Honeywell

OneWireless
Field Device Access Point Gen3 User's Guide

OWDOC-X256-en-322A
November 2020

Release 322.1

Revision	Supported Release	Date	Description
A	322	November 2020	Initial release of the document

Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Contents

1 About this guide

This document describes the procedures to install, configure, and operate the Field Device Access Point (FDAP1/FDAP2) and Field Device Access Point Gen3 (FDAP Gen3). FDAP is one of the components in the OneWireless Network solution for industrial control.

Intended audience

This guide is intended for people who are responsible for planning, administering, and operating the OneWireless Network. These people include Plant Managers, Process Engineers, and System Administrators.

Prerequisite skills

It is assumed that you are familiar with the operation of OneWireless Network, Experion system software, and the plant processes which Experion controls, Microsoft Windows operating systems, and network administration tasks.

How to use this guide

This guide provides guidance on:

- FDAP description
- FDAP installation
- FDAP configuration
- FDAP monitoring
- FDAP maintenance and troubleshooting

Required Honeywell documentation

The following documents and sources contain additional information required for deploying OneWireless Network. It is recommended to have these documents readily available for reference.

Document	Document ID	Description
OneWireless Network Planning and Installation Guide	OWDOC-X253-en-320A	This document provides information about planning, designing, and setting up the OneWireless Network using WDM, FDAPs, and field devices.
OneWireless WDM User's Guide	OWDOC-X254-en-320B	This document describes the procedures to provision, configure, operate, and monitor an ISA100 Wireless field device network using Wireless Device Manager (WDM).

Document	Document ID	Description
OneWireless Wireless LAN Controller Configuration Guide	OWDOC-X255-en-320A	This document provides information about planning, designing, setting up, and configuring a OneWireless Network using WDM, FDAPs, Cisco 1552S APs, and field devices.
FDAP Regulatory Compliance Guide	—	This document describes the FDAP Regulatory Compliance information.
OneWireless Parameter Reference Dictionary	OWDOC-X260-en-320A	This document provides information about the parameters associated with OneWireless devices.

You can download Honeywell documentation from http://www.honeywellprocess.com website.

2 Introduction to FDAP

Related topics

FDAP description
Types of FDAPs
Physical description of FDAP Gen3
Physical description of FDAP1/FDAP2
Features of FDAP
FDAP security
FDAP compliance information

2.1 FDAP description

Note that in this document, a reference to wireless field devices include ISA100 Wireless devices, WirelessHART devices, and Wired HART devices unless otherwise mentioned. Specific device type will be mentioned as and when applicable.

The Field Device Access Point (FDAP) is a ruggedized industrial radio device intended for use in hazardous location to provide wireless connectivity for Wireless compatible field devices. As an industrial meshing access point, FDAP provides secure and reliable wireless coverage for wireless field devices. It also serves as a routing access point for wireless field devices and is located between the wired DCS network and wireless-based wireless field devices. Once deployed in the field, FDAPs self-discover and self-organize into a managed, secure, and redundant wireless field device mesh network. With FDAPs, wireless field devices do not have to route data from other field devices. The following figure illustrates how FDAPs are used in a OneWireless Network:

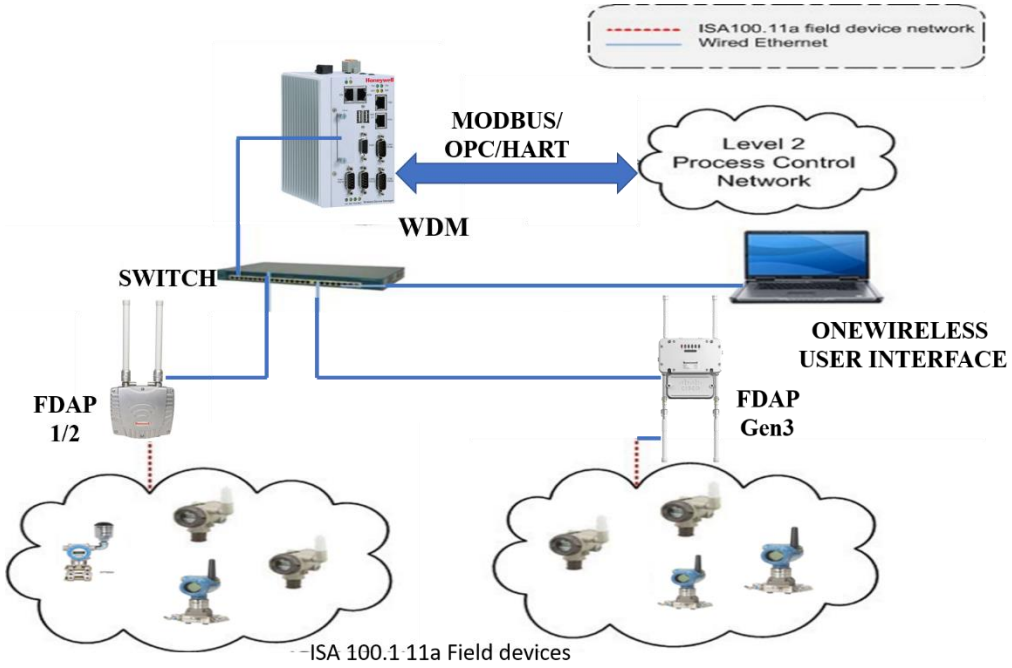


Figure 1: One-Wireless Network

FDAP uses IEEE 802.15.4 standard based radio technology and combines spatial diversity with advanced error correction schemes to communicate in a complex multi-path environment and in large communication areas. It has an Ethernet interface for connection to the backbone network and a wireless compliant radio to connect to the wireless field device network. It is a standalone, pole mountable, intrinsically safe device, suitable for use in hazardous locations. It is normally installed in the same area where industrial field devices are installed. FDAP supports 10/100 Mbps Fast Ethernet and has spatial antenna diversity.

Table 1: FDAP models

Model numbers	Hazloc Comlinace	Model numbers	Power options FDAP	POE Device Powered Through
OW-FDAP31	FDAP Gen3 certified for Class I Div1, Zone 0/1	OW-FDAP31	DC = 12 -30VDC & POE	NA
OW-FDAP32	FDAP Gen3 certified for Class I Div2, Zone 2	OW-FDAP32	DC = 12 -30VDC & POE	NA
FDAP3P	FDAP Gen3 certified for Class I Div2/Zone2	FDAP3P	POE	AC/DC

2.2 Types of FDAPs

FDAP as backbone router

FDAP has a radio board and an autonomous power subsystem that operates within a range of DC input. FDAP supports wireless radio communication, and it does not support Wi-Fi or other radio technologies. The FDAP may be used for Class I Division 2, Zone 2 and general-purpose applications.

NOTE	AC is only supported in FDAP1/ FDAP2 models.

FDAP as field router

A FDAP can be used as a Field Router (FR). If FDAP is not connected to the physical Ethernet, it functions as a line powered FR. FDAP as a line powered FR option can be used for extending field mesh into hazardous environments where normal infrastructure nodes are not suitable. The FDAP may be used as a field router for Class 1 Division 1, Zone 0/1 applications that require IS protection methods and design techniques. This also supports RS485 communication to transmit data from Modbus slaves over Wireless (FEWIO role).

R

2.3 Physical description of FDAP Gen3

FDAP Gen3 enclosure

The FDAP Gen3 has a rugged die-cast aluminum enclosure for outdoor use. The enclosure and all auxiliary components are designed to meet IP66 and IP67 ratings for protection against dust and water ingress. The enclosure has two N-type bulkhead connectors for antenna spatial diversity in the FDAP radios. The two of the half-inch rigid conduit hub has a gasket to seal out water and dust. A rigid conduit hub, internal and external ground studs, and a removable cover are provided for field installation. It has an internal Bluetooth Low Energy (BLE) module and this allows the device to be commissioned in the field. Six status LED's provide information about power, device health, Bluetooth, RS485 and Ethernet communication. The enclosure may be mounted on a pole or on a flat surface such as a wall using the available optional mounting brackets. The enclosure measures approximately 20 cm x 13 cm x 7 cm (L x W x H).

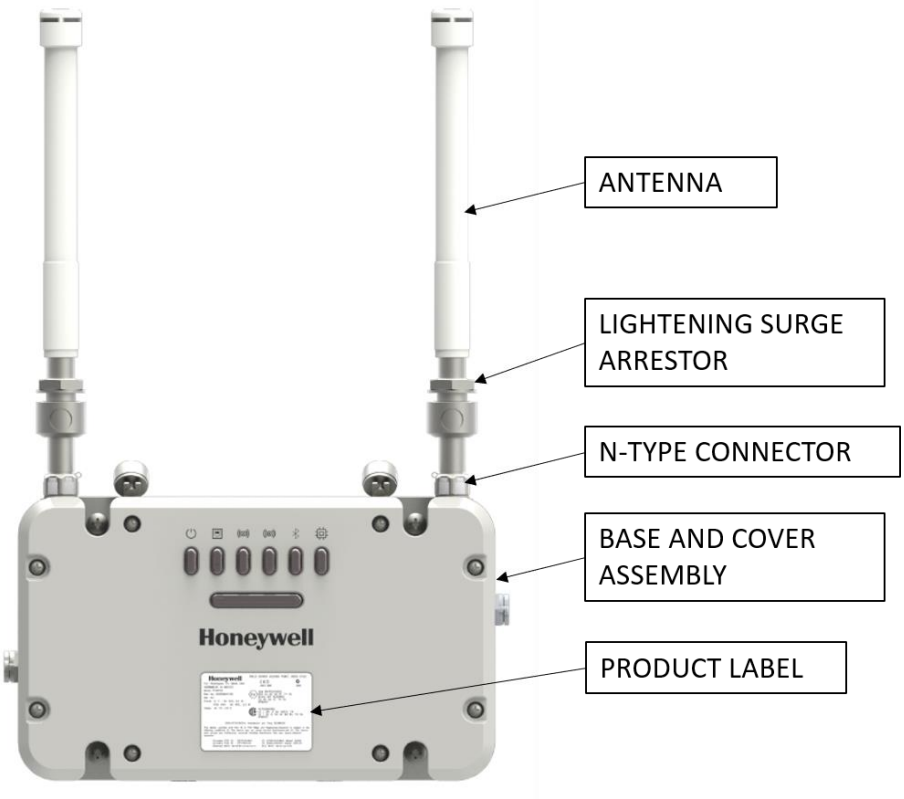


Figure 2.1: FDAP GEN3 WITH LIGHTENING SURGE ARRESTOR

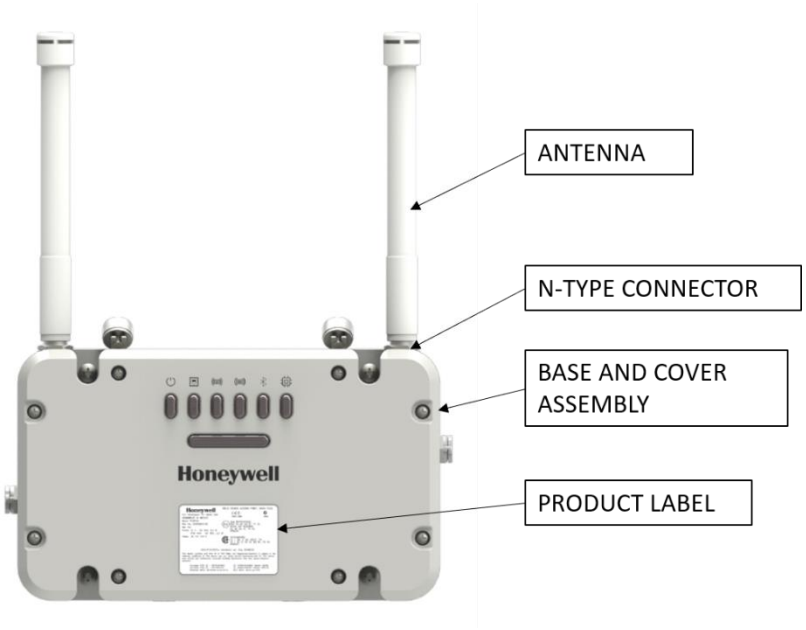


Figure 2.2: FDAP GEN3 WITHOUT LIGHTENING SURGE ARRESTOR

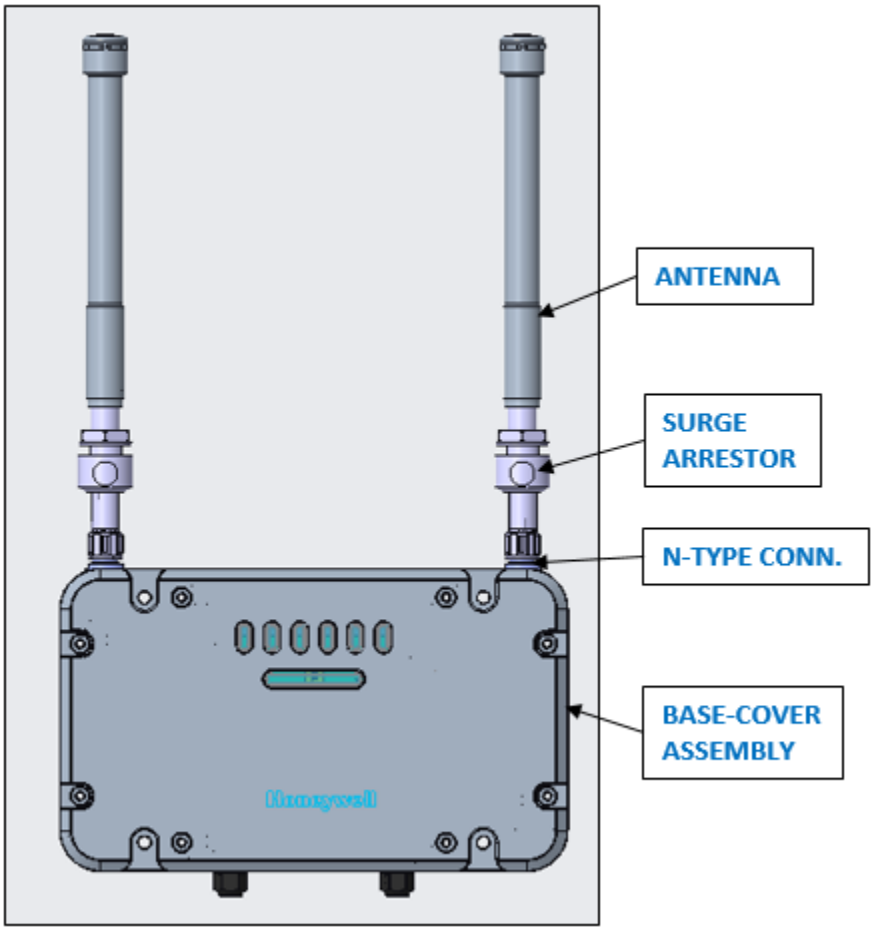
Bluetooth Low Energy (BLE) Module

The FDAP Gen3 has an internal BLE module that is used for communicating with the Provisioning Handheld Android device. The Provisioning Handheld device is used for commissioning the FDAP Gen3, reading, and setting the various FDAP Gen3 parameters. The BLE module has a range of 10 meter radius.

FDAP Gen3 communication radio

FDAP Gen3 has wireless compliant radios that operate in the 2.4 GHz ISM band. It uses spatial antenna diversity with sophisticated error correction schemes to improve communication and increase coverage in a typical industrial complex where multi-path propagation is prevalent.

Antennas



FDAP Gen3 uses dual antenna diversity to improve communication reliability in severe multi-path environment. This helps in improving radio coverage and provides robust communication links thereby reducing infrastructure cost and cost per wireless field device.

FDAP Gen3 has integral omni-directional antennas and it also supports a variety of high- and low-gain omni-directional antennas to provide flexibility in installation and to maximize performance of the wireless system. Refer ***FDAP Gen3 Regulatory Compliance Guide*** for details about certified antennas and the allowable maximum RF output power.

FDAP Gen3 has option to integrate lightning suppressors on the antenna ports. Lighting suppressors are required for all outdoor installations or indoor installations where FDAP Gen3 may be subjected to lightning surge. Optional remote mounted lightning suppressors are available for use in application where the remote antenna cable is exposed to lightning surge.

LED indicators

FDAP Gen3 has three LED's for indicating the status and health of the device. For more information about LED's, refer to "Table 3.1: LED indicators".

2.4 Physical description of FDAP1/FDAP2

FDAP1/FDAP2 enclosure

The FDAP1/FDAP2 has a rugged die-cast aluminum enclosure for outdoor use. The enclosure and all auxiliary components are designed to meet IP66 and NEMA Type 4X (FM only) ratings for protection against dust and water ingress. The enclosure has two water-tight type N bulkhead connectors for antenna spatial diversity in the FDAP1/FDAP2 radios. The half-inch rigid conduit hub has a gasket to seal out water and dust. A rigid conduit hub, internal and external ground studs, and a removable cover are provided for field installation. Externally accessible Infrared (IR) port allows the device to be commissioned in the field. Three status LED's provide information about power, device health, and communication. The enclosure may be mounted on a pole or on a flat surface such as a wall using the available optional mounting brackets. The enclosure measures approximately 20 cm x 13 cm x 7 cm (L x W x H).

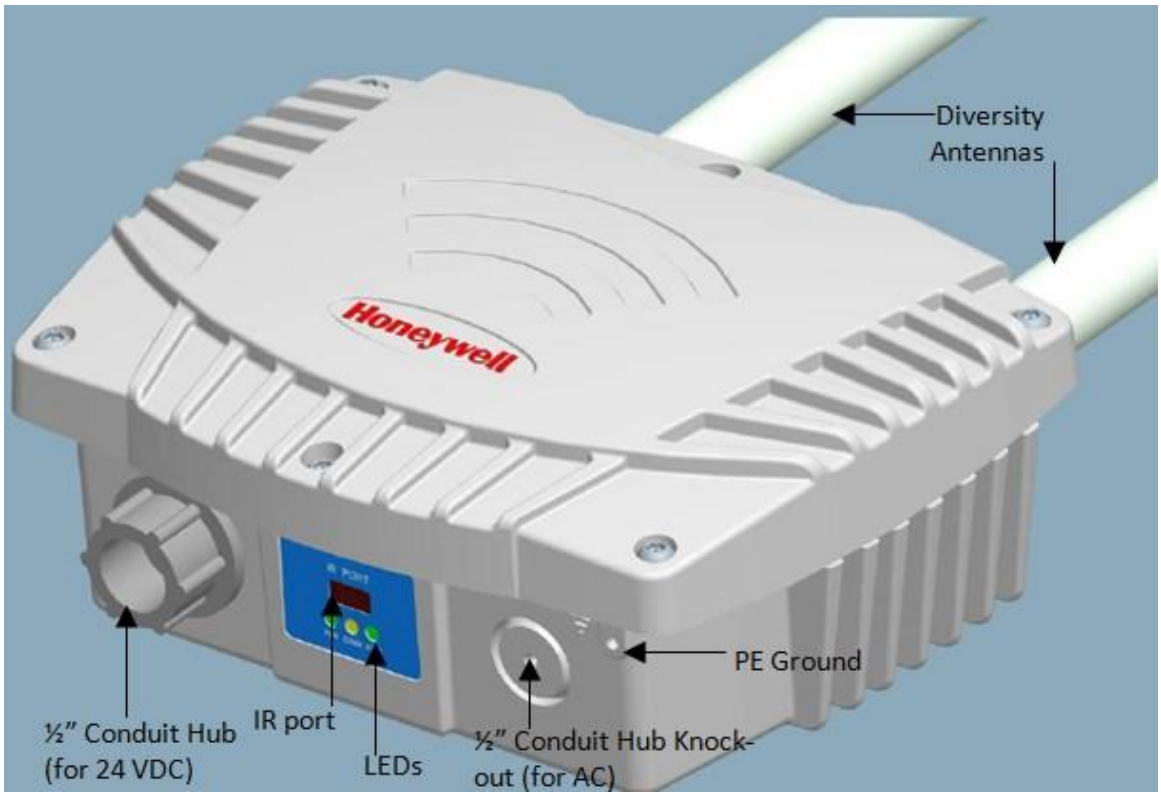


Figure 2: Physical description of FDAP

IR port

The FDAP1/FDAP2 has an externally accessible IR port that is used for communicating with the Provisioning Handheld device. The Provisioning Handheld device is used for commissioning the FDAP1/FDAP2, reading, and setting the various FDAP1/FDAP2 parameters. The IR port has a range of 20 cm and a beam width of 20 degrees.

FDAP1/FDAP2 communication radio

FDAP1/FDAP2 has wireless compliant radios that operate in the 2.4 GHz ISM band. It uses spatial antenna diversity with sophisticated error correction schemes to improve communication and increase coverage in a typical industrial complex where multi-path propagation is prevalent.

Antennas

FDAP1/FDAP2 uses dual antenna diversity to improve communication reliability in severe multi-path environment. This helps in improving radio coverage and provides robust communication links thereby reducing infrastructure cost and cost per wireless field device.

FDAP1/FDAP2 has integral omni-directional antennas and it also supports a variety of high- and low-gain directional and omni-directional antennas to provide flexibility in installation and to maximize performance of the wireless system. Refer ***FDAP1/FDAP2 Regulatory Compliance Guide*** for details about certified antennas and the allowable maximum RF output power,.

FDAP1/FDAP2 has integrated lightning suppressors on the antenna ports. The lightning suppressors are permanently attached and do not require field maintenance. Lighting suppressors are required for all outdoor installations or indoor installations where FDAP1/FDAP2 may be subjected to lightning surge. Optional remote mounted lightning suppressors are available for use in application where the remote antenna cable is exposed to lightning surge.

LED indicators

FDAP1/FDAP2 has three LED's for indicating the status and health of the device. For more information about LED's, refer to "Table 3.2: LED indicators".

2.5 Features of FDAP

The features of FDAP are as follows:

- **DC or Universal AC powered**: FDAP operates at DC or AC and provides better latency than battery-based wireless field device mesh network. It enables the use of wireless field devices for applications requiring fast update rates (less than 10 seconds) and short latency (less than 250 ms) and in areas where Wi-Fi radios are not allowed.

 NOTE	AC is only supported in FDAP1/FDAP2 models.

