Honeywell

ONEWIRELESS

RELEASE 323

Wireless Device Manager User's Guide

OWDOC-X254-en-323A June 2022

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.

Copyright 2022- Honeywell International Sàrl

Table of contents

ABOUT THIS GUIDE	9
Intended audience	9
Prerequisite skills	9
Revision History	9
Required Honeywell documentation	9
INTRODUCTION	11
Overview of Wireless Device Manager	11
About the OneWireless user interface	17
Overview of the OneWireless Network setup	17
GETTING STARTED WITH WDM	18
Mounting WDMX	18
Mounting WDMY	22
Connecting WDM and other OneWireless components	27
Establishing communication between OneWireless Network and Experion system	29
Configuring network properties on the computer	
Logging on to OneWireless user interface	31
Configuring WDM using the First Time Configuration Wizard	31
To configure WDM using the First Time Configuration Wizard	
Use Default Configuration	32
Manual Configuration Wizard	36
Restore from Backup	43
Understanding the OneWireless user interface	47
Dashboard parameters	48
Left Navigation Menu bar	54
Manage Devices	62
Property Panel	65
Understand the device icons	66
Status bar	72
Notification List	72
About map view	73
Installing the WDM license	
Prerequisites	
To install a WDM license	
Property panel of WDM, ISA100 Wireless & WirelessHART devices	81

WDM	81
WirelessHART Devices	93
ISA100 Wireless Devices	101
CONFIGURATION	109
Loading the Device Description file	109
Loading the Certificate	109
Provisioning	112
To provision the access points using over-the-air provisioning method	112
To provision the ISA100 Devices using over-the-air provisioning method	117
To provision line-powered FDAP routers/ field devices using over-the-air provisioning method	121
Provision the ISA100/WirelessHART devices using Common Join Key	125
Provision WirelessHART devices using Over-The-Air (RE)-Provisioning method	127
Remove Device	129
Android based provisioning for OneWireless Network	131
Install Android Provisioning Device Application from WDM	131
Application Installation	132
Android device specifications	133
Provisioning	134
ISA100 BLE	134
ISA100 IR Devices	142
WirelessHART Devices	144
Configuring the WDM	154
Configure default routing policy	154
Configure key rotation period	156
Configure Radio frequency Channel	156
Configuring the WDM redundancy	158
Configure WDM redundancy from the First Time Configuration Wizard	161
Configure WDM redundancy from the WDM Properties panel	161
Monitoring the WDM redundancy status	166
Monitor the redundancy status from the WDM Property panel	166
Perform redundancy-specific operations	171
Configuring device communication redundancy	173
Property panel - device communication redundancy	173
Report	175
Configure field devices	175
Configure field device properties	175

Configuring routing assignment	
Configure publication rate for ISA100 Wireless devices	
Configure publication rate for WirelessHART devices	
Calibrate Honeywell XYR6000 field devices	
Configuring field device channels for ISA100 Wireless devices	
Configure Mode and Scale	
Add channels to publication groups	
Configure channel instantiation	
Remove channels from publication groups	
Delete (un-instantiate) channels	
Enable Device Network System (DNS)	
To enable Device Network System (DNS) in Process Control Network (PCN)	
To enable Device Network System (DNS) in Special Interface Network (SIN)	
Enable Single Sign On	
Adding notes for devices	
OPERATIONS	193
Setting up the monitoring area	
Configure site maps	
Position the devices on the map	
Change the default map for a device	
Remove device from the map	
Configuring Connection Quality Options	
Verifying connectivity using maps	
Configuring alerts for Honeywell ISA100 Wireless field devices	
Monitoring the network and the devices	
Alarm and event management	
Understand alarms and events	
Monitor alarms and events	219
Viewing time synchronization parameters	
Viewing license agreement files	
Configuring radio power level	
ACTIVATE PROCESS CONTROL INTERFACES	
Establishing connection between WDM and external interfaces	
Serial interface connection	
Activating HART in OneWireless Network	
Configure HART serial interface	
Configure HART Ethernet/UDP interface	

Configure HART/IP interface	231
Monitor performance of HART interface	233
Monitor field devices from an asset management system	233
Activating Modbus in OneWireless Network	238
Enable Modbus in OneWireless Network	239
Configure the parameters in the Modbus tables	247
Import/Export Modbus register configuration	249
Activating OPC in OneWireless Network	251
Enable OPC interface	251
Configure OPC UA client system	251
Configure OPC DA client system	256
Configuring OPC communication using Experion SCADA and OPC Validator with mul WDMs in the same network	
Monitor OPC interface statistics	267
Monitor OPC interface for multiple WDMs	268
About integrating OneWireless Network with Experion using the CDA interface	272
Activating GCI interface on the WDM	274
To activate GCI interface on the WDM	274
Activate ENRAF Ethernet UDP interface on the OneWireless user interface	275
To activate ENRAF Ethernet/UDP interface on the OneWireless user interface	275
Configure ENRAF serial interface	276
Monitor performance of ENRAF interface	276
Activate MQTT in OneWireless Network	277
Enable MQTT interface	277
Configure MQTT Server	279
Configure MQTT Topics	283
Monitoring MQTT statistics	
ADMINISTRATION	289
Administering users	
About users and user roles	
Create user accounts	291
Edit user account	291
Delete user account	292
Change password	292
Reset password	292
Change user role	293
Manage user roles	293
Downloading support software	294

To download support software:	294
Upgrading device firmware	
Upgrading the WDM firmware	297
Upgrading the FDAP/access point firmware	299
Upgrading the ISA100 Wireless field device firmware	
Configuring system configuration backup	
About system configuration backup	
Configure manual backup	
Configure automatic backup	
Restoring the system configuration from a backup	
CONTROL OVER WIRELESS USING ONEWIRELESS	306
Deployment Topology:	
Topology for 1 sec or faster loops	
Topology for 4 sec or above loops	
Sending control commands to WirelessHART devices	
Control over wireless using OneWireless integrated with Experion	
PID - Profit Loop	313
Wireless control loop example using PID-PL in Experion	
Control over wireless using both input and output transmitters are wireless	316
Tank Level Control Over Wireless (Test Results)	
ISA SECURE LEVEL1 CERTIFICATION	
SECURE COMMUNICATIONS	319
TROUBLESHOOTING AND MAINTENANCE	320
Replacing devices	
Considerations	
Prerequisites	320
To replace devices:	320
Removing devices	
Considerations	
To remove a device:	
Resetting/removing WDM	
Delete PDA Devices	324
Restarting devices	
To restart a WDM:	326
To restart FDAP/Access Point/field device	326
About NTP status	
To view the NTP Status Display:	

NOTICES	337
TERMS AND DEFINITIONS	334
Reporting anomalies	
Exporting and saving system logs	
Generating reports	
NTP server reachable	328
NTP server unreachable	328

About this guide

This document describes the procedures to provision, configure, operate, and monitor ISA100 Wireless and Wireless HART field devices using the Wireless Device Manager.

Intended audience

This guide is intended for people who are responsible for planning, configuring, administering, and operating the OneWireless Network.

Prerequisite skills

It is assumed that you are familiar with the operation of the OneWireless Network.

Revision History

Revision	Supported Release	Date	Description
А	323	May 2022	Initial release of the document.

Required Honeywell documentation

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

Document	Description
OneWireless Network Planning	This guide provides information about planning, designing,
and Installation Guide	and setting up the OneWireless network using WDM,
(OWDOC-X253-en)	FDAPs, PCAP and field devices.
OneWireless Release Notes (OWDOC-X252-en)	This document provides information about the new functions and features in OneWireless.
OneWireless Wireless LAN	This guide provides information about planning, designing,
Controller Configuration Guide	setting up, and configuring a OneWireless network using
(OWDOC-X255-en)	WDM, FDAPs, PCAP, Cisco 1552S APs, and field devices.

OneWireless Process Control Access Point (PCAP) User Guide (OWDOC-X718-en)	This guide describes the procedures to install, configure, and operate Process Control Access Point (PCAP).
OneWireless Field Device Access Point (FDAP) User's Guide (OWDOC-X256-en)	This document describes the procedures to install, configure, and operate Field Device Access Point (FDAP).
OneWireless Migration User's Guide (OWDOC-X258-en)	This document assists you in understanding, planning, and performing the migration of the OneWireless Network.
OneWireless Parameter Reference Dictionary (OWDOC-X260-en)	This guide provides information about the parameters associated with OneWireless devices.
Wireless Device Manager Secure Communication Guide (OWDOC-X584-en)	This document provides information about installation, configuration, and setup of Secure Communications for a WDM or a system including a WDM to deploy Honeywell Secure Communications.

You can download Honeywell documentation from <u>https://process.honeywell.com</u> website.

Introduction

Overview of Wireless Device Manager

What is Wireless Device Manager?

The Wireless Device Manager (WDM) allows you to design, commission, configure, and monitor wireless network. You can also configure and commission the associated field devices from a centralized location. The WDM acts as a network gateway enabling third-party applications to communicate with field devices.

What is new in OneWireless R323?

- FDAP Gen3 Anchor hardware introduction with RTLS only capability
- Tag hardware introduction
- MQTT interface support
- Safety Watch integration
- Security Improvements
- Customer PAR fixes

Functions of WDM

The WDM performs the following roles and functions.

Role	Functions
Gateway	Acts as the communication interface for supported field devices.
	Provides wireless field device data cache for the OneWireless user interface
	and the external control systems.
	Allows communication between wired HART devices with OneWireless
	Adapter and the asset management system.
System Manager	Manages field device network and devices.
	Establishes communication between the devices.
	Performs policy-based control of the network runtime configuration.
	Monitors and reports the communication configuration, performance, and
	operational status.
Security Manager	Provides security keys to the Provisioning handheld devices that are used
	for issuing security keys to the field devices.
	Authenticates the provisioning data with which a field device tries to join the
	network.

Table. 1. WDM roles and functions

	Initiates key rotation for the field devices.
	Maintains session key for each device in the network.

Hardware description of WDM

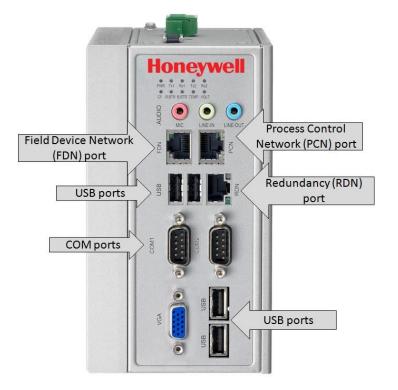


Fig. 1. WDMX hardware

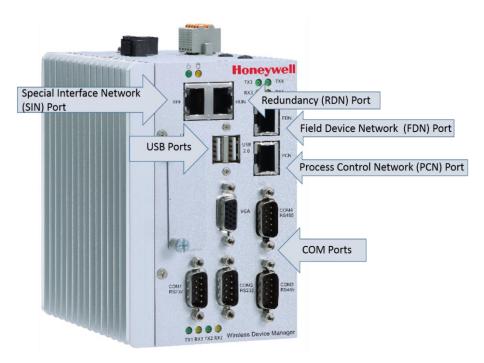


Fig. 2. WDMY hardware

Port name	Description	
Field Device Network (FDN)	Used for connecting the WDM with FDAPs/Access points.	
port	Attention	
	The FDN port is also known as the "FIN – Field Instrument Network" port in some WDMs.	
Process Control Network (PCN) port	Used for connecting monitoring clients and external controllers.	
Special Interface Network (SIN) port (only for WDMY)	Used for connecting 3rd party client applications existing on different network than a DCS network such as Vibration Analyzer tools etc. The client application can talk to WDM over SIN port using any of the existing interface in WDM other than CDA, collect required data from wireless transmitters.	
Attention The WDM contains an emb	edded firewall that restricts the data routing between the two network ports.	
COM ports	Used for connecting to devices such as modems, terminals and various peripherals.	
	• WDMS — Has three serial ports, two of which can be used as standard RS232 ports and the third port can be used as an RS485 port.	
	• WDMX — Has two serial ports, one of which can be used as standard RS232 port and the other can be used as an RS485 port.	
	• WDMY – Has four serial ports, two of which can be used as standard RS232 ports and the remaining ports can be used as RS485 ports.	
USB ports	Used for connecting USB flash drives. In addition, USB ports are used for connecting the PDA or provisioning device.	
	 WDMX – Has four USB ports WDMY – Has two USB ports 	
RDN (redundancy) port	WDM Virtual (WDMX/WDMY/WDMV)— Supports redundancy, implements redundant private path over RDN port, which is connected to the partner WDM through a crossover cable.	

Table. 2.Description of WDM ports

For more information about the technical specifications of the WDM models, see the specifications document available in the Honeywell Process Solutions website.

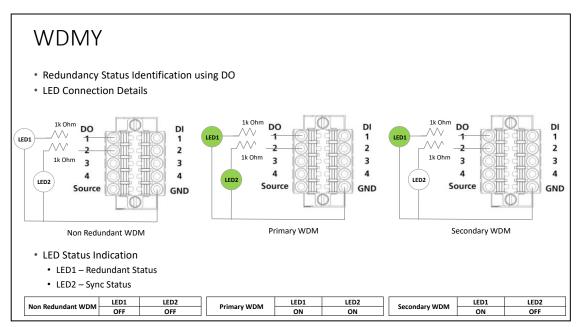
LED Behavior of WDMY

The following table describes the LED indicators located on the front panel of WDMY.

LED name	Status	Function
Power U	Green	Power is on and the computer is functioning normally
Power	Off	Power is off
Storage 1 (CFast)	Yellow	Blinking: Data is being saved or retrieved
0	Off	No data transmission
LAN 1/2/3/4	Green	Steady on: 100 Mbps Ethernet link
		Blinking: Data is being transmitted
	Yellow	Steady on: 1000 Mbps Ethernet link
		Blinking: Data is being transmitted
	Off	10 Mbps Ethernet link or LAN is not connected
Tx 1/2/3/4	Green	Blinking: Data is being transmitted
	Off	No connection
Rx 1/2/3/4	Yellow	Blinking: Data is being received
	Off	No connection

Table. 3. LED indicators

Redundancy Status Identification of WDMY



The following image explains the redundancy status identification of WDMY.

About the OneWireless user interface

The WDM provides an HTTP/HTML5-based user interface for configuring and monitoring all the devices connected to a network. To start managing the wireless field device network, you first need to configure the WDM. When you access the OneWireless user interface for the first time, the WDM needs to be configured using the First Time Configuration Wizard. After that, you can use the user interface for provisioning, commissioning, configuring, monitoring, and decommissioning Process Control Access Points (PCAP), Field Device Access Points (FDAP), Access Points, and field devices.

In addition, the user interface can be used for performing the following tasks.

- Network maintenance
- Security configuration
- Device configuration and maintenance
- Operator activities

The following are some of the benefits of OneWireless user interface.

- Is simple and easy to use
- Reduces commissioning time
- Reduces security threats with secured HTTPS-based user interface
- Provides simultaneous access to WDM using multiple logon sessions
- Supports device diagnostics summary display and related reports capability
- Supports effective node failure diagnosis
- Simplifies integration of the wireless field devices with process control interfaces
- Defines the application as an intranet application which trusts the system in a controlled network.

Overview of the OneWireless Network setup

Set up the OneWireless Network in the following sequence.

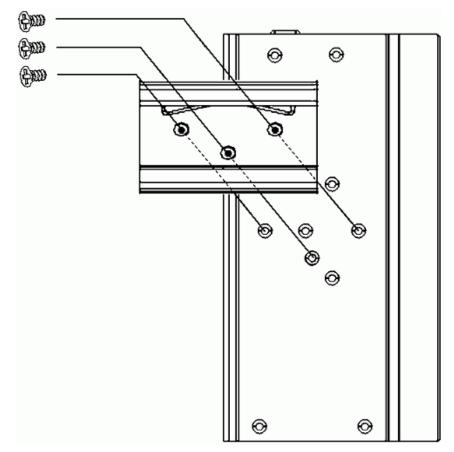
- 1. Install and configure the WDM.
- 2. Power up and provision all the Access Points (PCAP, FDAP2, FDAP Gen3).
- 3. Power up and provision all the FDAP routers.
- 4. Power up and provision all the field devices.

Getting started with WDM

Mounting WDMX

Mounting WDMX on DIN-Rail

1. Screw the provided DIN-Rail Kit onto the rear side of the WDMX as illustrated in the following figure.

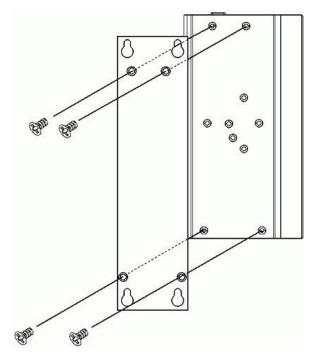


- 2. Hang the WDMX onto the DIN-Rail with an angle of inclination about 30 degrees.
- 3. Lower the WDMX straight down to slide over the Rail smoothly.

To remove the WDMX from the Rail, push down on the top of the WDMX, and then pull the bottom of the WDMX away from the Rail to disengage ATTENTION smoothly.

Mounting WDMX on a flat surface

1. Screw the provided Wall Mounting Kit onto the rear side of the WDMX as illustrated in the following figure.



2. Mount the WDMX on the wall using the 2 pairs of mounting holes.

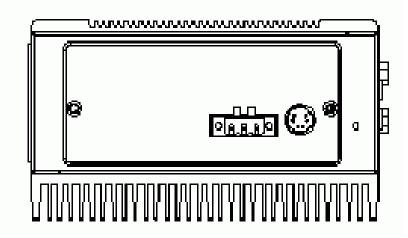


Fig. 3. Top view of the WDMX

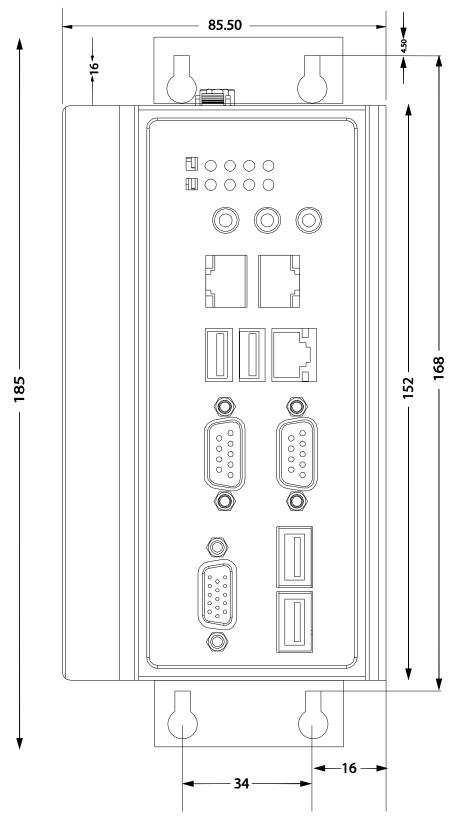


Fig. 4. Rear view of the WDMX

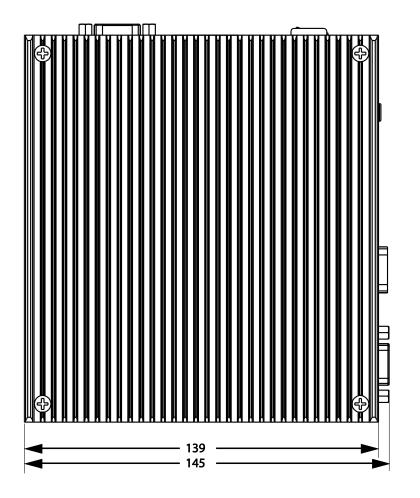


Fig. 5. Top view of the WDMX

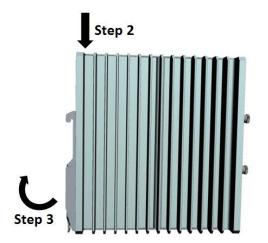
Mounting WDMY

Mounting WDMY on DIN-Rail

1. Use four screws included with the kit to attach the DIN-rail mounting bracket to the WDMY's rear panel and tighten the screws to secure the bracket to the WDMY as illustrated in the following figure.



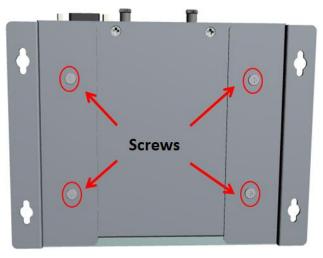
2. Insert the top of the DIN rail into the slot just below the upper hook of the DIN-rail mounting kit.



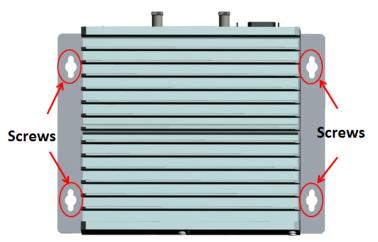
3. Press the WDMY towards the DIN-rail until it snaps into place.

Mounting WDMY on a flat surface

1. Use two screws for each bracket and attach the brackets to the rear of the WDMY as illustrated in the following figure.



2. Use two screws per side to attach the WDMY to a wall or cabinet.



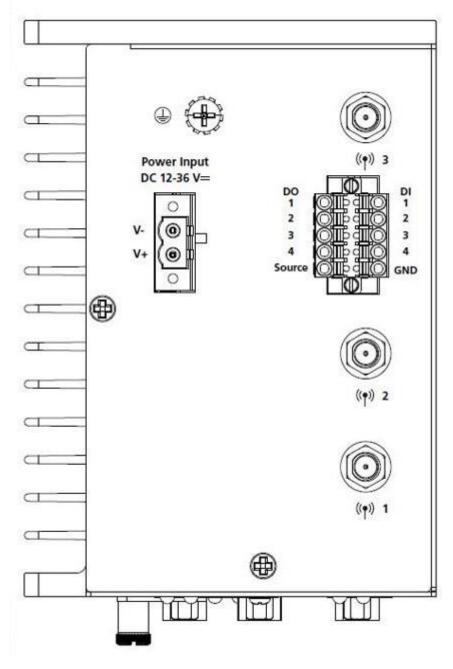


Fig. 6. Top view of the WDM

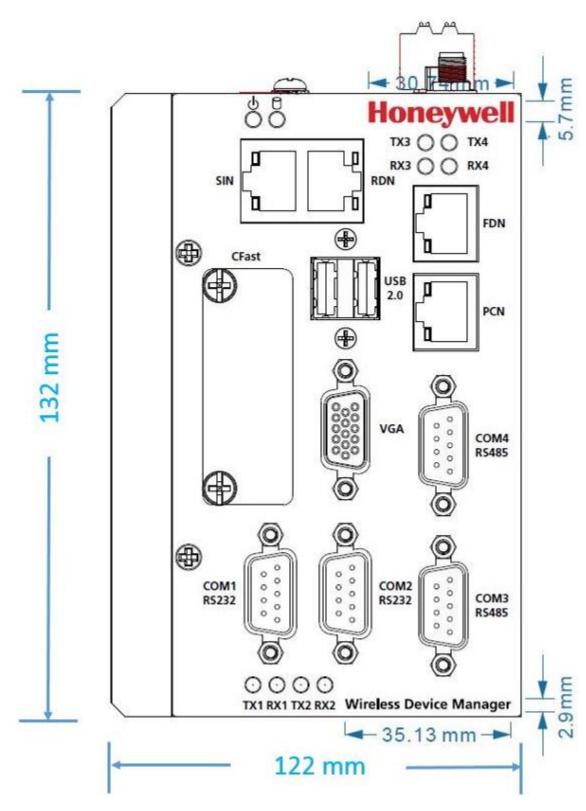


Fig. 7. Front view of the WDM

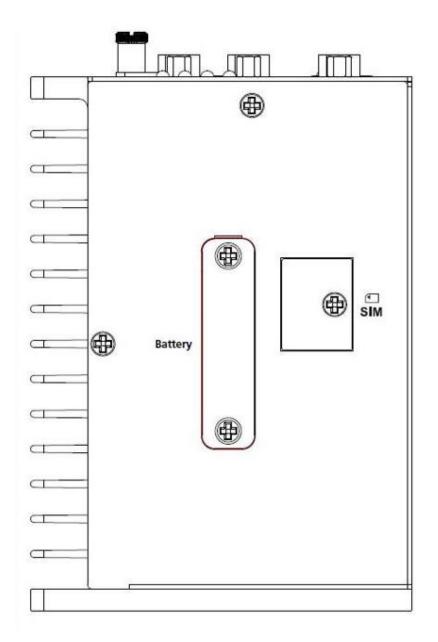


Fig. 8. Bottom view of the WDM

Connecting WDM and other OneWireless components

For more information on this section, see the OneWireless Wireless LAN Controller Configuration Guide (OWDOC-X255-en).

