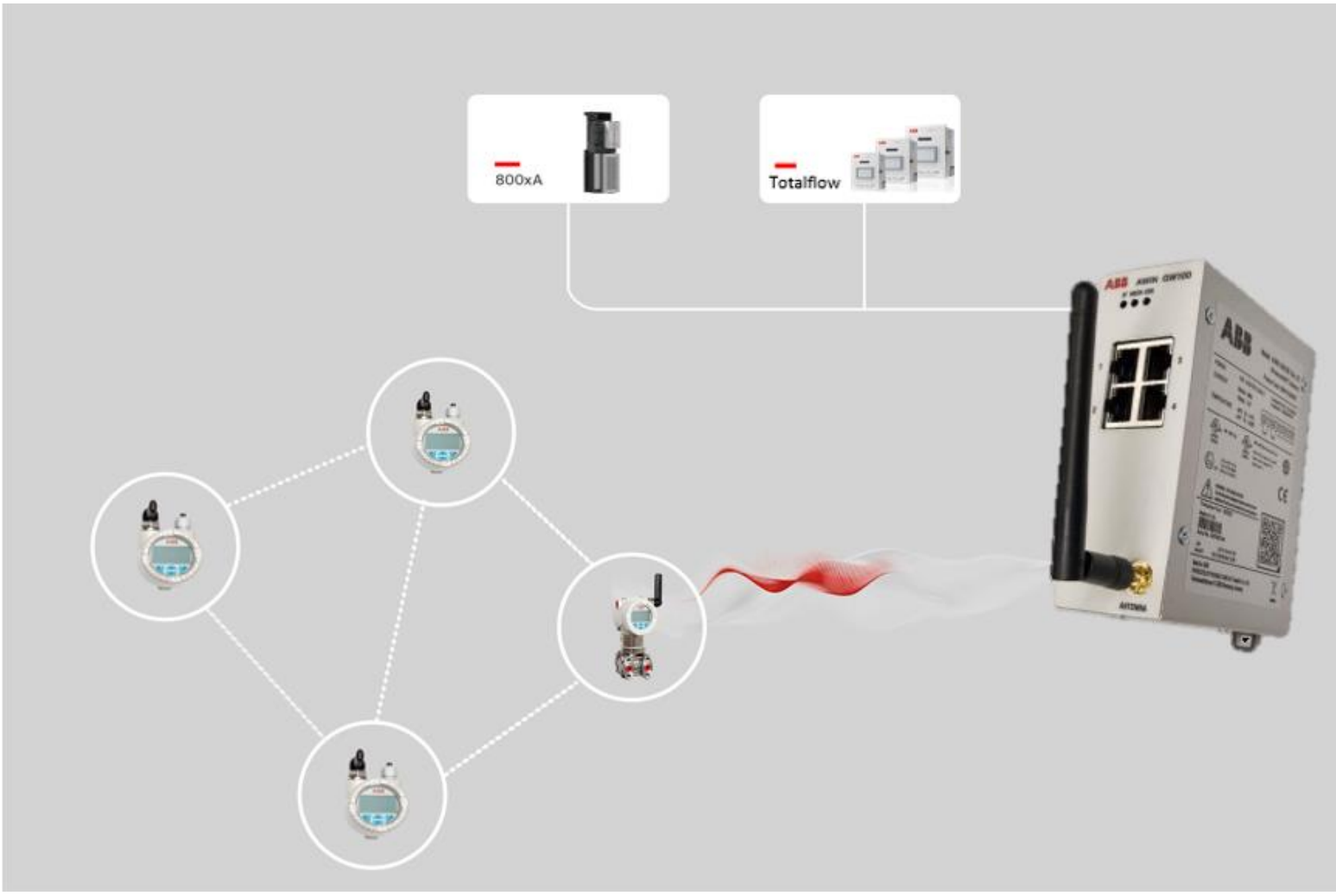
ENERGY INDUSTRIES

AWIN GW100 rev.2
ABB Wireless Industrial Network - User Manual



ENERGY INDUSTRIES

AWIN GW100 rev.2 ABB Wireless Industrial Network - User Manual

NOTICE

This document contains information about one or more ABB products and may include a description of or a reference to one or more standards that may be generally relevant to the ABB products. The presence of any such description of a standard or reference to a standard is not a representation that all of the ABB products referenced in this document support all of the features of the described or referenced standard. In order to determine the specific features supported by a particular ABB product, the reader should consult the product specifications for the particular ABB product.

ABB may have one or more patents or pending patent applications protecting the intellectual property in the ABB products described in this document.

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

This product is designed to be connected to and to communicate information and data via a network interface. It is the User's sole responsibility to provide and continuously ensure a secure connection between the product and the User's network or any other network (as the case may be). The User is expected to establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc.) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB is not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

TRADEMARKS

Ability is a trademark of ABB.

Release: November 2023

Document Number: 3BNP102992

Document Revision: A

Table of Contents

List of Figures

List of Tables

1 About This User Manual

1.1 Purpose and Scope

This manual is intended to provide the users an overview of practical aspects related to WirelessHART technology. It provides detailed description of factors to consider when designing WirelessHART networks, along with features offered by the AWIN GW100 rev.2 gateway to assist in evaluating network design. Moreover, this user manual provides information on the functionalities offered by the gateway through its web interface which can be used to configure a WirelessHART network. Towards the end, some tips are provided to assist in network and device troubleshooting.

Note. For detailed description of the new functionalities, the fixed problems, and the known problems in a firmware release of AWIN GW100 rev.2, refer to Release Note (3BNP102992).

1.2 Document Conventions

Microsoft Windows conventions are normally used for the standard presentation of material when entering text, key sequences, prompts, messages, menu items, screen elements, and so on.

1.3 Terminology

Table 1 lists terms used in this document and associated with the ABB Wireless Industrial Network. The reader should be familiar with these terms before proceeding further in this User Manual.

Table 1: Terminology

Term	Description
AWIN GW100 rev.2	WirelessHART Gateway (Second generation)
Epoch time	The number of seconds that have elapsed since January 1, 1970
LED	Light Emitting Diode
MAC	Unique address that a manufacturer assigns to each network device
Mesh Network	Mesh networking is a type of network topology in which a device transmits its own data as well as serves as a relay for other nodes
ModbusTCP	Communication protocol
Passphrase	Used much like a password
RTU	Remote Terminal Unit

Term	Description
Static IP Address	A fixed Internet Protocol (IP) address assigned to a computer or device
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WirelessHART	It is IEC 62591 specified wireless communication protocol designed for HART protocol
XML	Extensible Markup Language

1.4 Related Documentation

Table 2 lists the documents relevant to AWIN GW100 rev.2 WirelessHART Gateway.

Table 2: Related Documentation

Document ID	Title
3BNP102987	AWIN GW100 rev.2 Product Datasheet
3BNP102992	AWIN GW100 rev.2 Release Note
3BNP102988D2	Quick Setup Guide
3BNP103003D3	AWIN GW100 rev.2 - Specific Conditions of Use

1.5 Related Tools

Table 3 lists the tool relevant to AWIN GW100 rev.2 WirelessHART Gateway.

Table 3: Supported Tools

Document ID	Title
3BNP102928	AWIN WirelessHART Gateways Configurator

1.6 Warning, Caution, Information, and Tip Icons

This document includes **Warning**, **Caution**, and **Information** if/where appropriate to point out safety related or other important information. It also includes **Tip** to point out useful hints to the reader. The corresponding symbols should be interpreted as follows:

Electrical warning icon indicates the presence of a hazard, which could result in *electrical shock*.

Warning icon indicates the presence of a hazard, which could result in *personal injury*.

Caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard, which could result in *corruption of software or damage to equipment/property*.

Information icon alerts the reader to pertinent facts and conditions.

Tip icon indicates advice on, for example, how to design your project or how to use a certain function.

Although **Warning** hazards are related to personal injury, and **Caution** hazards are associated with equipment or property damage, it should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, comply fully with all **Warning** and **Caution** notices.

1.7 Target Audience

This user manual is primarily intended for all users.

This user manual does not contain last-minute product information and updates which might affect functionality and/or performance. For information on last revisions, late changes and restrictions, the user shall refer to the relevant release note.

1.8 Compatibility

To check compatibility of the revisions of the AWIN GW100 rev.2 gateway, refer to the relevant section of Release Note.

2 Technology Overview

2.1 WirelessHART Network

A WirelessHART network consists of a host; a WirelessHART gateway, network manager, and access point; and one or more WirelessHART field devices and/or adapters. The WirelessHART network is described in the HART specifications published by the FieldComm Group.

2.2 Host

A host provides control or aggregates data in a network. It often incorporates a Human Machine Interface (HMI) between the operator and the process. In the context of WirelessHART networks, a host usually communicates to a WirelessHART gateway using a protocol such as ModbusTCP or similar.

2.3 WirelessHART Gateway

The WirelessHART gateway provides protocol conversion between the protocol used by the WirelessHART network and that of the host.

The WirelessHART access point and network manager are often implemented in the same device or physical piece of hardware as the WirelessHART gateway. When this is the case, it is common to refer to the combination of all three entities as a WirelessHART gateway or simply a gateway. Although the term gateway only refers to the protocol-converting portion of the device, the assumption is made that most gateways contain the network management and access point capabilities.

2.4 WirelessHART Client

The WirelessHART client provides a connection between the wireless network and the gateway. Wireless devices connect to the gateway using a process called “joining.” During this process, wireless devices detect and respond to a network advertisement, request to join the network, authenticate to the network, and are allocated bandwidth for communication of HART message traffic. When devices have fully joined a network access point, they are termed “operational” and are able to communicate data via a request/response method known as client/server; or are able to “burst” data on a pre-determined interval using a publisher/subscriber method. Although both methods allow for data to be passed to the host, the burst method is preferred because of its efficient use of the bandwidth.

Consider the following example:

Request/response:

Message 1: Host sends request message with request for data to a field device.

Message 2: Field device sends response message with response data to host.

Burst:

Message 1: Field device publishes pre-configured message data such as a primary variable or loop current to the Host on a fixed interval.

From this example it is obvious that, the Burst method results in about half the network traffic, freeing the network to take care of other tasks such as keeping track of device configuration changes, communicating with joining devices, searching for lost devices, or gathering statistics on the health and stability of the network. In most cases, an efficient network will use a mixture of both communication methods.

The WirelessHART access point can send messages over the WirelessHART network using its IEEE 802.15.4-compliant radio transceiver. WirelessHART uses the first 15 channels of the IEEE 802.15.4 standard for communication and efficiently avoids interference and maximizes the bandwidth in the 2.4 GHz spectrum by continuously frequency hopping between channels according to a frequency hop sequence. This should not be confused with message hops, which refer to the paths that messages take between devices in a mesh network.

2.5 Network Manager

The WirelessHART network bandwidth is allocated by the network manager. The network manager assigns Absolute Slot Numbers (ASN), or message slots, to field devices wishing to publish burst messages over the network. Devices that have not been allocated bandwidth on the network are not able to communicate with the gateway and are not able to publish messages on the network. The network manager is responsible for the “joining” of field devices, allocation of network bandwidth, managing network security, maintaining a list of network devices, and providing communication paths through the mesh network.

The network manager is responsible for broadcasting the existence of the network to prospective field devices and instructs devices already joined to the network to broadcast on its behalf. Devices may discover the network via an advertisement from any other device already on the network. This advertisement contains a network ID that can be used to provide a unique distinction between otherwise overlapping networks. Only devices that have been programmed to join the network will respond to advertisements of the network ID.

Once an advertisement is received, the device may request to join the network by responding with the correct join key of the network. The join key is a 32-character, hexadecimal string that prevents unauthorized devices from joining the network. The network manager rejects device join attempts by any devices not providing the correct join key.

2.5.1 Network ID and Join Key

After the network manager validates the network ID and join key of the requesting device, the device is allocated with a session key to use it for communicating with the network manager. The session key may be a static key or it may be periodically changed or “rotated” by the network manager as an increased security measure. Only devices which have been allocated communication bandwidth and have valid session keys can communicate on the network. To further increase security, each field device is given a unique session key such that only the network manager can understand and decrypt the data from the field device.

2.5.2 Message Hops

The network forms around the access point, and all devices which can communicate directly with the access point are described as being one “hop” from the access point. Other devices may join the network as long as they can communicate with at least one other device that is

connected to the network. Given this logic, devices could be one or more hops from the access point as long as they have neighbors (or their neighbors have neighbors) which can communicate directly with the access point. Messages may be passed along from device to device in the wireless mesh until they reach their destination, either the host or a remote field device. In this way, the messages follow paths from the source device to the host and vice versa.

2.6 WirelessHART Field Device

The WirelessHART field device can connect into a plant process and can send and receive data over the mesh network. The WirelessHART field device typically consists of a sensor, a transducer, and a transceiver.

2.6.1 Sensors

The sensor connects into the plant process and measures (or controls) some aspect of the analog process, such as temperature, pressure, level, flow, position, etc. The sensor may also provide a discrete connection to the process as is the case with remote I/O field devices.

2.6.2 Transducers

The transducer converts or scales the measurement, so it may be used by a host system in the context of the process. Proportional-Integral-Derivative scaling or conversion takes place in the transducer portion of the field device.

2.6.3 Transceivers

The WirelessHART field device transmits or “hops” HART messages wirelessly to other devices or directly to the access point using an IEEE 802.15.4 compliant radio transceiver.

2.7 HART Field Devices and Wired 4… 20 mA Field Devices

Traditional HART capable “smart” 4… 20 mA devices are similar to WirelessHART field devices except that they use a Frequency Shift Keyed (FSK) HART modem to communicate over a wired loop instead of communicating via a radio transceiver.

2.8 WirelessHART Adapter

In many cases, it is desirable to use existing HART field devices as part of a WirelessHART network. This is possible through the use of a WirelessHART adapter, which bridges the connection between the wired and wireless transmission mediums. WirelessHART adapters contain a WirelessHART transceiver for connection to the WirelessHART network, as well as a 4… 20 mA FSK HART modem, which is used to communicate directly with a HART device via a wired loop.

2.8.1 Connecting to a HART Device

A WirelessHART adapter may be used with a HART field device to collect messages received over the HART 4… 20 mA loop and retransmit these messages via its WirelessHART transceiver. In the case of HART devices that transmit their Primary Variables (PVs) digitally, multiple HART devices may be connected in the same wired loop as a single WirelessHART

adapter, and the WirelessHART adapter may be capable of adapting or bridging the communication between the WirelessHART network and multiple wired devices.

2.9 WirelessHART Commands

The WirelessHART capable host, gateway, network manager, access point, adapters and WirelessHART field devices all communicate using a set of both standard and device specific HART commands. These commands comprise the Highway Addressable Remote Transducer (HART), protocol and form the backbone of both HART and WirelessHART communication standards. These commands are classified into several groups and may or may not be supported by a given network entity.

2.9.1 Universal commands

The commands must be supported by gateways, adapters, WirelessHART and wired 4… 20 mA HART devices. They are used to read the process variables and device status from the field devices.

2.9.2 Common practice commands

These commands are strongly recommended for implementation by gateways, adapters, and field devices as they provide additional functionality for communicating and configuring with field devices.

2.9.3 Wireless commands

These commands are divided into several sub-categories which are required to be implemented and supported by network manager and access point entities, gateways, adapters, and WirelessHART field devices. The commands handle network formation, maintenance, and security as well as other background functions required by the network.

2.9.4 Device-specific commands

These commands provide device-specific functionality to a field device. Additionally, device-specific commands may also be vendor-specific such that they provide unique features or additional capabilities to a vendor’s WirelessHART field devices.

3 Basic Features of AWIN GW100 rev.2

The AWIN GW100 rev.2 is a WirelessHART gateway. It can connect with up to 25 WirelessHART field devices and convert the HART data to Modbus TCP data for easy integration into almost any ModbusTCP based host system. The connection can be established via the onboard Ethernet ports. HART to Modbus TCP mapping is available in both automatic and manual modes. In automatic mode, the gateway automatically assigns registers to available parameters. Whereas, in case of manual mode the user must supply a custom Modbus list in the form of an XML file.