- **Antenna diversity**: FDAP uses spatial antenna diversity to improve communication success rates and to improve coverage in multi-path environments. This is necessary for the majority of industrial application where there is no direct line of site between field devices. Antenna diversity significantly improves data availability in such applications.
- **Fast Ethernet**: FDAP has 10/100 Mbps Fast Ethernet interface and can be integrated into any network that supports Ethernet communication.
- **Field Mesh network**: Multiple FDAPs can form a self-forming, self-healing wireless mesh network. This extends the range and coverage of the wireless sensor network and provides redundant communication paths for improved data availability. Unlike battery-power field devices, FDAPs are line powered and so can aggregate data from multiple field devices including other FDAPs without concerns about battery life.
- **Reduced cost**: FDAP reduces wireless field device cost, infrastructure cost, and cost per wireless I/O. It reduces the number of wireless routing devices and offers wireless coverage for wireless field devices. It has lesser installation cost than Access Points for sensor only applications.
- **Access points**: FDAP acts as a routing access point for wireless field devices and it is designed for sensor-only network for monitoring application segment.
- **IPv6 device**: FDAP is an Internet Protocol version 4 (IPv4) device. The IPv4 protocol provides an end-to-end data transmission across multiple IP networks. FDAP gets the IP address from DHCP Server in Field Device Network (FDN). You can ping an FDAP from the FDN network. You cannot ping an FDAP from the Plant Control Network (PCN). You cannot ping an FDAP when used as a Router.
- **Backbone router**: FDAP is a backbone router in a rugged industrial enclosure that acts as a bridge between the field device network and wireless backhaul network such as IEEE 802.11 WLAN.

2.6 FDAP security

OneWireless Network protects plant information and ensures safe operations with industry standard 128-bit encryption at the mesh, Wi-Fi, and wireless field device level. The FDAP offers a robust embedded wireless security.

FDAP authentication

FDAP1/ FDAP2 Authentication

In addition to data encryption, Wireless standard requires each FDAP1/ FDAP2 to be authenticated before joining the network. OneWireless Network relies on a more secured IR authentication key distribution method as it requires users to be physically next to the FDAP1/ FDAP2 to add it to the network. The authentication keys are generated and managed by the WDM. A Provisioning Handheld device is used to upload the authentication keys from the WDM to Provisioning Handheld device and to download keys to FDAP1/ FDAP2 using IR media. The IR media is used to send an authentication key from the Provisioning Handheld device to the FDAP1/ FDAP2. Therefore, all Provisioning Handheld devices and FDAP1/ FDAP2 have IR ports for device commissioning. The keys are encrypted when distributed over the network. Once a key is deployed to an FDAP1/ FDAP2, it is validated by the WDM before the FDAP1/ FDAP2 can join the OneWireless Network.

FDAP Gen3 Authentication

In addition to data encryption, Wireless standard requires each FDAP Gen3 to be authenticated before joining the network. OneWireless Network relies on a more secured Bluetooth Low Energy (BLE) Module authentication key distribution method as it requires users to be physically next to the FDAP Gen3 to add it to the network. The BLE module has a range of 10-meter radius. The authentication keys are generated and managed by the WDM. A Provisioning Handheld device is used to upload the authentication keys from the WDM to Provisioning Handheld device and to download keys to FDAP Gen3 using BLE module. The BLE module is used to send an authentication key from the Provisioning Handheld device to the FDAP Gen3. Therefore, all Provisioning Handheld devices and FDAP Gen3 have BLE modules for device commissioning. The keys are encrypted when distributed over the network. Once a key is deployed to an FDAP Gen3, it is validated by the WDM before the FDAP Gen3 can join the OneWireless Network.

Key deployment is a one-time activity, that is, the devices can rejoin the network after power down or after any other service interruptions without re-keying the device. OneWireless supports a key rotation mechanism to enable a secure network. Once the devices join the network, a master key and a session key is assigned to each device, and the session key can be rotated on a periodic basis. The key rotation period can be configured from the OneWireless user interface. For best system performance, it is recommended to set the key rotation period as infinite.

In addition, from OneWireless R210 release onwards, over the air provisioning is supported for all ISA100 devices. This allows the FDAPs to join the secure OneWireless Network and establish communication with other devices and the WDM.

Embedded Wireless security

To reduce security threats, wireless devices requires all process data to be 128-bit encrypted. The data is encrypted at the source and decrypted at the destination to provide end-to-end security for the process data. The FDAPs self-discover other neighboring wireless routing devices, such as Access Points, and routing wireless field devices, to form a reliable and secure wireless mesh network.
Wireless routing algorithm enables an FDAP to dynamically identify the best route to send data to and from wireless field devices. This algorithm enables the field device mesh network to dynamically re-optimize itself when FDAPs are added to or removed from the network.

2.7 FDAP compliance information

RED (Radio Equipment Directive)
This device complies with EN 302372 of the R&TTE Directive The device does not cause harmful interference and accepts any interference received.
WARNING! Changes or modifications made to this equipment not approved by Honeywell invalidate the compliance to RED.

FCC (Federal Communication Commission) Compliance Statement
FCC information: (**FCC ID: S5751307990)**
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

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

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

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

CAUTION! Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

WARNING! In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 7.9inches (20cm) or more from the body of all persons.

WARNING! Since the product uses standard antenna connector, thus only professional installation is permitted.

Industry Canada (IC) (IC ID: 573W-51307990)

Compliance Statements:

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.

2) This device must accept any interference, including interferencethat may cause undesired operation of the device.

Déclarations de conformité: Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Caution Statements:

• This equipment complies with radio frequency exposure limits set forth by Industry Cananda for an uncontrolled environment.

• This equipment should be installed and operated with a minimum distance of 20 cm between the device and the user or bystanders.

Déclarations de mise en garde:

• Cet équipement est conforme aux limites d'exposition aux radiofréquences defines par Indstrie Canada pourun environment non contrôlé.

• Cet équipement doit être installé et utilisé aven un minimum de 20 cm de distancedispositif et l'utilisateur ou des tiers.

This radio transmitter [573W-51307990] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device

Sl No.	Antenna Part	Manufacturer	Antenna Gain	Power Level Setting (dB)
1	AIR-ANT2450V-N	CISCO	5dBi	20dB
2	AIR-ANT2480V-N	CISCO	8dBi	17dB
3	OD24M-5	Laird Technologies	5dBi	20dB
4	HGV-2409U	L-COM	8dBi	17dB

Le présent émetteur radio [IC: 573W-51307990] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés cidessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont trictement interdits pour l'exploitationde l'émetteur

3 FDAP Installation

Related topics

Prerequisites for installation
Inspect FDAP and associated hardware
Identify FDAP site locations
Connect antennas for FDAP Gen3
Connect antennas for FDAP1/FDAP2
Recommendations for remote antenna connections
Ground the FDAP Gen3
Ground the FDAP1/FDAP2
Mount the FDAP Gen3
Mount the FDAP1/FDAP2
Connect power cables and Ethernet cables for FDAP Gen3
Power on and startup for FDAP Gen3
Power on and startup for FDAP1/FDAP2

3.1 Prerequisites for installation

Complete the network planning before installing FDAP. For information about network planning, refer to the *Network Planning and Installation Guide*. Complete the following tasks before installing the FDAP in the wireless network.

- **Network site planning**: Complete site planning to understand how a wireless network can be built and supported for your application using OneWireless components.
- **RF site assessment**: Perform an RF site assessment when designing a large wireless network. The site assessment should at a minimum include the following tasks:
  - Conduct the site assessment when the plant is operating, so that maximum possible interference can be measured and addressed.
  - Conduct RF spectrum analysis on the 2.40-2.49 GHz band to detect any potential RF interference. Strong interference sources should be addressed (removed, avoided or minimized) before the installation. Note that some frequencies may not be available for use in some locations and countries.
  - Arrange point-to-point mesh in various locations to measure the RF propagation ability in the site. Received Signal Strength Indicator (RSSI) can serve as an indicator of the RF environment. TCP/IP throughput testing and UDP/IP throughput and packet drop rate testing should be conducted in all selected locations to measure the quality of the signal strength in the site.
- **FDAP placement**: Determine FDAP placement after the completion of the network planning and RF assessment activities.
- **Power requirements**: Identify power requirements for the network. Determine wired cable runs to provide DC power to the FDAP.
- **Ethernet cable runs**: Determine Ethernet cable runs for FDAP and/or any other wired nodes in the network.

WARNING!

- This device must be professionally installed, this should be noted on grantee.
- To maintain compliance, only the antenna types that have been tested shall be used, antenna Part numbers which is listed on page 17.
- This device requires a significant technology engineering expertise towards understanding of the tools and relevant technology, not readily available to average consumer.
- Only a person professionally trained in the technology is competent.
- This device is not directly marketed or sold to general public.

3.2 Inspect FDAP and associated hardware

Ensure that all the hardware that are necessary for completing the installation for each FDAP are available. Examine whether the FDAP and the associated hardware like antennas and mounting brackets are damaged.

3.3 Identify FDAP site locations

The location of all FDAP should be determined to ensure optimum operation in a wireless network. After the completion of network site planning and RF assessment activities, the locations for FDAP are identified. Locations can be mapped so that the site preparation for FDAP can be started. For more information about prerequisites, refer to “Prerequisites for installation”.

3.4 Connect antennas for FDAP Gen3

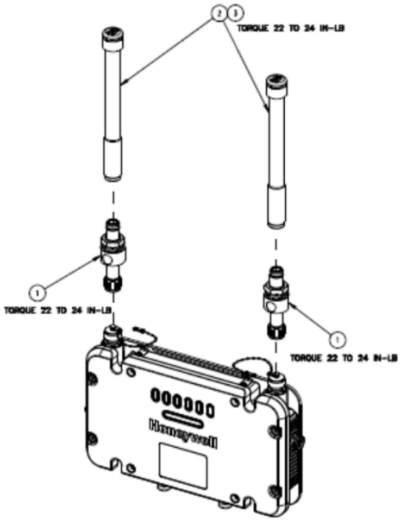
Antennas play a critical role in the setup and operation of wireless mesh systems. Depending upon the results of the site assessment and the requirements of the installed environment, proper antenna type (omni-directional versus directional, low-gain versus high-gains, and so on) should be determined. The various types of antennas offered with FDAP Gen3 enhance the wireless coverage of the field devices in multi-path environment. It is recommended to use same antenna type and gain on both antennas for optimum performance. The following antenna's is certified for the FDAP and devices. The user shall maintain the max set power level as mentioned in the table below.

Table 2: Antenna's Type Supported for the FDAP

Sl No.	Antenna Part	Manufacturer	Antenna Gain	Power Level Setting (dB)
1	AIR-ANT2450V-N	CISCO	5dBi	20dB
2	AIR-ANT2480V-N	CISCO	8dBi	17dB
3	OD24M-5	Laird Technologies	5dBi	20dB
4	HGV-2409U	L-COM	8dBi	17dB

Attention

After the antennas are connected, the connections should be sealed to protect them from the external environment. In environments where conductive deposits can accumulate on antenna such deposits must be removed to maintain optimum RF characteristics. The conduit openings at the bottom of the FDAP Gen3 must be sealed.



507	506	505	504	503	502	501	FIND NO.	PART NUMBER	DESCRIPTION
ASSEMBLY PART NUMBER									
REQUIRED QUANTITY (EMPTY CELLS DENOTES QTY ZERO)									
X	KIT, COAX CABLE ASSEMBLY, 10 METER								
	X	KIT, COAX CABLE ASSEMBLY, 3 METER							
		X	KIT, REMOTE OMNI ANTENNA						
			X	KIT, DUEL BAND OMNI ANTENNA					
				X	KIT, 8 dBi INTEGRAL OMNI ANTENNA				
					X	KIT, 5 dBi INTEGRAL OMNI ANTENNA			
						X	KIT, LIGHTNING SURGE ARRESTOR		
1							7	50018278-010	COAX CABLE ASSEMBLY, 10 m (32 ft)
	1						6	50018278-003	COAX CABLE ASSEMBLY, 3 m (9.8 ft)
		1					5	50018414-001	8 dBi REMOTE OMNI DIRECTIONAL ANTENNA
			1				4	50169041-001	4dBi/7dBi DUEL BAND OMNI ANTENNA
				1			3	50161093-001	8 dBi INTEGRAL OMNI ANTENNA
					1		2	50161092-001	5 dBi INTEGRAL OMNI ANTENNA
						1	1	50155902-001	LIGHTNING SURGE ARRESTOR

Figure 3: Antenna components

CAUTION

Take precautions against electrostatic discharge when handling antenna.

3.5 Connect antennas for FDAP1/FDAP2

Antennas play a critical role in the setup and operation of wireless mesh systems. Depending upon the results of the site assessment and the requirements of the installed environment, proper antenna type (omni-directional versus directional, low-gain versus high-gains, and so on) should be determined. The various types of antennas offered with FDAP1/FDAP2 enhance the wireless coverage of the field devices in multi-path environment. It is recommended to use same antenna type and gain on both antennas for optimum performance.

Attention

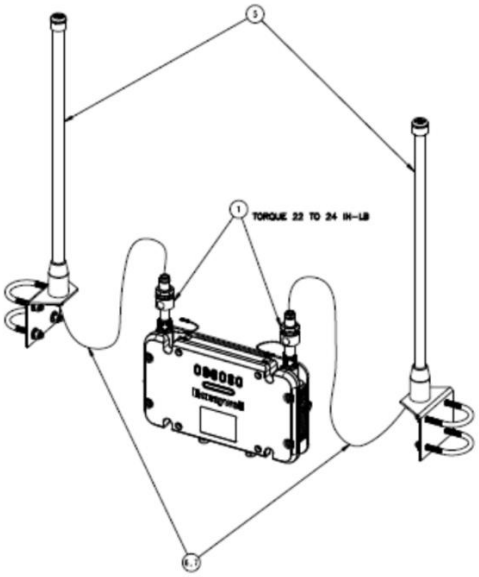
After the antennas are connected, the connections should be sealed to protect them from the external environment. In environments where conductive deposits can accumulate on antenna such deposits must be removed to maintain optimum RF characteristics. The conduit openings at the bottom of the FDAP1/FDAP2 must be sealed.

Figure 3: Antenna components

CAUTION

Take precautions against electrostatic discharge when handling antenna.

3.6 Recommendations for remote antenna connections.



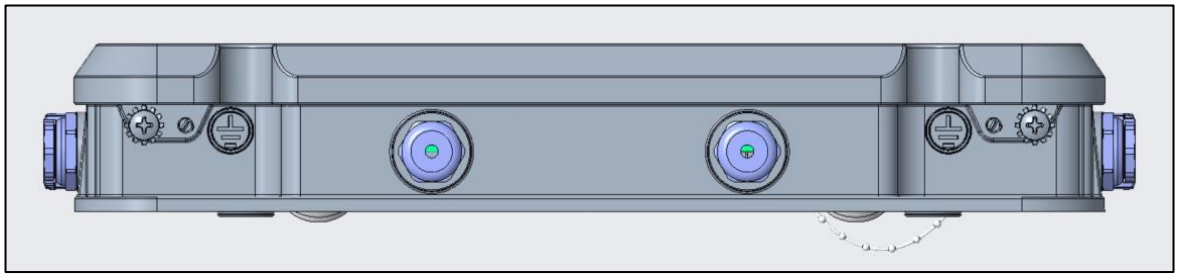
X							KIT, COAX CABLE ASSEMBLY, 10 METER		
	X						KIT, COAX CABLE ASSEMBLY, 3 METER		
		X					KIT, REMOTE OMNI ANTENNA		
			X				KIT, DUEL BAND OMNI ANTENNA		
				X			KIT, 8 dBi INTEGRAL OMNI ANTENNA		
					X		KIT, 5 dBi INTEGRAL OMNI ANTENNA		
						X	KIT, LIGHTNING SURGE ARRESTOR		
1							7	50018278-010	COAX CABLE ASSEMBLY, 10 m (32 ft)
	1						6	50018278-003	COAX CABLE ASSEMBLY, 3 m (9.8 ft)
		1					5	50018414-001	8 dBi REMOTE OMNI DIRECTIONAL ANTENNA
			1				4	50169041-001	4dBi/7dBi DUEL BAND OMNI ANTENNA
				1			3	50161093-001	8 dBi INTEGRAL OMNI ANTENNA
					1		2	50161092-001	5 dBi INTEGRAL OMNI ANTENNA
						1	1	50155902-001	LIGHTNING SURGE ARRESTOR
507	506	505	504	503	502	501			
ASSEMBLY PART NUMBER REQUIRED QUANTITY (EMPTY CELLS DENOTES QTY ZERO)							FIND NO.	PART NUMBER	DESCRIPTION

3.7 Ground the FDAP Gen3

The FDAP Gen3 provides internal and external grounding point to meet various local and regulatory grounding requirements. You should ensure that the FDAP Gen3 are grounded properly by a certified and authorized personnel, and that it conforms to all applicable codes and regulations. The materials required to provide a proper ground are defined by local regulations and should be obtained locally to ensure that the correct safety environment is achieved.

Attention

1. The recommended AWG of the ground cable from FDAP Gen3 ground to the ground pit should be at least 12 or better.
2. Ground Pit should be maintained as per the NEC recommendation. The ground resistance should be less than 5 ohms so that it provides safety to FDAP Gen3 under environmental transients such as lightning, sandstorm, etc.



3.8 Ground the FDAP1/FDAP2

The FDAP1/FDAP2 provides internal and external grounding point to meet various local and regulatory grounding requirements. You should ensure that the FDAP1/FDAP2 are grounded properly by a certified and authorized personnel, and that it conforms to all applicable codes and regulations. The materials required to provide a proper ground are defined by local regulations and should be obtained locally to ensure that the correct safety environment is achieved.

Attention

1. The recommended AWG of the ground cable from FDAP1/FDAP2 ground to the ground pit should be at least 12 or better.
2. Ground Pit should be maintained as per the NEC recommendation. The ground resistance should be less than 5 ohms so that it provides safety to FDAP1/FDAP2 under environmental transients such as lightning, sandstorm, etc.

Ensure all your grounding connections terminate here

3.9 Mount the FDAP Gen3

The assembled FDAP Gen3, along with antennas and lightning suppressors (if required) can be mounted in its site location. The FDAP Gen3 enclosure can be mounted on a 2-inch pole or on a wall using the appropriate optional mounting kit that is available with the unit.

3.9.1 Pole mounting

When pole mounting the FDAP Gen3, you can assemble and install the mounting hardware at the site. The mounting kit includes the following items:

(1) Mounting plate

(2) U-bolts with nuts

(3) Screws (to attach the FDAP Gen3 to the mounting plate)

(4) Washers (Split lock washer, Flat lock washer, Lock washer)

The pole mounting kit comprises of mounting plate, U-bolts with nuts, screws and washers as displayed in "Figure 5: Pole mounting". When using the mounting plate for the pole installation, secure the FDAP Gen3 to the bracket using the screws supplied with the bracket kit. The FDAP Gen3 can be mounted to the left or to the right of the pole using the same mounting hardware. It can also be mounted in line with the pole. However, if the integral antennas are too close to the pole, it might cause RF communication problem. For inline mounting, the FDAP Gen3 integral antennas should be on the top of the mounting pole.

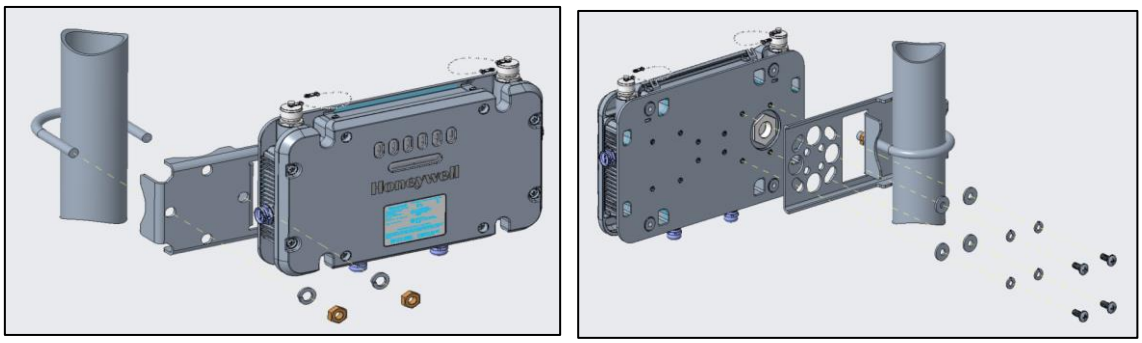
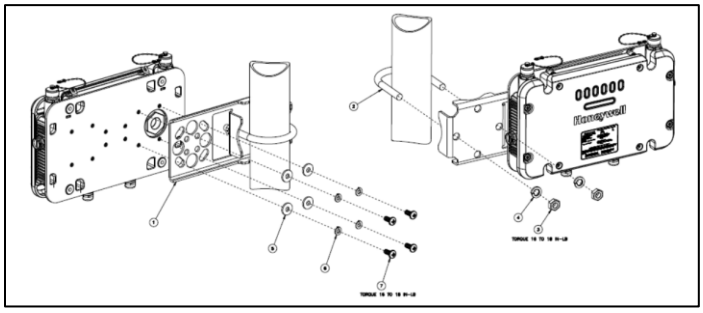


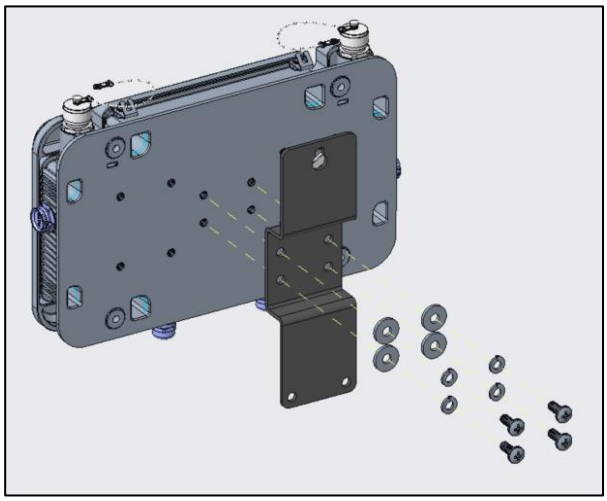
Figure 5: Pole mounting

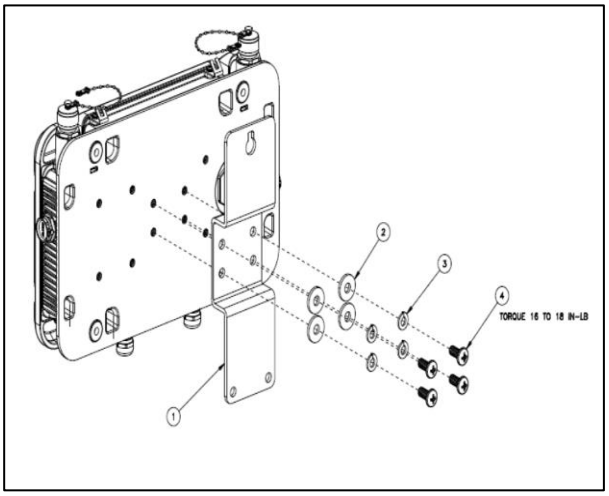


4	7	50155913-001	SCREW, 1/4-20 X 5/8, 316SS
4	6	50155915-001	SPLIT LOCK WASHER, 1/4, 316SS
4	5	50155916-001	FLAT LOCK WASHER,1/4, 316SS
2	4	30757526-109	LOCK WASHER, M10, 316SS
2	3	30753080-209	HEX NUT, M10, 316SS
1	2	30753066-201	"U" BOLT M10, 316SS
1	1	51305149-003	FLAT STYLE MOUNTING BRACKET 316SS
-501	FIND NO	PART NUMBER	DESCRIPTION
QUANTITY REQUIRED			
ASSEMBLY PART NUMBERS			

3.9.2 Wall or flat surface mounting

The wall mounting kit comprises a wall mounting plate and four screws as displayed in “Figure 6: Wall mounting”. Both mounting plates fasten to four threaded bosses on the back of the FDAP Gen3. The FDAP Gen3 should not be mounted on metallic walls because the integral antennas are too close to the wall and causes RF propagation problems.