Prerequisites

- Ensure that you provide the maximum power requirement of 48 W (10 ~ 36 VDC).
- Ensure that you have an FDN Ethernet switch when connecting multiple FDAPs/PCAPs/Access Points to the WDM.
- Ensure that you have Ethernet cables required for connecting the devices.
- Ensure that you have redundancy Ethernet cable for connecting the devices.
- Identify the location for mounting the devices.

Establish physical connection between WDM and Cisco 1552S Access Point

- 1. Connect the Ethernet cable from the Ethernet port on the Cisco 1552S Access Point (AP) to the non-trunk port on the Cisco switch.
- 2. Connect the Ethernet cable from the FDN port on the WDM to the non-trunk port on the Cisco Switch.

For more information about installing a Cisco 1552S AP, see the respective Cisco user documentation.

Establish physical connection between WDM and FDAP/PCAP

Connect the Ethernet cable from the FDAP/PCAP to the FDN port on the WDM. OR

If you are using multiple FDAPs, you can use an Ethernet switch to connect the FDAPs to the WDM.

For more information about installing and setting up the FDAP, see the Field Device Access Point User's Guide.

For more information about installing and setting up the PCAP, see the Process Control Access Point User's Guide.

WDM has the capability to act as the DHCP Server for the Field Device Network. However, if you are configuring an external DHCP Server for the network, ensure you connect the DHCP Server to the switch during this stage.

Establish physical connection between WDM and a computer

- 1. Connect the WDM power cable to a DC power supply.
- 2. Connect the Ethernet cable from the computer's network port to the PCN port on the WDM or to a switch connected to the PCN port.

Power up the components

After establishing connection with the WDM, power up the WDM, the FDAPs, PCAPs and the Access Points.



When powering up the WDM, if a duplicate IP address is configured on either the PCN port or the FDN port, the WDM startup operation ends, and ATTENTION no IP address is assigned. To recover, you must resolve the duplicate IP address from the network.

NOTE The malicious operation of critical Wireless device manager and access points result in system shutdown, starting the system unexpected system start up or restart, or otherwise impact process control. The critical Wireless device manager includes network switches for I/O network and host communication network, I/O Modules, power supply modules, and simulator. Critical OneWireless modules Include: Wireless Device Manager, Field Device Access Point, Access Point, WirelessHART field devices, Provisioning Device handheld, Switches. For maximum security, the Wireless device manager must be placed in a cabinet or locked closet to protect against unauthorized access to the critical modules.	

Establishing communication between OneWireless Network and Experion system

To establish communication between OneWireless Network and Experion system, connect an Ethernet cable from the PCN port of the WDM to the top-level yellow Level–2 switch port on the Experion network. If you have a secondary WDM, connect an Ethernet cable from the PCN port of the secondary WDM to the top-level green Level-2 switch port on the Experion network.

Ensure that the Experion Level-2 switch port where the WDM is connected, is set to auto speed, auto duplex.

ATTENTION Ensure that the Experion Level–2 switch port where the WDM is connected, has spanning-tree port fast enabled

Configuring network properties on the computer

Before migrating, you must configure the network properties on your computer to use a different IP subnet. This is because you cannot use the default FDN IP address of WDM (192.168.0.1) for migration.

Prerequisites

A desktop or a laptop computer for accessing the OneWireless user interface.



The steps in the following procedure are specific to Microsoft Windows XP operating system.

To configure network properties on the computer

- 1. Perform one of the following steps to open the Network Connections dialog box.
 - Choose Start > Settings > Network Connections. Or
 - Choose Start > Control Panel > Network Connections.
- 2. Right-click the network port connected to the WDM and click Properties.
- 3. On the **General** tab, select **Internet Protocol (TCP/IP)** check box, and then click **Properties**.



Note down the current settings in Internet Protocol (TCP/IP) Properties so that, if necessary, you can return to their original values.

4. Configure the **IP address** and the **Subnet mask** as 192.168.0.x and 255.255.255.0 respectively.

Do no 192.1

Do not configure the computer with the default IP address of the WDM, 192.168.0.1.

- 5. Click OK to close the Internet Protocol (TCP/IP) Properties dialog box.
- 6. On the General tab, click Configure.
- 7. Click the Advanced tab and then in the Property list, click Speed & Duplex.
- 8. In the Value list, click Auto and then click OK.
- 9. Click OK and close all the open dialog boxes.

You must turn on a single WDM at a time, at the default address because the second WDM removes itself from the network if its duplicate address is detected. The removed WDM does not recover unless power- cycled.

Logging on to OneWireless user interface

Prerequisites

- One of the following recommended Web browsers must be installed on the computer.
 - Mozilla Firefox 82.0.2 and above
 - Edge 86.0.622.38 and above
 - Google chrome 86.0.42 and above
- Honeywell recommends a browser resolution of 1280 X 1024. Any resolution is supported but it may be necessary to navigate scrollbars or adjust zoom levels to view the entire interface.

If you are using Internet Explorer, on the **Tools** menu, click **Internet Options**, click the **Advanced** tab, clear **Do not save encrypted pages to disk** check box in the **Security** area, and then click **OK**. (This is the default Internet Explorer setting.)

Perform the following steps to log on to the OneWireless user interface.

To log on to OneWireless user interface

1. Open the Web browser and type the URL for the WDM in the address bar.

If you are logging on to the user interface for the first time from the PCN side of the network, use the default<u>address, https://192.168.1.1</u> for logging on to the user interface. If you have connected to FDN side of the network, you must use the IP address 192.168.0.1.

- 2. If a security warning appears, confirm or allow the security exception.
- 3. In the **User ID** and **Password** fields, type the user name and password, and then click **Login**.

Configuring WDM using the First Time Configuration Wizard

After installing the WDM, you need to configure the WDM to enable it to function in the OneWireless Network. The First Time Configuration Wizard guides you through the initial configuration of the WDM. The First Time Configuration Wizard appears only when you log on to the OneWireless user interface for the first time or after the WDM is deleted (returning to factory defaults).

Considerations

The following are some of the network configuration rules that you must follow while configuring the network properties.

- FDN and PCN must be on separate subnets.
- FDN IP address must be outside the FDAP IP address range.
- FDN subnet mask must include FDN IP address and FDAP IP address range.

• Default PCN gateway must be on the same subnet as PCN.



If you are performing a migration, skip this section and proceed with the tasks available in the OneWireless Migration User's Guide.

To configure WDM using the First Time Configuration Wizard

Use Default Configuration

All the settings is configured with default values in this option.

- Log on to the OneWireless user interface using the default User Name and Password. The First Time Configuration Wizard appears.
- 2. On the Welcome page of the First Time Configuration Wizard, select **Use Default Configuration** and click **Next**.



	Honeywell					
	Welcome to OneWireless					
administrator Asministrator This wizard will guide you through the steps necessary to set up your new OneWireless System.						
	Choose the type of Configuration					
Use Default Configuration This option will automatically configure the Windess Device Manager using default settings.	Manual Configuration Wizard This option will allowyou to configure the Wireless Device Manager step by step.	Restore From Backup This option will allow you to canfigure the Wireless Device Manager from a previous backup.				
		NEXT				

3. Provide **Tag Name, Country Code, Description** in the Wireless device manager settings page and click **Next**.

		neywell	
Wireless Device Manager Edit WDM identification & m	Settings Administ	cally Configured Setup ater Information lange the default username and password	Configuration Summary Summary of all configurations
Manager within OneWireless. This nar on external interfaces such as OPC.	the unique name used to identify your Wireless Device ne may also be used to identify your Wireless Device Manager		eck box to configure this Wireless Device Manager as Managers. If an incornect partner PCV IP address is
Tag Name* Country Code wdm1 UNITED STATES (840) ~ Description		Enable Redundancy for WDM	Redundancy Role
Indicates required fields			BACK

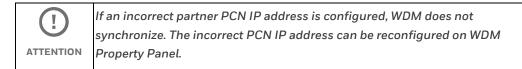
The **Tag Name** is the unique name that is used to identify the WDM. It can be up to 16 characters long and must begin with an alphabetic character. Do not use special characters in the Tag Name ";" underscore is the only acceptable character. After completing the initial configuration, you cannot change the WDM name.

The **Description** can be up to 255 characters long.

- 4. To configure redundant WDM, under **Redundancy Configuration**, configure the following:
 - a. Select Enable redundancy for this Wireless Device Manager check box.
 - **b.** Click the Redundancy Role, as required. You can select either Primary or Secondary option depending on the redundancy role.

() ATTENTION	Some of the settings may be disabled while configuring Secondary WDM as it follows the settings from the Primary WDM.
(i) TIP	When redundancy is enabled, the primary WDM is assigned physical ID A and the secondary WDM is assigned physical ID B. The physical IDs are displayed in the UI during normal operation. Tagging the physical hardware with matching labels makes it easy to distinguish the WDMs later.
ATTENTION	If you have selected the Redundancy Role as Secondary in the Wireless Device Manager Settings page, then the Location Settings page options are disabled.

5. Under Location, select the Country Code. The country code is used to define any location-specific settings within the OneWireless Network. For example, radio frequency options are location dependent and vary depending on the country code settings. After completing the first time configuration, you cannot modify the Country Code.



6. The **Administrator Information** page appears. Provide the Username, password and click **Next**.

	Honeyv	vell			
	Automatically Configu	ed Setup			
Wireless Device Manager Settings Edit WDM identification & redundancy Config	Administrator Information You can change the defaultu	ername and password	Configuration Summary Summary of all configurations		
Administrator Name & Password	nistrator. You can change the default user name in the First Time Co	-Francisco Wenned Hamming			
	issinator, fou can change the default user hands in the First Time up between 1 and 32 characters and can not contain space or a colon.				
Administrator Name	New Password *		Confirm Password	4	
		ø		ø	

7. You can view the details in **Configuration Summary** page with default values.

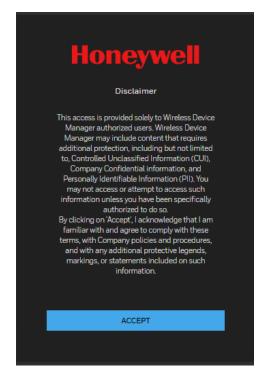
	Hon	eywell		
	Automatical	ly Configured Setup		
Wireless Device Manager Settings Edit WDM identification & redundancy Configuration	Administrato You can chang	r Information e the default username and password	Configuration Summary of	n Summary Il configurations
WDM Identification Tag Name Discription wdm1		Network ID ISA100 WHART 2 102	Field Device Network (FDN)	Subnet Mask 255.255.255.0
Redundancy Enable Redundancy Role Par No -	tner PCN IP address	Location Country Code UNITED STATES (840)	Enable DHCP Server Yes Access Point IP Address From 192168.0.101	To 192 168 0 200
	a Reference			
•			BACK	NEXT

			Automatica	lly Configured Setup		
Wireless De Edit WDM id	vice Manager Settings entification & redundancy Cor	figuration		or Information gethe default username and password	Conf Sum	iguration Summary nary of all configurations
Process Control	Network (PCN) ———			Time Settings	C Administrator Informa	tion
IP Address	Subnet Mask		fault Gateway	Use System Time	Admin Name	Confirm Password
192.168.1.1	255.255.25	5.0 0.0	0.0	Yes	administrator	
				Date	New Password	
Special Interface	e Network (SIN)			04/27/2021		
Enable	IP Address	Subnet Mask	Default Gateway			
No	192.168.2.1	255 255 255 0	0000	15:03:39		

- 8. Verify the WDM settings and click **Finish.**
- 9. After completion, use a default PCN IP Address to access OneWireless User Interface.
- 10. You can see the progress as shown below.



11. The following page appears after completion.



Manual Configuration Wizard

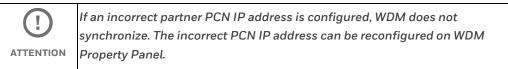
1. On the Welcome page of the First Time Configuration Wizard select **Manual Configuration Wizard** and click **Next**.

	Honeywell	
	Welcome to OneWireless	
	administrator	
	Administrator	
This wizard will gu	uide you through the steps necessary to set up your new One'	Wireless System.
	Choose the type of Configuration	
Use Default Configuration This option will automatically configure the Windess Device Manager using default settings.	Manual Configuration Wizard This option will allowyou to configure the Winess Device Manager step by step.	Restore From Backup This option will allow you to configure the Wireless Device Manager from a previous backup.
		NEXT

2. Provide **Tag Name, Description, Partner PCN IP address** in the Wireless device manager settings page and click **Next**.

	Hone	ywell			
	Manually Cor	figured Setup			
WDM Settings Enter WDM information Enter settings information	Retwork & Tim Enter settings in	e Iformation	Administrator Info	rmation	Configuration Summary Summary of all configurations
Wireless Device Manager Identification		Redundancy Co	nfiguration		
The Wireless Device Manager Name is the unique name used to identify your Wireless OneWireless. This name may also be used to identify your Wireless Device Manager on as OPC.					Vireless Device Manager as part of a pair P address is configured, WDM will fail to
Tag Name *				Redundancy	Role
wdm1		Enable Redu	ndancy for WDM	O Primary	O Secondary
Description		Partner PCN IP	address		
* Indicates required fields				BACK	NEXT

- 3. To configure redundant WDM, under **Redundancy Configuration**, configure the following:
 - a. Select Enable redundancy for this Wireless Device Manager check box.
 - **b.** Click the Redundancy Role, as required. You can select either Primary or Secondary option depending on the redundancy role.
 - c. In the Partner PCN IP Address box, type the PCN IP address of the partner WDM.



- 4. In the Location and Protocol page provide the Country Code, Protocols, ISA100 Network ID and WirelessHART Network ID.
- 5. Under Network ID, type the ISA100 Wireless Network ID. The ISA100 Wireless Network ID is a unique identifier for the network. It must contain a value between 2 (default) and 65435. After completing the first time configuration, you cannot change the Network ID. The WirelessHART Network ID is calculated based on the ISA100 Wireless Network ID. It is always +100 of the ISA100 Wireless Network ID value. If ISA100 Wireless Network ID is 2, then the WirelessHART Network ID is 102.

When multiple OneWireless networks (WDM's) are installed in the plant, make sure unique a Network ID is used.

	Honeywell		
	Manually Configured Setup		
WDM Settings Enter WDM information		nistrator Information ge password	Configuration Summary Summary of all configurations
Location Settings	Enabled Protocols	Network ID	
The Country Code is used when presenting location specific options within OneWireless. Radio frequency options will change based upon the country code setting.	Protocol can be selected from 'Wireless Protocol Settings' tab under Wireless Device Manager property panet. By default TSA 100' is supported.		unique identifier for FDN. If another ed in the same physical location, each fferent ISA100 network ID
Country Code	Protocols	ISA100 Network ID	WirelessHART Network ID
UNITED STATES (840)			
Tradicates neguined fields		BACK	NEXT

 In the Network and Time page provide the FDN IP Address, FDN Subnet Mask, PCN IP Address, PCN Subnet Mask, Access Point IP Address, Default Gateway and select the check box Enable DHCP Server (Assign addresses to Field Device Access Point).

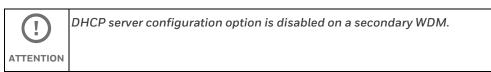
		Honeywe			
		Manually Configured Setu			
WDM Settings Enter WDM information	Cocation & Protocol Enter settings information	Retwork & Time Enter settings information		nistrator Information le password	Configuration Summary Summary of all configurations
Field Device Network (FDN)				Process Control Net	work (PCN)
	onnecting the WDM with one or more Field D s to Field Device Access Points based on the a		eris	The WDM must be conne PCN connections.	cted to your Process Control Network using the
FDN IP Address • FDN	N Subnet Mask *	DHCP Server(Assign addresses to Field (Point) *	levice	PCN IP Address *	PCN Subnet Mask *
	From *			Default Gateway	
Access Point IP Address				0.0.0.0	
Indicates required fields					
				ВАСК	NEXT

7. Under **Field Device Network (FDN)**, configure the network settings for the wireless field device network as follows.

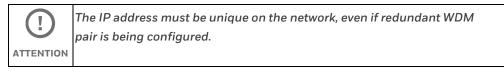
• **Field Device Network IP Address**: These settings are used to configure the wireless field device network Ethernet connection for the WDM. This is used for communication with FDAP. This field can be edited at any point in time.

!	• The IP address must be unique on the network, even if a redundant WDM pair is being configured.
ATTENTION	 After completing the initial configuration, you cannot change the Field Device Network IP Address specified in the First Time
	Configuration Wizard.

- Subnet Mask: A subnet mask identifies the bits of an IP address that are reserved for the network address. For example, if the IP address of a particular node is 192.168.2.3 with a subnet mask of 255.255.255.0, the subnet mask indicates that the first 24 bits of the address represent the network address. The last 8 bits can be used for individual node addresses on that network.
- Assign Addresses to Field Device Access Points (Enable DHCP Server): Select this check box to enable the WDM to act as the DHCP Server. Ensure you do not select the check box if the network has another DHCP Server. It is recommended to enable the WDM to act as the DHCP Server.
- Field Device Access Point IP Address: This option is enabled only if you have selected the Enable DHCP Server check box. Accept the default range or configure the IP address range according to the network settings in the plant network. The WDM that acts as the DHCP Server assigns IP addresses based on the range specified. Ensure that the IP addresses of the Access Points are not within the DHCP address range.
- If you do not enable DHCP Server during the first-time configuration, it is possible to enable this at a later stage using the Property Panel.



- 8. Under **Process Control Network (PCN)**, configure the process control network settings as follows.
- **Process Control Network IP Address**: The process control network settings are used to configure the process control network Ethernet connections for the WDM. This is used for communication with monitoring applications and external controllers.



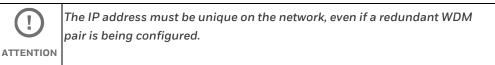
- Subnet Mask
- Default gateway: Used to access the subnets outside the PCN subnet. This is an

optional configuration option.

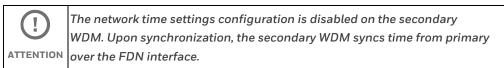
9. In the next page, provide the SIN details such as **SIN Subnet Mask**, **SIN IP Address Default Gateway** and select **the Network Time.**

		Hone	eywell		والمراجعة أستراب والمراجع والمراجع والمراجع
		Manually Co	nfigured Setup		
WDM Settings Enter WDM information	Location & Protocol Enter settings information	Network & Tir Enter settings		Administrator Information Change password	Configuration Summary Summary of all configurations
Special Interface Network (SIN)			Network Time		
Settings are used to configure the special interfa port is used for connecting 3rd party client appli such as Vibration Analyzer tools etc.				e from primary over the FDN in	e secondary WDM. Upon synchronization, the terface. By default, the network time is
Enable Special Interface Network	SIN IP Address		🔘 Use System Time	Use NTPServer	
SIN Subnet Mask	Default Gateway		Current Date		Current Time
	0.0.00				
•					
				ВАСК	NEXT

- 10. Under **Special Interface Network (SIN)**, configure the network settings for the special interface network as follows.
- Special Interface Network IP Address: These settings are used to configure the special interface network Ethernet connection for the WDMY. The SIN port is used for connecting 3rd party client applications existing on different network than a DCS network such as Vibration Analyzer tools etc. The client application can talk to WDM over SIN port using any of the existing interfaces HART, MODBUS, Enraf, GCI, OPC in WDM and collect required data from wireless transmitters.



- Subnet Mask:
- **Default gateway**: Used to access the subnets outside the SIN subnet. This is an optional configuration option.



11. Click **Use NTPServer** or Use **System Time**, as required. You can use either the NTP server or system time to configure the network time of the OneWireless Network.



1	ATTENTION	Consider the following while configuring an external NTP server.
		 NTP server must be on the PCN or FDN.
		 NTP server IP address must be within FDN or PCN subnet unless a default gateway has been configured on the PCN subnet and the NTP server is accessible through the default gateway.
		 Do not overlap NTP server IP address with the FDN and PCN IP addresses.
		 Do not overlap NTP server IP address with FDAP IP address range, if DHCP Server is enabled.

- 12. If you are selecting NTP server, enter the **NTP Server IP Address** and click **Next**. The **Administrator Information** page appears.
- 13. Type the user name and password in the **Administrator Name**, **New Password**, and **Confirm Password** fields.
 - The default username configured for the WDM is administrator. You can change the default username in the First Time Configuration Wizard, if required. However, you cannot change the username after completing the initial configuration.
 - The password must be between 8 and 32 characters and shall have one uppercase, one lowercase, one numeric and one special character.

		When setting up a redundant WDM pair, it is recommended that the same
	\mathbf{O}	default username and password are configured on primary and secondary
	ATTENTION	WDM. This is because when the primary and secondary WDMs
		synchronize, the secondary WDM's user account information is overwritten
		by the user accounts configured in the primary. Providing identical
		configuration on both WDMs, avoids confusion related to login credentials
		when the WDMs synchronize.
I		

		Honeywe			
		Manually Configured Set	up		
WDM Settings Enter WDM information	Content and the settings information	Network & Time Enter settings information	Administr 1811 Change pa	ator Information	Configuration Summary Summary of all configurations
' Administrator Name & Password The default user name confloured for th	d e WDM is administrator. You can change the	default user name in the First Time Configur	ation Wizard. If required	. However, you cannot change th	e user name after completing the ini
	en 1 and 32 characters and can not contain s				
administrator	New P	assword *	- 11	Confirm Password	

14. The Configuration Summary page appears which displays the summary of all the configuration information specified in the First Time Configuration Wizard. An incorrect entry is indicated by a warning icon.