3.1 Get Familiar with AWIN GW100 rev.2

The AWIN GW100 rev.2 is a DIN rail-mount wireless device with a protection rating of IP20 (see Figure 1). The gateway has RJ45 connectors for connection of Ethernet devices. The WirelessHART antenna connector allows remote mounting of the antenna. The gateway comes with built-in LEDs, see description in Table 4.

Table 4: LEDs Information

LEDs Information	
ST	Shows power and device status
MESH	Reports if WirelessHART devices connected
LINK/ DATA	Shows LAN status per port (not marked)
ERR	Reports the device error

The term WirelessHART gateway as used in this product is inclusive of three functions as defined by the HART specifications.
- Gateway (see section WirelessHART Gateway).
- Access point (see section WirelessHART Gateway).
- Network manager (see section Network Manager).

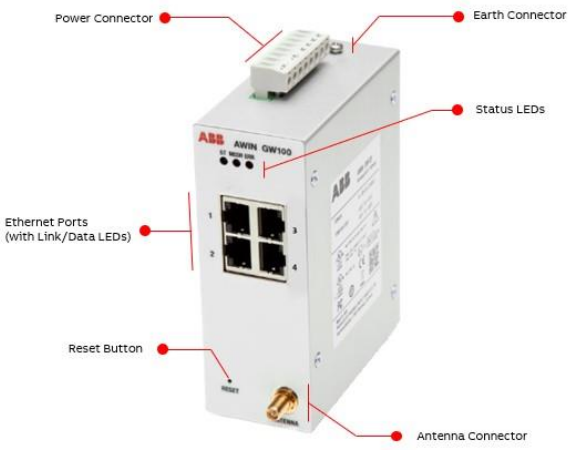


Figure 1: AWIN GW100 rev.2 gateway and its interfaces

3.2 DHCP Server

The AWIN GW100 rev.2 is compatible with networks that use a Dynamic Host Control Protocol (DHCP) server for allocating IP addresses.

3.3 Webserver

The AWIN GW100 rev.2 gateway comes with built-in webserver which allows the user to both configure and monitor WirelessHART network. Moreover, advanced diagnostics are also available via the webserver.

3.4 Operator Authentication for Webserver Access

Authentication mechanisms are used to authenticate an operator accessing the device and to verify that the operator is authorized to assume the requested role and perform services within that role.

Access to the management screens for the AWIN GW100 rev.2 gateway requires that you enter an ID and password. The factory defaults are:

– Access to configuration options

  For access to configuration options, use the following log-in:

  Username = admin

  Password = admin

– Access to monitoring screens

  For access to monitoring screens only, use the following log-in:

  Username = monitor

  Password = monitor

The user must change password after first login or at least before commissioning the gateway.

3.5 Modbus TCP Mapping

The AWIN GW100 rev.2 gateway can function as a protocol converter by mapping the HART command data from the WirelessHART network to Modbus TCP registers. This allows for easy integration of HART data into Modbus TCP host system.

3.6 Network Topology Table

The AWIN GW100 rev.2 gateway's web interface provides a table with connectivity information of WirelessHART devices. It also shows the strength of wireless mesh network in a color-coded format.

3.7 Network Connectivity

AWIN GW100 rev.2 has built-in four ports. Any one of the ports P1-P4 can be connected to an Ethernet switch. The switch can be part of a host network. A typical host system on the network can be a PLC or Automation controller using ModbusTCP protocol to communicate to the gateway. Multiple ports shall not be connected to the same switch or network. Only one port shall be connected to the host network.

The AWIN GW100 rev.2 is compatible with networks that use a Dynamic Host Control Protocol (DHCP) server for allocating IP addresses. AWIN GW100 rev.2 supports both static and dynamic IP address assignment.

The ethernet switch port connected to the AWIN GW100 rev.2 gateway shall have Flow Rate limiter enabled. Overall bandwidth should be capped to 10Mbps (recommended). Avoid mixing field network with other networks, such as control and client/server network. AWIN GW100 rev.2 belongs to a field network only.

AWIN GW100 rev.2 is not an interfacing device. Typically, it is located between level 0 (process) and level 1 (basic control) hierarchy of the automation pyramid. It shall be installed behind switch(es) and firewall(s) from the higher levels.

3.8 Hard Reset

A hardware reset restores the default IP address of 172.16.16.10 (subnet: 255.255.255.0) and resets the AWIN GW100 rev.2 to factory default settings.
To initiate a hardware reset, use a screwdriver or something alike to press and hold the “reset” button, located on the front of the device.
With unit powered on and fully booted:

1. Hold Reset button for 10 seconds and release button.
2. About 10 seconds later the ST and MESH (if it was on) turn off.
3. Gateway will wait ~20 seconds before flashing LEDs.
4. ST and RED LED flash for ~30 seconds.
5. Gateway's ST LED turns to solid GREEN and the system is ready.

Figure 2: Reset button location.

3.9 Declarations and Certificates

AWIN GW100 rev.2 holds the following certificates which makes it suitable for installation in hazardous areas. For terms and conditions, refer to the actual certificates. For other certificates related to regional compliance and declaration of conformity visit www.abb.com.

To comply with FCC, IC and CE RF exposure compliance requirements, the antenna used for this gateway must be installed to provide a separation distance of at least 20 cm from all persons.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

3.9.1 ATEX Certificate

The gateway is ATEX certified and is approved for the following marking. A copy of the certificate can be found in the document ID 4JNO000323, available at abb.com.

 **II 3 G Ex ec nC IIC T4 Gc**

3.9.2 IECEx Certificate

The gateway is IECEx certified. A copy of the certificate can be found in the document ID 4JNO000325, available at abb.com.

Ex ec nC IIC T4 Gc

-40°C ≤ Ta ≤ +70°C

3.9.3 Ordinary Locations

The gateway has been tested and approved for installation in safe areas by UL. The ORDLOC compliance information is available in UL File E521295, Volume D14 available at ul.com.

3.9.4 Hazardous Locations

The gateway has been tested and approved for installation in hazardous areas in the US and Canada. The HAZLOC compliance information is available in UL File E196811, Volume D11 available at ul.com

The gateway rating is as follows:

UL, USA Class I, Division 2 Groups ABCD T4

cUL, Canada Class I, Zone 2 Group IIC T4

The US National Electrical Code (NEC) and the Canadian Electrical Code (CEC) permit the use of marked equipment in the hazardous areas. The US UL and Canadian UL standards are based on the NEC and CEC.

3.9.5 EU Declaration of Conformity

EU Declaration of conformity can be found in document ID 4JNO000322. This document can be found at abb.com.

3.9.6 FCC Compliance

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

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

3.9.7 IC Compliance

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

3.9.8 UKCA

The device is compliant with the UK rules (UKCA).

UK MDOC cert number is: PxCAI22UKEx1246283X.

3.9.9 RCM Compliance

The device complies with the requirements of the relevant ACMA Standards made under the Radiocommunications Act 1992 and the Telecommunications Act 1997.

3.9.10 NCC Compliance

This device complies with Taiwan National Standards.

CCAK23LP1391T3

4 WirelessHART System Planning

4.1 Accessing the Site

To achieve the best radio performance possible, the installation sites have to be given careful consideration. The primary requirements for a reliable installation include:

- Antenna placement that allows for line-of-sight or adequate signal strength
- Primary power source that provides required current
- Protection of radio equipment from exposure to weather or temperature extremes
- Suitable entrances for antenna, lightning arrestor, interface or other required cables, if using remote antennas.

These requirements can be quickly assessed in most applications. A possible exception is the first item, verifying that a clear line-of-sight exists. A non-obstructed path is ideal; however, minor obstructions in the signal path will not always block communication. In general, the need for a clear path becomes greater as the transmission distance increases.

4.2 Path Quality Analysis

With the exception of short-range applications, a path loss study is generally recommended for new installations. The exceptions include distances of less than 50 m, where no test is required in 90% of applications. If a test is to be conducted a path loss study is practical. It predicts the signal strength reliability and estimates the fade margin of a proposed radio link. While terrain, elevation and distance are the major factors in this process, a path loss study also considers antenna gain, coaxial cable loss, transmitter power and receiver sensitivity to arrive at a final prediction.

Path loss studies are normally performed by a communications consultant, wireless hardware vendor or system integrator who uses topographic maps or a software path analysis to evaluate a proposed path.

Although path studies provide valuable assistance in system planning, they are not perfect in their predictions. It is difficult, for example, to consider the effects of man-made obstructions or foliage growth without performing an actual on-air test. Such tests can be done using temporarily installed equipment. ABB can provide radio survey service (AWIN Survey Service) to assess radio environment.

4.3 Signal Strength

The strength of radio signals in a well-designed radio network must exceed the minimum level needed to establish basic communication. The excess signal is known as the fade margin, and it compensates for variations in signal level which may occur from time to time due to foliage growth, minor antenna misalignment or changing atmospheric losses.

While the required amount of fade margin differs from one system to another, experience has shown that a level of 20 dB above the receiver sensitivity threshold is sufficient in most systems. AWIN GW100 rev.2 provide the means for direct measurement of received signal strength using “RSSI (Received Signal Strength Indicator)” readings available in the gateway’s network statistics webpage.

4.4 Antennas and Cabling

The single most important item affecting radio performance is the antenna system. Consider carefully this part of an installation, or the performance of the entire system will be compromised. Quality high gain antennas should be used at all stations. The antennas should be specifically designed for use at the intended frequency of operation and with matching impedance (50 ohm).

Antennas are made by several manufacturers and fall into two categories – omnidirectional and directional (see Figure 3). An omnidirectional antenna provides equal radiation and response in all directions and is, therefore, appropriate for use at master stations which must communicate with an array of remote stations scattered in various directions. Omni-antennas should also be used where clients will be mobile.

At remote fixed stations, a directional antenna, such as a Yagi, is typically used. Directional antennas confine the transmission and reception of signals to a relatively narrow beam width, allowing greater communication range and reducing the chances of interference from other users outside the pattern. It is necessary to aim these antennas in the desired direction of communication (i.e., at the master station).

The end of the antenna (farthest from support mast) should face the associated station. Final alignment of the antenna heading can be accomplished by orienting it for maximum received signal strength.

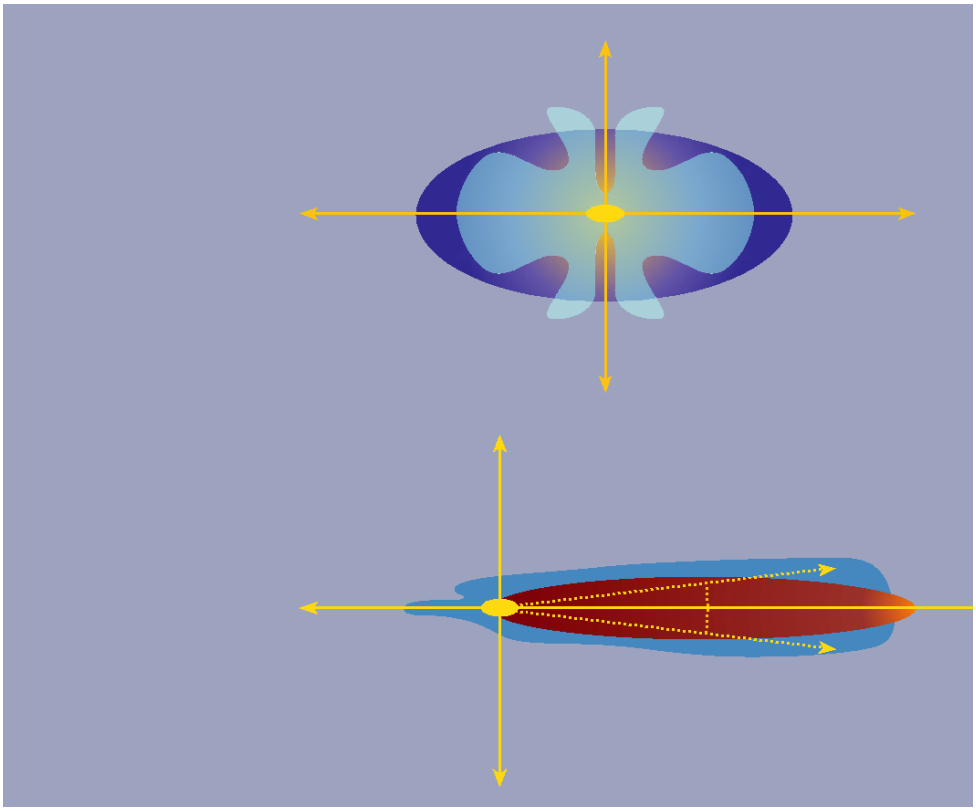


Figure 3: Omnidirectional and directional antenna performance characteristics

4.4.1 Coaxial cable considerations

The importance of using a low-loss antenna coaxial cable is often neglected during radio installation. Using the wrong cable can cause huge reductions in efficiency, and these losses cannot be recovered with any amount of antenna gain or transmitter power.

For every 3 dB of coaxial cable loss, half the transmitter power will be lost before reaching the antenna. The choice of coaxial cable to use depends on: 1) the length of cable required to reach the antenna, 2) the amount of signal loss that can be tolerated, and 3) cost considerations. For long-range transmission paths, where signal is likely to be weaker, a low-loss cable type is recommended.

For a short-range system, or one that requires only a short antenna coaxial cable, a less efficient cable may be acceptable and will cost far less than large diameter cable. Refer to Table 5 for values that allow judging the effectiveness of various cables at 2.4 GHz.

Table 5: Cable types and signal loss (dB)

Cable type	2.4 GHz loss (dB/100 ft.)
RG-58	25.01
RG-213	12.51
PFP-240	12.76
PFP-400	6.68
PFP-500	5.41
PFP-600	4.37

4.4.2 Antenna mounting considerations

The antenna manufacturer's installation instructions must be strictly followed for proper operation of a directional or omnidirectional antenna. Using proper mounting hardware and bracket ensures a secure mounting arrangement with no pattern distortion or detuning of the antenna. The following recommendations apply to all antenna installations:

- Mount the antenna in the clear, as far away as possible from obstructions such as buildings, metal objects, dense foliage, etc. Choose a location that provides a clear path in the direction of the opposite antenna. If the antenna is co-located with another antenna (other than second antenna connector on the same radio), try to get at least one foot vertical (31cm) or one foot (31cm) horizontal separation between the two.
- Polarization of the antenna is important. Most systems use a vertically polarized omnidirectional antenna at the master station. Therefore, the remote antennas must also be vertically polarized (elements perpendicular to the horizon). Cross-polarization between stations can cause a signal loss of 20 dB or more.
- When installed indoors, the radio must be grounded through the DIN rail for DIN rail-mount versions or using the ground lug on the wall-mount versions. A surge arrestor must be used on the antenna for outdoor installations.

4.5 Recommendations for Establishing a Robust WirelessHART Network

To establish a robust WirelessHART network, follow these guidelines:

- All WirelessHART devices shall be operated as mesh nodes.
- If possible, install gateway or it's antenna in the center of the target coverage area.
- Antenna should be mounted with free clearance around it (recommendation - 30cm) and above the ground (1.5m or above). Antenna shall be installed vertically.
- There should be at least 5 devices or 10% of the total, whichever is larger, in the one-hop ring.
- Every device should have at least 3 good neighbors. A good neighbor is a neighbor that has RSSI >-75dBm or has >50% path stability. If not possible, add repeaters.
- Line of sight installation shall be kept to within 200m.

4.6 Maintaining System Performance

Over time, any communications system requires a degree of preventative maintenance to ensure peak operating efficiency. Periodic checks of master and remote sites should be made to identify and correct potential problems before they become threats to system operation. The following areas should be given special attention:

4.6.1 Antennas and coaxial cable

Visually inspect the antenna and coaxial cable for physical damage, and make sure that the coaxial connections are tight and properly sealed against the weather. When using directional antennas, be sure that the antenna heading has not shifted since installation.

4.6.2 Cable connections

All power, data, and ground connections should be secure and free of corrosion.