4	4	50155913-001	SCREW, 1/4-20 X 5/8 L, 316SS
4	3	50155915-001	SPLIT LOCK WASHER, 1/4, 316SS
4	2	50155916-001	FLAT LOCK WASHER,1/4, 316SS
1	1	51202381-300	WALL MOUNTING BRACKET, 316SS
-502	FIND NO	PART NUMBER	DESCRIPTION
ASSEMBLY PART NUMBERS			
QUANTITY REQUIRED			

Figure 6: Wall mounting

3.10 Mount the FDAP1/FDAP2

The assembled FDAP1/FDAP2, along with antennas and lightning suppressors (if required) can be mounted in its site location. The FDAP1/FDAP2 enclosure can be mounted on a 2-inch pole or on a wall using the appropriate optional mounting kit that is available with the unit.

3.10.1 Pole mounting

When pole mounting the FDAP1/FDAP2, you can assemble and install the mounting hardware at the site. The mounting kit includes the following items:

(1) Mounting plate

(2) U-bolts with nuts

(3) Screws (to attach the FDAP1/FDAP2 to the mounting plate)

The pole mounting kit comprises of mounting plate, U-bolts, and nuts as displayed in "Figure 5: Pole mounting". When using the mounting plate for the pole installation, secure the FDAP1/FDAP2 to the bracket using the screws supplied with the bracket kit. The FDAP1/FDAP2 can be mounted to the left or to the right of the pole using the same mounting hardware. It can also be mounted in line with the pole. However, if the integral antennas are too close to the pole, it might cause RF communication problem. For inline mounting, the FDAP1/FDAP2 integral antennas should be on the top of the mounting pole.

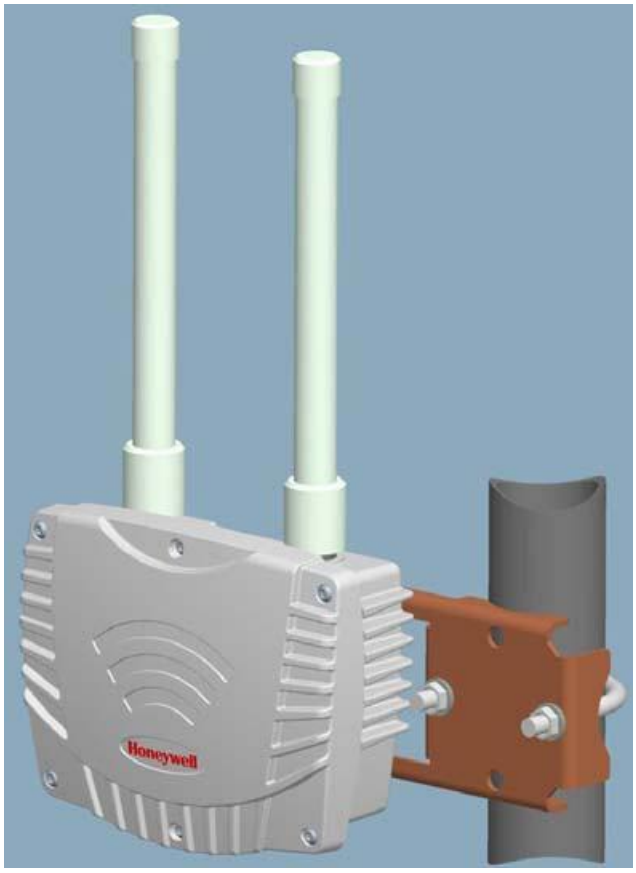


Figure 5: Pole mounting

3.10.2 Wall or flat surface mounting

The wall mounting kit comprises a wall mounting plate and four screws as displayed in “Figure 6: Wall mounting”. Both mounting plates fasten to four threaded bosses on the back of the FDAP1/FDAP2. The FDAP1/FDAP2 should not be mounted on metallic walls because the integral antennas are too close to the wall and causes RF propagation problems.

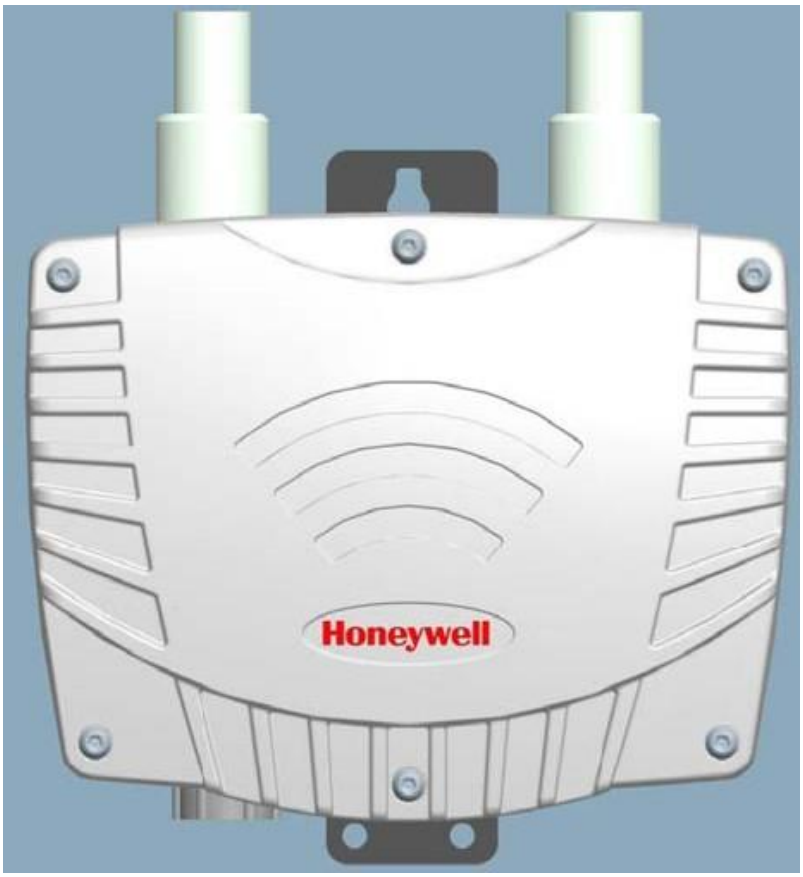


Figure 6: Wall mounting

3.11 Connect power cables and Ethernet cables for FDAP Gen3

FDAP Gen3 has one Ethernet cable and one power cable. Ethernet interconnection is limited to installations outside Class I Division 1, Zone 0/1 locations. You have to construct conduit and cable runs for power and Ethernet. The FDAP Gen3 can be powered directly by external DC power supply such as distributed DC source. Ensure that all wires inside the enclosure are routed and secured properly as displayed in “Figure 7: Ethernet and field DC power”. The FDAP Gen3 has integrated terminal blocks that allow field wiring to be directly terminated inside the FDAP Gen3 without an additional external junction box. DC Power connection, Ethernet and Serial connections can be terminated inside the FDAP Gen3.

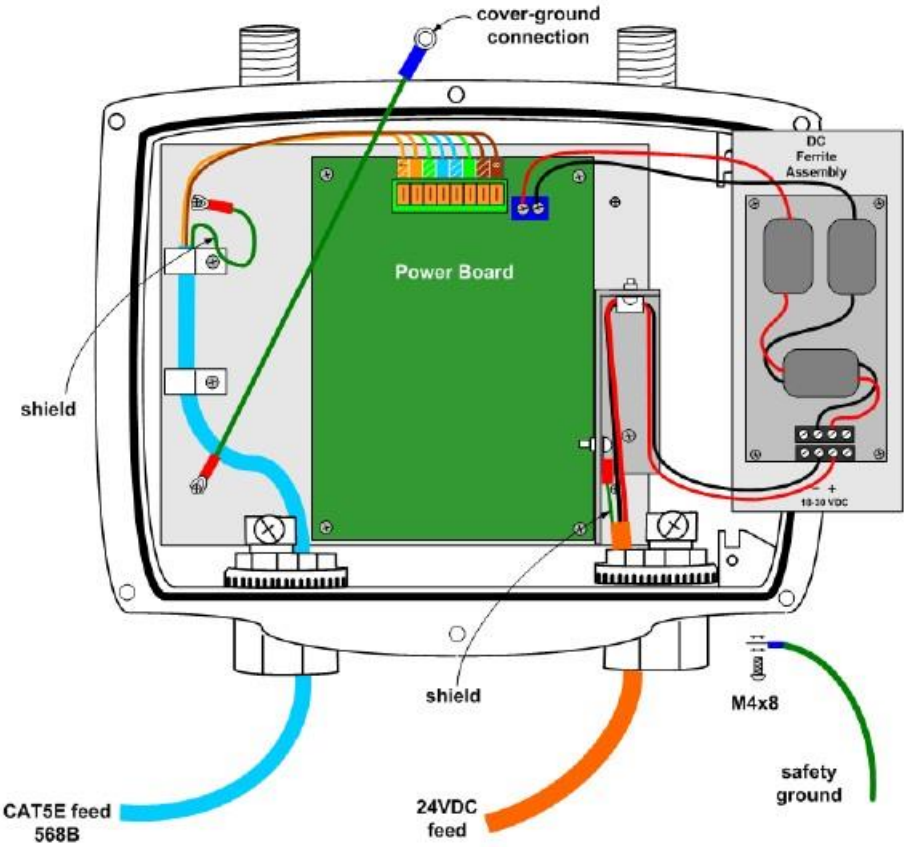
Attention
RS-485 or Ethernet can be used one at a time to meet IP (66/67) requirements.

3.11.1 DC power wiring

When powered from an external DC source, the power cable should be terminated directly onto the terminal block of the DC Ferrite Assembly. Connected wires then pass through the mounted ferrites on the assembly board, which then connects to the two-position terminal block on the Power Board. The polarity of the connector is marked next to the connector on the Power Board. The power cable should be shielded and the drain wire grounded inside the enclosure as displayed in “Figure 7: Ethernet and field DC power”.

Secure all connections and wires and connect the *cover-ground connection* lug to the enclosure cover to complete the wiring.

Figure 7: Ethernet and field DC power



Attention

For installations that require CE-mark compliance, the DC power source must be a CE-mark approved power supply. In addition, the DC cable between the approved DC power source must be no more than 3.0 meters (9.8 feet) from the FDAP Gen3.

3.11.2 Ethernet wiring

FDAP Gen3 has one Ethernet input for optional connection to a wired network or a wireless access point. If the FDAP Gen3 is connected to a wired Ethernet, you should run the Ethernet cabling from the control system through the conduit to the FDAP Gen3 site. You have to install the FDAP Gen3 based on the Ethernet connection. If Ethernet cable is connected, it acts as an FDAP (access point) and if the Ethernet cable connection is removed it acts as a line powered FR (routing device). Ethernet interconnection is limited to installations outside Class I Division 1,
Zone 0/1 locations. An 8 - position Insulation Displacement Connector (IDC) terminal block allows twisted pair Ethernet cable to be connected to the FDAP Gen3 without stripping the wires or crimping on modular RJ-45 plugs. The drain wire from the CAT5E cable shield should be connected to the internal grounding point on the conduit hub. The cable should be solid core to ensure good signal quality and performance of up to 100 m.

Terminating the Ethernet cable

To terminate the Ethernet cable, perform the following steps.

1. Strip the outer jacket of the CAT5e cable and connect the shield drain wire to the internal grounding lug on the conduit hub. Do not strip the individual twisted pair wires.
2. Connect the twisted pair wires to the IDC following the color chart marked next to the IDC. Note that the color chart on the FDAP Gen3 Power and I/O board assumes that the cable conforms to EIA/TIA 568B color code which is the predominant color code for CAT5e cable. Refer to “Table 3: Ethernet IDC block pin-out” for the necessary adjustment if the older EIA/TIA 568B color coded cable is used. Most of the CAT5E cables conform to TIA/EIA 568B.

Table 3: Ethernet IDC block pin-out

PIN #	TIA/EIA 568A	TIA/EIA 568B	Data
1			Transmit+
2			Transmit-
3			Receive+
4			Unused
5			Unused
6			Receive-

PIN #	TIA/EIA 568A	TIA/EIA 568B	Data
7			Unused
8			Unused

Testing Ethernet connection

A standard RJ-45 modular jack is available on the FDAP Gen3 Power and IO board. The RJ-45 jack may be used to test cable integrity after terminating the cable at the IDC connector. After terminating the field cable at the IDC, connect the cable tester to the RJ-45 jack. An end-to-end cable test can then be performed to ensure proper wiring at the IDC connector.

3.12 Connect power cables and Ethernet cables for FDAP1/FDAP2

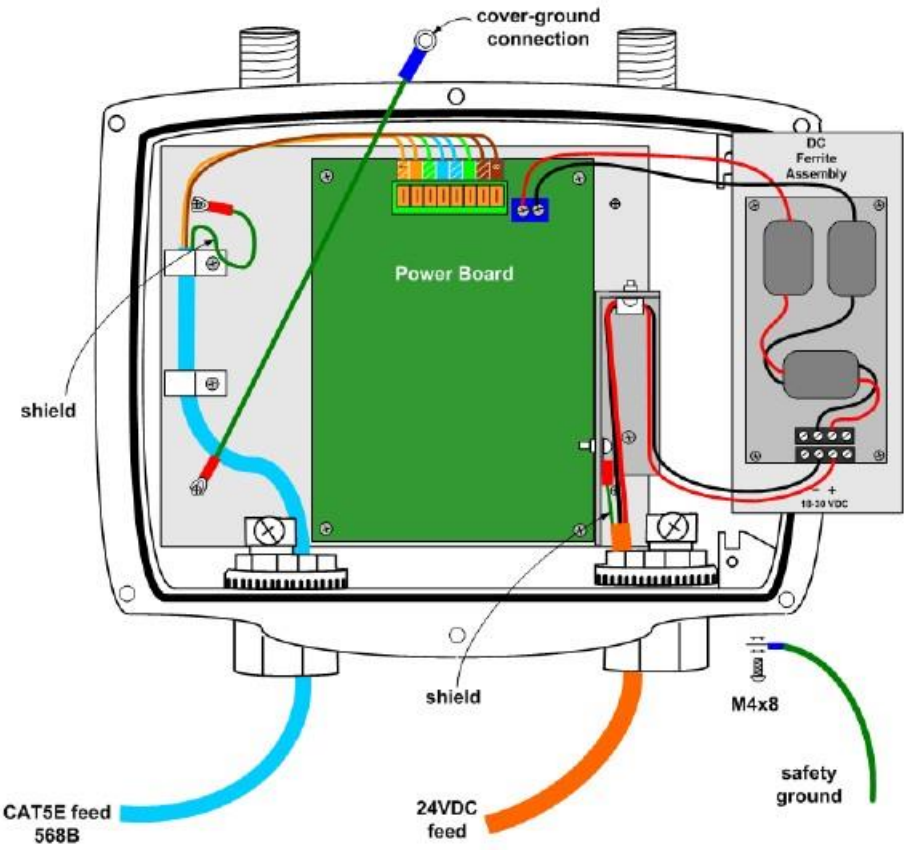
FDAP1/FDAP2 has one Ethernet cable and one power cable. Ethernet interconnection is limited to installations outside Class I Division 1, Zone 0/1 locations. You have to construct conduit and cable runs for power and Ethernet. The FDAP1/FDAP2 can be powered directly by universal AC power supply or by external DC power supply such as distributed DC source. Ensure that all wires inside the enclosure are routed and secured properly as displayed in “Figure 7: Ethernet and field DC power” and “Figure 8: Ethernet and field AC power”. The FDAP1/FDAP2 has integrated terminal blocks that allow field wiring to be directly terminated inside the FDAP1/FDAP2 without an additional external junction box. Power (both AC and DC) connection, Ethernet and Serial connections can be terminated inside the FDAP1/FDAP2.

3.12.1 DC power wiring

When powered from an external DC source, the power cable should be terminated directly onto the terminal block of the DC Ferrite Assembly. Connected wires then pass through the mounted ferrites on the assembly board, which then connects to the two-position terminal block on the Power Board. The polarity of the connector is marked next to the connector on the Power Board. The power cable should be shielded and the drain wire grounded inside the enclosure as displayed in “Figure 7: Ethernet and field DC power”.

Secure all connections and wires and connect the *cover-ground connection* lug to the enclosure cover to complete the wiring.

Figure 7: Ethernet and field DC power



Attention

For installations that require CE-mark compliance, the DC power source must be a CE-mark approved power supply. In addition, the DC cable between the approved DC power source must be no more than 3.0 meters (9.8 feet) from the FDAP1/FDAP2.

3.12.2 AC power wiring

When powered from an external AC source, the power cable should be terminated at the terminal block on the AC/DC conversion module, marked as 24 VDC Power Brick as displayed in “Figure 8: Ethernet and field AC power”.

(1) To facilitate wiring, remove the Power Brick assembly from the enclosure by loosening the two retaining screws and sliding the brick assembly out.

(2) Terminate the AC cables at the AC terminal block on the Power Brick module. The module has polarity markings for Live (L), Neutral (N) and Ground.

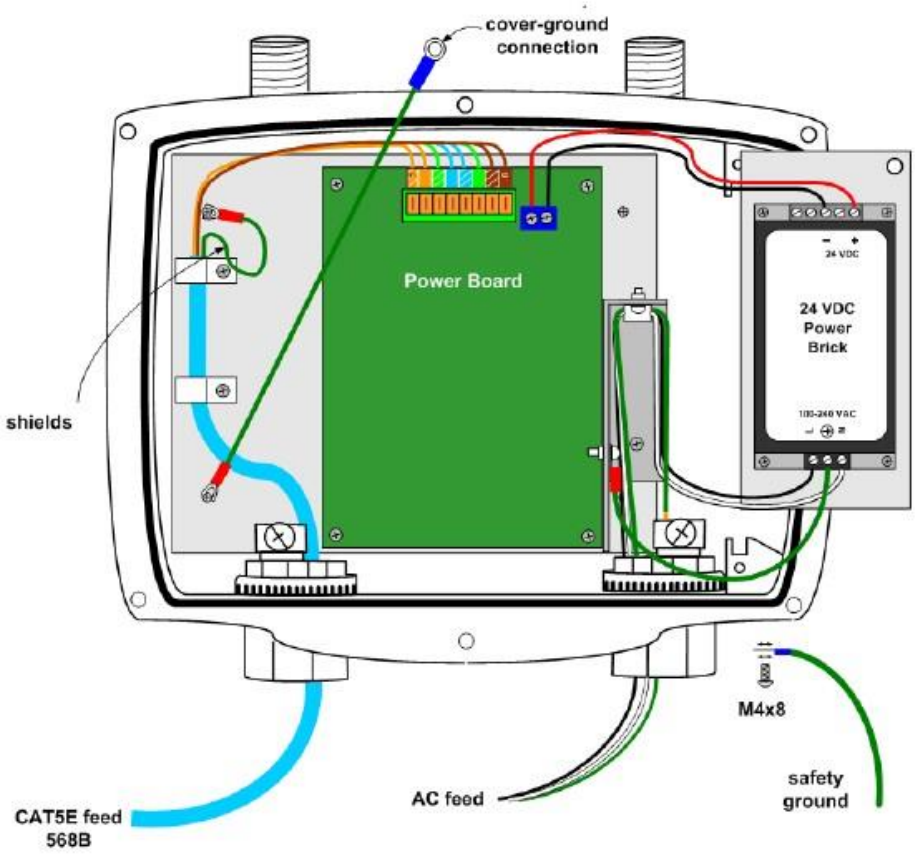
(3) Ensure that all connections are secure and then slide the module back into the enclosure and secure it with the retaining screws.

(4) Secure all connections and wires and connect the *cover-ground connection* lug to the enclosure cover to complete the wiring.

Attention

If an AC power option is ordered from the factory, the DC output of the power conversion module should be pre-wired to the DC terminal block on the Power Board. Verify that the connection is secure and has the correct polarity as marked.

Figure 8: Ethernet and field AC power



Attention

Note that AC wiring only applies to the FDAP2, which is FM approved. AC wiring is not covered under IECEx certification.

3.12.3 Ethernet wiring

FDAP1/FDAP2 has one Ethernet input for optional connection to a wired network or a wireless access point. If the FDAP1/FDAP2 is connected to a wired Ethernet, you should run the Ethernet cabling from the control system through the conduit to the FDAP1/FDAP2 site. You have to install the FDAP1/FDAP2 based on the Ethernet connection. If Ethernet cable is connected, it acts as an FDAP1/FDAP2 (access point) and if the Ethernet cable connection is removed it acts as a line powered FR (routing device). Ethernet interconnection is limited to installations outside Class I Division 1,
Zone 0/1 locations. An 8 - position Insulation Displacement Connector (IDC) terminal block allows twisted pair Ethernet cable to be connected to the FDAP1/FDAP2 without stripping the wires or crimping on modular RJ-45 plugs. The drain wire from the CAT5E cable shield should be connected to the internal grounding point on the conduit hub. The cable should be solid core to ensure good signal quality and performance of up to 100 m.

Terminating the Ethernet cable

To terminate the Ethernet cable, perform the following steps.

3. Strip the outer jacket of the CAT5e cable and connect the shield drain wire to the internal grounding lug on the conduit hub. Do not strip the individual twisted pair wires.
4. Connect the twisted pair wires to the IDC following the color chart marked next to the IDC. Note that the color chart on the FDAP1/FDAP2 Power and I/O board assumes that the cable conforms to EIA/TIA 568B color code which is the predominant color code for CAT5e cable. Refer to "Table 3: Ethernet IDC block pin-out" for the necessary adjustment if the older EIA/TIA 568B color coded cable is used. Most of the CAT5E cables conform to TIA/EIA 568B.

Table 3: Ethernet IDC block pin-out

PIN #	TIA/EIA 568A	TIA/EIA 568B	Data
1			Transmit+
2			Transmit-
3			Receive+
4			Unused
5			Unused
6			Receive-

PIN #	TIA/EIA 568A	TIA/EIA 568B	Data
7			Unused
8			Unused

Testing Ethernet connection

A standard RJ-45 modular jack is available on the FDAP1/FDAP2 Power and IO board. The RJ-45 jack may be used to test cable integrity after terminating the cable at the IDC connector. After terminating the field cable at the IDC, connect the cable tester to the RJ-45 jack. An end-to-end cable test can then be performed to ensure proper wiring at the IDC connector.