Honeywell Manually Configured Setup					
WDM Settings O Location & Protocol Network & Time Enter WDM Information Enter settings information O Network & Time			Configuration Summary ummary of all configurations		
	letwork ID	Field Device Network (FDN) IP Address 192.168.0.1	Subnet Mask 255.255.255.0		
Enable Redundancy for WDM Redundancy Role Partner PCN IP address C	ocation Country Code JNITED STATES (840)	Enable DHCP Server Yes Access Point IP Address From 192 168 0 101	Te 192 168 0 200		
N]	BACK	NEXT		
Honey Manually Configu					
WDM Settings Enter VDDM information Enter settings information Network 8 Time Enter settings information			Configuration Summary Summary of all configurations		
IP Address Subnet Mask Default Sateway 19216811 2552552550 0.000	Fime Settings Use System Time Yes Date 04/27/2021 Time	Administrator Information Admin Name administrator Confirm Pasaword	New Password		
	03-05-07 PM				
•					
		ВАСК	NEXT		

15. Verify the WDM settings, correct errors if any, and then click **Finish**. The Finish button is disabled if there are any errors in the configuration information that you have provided.

			Hon	eywell		
			Automatical	lly Configured Setup		
	ice Manager Settings atification & redundancy Co	nfiguration		or Information ge the default username and password		guration Summary ary of all configurations
F Process Control N	letwork (PCN) ———			Time Settings	📊 _ Administrator Informat	ion
IP Address	Subnet Mas	k D	afault Gateway	Use System Time	Admin Name	Confirm Password
192.168.1.1	255.255.25	55.0 0.	D.O.O	Yes	administrator	*******
Special Interface	Network (SIN)			Date 04/27/2021	New Password	
Enable	IP Address	Subnet Mask	Default Gateway	Time		
No	192.168.2.1	255.255.255.0	0.0.0	15:08:11		
••					васк	FINISH

16. You can see the progress as shown below.

	42%	
Please w	ait while configuring Wireless De	evice
	Manager	

17. The following page appears after completion.

Honeywell	
Disclaimer	
This access is provided solely to Wireless Device Manager authorized users. Wireless Device Manager may include content that requires additional protection, including but not limited to, Controlled Unclassified Information (CUI), Company Confidential information (CUI), Company Confidential information (PII). You may not access or attempt to access such information unless you have been specifically authorized to do so. By clicking on 'Accept', I acknowledge that I am familiar with and agree to comply with these terms, with Company policies and procedures, and with any additional protective legends, markings, or statements included on such information.	
ACCEPT	

Restore from Backup

 On the Welcome page of the First Time Configuration Wizard select Restore from Backup and click Next.

	Honeywell	
	Welcome to OneWireless	
	administrator Administrator	
This wizard will	guide you through the steps necessary to set up your new Or	neWireless System.
	Choose the type of Configuration	
Use Default Configuration This option will automatically configure the Wireless Device Manager using default settings.	Manual Configuration Wizard This option will allow you to configure the Wineless Device Manager step by step.	Restore From Backup This option will allow you to configure the Wireless Device Manager from a previous backup.
		NEXT
	rior releases, a conversion tool	-

- 2. Restore from Backup can be done by the following ways:
 - **USB Connected To WDM**: Select a backup file from a USB device connected to one of the USB ports on the Wireless Device Manager.
 - **Network Backup Location**: Specify a UNC path to SMB network attached storage an select a backup file from the list of backups at the location.
 - File Upload from Local: Select a single backup available from location accessible from the computer you are currently using.

File Upload from Local

ATTENTION

1. Select File Upload from Local and click Next.

	Honeywell	
	Restore From Backup	
Select Backup Source		
USB Connected To WDM Select a backup file from a USB device connected to one of the USB ports on the Wireless Device Manger.	Network Backup Location Specify a UNIC puth to SMB network attached storage and select a backup file from the list of backups at the location	File Upload From Local Select a single backup available from a location accessible from the computer you are currently using
		BACK NEXT

2. Browse the file and click **Upload**.

Honeywell Restore From Backup		
File Upload From Client Click Browse to select a backup file from the system where the UI is being accessed. On click an open file dialog will be appear. This will allow the use after selecting the file to upload the backup file to WOM. Click on 'Restore' to restore the configuration on the WOM once upload is completed. File Path *	er to select the back up file to restore Wi	DM configuration. Click on 'Upload'
Choose file		D BROWSE
alicates required fields	ВАСК	UPLOAD

3. It will ask for encryption password

Ē	A password is required for restoring the backup
NOTE	Contact GTAC for migrating the old backup files to new file format encrypted with user defined password

4. Click Next.

		Honeywell	
		Restore From Backup	
NAME	LOCATION	BACKUPDATE	DESCRIPTION
A_P_2021-04-15T12-52Z tar.gz	USB0	April 15th 2021, 06:22:00 pm	Automatic backup created on 4/15
		•	
			BACK

5. Click **Restore**.

Honeywell Restore From Backup							
WDM Identification	Field Device 1 FDN IP Address 172.20.229.65	Subnet Mask		Process C PCN IP Add 172.20.56		N) Inubnet Mask 155.255.255.0	Default Gateway 0.0.0.0
File Details File Name A_P_2021-04-15T12- 52Z1argz	File Description Automatic back device USB0	up created on 4/15/21 at 12	52 GMT on USB	Firmware Revis OW320.3-4.0			Notifications Notifications 24
Redundancy Enable Redundancy for WDM Primary		Synchronization State Synchronized	WDM Redund CC_WDM2_S		FDN Redundancy Pari 172.20.229.66	ther PCN Redundancy 172.2056.61	Partner
						ВАСК	RESTORE

- 6. Verify the WDM settings, correct errors if any, and then click **Finish**. The Finish button is disabled if there are any errors in the configuration information that you have provided.
- 7. You can see the progress as shown below.

	(
	42%	
0Ia	ase wait while configuring Wireless D	evice

8. The following page appears after completion.

Honeywell

Disclaimer

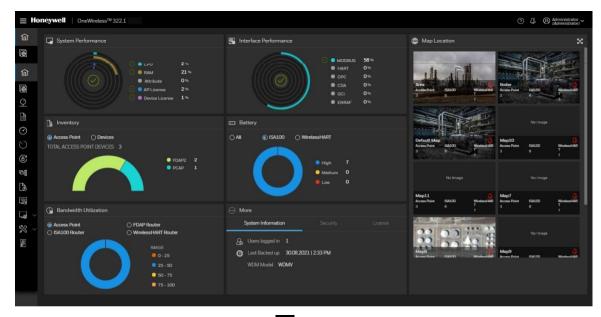
This access is provided solely to Wireless Device Manager authorized users. Wireless Device Manager may include content that requires additional protection, including but not limited to, Controlled Unclassified Information (CUI), Company Confidential information, and Personally Identifiable Information (PII). You Personally identifiable information (PII). You may not access or attempt to access such information unless you have been specifically authorized to do so. By clicking on 'Accept', I acknowledge that I am familiar with and agree to comply with these terms, with Company policies and procedures, and with any additional protective legends, making a pathamata including a such

markings, or statements included on such information.

ACCEPT

Understanding the OneWireless user interface

After configuring the WDM using the First Time Configuration Wizard, the following OneWireless user interface appears.



Select the hamburger button 🔳 to expand the Menu Bar.



Fig. 9. OneWireless user interface

The OneWireless user interface comprises of the following main elements.

• Left Navigation Menu bar: Consists of Home, Main menu, Action menu and Logout. It gives an access to various functions for monitoring and maintaining the OneWireless Network. These user interface controls are contextual and are enabled based on user role and devices/channels selected in the Map location.

- **Dashboard parameters:** It consists of parameters such as System Performance, Interface Performance, Inventory, Battery, Bandwidth Utilization, System Information, Security and License
- Map Location: Provides a visual representation of the OneWireless Network.
- **Status bar**: Provides an overview of the network status by displaying the number of online devices, active alarms, WDM redundancy status,
- Notification list: It provides the progress of any maintenance operation.

Dashboard parameters

• System Performance:

Provides information about System health parameters like CPU, RAM, Attribute, AP License and Device License. This can be used to determine the cause of problems by measuring the performance of hardware, software services, and applications. When any of the values shows more than 80%, then icon changes to icon for the corresponding attributes.



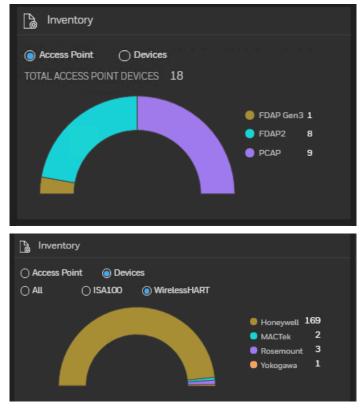
• Interface Performance:

Provides the information about individual external interface bandwidth utilization. Rate 0% means the interface might be disabled or no communication between client.



• Inventory:

Provides an overview on number of devices and Access Points connected to the OneWireless network.



This page is read only, by default it is selected as Access Point.

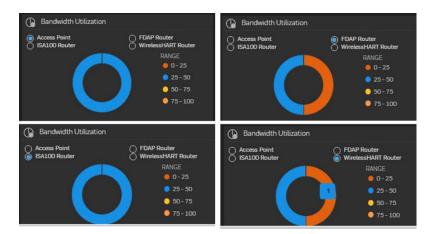
• Battery:

Provides the battery usage of devices connected to OneWireless network.



• Bandwidth Utilization:

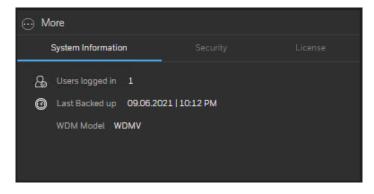
Provides the bandwidth utilization of Access point, FDAP as Router, ISA100 as Router and Wireless HART Router connected to OneWireless network.



• More:

Provides information on System Information. Security and License **System Information**:

Provides the list of users logged in, last Backup information and WDM model.



• Security:

Provides the information on seccurity configuration of system and green color indicates enabled and grey color indicates disabled.

	Security	
io 🕤	IP Sec	۲
Address Filtering 🛛 🍥	Mac Address Filtering	۲
avisioning 📀	Rouge Devices	Ð.
CAP Provisioning 💮		

• License:

Provide the information on license installed.



Selection Panel: The Selection Panel in the OneWireless user interface provides a list of all the devices configured in the OneWireless Network. See <u>Manage Devices</u> section for more information.

Manage Devices									
Search by category						election F			
S : □ Show	Radio Identification							⊞	×
TAG NAME	DEVICE TYPE	STATUS	VENDOR	MODEL.	REVISION	SERIAL	IPV6 ADDRESS	POWER	
💌 wdm1	Device Manager	Joined	Honeywell	WDM	OW322.1-36.0		FE80::4E7C.CO		
AP_0096	Access Point	Joined	Honeywell	FDAP2	OW322.1-25.0	2011160002	FE80::4E78.CO	Line	
FC_1808	Access Point	Joined	Honeywell	PCAP	OW322.1-35.0	2021070010	FE80::4E78.CO		
FDAP2_R3_1	Router	Joined	Honeywell	FDAP2	OW322.1-14.0	2014490009	FE80 : : 0040.84	Line	
• LPFR_0041	Router	Joined	Honeywell	FDAP2	OW322.1-35.0	1033001	FE80 : : 0040.84		
✓	WirelessHART(R)	Joined	Honeywell	Emulator		66051	FE80::0018:1E	High	
🗸 😫 MacTek_a	WirelessHART(A,	Joined	MACTek	Wireless Adapter			FE80::0018:1E		
✓ ● CD_475_3_	ISA100(R)	Joined	Honeywell	XYR 6000 Corr	Corrosion versio	504084300000	FE80 : : 0040.84	High	
✓ ● TD_105_5_	ISA100(R)	Joined	Honeywell	XYR 6000 TempDI	Temperature DI v	408105	FE80 : : 0040.84	High	
✓ ● HD_466_3	ISA100	Joined	Honeywell	XYR 6000 HLAI	HLAI version 279	504084300000	FE80 :: 0040.84	High	
V 🥚 P0_5738	ISA100	Joined	Honeywell	STW TempAIDO	Sensor version 0	\$10203040506_	FE80::0102:03	High	

Property Panel : The Property Panel in the OneWireless user interface under Manage Devices provides configuration properties of all the devices configured in the OneWireless Network. See the **Property Panel** section for more information.

Manage	Devices				Property Panel	
Sector	attractor	√		= x ×	FDAP2_R320_F803	
TAD	une	DEVICE TYPE	STATUS	VENDOR	Access Point Summary	
	FC_1808	Access Point	Joined	Honeywell	Device Management	
	FDAP2_R320_FB_	Router	Joined	Honeywell	Data Layer Management	
	LPFR_0041	Router	Joined	Honeywell	Neighbor Diagnostics	
~ 0	EML_85656	WirelessHART(R)	Joined	Honeywell	Channel Diagnostics	
	MacTek_adapter	WinslessHART(A,R)	Joined	MACTER	Statistics (DMAP)	
- × 0	CD_475_3F_6FLR	ISA100(R)	Joined	Honeywell	Network Address Filter	
• •	T0_105_5FL_SFT	(SA100(R)	Joined	Honeywell	NETWORK ADDRESS FIELD	
× 0	H0_466_3CLL_P_	ISA100	Joined	Honeywell	Radio Disconnect History	
× ()	P0_573	ISA100	Joined	Haneywell	RESET	APPLY
1-10 of 20			Go to page 1 →	Devices per 10 ~	MESEI	APPLY .

Manage Filters: The Filter option allows you to customize the device list by filtering the devices. By default, all the devices appear in the device list. You can filter by **Device Type**, **Device Status**, **Vendor, Model**, **Power Source**, **Alarm Priority**, **Hop Level**, and **Maps**.

Mana	ige Devices								
S	: Show Red	io Identification							3
	TAG NAME	DEVICE TYPE	STATUS	VENDOR	MODEL	REVISION	SERIAL	Manage Filters	
	PC_1808	Access Point	Joined	Honeywell		OW322.1-35.0	2021070010	DeviceType	
	FDAP2.R02	Router	Joined	Honeywell	FDAP2	OW322.1-14.0	2014490009	 Status	
	LPFR,0041	Router	Joined	Honeywell	FDAP2	OW322.1-35.0	1033001	Vendor	
	EML_65656	WirelessHART(R)	Joined	Honeywell	Emulator		66051	Model	
	MacTek_ad.	WirelessHART(A,R)	Joined	MACTek	Wirelast Adapter			PowerSource	
	0 CD_475_3F.	ISA100(R)	Joined	Honeywell	XVR 6000 Corr	Corrosion version 2	5040843000000204	AlamPriority	
	10.105.5F.	ISA100(R)	Joined	Honeywell	XVR 6000 TempDi	Temperature DI ver	408105	Map	
	🔵 но,466,3С.	ISA100	Joined	Honeywell	XYR 6000 HLAI	HLAI version 279	504094300000066	HopLavel	
	P0,573	ISA100	Joined	Honeywell	STW Temp/UDD	Sensor version 001	5102030405060708	and a second	
1-100	F20 devices				Go to page	1 →		Devices per page	10
Access Div	nts - 4, ISA100 - 9, Win	instator - E Thereit	High CO Martin	n 🙃 Los 🙃 Primary-	Synchronized Physical ID- B			Aug 10, 20	



When you set a filter, various system views are altered. For example, the map highlights only the devices for which the filter option is applied.

Filter includes an option to filter by Map. This includes the Unplaced map so any device that has not been placed on a map can easily be detected. Note that since a device can be placed on more than one map, it can appear in the set of filtered devices for different maps. The following sections explain each element of the user interface in detail.

Left Navigation Menu bar

偭	HOME
MAIN	I
₽	MONITORING
Ŷ	ALARMS & EVENTS
<u> [iii</u>	REPORTS
ACTIO	DNS
Ø	PROVISIONING
\odot	MANAGE DEVICES
ß	SINGLE SIGN ON
6g	CHANNELS
Pe	FIRMWARE UPGRADE
()	EXTERNAL INTERFACES
L_®	SYSTEM
\approx	MAINTENANCE
8	MANAGE LICENSES
ሳ	LOGOUT

The Left Navigation Menu bar in the user interface is described in the following table.

Tab/icon	Description
Tab/icon Home	<text><text><text></text></text></text>
Main Group	Image: Second part of the function First function First function First function First function Image: Second part of the function Image: Second part of the func
Monitoring	Monitoring menu displays all the maps configured in the WDM.
	Use the Monitoring menu to add, configure, and commission wireless field devices and monitor the devices in Map view. For more information about the map view, see the section <u>About map view</u> ATTENTION
	The Monitoring tab is disabled on the secondary WDM.
Alarms & Events	The Alarms & Events menu displays the alarms and system events generated by the wireless field devices in a tabular format. An alarm is generated whenever an abnormal condition occurs. An event is any significant change in the system and includes alarms and operator actions. The Alarms & Events menu contains the following sub elements.

	 The Active Alarms tab: Lists the active events in the system with more details like priority, event class, category, source, location, start time and description. If the alarm the system with the system and the event log for a particular period.
Reports REPORTS	 Reports menu displays device performance and connectivity reports. Use the Reports menu to generate and view predefined reports that are used to maintain and optimize the network and the field devices. The following are the reports that can be generated: Battery Life Device Health Overview Device Summary Connection Summary Connection History Inventory Summary Availability Summary For more information, see "Generating reports"
Actions group Provisioning	You can choose the type of device to be provisioned and delete WDM or Devices from this option. See section " <u>Provisioning</u> " for more information.

100

	 Note the following points while deleting a device from the network. Deleting a joined ISA100 Wireless device removes the provisioning data and the configuration data from the device and the WDM. Also, the device restores to factory default state. Deleting a joined WirelessHART device removes the provisioning data from the device and all the information about the device from WDM. Deleting an offline device removes the provisioning data and the configuration data must be manually cleared from the device using the PDA. Note: For the secondary WDM, only the Delete WDM option is available.
Manage Devices	<text><text></text></text>

Single Sign On	WDM supports single sign on feature.
SINGLE SIGN ON	<complex-block></complex-block>
Channels CHANNELS	 Activate: Activates all the channels of the selected field device. Clicking the Activates all the channels of the selected field device channel state from OOS to the currently configured Normal mode. Inactivate: Inactivates all the channels of the selected field device channel state from AUTO to OOS.
FIRMWARE UPGRADE	devices. Upgrade firmware for WDM, Access Points and ISA100 Devices.

	 WDM: Initiates firmware upgrade operation for the WDM and the application firmware of the ISA100 Wireless field devices. Radio: Initiates firmware upgrade operation for the access
	points and the radio firmware of the ISA100 Wireless field devices.
	• Sensor Application: Initiates firmware upgrade operation for the Sensor Applications and the application firmware of the ISA100 Wireless field devices.
	For more information, see section " <u>Upgrading device firmware</u> "
External Interfaces	External Interfaces such as MODBUS, HART, OPC, GCI, CDA and ENRAF are available on the primary WDM.
	Extend Interface: Extend Interface: Sector Fearse Control Control C
System Image: System System Manage users Manage roles 	Manage Users: Opens the Manage Users dialog box that contains the options to add, delete, or edit new user accounts. Manage Vers Index to the contains the options to add, delete, or edit new user accounts. Index to the contains the
SOFTWARE DOWNLOAD C EXPORT SYSTEM LOGS C S BACKUP SETTINGS	Wit Administratur prof Prof Instaliar Shafura Administratur
	• Manage Roles: Opens the Manage Roles dialog box that enables you to modify the configured user-permitted operations.

 Software Download: Enables you to download software provided
 on WDM. Image: State of the system log: Enables you to export and save the system logs that record information about events in the application
 Backup Settings: The backup file created can be used to restore
the system configuration to a new WDM, or a WDM that has been reset to factory defaults.
 — Remote Event logging: Select specific or all alarm/events from WDM to be sent to a remote server (syslog-ng compatible server).

	See " <u>Configure i</u>	<u>manual backup"</u>	' for more info	rmation	
	Backup Settings The backup file created can be used to restore the system	or riguration to a new WDM, or a WOM that has been reset to factory default			
	Select Property	Backup Settings			
	Select specific or all altern-levents from WDM to be sent to a rig competible serve()	rencle server (syslog- configuration automatically:	ation backup to back up the system		
				NEXT	
	 Templat 	t es : Uploads the	vendor suppl	ied ISA100 Wireles	s device
Maintenance	DD file t	o the WDM Wir	elessHART de	vice DD files are no	nt
	support	ed on WDM.			
	Templates				
	Cick Load ISAL00D0/Modbus File to select a	nd load a Device Definition (DD) file or Modbus configuration bac	kup file to the Wireless Device Manager.		
	VENDOR	MODEL	DEVICE REVISION	DO FILE REVISION	
	GE Energy	ISA100-STAPS 70M303	0003		
	Yokogawa				
	Vologawa	FN310 HART 6501	0001.		
	Honeywell	EnratWFI	0001		
	Honeywell	STX800 FEWIO			
	Honeywell	XYR 6000 TempDi	0001		
					a
	Point Pi	cker: Enables yo	ou to browse p	parameters on all d	evices
	and the	h drag and drop	parameter in	to MODBUS coil or	[,] register
	configui	ration			
	conniga				
	Point Picker Point Picker enables you to browse parameters	for all the devices.			
Aaintenance	Search by device Q				
	Show Sensor Parameters				
	SELECT DEVICE/CHANNEL	SELECT ATTRIBUTE	Device Detail		
	✓ wdm1 AP,0096	AVAILABILITY AVAILABILITYSTART	Attribute AP_0096 Description	Device Type Access Point More Detail	
	LPFR_0041	BACKWARD_COMPATIBILITY			
	EML_64G4A_5FL CD 475 3F 6FLR	BACKWARD_COMPATIBILITY_NO COMMREDUNALARMEN			
	 CD_475_3P_5PUR PD_573 				
	V TD_1049_7F_5FLR	DEV_DESC			
	✓ TD_1010_41.6FLR	DEVICE_ROLE_ASSIGNED			
	Showing 9 Devices	DIV CORRECT PKT COUNT			
	Attention				
	This group is di	sabled on the se	econdary WDI	М.	
	Displays the use	er who has curre	ntly loaged or	n to the OneWireles	SS LISPr
🔘 Test1 🗸			nity togged of		55 0501
(Administrator)	interface.				