4.6.3 Power supply

The input voltage to the gateway should be measured to verify that it is within the operating specifications for the radio. Batteries, if used, should be checked for charge level and signs of leakage or corrosion.

5 Installation

Installation, operation, and maintenance may only be carried out by qualified electricians. Follow the installation instructions described. When installing and operating the device, the applicable regulations and safety directives (including national safety directives), as well as general technical regulations, must be observed. Observe the technical data in this user manual and subsequent documentation (www.abb.com).

- In order to protect the modules against electrostatic discharge when working on control cabinets (or junction boxes), the operating personnel must remove electrostatic discharge before opening junction boxes or control cabinets and before touching the gateway.
- The AWIN GW100 rev.2 is snapped onto a standard rail within a control cabinet or switch box. Power is supplied via power plug. The control cabinet or switch box must comply with the specifications of EN 60950-1:2001 with respect to fire enclosure. For power supply requirements refer to document *3BNP103003D3 Specific Conditions Of Use*.
- The device must not be opened or modified. Do not repair the device yourself; replace it with an equivalent device. Repairs may only be carried out by ABB. The manufacturer is not liable for damage resulting from violation.
- The IP20 degree of protection (EN 60529) of the device is intended for a clean and dry environment. Do not subject the device to any load that exceeds the prescribed limits.
- To avoid electromagnetic interference, this product should not be installed or used in residential environments.

The device is designed for installation in zone 2, potentially explosive areas.

Correct usage in potentially explosive areas.

- Do not use the device in atmospheres with a danger of dust explosions.
- Observe the specific conditions of use (3BNP103003D3) in potentially explosive areas.
- The equipment shall be installed inside of a suitably certified tool-secured enclosure that provides a minimum ingress protection of IP54 in accordance with EN IEC 60079-0.
- Only passive antennas may be operated with the gateway.

The device must be stopped and immediately removed from the Ex area if it

- is damaged.
- was subject to an impermissible load.
- was stored incorrectly.
- malfunctions.

5.1 Mounting the Gateway

5.1.1 Mounting the AWIN GW100 rev.2

Figure 4 shows a typical AWIN GW100 rev.2 installation with end clamps and a DIN rail grounding block.

Figure 4: Installation showing end clamps

When mounting the gateway onto a standard 35 mm DIN rail, end clamps should be mounted on both sides of the module(s) to stop the modules from slipping on the DIN rail (see Figure 4).

Modules are installed from left to right on the mounting rail. Install modules to mounting rail as described in the following steps.

5. Attach the AWIN GW100 rev.2 to the mounting rail by positioning the keyway at the top of the module onto the mounting rail (see Figure 5). Then rotate the module inward until the DIN rail latch locks the module in place on the rail. Next, check that the module is fixed securely to the rail by lightly pulling outward on the module.

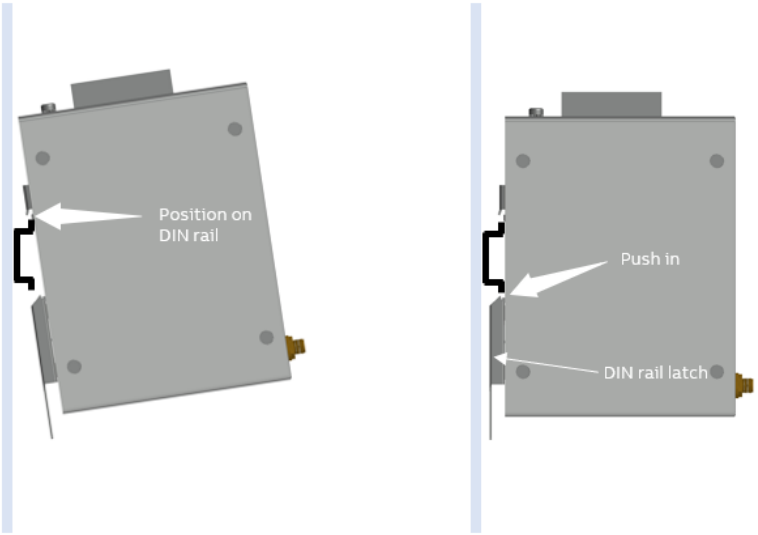


Figure 5: Installing AWIN GW100 rev.2 on the DIN rail

6. Continue attaching any other module(s) to the mounting rail as described in Step 1.

ABB recommends the use of end clamps to prevent modules from sliding left and right on the mounting rail.

7. When all modules are installed, place an end clamp tight up against the left side of the left-most module on the mounting rail. Then place a second end clamp tight up against the right side of the right-most module on the mounting rail.
8. Connect AWIN GW100 rev.2's earth connection to an earth ground.

Connect the DIN rail to protective earth ground using a grounding terminal block. To remove AWIN GW100 rev.2 follow the procedure shown in Figure 6.

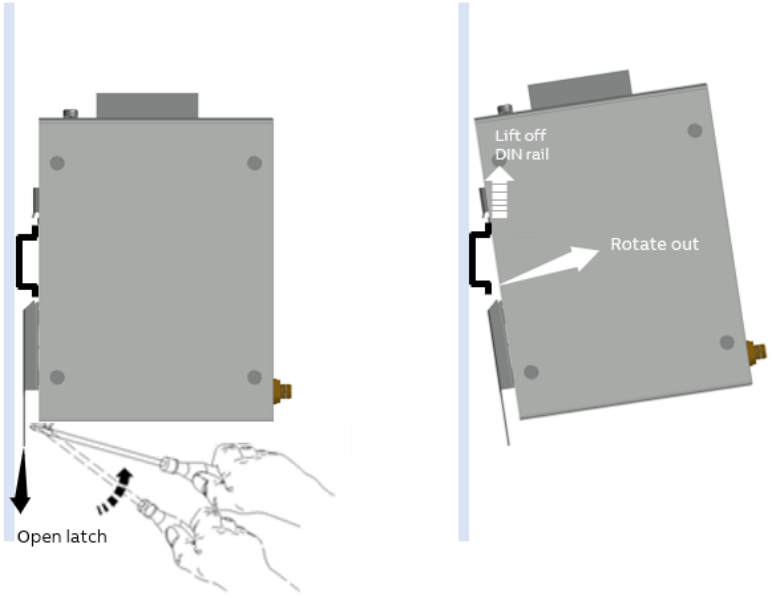


Figure 6: Removing AWIN GW100 rev.2 from the DIN rail

5.2 Making connections and powering up

5.2.1 Power connections

Installation notes:

- Installation, operation and maintenance may be carried out only by qualified electricians. Follow the specified installation instructions. The applicable specifications and safety directives (including the national safety directives), as well as the general technical regulations must be observed during installation and operation. The technical data should be taken from the packaging instructions and the certificates (conformity assessment, other possible approvals).
- Opening the device or making changes to it is not permitted. Do not repair the device yourself but, replace it with an equivalent device. Repairs may be carried out only by the manufacturer. The manufacturer is not liable for any damage due to violation of the prescribed regulations.

- The IP20 degree of protection (EN 60529) of the device is intended for a clean and dry environment.
- Do not subject the device to any load that exceeds the prescribed limits.
- Only passive antennas may be installed on the devices.
- The device is not designed for use in environments with danger of dust explosions.

Power supply of the device must comply with the suitable requirements:

- Class 2 circuit according to National Electrical Code, NFPA-70 and Canadian Electrical Code, Part 1, C22.1
- Limited Power Supply (LPS) according to EN/IEC 60950-1 or EN/IEC 62368-1
- Limited-energy circuit according to EN/IEC 61010-1

Connect a regulated power source to the transceiver. The supply voltage can range from 10.8 to 30.5 VDC with a nominal voltage of either 12 VDC or 24 VDC is recommended. The power supply must be able to supply 130 mA of current at 24 VDC. Figure 7 provides wiring information for the AWIN GW100 rev.2. Operating ambient temperature range is -40…70 °C.

Figure 7: AWIN GW100 rev.2 power connections

5.2.2 Ethernet connections

Connect a CAT5 Ethernet cable between the port on the AWIN GW100 rev.2 and the network adapter card on your computer. Use either a crossover (C/O) or 1:1 cable as the radio has autocross functionality. The cable should not exceed 100 m (329 ft.) in length. Alternatively, an Ethernet switch can be used for connection.

5.2.3 Antenna connections

There is one antenna connector on the AWIN GW100 rev.2 (see Figure 4). A single antenna is used for the WirelessHART mesh network.

Observe the maximum RF power allowed in your country. Only use antennas and cables recommended by ABB.

6 Configuration

6.1 Configuring a PC to communicate with AWIN GW100 rev.2 WirelessHART Gateway

1. Connect the AWIN GW100 rev.2 to an Ethernet network using a CAT5 cable plugged into the RJ45 socket (P1 port).
2. Go to the **Network Connections** dialog box, and then click **Local Area Connections** button. Right-click and select **Properties** from the context menu.
3. Highlight **Internet Protocol (TCP/IP)**, and then click **Properties** button.
4. Click **Use the following IP address** button, and enter a desired IP address for the PC, for example, 172.16.16.16 in the “IP address:” field.

IP address assigned to the PC must be different to that of the AWIN GW100 rev.2 gateway.

5. Enter 255.255.255.0 in the “Subnet mask:” field, and then click **OK** button.

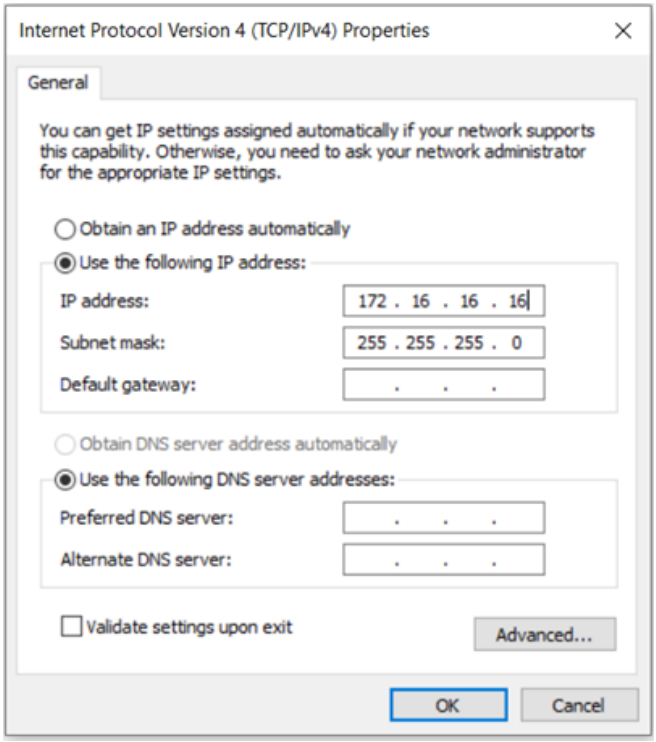


Figure 8: Properties window to change IP address of a PC

These steps may be different depending on MS Windows version used. These steps are valid for Windows 10 only.

6.2 Log onto AWIN GW100 rev.2 WirelessHART Gateway

1. Apply power to the gateway and run a browser program (such as, Internet Explorer or Chrome) on your computer. Wait until the ST LED is on (not flashing), indicating the boot-up procedure is complete and the AWIN GW100 rev.2 is operational.
2. Enter the following IP address into the “Address” field of the browser: https://172.16.16.10

   If a browser prompts security warning (due to certificate) then proceed.
3. Provide the following details on the login screen and select Login.

   Enter the default login credentials:

   – **Username:** admin

   – **Password:** admin

Figure 9: Login screen

6.3 View Gateway Information

After login, the home page shows the following basic information about the AWIN GW100 rev.2 gateway.

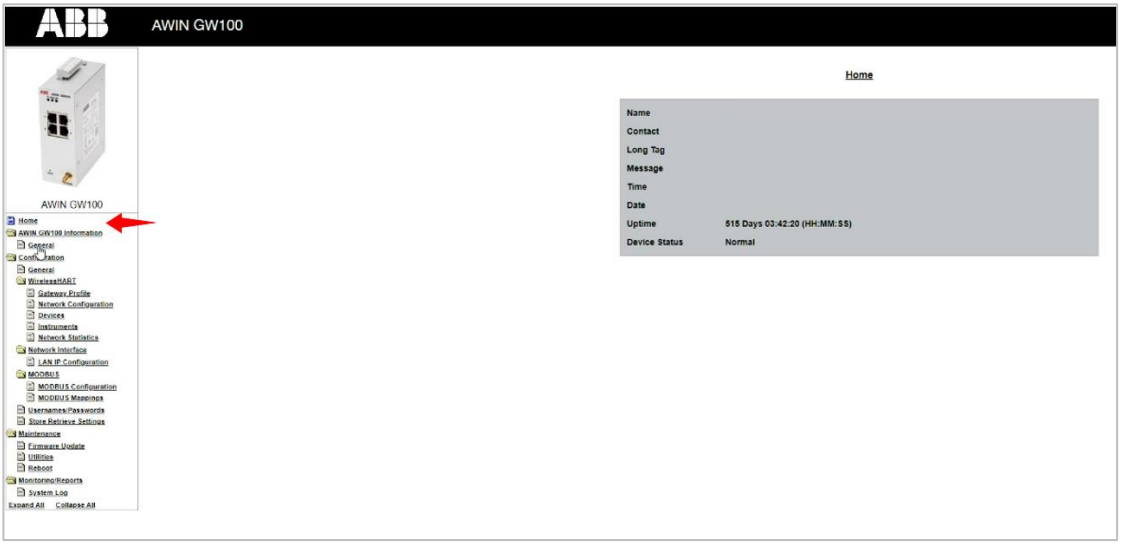


Figure 10: Home screen showing AWIN GW100 rev.2 data.

The fields in this window are:

Table 6: Home screen fields

Field	Description
Name	A user adjustable field. Information on where this device was installed or the site name is shown here. The factory default is a blank field.
Contact	The name of the individual responsible for the operation of this device.
Long Tag	A user adjustable field that can be interfaced to a HART system. It may be the same as the “Name” field.
Message	A HART parameter field that can store a short message about the device or network.
Time	Time of the device’s internal clock.
Date	Date of the device’s internal clock.
Uptime	Shows how long the device has been operating.
Device Status	Shows the current operating condition of the gateway.

On the left side of the window are navigation links to access various information screens. The screens are grouped by category. To expand all the categories and see all the available screen selections, click **Expand All** at the bottom of the screen. To collapse all categories, click **Collapse All** at the bottom of the screen.

To make changes to the data shown on Home page, click on **Configuration** > **General**. See Figure 11 for details.

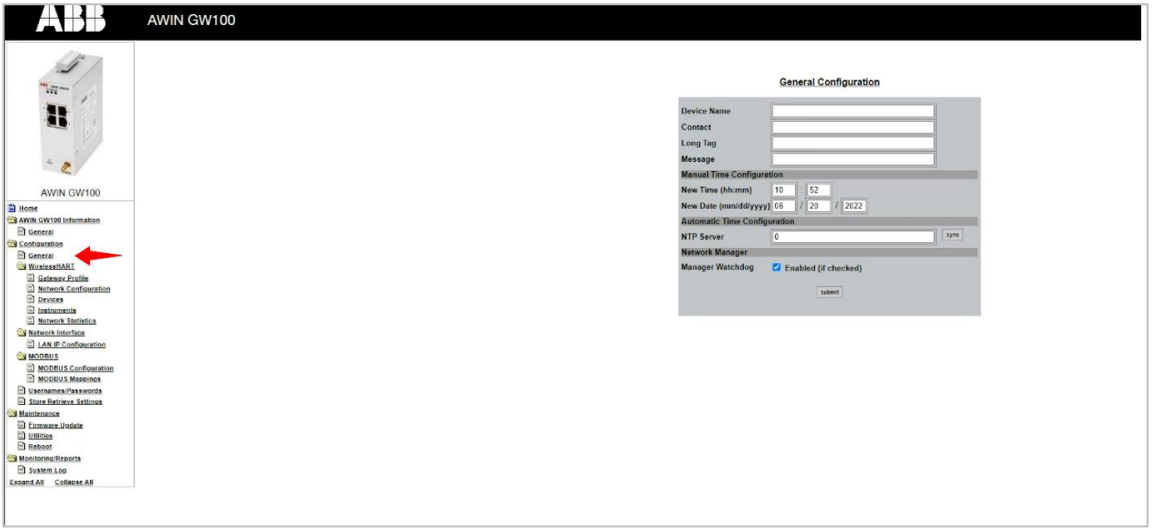


Figure 11: General Configuration screen showing configuration data.