3.13 Power on and startup for FDAP Gen3

The FDAP Gen3 has status LED’s to indicate the various stages of operation.

Figure 9.1: LED indicators

The following table identifies the LED’s and describes the operating conditions of the unit when the LED’s are turned ON.

Table 3.1: LED indicators

LED	Description
Power LED (Red)	Indicates that the power is supplied to FDAP Gen3. When the FDAP Gen3 is powered ON, Power LED turns ON automatically.
Ethernet Active LED (Green)	Indicates that FDAP Gen3 is connected to FDN network . When the FDAP Gen3 is connected to FDN Network, Ethernet Active LED turns ON automatically.
Ethernet Link LED (Green)	Indicates the Ethernet link activity. • The LED is steady when there is a valid Ethernet link but no data activity. • The LED blinks when there is data activity on the Ethernet link.
Status LED/Heart Beat LED (Green)	Indicates the software status of FDAP Gen3 factory image. The Status LED blinks ON/OFF once every second to indicate that the FDAP Gen3 factory firmware is in the working condition.

BLE Status LED (Green)	BLE Status LED provides the different states of BLE connection: • ALWAYS OFF - Advertisement off, controlled through WDM UI, typically done when FDAP already joined the network. • 10 seconds OFF, 1 second ON – FDAP Gen3 in advertisement mode, waiting for connection from BLE Central (ex: Mobile App). • 2 seconds OFF, 2 seconds ON – FDAP Gen3 is connected to BLE Central (ex: Mobile App). NOTE: Only connected, not yet BONDED. • 1 second OFF, 1 second ON - FDAP is bonded to BLE Central (ex: Mobile App). • ALWAYS ON - FDAP is ready for secure data exchange with BLE Central (ex: Mobile App). • And special case of BLE module firmware download, where LED is toggled every 250ms (that is 250ms ON, 250ms OFF). NOTE: When BLE module firmware download is in progress, connection to FDAP Gen3 by BLE Central (ex: Mobile App) is not possible.
Comm LED (Green)	Indicates the RS485 port's activity. • The LED blinks when there is data activity on the RS485 port.

3.14 Power on and startup for FDAP1/FDAP2

The FDAP1/FDAP2 has status LED's to indicate the various stages of operation.

Figure 9.2: LED indicators

The following table identifies the LED's and describes the operating conditions of the unit when the LED's are turned ON.

Table 3.2: LED indicators

LED	Description
Power LED (Green)	Indicates that the power is supplied to FDAP1/FDAP2. When the FDAP1/FDAP2 is powered ON, Power LED turns ON automatically.
Status LED/Heart Beat LED (Green)	Indicates the software status of FDAP1/FDAP2 factory image. The Status LED blinks ON/OFF once every second to indicate that the FDAP1/FDAP2 factory firmware is in the working condition.
Comm LED (Green)	Indicates the Ethernet link activity. • The LED is steady when there is a valid Ethernet link but no data activity. • The LED blinks when there is data activity on the Ethernet link.

4 FDAP Configuration

Related topics

Establish connection between WDM and FDAP
Provision an FDAP
Description of FDAP parameters

4.1 Establish connection between WDM and FDAP

To establish connection between WDMA and FDAP, power on the FDAP and connect FDAP to the WDM through FDN port of WDM. If you are using multiple FDAPs, you can use an Ethernet switch to connect the FDAPs to the WDM. WDM enables you to commission, configure, and monitor the FDAPs connected to it from a centralized location. All FDAP configuration parameters are easily accessible from the WDM, which centralizes all key functions required to manage the field device network and wireless field devices.

Log on to the OneWireless user interface and configure the WDM using the First Time Configuration Wizard. The First Time Configuration wizard appears only for the first log on. For more information about First Time Configuration and OneWireless user interface details, refer to the *Wireless Device Manager User's Guide*.

4.2 Provision an FDAP

The FDAP should be given a unique authentication key to associate it with the wireless network in which it is installed and operated. The authentication keys are generated and managed by the WDM. You can provision an FDAP using over-the-air provisioning or using a Provisioning Handheld device. A Provisioning Handheld device is used to upload the authentication keys from the WDM to the Provisioning Handheld device, and then download the keys to FDAPs using IR media. You can send provisioning information (security, wireless) from Provisioning Handheld device to the FDAP using IR communication link. Once the unit is set up and the authentication is completed, the FDAP joins the network and starts communicating.

Attention

Before provisioning an FDAP, ensure that you have configured the WDM using the First Time Configuration Wizard and the authentication keys are transferred to the Provisioning Handheld device from the WDM.

For more information about the procedure to provision an FDAP, refer to the *Wireless Device Manager User's Guide*.

4.3 Description of FDAP parameters

Once the FDAP joins the network, you can configure and monitor the FDAP by using OneWireless user interface. The Selection Panel in the OneWireless user interface provides a list of all the devices in the OneWireless Network. The Property Panel in the OneWireless user interface provides configuration properties of all the devices configured in the OneWireless Network. Select the required FDAP from the list of devices in the Selection Panel, and then view the FDAP parameter details in the Property Panel.

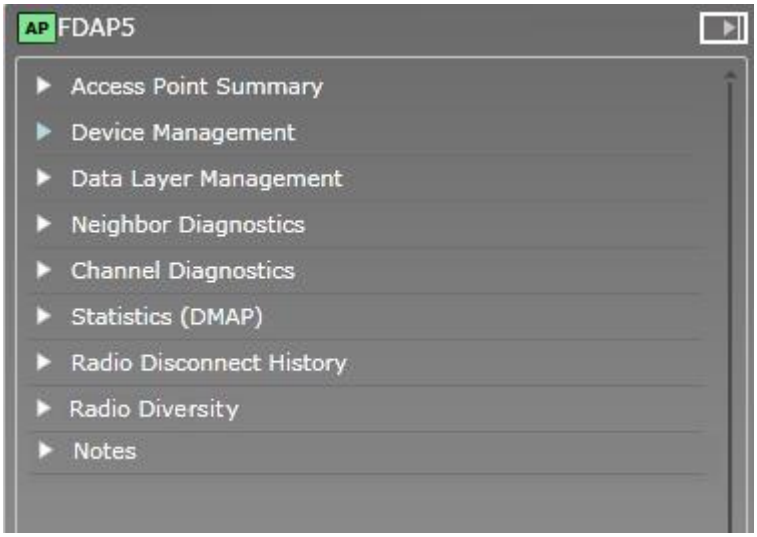
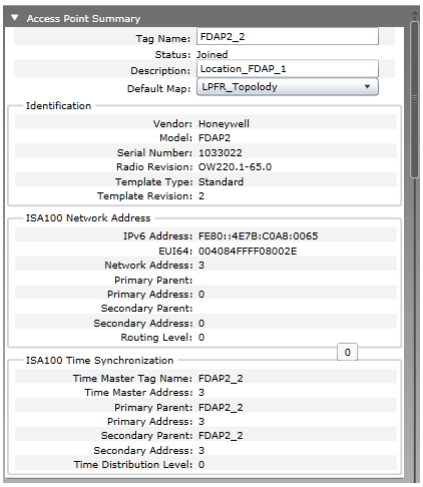
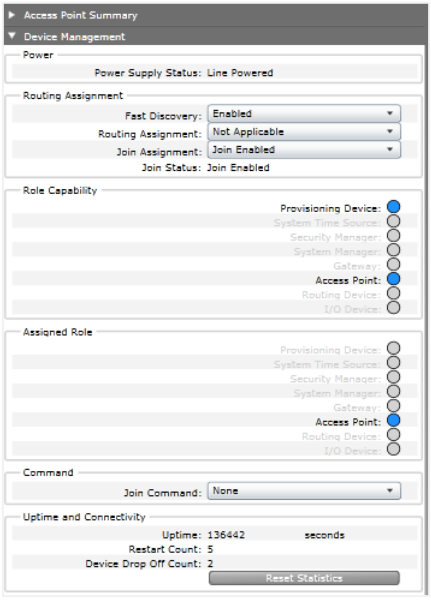


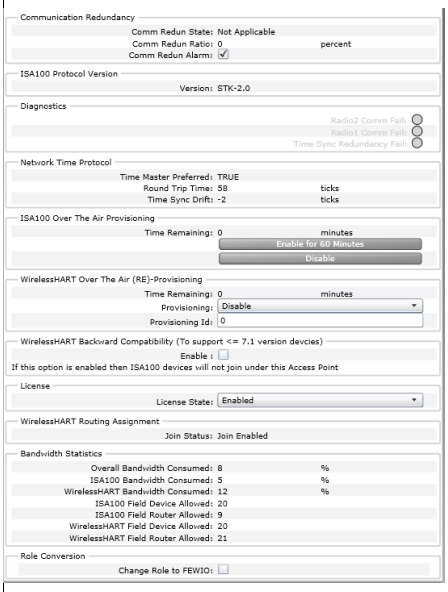
Figure 10: FDAP Property Panel

The following table describes the FDAP parameter details.

Table 4: FDAP parameters in the selection panel

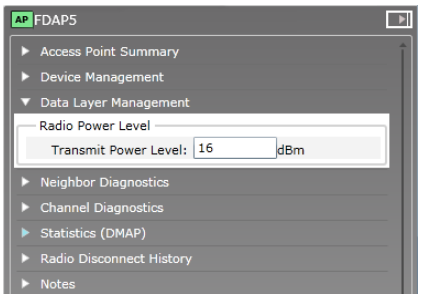
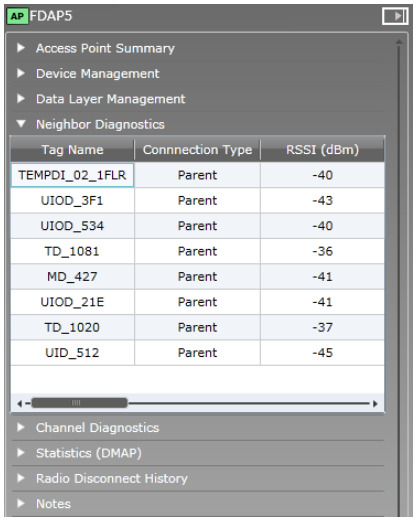
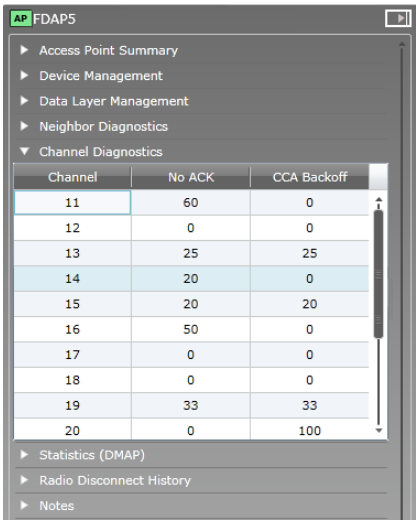
Panel	Group elements	Description
Access Point Summary 		Tag Name: Displays the default device name. You can rename the device. Device name can be up to 16 alphanumeric characters long and it should begin with an alphabet.
		Status: Displays the device status as **Joined** or **Offline**.
		Default Map: You can select the required map on which the device must be placed.
		Description: Displays the entered description for the device. You can type the required description for the device.
	Identification	Displays the identification details like Vendor, Model (device type), Serial Number (EU ID of the device), Radio Revision (firmware revision number), Template Type, and Template Revision.

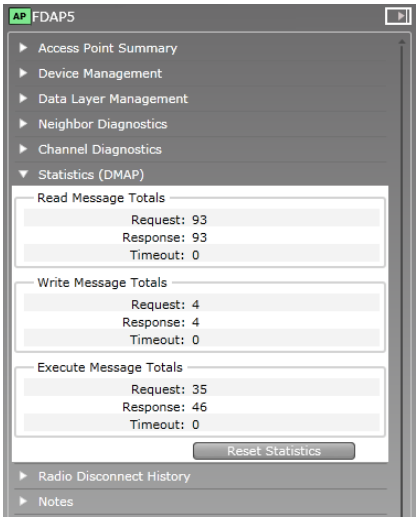
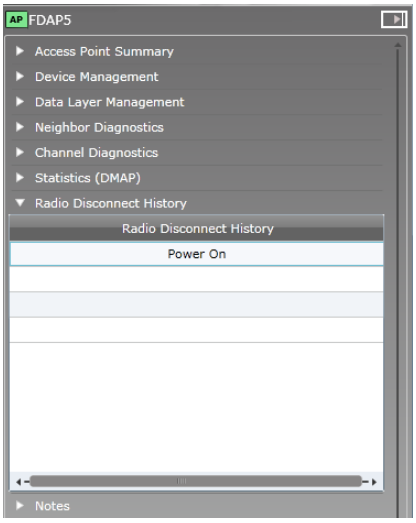
Panel	Group elements	Description
	ISA100 Network Address	Displays the network address details like IPv6 Address (128-bit network address), EUI64 (unique ID), Short Address (16-bit number assigned by system manager), and the Routing Level. **Note**: When you move the mouse pointer over the partially visible data on the Property Panel, the complete data is visible.
	ISA100 Time Synchronization	Displays the tag name and the 16–bit address of the time master of the device, and the time distribution level.
Device Management 	Power	Displays the power supply status as Line Powered (for access points) or Battery Powered (for routing devices). By default, power status is always Line Powered for FDAP.
	Routing Assignment	Displays the routing configuration of the device. The different types of configuration are Non-Routing Device, Routing Device, and Not Applicable. By default, Routing Assignment is not applicable for FDAP and it should not be changed.
	Role Capability	Displays the capable roles of a device. By default, FDAP can be an access point device, if you enable over-the-air provisioning then it can act as a provisioning device. The different roles that can be configured are Provisioning Handheld device, System Time Source, Security Manager, System Manager, Gateway, Access Point, Routing Device, and I/O Device. If the Ethernet is plugged, it acts as an access point and if the Ethernet is unplugged, it acts as a routing device.
	Assigned Role	Displays the current assigned role of the device.
	Command	Consists of the **Join Command** parameter which is used to restart a device or to reset a device to factory default state. Join Command parameter has the following options: • **None** • **Warm Restart**: To restart a device. Warm Restart preserves static and constant attributes data. • **Restart as Provisioned**: To reset the device to factory default state. Restart as Provisioned corresponds to the provisioned state of the device in which the device only retains the data received during its provisioning.

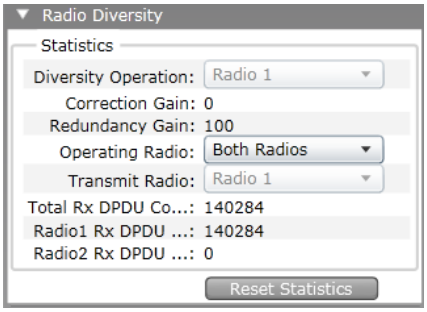
Panel	Group elements	Description
	Uptime and Connectivity	Displays the uptime and connectivity details, which are as follows: • **Uptime**: Time (in seconds) during which the device is online. • **Restart Count**: Number of times the device is restarted. The Restart Count begins from one when it is reset to default. • **Device Drop Off Count**: Number of times the device is disconnected from the network. • **Reset Statistics**: Resets only the Device Drop-off Count. Click to reset the Device Drop Off Count. **Attention** When a device is reset to default through a Provisioning Handheld device, the Restart Count and Device Drop-off Count are reset to 0.
	Communication Redundancy	Displays the Communication Redundancy State, Communication Redundancy Ratio details. The **Communication Redundancy State** is the redundancy communication link between the primary and secondary parent. Select the **Comm Redun Alarm** check box to enable the "Non-Redundant Communication" alarm for this FDAP. **Attention** This alarm is applicable only when the FDAP is acting as an FDAP router.
	ISA100 Protocol Version	Displays the supported version of ISA100 protocol.
	Diagnostics	Displays the ISA100 Wireless radio diagnostics details.
	Network Time Protocol	Displays the Time Master Preferred, Round Trip Time, Time Sync Drift details. **Time Master Preferred**: Time Master preferred is set if the Node/Device is NTP Sync capable or incapable. **Time Sync Drift**: Time Sync Drift is the time drift of the Node/Device from its Parent in clock ticks. **Round trip time**: The duration of the response of the Ping from system manager.
	Over-The-Air provisioning	Consists of the over-the-air provisioning parameters for enabling and disabling over-the-air provisioning. It also displays the time remaining for over-the-air provisioning.
	WirelessHART Backward Compatibility	Check the **Enable** option if FDM supports WirelessHART.

	License	Displays the status of the WDM license.
	WirelessHART Routing Assignment	Displays the status of WirelessHART device joining is allowed or not
	Bandwidth Statistics	Display the bandwidth consumed by FDAP or FDAP as router and approximate device can join under this FDAP or FDAP as router Bandwidth statistics displays Overall bandwidth consumed and also the breakup of ISA100 and WirelessHART device bandwidth consumed. Approximate ISA100 device with 10sec or above publish rate are allowed to join the network Approximate WirelessHART device with 8sec or above publish rate are allowed to join the network
	Role Conversion	FDAP as router can be converted to FEWIO role or vicevesa.

Need to update BLE related configurations of FDAP Gen3- Mahesh to provide the inputs

Panel	Group elements	Description
Data Layer Management 	Radio Power Level	Displays the transmission power level. The default power level is 16 dBm.
Neighbor Diagnostics 		Displays the neighboring devices diagnostics like the Device Tag Name, RSSI, RSQI, Transmit Fail, Transmit CCA Backoff, Transmit NACK, and Clock Sigma.
Channel Diagnostics 		Displays the device's channel diagnostics like channel, No ACK, and CCA Backoff.

Panel	Group elements	Description
Statistics (DMAP) 		Displays the details about the ISA100 Wireless data link layer statistics for a selected device. Displays the Read Message Totals, Write Message Totals, and Execute Message Totals details.
Radio Disconnect History 		Displays the radio disconnect history details.
Radio Diversity	Error Distribution Count	Displays the error distribution counter, which corresponds to the error packet counter for the number of bytes corrected. The error packet counter is the total count of error packets received on both antennas with Cyclic Redundancy Check (CRC) error.

Panel	Group elements	Description
	Statistics	Diversity Operation: Displays the FDAP antenna operational status. The status can be Both Radios, Radio 1, or Radio 2. Correction Gain: Displays the correction gain, which is the total packet corrected by packet error correction algorithm. Redundancy Gain: Displays the redundancy gain, which is the minimum value of total packets received by antenna 1 without any packet errors + minimum value of total packets received by antenna 2 without any packet errors / total packets received by antenna 1 and 2 without any packet errors. Reset Statistics: Resets all the radio diversity values. Click to reset all the radio diversity values.
Notes 		Displays notes entered for the FDAP. You can type notes regarding the FDAP.

5 Field Expandable Wireless IO

Related topics

- Overview
- FEWIO Solution
- Converting FDAP Router to FEWIO device
- Connecting Modbus TCP devices to FEWIO device
- Connecting Modbus RTU devices to FEWIO device
- Configure FEWIO device in WDM
- Configuring and Viewing the Modbus Registers
- Converting FEWIO device to FDAP Router
- Experion Integration

5.1 Overview

Field Expandable Wireless IO (FEWIO) is an innovative solution aimed to provide a method for integrating legacy Modbus devices into OneWireless system. Honeywell Field Device Access Point (FDAP) is configured in way wherein it can be used as an expandable wireless device that extracts the data from the legacy Modbus devices, wirelessly. This is a licensed feature.

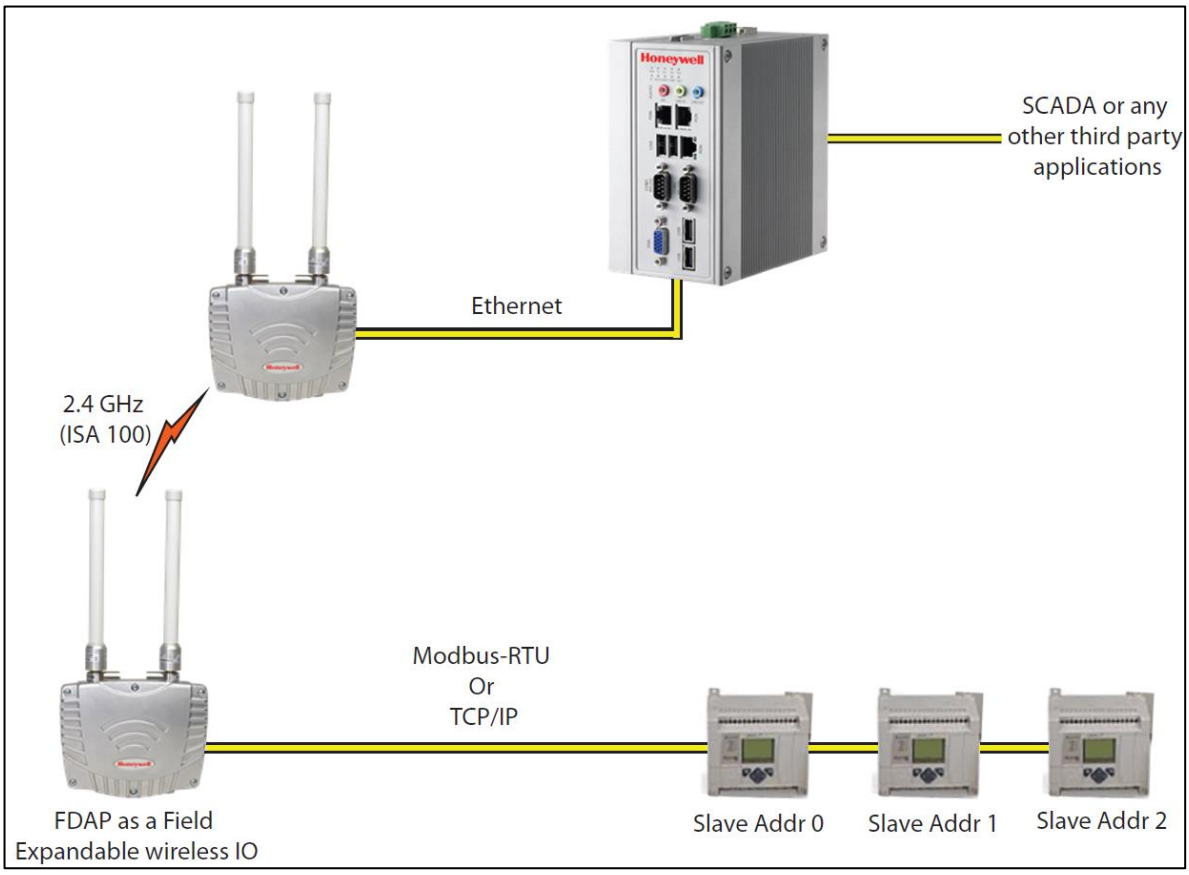
Typically, in a plant there are thousands of legacy wired Modbus devices and managing (monitoring, viewing, accessing data) them is a mammoth task. To wirelessly enable this, you can use the FEWIO solution. This solution will give huge cost savings (no wiring, switches will be needed) and will make the data easily accessible.