Action List	Displays the status and notification.
Φ	Action List × Status(0) Notifications(0) No Status Found
(Administrator) ~ Change Password	Enables you to change the current user's password.

Manage Devices

Manage Devices provides a list of all the devices configured in the OneWireless Network. It also provides an option to view the extended view of the Devices. You can read and write the properties, view alarms/events for all the devices.

The default view of the Manage Devices displays all the devices arranged in the order -WDM, FDAPs, PCAPs, Access Points, and field devices. You can configure multiple locations for organizing the devices. The following illustrations depict the default view of the Manage Devices.

You can adjust the width of the column by adjusting the highlighted bar in the following image.

C : □ Show R	adio Identification							⊞ X
TAG NAME		STATUS	VENDOR	MODEL	REVISION	SERIAL	IPV6 ADDRESS	POWER
wdm1_PCT	Device Manager	Joined	Honeywell	WDM	OW322.1-33.0		FE80::4E7C.CO	Line
FDAP2_FC	Access Point	Joined	Honeywell	FDAP2	OW322.1-33.0		FE80::4E7B:CO	Line
MAPO3_DA	Access Point	Joined	Honeywell	PCAP	OW322.1-33.0	2021070001	FE80::4E7B:CO	Line
MAP03_DA	Access Point	Joined	Honeywell	FDAP Gen3	OW322.1-31.0	4294967295	FE80::4E7B:CO	Line
MAP04_EC	Access Point	Joined	Honeywell	PCAP	OW322.1-33.0	4294967295	FE80::4E7B:CO	Line
MAP05_D9	Access Point	Joined	Honeywell	PCAP	OW322.1-33.0	4294967295	FE80::4E7B:CO	Line
MAP07_D9	Access Point	Joined	Honeywell	PCAP	OW322.1-33.0	4294967295	FE80::4E7B:CO_	Line
MAPO9_D8	Access Point	Joined	Honeywell	PCAP	OW322.1-33.0	2021070004	FE80::4E7B:C0	Line
MAP10_D8	Access Point	Joined	Honeywell	PCAP	OW322.1-33.0	4294967295	FE80::4E7B:C0	Line
MAP11_DA	Access Point	Joined	Honeywell	PCAP	OW322.1-33.0	4294967295	FE80::4E7B:CO	Line



If any unprovisioned devices ae available in the selection panel, go to Provisioning from Left Navigation Menu and Accept the device for provisioning

For more information see the section "selection panel"

The following table describes the different elements/icons available in the Manage Devices.

Element F

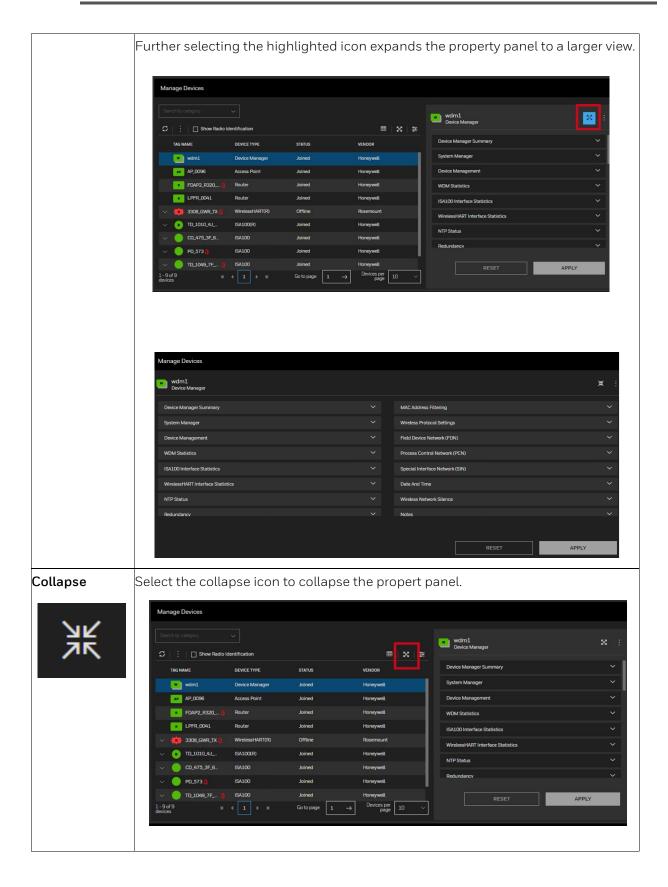
Manage

Columns

Function

Allows you to select the required attribute columns such as device type, status, vendor, model, serial number, and so on.

Ħ	D HOME	Manage Devices							
	MAIN	Search by Labegory							
		C : Show Radio Ide							. × :
	REPORTS		DEVICE TYPE STATUS	VENDOR	MODEL	REVISION	SERIAL	Manage Columns	
	ACTIONS	wdm1	Device Manager Joined	Honeywell					
	PROVISIONING	AP_0096	Access Point Jained	Honeywell	FDAP2	0W322.1-25.0	2011160002		
	SINGLE SIGN ON	plants concernation and	Access Point Joined	Honeywell	PCAP FDAP2	0W3221-35.0 0W322.1-14.0	2021070010	Vendor	
	CHANNELS	~ 🗰 EML_65656 1	WirelessHART(R) Joined					Model	
	FIRMMARE UPGRADE	and the second sec	WirelessHART(A,R) Joined	MACTek	Wireless Adapter		0	Revision	
	SYSTEM V		ISA100(R) Joined	Honeywell	XYR 6000 Cerr	Temperature DI vers	408105	FE80::0040:8430_	High
	MANAGELICENSES		ISA100 Jained	Honeywell	STW TempAIDO	Sensor version 001	\$102030405060708	FEB0::0102:0304_	High
		 SL_Temp_7 1 - 10 of 18 devices 	ISA100 Joined	1 2 F H	STW TempDi Go to p	TempUID Venion 0	5040840000070055	PE80::0040.8400	High wicesperpage 10 v
	U LOSOUT	WirelassHART - 6 💣 Urgert 📵 High							Aug 10, 2021, 5:40:00
xpand	Select the de	property t	to expand t	-					
xpand	on individual " <u>Property pa</u> Manage Devices	. property t <mark>nel</mark> " sectic	to expand th on.	ne prop					
xpand	on individual " <u>Property pa</u> Manage Devices Lists all the devices in the network	. property t nel [®] sectio	to expand t	ne prop		or more	e inforn		
xpand	on individual " <u>Property pa</u> Manage Devices	. property t nel." section k. The user will be able to read and	to expand th on.				e inforn		
xpand	on individual " <u>Property pa</u> Ust all the deccase in the nativo Lats all the deccase in the nativo Caserthey category C _ thew Radeo Identified	property t nel" section 4. The user will be able to read and atom :	co expand th on. where a properties, view damps have	ne prope	erties. F	or more	e inforn		see the
xpand	on individual "Property pa Lits all the derices Lits all the derices in the network Celerch by Category C C Show Radio Identified Tation Kate	. property t nel" section k. The user will be able to read and k. The user will be able to read and allon : Levuce type	co expand th on. whethe populies, view alams/view	ne prope s forall the devices VERNOR	erties. F	For more	e inforn		see the
xpand	on individual "Property pa Lits all the derects in the networ Calenth by calegory C C Show Radie Identified Take NAME	property t nel" section 4. The user will be able to read and atom :	co expand th on. whe he properties, view alarms/even status journed	La forall the devices VENDOR Honeywell	erties. F	For more wdm1 Device Manager Sum	e inforn		see the *
xpand	on individual "Property pa Lits all the derocas in the network Caserch by category C C Show Radie Identified Tice NAME With I Manage Devices Lits all the derocas in the network Caserch by category C C C C C C C C C C C C C C C C C C C	. property t nel" section 4. The user will be able to read and 4. The user will be able to read and 5. The user will be user will be able to read and 5. The us	co expand th on. whethe populies, view alams/view	te forall the devices VERKOB Honsywell	erties. F	For more wdm1 wdm1 Device Manager Sum System Manager	e inforn		see the *
xpand	on individual "Property pa Lits all the derects in the networ Calenth by calegory C C Show Radie Identified Take NAME	. property t nel" section 4. The user will be able to read and 4. The user will be able to read and 5. The user will be user will be able to read and 5. The us	svarus Joined	La forall the devices VENDOR Honeywell	erties. F	For more wdm1 bevice Manager Sum System Manager Device Manager	e inforn "		see the *
xpand	on individual "Property pa Lits all the derivations in the network Callerth My callingery Callerth My Callerth My Callerth My Callingery Callerth My Callerth My Callinge	E property t nel" section 4. The user will be able to read and 4. T	status Joned Joned	La forall the devices VEKDOB Honeywell Honeywell Rosemourt	erties. F	For more wdm1 bvice Manager Sum System Manager Device Manager Device Manager Device Manager	e inforn « may		see the *
xpand	on individual "Property pa Lits all the derivations in the network Called the derivations of the network Called the network of the network of the network Called the network of the network of the network Called the network of the ne	E property t nel" section 4. The user will be able to read and 4. T	srans Joined Joined Joined Joined Joined	a foral the devices VEKDOB VEKDOB VEKDOB Honsywell Rosemourf Honsywell	erties. F	For more wdm1 Device Manager Sum System Manager Device Manager	e inforn « may		see the * ```````````````````````````````````
xpand	on individual "Property pa Lits all the derivations in the network Callerth My callingery Callerth My Callerth My Callerth My Callingery Callerth My Callerth My Callinge	E property t nel" section 4. The user will be able to read and 4. T	status Joined Joined Office	La forall the devices VEKDOB Honeywell Honeywell Rosemourt	erties. F	For more wdm1 Device Manager Sum System Manager Device Manager Device Manager Device Manager Device Manager UM Statistics ISA100 Interface Stat WirelessHART Interfa	e inforn « may		see the * *
xpand	on individual "Property pa Lits all the derivations in the network Called the derivations of the network Called the network of the network of the network Called the network of the network of the network Called the network of the ne	E property t nel" section 4. The user will be able to read and 4. T	srans Joined Joined Joined Joined Joined	a foral the devices VEKDOB VEKDOB VEKDOB Honsywell Rosemourf Honsywell	erties. F	For more wdm1 Device Manager Sum System Manager Device Management WDM Statistics ISAL00 Interface Stat WirelessHART Interfa NTP Status Redundancy	e inforn « may		see the
xpand	on individual "Property pa Lits all the derivations in the network Called the derivations of the network Called the network of the network of the network Called the network of the network of the network Called the network of the ne	E property t nel" section 4. The user will be able to read and 4. T	srans Joined Joined Joined Joined Joined	a foral the devices VEKDOB VEKDOB VEKDOB Honsywell Rosemourf Honsywell	erties. F	Cor more wdm1 Device Manager Sum System Manager Device Manager Device Manager Device Manager Statistics Statophice Stat WirelessHART Interfe NTP Status Redundancy Redundancy Redundancy Interfe	e inforn « may		see the * * * *
xpand	on individual "Property pa Lits all the derivations in the network Called the derivations of the network Called the network of the network of the network Called the network of the network of the network Called the network of the ne	E property t nel" section 4. The user will be able to read and 4. T	srans Joined Joined Joined Joined Joined	a foral the devices VEKDOB VEKDOB VEKDOB Honsywell Rosemourf Honsywell	erties. F	Widm1 Device Manager Sum System Manager Device Manager Sum System Manager Device Management WDM Statistics ISA100 Interface Stat WirelassHART Interfa NTP Status Redundancy History IP Address Filtering	e inform may astes es statutes		see the * * * * *
xpand	on individual "Property particles" Los al the devices in the network Los al the devices in the network Los all the devices in the network Control of the devices To: NAME Control of the devices Control of the device	E property t nel" section 4. The user will be able to read and 4. T	srans Joined Joined Joined Joined Joined	a foral the devices VEKDOB VEKDOB VEKDOB Honsywell Rosemourf Honsywell	erties. F	Cor more wdm1 Device Manager Sum System Manager Device Manager Device Manager Device Manager Statistics Statophice Stat WirelessHART Interfe NTP Status Redundancy Redundancy Redundancy Interfe	e inform may astes es statutes		see the * * * * *



anage Filters	Allows you to	o custor	nize the	device lis	st by filte	ering the	devices.	By default	t, all th
	devices appe	ear in th	e device	list. You	can filte	r by Devi	се Туре,	Device Sta	atus,
<u>\$</u>	Vendor, Mod	lel, Powe	er Source	e, Alarm	Priority, I	Hop Leve	el, and M	aps.	
- o	Show Radio Identifica	ation :							
	TAG NAME	DEVICE TYPE	STATUS	VENDOR	MODEL	REVISION	SERIAL		
	wdm1 d	Device Manager	Joined	Honeywell	WDM	OW322.1-11.0		FI DeviceType	~
	AP_0096	Access Point	Joined	Honeywell	FDAP2	0W322.1-11.0	2011160002	FI Status	~
	R LPFR_0041 4	Router	Joined	Rosemount	FDAP2 330BA Wireless G	OW320.3-04.0	1033001	Fl Vendor	~
	 3308_GWR_TX 4 TD_1010_4J_6F 	ISA100(R)	Joined	Honeywell	XYR 6000 TempDI	Temperature DI Ver 28	1230000010	Model	~
	CD_475_3F_6FLR		Joined	Honeywell	XYR 6000 Corr	Corrosion version 252	5040843000000204	PowerSource	~
								AlarmPriority	~
								Мар	'
	S Show Radio Identific	ation							⊞ ¥
	TAG NAME	DEVICE TYPE	STATUS	VENDOR	MODEL	REVISION	SERIAL		
	wdm1 4	Device Manager	Joined	Honeywell	WDM	OW322.1-11.0		FI DeviceType	
	AP_0096	Access Point	Joined	Honeywell	FDAP2	OW322.1-11.0	2011160002	FI Access Point	
	R LPFR_0041	Router	Joined	Honeywell	FDAP2	OW320.3-04.0	1033001	FI Router	
	✓ 🌞 3308_GWR_TX 4	WirelessHART(R)	Offline	Rosemount	330BA Wireless G		1008912	FI Router(PM)	
	✓ ● TD_1010_4J_6F	ISA100(R)	Joined	Honeywell	XYR 6000 TempDI	Temperature DI Ver 28	1230000010	FI ISA100	
	∨ O _475_3F_6FLR	ISA100	Joined	Honeywell	XYR 6000 Corr	Corrosion version 252	S040843000000204	FI WirelessHART(A) HART(Wired) WirelessHART WirelessHART(R)	

Property Panel

The Property Panel in the OneWireless user interface under Manage Devices provides configuration properties of all the devices configured in the OneWireless Network. This panel is docked under Manage Devices of the main menu and is vertically expandable and collapsible.

The Property Panel allows you to perform configuration tasks pertaining to WDM, FDAPs, Access Points, and field devices and their channels. It also allows monitoring the configuration attributes of the devices such as PV, communication links, signal quality, and so on.

Selecting the required device in the Selection Panel displays all the configuration parameters of the devices that are accessible from the Property Panel. These configuration parameters are grouped into accordion panels that can be individually expanded or collapsed.



On the Access Point user interface, some accordion panels like System Manager, Configuration, Date and Time, Provisioning and Provisioning ATTENTION Devices are not displayed. For example, see the following figure.

Manage Devices		
wdm1 Device Manager	×	
Device Manager Summary	MAC Address Filtering	
System Manager	Wireless Protocol Settings	
Device Management	Field Device Network (FDN)	
WDM Statistics	Process Control Network (PCN)	
ISA100 Interface Statistics	Special Interface Network (SIN)	
WirelessHART Interface Statistics	Date And Time	
NTP Status	Wireless Network Silence	
Redundancy	Notes	
Redundancy History		
IP Address Filtering		
	Alarms(1)	
	RESET	

The following table describes the different elements/icons available in the Property Panel.

Element	Function
~	Click to expand the Property Panel.
^	Click to collapse the Property Panel.
APPLY	Click to save any configuration changes applied. This icon is enabled only if you have made any changes in the user interface.
RESET	Click to reset any unsaved changes made to the devices through the Property Panel. This icon is enabled only if you have made any changes in the user interface.
Alarms(O)	Allows you to view the alarm details (Priority, Start Time, and Description) for any device selected in the Selection Panel.

Understand the device icons

The Selection Panel, map view, and the Property Panel display various device icons for representing the network components. The following table summarizes the appearance of the device icons and their corresponding description/state.

If the device icon is	Then it represents
w	Non -Redundant WDM
w	Redundant WDM
R	FDAP router
АР	Access Point or FDAP access point
AP	Offline FDAP access point
R	Offline FDAP router

	1
AP 0	FDAP Access Point is in silence mode
Over-the-air provisioning icons	
AP	Access point with OTAP enabled
R	FDAP router with OTAP enabled
АР	Access point in Non-provisioned state
R	FDAP router in Non-provisioned state
	Field device in Non-provisioned state
AP	Access point in joining/provisioning state
R	FDAP router in joining/provisioning state
	Field device in joining/provisioning state

R	FDAP router in rejected state
	Field device in rejected state
	Field device in write protect state.
Field device icons	
R	Routing field device (field device with routing capability)
	Field device that has joined the network
	Field device in offline state
Channel icons	
•	

	For ISA100 Wireless device, Channel in Auto/MAN mode
	For WirelessHART Device, the variable status is Good.
	For ISA100 Wireless device, Channel in inactive/OOS mode.
	Channel becomes grey when the data is being fetched from the device. For a digital output channel, grey indicates the MAN mode, where you can manually set the output value.
	For ISA100 Wireless devices the channel status is offline. For WirelessHART devices the variable status is Bad
WDM redundancy icons	
Primary view	
w	Primary is Unknown (default Secondary).
w	Primary is Offline (default Secondary).
w	Primary is Joining (default Secondary).
w	Primary is Joined, redundancy sync state (secondary) is No Partner or Unknown (default Secondary).
w	Primary is Joined, Partner is visible over private path but not synced. Partner may be incompatible.
w	Primary is Joined, Initial sync is in progress.

Secondary view	
w	Secondary is Unknown (default Primary).
w	Secondary is Offline (default Primary).
w	Secondary is Joining (default Primary).
w	Secondary is Joined, Redundancy sync state No Partner or unknown (default Secondary).
w	Secondary is Joined, Partner is visible over private path but not synced. Partner may be incompatible.
w	Secondary is Joined, Initial sync is in progress.
w	Secondary is Joined, WDMs are synchronized.

Status bar

The status bar that is located at the bottom of the user interface window displays messages that indicate the overall status of the network. These status messages are grouped into different panes in the status bar.

Table. 5.	Status	bar	panel	
-----------	--------	-----	-------	--

Pane	Description
Access Points - 2, ISA100 - 4, WirelessHART - 1	Number of online devices.
4 Urgent 📵 High 1 Medium Օ Low 🧿	Displays all the active alarms. Click the Alarms box to open the Active Alarms table in the Alarm/Events tab.
Primary- Synchronized	Displays the redundancy role and synchronization status.
Aug 30, 2021, 6:42:47 PM	Displays the date and time.

Notification List

Pane	Description
	Firmware upgrade status is displayed when you have
Action List X	initiated a firmware upgrade of any device. As the
Status(1) Notifications(0)	status bar displays the progress, you can close the
ISA100 Radio Firmware	Firmware Upgrade dialog box to allow the operation
Upgrade	to run in the background. Click this box to open the
Total Selected Devices (to Upgrade)	Firmware Upgrade dialog box.
↑ Completed Inprogress	
0 1	
Failed Aborted	
	Channel Activation/Inactivation
Action List X	
Status (1) Notifications (0)	
ISA100 Channels (V) Total Selected Channels (to Activate)	
6	
Activate Channels In Activate Channels	

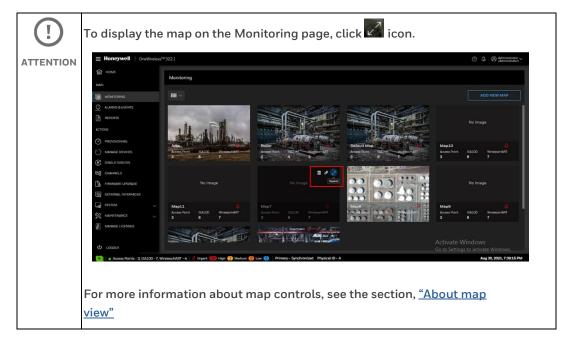
About map view

Use the map view to create a visual topology map of the network. The devices can be arranged in a map view according to the plant network topology. The map view allows you to create a real plant topology by dragging and dropping the devices from the device list in the Manage Devices. Arrange the devices on the map according to the plant setup and set the map visibility and overlays such as connection strength and publishing rate. For more information about creating a map view, see the section <u>"Setting up the monitoring area"</u>.



Fig. 10. Map view

You can select individual devices by selecting the checkboxes near the device.



The following are the map navigation controls that are available in the map view.

Table. 6. Map navigation controls				
Map navigation control	Description			
< ↓ ►	Pan control is used to move the map in the up, down, left, and right directions. You can also pan the map by clicking and dragging on the map view.			
 ⊙ 	Zoom control is used to zoom in or zoom out the map view. You can also use the scroll button on the mouse, to zoom in or zoom out the map view.			
Default Map A	WDM allows you to configure multiple maps to reflect the real plant topology. By default, the default Map appears. Click the map list and select the required map to be displayed.			
	Allows to navigate to Monitoring window.			
>>>	Expands the entire options provided below. 🔀 面 용 🥃 🛛 : 😂 ⓒ ⓒ ⓒ []			
\$	Allows to customize the device list by filtering the devices. See Section " <mark>Manage Filters</mark> " for more information			
	Allows to add a Map.			
Ē	Allows to remove devices from Map.			
৵ᡐ	Displays the connection Status Options which enables you to define the quality thresholds for link quality. For more information about Connection <u>Quality Configuring</u> <u>Connection</u>			
Ē	Displays the property panel.			

