/day.

1. Set up the maximum integer, if necessary.
2. Set up scaled integer limits corresponding to the lower and upper range values.
3. Determine the gain:

$$= \frac{y_2 - y_1}{x_2 - x_1}$$

$$\frac{4095 \quad 0}{300 \quad (\ 100)}$$

$$\frac{4095}{400}$$

$$10.2375$$

4. Determine the offset:

$$(\text{Gain} \times x_1) \quad y_1 \quad 32768$$

$$[10 \times (\ 100)] \quad 0 \quad 32768$$

$$1000 \quad 32768$$

$$31768$$

5. The calculated scale factor of 10.2375 was rounded down to 10, so the actual transmitter range will slightly exceed the desired range of -100 to 300. To allow proper scaling of the analog input point data by the Honeywell control system, calculate the actual transmitter range corresponding to scaled integer values of 0 and 4095:

   Lower range value

$$x_1 \quad 100$$

   Upper range value

$$\frac{y_2 \quad y_1}{\text{Gain}} \quad x_1$$

$$\frac{4095 \quad 0}{10} \quad 100$$

$$309.5$$

Example 2 Scale the mass flow rate so 0 represents -100 pounds/minute (lb/min) and 30,000 represents 200 lb/min.

Scale factor:

$$\frac{y_2 \quad y_1}{x_2 \quad x_1}$$

$$\frac{30000 \quad 0}{200 \quad (\ 100)}$$

$$\frac{30000}{300}$$

$$100$$

Offset:

$$(Gain \times x_1) \quad y_2 \quad 32768$$

$$[100 \quad (\ 100)] \quad 0 \quad 32768$$

$$22768$$

Method 2

Choose a maximum integer equal to or less than 65534, then using the linear equation presented to solve for A (the scale factor) and B (the offset), as shown in Example 3.

1. Write the integer value of y (the maximum integer) to the appropriate I/O point
2. Write the integer value of A (the scale factor) to the appropriate I/O point
3. Write the integer value of B (the offset) to the appropriate I/O point

Example 3 The mass flow rate needs to remain between 30 and 40 grams per minute (g/min). Scale the mass flow rate so 0 represents a flow rate of 40.000 g/min, and 10,001 represents a flow rate greater than 40.000 g/min.

$$10000 \quad A(40) \quad (B \quad 32768)$$

$$0 \quad A(30) \quad (B \quad 32768)$$

Solve for A:

$$10000 \quad A(10)$$

$$A \quad \frac{10000}{10}$$

$$A \quad 1000$$

Solve for B:

$$10000 \quad 1000(40) \quad (B \quad 32768)$$

$$10000 \quad 40000 \quad (B \quad 32768)$$

$$10000 \quad 40000 \quad 32768 \quad B$$

$$B \quad 62768$$

- The maximum integer is 10,000. If the mass flow rate exceeds 40.000 g/min, the transmitter returns the integer 10,001.
- The scale factor is 1000. A change of 1 in the value of the integers represents a change of 0.001 g/min in the mass flow rate.
- The offset is 62,768. If the mass flow rate drops to 30.000 g/min, the transmitter returns a 0.

NOTES:

Reference Manual
00809-0100-4420, Rev BA
August 2007

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

Emerson Process Management
Shared Services LTD.
Heath Place
Bognor Regis
West Sussex PO22 9SH
England
T 44 (1243) 863 121
F 44 (1243) 867 554

Emerson Process Management
Asia Pacific Private Limited
1 Pandan Crescent
Singapore 128461
T (65) 6777 8211
F (65) 6777 0947/65 6777 0743
Enquiries@AP.Emersonprocess.com

EMERSON™
Process Management