Manager Watchdog function continuously monitors the stability of the network manager and resets or reboots the gateway if deemed necessary. This is a user configurable function and can be enabled and disabled. By default, it is enabled.

6.4 General AWIN GW100 rev.2 Gateway Information

Click **Device Information** > **General** in the left navigation column to view the current network configuration and device version of the AWIN GW100 rev.2.

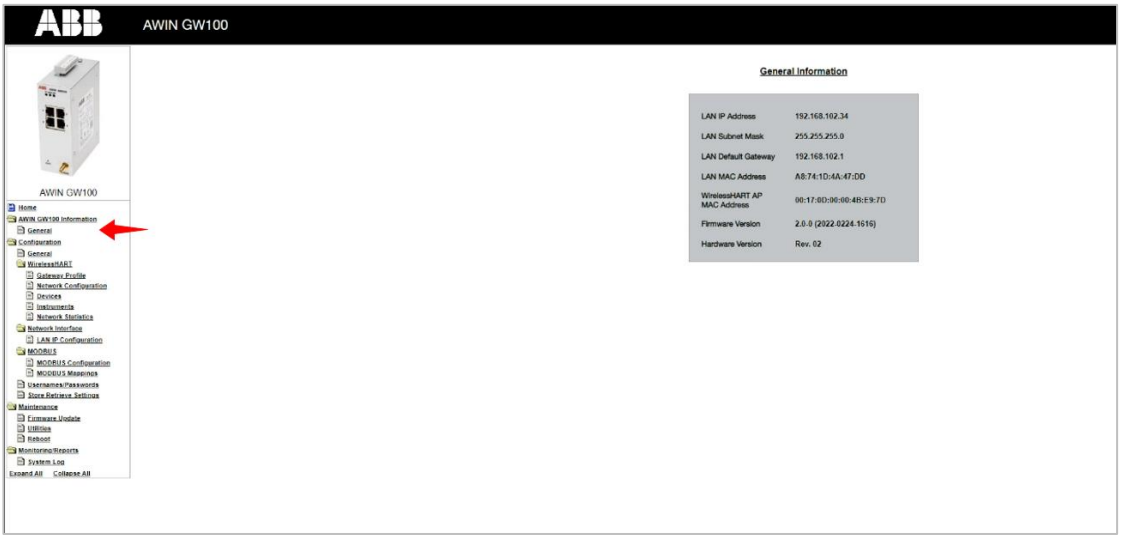


Figure 12: General AWIN GW100 rev.2 Information screen

The fields in this window are:

Table 7: Information screen fields

Field	Description
LAN IP Address	The logical address of the LAN port. The IP address uniquely identifies this device on the network.
LAN Subnet Mask	Bit mask used to tell how much of an IP address identifies the subnetwork the host is on, and how much identifies the host. This subnet mask applies to the 10/100 Mbps LAN port.
LAN Default Gateway	A node on the network that serves as an access point to a different network for the LAN port.
LAN MAC Address	(Media Access Control address, MAC address) is the address for the network card.
WirelessHART AP MAC Address	MAC address for the WirelessHART radio in the gateway.
Firmware Version	Version of software loaded into the AWIN GW100 rev.2.
Hardware Version	Shows version and revision level of the circuit boards.

6.5 WirelessHART Profile Configuration

1. Click **Configuration** > **WirelessHART** > **Gateway Profile** in the left navigation column to view and select the WirelessHART Gateway Profile.

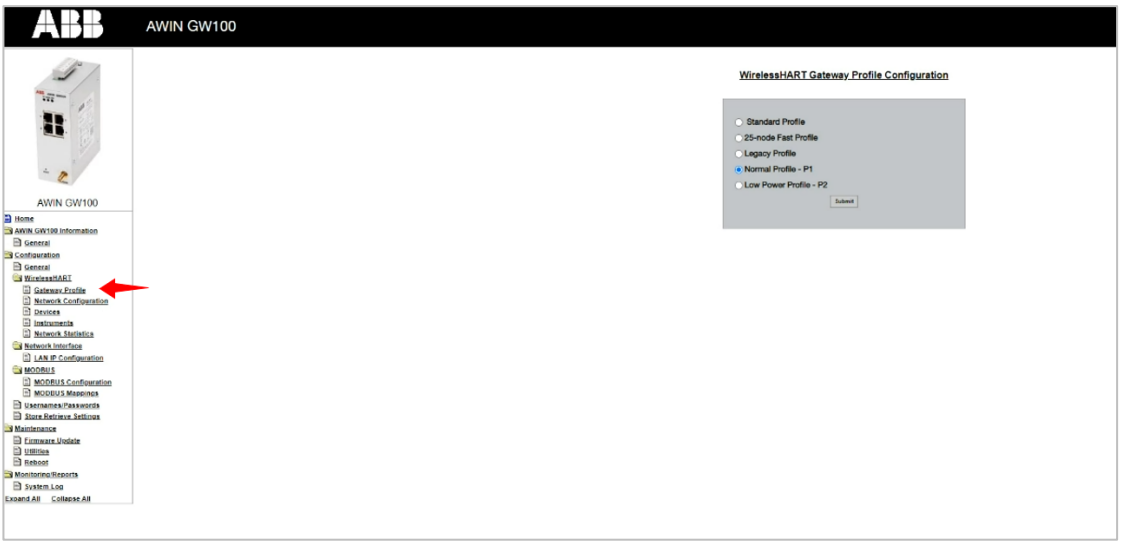


Figure 13: Gateway Profile Configuration screen

There are five profiles available as shown in Table 8.

Table 8: Gateway Profiles

Mode	Description
Standard Profile	It creates a standard WirelessHART frame size.
25-node Fast Update	It allocates additional time slots for faster updates. It is recommended for time sensitive applications.
Legacy Mode	It is optimized for networks consisting of loop powered WirelessHART adapters to reduce power consumption.
P1	This profile allows about 4.5 pkt/s to be injected by the gateway into the network. It is the factory default profile. **Note:** This profile option is available in firmware version 1.5-1.
P2	This profile has one-eighth of the downstream capacity. Using P2 can save all devices battery power but takes longer to build the network and greatly reduces downstream application bandwidth. **Note:** This profile option is available in firmware version 1.5-1.

Table 9: WirelessHART gateway profile settings

WirelessHART Gateway Profile	Frame Size for Upstream Traffic	Frame Size for Downstream Traffic	Frame Size for Advertising Traffic
Default	Standard	Standard	Standard
25-Node Fast Update	128	128	128
Legacy Mode	1024	256	128
P1	1024	256	128
P2	1024	2048	128

2. Click **Submit** button to save the changes.

The AWIN GW100 rev.2 must be rebooted for the changes to take effect.

6.6 Configuration of WirelessHART Network

Click on **Configuration** > **WirelessHART** > **Network Configuration** in the left navigation column to configure the WirelessHART network.

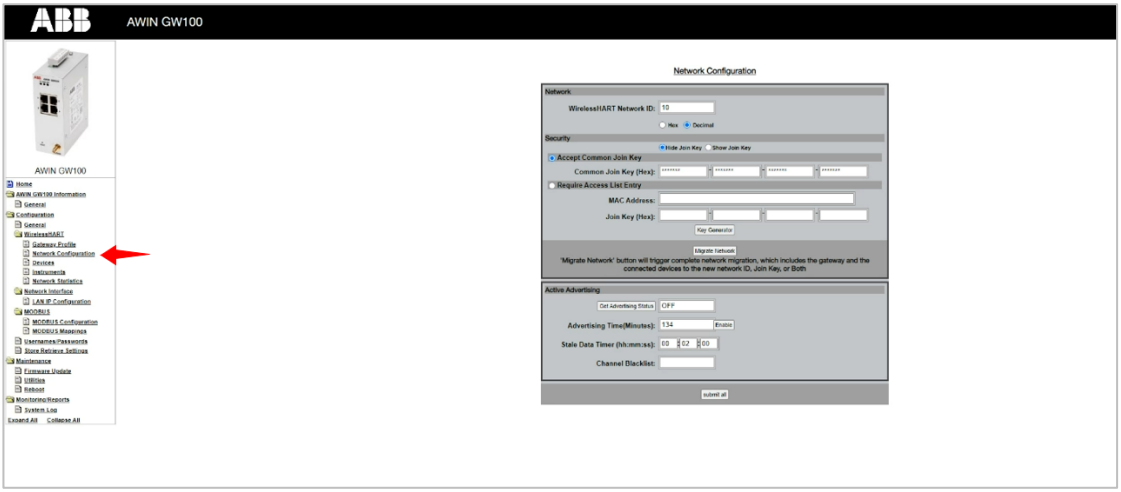


Figure 14: Network Configuration screen

Various WirelessHART Network Parameters are as follows:

Table 10: WirelessHART Network Parameters

Field	Description
WirelessHART Network ID	Can be provided in hexadecimal or decimal format.
Accept Common Join Key	To enable the Common Join Key security mode, click the **Accept Common Join Key** radio button. See Security section for details.
Common Join Key	If “Accept Common Join Key” is enabled then provide common join key in hexadecimal format with 32 characters. Devices that have this Common Join Key can join the network. See Security section for details.
Require Access List Entry	Allows access via an external join list in addition to a Join Key. See Security section for details.
MAC Address	Network card address for the corresponding WirelessHART device being configured.
Join Key	A device that has this Join Key must also have the corresponding MAC address to join the network.
Key Generator	This functionality automatically creates a join key.
Migrate Network	When selected, this functionality migrates the complete network (AWIN GW100 rev.2 gateway and connected WirelessHART) devices to the new WirelessHART network ID or Join Key or both. Depending on what was changed by the user on the page. This option is related to Accept Common Join Key functionality.
Get Advertising Status	When active advertising is “ON,” the AWIN GW100 rev.2 sends frequent beacons to join the network.
Advertising Time	The period of time Active Advertising is enabled. It can be enabled by selecting Enable button to the right of the field.

Field	Description
Stale Data Timer	Data from WirelessHART devices is cached in the gateway. This allows the gateway to respond quickly to host requests without having to constantly obtain fresh device data (a much slower transfer). To ensure the validity of the data stored in cache, each point of data is time stamped. If the cached value has not updated within one-third of the stale data timer value, a downstream request for the update will be sent to the device. If the data in cache is not updated within the stale data timer interval, a Modbus Exception code will be generated to the host system and the cached value will be cleared from the gateway.
Channel Blacklist	Allows specific WirelessHART channels to be blocked from use in the channel-hopping scheme. Channels must be blocked in pairs, so an odd number of channels is always available. To provide blacklist channels: Separate channel numbers with a comma and no spaces, example: 3,5,11,12. See section Channel Blacklist for details.

By selecting **Submit All**, the parameters configured on this page are saved and downloaded to the AWIN GW100 rev.2 gateway.

6.6.1 Security

Two methods of security are available in a WirelessHART network created by AWIN GW100 rev.2.

Accept Common Join Key

The Common Join Key security method uses a single, common key value entered in all WirelessHART devices and the AWIN GW100 rev.2 gateway. Each WirelessHART device sends the same common key. If the key matches the entry in the gateway, the device is allowed to join the network.

In the **Common Join Key** field, enter the common key value.

Require Access List Entry

The Access List security method allows access via an external join list in addition to a Join Key.

To enable the Require Access List security mode, click the **Require Access List Entry** radio button. In the **MAC Address** field, enter the MAC addresses of the WirelessHART devices in the network.

In the **Join Key** field, enter the key value. The key value consists of four fields of hexadecimal characters (0-9, A-F) for a total of 32 characters. Click **Submit** button after entering each MAC address.

After entering all the MAC addresses and corresponding Join Keys, reboot the gateway and allow approximately 30 minutes to 1 hour for the network to form.

6.6.2 Channel Blacklist

Channel blacklisting is a way of limiting the number of channels used in a network. When channels are blacklisted, they are not used in the network.

Although the network may operate on as few as five channels, it is recommended that the network run on as many channels as possible for more overall available bandwidth. Note that the number of usable channels must be an odd number.

To blacklist a channel, enter the frequency of the **Channel Blacklist** field. The channel must be blacklisted in pairs. Table 11 lists the frequency of each channel.

Table 11: Frequency of each channel of Network

Channel No.	Frequencies	Channel No.	Frequencies
1	2405	9	2445
2	2410	10	2450
3	2415	11	2455
4	2420	12	2460
5	2425	13	2465
6	2430	14	2470
7	2435	15	2475
8	2440		

6.7 View Devices

Click **Configuration** > **WirelessHART** > **Devices** in the left navigation column to view the number of devices in the WirelessHART network.

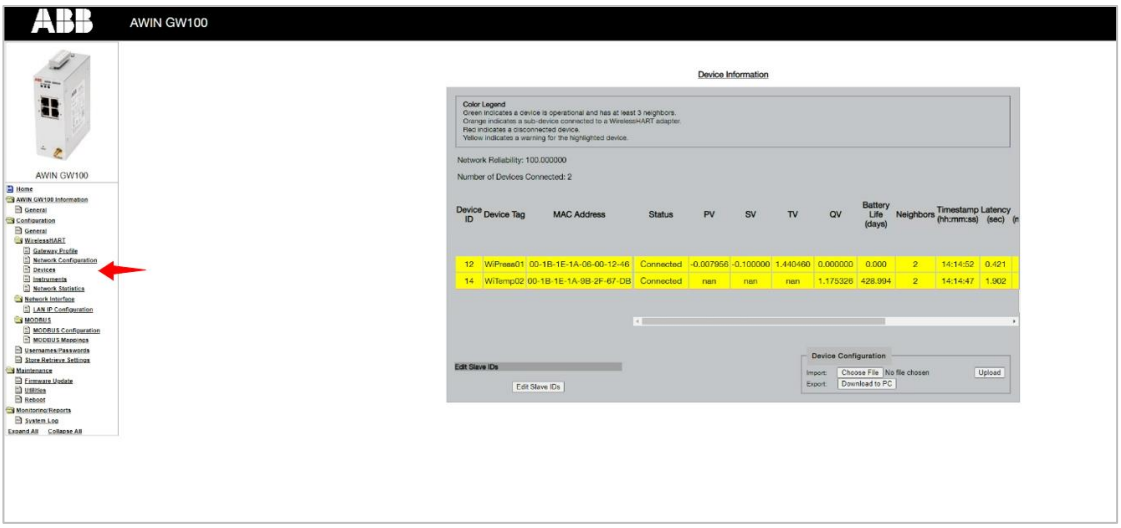


Figure 15: Device Information screen

The device information page displays data about the devices in the WirelessHART network. The Device ID is used for addressing the device via Modbus TCP. Devices connected to WirelessHART adapters appear below the adapter and do not have a MAC address.

Network reliability is a measure of the percentage of packets received by the AWIN GW100 rev.2 divided by the total packets on the network.

The list of devices is color coded to indicate the status of each device.

Table 12: Color code

Color	Description
Green	The WirelessHART device is operating properly, connected to the network and has at least three neighbors.
Yellow	The WirelessHART device is operating properly, connected to the network and has less than three neighbors.
Orange	The HART device is connected to the WirelessHART adapter shown above it.
Red	The device is no longer communicating with the WirelessHART network.

The **Devices** information page refreshes automatically. For a better performance, disable webpage caching in the browser you are using.

For Internet Explorer 11 it can be done as follows:

1. From the top right corner of Internet Explorer 11, click the **settings** icon.
2. From the menu, select **Internet options**.
3. On the **General** tab, locate the **Browsing history** section, and click **Settings**.
4. On the **Temporary Internet Files** tab, confirm that **Every time I visit the webpage** is selected.
5. On **Caches and databases** tab, confirm that **Allow website caches and databases** is not selected.
6. Click **OK**.