 Table. 6.
 Map navigation controls

÷	Allows to select/ unselect devices.
\odot	Allows to view the devices in the map.
\odot	Displays the Device Replacement Help window.
::	Displays Full screen.
Ø	Following options displays: • View • Overlay
Show Map < View Show Grid Overlay Lock Map Map Opacity Collapse All Expand All	 The View option provides options for controlling the map displayed. The following are the View options: Show Map: Select the Show Map check box to display the map image. Show Grid: Select the Show Grid check box to display grid overlay on the map. Lock Map: Select the Lock Map check box to lock the map, locking of the map prevents moving of devices. Map Opacity: Move the slider to adjust the opacity of the map. Move the slider left to increase the visibility (fade in) of the map and move the slider right to decrease the visibility (fade out) of the map. Collapse All: Click the Collapse All option to collapse all expanded devices on the map.
	Overlay to view the Overlay options. The Overlay options provides options for controlling connections displayed. The following are the Overlay options: Display No Connections

	Display All Connections
Display No Connection < Overlay	Display All Connections
Display All Connection	Display Routing Connections
Display Routing Connections	Display Synchronization Connections
Olisplay Synchronization Connections	Attention
	Depending on the Overlay option selected, the other options
	available are displayed.
Display No Connection Overlay	Click the Display No Connections option for not displaying any connections on the map.
Display All Connection Display Routing Connections	
Display Synchronization Connections	
	Click the Display All Connections option for displaying all connection details on the maps. The following are the options:
Display No Connection (Overlay	Show Inactive Connections: Select the Show Inactive
Show Inactive Connections Display All Connection No Display Of Data Display Routing Connections	Connections check box to display inactive connections.
Display RSQI Display Synchronization Connections	No Display of Data: Click No Display of Data for not
O Display Tx Fail Ratio	displaying the data.
	• Display RSQI: Click Display RSQI to display RSQI.
	• Display RSSI: Click Display RSSI to display RSSI.
	• Display Tx Fail Ratio: Click Display Tx Fail Ratio to
	display Tx Fail Ratio.
	Click the Display Routing Connections option for displaying all routing connection details on the maps. The following are the options:
	Show Secondary Connections: Select the Show
	Secondary Connections check box to display
Display Mc Connection Coverlay Display All Connection	secondary connections.
Show Secondary Connections No Display Routing Connections Display Synchronization Connections	No Display of Data: Click No Display of Data
Display RSQI Display RSSI Display RSSI Display Tx Fail Ratio	• for not displaying the data.
Display Routing Level	• Display RSQI: Click Display RSQI to display RSQI.
	• Display RSSI: Click Display RSSI to display RSSI.
	• Display Tx Fail Ratio: Click Display Tx Fail Ratio to
	display Tx Fail Ratio.
	Display Routing Level: Click Display Routing Level to
	display routing level.

Otsplay No Connection	Click the Display Synchronization Connections option for
buyery in Contractor buyery in Contractor buyery and Contractor	displaying all clock connection details on the maps. The following are the options:
No Display Of Data Display XFQ1	 Show Secondary Connections: Select the Show Secondary Connections check box to display secondary connections.
Display Time Mester Address Display Time Distribution Level	 No Display of Data: Click No Display of Data for not displaying the data.
	• Display RSQI: Click Display RSQI to display RSQI.
	• Display RSSI: Click Display RSSI to display RSSI.
	 Display Tx Fail Ratio: Click Display Tx Fail Ratio to display Tx Fail Ratio.
	• Display Clock Sigma: Click Display Clock Sigma to display clock sigma. Clock sigma represents the standard deviation of clock corrections with respect to a node and a neighbor in units of microseconds.
	• Display Time Master Address: Click Display Time Master Address to display time master address. The Time Master Address is the network address of the time master access point.
	• Display Time Distribution Level: Click Display Time Distribution Level to display time distribution level. The Time Distribution Level is the distance to the time master.
	For more information about connectivity option ranges, see section <u>"Verifying connectivity using maps"</u>

The device icons in the map view contain the following indicators using which you can analyze the battery level, publishing rate, and bandwidth usage of devices.

Device performance indicators	Description
	Displays the battery level as low, medium, high, or unknown.
1	Displays the publishing rate at which the PV data is published.
4	Displays the bandwidth usage of the devices. This attribute is used to determine the communication resource usage of field devices. It is computed based on the percentage of active neighbors and the percentage of links allocated. When the bandwidth usage becomes 100%, the device is no longer be able to handle additional communication requests.
<u>A</u> ⁰ Line	It represents that the device is line powered

 Table. 7.
 Field device performance indicators

Installing the WDM license

Prerequisites

- Ensure that you have logged on to the OneWireless user interface.
- Ensure that you have a valid WDM license key. You can obtain the license key as a part of OneWireless ordering process.

To install a WDM license

1. On the Left Navigation Menu bar, click **Manage Licenses**. The Licensing window appears and click **CHANGE**.

Honeywell OneWireless	TM 322.1.36.0		③ ⑤ ⑧ Administrator (Administrator)
П номе	Licensing		
	FEATURE	CURRENT STATUS/VALUE	NEW STATUS/VALUE
	Release		
	Number of Access Points	100	
REPORTS	Number of Devices	3000	
ACTIONS	Modbus Interface	Enabled	
	HART Interface	Enabled	
MANAGE DEVICES	OPC Interface	Enabled	
SINGLE SIGN ON	CDA Interface	Enabled	
CHANNELS	GCI Interface	Enabled	
FIRMWARE UPGRADE	ENRAF Interface	Enabled	
EXTERNAL INTERFACES	WirelessHART	Enabled	
SYSTEM V	Field Expandable Wireless IO	Enabled	
	Professional Installation	Enabled	
	Demonstration Only	Enabled	
MANAGE LICENSES			CANCEL CHANGE

2. Type a **System Number** and an **Authorization Number** that you obtained from Honeywell and click **VALIDATE**.

E Honeywell OneW	ireless	^w 322.1			③ 4 Administrator (Administrator)
HOME		Licensing			
MAIN		Licensing			
		System Number !	Authorization Number*		
alarms&events					
REPORTS		FEATURE	CURRENT STATUS/VALUE	NEW STATUS/VALUE	
ICTIONS		Release			
2		Number of Access Points	100		
		Number of Devices	3000		
MANAGE DEVICES		Modbus Interface	Enabled		
SINGLE SIGN ON		HART Interface	Enabled		
CHANNELS		OPC Interface	Enabled		
FIRMWARE UPGRADE		CDA Interface	Enabled		
EXTERNAL INTERFACES		GCI Interface	Enabled		
SYSTEM		ENRAF Interface	Enabled		
		WirelessHART	Enabled		
MANAGE LICENSES		Field Expandable Wireless IO	Enabled		
u		Professional Installation	Enabled		
U LOGOUT		Demonstration Only	Enabled		
0 00001		⁹ Indicates required fields		CANCEL	VALIDATE

Based on the features enabled in the license, the **Licensing** window shows the difference in Status/Value.

ystem Number *	Authorisation Number *	
999999		
FEATURE	CURRENT STATUS/VALUE	NEW STATUS/VALUE
Release	320	320
Number of Access Points	100	100
Number of Devices	500	500
Modbus Interface	Enabled	Enabled
HART Interface	Enabled	Enabled
OPC Interface	Enabled	Enabled
CDA Interface	Enabled	Enabled
GCI Interface	Enabled	Enabled

If your **System Number** and **Authorization Number** are valid, then the **ACTIVATE** button changes to **VALIDATE** button.

An error is displayed if the System Number and the Authorization Number is not valid. To correct the error, enter a valid System Number and ATTENTION Authorization Number and re-try.

3. Click ACTIVATE and click FINISH when done.

rstem Number	Authorisation Number *		
FEATURE	CURRENT STATUS/VALUE	NEW STATUS/VALUE	
Release	320		
Number of Access Points	100		
Number of Devices	500		
Modbus Interface	Enabled		
IART Interface	Enabled		
DPC Interface	Enabled		
CDA Interface	Enabled		
GCI Interface	Enabled		

The WDM license activates and displays the feature status / value as **Enabled**. You can click **Change** to modify and use a different System Number and Authorization Number.

Property panel of WDM, ISA100 Wireless & WirelessHART devices

WDM

Manage Devices		
wdm1 Device Manager		₩ :
Device Manager Summary	MAC Address Filtering	
System Manager	Wireless Protocol Settings	
Device Management	Field Device Network (FDN)	
WDM Statistics	Process Control Network (PCN)	
ISA100 Interface Statistics	Special Interface Network (SIN)	
WirelessHART Interface Statistics	Date And Time	
NTP Status	Wireless Network Silence	
Redundancy	Notes	
Redundancy History		
IP Address Filtering		
	Alarms(1)	
	RESET APPLY	

Fig. 11. WDM Property Panel

TI	£ - 11	+	···!	+l	-1:	properties				
Ine	TOHOWING	table c	iescribes.	the (aitterent	properties	avallable ir	i the r	property	Panel
			0000110000		01111010110	0.000.000		· • • • •	o. o p o. cj	

Property Panel	Description
Device Manager	Device Manager summary information.
Device Manager Summary	
Tag Name : wdm1	
Status : Joined	
Description : Pri_WDM	
Identification	
Vendor : Honeywell	
Model : WDM	
Revision : OW322.1-36.0	
ISA100 Network Address	
IPv6 Address : FE80 :: 4E7C:COA8:FDOB	
EUI64 : 008800FFFF007506	

System Manager	
System Manager	^
Access Point License	
Total AP Licenses :	
Licensed AP Count :	
Unlicensed AP Count :	
Field Device License Total FD Licenses :	3000
Licensed FD Count :	
Unlicensed FD Count :	
Network Topology	Routing Enabled, Line Powered Only 🗸 🗸
Maximum Route Depth :	
Link Quality Threshold :	99
Link Strength Threshold	-95 dBm
Default Join Policy :	Join Enabled 🗸
EUI64 address	008800FFFF007507
Network Information	
ISA100 Subnet ID : WirelessHART Subnet ID :	
Country Code :	
Network Security	
Session Key Rotation Period :	Infinite
ISA100 Network Provisioning	
Over the Air Provisioning :	Enabled ~
Other Statistics	
Join Security Failures :	
Join Security Failures : Capacity Utilized :	
Capacity Utilized : System Manager Statistics	
Capacity Utilized : System Manager Statistics	0.600000 %
Capacity Utilized : System Manager Statistics	0.600000 %
Capacity Utilized : System Manager Statistics RESET STATIST	0.600000 %
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count	0.600000 %
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count - Routers :	0.60000 %
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices :	0.60000 % CS ALL DEVICES
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices : Field Devices as Routers :	0.60000 % CS ALL DEVICES
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Field Devices : Field Devices : Enraf Devices : Enraf Devices :	0.60000 %
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers Field Devices : Field Devices : Enraf Devices :	0.60000 %
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices as Routers : Enraf Devices : FDAP Router Maximum Device Count Enraf Devices :	0.60000 %
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers Field Devices as Routers Field Devices as Routers Enraf Devices : Enraf Devices :	0.60000 % CS ALL DEVICES
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices : Field Devices as Routers : Enrarl Devices : FIELD PROUTER Maximum Device Count Enrarl Devices : System Manager Log level	0.60000 % CS ALL DEVICES
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices : Field Devices as Routers : Enrarl Devices : FIELD PROUTER Maximum Device Count Enrarl Devices : System Manager Log level	0.60000 % CS ALL DEVICES
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices as Routers : Field Devices as Routers : Enraf Devices : Field Devices count Enraf Devices : Log Level : Log Level : Fixed Channels Channel 15 (2425 Mil	0.60000 % CS ALL DEVICES 15 120 25 10 11 High ✓ to): ■
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices as Routers : Field Devices as Routers : Enraf Devices : FDAP Router Maximum Device Count Enraf Devices : System Manager Log level Log Level : Fixed Channels	0.60000 %
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers Field Devices as Routers Field Devices as Routers Field Devices as Routers FDAP Router Maximum Device Count Enrarl Devices : System Manager Log level Log Level : Channel 15 (2425 Mi Channel 20 (2430 Mi	0 60000 % CS ALL DEVICES
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices as Routers : Field Devices as Routers : Enraf Devices : Field Devices count Enraf Devices : Data Devices : Log Level : Fixed Channels Channel 15 (2425 Mi Channel 25 (2475 Mi Channel 25 (0,00000 %
Capacity Utilized :: System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices as Routers : Field Devices as Routers : Enraf Devices : Field Devices as Routers : Enraf Devices : Enraf Devices : Field Devices : Enraf Devices : En	0,60000 % CS ALL DEVICES
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices as Routers : Field Devices as Routers : Enraf Devices : Field Devices count Enraf Devices : Data Devices : Log Level : Fixed Channels Channel 15 (2425 Mi Channel 25 (2475 Mi Channel 25 (0,00000 % CS ALL DEVICES 15 120 25 10 11 High ✓ 12: □ 12: □ 12: □ 12: □ 13: □ 14:
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices as Routers : Field Devices as Routers : Enraf Devices : FIEld Devices count Enraf Devices : System Manager Log level Cog Level : Fixed Channels Channel 15 (2425 Mi Channel 25 (2475 Mi Channel 11 (2405 Mi Channel 11 (2405 Mi Channel 11 (2415 Mi Channel 12 (2415 Mi Channel 13 (2415 Mi Ch	0,60000 % CS ALL DEVICES 15 120 25 10 11 11 High ✓ 12: □ 12: □ 12: □ 13: □ 14: □
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices as Routers : Field Devices as Routers : Enraf Devices as Routers : Enraf Devices : FDAP Router Maximum Device Count Enraf Devices : System Manager Log level Log Level : Fixed Channels Channel 15 (2455 Mi Channel 25 (2475 Mi Channel 12 (2410 Mi Channel 11 (2405 Mi Channel 12 (2410 Mi Channel 20 Channel 20	0,00000 % CS ALL DEVICES 15 120 25 10 11 11 12 12 25 10 11 11 12 12 12 12 12 12 12 12
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices as Routers : Field Devices as Routers : Field Devices as Routers : Enraf Devices : Field Devices as Routers : Channel 15 (2425 Mi Channel 15 (2425 Mi Channel 15 (2410 Mi Channel 11 (2405 Mi Channel 11 (2405 Mi Channel 11 (2430 Mi Channel 11 (2435 Mi Chan	0,00000 % CS ALL DEVICES
Capacity Utilized :: System Manager Statistics RESET STATIST Access Point Maximum Device Count Routers : Field Devices : Field Devices as Routers : Field Devices as Routers : Field Devices as Routers : Field Devices count Errarf Devices : System Manager Log level Errarf Devices : System Manager Log level Fixed Channels Channel 15 (2425 Mi Channel 25 (2475 Mi Channel 25 (2475 Mi Channel 15 (2430 Mi Channel 16 (2440 Mi Chan	0,00000 % CS ALL DEVICES
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices as Routers : Field Devices as Routers : Enraf Devices : Field Devices as Routers : Enraf Devices : Field Devices as Routers : Channel 15 (2425 Mi Channel 25 (2475 Mi Channel 15 (2425 Mi Channel 11 (2405 Mi Channel 11 (2435 Mi Channel 11 (2435 Mi Channel 11 (2435 Mi Channel 11 (2435 Mi Channel 13 (2435 Mi	0,00000 % CS ALL DEVICES
Capacity Utilized : System Manager Statistics RESET STATIST Access Point Maximum Device Count Routers : Field Devices as Routers : Field Devices count Errarf Devices : System Manager Log level Fixed Channels Fixed Channels Channel 15 (2425 Mi Channel 25 (2475 Mi Channel 15 (2430 Mi Channel 15 (2440 Mi C	0,00000 % CS ALL DEVICES 15 120 25 10 10 11 High ✓ t2: □ t2: □
Capacity Utilized : System Manager Statistics RESET STATISTI Access Point Maximum Device Count Routers : Field Devices as Routers : Field Devices as Routers : Enraf Devices : Field Devices as Routers : Enraf Devices : Field Devices as Routers : Channel 15 (2425 Mi Channel 25 (2475 Mi Channel 15 (2425 Mi Channel 11 (2405 Mi Channel 11 (2435 Mi Channel 11 (2435 Mi Channel 11 (2435 Mi Channel 11 (2435 Mi Channel 13 (2435 Mi	0,00000 % CS ALL DEVICES

Network Topology

Displays the number of hops in a network including,

- number of layers
- signal strength
- signal quality

Network Information

Displays the Wireless Network ID and the country code.

Network Security

A security feature that indicates the duration after which the keys are upgraded.

Other Statistics:

Percent Join Failures: The percentage of devices that were unable to join the network.

Percent Capacity Utilized: The utilized percentage of WDM.

System Manager Log level

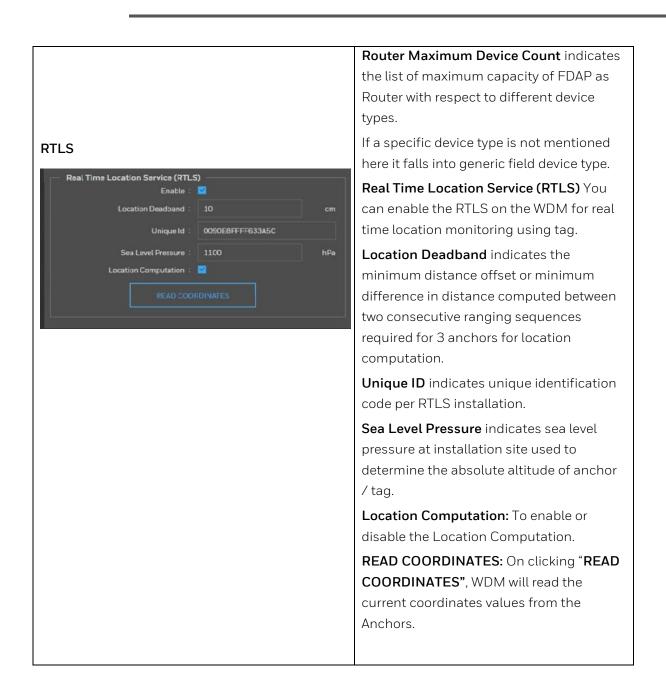
Log Level indicates the priority of the logs. For example, if multiple issues are reported during a short span of time, the Log Level is set to High to collect all the related logs.

Channel Configuration

A minimum of 5 channels must be configured including Fixed and Configurable channels.

Access Point Maximum Device Count

indicates the maximum capacity of Access Point with respect to different device types.



Device Management	Command to reset the WDM and
Device Management	enable/disable the USB ports present on
Device Management	the WDM.
RESETWOM	You can disable the physical USB ports
	present on the WDM for security reasons.
All USB Ports Enable USB Ports :	It provides the WDM Model.
WDM Developer Mode Enable :	Allows to enable the User Interface
	Accessing Over FDN.
WDM Hardware Model : WDMV	You can provide the NTP frequency
User Interface Accessing Over FDN	Tolerance.
Enable : 🗹	
NTP	
Max Ntp Frequency Tolerance : 500	
WDM Statistics	Hardware statistics of WDM.
WDM Statistics	
CPU Free : 98.686506 %	
CPU Free Min : 94.192497 %	
Uptime : 2d, 0h, 50m, 46s	
Current Date	
Current Date : 08/11/2021 Current Time : 09:01:57 AM	
Current TimeZone	
Memory Total : 8144776 kilobytes	
Free : 6777564 kilobytes	
Resource Pools	
Attributes : 103	
Executes Max : 0	
Waiters : O	
Waiters Max : 11	
RESET STATISTICS	
Gateway Log level	
Log Level : Low ~	
Current TimeZone Time Zone : UTC Memory Total : 8144776 kilobytes Free : 6777564 kilobytes Resource Pools Attributes : 103 Attributes Max : 139 Executes Max : 0 Waiters : 0 Waiters : 0 Gateway Log level	

ISA100 Interfac	e Statistics		Statistics of ISA100 Wireless device
ISA100 Interface Statistics Statistics Tran Re Tim	e Statistics Devices Online : 8 Devices Max : 9 Fransmit Count : 6643 Transmit Rate : 0.001185 narmit Rate Max : 27.972029 Receive Count : 360662 Receive Count : 360662 Receive Rate : 2.124989 ceive Rate Max : 17.000000 Timeout Count : 23 Timeout Count : 23 Timeout Rate : 0.00000 count Rate Max : 5.00000 C/CRC failures : 2	msg msg/sec msg/sec msg/sec msg/sec msg/sec msg/sec	Statistics of ISA100 Wireless device connected to WDM.
Wireless HART Interface Statistic Statistics Trai Re Tim	nterface Statistics cs Devices Online : 6 Devices Max : 7 Transmit Count : 6924 Transmit Rate Max : 0.588235 Receive Rate : 0.556475 sceive Rate Max : 1.000059 Timeout Count : 72 Timeout Rate : 0.000000 neout Rate Max : 0.008830 IC/CRC failures : 0	msg msg/sec msg/sec msg/sec msg msg/sec msg msg/sec msg sec msg/sec	Statistics of WirelessHART device connected to WDM.

TP Status				Network Time Protocol (NTP), a networkir
NTP Status			^	protocol for clock synchronization betwee
— System status ——				a server and other devices.
	Mean offset :	-0.595300	msec	
Mea	an frequency offset:	38.881001	ppm	WDM uses NTP for clock synchronization
	Leap indicator :	None		The NTP time source could be an externa
	Sync source :			NTP server or it could be an Access Point
	Last system event :	ClockSync		
— Peer status ———				present in the network.
	Dispersion :	15.164000	msec	
	Root dispersion :	0.000000	msec	
	Peer address :	192.168.253.101		
Pe	er Selection status :	SysPeer		
	Last event :	SysPeer		
Peer association stat	us			
	Host Reachable :			
Pe	rsistent Association :			
Flash error status				
		•		

Redundancy	Details of Primary and Secondary WDMs.
	Includes synchronization state & time, IP
Redundancy	for secondary WDM, various commands to
6	initiate synchronization and switchover,
Summary Redundancy Role : Primary	
Synchronization State : Synchronized	and so on.
Initial Sync Progress (%) : 100	
Inhibit Sync Reason :	
Redundancy Physical ID : B	
Configuration	
Redundancy Enabled :	
Partner PCN IP Address : 192.168.254.12	
Commands	
DISABLE SYNCHRONIZATION	
DISABLE SYNCHRONIZATION	
ENABLE SYNCHRONIZATION	
INITIATE SWITCHOVER	
TOGGLE PHYSICAL ID	
BECOME PRIMARY	
Status	
Hardware Supported : 🔽 Partner Creds Syncd : 🔽	
Redun Controllability : Equal	
Redun Compatibility: Compatible	
Auto Sync State : Enabled	
Pending Critical Data: 0 bytes Pending Non-Critical Data: 0 bytes	
Last Sync DateLast Sync Date : 08/09/2021	
Last Sync Time : 08:39:10 AM	
Last Loss of Sync Date	
Last Loss of Sync Date : 08/09/2021 Last Loss of Sync Time : 07:17:19 AM	
Statistics	
Tx Count: 716624488 bytes	
Rx Count : 567618800 bytes	
Tx Rate : 3998.245605 bytes/sec	
Rx Rate : 2940.000488 bytes/sec Tx Rate Max : 198054.000000 bytes/sec	
Rx Rate Max : 5880.000000 bytes/sec	
Initial Sync Time Max : 11 sec	
Switchover Time Max : 3947 msec	
RESET STATISTICS	

Redundancy History		Time stamped WDM redundancy events.
Redundancy History	/	
TIME STATE	REASON	
08/09/2021 02:09:10 PM Synchronized	(PrimaryRole)	
08/09/2021 02:08:58 PM SyncinProgress	EnableSyncCommand	
08/09/2021 02:08:58 PM AutoSyncEnabled	EnableSyncCommand	
08/09/2021 02:08:58 PM EnableSyncCommand		
08/09/2021 01:41:42 PM Primary	PreviouslyPrimary	
IP Address Filtering		IP Address Filtering:
IP Address Filtering	^	PCN and SIN ports on WDM are protected
		with IP address filtering. An administrator
 Filter Option 		can allow or deny a client access to PCN
Filtering : Disable	<u> </u>	and SIN ports on WDM by filtering his
Interface type : PCN	<u> </u>	machine IP address.
 IP Address List 		
IP Address 1 :		NOTE:
		Make sure that you do not enter your own
IP Address 2 :		machine IP Address to be denied, as this
IP Address 3 :		may lead to blockage of access to WDM
IP Address 4 :		interface.
IP Address 5 :		
IP Address 6 :		
IP Address 7 :		NOTE:
IP Address 8 :		Configure all IP addresses before enabling
IP Address 9 :		the Filtering Option.