You can connect multiple Modbus devices to OneWireless Network using the Honeywell Field Device Access Point (FDAP). FDAP will change its role to FEWIO and extracts the data from Modbus (RTU/TCP) slave devices and converts it to the ISA100 environment. The legacy devices are connected to the FDAP using the RS-485 protocol or TCP/IP. The collected data in WDM can be accessed by a SCADA or any other third party applications.

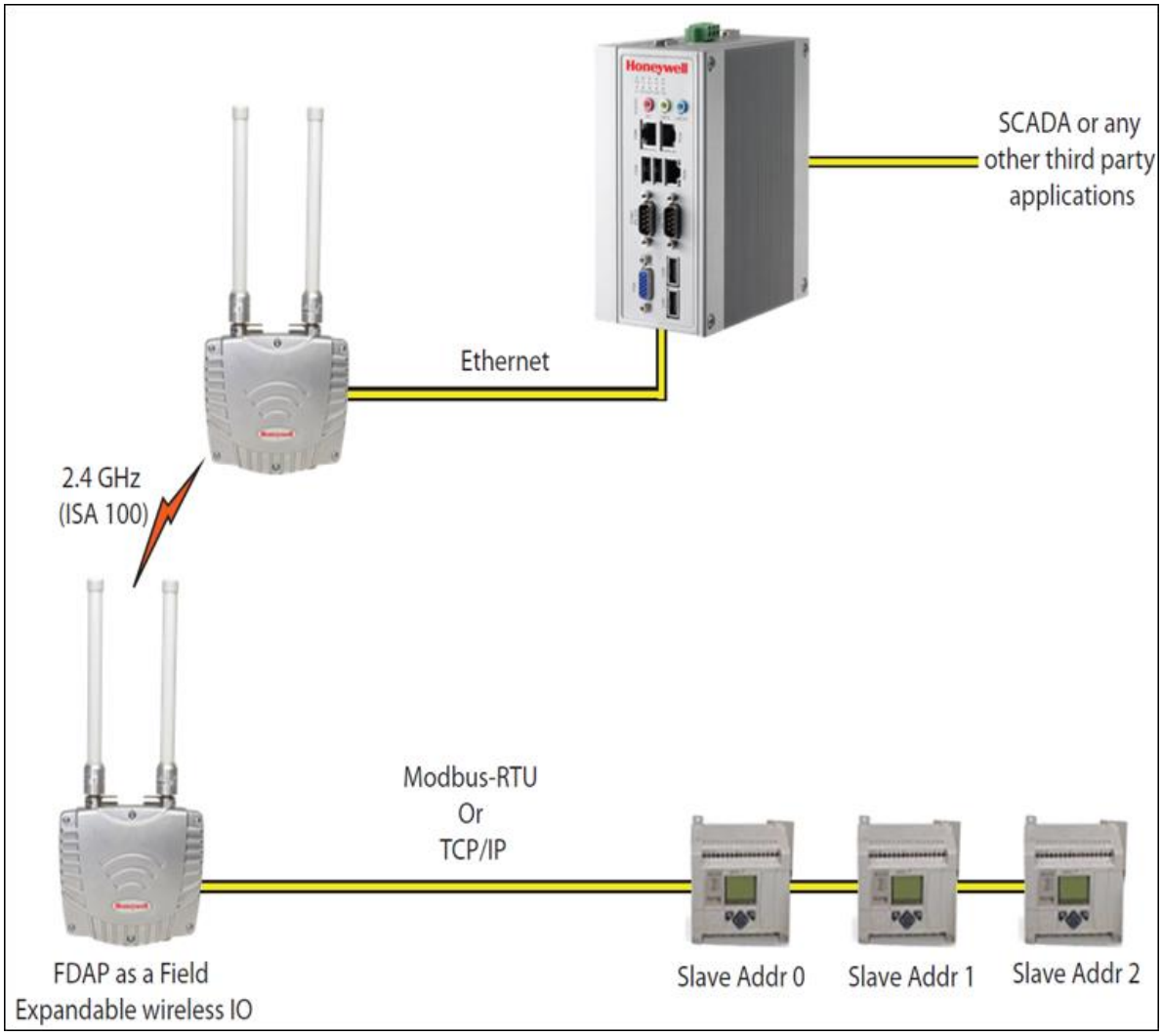
Only FDAP acting as a field router can be converted to FEWIO.

5.2 FEWIO Solution

The below figure shows a graphical overview of the FEWIO solution with FDAP1 and FDAP2.



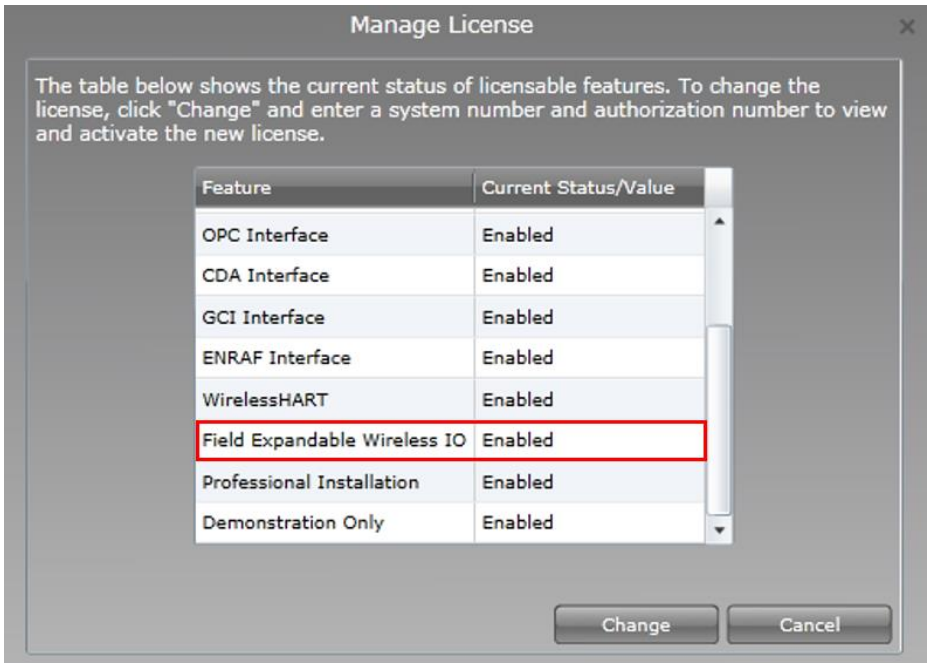
The below figure shows a graphical overview of the FEWIO solution with FDAP1/FDAP2 and FDAP Gen3.



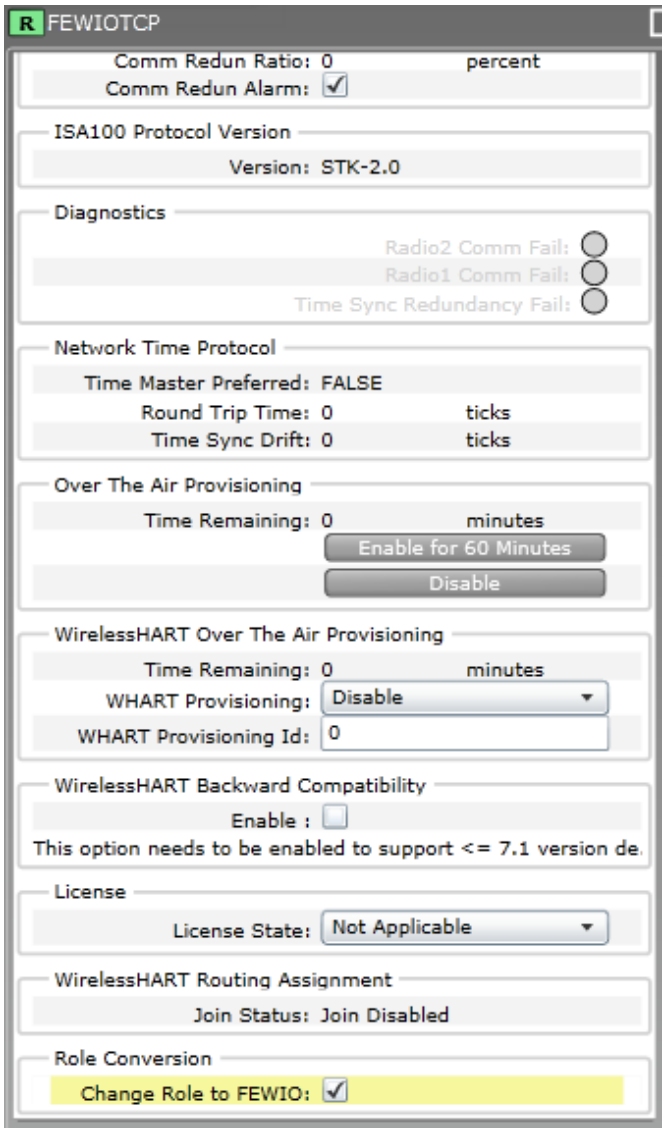
5.3 Converting FDAP Router to FEWIO device

To convert FDAP Router to FEWIO

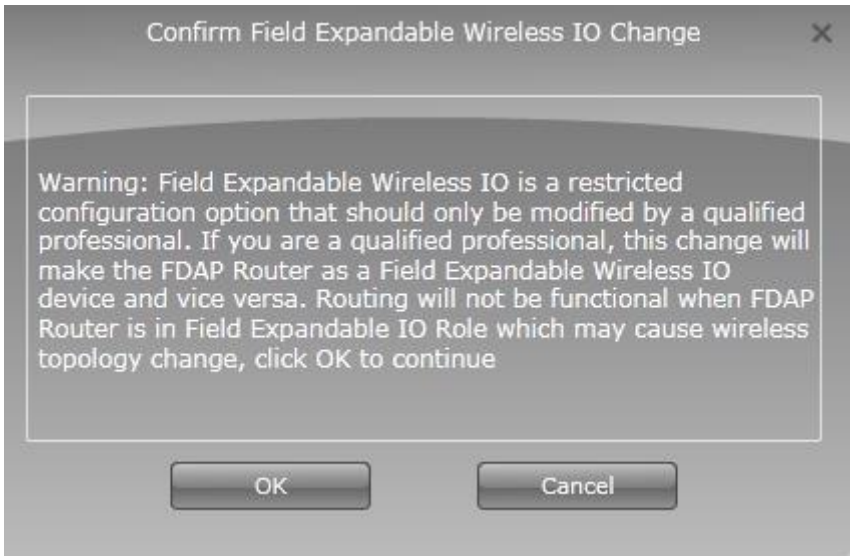
1. Ensure that you have the licensed version of WDM that includes FEWIO feature.
   On the ribbon bar, in the **System** group, click **Licensing**.
2. The **Manage License** dialog box appears



3. Click **Cancel**.
4. On the Selection Panel, select the FDAP router that needs to be converted as FEWIO.
5. On the Property Panel, expand **Device Management.**
   Under **Role Conversion,** Select the **Change Role to FEWIO** checkbox.

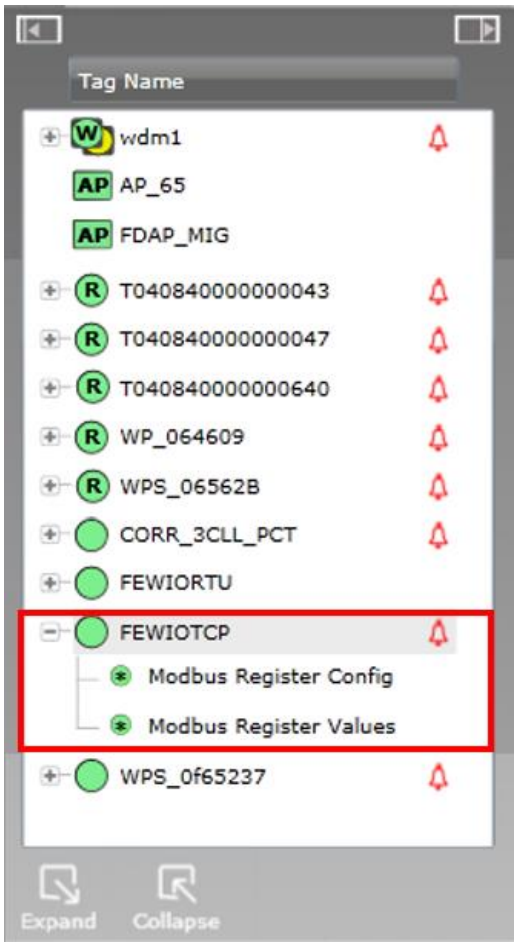


6. The **Confirm Field Expandable Wireless IO Change** dialog appears.



7. Click **OK**.

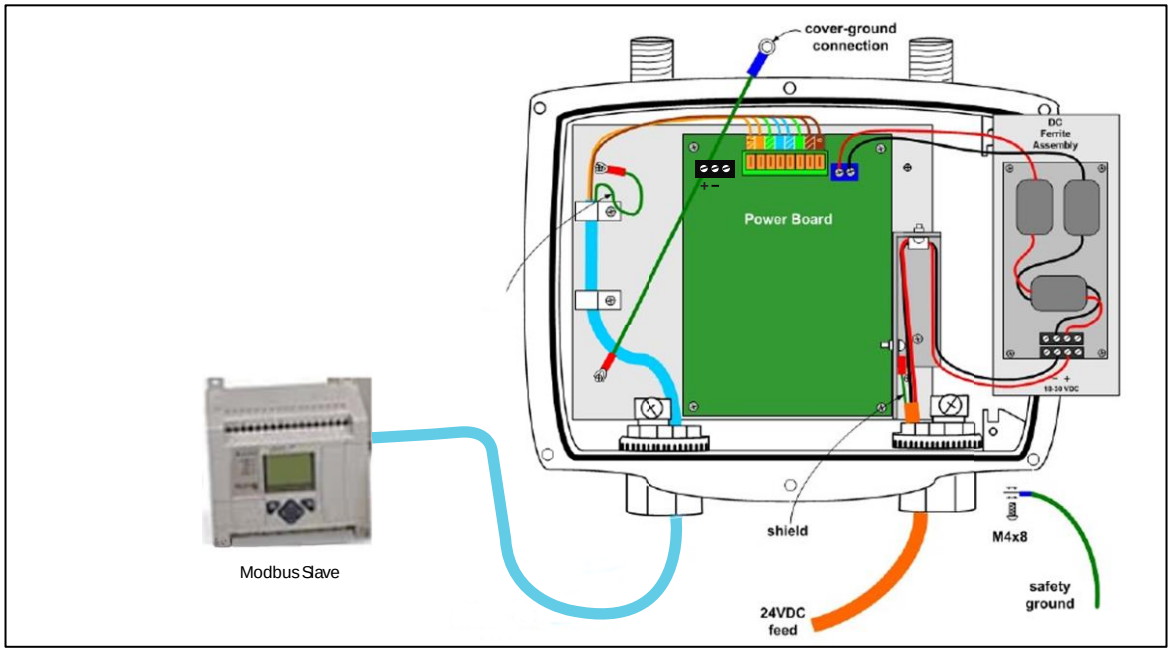
8. Click **Apply**.
   The device will drop out from the network and rejoins as FEWIO.



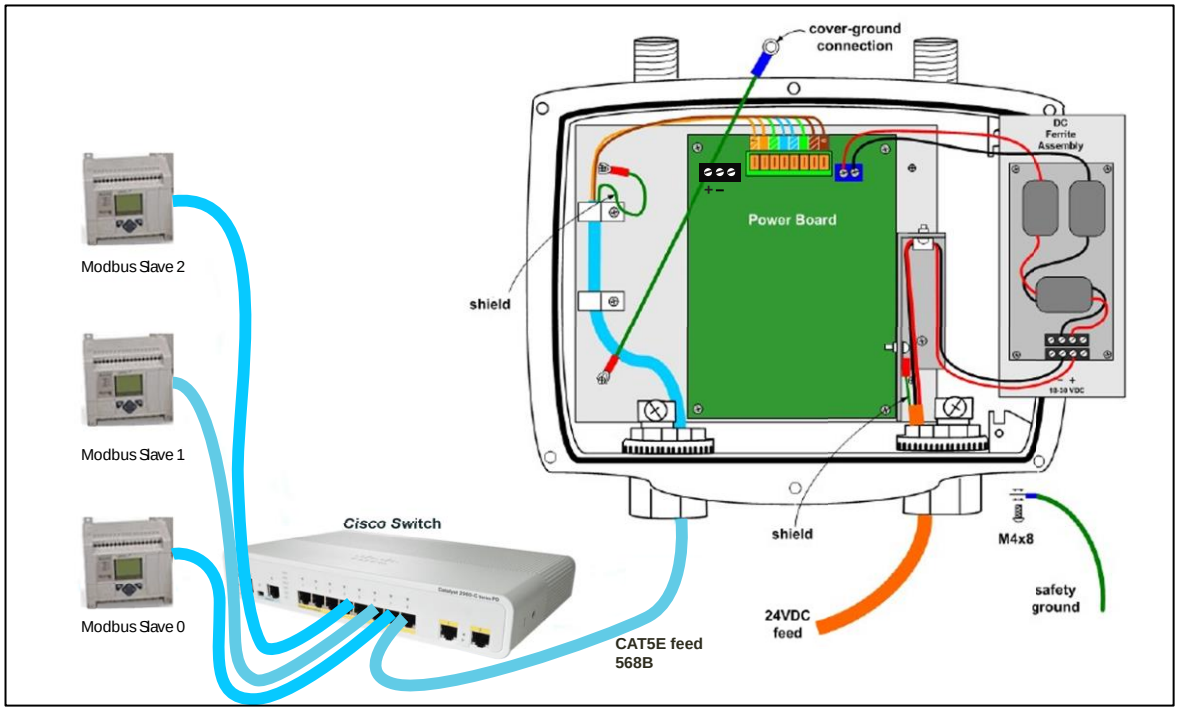
5.4 Connecting Modbus TCP devices to FEWIO device

Aravind to provide image for Gen3

FDAP router Ethernet cable should be connected to Modbus Slave Ethernet port as shown below.



FDAP router Ethernet cable should be connected via a Cisco Switch, if you have multiple TCP Modbus slaves as shown below.

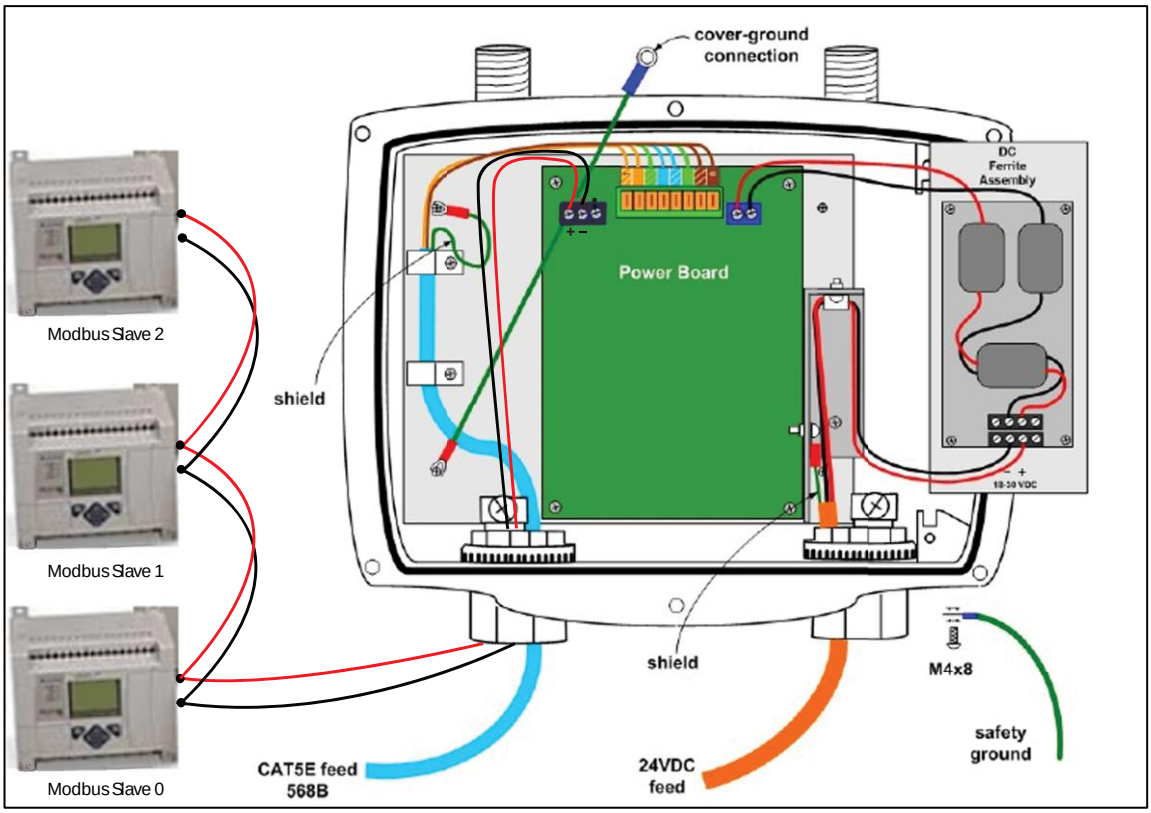


5.5 Connecting Modbus RTU devices to FEWIO device

Aravind to provide image for Gen3

FDAP supports 2 wire RS-485 interface. A 3-pin connector is available on the Power Board of the FDAP when FDAP top cover is opened as shown in the below picture. V+ and V- are the two pins that needs to be connected to slave RS-485 2-wire connection (DATA+ and DATA-) as shown below.