It is recommended to use Chrome or Firefox browsers with disabled webpage cache.

The following information is shown for each device.

Table 13: Device Information

Field	Description
Device ID	The identification number assigned to the attached WirelessHART and HART devices. It can be changed by using the “Edit Slave IDs” option on the same page. See Section Edit Slave Device for details.
Device Tag	Long tag of the HART device.
MAC Address	Displays the network card address for the corresponding WirelessHART device.
Status	Displays whether a device is connected or disconnected.
PV	Displays the Primary Value of the corresponding HART device.
SV	Displays the Secondary Value of the corresponding HART device.
TV	Displays the Tertiary Value of the corresponding HART device.
QV	Displays the Quaternary Value of the corresponding HART device.
Battery Life	Displays the expected remaining life of the battery powering the devices (if “65535” is displayed, the device is line powered with a power supply or waiting for battery life information to be provided by the device).
Neighbors	The number of neighbors a WirelessHART device can communicate with.
Timestamp	In (hh:mm) format, is the time when the data was most recently polled.
Latency	Measure of time it takes to respond and update all the corresponding data fields (measured in seconds).
Bandwidth	In (msec/packet) format, is the available data rate to the corresponding device.
Joins	The number of times a device connected to the gateway since bootup.
Command 3 period	HART command 3 continuous burst period.
Command 3 status	HART command 3 burst status (ON/OFF).
Active Pipe	This field shows the status of pipe for a device. **Note**: The Active Pipe option is available in firmware version 1.5-1.
Fast Pipe Control	Fast pipe can be enabled and disable for a device using this function. Notes: Only one device can have a pipe at any point in time. The Fast Pipe Control option is available in firmware version 1.5-1.

6.7.1 Delete a Device

To remove a device from the list (i.e. WirelessHART network), right-click on the disconnected device in **Devices** page and a delete option will appear. Select this option to confirm.

Only devices that are not connected may be deleted from the device list.

To delete an active device, power down the device and wait until the status column indicates the device is disconnected and the row is red.

6.7.2 Edit Slave Device

To edit a slave device, click **Edit Slave IDs** button and enter the new ID number in the field next to each device. When finished, click **OK** button to save the changes, or click **Cancel** button to discard changes.

It may take a few seconds for the new ID numbers to take effect.

6.7.3 Device Configuration

Export Device Configuration

The gateway provides an option, **Download to PC**, to export the existing configured devices configuration in XML format.

Import Device Configuration

The gateway provides an option to import new configuration, **Upload**, for connected devices in XML format. Once the import file is uploaded, the gateway downloads the new configuration to the connected devices. This option simplifies and automates devices configuration.

The details of the XML format are provided in Appendix.

ABB's AWIN WirelessHART Gateways Configurator (3BNP102928) can be used to import, edit and export device configuration. For further details, refer to Bulk Configuration Guide (4JNO000307).

6.8 Instrument Table

Click **Configuration** > **WirelessHART** > **Instruments** in the left navigation column to view the number of devices in the WirelessHART network.

This page has similar information as shown in Devices page. However, it has information about the burst commands cached in the gateway.

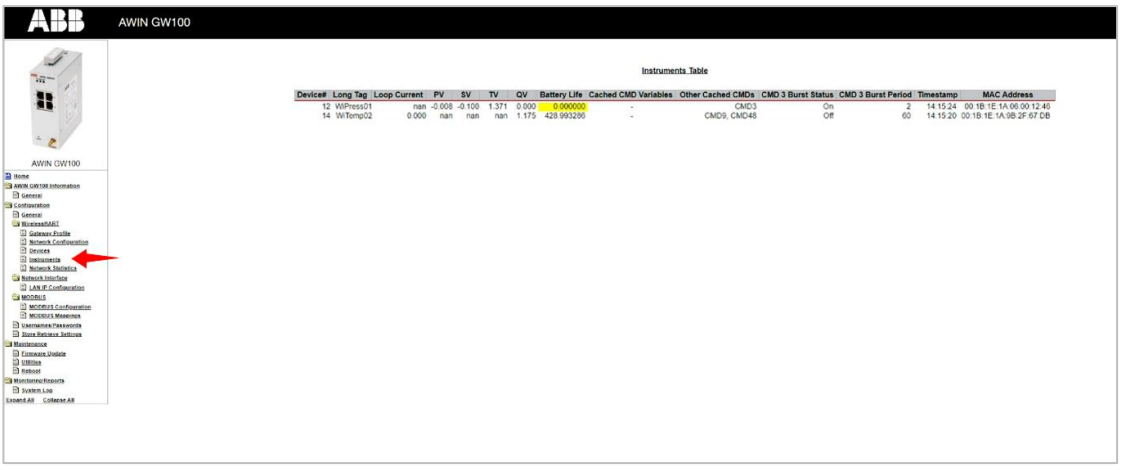


Figure 16: Instruments table screen

6.9 Network Statistics

Click **Configuration** > **WirelessHART** > **Network Statistics** in the left navigation column to view the topology of WirelessHART network.

This page is designed to show the connection status and connectivity information of connected devices, along with information about the routing structure of the network. This page shows the topology information in a table rather than on a map. User can expand each device connectivity information to see its neighbors. The page also shows the summary of key performance indicators.

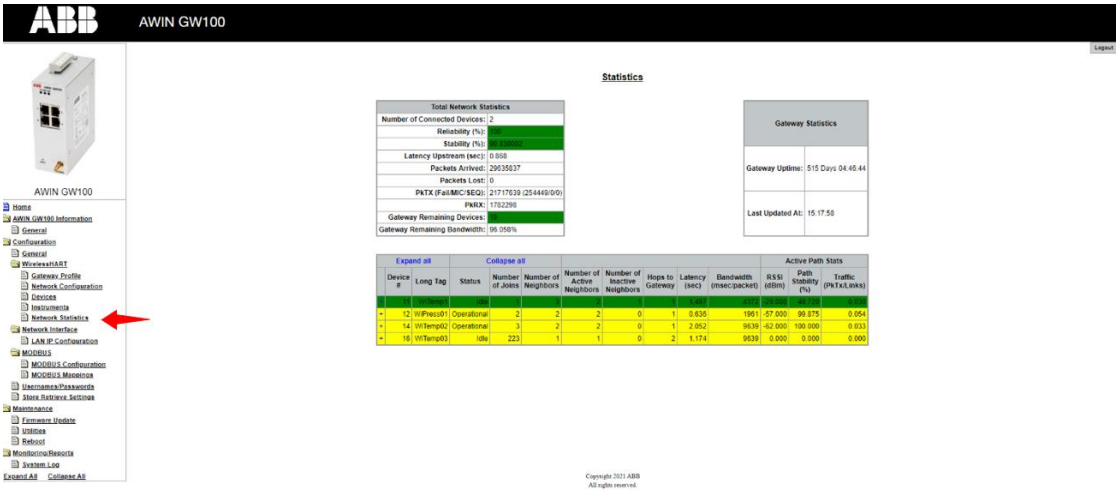


Figure 17: Network Statistics screen

6.10 IP Configuration

Click **Configuration** > **Network Interface** > **IP Configuration** in the left navigation column to show the Local Area Network (LAN) configuration parameters.

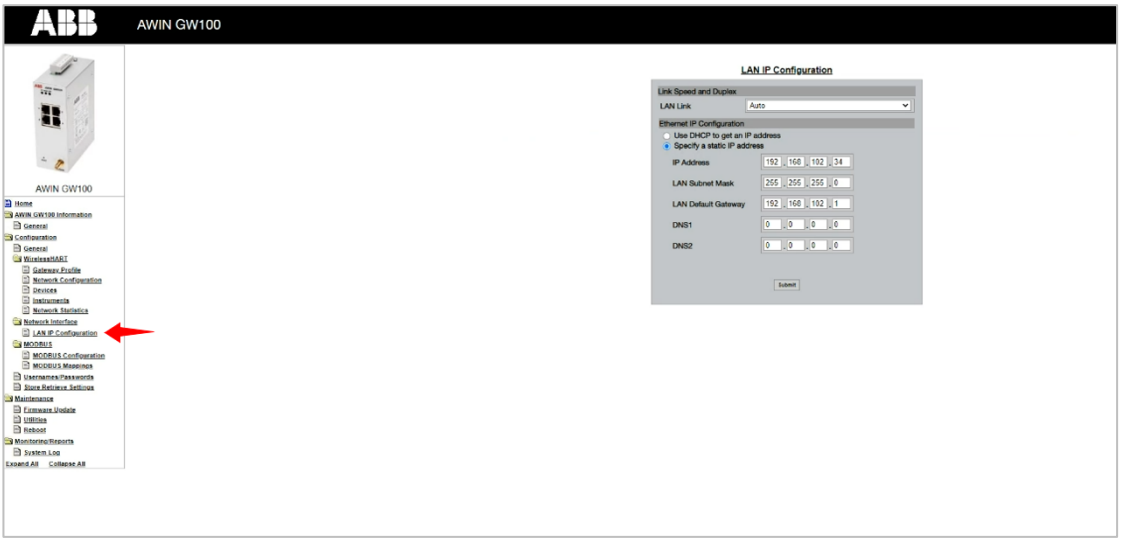


Figure 18: IP Configuration screen

The buttons and fields in this window are:

- **Link Speed and Duplex** determines the speed of the communication channel. Leave the setting at AUTO if not sure about the link speed. If manual option is selected, then the connected device must be set to the same speed.
- **Ethernet IP Configuration** selects the method your network uses to obtain IP addresses. If using static IP addresses, enter the IP address assigned to the gateway. Each device on the network must have a different IP address.

If a DHCP server is on the network and will assign IP addresses to the AWIN GW100 rev.2, click **Use DHCP to get an IP address** radio button.

If the IP address is changed from the factory default, you will need to know this to log back into the gateway for future configuration changes.

Enter a “LAN Default Gateway,” if desired.

6.11 Modbus Configuration

Click **Configuration** > **MODBUS** > **MODBUS Configuration** in the left navigation column to show the Modbus Configuration parameters.

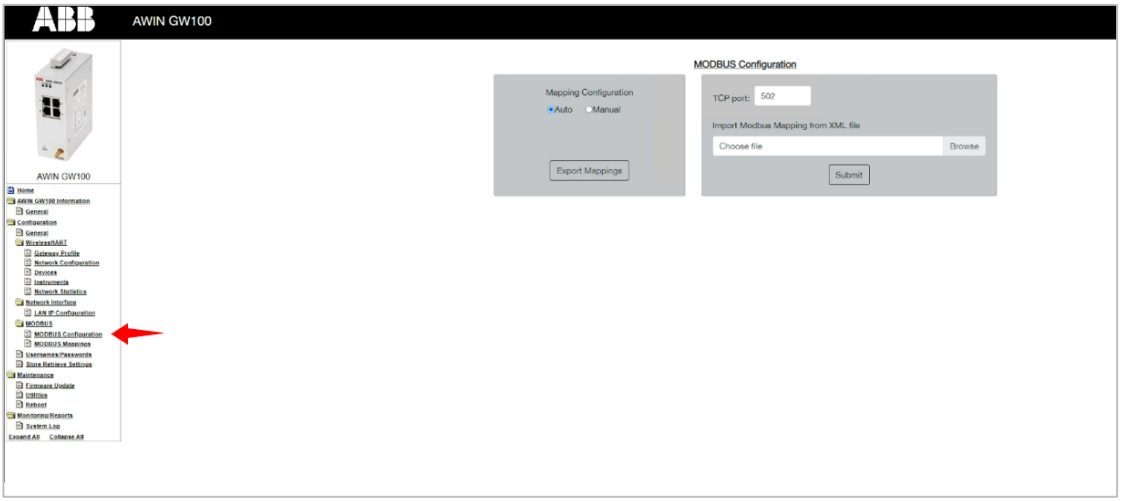


Figure 19: Protocol Configuration screen

The gateway offers two options for Modbus configuration.

- **Auto (default option):** If this option is selected, then the available gateway and devices' parameters are automatically mapped to the holding registers.
- **Manual:** If this option is selected, then the user must also provide the custom Modbus map they wish to use. The map must be uploaded using the Browse option followed by **Submit** button. For details on the Modbus file structure refer to the section Modbus Import File Structure.

  In the Modbus **TCP Port** field, enter the Ethernet port number. The default is 502. Click **Submit** to save changes. The device must be rebooted for the changes to take effect.

User can also export the Modbus map as-is currently configured in the gateway using the **Export Mappings** button on this page.

Modbus does not natively guarantee secure communication. Any node able to communicate with the AWIN GW100 rev.2 via Modbus can perform unwanted changes or misconfigurations that may disrupt the intended operation of the AWIN GW100 rev.2 and the connected systems to it.

It is recommended to limit the Modbus communication within trusted networks and to strictly control accesses to such networks.

6.12 Modbus Map

Click **Configuration** > **MODBUS** > **MODBUS Mapping** in the left navigation column to show the current Modbus map.

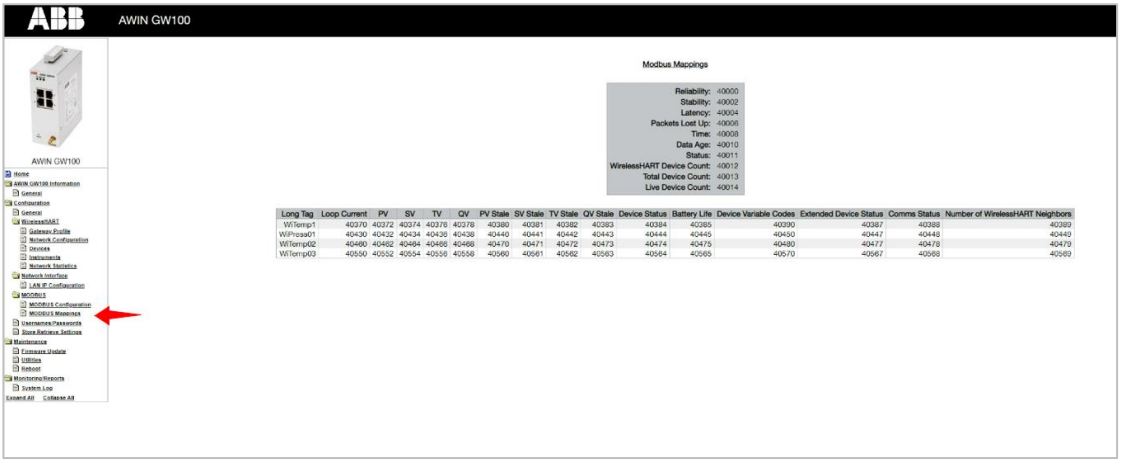


Figure 20: Modbus Mapping screen

6.13 Passwords

There are administrator password and monitor password. The administrator can make changes to the configuration, whereas a monitor can only view information.

To change or set passwords, click **Configuration** > **Username/Passwords** in the left navigation column. Passwords must be 10 characters long.