IP Address 10 :

IP Address 12 :

IP Address 17 :

IP Address 19

_

MAC Address Filtering	MAC Address Filtering: PCN and SIN	
	ports on WDM are protected with MAC	
MAC Address Filtering	Address filtering. An administrator can	
	allow or deny a client access to PCN and	
Filter Option	SIN ports on WDM by filtering his machine	
Filtering : Disable 🗸 🗸	IP address.	
	IF dudiess.	
Interface type : PCN ~	NOTE:	
MAC Address List	For a host computer, if MAC is denied	
	and IP is allowed or vice versa, the	
MAC Address 1 :		
MAC Address 2 :	settings may not work as intended.	
MAC Address 3 :	NOTE:	
MAC Address 4 :	Make sure that you do not enter your	
MAC Address 5 :	machine MAC Address to be denied, as	
MAC Address 6 :	this may lead to blockage of access to	
	WDM interface.	
MAC Address 7 :		
MAC Address 8 :	NOTE:	
MAC Address 9 :	Configure all MAC addresses before	
MAC Address 10 :	enabling the Filtering Option.	
MAC Address 11 :		
MAC Address 12 :		
MAC Address 13 :		
MAC Address 14 :		
MAC Address 15 :		
MAC Address 16 :		
MAC Address 17 :		
MAC Address 18 :		
MAC Address 19 :		
MAC Address 20 :		

Wireless Protocol Settings	Wireless protocol used. It could be either a complete ISA100 Wireless/WirelessHART network or a shared network of both ISA100 Wireless and WirelessHART. NOTE WirelessHART license needs to be enabled for WirelessHART or mixed configuration settings to be selected. You may need to install the license and then come back to wireless protocol settings to change
FDN Field Device Network (FDN) IP Address IP Address IP Address: IP Address: IP Address: IP Address: IP Address: IP Address: DHCP Server Settings Enable DHCP : ▼ FDAP IP Address Low : I92.168.253.101 FDAP IP Address High : I92.168.253.150	FDN details
PCN Process Control Network (PCN) IP Address IP Address IP Address Subnet Mask : 255.255.255.0 Default Gateway : 0.0.0	PCN details

SIN Special Interface Network (SIN) IP Address Enable SIN : IP Address : IP Address : IP Address : Subnet Mask : 255.255.255.0 Default Gateway : 0.0.0	 SIN details ATTENTION: Make sure SIN IP address is not in same series of PCN or FDN IP address WDM must reboot after SIN IP address is changed
Date and Time	Data and time information. You can either manually set the date and time or synchronize your WDM with the
Use System Time : System Time Current Time : 01:54:09 PM Current Date : 15 April 2021 SET SYSTEM TIME Use NTP Server :	NTP server.
NTP Server Address :	
TAI Offset (sec) : 35	

Wireless Network Silence Image: Wireless Network Silence Image: Network Silence <th> In this state, only the access points are available while all the other devices are offline. Network Silence can be enabled in 3 ways. On Demand: by manually starting or stopping this feature. Enable Scheduling: by scheduling network silence for a later time along with the duration. Schedule by Date/Time: by scheduling network silence for a later al later date or time along with the start and stop time. </th>	 In this state, only the access points are available while all the other devices are offline. Network Silence can be enabled in 3 ways. On Demand: by manually starting or stopping this feature. Enable Scheduling: by scheduling network silence for a later time along with the duration. Schedule by Date/Time: by scheduling network silence for a later al later date or time along with the start and stop time.
Alarms(1) Alarms(1) PRIORITY START TIME DESCRIPTION Urgent 04/15/2021 7:30:35 PM Demonstration License	Provides the information on Alarms which consists of Priority, Start time and description of the event.
Notes	Add notes specific to WDM, if any.

WirelessHART Devices

EML_65656 WirelessHART(R)			×	
WirelessHART Device Summary	Device Variables			
Device Information	Neighbor Diagnostics			
HART Information	Statistics			
Device Management	Input Publication			
Device Status	Notes			
Wireless Network Id				
Data Read and Write	Alarms(0)			
		RESET	APPLY	

The following table describes the different properties available in the property Panel.

Property Panel		Description
Wireless HART Device S	ummary	Device Summary of the selected device.
WirelessHART Device Summary Tag Name : Status : Description : Default Map : Identification Vendor : Serial Number : Sensor Revision : Template Type :	►ML_65656 Joined Pumphouse Pumphouse Honeywell Emulator 66051 1 Standard	The node manufacturer identification and network identification information and time synchronization information are displayed for both primary and secondary parent.
	FE80::001B:1E17:9906:5656 001B1E17:9906:5656 11 FC_1808 3 AP_0096 4 1 PC_1808 3 AP_0096 4 FC_1808 3 AP_0096 4 FC_1808 3 AP_0096 4	
Short Tag	Emulator 1 4 1 7 415318 HONEYWEL HONEYWEL HONEYWEL HONEYWEL	Overall health of the device. This data is fetched using command 48.

HART Information	Common HART parameters
HART Information	
Polling Address : 1 Max Device Variables : 4 Config Change Counter : 47 Device Profile : WirelessHART Process Automation	
Device Flags C8PSK Multi Drop Only: C8PSK Capable Field Device: IEEE 80215424GHz DSSS: Protocol Bridge Device: EEPROM Control: Multi Sensor Field Device:	
Loop Current Mode : Disabled Loop Current : 4.332500 mA Percent Range : 0.853555 % Write Protect : None Final Assembly Number : 66051 Phy Signalling Code : Wireless	
Device parameters	Common device parameters
Device Management	
Device Drop Off Count : 2 Uptime : 182662 seconds Assigned Rote : Device, Routing_WHART ~ ~ RESET STATISTICS WARM RESTART Firmware Version : 0W3102-05.0	
Routing Assignment Routing Assignment : Routing Enabled	
Battery Estimates Power Source : Battery Powered Battery Life : 365.000000 Days	
Radio Power Level Transmit Power Level : 20 dBm	

		Overall health of the device. This data can
evice Status		be fetched by command 48.
Device Status	^	
	~	
Device Status		
	•	
	•	
	•	
	•	
	•	
	•	
	•	
Extended Device Status		
	•	
	•	
	•	
Device Status0		
	<u> </u>	
Device Status1		
	•	
	•	
	•	
Device Status2		
	•	
	-	
	-	
	-	
	•	
]	
Device Status3		
	-	
	•	
Analog Ch Saturated		
	•	
	•	
Analog Ch Fixed		

OWDOC-X254-en-323A

Wireless Network ID	Network ID details
Wireless Network Id ^ New NetworkId : 3366 Current NetworkId : 3366	
Data Read and Write	Data Write and Read
Catalander all Red Cananadi Red Cananadi </th <th>To read and write the parameters of wireless HART device through custom commands For more information See "Sending control commands to WirelessHART devices"</th>	To read and write the parameters of wireless HART device through custom commands For more information See "Sending control commands to WirelessHART devices"

Device Variables	Device variables. The required slot variables
Device Variables	are configured in one of the burst
	messages by selecting command 9 for
Slot O Device Variable Code : 246 (Primary Variable)	period burst.
Value : 26.000198	
Status : Good, Not Limited	
Unit : °C	
Classification : Temparature	
Slot 1 Device Variable	
Code : 247 (Secondary Variable)	
Value : 5.102450	
Status : Good, Not Limited Unit : mbars	
Classification : Pressure	
L	
Stot 2 Device Variable Code : 248 (Tertiary Variable)	
Value : 58.267445	
Status : Good, Not Limited	
Unit : Percent	
Classification : Analytical	
Slot 3 Device Variable	
Code : 249 (Quaternary Variable)	
Value : 1.154340	
Status : Good, Not Limited	
Unit : mA	
Classification : Current	
Slot 4 Device Variable	
Code : 0 Value : nan	
Status : Bad, Not Limited	
Unit : Unknown	
Classification : Not Classsified	
Slot 5 Device Variable	
Code : 0	
Value : nan	
Status : Bad, Not Limited	
Unit : Unknown	
Classification : Not Classified	
Slot 6 Device Variable	
Code: 0	
Value : nan	
Status : Bad, Not Limited Unit : Unknown	
Classification : Not Classsified	
Stot 7 Device Variable Code : 0	
Value : nan	
Status : Bad, Not Limited	
Unit : Unknown	
Classification : Not Classsified	

Neighbor Diagnostics	Neighboring devices in the same network.
Neighbor Diagnostics	These are the devices with which the selected device can communicate.
TAG NAME CONNNECTION TYPE RSSI (DBM) RSQI RECEIVE SUCCES MAP03_DA38_1802 Primary -51 224 188 MAP6_1552S_C580 Secondary -55 217 219	The table displays the signal strength, packet transfer rate, receive and transmit success rate, and connection type of these devices.
Statistics	Publication statistics of WDM.
Statistics Command Message Totals Request : 722 Response : 722 Timeout : 1	The commands sent by WDM, the response time for each command, and total messages that were published since the device is online.
Publish Messages Totals Publish Count : 3761 Availability Available Since : 12/31/1969 23:59:59:204868 Availability : 99:966805	It also displays the availability of the device in the network and the duration the device has been online since joining the network for the first time.
Other Statistics Average Latency : 0.156159 sec Average Turnaround Time : 1.795833 sec	Average Latency is the average time taken for a packet available at device to reach the WDM.
	Average Turnaround time is average time it has taken for a request sent by WDM and response to come back at WDM.

nput Publication			shing (Burst message) feature of essHART devices.
Input Publication	^		
Burst Message 0	: Active as Configured	The b	urst configuration can be defined for
Burst trigger mode Actual burst rate	Continuous Obseconds		device.
Minimum burst rate	; 60 seconds 🗸		
Maximum burst rate State limit	: 60 seconds 🗸	There	would be multiple burst messages for
Burst mode control		each	device. Only one burst message is
Burst command Source device	Crind 9 (Device Variables with Status) EML_65656		
Source device	: EML_00636 ~		le to configure 8 seconds or lesser. All
Slot O	; 296 (Primary Variable) 🗸 🗸	other	burst messages can be configured for
Slot 1 Slot 2	247 (Secondary Variable)	16 se	conds or greater only.
Slot 3	249 (Quaternary Variable)	1000	
Slot 4	; 250 (Not Used) 🗸		
Slot 5	; 250 (Not Used) ~		
Slot 6	250 (Not Used)		
Statistics			
Messages Received	: 3045		
Success Rate (%)	; 100		
Average Update Time (sec) Maximum Update Time (sec)	59.999672 : 61		
- Burst Message 1			
Burst Status	Disabled		
Actual burst rate	: Continuous : Oseconds		
Minimum burst rate	: 60 seconds v		
Stale limit	: 5		
Burst mode control	: Disabled v		
Burst command Source device	: Cmd 1 (Primary Variable) : EML_65656		
Device Variable Codes			
Siot O Siot 1	250 (Not Used) ~		
Slot 2	: 250 (Not Used) 🗸		
Slot 3	250 (Not Used)		
Slot 4 Slot 5	250 (Not Used)		
Slot 6	250 (Not Used)		
Silot 7	250 (Not Used)		
Statistics	. 0		
Messages Missed	. 0		
Success Rate (%) Average Update Time (sec)	. o		
Maximum Update Time (sec)	: 0		
Burst Message 2 Burst Status	. Disabled		
Burst trigger mode	: Contínuous		
Actual burst rate Minimum burst rate			
Maximum burst rate Stale limit	and the second s		
Stalo limit Burst mode control			
	: Crind 3 (Dynamic Variables/Loop Current) 🤍		
Source device	: EML_63636 v		
Slot O	; 250 (Not Used) ~		
	250 (Not Used) ~ 250 (Not Used) ~		
	250 (Not Used)		
Stat 4	250 (Not Used) 🗸 🗸		
	250 (Not Used)		
	250 (Not Used)		
Statistics			
Messages Received Messages Missed			
Success Rate (%)	: 0		
Average Update Time (sec) Maximum Update Time (sec)			

Notes	Add notes specific to the WirelessHART
Notes ^	device, if any.
notes	

ISA100 Wireless Devices

PD_573 ISA100					¥ :
ISA100 Device Summary	~	Network Address Filter			~
Channel Configuration	~	Statistics (UAP)			~
Device Management	~	Application Management			~
Data Layer Management	~	Radio Disconnect History			~
Neighbor Diagnostics	~	Input Publication			~
Channel Diagnostics	~	Notes			~
Statistics (DMAP)	~				
		Alarms(1)			~
			RESET	APPLY	

Property Panel		Description
ISA100 Device Summa	ary	Device summary for the selected device.
ISA100 Device Summary	PD_573 Joined Boiler Boiler Honeywell STW TempAIDO \$102030405060708 OW3221-35.0 Sensor version 001 Standard 1 FE80 :: 0102030405060708 0102030405060708 22 FDAP2_R320_FB03 5 FC_1808 3 2	
Time Master Address : Primary Parent : Primary Address : Secondary Parent : Secondary Address : Time Distribution Level :	FDAP2_R320_F803 5 FC_1808 3	
Channel Configuration Channel Configuration Channel 1 : Channel 2 :	Al	List of channels (objects) supported for the selected device.
Device Profile parameters Device Profile Parameters Device Identity : CTS Version : ITS Version : Plag Status Fault in Sensor or Actuator Element : Detail Information Available :	0048574C40040001 1 2	Standard device parameters.

evice Vendor Parameters	This information is dependent on the vendor of the tendor of t	٦e
Device Vendor Parameters	 ISA100 Wireless device. 	
Diag Status Detail		
SPI Comm Fail :		
RAM Fault :		
Flash Fault : 🔵		
EEPROM Fault :		
Device Revision : 1 Software Version : 1		
Device Power		
Power Source : AA size - 2 Batteries		
Battery Voltage : 0.000000	Votts	
Battery Read Timeout : 28800		
Temperature : 21.360001	degC	

evice Management	Device specific information.
Device Management	Routing Assignment: Role of the device currently
Power	routing device or I/O device.
Routing Assignment	Role Capability: Roles the device can play.
Fast Discovery : Not Applicable	
Routing Assignment : Routing Disabled \checkmark Join Assignment : Join Disabled \checkmark	Assigned Role: Role assigned to the device by WDM.
ISA100 Join Status : Join Disabled	Join Command: Specifies applicable restart action
Role Capability	Uptime indicates the duration for which it has bee
Provisioning Device : 💿 System Time Source : 💿	online since the last join.
	Restart Count is the number of times the device
Gateway : Access Point :	has been restarted, whatever the reason.
Routing Device : 🔵	
I/O Device : 🛛 🔵	Device Drop Off Count is the number of times that
Assigned Role	a device has dropped off from the network.
	By enabling HighThrough Put Link feature, ISA
System Time Source : O	100 wireless devices communication improves,
	and they do not go to the sleep mode. This featur
	can be enabled only for Line Powered Devices.
I/O Device :	If you are using an Enraf Flexline/WFI devices and
Command Join Command : None ~	Engauge Tool to talk to devices, you need to enab this setting for the Flexline/WFI Device you are
Uptime and Connectivity Uptime : 191094 seconds	reading the information from If you are using to
Restart Count : 19	scan all Flexline/WFI devices using Engauge tool
Device Drop Off Count : 0	please enable this setting for all Flexline/WFI
	devices in the network.
Communication Redundancy	
Comm Redun State : Redundant Comm Redun Ratio : 99 percen	
Comm Redun Alarm : 💆	Neighbor Discovery: Device discovers new
ISA100 Protocol Version	neighbors as per the configured frequency. Do no
Version : STK-2.0	change these settings unless you really want the
High Throughput Link Enable :	
	device to discover routers nearby faster. Making
Neighbor Discovery Frequency : 1 hour	faster discovery reduces battery life of the device.
Radio Diagnostics	
Radio Comm Fail : O	
Battery Estimates	
Percent Remaining : 69 percent	
Years Remaining : 4.723288 years	

Data Layer M	anagemen	t	_	Wireless t	ransmit po	ower level.		
ata Layer Managemen	t	^						
- Radio Power Leve	ι							
Transmit Power	Level : 16	dBm						
Naisekkas Dia								
Neighbor Dia	gnostics			Neighbor Diagnostics				
Neighbor Diagnostics TAG NAME CONN	INECTION TYPE RSSI (DBI	M) RSQI RECEIVE SUCCESS T	TRANSMIT SUC	TRANSMIT SUCCESS	TRANSMIT FAIL TR	ANSMIT CCA BACKOFF	TRANSMIT NACK	
FDAP2_R320_FB03			10546					1
FC_180B	Secondary -36	248 1760						-14
device can co This table disp	mmunicate plays the sig	gnal strength, p						
device can co This table disp connection ty	mmunicate blays the sig pe of these	gnal strength, p		ansfer rate,	receive ar	nd transm		
device can co This table disp connection ty Channel Diag	mmunicate blays the sig pe of these I notics	gnal strength, p	oacket tra	ansfer rate, Channel ii	receive ar	nd transm n.	it succes	s rate, and
device can co This table disp connection ty	mmunicate blays the sig pe of these I notics	gnal strength, p		ansfer rate, Channel in No ACK &	receive ar nformation CCA Back	nd transm n. coff indica	it succes	s rate, and
device can co This table disp connection ty Channel Diag	mmunicate blays the sig pe of these motics	gnal strength, p devices.	oacket tra	ansfer rate, Channel ii	receive ar nformation CCA Back	nd transm n. coff indica	it succes	s rate, and
device can co This table disp connection ty Channel Diag	mmunicate blays the sig pe of these I notics	gnal strength, p	oacket tra	ansfer rate, Channel in No ACK &	receive ar nformation CCA Back	nd transm n. coff indica	it succes	s rate, and
device can co This table disp connection ty Channel Diag	mmunicate blays the sig pe of these motics	gnal strength, p devices.	oacket tra	ansfer rate, Channel in No ACK &	receive ar nformation CCA Back	nd transm n. coff indica	it succes	s rate, and
device can co This table disp connection ty Channel Diag Channel Diagnostics CHANNEL	mmunicate blays the sig pe of these motics	gnal strength, p devices. CCA BACKOFF	oacket tra	ansfer rate, Channel in No ACK &	receive ar nformation CCA Back	nd transm n. coff indica	it succes	s rate, and
device can co This table disp connection ty Channel Diag Channel Diagnostics CHANNEL 11	mmunicate blays the sig pe of these motics NOACK	gnal strength, p devices. CCA BACKOFF 0	oacket tra	ansfer rate, Channel in No ACK &	receive ar nformation CCA Back	nd transm n. coff indica	it succes	s rate, and
device can co This table disp connection ty Channel Diag Channel Diagnostics CHANNEL 11 12	mmunicate blays the sig pe of these Inotics NOACK 0 0	gnal strength, p devices. CCA BACKOFF 0 0	oacket tra	ansfer rate, Channel in No ACK &	receive ar nformation CCA Back	nd transm n. coff indica	it succes	s rate, and
device can co This table disp connection ty Channel Diag Channel Diagnostics CHANNEL 11 12 13 14	mmunicate plays the sig pe of these motics NOACK 0 0 0 0	gnal strength, p devices. ССА ВАСКОFF 0 0 0 0	oacket tra	ansfer rate, Channel in No ACK &	receive ar nformation CCA Back	nd transm n. coff indica	it succes	s rate, and
device can co This table disp connection ty Channel Diag Channel Diagnostics CHANNEL 11 12 13	mmunicate olays the sig pe of these notics NOACK 0 0 0	gnal strength, p devices. CCA BACKOFF 0 0 0	oacket tra	ansfer rate, Channel in No ACK &	receive ar nformation CCA Back	nd transm n. coff indica	it succes	s rate, and

Statistics (DMAP)	Read/Write/Execute requests sent by WDM.
Statistics (DMAP)	
Read Message Totals	
Request : 3324	
Response : 3324	
Timeout : 0	
Write Message Totals	
Request: 97	
Response : 97	
Timeout : 0	
Execute Message Totals	
Request : 308	
Response : 307	
Timeout : 0	
Availability	
Availability Since : 12/31/1969 23:59:59:073663	
Availability: 99.939697 %	
RESET STATISTICS	
Radio Disconnect History	The history of last 5 disconnect reasons from the
Radio Disconnect History	network.
RADIO DISCONNECT HISTORY	
Time Sync Clock Timeout	
Power On	
Power On	
Power On	

	1
Statustics UAP	Statistics related to WDM communication with the
Statistics (UAP)	field device.
Publication Message Totals	
Input: 3185	Statistics includes publications sent between the
Input Missed : 0 Input Stale : 0	
Output : 0	device and the WDM,
Output Timeout : 0	This table captures the number of requests sent by
Publication Success Rate : 100,000000 percent Publication Latency : 5.517426 sec	WDM and the responses given by the device for
Function Laterity - 3.31/420 Set	
Read Message Totals Request : 82	Read/Write/Execute messages.
Response : 88	
Timeout : 0	
Turnaround Time : 13.256098 sec	
Write Message Totals	
Request : 0	
Response : 0	
Timeout : 0 Turnaround Time : 0.000000 sec	
Execute Message Totals Request : 0	
Response : 0	
Timeout : 0	
Turnaround Time : 0.000000 sec	
RESET STATISTICS	
Application Management	Static revision number.
Application Management	
Static Revision : 3	
	Attributes (abjects) of the device set of the
Input Publication	Attributes (objects) of the device selected for
Input Publication	Attributes (objects) of the device selected for publication.
Input Publication	
	publication.
Input Publication	publication. Some devices have only Input Publication
Publication Group1 Contract Status : Active	publication.
Input Publication Publication Group1 Contract Status : Active Rate : 1 minute	publication. Some devices have only Input Publication
Input Publication Group1 Publication Group1 Contract Status : Active Rate : 1 minute Stale Limit : 5 Destination : wdm1 Attribute 1	publication. Some devices have only Input Publication attributes while others have Output Publication
Input Publication Group1 Publication Group1 Contract Status : Active Rate : 1 minute State Limit : 5 Destination : wdm1 Attribute 1 Channet : CH01_AI	publication. Some devices have only Input Publication attributes while others have Output Publication
Input Publication Group1 Publication Group1 Contract Status : Active Rate : 1 minute State Limit : 5 Destination : wdm1 Attribute 1	publication. Some devices have only Input Publication attributes while others have Output Publication
Input Publication Group1 Publication Group1 Contract Status : Active Rate : 1 minute State Limit : 5 Destination : wdm1 Attribute 1 Channet : CH01_AI	publication. Some devices have only Input Publication attributes while others have Output Publication
Input Publication Group1 Contract Status : Active Rate : 1minute State Limit : 5 Destination : wdm1 Attribute 1 Channel : CH01_AI Attribute : PV	publication. Some devices have only Input Publication attributes while others have Output Publication
Input Publication Group1 Contract Status : Active Rate : 1 minute State Limit : 5 Destination : wdm1 Attribute 1 Channel : Channel : CH01_AI Attribute 2	publication. Some devices have only Input Publication attributes while others have Output Publication
Input Publication Group1 Publication Group1 Contract Status : Active Rate : 1 minute Rate : 1 minute State Limit : 5 Destination : wdm1 Attribute 1 Channet : CH01_AI Attribute 2 Channet : CH02_BI Channet : CH02_BI	publication. Some devices have only Input Publication attributes while others have Output Publication
Input Publication Group1 Contract Status : Active Rate : 1 minute State Limit : 5 Destination : wdm1 Attribute 1 Channel : Channel : CH01_AI Attribute 2 Channel : Channel : CH02_BI	publication. Some devices have only Input Publication attributes while others have Output Publication

Notes	Add notes specific to the ISA100 Wireless device, if
Notes ^	any.
notes	



The same parameters are available for the thumb adapter too. For wired HART devices however, the parameters vary. See the user interface for correct parameters.