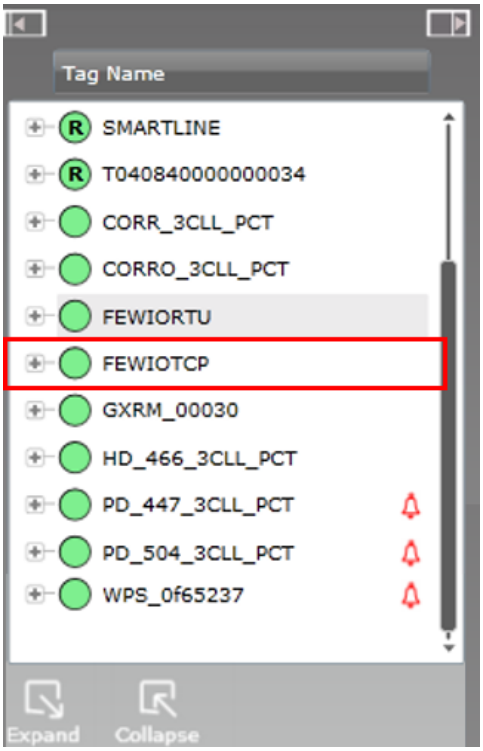
Ethernet is not supported in Gen3



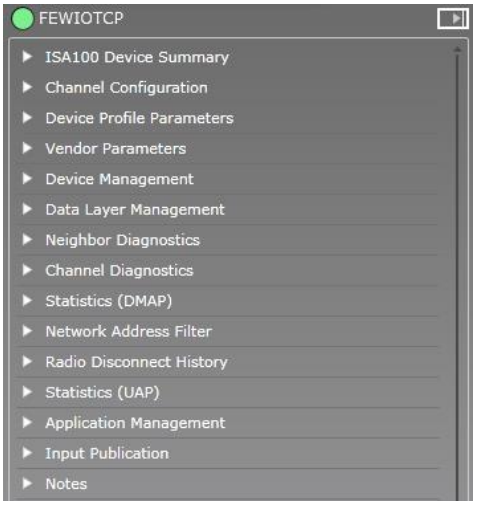
5.6 Configure FEWIO device in WDM

To configure FEWIO device in WDM:

1. Make sure that FEWIO DD file is loaded in WDM.
2. On the Selection Panel, select the applicable **FEWIO**, which needs to be configured.

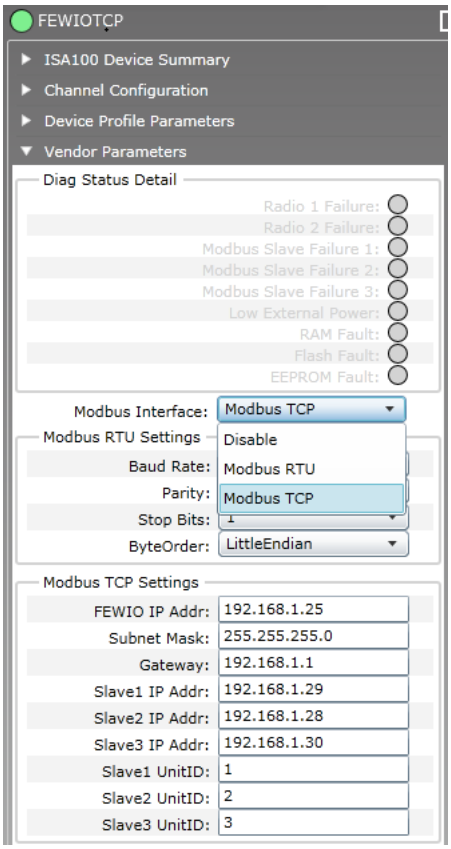


3. On the Property Panel, expand **Vendor Parameters.**



4. In the **Modbus Interface** list, click the required option. The following are the interface options available.
   - Modbus RTU
   - Modbus TCP

Attention
Based on the connected Modbus devices, select the appropriate option.



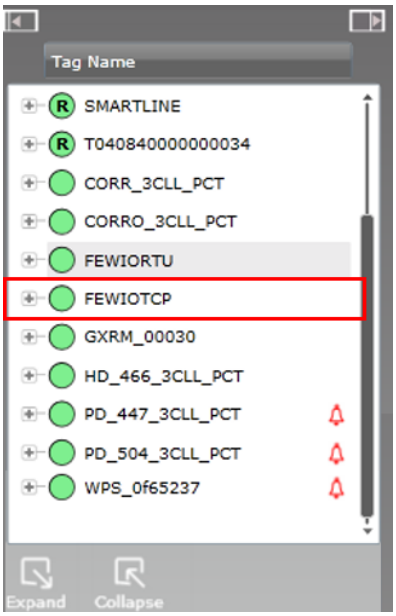
5. Configure one of the following depending on the Modbus interface option that you have selected.
   - If you have selected **Modbus TCP** Interface, configure the following under **Modbus TCP Settings**.
     - **FEWIO IP Addr**: IP address that needs to be assigned to FEWIO and the IP address Subnet should be same as the IP address of slaves.
     - **Subnet Mask**: Subnet Mask
     - **Gateway:** Gateway IP address.
     - **Slave1 IP Addr**: IP address of Slave1
     - **Slave2 IP Addr**: IP address of Slave2
     - **Slave3 IP Addr**: IP address of Slave3
     - **Slave1 UnitID**: Unit ID of Slave1 used for the Modbus TCP port.
     - **Slave2 UnitID**: Unit ID of Slave2 used for the Modbus TCP port.
     - **Slave3 UnitID**: Unit ID of Slave3 used for the Modbus TCP port.
   - If you have selected **Modbus RTU** Interface, configure the following under **Modbus RTU Settings**.
     - **Baud Rate:** Select the baud rate used for the Modbus RTU serial port. Options include: **9600,19200, 38400, 57600, 11520**.
     - **Parity:** The parity used for the Modbus RTU serial port. Options include: **Even** and **Odd**.
     - **Stop Bits:** Options include: **1** and **2**.

- **Byte Order:** Select a byte order that matches the expected byte order of the Modbus client. Options include: **Big Endian**, **Little Endian, Big Endian Bytes Swapped**, and **Little Endian Bytes Swapped**.

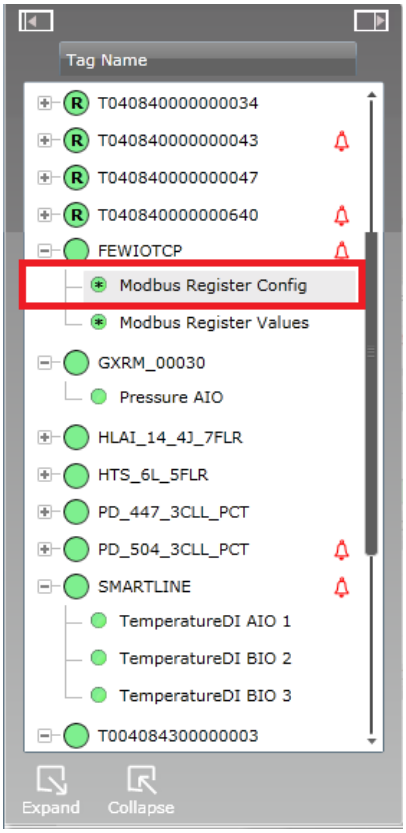
5.7 Configuring and Viewing the Modbus Registers

To configure the Modbus Registers:

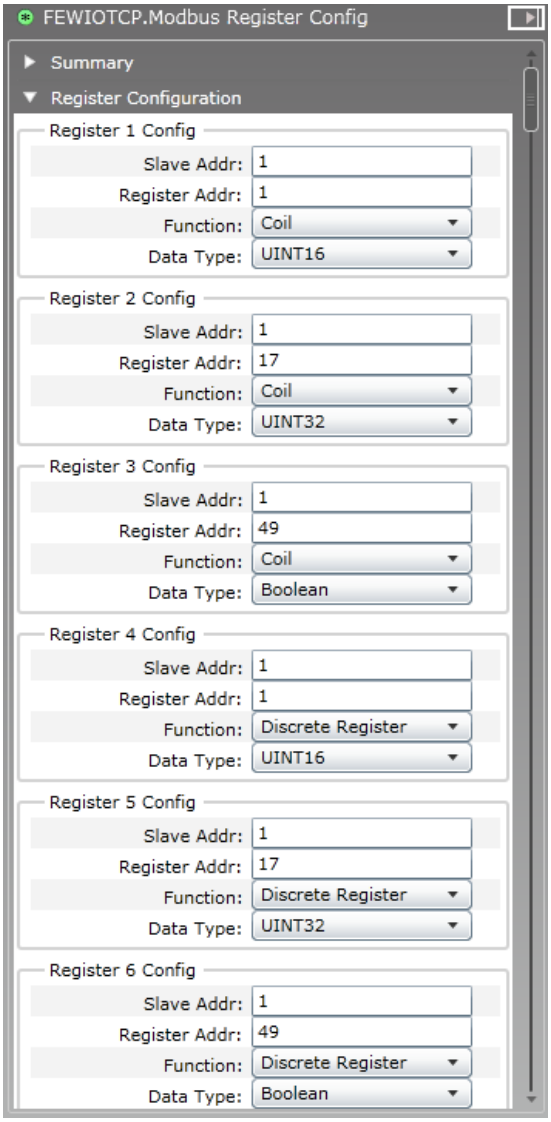
1. On the Selection Panel, select the **FEWIO**.



2. Expand the FEWIO and select the **Modbus Register Config** option



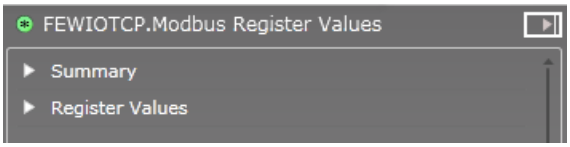
3. On the Property Panel, expand **Register Configuration.**



4. Configure the following under each **Register Config:**
   - **Slave Addr**: Slave Address
   - **Register Addr**: Register Address
   - **Function:** Select required function option from the dropdown list.Options include: **Input Register, Holding Register**, **Coil** and **Discrete Registers.**
   - **Data Type:** Select required datat type option from the dropdown list. Options include: **INT16, INT32, UINT16, UINT32, Float** and **Boolean.**
5. Click **Apply**.

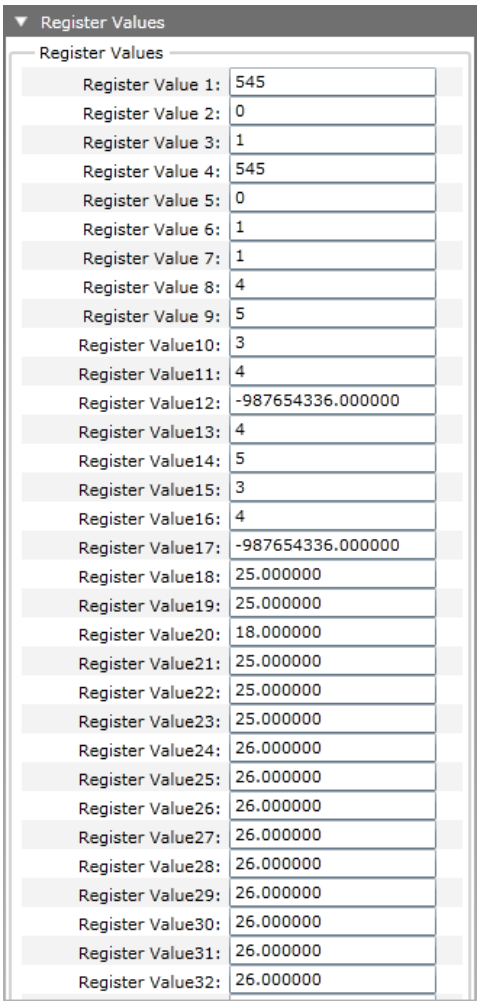
To view the configured Modbus Registers

1. On the Selection Panel, select **Modbus Register Values**.
2. On the Property Panel, expand **Register Values.**



3. Now, you can view the respective register values as shown below.

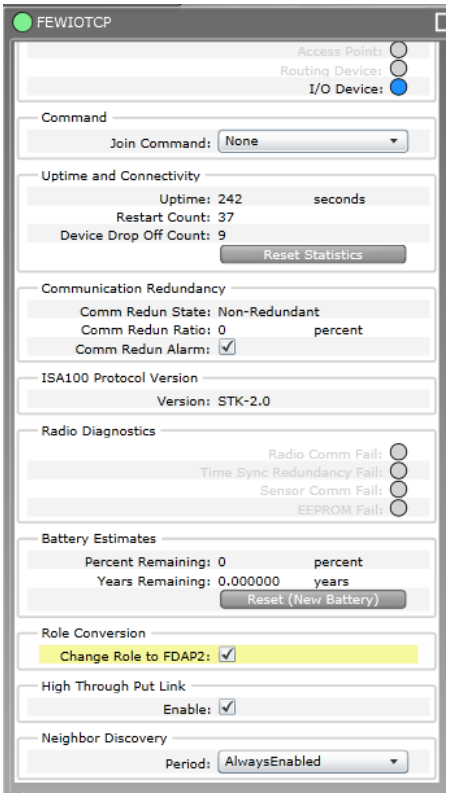
The values shown for each register is the value read from the respective slave device registers as configured in the register configuration.



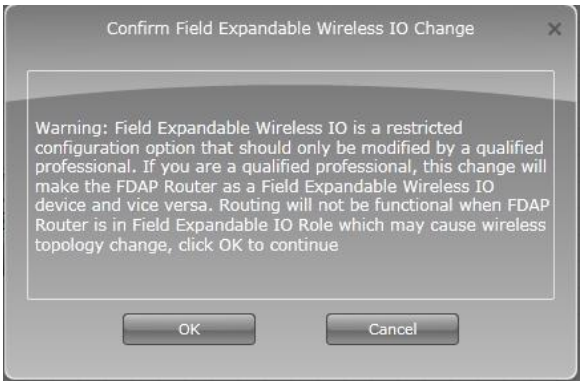
5.8 Converting FEWIO device to FDAP Router

To convert FEWIO to FDAP Router

1. On the Selection Panel, select the FEWIO that needs to be converted as FDAP router.
2. On the Property Panel, expand **Device Management.**
   Under **Role Conversion,** Select the **Change Role to FDAP2** checkbox.

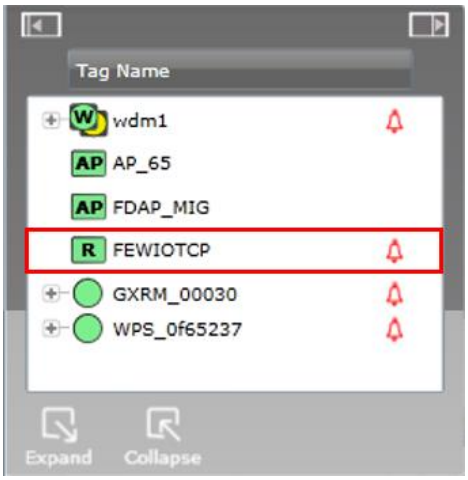


3. The **Confirm Field Expandable Wireless IO Change** dialog appears.



4. Click **OK**.

5. Click **Apply**.
   The device will drop out from the network and rejoins as FDAP router.



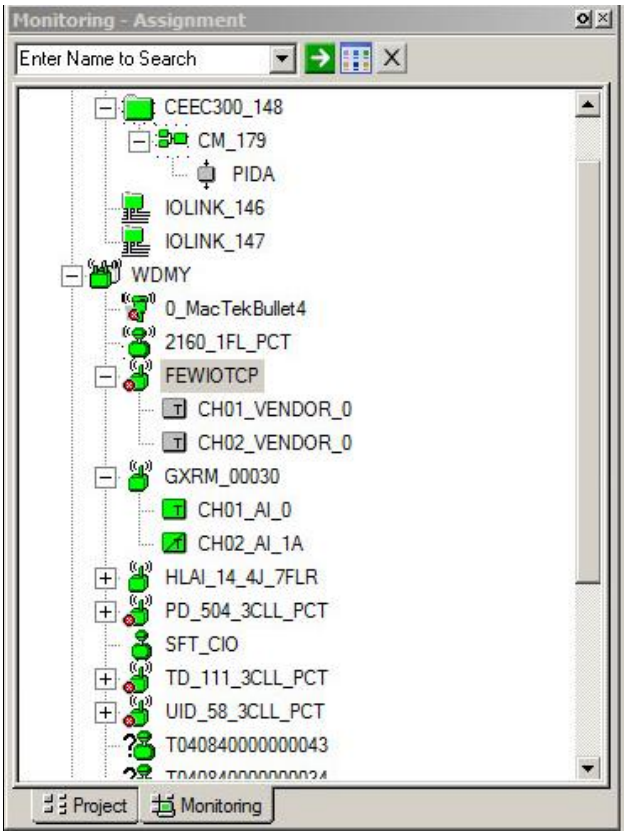
5.9 Experion Integration

FEWIO device is natively integrated with Experion system. All parameter read and write, configuration support is provided in Experion for FEWIO device through ISA100 DD file.

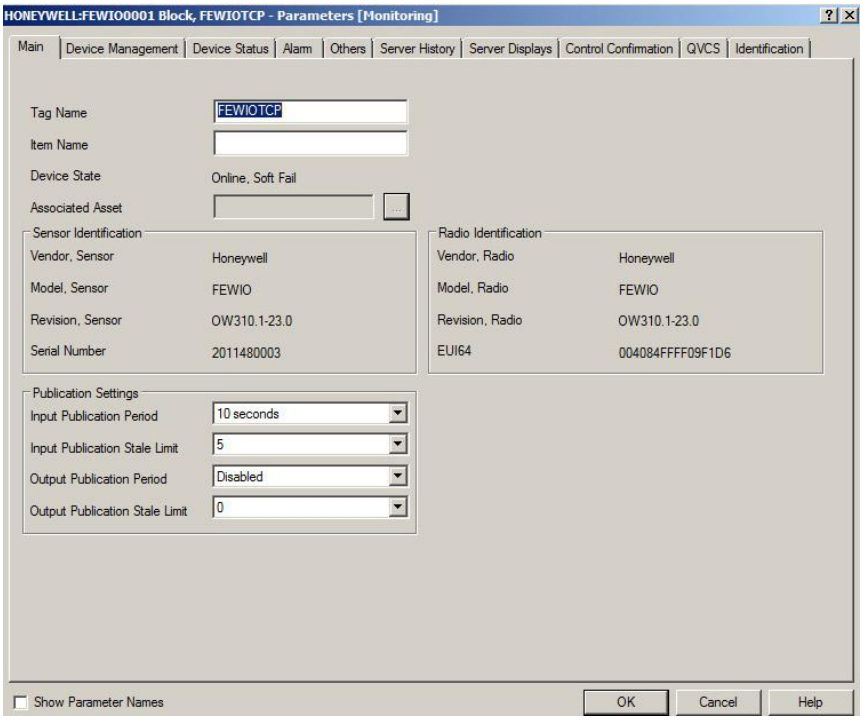
FEWIO comes as an un-commissioned ISA 100 device in Experion Control Builder, just like any other ISA 100 field devices. It will be commissioned and configured similar to other ISA100 Devices.

To Configure the Modbus Registers of FEWIO

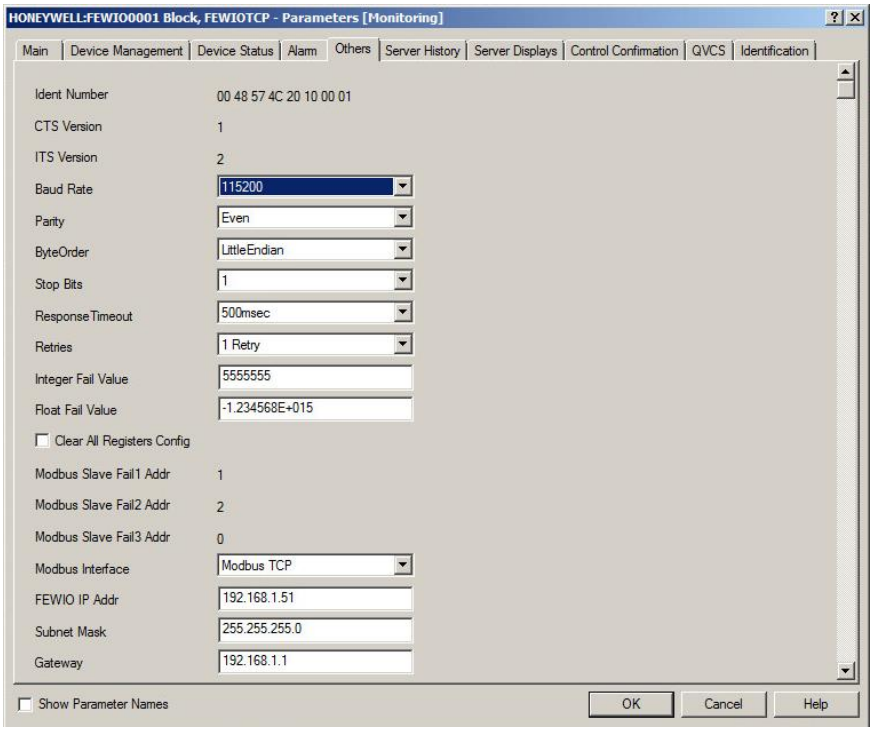
1. Make sure that FEWIO DD file is loaded in Control Builder.
2. Commission the FEWIO device in the Control Builder.
3. Once commissioned, FEWIO will appear in Control builder as shown below.