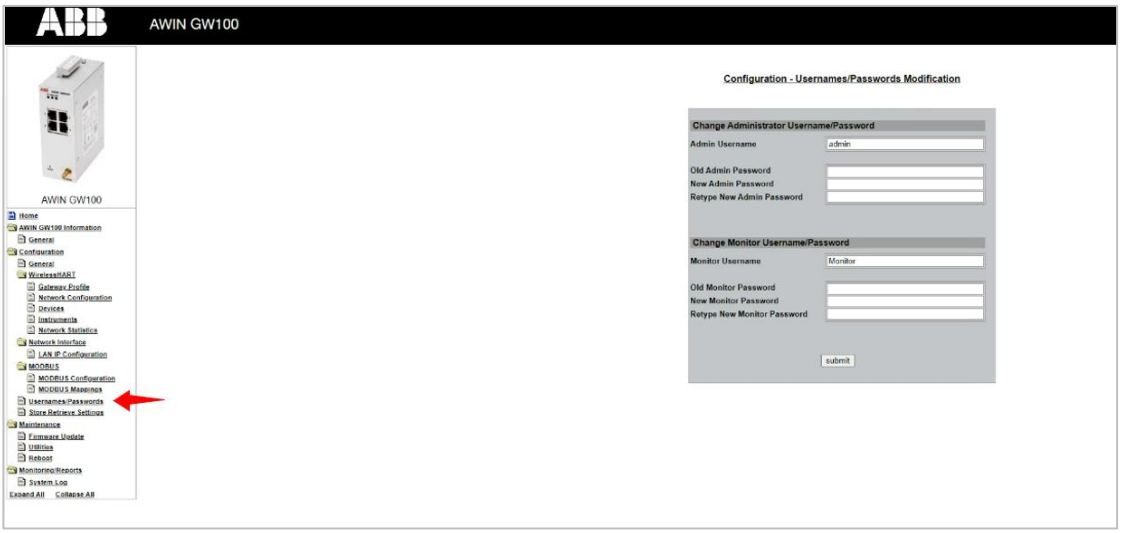


Figure 21: Configuration - Username/Password Modification screen

6.14 Store and Retrieve Settings

The **Configuration > Store Retrieve Settings** screen provides the following options:

– **Factory Default** – it can load the factory default parameters. To do so, select **Set Factory Defaults**.

In this case, IP address is not restored to factory default. It remains as-is. However, if you want to also reset IP address, you can use hard reset option.

– **Upload Configuration to device** – it can upload the configuration to the gateway from a previously saved file. User must “Choose” the Config file, add “Passphrase”, and click “Send Configuration to Device”.

– **Send Configuration to File** – it can export gateway’s existing configuration to a PC’s hard drive. A “Passphrase” is required.

– **Export As-Built Configuration** - it can export gateway’s existing configuration in text format. It will only export configuration of connected devices.

A 10-character passphrase is required to protect/validate the file before it can be saved or retrieved from a PC. It prevents unauthorized users from applying the system configuration file to an unauthorized access point to gain access to the network. Always record this passphrase when saving a configuration file. It will need to be re-entered each time that specific configuration file is uploaded to the AWIN GW100 rev.2.

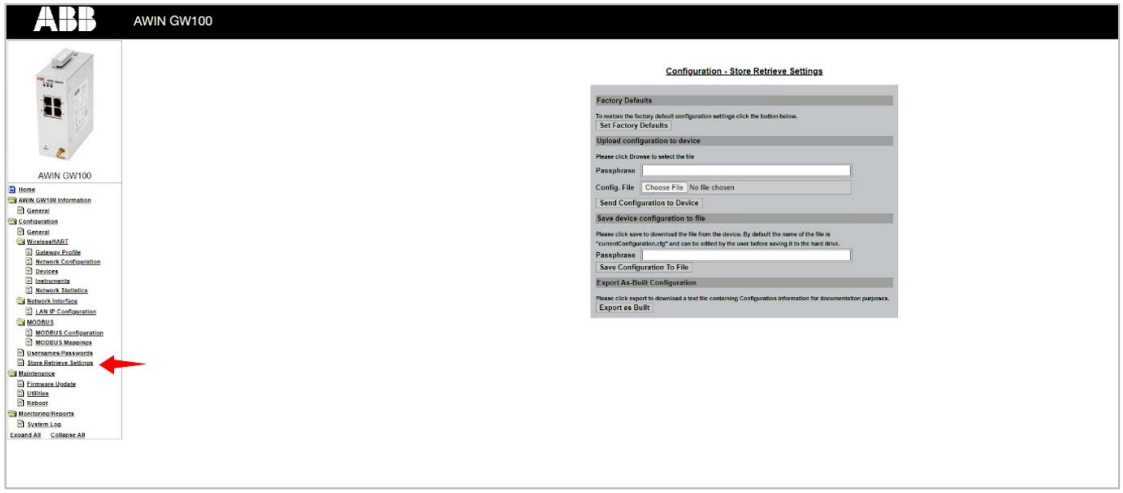


Figure 22: Configuration - Store Retrieve Settings screen

6.15 Maintenance

6.15.1 Firmware Update

Click on **Maintenance** > **Firmware update** in the left navigation column to view the current version of firmware and install a new version (see Figure 23).

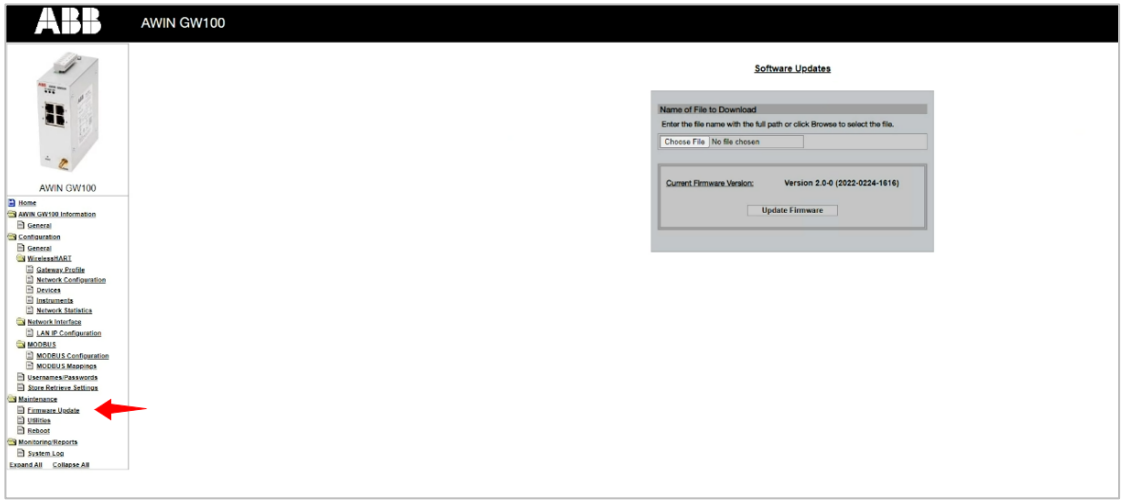


Figure 23: Firmware Update screen

To install a new version of firmware, download the firmware to a local drive on the connected computer. Enter the file path in the field or click **Choose file** button to locate the file. Click **Update Firmware** button to install the update. Follow the messages that appear during the update process.

6.15.2 Utilities

Click **Maintenance** > **Utilities** in the left navigation column to access the “Utilities” screen (see Figure 24).

The “Utilities” screen includes a field to enter an IP address or host name. Click **Ping** button to find out if it is connected and functional.

The “Utilities” screen also includes an **Auto Logout Timer** field. If no activity occurs from the user within the selected time, the web manager will logout. Click the desired radio button and then click **Submit** button. The factory default setting is “Disable.”

The “Utilities” screen also includes a **Reform WirelessHART Network** option. The user can re-form the WirelessHART network established by the gateway by clicking “Reform Now” button.

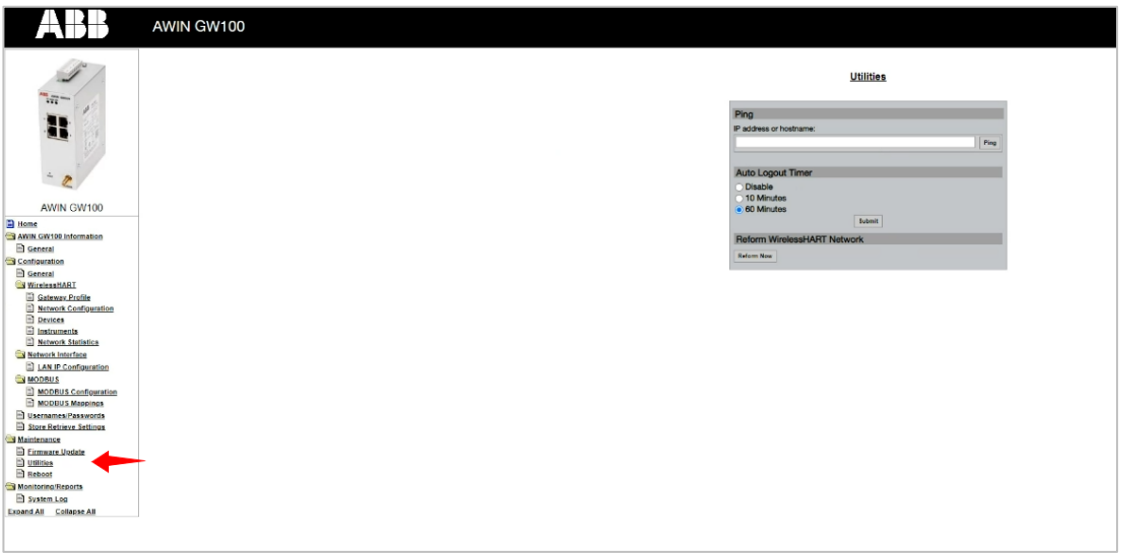


Figure 24: Maintenance- Utilities screen

6.15.3 Reboot

Click **Maintenance** > **Reboot** in the left navigation column to reboot the WirelessHART gateway (see Figure 25).

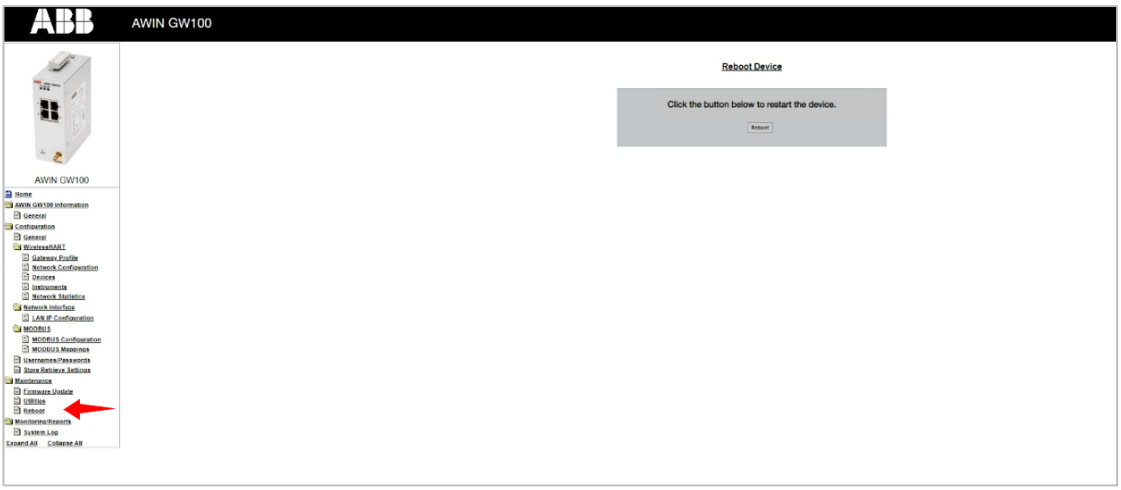


Figure 25: Maintenance- Reboot Screen

This allows a WirelessHART gateway to be rebooted without having to physically access the gateway.

6.16 System Logs

Click **Monitoring/Reports** > **System Log** in the left navigation column to access the system log screen. This screen allows viewing of the “System Log”.

Figure 26: Home screen with monitoring/report options in the left navigation column

The system log may be requested to assist personnel during device troubleshooting. This page may take a few seconds to load or alternatively click the "update" button.

7 Monitoring

The AWIN GW100 rev.2 gateway provides a user account for users which are interested in only reading data from the gateway.

To view these pages login to the gateway using the following credentials:

- **Username**: monitor
- **Password**: monitor

If the username or password was changed then insert those credentials on login screen.

7.1 View Gateway Status

After login, the home page shows the following basic information about the AWIN GW100 rev.2 gateway. It also shows a traffic light, with current gateway status.

- Red light means system error.
- Orange light means configuration download (or settings implementation) in progress.
- Green light means all good.

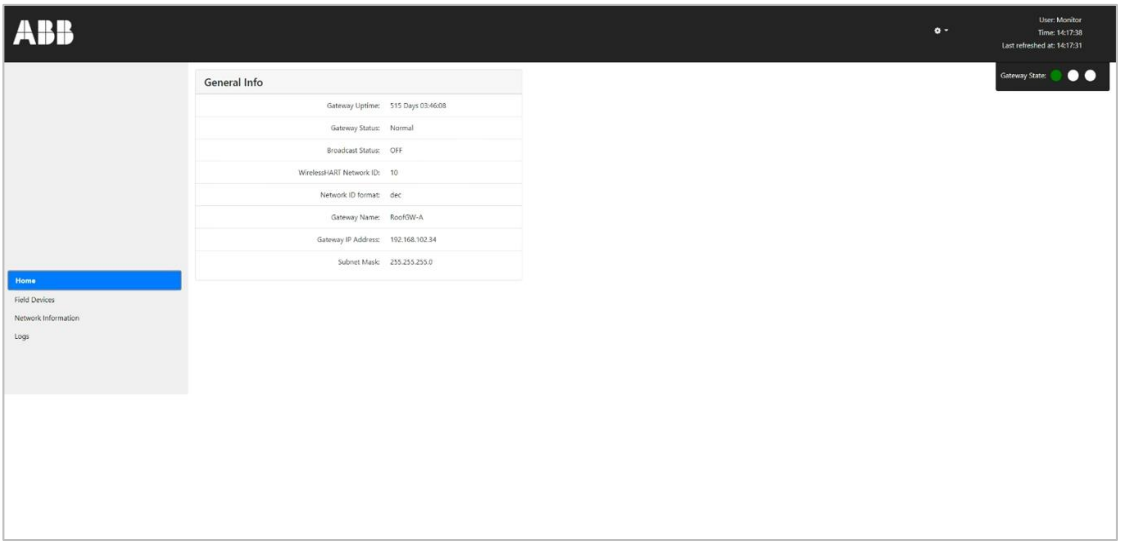


Figure 27: Monitor user Home screen.

7.2 View Devices Data and Status

After login, select **Field Devices** page. It shows devices data and connectivity information. Pages are refreshed automatically.

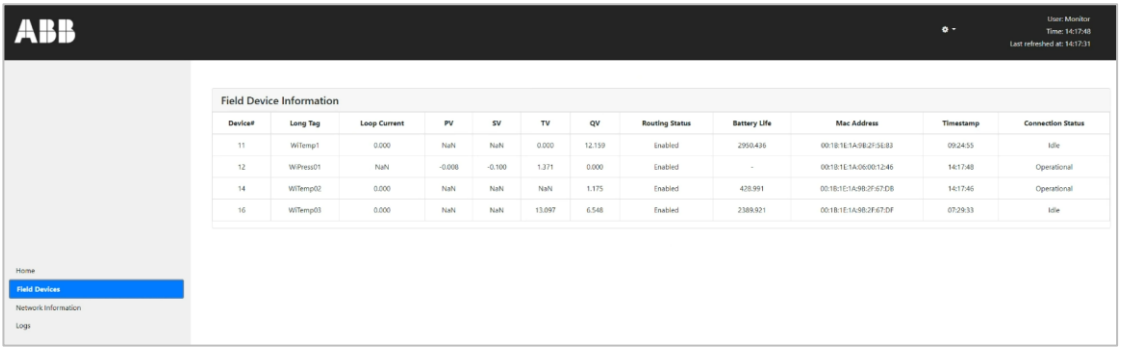


Figure 28: Monitor user Field Devices screen.

7.3 View WirelessHART Network Topology

After login, select **Network Information** page. It shows devices topology information in a table format.