Configuration

Loading the Device Description file

A Device Description (DD) file is usually a zip file that can be downloaded from the https://process.honeywell.com website. It contains information about the device type, commands that are supported by the device, and other device-specific data. A DD file for a particular field device is used to describe the device and to interpret messages and the device status.

!	• The Device Description (DD) files are available only for ISA100 Wireless devices.
ATTENTION	• To ensure consistency in the channel names, load the DD files before the device joins the network.

To load the Device Description file for ISA100 Wireless devices

- 1. Click Maintenance from Left Navigation Menu bar and Select Templates.
- 2. Click Load.

The File Open dialog box appears.

- 3. Select the Device Definition (DD) file or Modbus configuration backup file to the Wireless Device Manager.
- 4. To delete the existing ISA100 DD file, click **Delete.**
- 5. Repeat steps to load the ISA100 DD/Modbus files for all the device types.

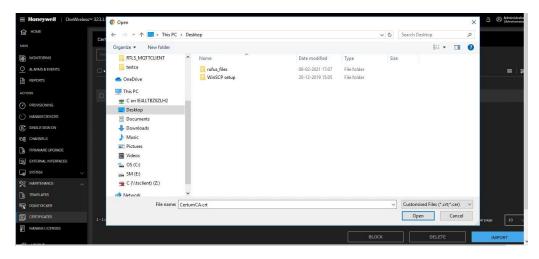
Loading the Certificate

This feature helps to import the certificates to the WDM. CA certificate must be imported for MQTT connection. Secure connections between the RTLS and WDM requires a handshake after the connection is established. During the handshake, the server sends a certificate to the client, the client then verifies against a set of trust certificates. It also checks the certificate to ensure that it has not expired. Verifying the certificate is trusted requires that a trust certificate store be loaded prior to establishing the connection.

The client will send a certificate to the server only if the server requests one. This is known as client authentication. Using the certificate(s), cipher parameters are passed between the client and server to set up the secure connection. Even though the handshake is performed after the connection is established, the client or server can request a new handshake at any point in time.

To load the Certificate

- 1. Click **Certificates** from Left Navigation Menu bar.
- 2. Click **Import** from the **Certificates**.



- 3. Browse and select the certificate file (.crt or .cer) available and click Open.
- 4. The certificate status appears as **Active** on the **Certificates** Window, if the certificate is valid.

= Honeywell OneWir	eless™ 323.1.01.0				() (Administra (Administra
偷 HOME	Certificates				
	Select Certificate Type				
MONITORING					
					■
REPORTS	ISSUED TO 🗘	ISSUED BY	EXPIRATION DATE	SERIAL NO 🗘	STATUS 0
ACTIONS	MyTostCA	MyTestCA	12/08/2022 10:13:11 PM	568481F2E65C502A054F07C547	Active
MANAGE DEVICES					
SINGLE SIGN ON					
E CHANNELS					
RRNWARE UPGRADE					
EXTERNAL INTERFACES					
	×				
POINT PICKER					
	1 - 1 of 1 records		Go to page 1	\rightarrow	Records per page 10
MANAGE LICENSES				BLOCK	LETE IMPORT

- 5. To delete the existing certificate, select MytestCA and click DELETE.
- 6. A pop -up window appears for the confirmation, click **DELETE.**

= Honeywell OneWirel	less™ 323.1.01.0				a (8)	Administrate (Administrate
Sector States - Sector Sector						
I HOME						
MAN						
ACTIONS						
			Delete Certificates			
SINGLE SIGN ON						
ELE CHANNELS		Are you su	e you want to delete the selected certificat	tes?		
B FIRMWARE UPGRADE						
EXTERNAL INTERFACES		CAN	CEL DELETE			
G SYSTEM V						
TEMPLATES						
POINT PICKER						
MANAGE LICENSES						L
டு பலையா					DELETE. IMPO	RT
	0 WirelassHART - 0 / Unterf - 10 Hich - 10 Medium (Jan 12, 202	

- 7. To block the existing Certificate, select $\ensuremath{\text{MytestCA}}$ and click $\ensuremath{\text{BLOCK}}.$
- 8. A pop -up window appears for the confirmation, click **BLOCK.**

= Honeywell OneWireless	[™] 3231.01.0				(). (Administrate
D HOME					
MAIN					
MONITORING					
ALARMS & EVENTS					
REPORTS					
ACTIONS					
MANAGE DEVICES		Block	Certificates		
SINGLE SIGN ON					
CHANNELS		Are you sure you want	to block the selected certificates?		
FIRMWARE UPGRADE					
EXTERNAL INTERFACES		CANCEL	BLOCK		
SYSTEM V					
MAINTENANCE					
TEMPLATES					
POINTPICKER					
CERTIFICATES					
MANAGELICENSES					
U LOGOUT					IMPORT
Access Doints - 0 IS&100 - 0 W	Greless HART - 0 📩 Urnert - 🦛 Binh - 🦚 Merlium - 🖷	I av 🙃 Non-redundante No Dartner - Ob	unical ID + NA		Inn 12 2022 12-20-15

9. The certificate status changes to **Blocked** on the **Certificates** Window as shown below.

OneWireless	× +				v – 0
	t secure https://192.168.0.2/ma	-			익 🖄 🏚 😩
👖 Apps M Gmail 💽 You	Tube Ҟ Maps 📙 OneWireles	5			E Reading
Honeywell OneWireless*	₩ 323.1.02.0				Administrator Admi
HOME	Certificates				
	Certificates				
	⊠ • S				≡ ≉
REPORTS	ISSUED TO 🗘	ISSUED BY 🗘	EXPIRATION DATE	SERIAL NO 🗘	STATUS 🗘
ACTIONS	MyTestCA	MyTestCA	12/08/2022 10:13:11 PM	5684B1F2E65C502A054F07C547_	Blocked
SINGLE SIGN ON					
BE CHANNELS					
FIRMWARE UPGRADE					
References					
SYSTEM V					
S MAINTENANCE ^					
TEMPLATES					
POINT PICKER			Go to page 1	\rightarrow	Records per page 10 🗸
CERTIFICATES				BLOCK DEL	ETE IMPORT
Ш LOGOUT					
Access Points - 0, ISA100 - 0, Wir	relessHART - 0 🦨 Urgent 🕕 High 📀 M	adium 🔞 Low 🔘 Non-redundant - No Partner 🏻 Phys	ical ID - NA		Jan 20, 2022, 4:14:47 I
🕂 🔎 Type here to sea	ırch	0 🛱 🧮 🩋 🥶	🗯 父 👗 🧕	🥥 30°C :	Sunny へ 📥 🖫 🕬 🕺 4:15 PM 🖓

10. Once the certificate expires, the MytestCA status appears as Expired.

← → C ▲ Not secu	re https://192.168.0.1/manageCertific	ates			Q @ 🛧 🗯 🗖 😩
	323.1.01.0				() (Administrator
101 HOME	Certificates				
	Select Certificate Type				
					≡ ≇
REPORTS	ISSUED TO 🗘	ISSUED BY 🗘	EXPIRATION DATE	SERIAL NO 🗘	STATUS 🗘
ACTIONS	MyTestCA	MyTestCA	12/08/2022 10:13:11 PM	5684B1F2E65C502A054F07C547	
SINGLE SIGN ON					
CHANNELS					
FIRMWARE UPGRADE					
EXTERNAL INTERFACES					
SYSTEM V					
MAINTENANCE ^					
POINT PICKER				_	
			Go to page 1	→	Records per page 10 🗸
MANAGE LICENSES				BLOCK DELI	IMPORT

Provisioning

To provision the access points using over-the-air provisioning method

Perform the following procedure to provision the access points using over-the-air provisioning method

- 1. Click **Provisioning** from Left Navigation Menu bar.
- 2. Select Access Points from Select OTA Provisioning and click Next.

Honeywell OneWireless	™ 322.1.37.0			⑦ ④ ⑧ Administrator (Administrator) ✓
III HOME	Provisioning			
	Select OTA Provisioning			
	Access Points Access points can be provisioned using over-the-air provisioning method.	ISA100 Devices ISA100 Wrieless devices and Access points as routers can be provisioned using over-the-air provisioning method.		
ACTIONS	Select Common Join Key Provisioning	Select PDA Provisioning		
	ISA100 And WirelessHART Devices	O Download Keys		
MANAGE DEVICES	WirelessHART and ISA100 devices can be provisioned using Common Join Key method.	ISA100 and WirelessHART devices can be provisioned using provisioning devices.		
	Delete WDM or Devices			
FIRMWARE UPGRADE	O Delete WDM	O Delete Devices	O Delete PDA Devices	
EXTERNAL INTERFACES		Delete the devices from WDM and reset the device to factory configurations.		
SYSTEM V				
🕺 MAINTENANCE 🗸 🗸				
MANAGE LICENSES			BACK	NEXT
U LOGOUT			BACK	HEXT

3. Click Next in Enable OTAP on WDM page.

Access Point Provisioning			
Enable OTAP on WDM Enable Over the air provisioning for Access Points	Device Discovery Un-provisioned Access Points are discovered in the network	Drag and drop your Access Points from list	Summary B Displays all Access Points information
TAG NAME	DEVICE TYPE	STATUS	
wdm1_PCT	Device Manager	OTAP Enable	ed
		BACK	NEXT

4. Select the required access point in the Selection Panel and then click **Accept**.

Enable OTAP on WDM Enable Over the air provisioning Points	for Access Device Discovery Un-provisioned Access Points are discovered in the network	Location Drag and drop your Access Points from list	Summary Displays all Access Points information
Select			
🗹 🖌 🎵 Total Devices !	Selected 1		田 い
TAG NAME	DEVICE TYPE	STATUS	PROGRESS
AP_0096	Access Point	UnProvisioned	Not Started
- 1 of 1 devices	H 4 1 > H	Go to page $1 \rightarrow$	Devices per page 10 💉
MINIMIZE		REJECT	ACCEPT

OWDOC-X254-en-323A

- 5. Reject all unintended devices till the devices that you want to appear in the OneWireless user interface. The unintended devices must not be deleted and must remain in rejected state. This is to make sure that the rejected devices are available for you to provision them in future.
- 6. For rejecting the device, click the required devices and select **REJECT**.

Ð	•	You can select multiple access points from the Selection list,
\mathbf{O}	•	It is recommended that you select and accept only 10 devices at a
ATTENTION		time.

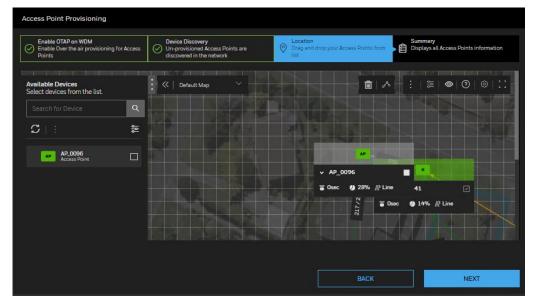
- 7. The confirmation window appears. Click Accept.
- 8. The **Progress** column displays the status as **In Progress**, **Provisioning**, and then **Joined** after completion. Do not close the window when over-the-air provisioning is initiated for devices.

Access Point Provisioning			
Enable OTAP on WDM Compatible Over the air provisioning for Access Points	Device Discovery Un-provisioned Access Points are discovered in the network	Drag and drop your Access Points from list	Summary Displays all Access Points information
Select v			
S			王 (1997) (197
TAG NAME	DEVICE TYPE	STATUS	PROGRESS
AP_0096	Access Point	Provisioned	
1 - 1 of 1 devices	H 4 1 🕨 H	Go to page $1 \rightarrow$	Rows per page $10 \sim$
MINIMIZE		BACK	NEXT

9. Device joins once the progress is completed and click **NEXT.**

Enable OTAP on WDM Enable Over the air provisioning for Access Points	Un-provisioned Access Points are discovered in the network	Drag and drop your Access Points from list	Summary Displays all Access Points information
Select 🗸			
S			⊞ :
TAG NAME	DEVICE TYPE	STATUS	PROGRESS
AP_0096	Access Point	Joined	
- 1 of 1 devices	н «П » н	Go to page 1 →	Rows per page 10
	H 4 1 🕨 H		

10. Drag and dop the Access Point from the list to the map and click **NEXT**.



11. In the **Summary** page you can see all the Access points information. Click **FINISH**.

Enable OTAP o	-	Device Discovery Un-provisioned Access P discovered in the network	oints are 💿 🖸	ocation rag and drop your Access Poi	Summary ints from 🗎 Displays a	, all Access Points information
Points		discovered in the network		st		
TAG NAME	VENDOR	MODEL	SERIAL	RADIO VERSION	APP VERSION	STATUS
AP_0096	Honeywell	FDAP2	2011160002	OW322.1-40.0	OW322.1-40.0	Joined
- 1 of 1 devices		H (1) H	Go to pa		ск	Devices per page 10

- 12. A confirmation message appears to disable OTAP.
- 13. After confirmation, the Access Point is displayed in the selection Panel.

Manage Devices								
Search by category								
S : □ Sho	w Radio Identificatio							⊞ ¥ ≋
TAG NAME	DEVICE TYPE	STATUS	VENDOR	MODEL	REVISION	SERIAL	IPV6 ADDRESS	POWER
💌 wdm1	Device Mana	Joined	Honeywell	WDM	OW322.1-30.0		FE80 : : 4E7C	Line
* AP_0096	Access Point	Joined	Honeywell	FDAP2	OW322.1-25.0	2011160002	FE80::4E7B	Line
FDAP2 🔱	Router	Joined	Honeywell	FDAP2	OW322.1-14.0	2014490009	FE80 : : 0040:	Line
LPFR	Router	Joined	Honeywell	FDAP2	OW322.1-23.0	1033001	FE80 : : 0040:	Line
× 🏟 3308 🖇	WirelessHAR	Offline	Rosemount	266E		1008912	FE80::0018	High
∨ 🖲 то_10	ISA100(R)	Joined	Honeywell	XYR 6000 Te	Temperature	1230000010	FE80 : : 0040:	High
∨ 🛑 CD_47	ISA100	Joined	Honeywell	XYR 6000 Corr	Corrosion ver	S040843000	FE80 : : 0040:	High
PD_573 4	ISA100	Joined	Honeywell	2012	Sensor versio	S102030405	FE80 : : 0102:	High
∨ 🛑 тр_10 🌢	ISA100	Joined	Honeywell	XYR 6000 Te	Temperature	1230000049	FE80 : : 0040:	Low
EML_6 1 - 9 of 9 devices	WirelessHART	Offline	Honeywell	1799 Go to pag		66051	FE80 : : 0018 Devices	High perpage 10 v

To provision the ISA100 Devices using over-the-air provisioning method

ISA100 Wireless devices in the OneWireless Network can be provisioned using over-the-air provisioning method. WDM provisions the access points and the access points that are enabled to function as provisioning devices can provision the field devices/line-powered FDAPs. Provisioning role can be enabled in Honeywell FDAPs when acting as a back bone router or line-powered field router. To enable over-the-air provisioning capability, you must enable this feature in the user interface.

Any access point that is in the factory default state, when connected to the OneWireless Network can join the network as an Non-provisioned device. In this state, the WDM contains only the basic details about the device such as the Tag Name, EUI64, and Radio Revision. Also, there is no active data communication between the WDM and the device in the Non-provisioned state. You can accept or reject a Non-provisioned device using the user interface. If accepted, the WDM sends the provisioning data to the device and the device transitions to provisioning state. A device with the new security data sends a join request to the WDM. This is similar to the join request received by the WDM when a device is provisioned using a provisioning device.

Perform the following procedure to provision the ISA100 devices using over-the-air provisioning method.

1. Click **Provisioning** from Left Navigation Menu bar.

Provisioning			
Select OTA Provisioning			
Access Points Access points can be provisioned using over-the- air provisioning method.	ISA100 Devices ISA100 Wireless devices and Access points as routers can be provisioned using over-the-air provisioning method.		
Select Common Join Key Provisioning	Select PDA Provisioning		
O ISA100 And WirelessHART Devices WirelessHART and ISA100 devices can be provisioned using Common Join Key method.	Download Keys ISA100 and WirelessHART devices can be provisioned using provisioning devices.		
Delete WDM or Devices			
O Delete WDM Delete WDM will reset the WDM to factory configurations.	O Delete Devices Delete the devices from WDM and reset the device to factory configurations.	O Delete PDA	Devices evices from WDM
		АСК	NEXT
	В	AUN	NEXI

 $2. \hspace{0.1in} \text{Select ISA100 Devices and click Next.}$

3. ISA100 provisioning window appears.

ISA100 Provisioning				
Enable OTAP Enable over the air provisioning f	Device Discov or AP 🗮 Un-provisioned network		cation ag and drop your devices from list	Summary Displays all provisioning information
Select	v iscovered 3			⊞ \$
TAG NAME	TIME	DEVICE TYPE	STATUS	PROGRESS
AP_0096	OMinutes	Access Point	Joined	Not Started
FDAP2_R320_FB03	OMinutes	Router	Joined	Not Started
LPFR_0041	OMinutes	Router	Joined	Not Started
1 - 3 of 3 devices	K (1)	M Gotopa	g^{e} 1 \rightarrow	Devices per page 20
		BACK	NEXT	ENABLE FOR 60 MIN

Here you can Manage Filters, manage columns and select the required device for the air provisioning method.

4. Select the device and click **Enable for 60 Min** in **Enable OTAP** page.

ISA100 Provisioning					
Enable OTAP Enable over the air provisioning	for AP Device Discovery Un-provisioned devinetwork		ca tion ag and drop your devices from list	Summary Displays all provisioning informat	ion
🖃 🗸 🛛 🗂 Total Devices S	Selected 1			E	
TAG NAME	ТІМЕ	DEVICE TYPE	STATUS	PROGRESS	
✓ AP_0096	OMinutes	Access Point	Joined	Not Started	
FDAP2_R320_FB03	OMinutes	Router	Joined	Not Started	
LPFR_0041	OMinutes	Router	Joined	Not Started	
1 - 3 of 3 devices	N (1) H	Go to pa	$ge 1 \rightarrow$	Devices per page	20
		BACK	NEXT	ENABLE FOR 60 N	IIN

5. Select the **Tag Name** and click **Accept** in **Device Discovery** page.

ISA100 Provisioning			
Enable OTAP Image: Control of the stress of the s	Device Discovery Un-provisioned device appear in the network	Location Orag and drop your devices from list	Summary Displays all provisioning information
Select V	D		≋ ⊞
TAG NAME	DEVICE TYPE	STATUS	PROGRESS
V PD_585	ISA100	UnProvisioned	Not Started
1 - 1 of 1 devices	₩ 4 1 > ₩	Go to page $1 \rightarrow$	Rows per page $20 \sim$
MINIMIZE	ВАСК	REJECT	ACCEPT

You can accept or reject devices.

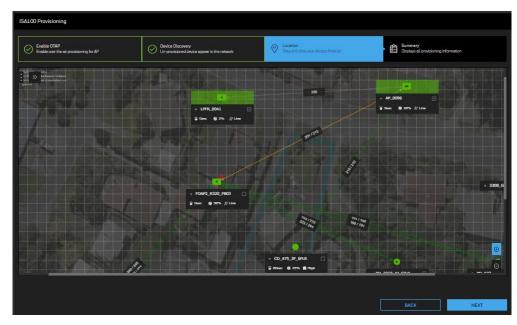
- 6. A pop -up window appears for the confirmation, click **Accept.**
- 7. It takes time to discover and accept the device.

ISA100 Provisioning			
Enable OTAP C Enable over the air provisioning for AP	Device Discovery Un-provisioned device appear in the network	Location Orag and drop your devices from list	Summary E Displays all provisioning information
Select ~			⊞ ≈
TAG NAME	DEVICE TYPE	STATUS	PROGRESS
PD_585	ISA100	UnProvisioned	
1 - 1 of 1 devices	M 4 1 + M	Go to page $1 \rightarrow$	Rows per page 20 \lor
MINIMIZE		ВАСК	NEXT

8. After the device is accepted, click **Next.**

ISA100 Provisioning			
Enable OTAP O Enable over the air provisioning for AP	Device Discovery Un-provisioned device appear in the network	Location Drag and drop your devices from list	Summary B Displays all provisioning information
Select ~			⊞ æ
TAG NAME	DEVICE TYPE	STATUS	PROGRESS
No records found			
0 - 0 of 0 devices	H 4 1 > H	Go to page 1 ->	Rows per page 20 🗸
MINIMIZE		ВАСК	NEXT

9. Drag and drop the devices from the list to the map and click **Next.**



10. You can view all the provisioning information in Summary page.

Enable OTAP Enable over the air pro	visioning for AP	Device Discovery Un-provisioned device appear in the network	Drag and drop your devices f	ion list	Summary Displays all provisioning information
	VENDOR	MODEL	SERIAL	RADIO VERSION	STATUS
PD_585	Honeywell		\$00000000000000000000000000000000000000		UnProvisioned
1 of 1 devices			Go to page $1 \rightarrow$		Rows per page 20

11. After completion, click **Finish.**

12. Click **OK** when confirmation window appears.

To provision line-powered FDAP routers/ field devices using over-the-air provisioning method

ISAL00 Devices ISAL00 Wireless devices and Access points as routers can be provisioned using over-the-air provisioning method.	
Select PDA Provisioning	
O Download Keys ISA1C0 and WirelessHART devices can be provisioned using provisioning devices.	
O Delete Devices Delete the devices from WDM and reset the device to factory configurations.	O Delete PDA Devices Delete the PDA devices from WDM
	BACK
	SALOD Wireless devices and Access points as muters can be provisioned using over-the-air provisioning method. Select PDA Provisioning Download Keys ISALOD and WirelessHART devices can be provisioned using provisioning devices. Delete Devices Delete Devices from WDM and reset the device to factory

1. Select ISA100 Devices from Select OTA Provisioning.

- 2. Select the Access Point and click **Next**.
- 3. Select Enable for 60 Minutes if it is not enabled through WDM from property panel.