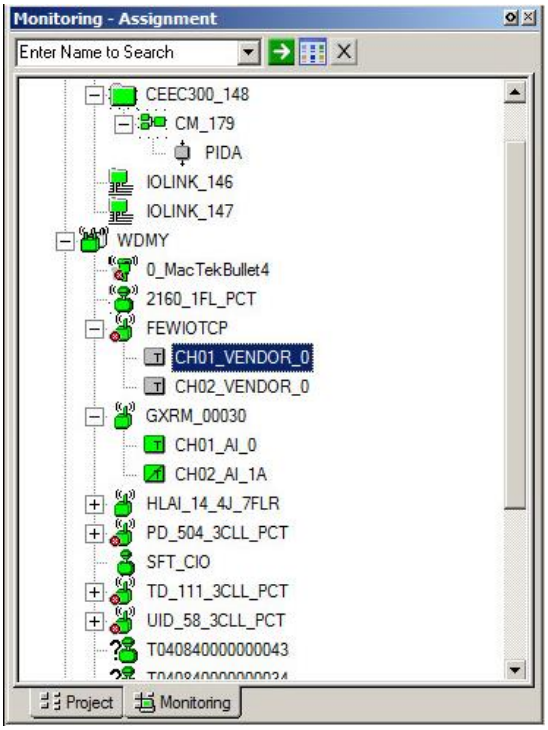
4. Double click on the FEWIO that needs to be configured.
   The **FEWIO-Parameters [Monitoring]** window appears



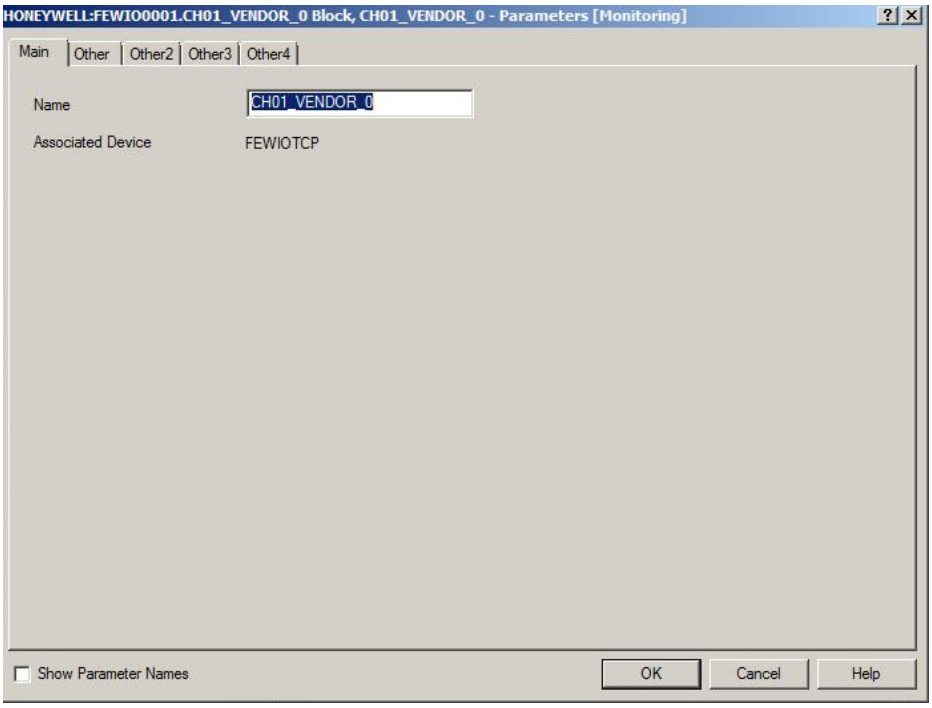
5. Go to **Others** tab and configure the parameters in the same way as configured in WDM



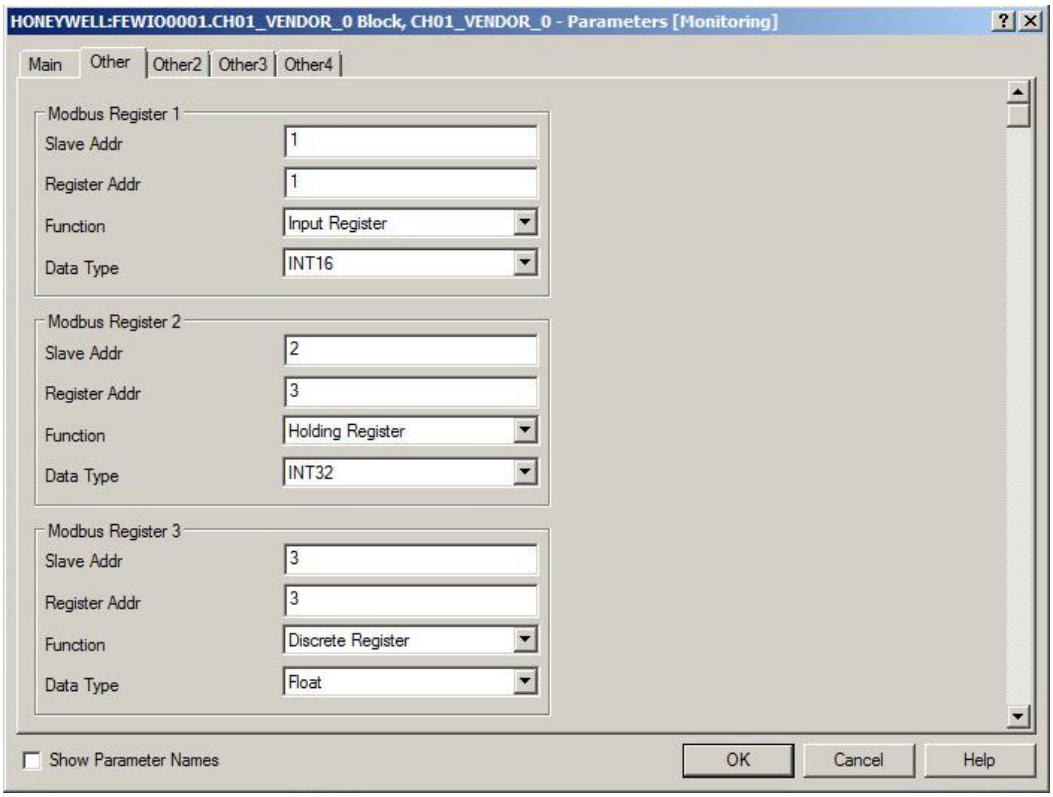
6. Click OK.
7. On the **Monitoring-Assignment** window, under the **FEWIO**, double Click **CH01_VENDOR_0**



8. The **CH01_VENDOR_0-Parameters [Monitoring]** window appears.



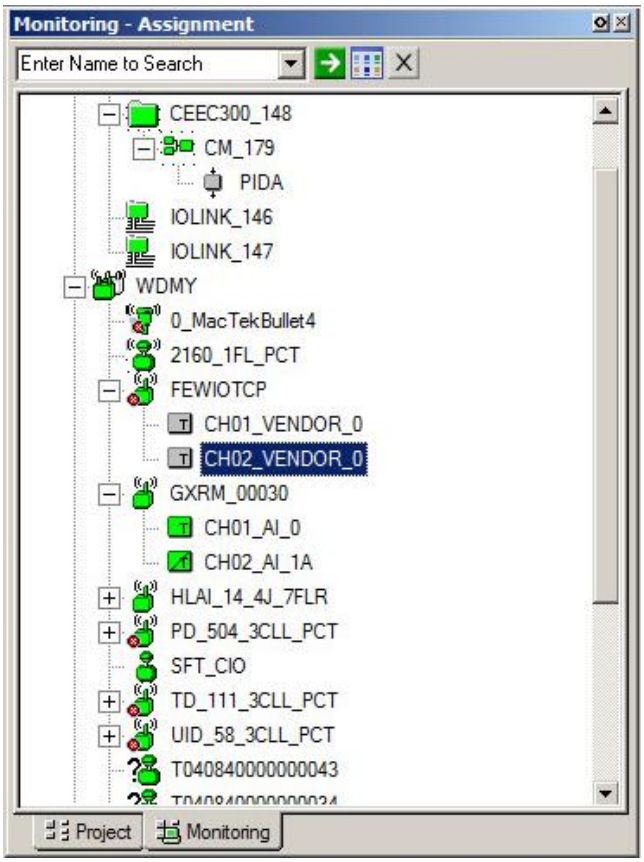
9. Go to **Other** tab and configure the parameters in the same way as they are configured in WDM.



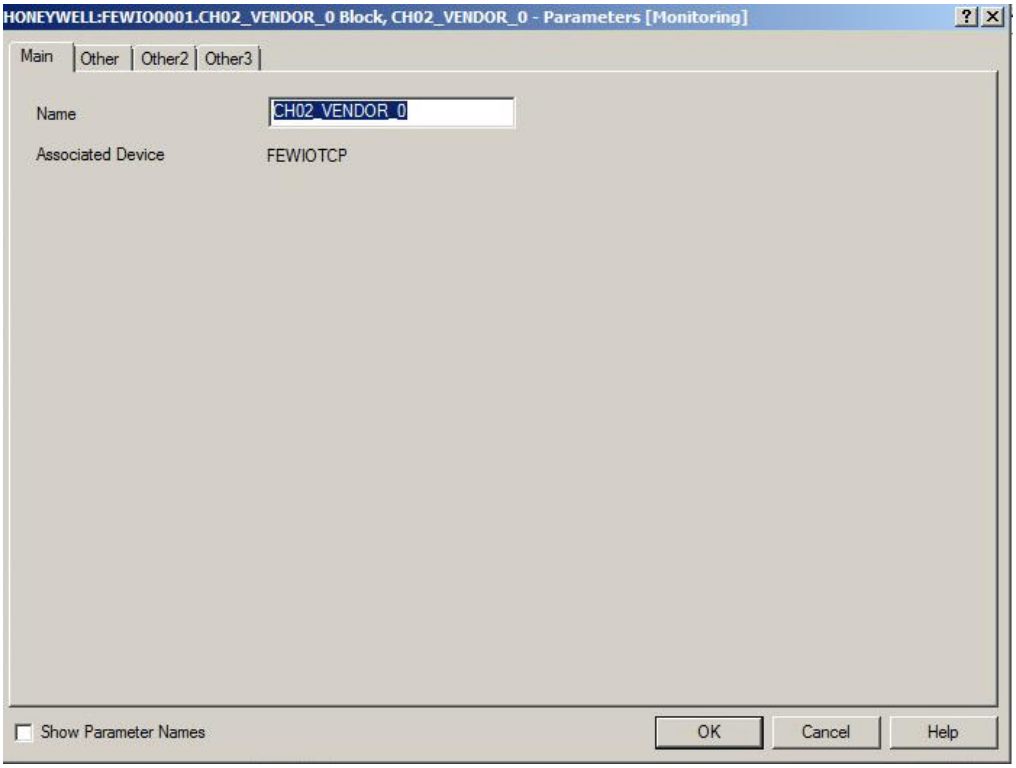
10. Click Ok.

To view the configured Modbus Registers

1. On the **Monitoring-Assignment** window, under the **FEWIO**, double Click **CH02_VENDOR_0.**

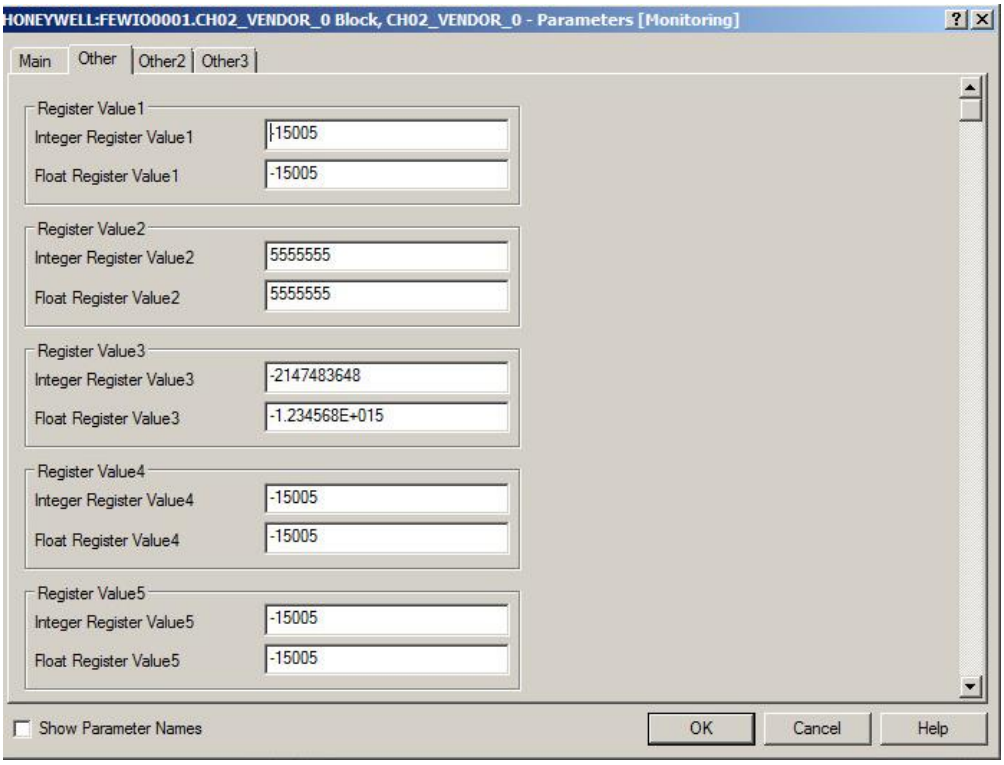


2. The **CH02_VENDOR_0-Parameters [Monitoring]** window appears



3. Go to **Other** tab and view the configured parameters.

   The values shown for each register is the value read from the respective slave device registers as configured in the register configuration.


HONEYWELL:FEWIO0001.CH02_VENDOR_0 Block, CH02_VENDOR_0 - Parameters [Monitoring]
Main
Other
Other2
Other3
Register Value1
Integer Register Value1
-15005
Float Register Value1
-15005
Register Value2
Integer Register Value2
5555555
Float Register Value2
5555555
Register Value3
Integer Register Value3
-2147483648
Float Register Value3
-1.234568E+015
Register Value4
Integer Register Value4
-15005
Float Register Value4
-15005
Register Value5
Integer Register Value5
-15005
Float Register Value5
-15005
Show Parameter Names
OK
Cancel
Help

6 FDAP Monitoring

Related topics

- Overview about monitoring
- Verify connectivity using maps
- Monitor using Provisioning Handheld device
- Monitor using events
- Monitor using reports

6.1 Overview about monitoring

The status and performance of FDAPs operating in a wireless network can be monitored in a number of ways.

- The **Monitoring** tab in the OneWireless user interface enables you to monitor FDAPs that are commissioned in the network.
- The **Alarms & Event** tab in the OneWireless user interface enables you to monitor events generated by the FDAPs.
- The **Reports** tab in the OneWireless user interface enables you to view and generate custom reports about connectivity and device health of the FDAPs in a network.

6.2 Verify connectivity using maps

The OneWireless user interface enables you to create multiple locations and upload site map to the location. You can position the devices on the map to reflect the physical design and structure of your plant. You can visually inspect network topology map and connectivity. You can navigate to the device in the topology map and check the link signal quality and connectivity. In addition, you can examine device communication statistics information like Receive Signal Quality Index (RSQI) and Receive Signal Strength Index (RSSI). This helps the network services engineer to verify the wireless mesh connectivity and FDAP connectivity in the OneWireless user interface.

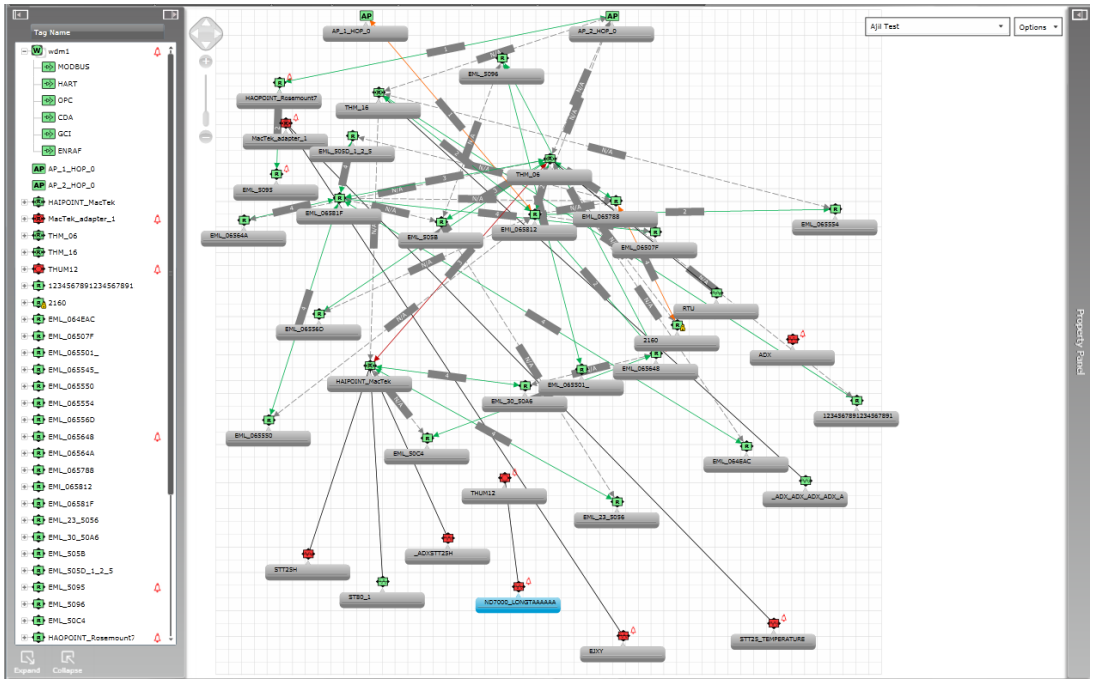


Figure 11: Map view

For more information about setting up a monitoring area and for location specific monitoring, refer to the *Wireless Device Manager User's Guide*.

6.3 Monitor using Provisioning Handheld device

FDAP is authenticated using a Provisioning Handheld device. Once the FDAP is authenticated, it joins the network. Provisioning Handheld device can be used to monitor the status of the authenticated FDAP and Provisioning Handheld device displays status as Discover, Secure, Joined, or Not Joined. You can read and set various FDAP parameters through the Provisioning Handheld device. If the FDAP is not joining the network, you can read the FDAP parameter data through the Provisioning Handheld device and troubleshoot.

6.4 Monitor using events

You can monitor system events generated by the FDAP. Events are generated when the FDAP joins the network, when the FDAP is Online, or when the FDAP is Offline or switched off. You can also export the event log created for a particular time period. For more information about monitoring device using events, refer to the *Wireless Device Manager User's Guide*.

6.5 Monitor using reports

You can generate and view various reports about connectivity, and device health of FDAPs in a network. You can generate and view the following reports:

- Battery Life
- Device Health Overview
- Device Summary
- Device History
- Connection Summary
- Connection History
- Inventory Summary

You can print the report and save the report in *.csv* format. For more information about reports, refer to the *Wireless Device Manager User's Guide*.

7 FDAP Maintenance and Troubleshooting

Related topics

Replace an FDAP
Remove an FDAP
Upgrade an FDAP firmware
Troubleshoot an FDAP

7.1 Replace an FDAP

You can replace a failed FDAP with a new device only if the new device specification is identical to the failed one. For more information about the procedure to replace an FDAP, refer to the *Wireless Device Manager User's Guide*.

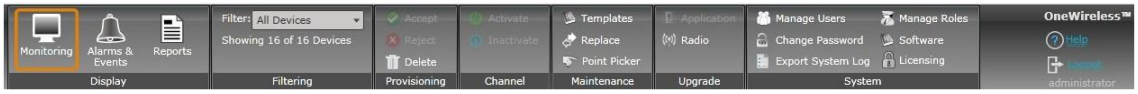


Figure 12: Maintenance icons

Attention

Any maintenance required is limited only to the external enclosure surface, cable connections, antennas, and the firmware. A failed unit should be returned to Honeywell for maintenance, repair, or replacement.

7.2 Remove an FDAP

You can remove a failed FDAP from the network. Once the FDAP is removed it will not be able to join the network until it is assigned a new provisioning key. For more information about the procedure to remove an FDAP, refer to the *Wireless Device Manager User's Guide*.

7.3 Upgrade an FDAP firmware

FDAPs have only radio firmware and the radio firmware can be upgraded over-the-air. For more information about the procedure to upgrade a firmware for FDAP, refer to the *Wireless Device Manager User's Guide*.

7.4 Troubleshoot an FDAP

FDAP does not have any user-serviceable parts inside the FDAP enclosure; any failure within the FDAP requires a hardware replacement. If a fault or a failure is indicated or suspected in an FDAP in the network, there are many ways to diagnose a problem. You can diagnose a problem using the following methods:

- Diagnose using events
- Diagnose using reports
- Diagnose using system logs
- Diagnose using Provisioning Handheld device

System logs

The system log contains events logged in the system. The system log information is helpful to System Administrators, Field Engineers, and technical support personnel. You can generate and view the system log details. You can save the system log details in *tar.gz* format. For more information about system logs, refer to the *Wireless Device Manager User's Guide*.

Recovering from failures

Failure indication may be signaled through the FDAP status LEDs. You can restart the FDAP if a failure is suspected. For more information about the procedure to restart the FDAP, refer to the *Wireless Device Manager User's Guide*.

8 Appendix

Related topics

FDAP GEN3 Technical Specification
FDAP Technical Specification
FDAP Gen3 Dimension Drawing
FDAP Dimension Drawing
FDAP GEN3 IS Control Drawing
FDAP IS Control Drawing (51202683)
FDAP GEN3 Label Drawing
FDAP Label Drawing

8.1 FDAP GEN3 Technical Specification

Model Numbers	FDAP31 (Class 1 Div 1 / Zone 2) FDAP32 (Class 1 Div 2 / Zone 2)
Multiple Standards / Field Protocols	ISA100 Wireless
Weight	3.86 kg (5.5 lbs)
Dimensions	216 x 170 x 86 mm (8.47 x 6.73 x 3.37 in)
Power	PoE at 2Watts
External Ports and Connections	2 X external antenna ports for 2.4 GHz ISA100 Wireless and WirelessHART field instruments 1 X grounding cable
Internal Connections	1 X 10/100 Mbps auto-negotiation Ethernet port
Environmental Ratings	IP66, IP67,G3 corrosion resistance per ANSI/ISA-S71.04-1985
Operating Temperature	-40 to +70° C (IECEx) -40 to +70° C (ATEX) -40 to +70° C (CSA)
Operating Humidity	0~95% non-condensing
Transportation and Storage Humidity	0~95% non-condensing
Mechanical Shock	4G- 5G Operational, 15 G Non-Operational
Data Rates and Modulations	Radio: 250 Kbps, DSSS/O-QPSK Wired: 10 / 100 Mbps Fast Ethernet
Frequency Band and Operating Channels	Unlicensed ISM Band (2.4 – 2.483 GHz) 13 DSSS channels for ISA100 Wireless and/or WirelessHART
Compliance	Radio Approvals FCC Part 15.247 Subparts B and C Canada – Industry Canada Method RSS-210, Issue 7 RSS-Gen, Issue 2 ICES-003, Issue 4 Australia and New Zealand – ACMA AS NZS 4268-2008 European Union – ETSI EN 300 328 V1.8.1 EN 301 489-17 V2.2.1 EN 301 489-1 V1.9.2 IEC61326-1, 2006 CE Mark R&TTE Directive 1999 / 5 / EC EMC Directive 2004 / 108 / EC LVD Directive 73 / 23 / EEC ATEX Directive 94 / 9 / EC Hazardous Environment Ratings FM: Class I, Division 2 Group A, B, C, D / Zone 2 Group IIC T4 CSA: Class I, Division 2, Group C, D; T4 Ex nA nC [ic] IIC T4 GcIECEx: Ex nA nC [ic] IIC T4 Gc ATEX: II 3G Ex nA nC [ic] IIC T4 Gc
Security	128-bit AES encryption