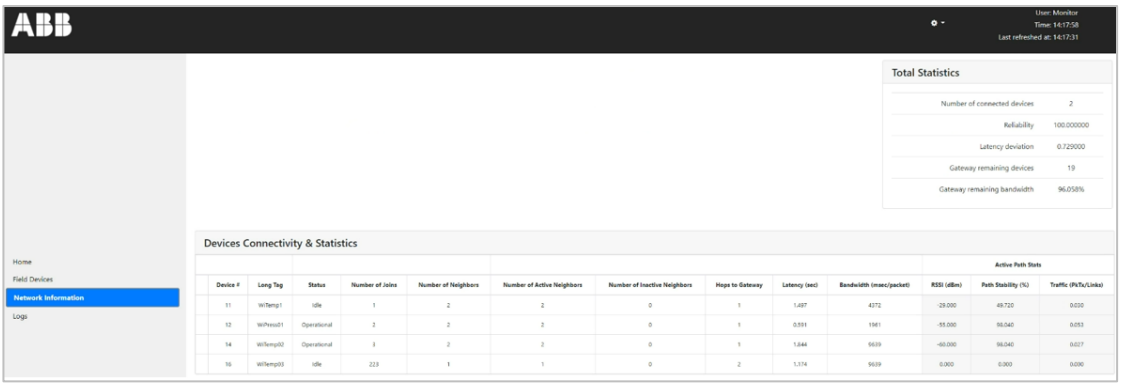


Figure 29: Monitor user Network Information screen.

7.4 Log File, Alarm & Warnings

After login, select Logs page. This page shows two things:

- Complete system logs – records of all system interactions
- Alarms and warnings – records of only major events. It includes device dropout, rejoin, network manager reset and battery warning.

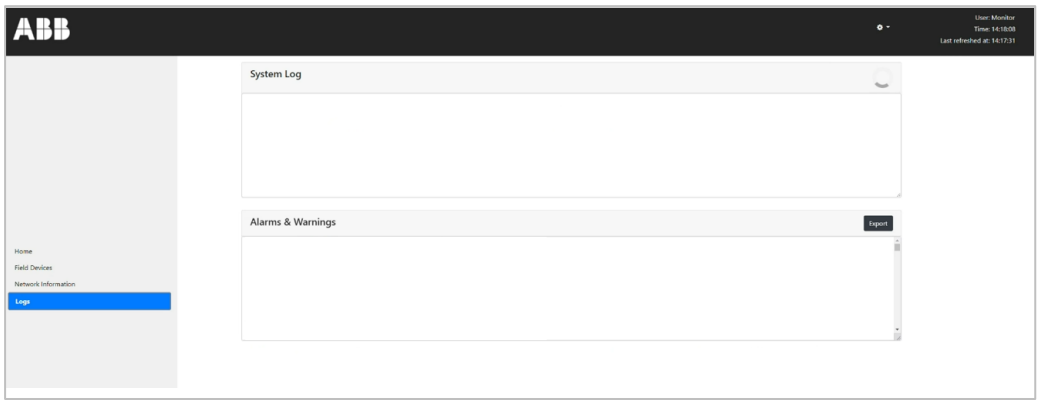


Figure 30: Monitor user Logs screen.

7.5 System Information

After login, select **System** from the top drop-down menu. It shows firmware information.

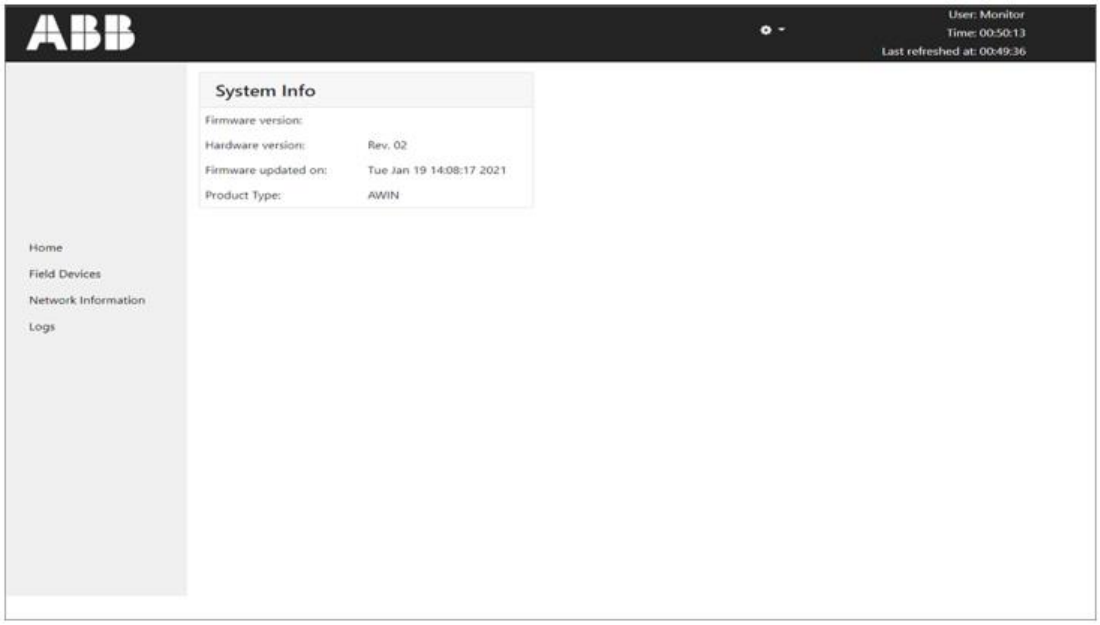


Figure 31: Monitor user -System Information screen

8 Troubleshooting

8.1 LED Indicators

Figure 32 shows the LEDs location on the front of the gateway itself. Unmarked LEDs are explicitly pointed in the figure.

Figure 32: AWIN GW100 rev.2 LED locations

Table 14: Color code

LED name	Description
ST (multi color)	**STATUS** **Flashing (green)** - device initializing **Flashing (red)** - device rebooting or error recovery **ON (green)** - power/device active
MESH (green color)	**DEVICE(S) CONNECTIVITY** **ON** - WirelessHART device(s) connected **OFF** - No WirelessHART devices found/connected
ERR (red)	**ERROR** **OFF** - no errors **ON** - internal error
RED	**OFF** - not in use
PRI	**OFF** - not in use
P1, P2 (green color)	**1000Mbps LAN NETWORK (Top LED)** **ON** – 1000Mbps LAN connected **OFF** – 1000Mbps LAN not connected **10/100Mbps LAN** **NETWORK (Bottom LED)** **ON** – 10/100Mbps LAN connected **OFF** – 10/100Mbps LAN not connected **Flashing (green)** - Transmission/Reception ongoing
S1, S2 (green color)	**OFF** - not in use

8.2 General Troubleshooting

When troubleshooting a WirelessHART network, the first step is to check the power and antenna connection. Once that has been established, check that the gateway is powered on by looking at ST LED.

Refer Table 15 to identify various problems and possible solutions.

Table 15: Troubleshooting procedures

Problem	Solution
Unable to open Webserver	1. Ensure power is applied to AWIN GW100 rev.2. 2. Ensure cable is connected between PC and AWIN GW100 rev.2. If so, LINK LED is ON. 3. Verify network settings of PC match network settings of AWIN GW100 rev.2. They should be on same subnet. Confirm IP addresses of LAN interface. If IP address is unknown, the AWIN GW100 rev.2 can be hard to reset. This will result in factory default configuration, and all previous configuration will be lost. See Section Basic Features of AWIN GW100 for details. 4. The LAN Link and Duplex selection in the AWIN GW100 rev.2 should match the settings of the connected wired network. Select Auto if in doubt. 5. If the device still retains the error state, then try soft or hard reset.
WirelessHART field devices take a long time to connect to the network or WirelessHART field devices are not communicating to the AWIN GW100 rev.2 gateway	1 Log into the AWIN GW100 rev.2 and verify that Active Advertising is on. By default, Active Advertising is ON for 60 minutes. This feature can be re-activated for adding new devices to the network more quickly. 2 Verify that the field devices are powered up and also verify the correct Network ID and Join Key are programmed into the devices. Make sure to use the proper decimal and hexadecimal representations of the Network ID and Join Key, as they can vary between vendors. 3 Make sure that the devices are within the communication range of the gateway or another WirelessHART device configured in the same network. 4 Make sure that there is no competing WirelessHART gateway with same Network ID and Join Key running in parallel in the target coverage area.
Error LED illuminates after bootup	Log into web manager, if possible, to check the status of the AWIN GW100 rev.2. If it states on Home page: “Error Retrieving AP Mote Data From Network Manager”, then wait for at least two minutes to let the gateway clear the error itself. If it persists afterwards, then reboot the gateway. It can be done through the reboot option in the maintenance menu. If it is not possible then power cycle the gateway.
Error LED illuminates	If the gateway is subjected to excessive ethernet frames (or data/broadcast storm) then it can result in reduced performance and in extreme cases may result in freeze of communication in the gateway. In such event, normal operation can be resumed by removing the cause of the “data/broadcast storm” and physically restarting the device by power cycling.

Problem	Solution
	In exceptional cases where a reboot does not fix the problem then the device must be reset. Either **Set Factory Defaults** (soft reset function) or **Hard Reset** options can be utilized.
Status: “Network Manager Queue Full”	Slow down the scan rate of the host system (the network queue can store 100 messages and can be overloaded if scanning occurs too quickly).
Modbus Exception	Verify Modbus register addresses. Verify WirelessHART field device, adapter or wired HART device supports the command. Trying to read data from unmapped register will result in exception. Trying to read data from a device during handshaking state will result in exception.
Device connects and disconnects	If the device does not have good radio signal, then it can have unstable connection. This can be seen by looking into RSSI, latency, stability and number of joins in network statistics page. If the number of joins keep going up, then add repeater nodes (if possible) to improve network reliability, stability and availability. RSSI of the device’s active link should be better than -75dBm.
Unable to connect new device	If it is not possible to add a new device, make sure that there is remaining capacity left in the gateway to add new device. To check, login to the network statistics page. Up to 24 devices can connect to AWIN GW100 rev.2. The gateway itself is counted as one device, bringing total to 25 devices. Connected devices number can be reduced to 8 if all devices burst 3 messages simultaneously at 1sec update period.
I/O Schedule Upload Failed	When downloading the devices configuration to a gateway where some devices are offline will result in this error. This error is followed with a summary of device(s) which failed. For all other devices, configuration upload is successful. Try to bring the offline device online and import again.
Low battery lifetime	If a device shows low battery lifetime then replace its battery by following the service manual of that device.
Radio signal is weak	Make sure there is clearance around the antenna. Look into the guidelines for installation of antenna in the antenna used in the setup.
Weak mesh network	Login to the network statistics page and verify that each device can communicate to at least 3 neighbors (recommended). If so, the device row will be color coded green. If not, make sure that all connected devices are operating as mesh nodes (i.e., routing enabled). You can verify this by logging into the monitor account and looking at **Devices Information** page. To enable/disable routing status the user can use Devices Configuration import file.
Port is closed or device is unresponsive.	Check that the limits are not reached: – Maximum 4 Modbus clients can connect simultaneously. If the limit is not reached, then wait for up to 5 minutes for the service to restart, port to open. If the gateway remains in closed state and does not recover itself within few minutes, then simply reset the device by power cycling. If the device still retains the error state, then try soft or hard reset.

Problem	Solution
Device is stuck in handshaking state	Reboot the device stuck in handshaking state. If not possible, then reform network or power cycle the gateway. **Note**: Power cycling the gateway or reforming the network will force all devices to drop off the network and reconnect. This will impact network availability.
Error Retrieving AP Mote Data From Network Manager	Wait for System Recovery to automatically initiate system recovery. It is often seen during the boot up process. If this error is persistent after 10+ minutes of boot up then a power cycle may be required.
Network Manager Has Reset.	Wait for System Recovery to automatically initiate system recovery. It is often seen during the boot up process or during network configuration. If this error is persistent after 10+ minutes of boot up then a power cycle may be required.

8.3 Modbus Exception Codes

The following exception codes are supported.

Table 16: Exception codes

Exception code	Meaning
0x01 ILLEGAL_FUNCTION	No request bytes present.
0x02 ILLEGAL_DATA_ADDRESS	Starting address does not exist in mapping.
0x03 ILLEGAL_DATA_VALUE	Starting register valid, but length of requests spans at least one unmapped register.
	WirelessHART device is disconnected in simplified in mapping.
0x06 SLAVE DEVICE BUSY	Slave is engaged in processing another command. Retry later. This can happen when: – The data is stale. This can be either because the data is old, or because the device is responding with a non-successful response code. – There is an update to the Modbus mapping in progress.
0x0b GATEWAY TARGET DEVICE FAILED TO RESPOND	Indicates that no response was obtained from the target device. This can happen when: – Device is disconnected. – Sending request to WirelessHART network failed.

To avoid Modbus exception notification, read each individual device data independently. In a case of device disconnection, if you try to read data from multiple devices in one block read, it will result in complete Modbus block read error.

9 Good to Know

9.1 How to Create a Gateway Backup?

To create a gateway backup, follow these steps:

1. Log onto the gateway as admin.
2. Browse to **Store and Retrieve** page.
3. Under **Save Device Configuration** to file, add a “passphrase” and click **Save Configuration to File**. Follow the instructions on the screen. This will save the gateway configuration but not the Modbus map.

   Note: Record Passphrase for future use.
4. Browse to **Modbus Configuration** page.
5. Click **Export Mapping** and save the Modbus map file.

   Note: These two files now are part of the backup.

9.2 How to Replace a Gateway by Restoring a Previous Backup?

To replace a gateway, or restore to a previous backup, follow these steps.

1. Log onto the gateway as admin.
2. Browse to **Store and Retrieve** page.
3. Under **Upload Configuration to device**, add the “passphrase” and click “Choose File”. Follow the instructions on the screen. Select the previously saved Configuration file.

   Note: The Passphrase is the same which was used to generate the Configuration file.
4. Browse to Modbus Configuration page.
5. Select **Manual** mode.
6. Click **Browse** and choose the previously saved Modbus map file. After successful import, select **Submit**.
7. Go to **Maintenance** > **Reboot** page and reboot the gateway. After reboot the gateway should be restored to the previous backup.

9.3 How to Replace a Malfunctioned Device?

To replace a device, follow these steps.

6. Create a backup of the Modbus map. Browse to **Modbus Configuration** page and click **Export mapping**.
7. Disconnect the device to be removed.
8. Once disconnected, delete device via right-click functionality in **Devices** webpage.

9. Once deleted, turn on new device to join network. If the device is already configured with same device tag then simply proceed to step 5. Else, you can use either the HART handheld, ABB FIM or AWIN WIrelessHART Gateways Configurator to change tag name. Refer to their user manual for details.
10. Afterwards, go to **Modbus Configuration** page, select **Manual** mode and import the Modbus map saved in Step1.

Note: The device's Long Tag can be changed at any time via the IO Schedule.

9.4 How to Change Device Tag Name?

The long tag of a device can be changed by using HART handheld, ABB FIM and AWIN WirelessHART Gateways Configurator.

Refer to the user manual of these products for detail procedure. For using AWIN Gateways WirelessHART Configurator refer to document number 3BNP102911.

9.5 How to Use Remote Antenna?

In general, for non- hazardous area deployments, a standard 2.4GHz antenna can be used. Refer to the antenna user manual for details.

As an example, see the following illustration for remote antenna connectivity with AWIN GW100 rev.2.