Quality of Service	Supported
Transmit Power (Maximum)	18 dBm
Receive Sensitivity (Typical)	-100 dBm @ 250 kbps
Network Interface	10/100 Mbps Ethernet, auto-sensing
Number of Supported ISA100 Wireless and WirelessHART Field Instruments	10 ISA100 Wireless or 8 WirelessHART Field Instruments at 0.5 second reporting rate OR 5 ISA100 Wireless and 4 WirelessHART Field Instruments at 0.5 second reporting rate 25 ISA100 Wireless or 25 WirelessHART Field Instruments at 1 second reporting rate OR 12 ISA100 Wireless and 12 WirelessHART Field Instruments at 1 second reporting rate 50 ISA100 Wireless or 50 WirelessHART Field Instruments at 2 seconds reporting rate OR 25 ISA100 Wireless and 25 WirelessHART Field Instruments at 2 seconds reporting rate80 ISA100 Wireless Field Instruments at 5 seconds or 80 WirelessHART Field Instruments at 4 seconds reporting rate OR 40 ISA100 Wireless and 40 WirelessHART Field Instruments at 5 seconds and 4 seconds reporting rate respectively 100 ISA100 Wireless Field Instruments at 10 seconds or slower or100 WirelessHART Field Instruments at 8 seconds or slower reporting rate OR 50 ISA100 Wireless and 50 WirelessHART Field Instruments at 10 seconds and 8 seconds or slower reporting rate respectively
Number of Supported Enraf FlexLine Radar Gauges / Wireless Field Interface (WFI)	13 Enraf FlexLine Radar Gauges / WFI
Maximum Number of Wireless Network Hops Between an Access Point and a Field Device	4 Hops
Warranty	1 Year
ECCN	5A002 ENC

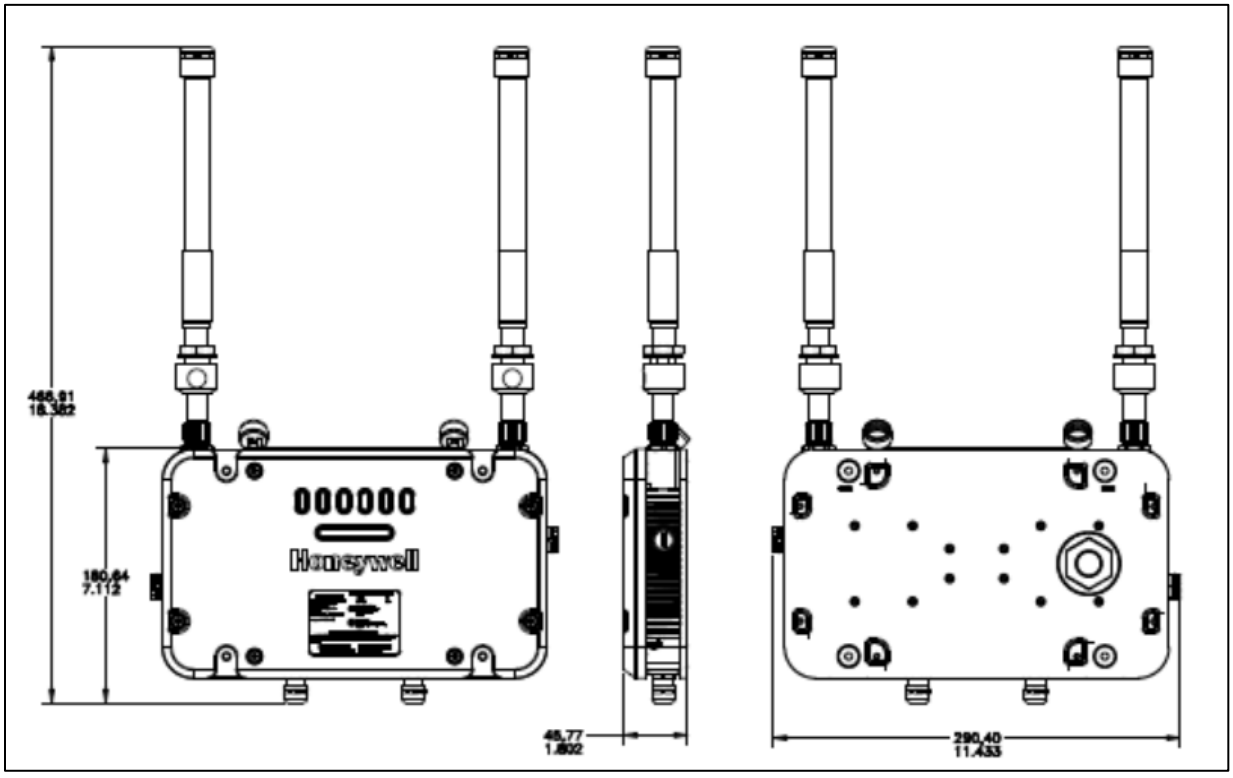
8.2 FDAP Technical Specification

Model Numbers	FDAP1 (Class 1 Div 1/Zone 0) FDAP2 (Class 1 Div 2/Zone 2)
Multiple Standards/Field Protocols	ISA100 Wireless and WirelessHART
Weight	3.86 kg (5.5 lbs)
Dimensions	216 x 170 x 86 mm (8.47 x 6.73 x 3.37 in)
Power	24 VDC +/- 10% at 2 Watts 90 – 264 VAC, 50/60 Hz
External Ports and Connections	2 X external antenna ports for 2.4 GHz ISA100 Wireless field instruments
Internal Connections	1 X 10/100 Mbps auto negotiation Ethernet port 1 X shielded power cable 1 X grounding cable
Environmental Ratings	IP66, G3 Corrosion resistance per ANSI/ISA-S71.04-1985, NEMA Type 4X (FM only)
Operating Temperature	FDAP1: -40 to +70 °C FDAP2: -40 to +60 °C
Transportation and Storage Temperature	-40 to +85 °C
Operating Humidity	0~100% non-condensing
Transportation and Storage Humidity	0~100% non-condensing
Mechanical Shock	4G
Data Rates and Modulations	Radio: 250 Kbps, DSSS/ O-QPSK Wire: 10/100 Mbps Fast Ethernet
Frequency Band and Operating Channels	Unlicensed ISM Band (2.4 – 2.483 GHz) 15 DSSS channels for ISA100 Wireless

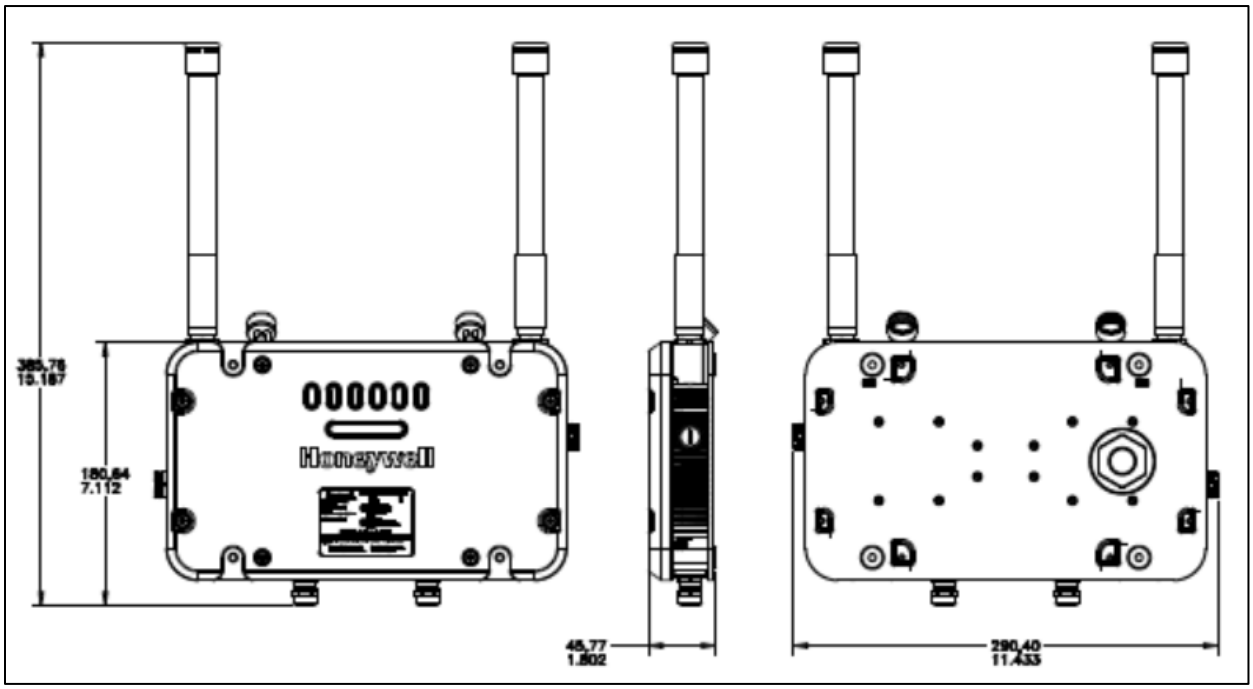
Compliance	Radio Approvals FCC Part 15.247 Subparts B and C Canada – Industry Canada Australia – ACMA AS NZS 4771-2000 Method RSS-210, Issue 7 RSS-Gen, Issue 2 ICES-003, Issue 4 European Union – ETSI EN 300 328 V1.7.1 EN 301 893 V1.4.1 EN 301 489-17 V1.2.1 EN 301 489-1 V1.6.1 IEC61326-1, 2005 CE Mark R&TTE Directive 1999/5/EC EMC Directive 2004/108/EC LVD Directive 73/23/EEC ATEX Directive 94/9/EC Hazardous Environment Ratings FDAP1 Model: IECEx: Ex ia IIB T4 FM: Class I, Division 1 Group C, D / Zone 0 Group IIB T4 FDAP2 Model: FM: Class I, Division 2 Group A, B, C, D / Zone 2 Group IIC T4
Security	128-bit AES encryption
Quality of Service	Supported
Transmit Power (maximum)	DSSS: 18 dBm
Receive Sensitivity (Typical)	DSSS (2.4 GHz): -95 dBm @ 250 kbps
Network Interface	10/100 Mbps Ethernet, autosensing
Number of Supported Enraf FlexLine Radar Gauges	FDAP as an access point (connected to a high speed backbone1): 13 Enraf FlexLine Radar Gauges FDAP as a router (routing data to another field device): 10 Honeywell Enraf FlexLine Radar Gauges with 1 second publication rate with input only channels 5 devices with 1 second publication rate with both input and output channels

Number of Supported SKF WVT Field Devices	FDAP as an access point (connected to a high speed backbone1): 15 Wireless Vibration Transmitter (WVT) Field Devices FDAP as a router (routing data to another field device): Number of Wireless Vibration Transmitter (WVT) Field Devices under FDAP as a router is 8
Maximum Number of Wireless Network Hops Between an Access Point and a Field Device	4 hops
Warranty	1 year
ECCN	5A002 ENC

8.1 FDAP Gen3 Dimension Drawing

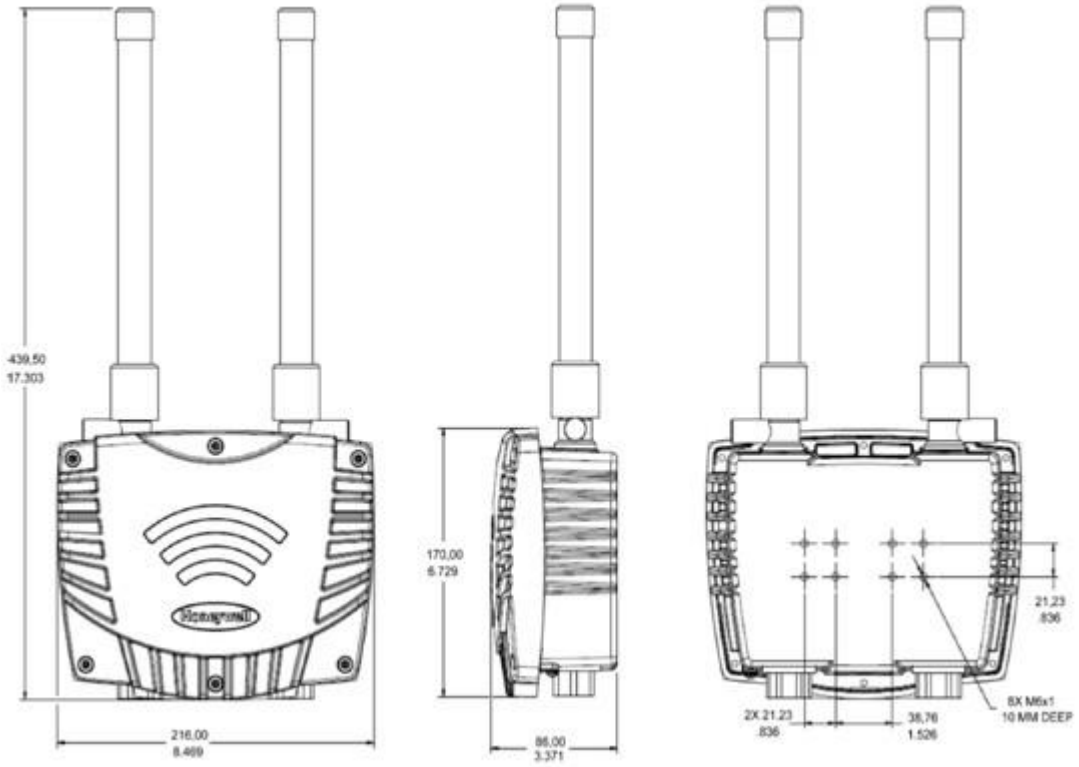


FDAP GEN3 WITH LIGHTENING SURGE ARRESTOR



FDAP GEN3 WITHOUT LIGHTENING SURGE ARRESTOR

8.2 FDAP Dimension Drawing



8.3 FDAP GEN3 IS Control Drawing

TBD

8.4 FDAP IS Control Drawing (51202683)

PRE REL		
ISS	REVISION & DATE	APPD
B	6/27/2014	AT

OneWireless FDAP
IECEx & FM APPROVED INTRINSICALLY SAFE
INSTALLATION CONTROL DRAWING

1. Intrinsically safe installation shall be in accordance with
   a. FM (USA): ANSI/NFPA 70, NEC® Articles 504 and 505.
   b. IECEx: Requirements of IEC 60079-14, 12.3 (See also 5.2.4).
2. ENTITY approved equipment shall be installed in accordance with the manufacturer's Intrinsic Safety Control Drawing.
3. The Intrinsic Safety ENTITY concept allows the interconnection of two ENTITY Approved Intrinsically safe devices with ENTITY parameters not specifically examined in combination as a system when:
   Uo, Voc, (or Vt in the USA) ≤ Ui or Vmax; Io, Isc, (or It in the USA) ≤ Ii or Imax; Ca or Co ≥ Ci + Ccable; La or Lo ≥ Li + Lcable; Po ≤ Pi. Where two separate barrier channels are required, one dual-channel or two single-channel barriers may be used, where in either case, both channels have been Certified for use together with combined entity parameters that meet the above equations.
4. System Entity Parameters:
   FDAP1: Vmax ≥ Voc or Uo, Imax ≥ Isc or Io; Pi ≥ Po.
   FDAP1: Ci + Ccable ≤ Control Apparatus Ca.
   FDAP1: Li + Lcable ≤ Control Apparatus La.
5. When the electrical parameters of the cable are unknown, the following values may be used:
   Capacitance: 197pF/m (60 pF/ft)
   Inductance: 0.66µH/m (0.020µH/ft).
6. Control equipment that is connected to Associated Equipment must not use or generate more than 250 V.
7. Associated equipment must be FM or IECEx (depending on location) listed. Associated equipment may be installed in a Class I, Division 2 or Zone 2 Hazardous (Classified) location if so approved.
8. Non-Galvanically isolated equipment (grounded Zener Barriers) must be connected to a suitable ground electrode per:
   a. FM (USA): NFPA 70, Article 504 and 505. The resistance of the ground path must be less than 1.0 ohm.
   b. IECEx: Requirements of IEC 60079-14, 12.2.4.
9. Intrinsically Safe DIVISION 1/ Zone 0 WARNING: SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR USE IN HAZARDOUS LOCATIONS.
10. Division 2/ Zone 2: WARNING: DO NOT OPEN WHEN AN EXPLOSIVE GAS ATMOSPHERE IS PRESENT.
11. NO REVISION OF THIS CONTROL DRAWING IS PERMITTED WITHOUT AUTHORIZATION FROM THE AGENCIES listed.

DRAWN			Honeywell
CHECKED			FM & IECEx CONTROL DRAWING ONEWIRELESS FDAP DIVISIONS 1 / ZONE 0
DEV ENG			
MFG ENG			
QA ENG			
TOLERANCE UNLESS NOTED		A/A4	51202683
MASTER FILE TYPE: MS WORD	ANGULAR DIMENSION	SCALE: None	USED ON / SH. 1 OF 2

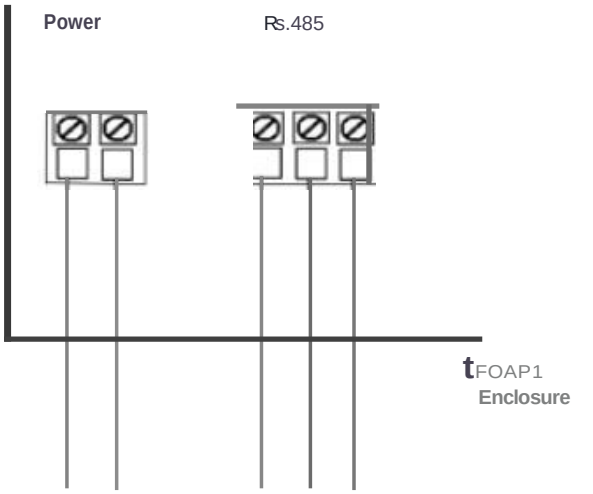
IECEx & FM APPROVED INTRINSICALLY SAFE INSTALLATION CONTROL DRAWING

MODEL: FDAPl

HAZARDOUS CLASSIFIED LOCATION

FM: CLASS I DIV 1 GROUPS C,D,T4;
CLASS 1, ZONE 0, El</AExi GROUP 1 IB,T4;
AMBIENT LIMITS: 40•C STa S 75•C

IECEx: Exi 1 18T4; AMBIENT LIMITS: -40'C STa S 7o'C



Vmaxi\J 1 = WV
Im'°"" = 150mA
Pmax1Pi • 1W
Cl = OuF
U•52 uH

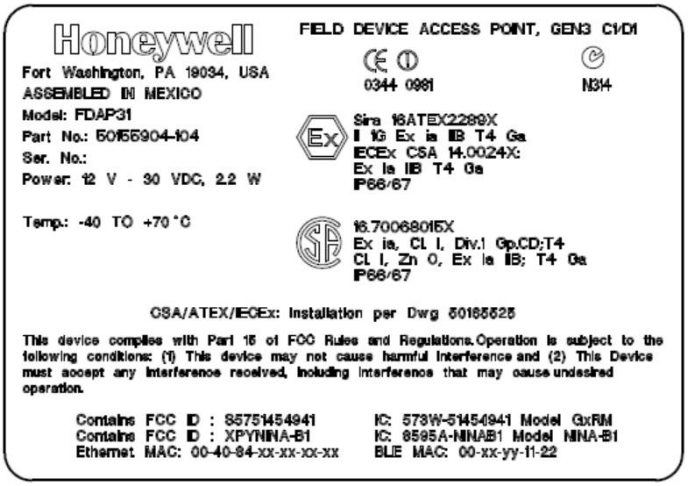
Voc/Uo = 5 83\V
IGIt> • 150mA
Po •261mW
Co = 95uF
Lo = 15 9 uH

Noto: RS485 enllly para!Nlters are applicable to FM Aj>pfOllal only

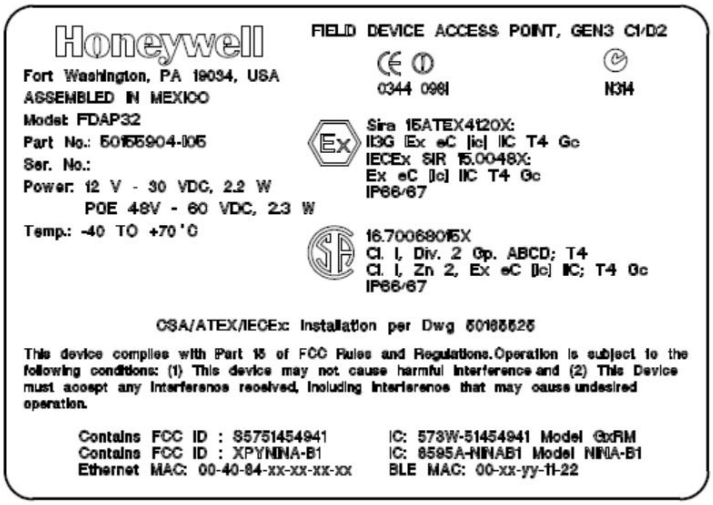
Note: Etherne.t connections ace not a.Jlowed in intrinsic sUety insta.Jbtion:s

Honeywell	4	**51202683**
	SCALE: None | REV B DATE 6127114	SH.2 of 2

8.5 FDAP GEN3 Label Drawing



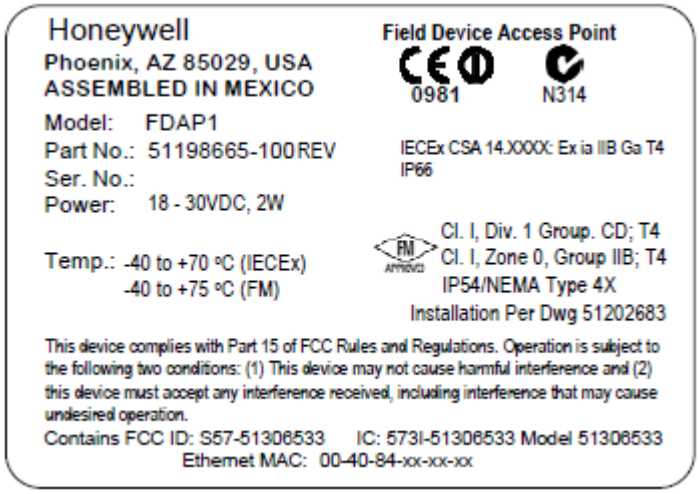
FDAP GEN3 C1/D1



FDAP GEN3 C1/D2

The labels shown above are for reference purposes only.

8.6 FDAP Label Drawing



The labels shown above are for reference purposes only.

9 Notices

CAUTION

Take precautions against electrostatic discharge to prevent damaging the sensor module.

WARNING

POTENTIAL ELECTROSTATIC CHARGING HAZARD

The externally mounted antenna has a surface resistivity greater than 1Gohm per square. When the FDAP is installed in potentially hazardous locations care should be taken not to electro-statically charge the surface of the antenna shroud by rubbing the surface with a cloth, or cleaning the surface with a solvent. If electro-statically charged, discharge of the antenna to a person or a tool could possibly ignite a surrounding hazardous atmosphere.

Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Third-party licenses

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third_party_licenses on the media containing the product, or at https://www.honeywell.com/en-us/privacy-statement

9.1 Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions support website at:

http://www.honeywellprocess.com/support

If you have comments about Honeywell Process Solutions documentation, send your feedback to:

hpsdocs@honeywell.com

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

9.2 How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the

instructions at: https://honeywell.com/pages/vulnerabilityreporting.aspx

Submit the requested information to Honeywell using one of the following methods:

- Send an email to

  security@honeywell.com. or
- Contact your local Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts”
  section of this document.