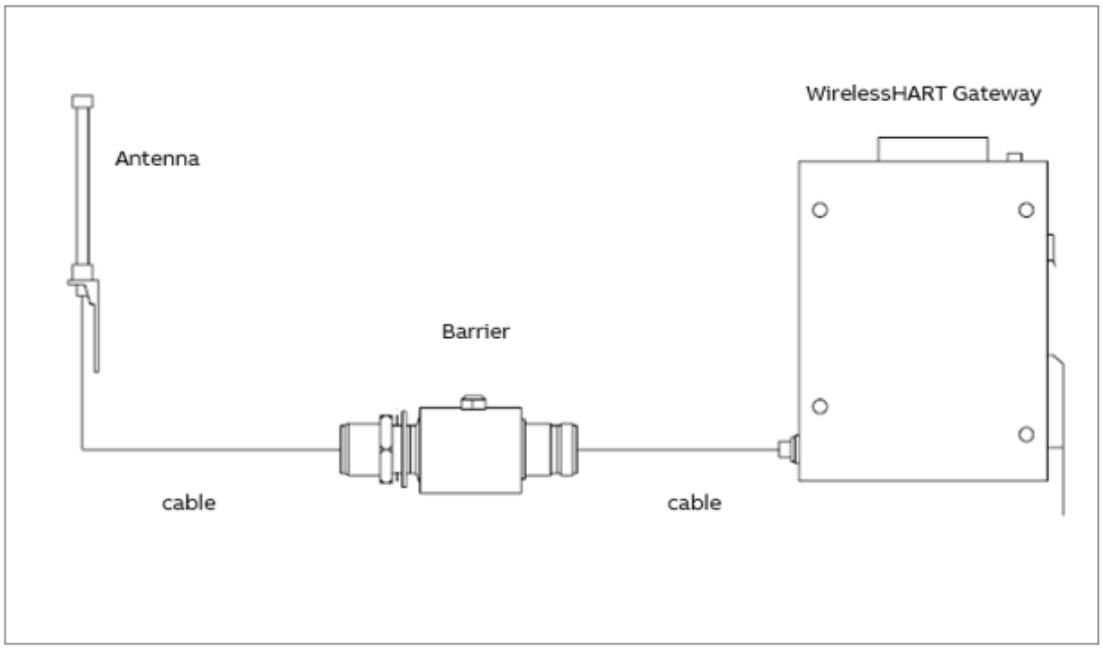


Figure 33: Example of remote antenna assembly

9.6 How is Battery Life Cached in the Gateway?

The battery life of a device reported in the gateway webpage and on Modbus connection is populated as follows:

- Gateway checks for response to Command 778.
- Gateway checks for device variable code 243 (“battery life”) in Command 9.
- Gateway checks for variable units code of 53 (“days”) in Command 3.

If a valid message is received, then battery life is set.

Battery life will be displayed as 65535.000 until battery life value is reported by device in burst message. Initially, it may take some time to populate.
Battery life of 65535.000 is also displayed for loop powered devices.

9.7 What Happens When Multiple Devices Have Same Tag Name?

If same tag name is used by multiple devices in the same WirelessHART network, then they will still join the network but will not operate as desired on Modbus connection. Modbus map is assigned based on Device’s tag name. Therefore, every device should have a unique tag name, else Modbus exception will occur.

9.8 What Value is Displayed on Modbus Registers when a Device Goes Offline?

- When a device goes offline the PVStale, SVStale, TVStale and QVStale reports zero value.
- Communication status register also shows device disconnection. However, this does not happen immediately.
- Trying to read data from Modbus registers of a disconnected device will result in Modbus exception.

9.9 What Value is Displayed on the Gateway Webpage when a Device Goes Offline?

- When a device goes offline the Devices page (in admin account) marks the device as disconnected with a red color row entry.
- When a device goes offline the Devices page (in monitor account) marks the device as idle.
- The last recorded device values are displayed on the webpages.

9.10 How to Check that WirelessHART Network is Operating as Normal?

Gateway's good health status can be verified by two means:

(1) Check via LEDs status on the hardware.

(2) Check traffic light on the gateway's webpage.

Check LEDs

– ST LED is solid green.

– MESH LED is solid green, if WirelessHART devices are connected.

– ERR LED is off.

Check Gateway's Webpage

– Login as 'monitor' user.

– Check traffic LED on the 'Home' page. It should be green color.

9.11 How to Check that you have a Strong WirelessHART Mesh Network?

– Login to the Gateway as **admin** user.

– Select **Network Statistics** page.

– Every device shall have 3 or more neighbors (recommended).

– Active path RSSI shall be better than -75 dBm (recommended).

9.12 What to do if you have Duplicate Tag Names?

Only unique tag names of devices shall be used with the AWIN GW100 rev.2. Refer to section 9.4 for details.

9.13 Reference Architecture - AWIN GW100 rev.2 Connectivity for Gateway Configuration

The user can access the webserver of the gateway by connecting to the gateway using ports P1/P2 on the gateway itself. The user can connect directly to the gateway or via a local network (See Figure 34). The user is automatically logged out of the webserver when the inactivity timer expires.

Login to the webserver is not required during normal operations. It is only needed for setup or troubleshooting.

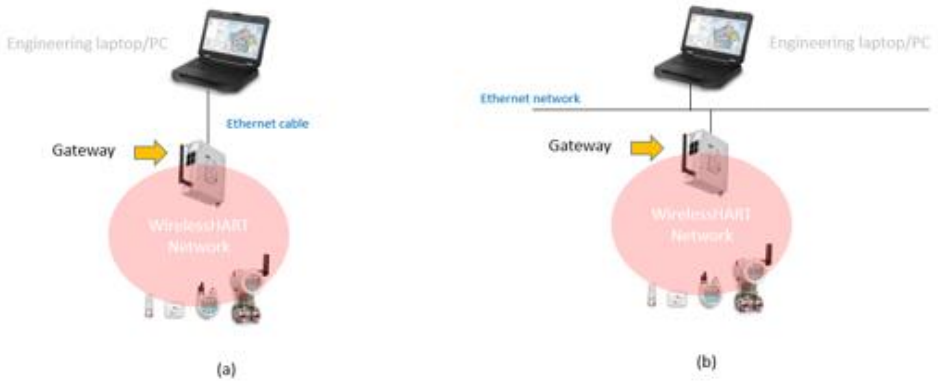


Figure 34: AWIN GW100 rev.2 configuration via (a) direct connection, or (b) network to a PC

9.14 Reference Architecture - AWIN GW100 rev.2 Connectivity with Control System

During normal operations, AWIN GW100 rev.2 will be connected to a Modbus network.

It is used for communicating wireless instruments data to the control systems (such as PLC, DCS). See

Figure 35 for illustration.

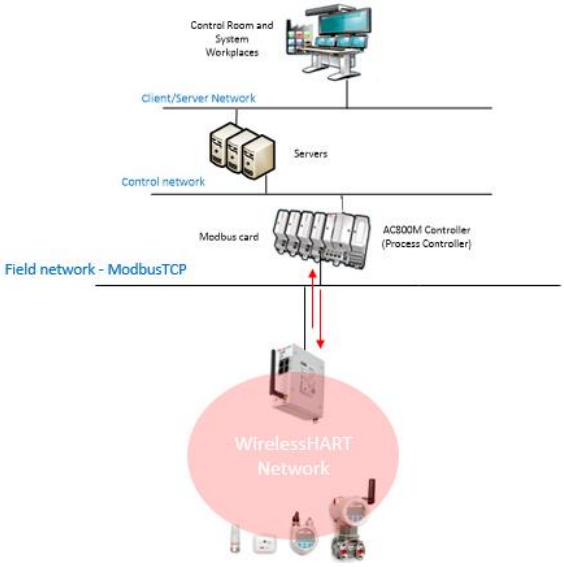


Figure 35: AWIN GW100 rev.2 connectivity to control system (AC800M)

9.15 How to Commission a New Sensor to an Existing Network with Known Network ID and Join Key?

Log onto the gateway as **admin** user. Change the WirelessHART Network ID and Join Key to be the same as is in the sensor which needs to be commissioned. After changing press **Submit all.** If the sensor is in the range of the gateway, it will after a few minutes appear in the **Devices** page. Other devices will have gone offline during this time as the gateway is now operating with different network credentials. Once the new sensor has joined and connected then migrate this new sensor to the other network where the other sensors are residing. To do so, change the Network ID and Join Key in the gateway to that of the previous network and submit **Migrate Network** button. Let this process complete. Afterwards, the previously joined sensors and the newly commissioned sensor will appear in the same network.

Note. If some sensors do not appear, it could be that they have gone into deep sleep mode and may require a trigger to re-join the network. Refer to each sensor's user manual for details.

9.16 How to Dispose this Product – End of Lifecycle?

This product is compliant with European Directive 2012/19/EU, which is concerning waste of electrical and Electronic Equipment. For notes on disposal in Europe visit www.abb.com.

Appendix A. Appendix

Appendix A.1 WirelessHART Field Device Data Available for Modbus Mapping

The following data (see, Table 17) is available from WirelessHART devices in the gateway. This data is available for communication over ModbusTCP link.

Space in holding registers is reserved for device variable codes but are currently not supported.

Table 17: WirelessHART devices data available for Modbus mapping

Parameter	Register Length	Data Type	Description
Loop Current	2	Floating Point	Loop current of a device in the network
PV	2	Floating Point	Primary variable
SV	2	Floating Point	Secondary variable
TV	2	Floating Point	Tertiary variable
QV	2	Floating Point	Quarterly variable
PVStale	1	Unsigned 8-bit Integer	This variable is set to '1', meaning NEW, if the last recorded PV value was received within 3 times the burst period of command 3 set in that device. If the PV value is outdated then the value is set to '0', meaning OLD data.
SVStale	1	Unsigned 8-bit Integer	This variable is set to '1', meaning NEW, if the last recorded SV value was received within 3 times the burst period of command 3 set in that device. If the SV value is outdated then the value is set to '0', meaning OLD data.
TVStale	1	Unsigned 8-bit Integer	This variable is set to '1', meaning NEW, if the last recorded TV value was received within 3 times the burst period of command 3 set in that device. If the TV value is outdated then the value is set to '0', meaning OLD data.
QVStale	1	Unsigned 8-bit Integer	This variable is set to '1', meaning NEW, if the last recorded QV value was received within 3 times the burst period of command 3 set in that device. If the QV value is outdated then the value is set to '0', meaning OLD data.
Device Status	1	Unsigned 8-bit Integer	As specified in HART specification.
Battery Life	2	Floating Point	Remaining days for battery powered devices. For line powered devices it is set to 65535.000 (decimal format).
Extended Device Status	1	Unsigned 8-bit Integer	Taken from Command 48 and is defined in HART specifications' Common Table 17.
Communication Status	1	Unsigned 8-bit Integer	Reported as 1 (device connected) & 0 (not connected)

Parameter	Register Length	Data Type	Description
Number of WirelessHART Neighbors	1	Unsigned 8-bit Integer	Number of neighbors of a device

Appendix A.2 WirelessHART Network Statistics Data Available for Modbus Mapping

The following data (Table 18) is available from WirelessHART gateway itself related to the overall network statistics. This data is available for communication over ModbusTCP link.

Parameter	Register Length	Data Type	Description
Reliability	2	Floating Point	The percentage of data packets generated by motes (or accepted via send API) that the manager received.
Stability	2	Floating Point	The ratio of number of acknowledged packets by the total number of packets transmitted.
Latency	2	Unsigned 32-bit Integer	The average time required for a data packet to travel from the originating mote to the manager.
Packets Lost Upstream	2	Unsigned 32-bit Integer	Total number of lost upstream packets across all devices and sessions.
Time	2	Unsigned 32-bit Integer	Current time of the gateway. Seconds since Epoch according to system's real-time clock.
Data Age	1	Unsigned 16-bit Integer	This value is seconds elapsed since last update of network statistics data. Statistics are averaged over a period of 15 minutes.
Status	1	Unsigned 16-bit Integer	0 – Normal, 2 – WirelessHART queue or stack is full.
WirelessHART device count	1	Unsigned 8-bit Integer	Number of native WirelessHART devices (excluding gateway and wired instruments [i.e. sub devices]).
Total device count	1	Unsigned 8-bit Integer	Number of total devices in the network (excluding gateway but including wired instruments [i.e. sub devices]).
Live device count	1	Unsigned 8-bit Integer	Number of live devices in the network (excluding gateway but including wired instruments [i.e. sub devices]).

Table 18: WirelessHART gateway parameters available for Modbus mapping

Appendix A.3 Automatic Modbus Mapping Structure

Mapping for Field Devices

Table 19: Mapping for Field Devices

Parameter	Device no 1 in list		Device no 2 in list	
	Start Register	End Register	Start Register	End Register
Loop Current	40100	40101	40130	40131
PV	40102	40103	40132	40133
SV	40104	40105	40134	40135
TV	40106	40107	40136	40137
QV	40108	40109	40138	40139
PVStale	40110	-	40140	-
SVStale	40111	-	40141	-
TVStale	40112	-	40142	-
QVStale	40113	-	40143	-
Device Status	40114	-	40144	-
Battery Life	40115	40116	40145	40146
Extended Device Status	40117	-	40147	-
Communication Status	40118	-	40148	-
Number of WirelessHART Neighbors	40119	-	40149	-

Note the following important information:

- For every device, 30 registers are reserved. All new devices joining the network are allocated registers in ascending order.
- Devices are assigned registers in the order they join the WirelessHART network.
- Gateway supports function code 3 and holding registers only.
- Modbus ID (a.k.a Slave ID) of the gateway is fixed to 255.

Mapping for Gateway Parameters' Itself

Table 20: Mapping for Gateway Parameters

Parameter	Start Register	End Register
Reliability	40000	40001
Stability	40002	40003
Latency	40004	40005
Packets Lost Upstream	40006	40007
Time	40008	40009
Data Age	40010	-
Status	40011	-
WirelessHART device count	40012	-
Total device count	40013	-
Live device count	40014	-

Appendix A.4 Modbus Import File Structure

The following XML file structure is used for Field Devices Modbus map:

```
<?xml version="1.0" encoding="UTF-8"?>
<ArrayOfSlaves xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
 <Gateway>
  <Reliability> 40000</Reliability>
  <Stability> 40002</Stability>
  <Latency>40004</Latency>
  <Packets_Lost_Up>40006</Packets_Lost_Up>
  <Time>40008</Time>
  <Data_Age>40010</Data_Age>
  <Status>40011</Status>
  <WiHARTDeviceCnt>40012</WiHARTDeviceCnt>
  <TotalDeviceCnt> 40013</TotalDeviceCnt>
  <LiveDeviceCnt>40014</LiveDeviceCnt>
 </Gateway>
 <Slave>
  <LongTag>Wimon470</LongTag>
  <LoopCurrent>40100</LoopCurrent>
  <PV>40102</PV>
  <SV>40104</SV>
  <TV>40106</TV>
  <QV>40108</QV>
  <PVStale>40110</ PVStale>
  <SVStale>40111</SVStale>
  <TVStale>40112</TVStale>
  <QVStale>40113</QVStale>
  <DevStatus>40114</DevStatus>
  <BattLife>40115</BattLife>
  <DevVariableCodes>40120</DevVariableCodes>
  <ExtDevStatus>40117</ExtDevStatus>
  <CommStatus>40118</CommStatus>
  <NumWiHartNeighbors>40119</NumWiHartNeighbors>
 </Slave>
```

Appendix A.5 Device Configuration File Structure

The following XML file structure is used for Field Devices:

```
<?xml version="1.0" encoding="UTF-8"?>
<IOSchedule>
 <Gateway>
  <LongTag>####</LongTag>
  <Network_ID>####</Network_ID>
  <Network_ID_Format>####</Network_ID_Format>
  <Join_Key>####</Join_Key>
  <IP_Address>####</IP_Address>
  <IP_Address_Assignment>####</IP_Address_Assignment>
  <Subnet_Mask>####</Subnet_Mask>
  <Active_Advertising>####</Active_Advertising>
  <Advertising_Time>####</Advertising_Time>
  <Gateway_Profile>####</Gateway_Profile>
  <Modbus_TCP>####</Modbus_TCP>
 </Gateway>
 <Slave>
  <MAC_Address>####</MAC_Address>
  <Current_Long_Tag>####</Current_Long_Tag>
  <Network_ID_Slave>####</Network_ID_Slave>
  <Network_ID_Format_Slave>####</Network_ID_Format_Slave>
  <Join_Key_Slave>####</Join_Key_Slave>
  <Burst_Period>####</Burst_Period>
  <Routing_Device>####</Routing_Device>
 </Slave>
…
</IOSchedule>
```

MAC address to be added in the format, such as, 00-1B-1E-1A-9A-00-00-91.

Network_ID_Format is either dec or hex.

Gateway profile options are: default, 25 node, legacy, P1 or P2.

Active_Advertising: enable or disable.

IP_Address_Assignment is either manual or DHCP.

Burst period to be provided as 1/32 of a millisecond.

Visit us

abb.com/awin

Document Number: 3BNP102992 Rev. A