The access point functions as a provisioning device for 60 minutes. The Non-provisioned field devices and the line-powered FDAP routers that are in the factory default state start

ISA100 Provisioning Summary Displays all provisioning information Drag and drop your devices from list ø ice appear in the Select 🖃 🗸 | 🎵 | Total Devices Selected 💶 Ħ 흻 тима AP_0096 50 Minut nt(PM) Not Started ~ LPFR 0041 OMinutes Not Started Joined Go to page $1 \rightarrow$ is per pag ENABLE FOR 60 MIN

appearing in the Selection Panel. Note that if you do not accept or reject the devices within 60 minutes, the devices automatically disappear from the user interface.

4. The **Device Discovery** page appears. This page displays all the Unprovisioned devices that you have selected for enabling over-the-air provisioning.

Enable OTAP Enable over the air provisioning for AP	Device Discovery Un-provisioned device appear in the network	Location Drag and drop your devices from list	Summary Displays all provisioning information
Select ~			
🛛 🗸 🛛 🎵 Total Devices Selec	ted 2		田 \$
TAG NAME	DEVICE TYPE	STATUS	PROGRESS
FDAP2_R320_FB03	Router	UnProvisioned	Not Started
LPFR_0041	Router	UnProvisioned	Not Started
- 2 of 2 devices	N 4 1 > N	Go to page $1 \rightarrow$	Rows per page 100 ×

- 5. To reject a device from joining the network using over-the-air provisioning method.
 - Select the required device and click Reject. The Reject Over the Air Devices window displays.
 - Click Reject. The Progress column displays the status as In Progress, and then Completed, when complete.

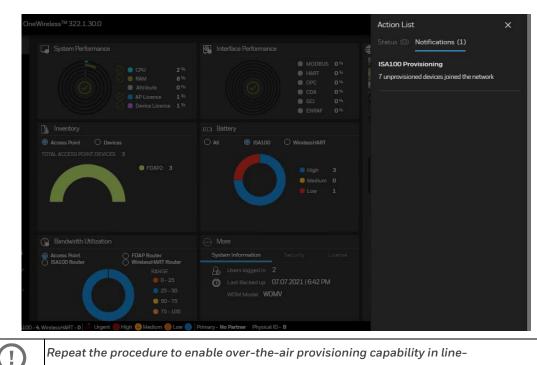
6. Click **Accept**. The **Progress** column displays the status as **In Progress**, **Provisioning**, and then **Joined**, when complete. Do not close the window when over-the-air provisioning is initiated for devices.

ISA100 Provisioning			
Enable OTAP C Enable over the air provisioning for AP	Device Discovery Un-provisioned device appear in the network	Orag and drop your devices from list	Summary Displays all provisioning information
Select ~			
S			田 않
TAG NAME	DEVICE TYPE	STATUS	PROGRESS
FDAP2_R320_FB03	Router	UnProvisioned	
1 - 1 of 1 devices	H 4 1 > H	Go to page $1 \rightarrow$	Rows per page $100 imes$
MINIMIZE		BACK	NEXT

All the line-powered FDAP routers and the field devices that you have selected for over-theair provisioning are provisioned.

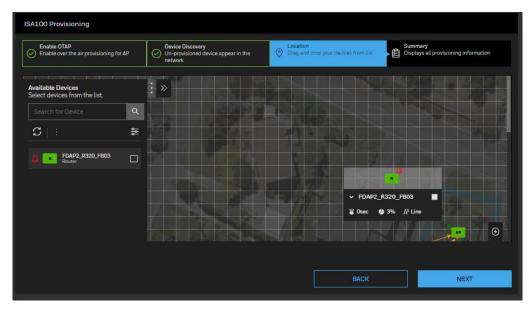
Enable OTAP Enable over the air provisioning for AP	Device Discovery Un-provisioned device appear in the network	Location Drag and drop your devices from list	Summary Displays all provisioning information
Select ~			
S			⊞ :
TAG NAME	DEVICE TYPE	STATUS	PROGRESS
FDAP2_R320_FB03	Router	Joined	
- 1 of 1 devices	M 4 1 > M	Go to page $1 \rightarrow$	Rows per page 100

Also, you can minimize the screen by selecting **MINIMIZE** button and you can view it in the notification bar.



ATTENTION Repeat the procedure to enable over-the-air provisioning capability in linepowered FDAP routers. This enables the line powered FDAP routers to provision distant nodes in the network.

7. Drag and drop the device from the selection list to Map and click **NEXT**.



8. Summary page displays all the provisioning information. Click **FINISH**.

Enable OTAP Enable over the air prov	isioning for AP	Device Discovery Un-provisioned device appear in the network	Location O Drag and drop your	devices from list	nmary plays all provisioning information
TAG NAME	VENDOR	MODEL	SERIAL	RADIO VERSION	STATUS
FDAP2_R320_FB03	Honeywell	FDAP2	2014490009	OW322.1-14.0	Joined
- 1 of 1 devices		H 4 1 1 H	Go to page 1 →		Rows per page 100

- 9. To filter the device list:
 - a. Select Manage Devices from Left Navigation Menu bar.
 - b. Go to the filter option 🚔, expand Status > Un-Provisioned

The Non-provisioned devices appear in the Selection panel. The extended Selection panel enables you to view the available device parameters.

The device establishes a communication link with the access point after it attains the Nonprovisioned state. This link persists even if the device is not provisioned using the connected access point. If the device needs to be provisioned using a different access point, reject the device and then delete it from the user interface, so that the device can rejoin through a different access point for provisioning.

Provision the ISA100/WirelessHART devices using Common Join Key

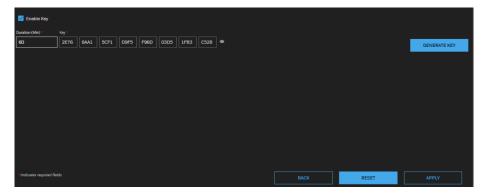
ISA100/WirelessHART devices can be provisioned in the OneWireless Network using Common Join Key method as described below. Any ISA100/WirelessHART device that came out of factory or provisioned for different network can be provisioned into this network without using any specific OEM tool.

To provision the ISA100/WirelessHART devices using Common Join Key

- 1. Select **Provisioning** from Left Navigation Menu bar.
- 2. Select Common Join Key Provisioning for ISA100/WirelessHART Devices as shown below.

Honeywell OneWireless	3221.40.0		③ ① ④ Administrator ~
🛍 номе	Provisioning		
MAN MONITORING ALARMS & EVENTS REPORTS	Select OTA Provisioning O Access Points Access points an be provisioned using over-the-air provisioning method.	O ISA100 Devices ISLI00 Wreless devices and Access points as noters can be provisioned using over- the-air provisioning method.	
ACTIONS	Select Common Join Key Provisioning	Select PDA Provisioning	
PROVISIONING MANAGE DEVICES SINGLE SIGN ON	ISA100 And WirelessHART Devices WeilesHART and ISA100 devices can be provisioned using Common Join Key method.	O Download Keys ISAL00 and WinitesHART devices can be provisioned using provisioning devices.	
E CHANNELS	Delete WDM or Devices		
FIRMWARE UPGRADE EXTERNAL INTERPACES	O Delete WDM Delete WDM will reset the WDM to factory configurations.	O Delete Devices Delete the devices from WDM and reset the device to factory configurations.	O Delete PDA Devices Delete the PDA devices from WDM
SYSTEM V MAINTENANCE V MANAGELICENSES			
ப் Logout			BACK NEXT
		s not supported in R22.	1

- 3. Click Next.
- If the ISA100/WirelessHART devices are shipped from factory, configured with this system network Id and known join key, then in the Key box, type the Common Join Key supplied by the device vendor.
- 5. If the ISA100/WirelessHART devices comes with the unknown key and you want to provision them to this network, then enter the key you need to use for provision, or generate a random key using **Generate Key** button. Configure the Common Join Key and the WirelessHART network ID to the WirelessHART device using any third-party provisioning tools.



- 6. In the Enabled Duration (min) box, enter the duration in minutes and click Apply.
- 7. The device joins the network using the configured network ID and the Common Join Key.
- 8. Click **OK** on the confirmation message.

Provision WirelessHART devices using Over-The-Air (RE)-Provisioning method

WirelessHART devices can be provisioned in the OneWireless Network using Over-The-Air (RE)-Provisioning method as described below. Any WirelessHART device which is factory delivered or provisioned for different network can be re-provisioned into this network over the air without using any specific OEM tool.

To provision WirelessHART devices using WirelessHART Over-The-Air (RE)-Provisioning method

- 1. Select **PROVISIONING** from Menu bar.
- 2. Select Common Join Key Provisioning for WirelessHART Devices as shown in the following image.

Honeywell Ore₩reless™	122.1.40.0		⊙ ⊕ ⊕ Advancement ~
습 HOME	Provisioning		
A NONTOING	Select OTA Provisioning		
D HENORIZ O RYANIZ PEDADIZ AR	C Access Points Access points can be provident using over the an providency method.	O ISA100 Devices SA100 Weeks and Access points as notion can be provisioned using over the ef groupsoring wethout	
401045	Select Common Join Key Provisioning	Select PDA Provisioning	
O PROVISONNE	6 ISA100 And Wireless HART Devices	O Download Keys	
 MANAGEORYCES SHELESEN ON 	Winised-WIT and EdUCD devices can be provisioned using Common Join Reg method.		
ing owned	Delete WDM or Devices		
Primary Linguage Sign controls Sign controls Sign controls	O Delate WDM Delate WDM with Next The WDM to factory configurations.	O Delete Devices Delete the devices how WDM and read the device to factory configurations.	Orderte PDA Devices Dearts the PDA devices from WDM
St MANTTAINCE			
MANAGE LICENSES			MAX NEXT
O 1000/T			

- 3. Click NEXT.
- 4. In the **Key** box, type the key details of the WirelessHART device provided by the manufacturer or key present/stored in the device.

🗹 Enable Key											
Duration (Min) *											
60	2E76	6AA1	5CF1	D9F5	F96D	03D5	1FB3	C528			GENERATE KEY
*Indicates required fie	NCIS								BACK	RESET	

- 5. Enter duration in minutes and click **APPLY**.
- 6. Select Manage Devices from Menu bar.
- 7. Select the required field device access point. The selected Access point must be in the vicinity of the device to be re-provisioned to this network.
- 8. Expand **Device Management** in the Property panel.

9. Under **WirelessHART Over The Air (RE)-Provisioning**, type the WHART provisioning Id provided by the manufacturer or stored in the device in the **WHART provisioning Id** box.

— WirelessHART Over The Air (RE)-Prov	visioning
Time Remaining :	59 minutes
Provisioning :	Enable 🗸
Provisioning Id :	xxxx

- 10. Click **APPLY**.
- 11. After a few minutes, the WirelessHART device joins the network through the FDAP on which Over-The-Air (RE)- provisioning is enabled.
- 12. Select the Wireless HART device from Manage Devices.
- 13. Expand **Wireless Network ID** in the Property panel. In the **New Network Id** box, type the Wireless Network ID of this system.

Wireless Network Id		^
	New Networkid: Current Networkid:	

14. Click **APPLY**.

15. Go to **Device Management** and select **Warm Restart** to the device to join permanently to this network.

The WirelessHART device that you have selected for WirelessHART Over-The-Air RE-Provisioning is provisioned.



16. Disable Over-The-Air (RE)-provisioning in FDAP and Common join key in WDM.

Remove Device

To remove a device

- 1. Click **PROVISIONING** in the Left Navigation Menu bar.
- 2. Select the check box for the provisioning device to be removed from **Delete WDM or Devices** option.

E Honeywell OneWireless ¹⁰⁰ 322.1.14.001					
III I I I I I I I I I I I I I I I I I					
MAIN	Provisioning Choose the type of device to be provisioned.				
MONITORING					
ALARMS & EVENTS					
REPORTS	Select Common Join Key Provisioning				
ACTIONS	ISA100 And WirelessHART Devices				
	WirelessHART and ISA100 devices can be provisioned using Common Join Key method.				
MANAGE DEVICES	Select PDA Provisioning				
SINGLE SIGN ON	O Download Keys				
CHANNELS	- ISA100 and WirelessHART devices can be provisioned using provisioning devices.				
FIRMWARE UPGRADE	provisioning centes.				
EXTERNAL INTERFACES	Delete WDM or Devices				
SYSTEM V	O Delete WDM	O Delete Devices	O Delete PDA Devices		
🛠 maintainance 🗸 🗸	Delete WDM will reset the WDM to factory configurations.	Delete the devices from WDM and reset the device to factory configurations.	Delete the PDA devices from WDM		
MANAGE LICENSES					NEXT
(b) Losour					

- 3. Click **NEXT**.
- 4. Click **DELETE**.

Delete WDM Deleting the WDM remove	es all the configuration data and	resets the WDM to factory de	faults.			
TAG NAME	DEVICE TYPE	LOCATION	VENDOR	MODEL	REVISION	PROGRESS
wdm1	Device Manager	Unplaced	Honeywell	WDM	OW322.1-14.0	Not Started
Reset PCN and FD						
					BACK	DELETE

5. Select **Reset PCN and FDN IP Address** checkbox to reset the IP address.

Delete devices

See section <u>To remove a device</u>: for more information.

Delete PDA Devices

See section <u>To remove a device</u>: for more information.

Android based provisioning for OneWireless Network

This application is developed to provision ISA100 and WirelessHART devices using an Android mobile phone or a tablet.

Prerequisites

- Ensure that you have installed Android application "AndroidProvDev" in your device. You do not need any driver files to be installed into Tablets or Smart phones.
- Ensure that you have logged on to the OneWireless user interface.
- Ensure that the Android mobile phone or a tablet is connected to the computer and the connection status appears in an external device in the computer.
- Android Smart phones must have Bluetooth V4.0 LE (BLE-Bluetooth Low Energy) Compatibility.

Install Android Provisioning Device Application from WDM

Perform the following procedure to Install Android Application from WDM.

1	. Click Syst e	em from left navigation mer	nu and select Software Download.	
	Honeywell On	eWireless™ 322.1.27.0	· ()	Shafana (Administrator) ✓
		Software Download		
	REPORTS	Select Software		
	ACTIONS			
	SINGLE SIGN ON			
	CHANNELS			
	FIRMWARE UPGRADE			
	REAL EXTERNAL INTERFACES			
	SYSTEM A			
	A MANAGE USERS			
	MANAGE ROLES			
	C EXPORT SYSTEM LOGS			
	BACKUP SETTINGS			

2. Select **Android Provisioning Device Application** from the select Software list and click **Download.**

DOWNLOAD

Software Download		
Select Software		
Select Software		
Provisioning Device Application		
OPC-UA Proxy		
Modbus Configuration Backup		
Secure Communication Software		
Android Provisioning Device Application		
	CLEAR	DOWNLOAD

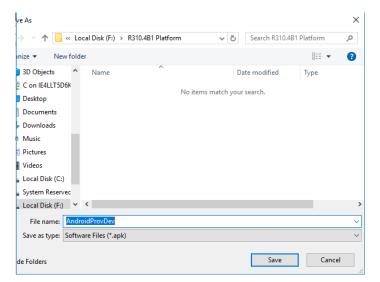
3. Software downloaded successfully message appears after downloading the software.

You can install the Android Provisioning Device Application by following steps:

- Save Android Prov Dev. apk to your Android device.
- Using your Android device, open File Explorer and navigate to AndroidProvDev.apk. Click on the apk file to start the installation.

Application Installation

1. Install the application "AndroidProvDev" file in android device.



2. Download the application "AndroidProvDev" file to computer/laptop (Local

Machine).

3. Transfer "AndroidProvDev" file from computer/laptop to Android mobile like any other file transfer.

4. Go to the location on mobile phone where you have transferred the "AndroidProvDev" file and click the file to install the application.

A pop-up message appears and click **INSTALL** to install the application as shown in the following image.

	OneWireless
	Do you want to install this application?
	CANCEL INSTALL
5.	After a successful installation, click OPEN to launch the application
	S OneWireless
	App installed.
	DONE OPEN

Android device specifications

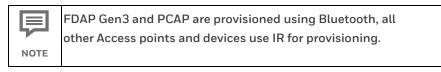
Attribute	Specification
CPU	1 GHz Speed
OS	Android 6.0 or above
Display	5 inches
RAM	2 GB
ROM	32 GB
Connectivity	Bluetooth 4.2 or above

Provisioning

This application is developed for the following Device categories.

- 1. ISA100 BLE Devices
- 2. ISA100 IR Devices
- 3. WirelessHART devices

You can see these protocols while launching the application.



ISA100 BLE

Provisioning Process for ISA100 BLE Devices

1. In the OneWireless application, select **ISA100 BLE** from the Choose Protocol dropdown list..

Choose Pr	ligure Device					
Select						
ISA10	BLE					
ISA100	IR					
Wirele	SHART					
				·		
	Allow I	Bluetooth	n permi	ssion v	vhen pr	ompted

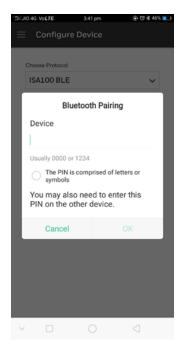
the device. This is

2. Select the available ISA100 BLE Device to get connected with the application.

	{Volte} Configure	12:33 pm e Device	✿ (ê)· 면 \$ 50% ■)
Choo	ese Protocol		
IS/	100 BLE		~
Selec	t Device to C	onnect	φ
Avai	lable Devic	es	
*	WCI_ISA1	00_BLE4084	FFFF00FC0E
*	WCI_ISA1	00_BLE4084	FFFF00FC33
*	WCI_ISA1	00_BLE4084	FFFF00FC06
*	WCI_ISA1	00_BLE4084	FFFF00FC18
*	WCI_ISA1	00_BLE4084	FFFF00FC32
*	WCI_ISA1	00_BLE4084	FFFF00FC07
\sim			

	If the PCAP or FDAP Gen3 is in Reset to factory default state, use the default PIN "192021" to pair the device.
NOTE	If the PCAP or FDAP Gen3 is provisioned to a WDM and default pin is
	changed, see "BLE options" in Table. 7 in Process Control Access Point
	(PCAP) User's Guide / FDAP User's Guide to get the pin number.

3. Provide the PIN number to pair the device.



4. The following options are available after pairing with the device.

"filJ	10 4G Vo LTE	4:15 pm	@• তি ≉ 44% 💽 •
	Actio	ns	
		Device Information	
		Provision Device	
		Tag Name	
		Radio Power Level	
\sim			

Device Information:

Provides the field device information such as; Tag Name, Serial No, Power level and so on.

"filJIO 4G Vo LTE	4:15 pm	(한 영 🕸 44% 💶)
< Devic	e Information	
Tag Name	: T04084FF	EEEOOEC20
Vendor	: Honeywel	
Model	: PCAP	
Serial No	: 1	
EUI64	: 00-40-84 FC-20	-FF-FF-00-
Revision	: OW321.2-	-12.0
IPv6 Addres		0:0000:0000 7B:C0A8:006
Power Level	: -1 dBM	
Subnet ID	: 3	
Join Status	: Joined	
R	ead Device Informa	ation
~ □		
Re	ead Device	Informati
BI	_E device is	connecte
IOTE Th	nis behavior	r is comm

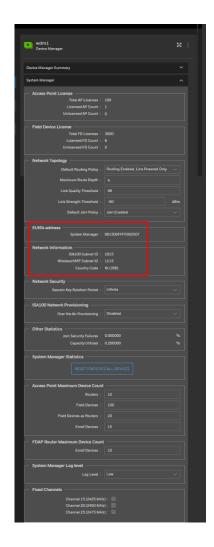
Provision Device

• You can reset or Provision Field Device to a specific network.

Provision information from Honeywell WDM User Interface

1. Get the SMEUI64 and Subnet ID from WDM to update it in mobile application.

ିଶା JIO 4G <i>VoLTE</i>	4:22 ;	om @-ੴ≵43%, 💽
< Provisio	ning	
Subnet ID		
1015		
UtcDrift		
35		
System Manage	r Eui64	
0090E8FFF	F6338F6	5
System Manage	r IP Addres	5
192.168.2	52.15	
Join Key		
2E766AA	1 -	5CF1D9F5
F96D03D	5 -	1F83C528
P	rovision	Device
Rese	t Device	to Defaults
× 🗆		



- SMEUI64 Address: Get the EUI64 address from Honeywell WDM User Interface as highlighted in blue color and the same must be used in SMEUI64 address in the Android Mobile Application.
- Subnet ID: Get the ISA100 Subnet ID from Honeywell WDM User Interface which is highlighted in red and the same must be used in Subnet ID in the Android Mobile Application.

2. Get the IPv4 Address from WDM and Joining Key.

wdm1 Device Manager			52
Device Manager Summary			~
System Manager			~
Device Management			~
WDM Statistics			~
ISA100 Interface Statistics			~
WirelessHART Interface Stat	stics		~
NTP Status			~
Redundancy			~
Redundancy History			~
IP Address Filtering			~
MAC Address Filtering			~
Wireless Protocol Settings			~
Field Device Network (FDN)			^
- IP Address			
	IP Address :	192 168 252 15	
	Subnet Mask :	255.255.254.0	
 DHCP Server Settings 	Enable DHCP :	8	
FDAP	P Address Low :	192 168 253 100	
FDAP I	PAddress High:	192.168.253.150	
Process Control Network (PC	N		~

- Get the IP Address from Honeywell WDM FDN (Field Device Network) Address as highlighted in the earlier image and use the same in Android Mobile Application.
- Get the common Join Key (Wireless HART provisioning Even though it is reflecting as WirelessHART Provisioning, the same common join key is applicable for ISA100 as well) from Honeywell WDM user interface.
- Select the **Enable Key** check box to provide the Enabled Duration in between 60 to 600 minutes Range.

Enable Key													
Duration (Min)													
60	2E76	6AA1	5CF1	D9F5	F96D	0305	1FB3	C528	٠			GENERATE KEY	
*Indicates required fie										BACK	RESET	APPLY	

5. Once you update the actual values in the Android mobile application, click **Provision Device** to provision.

"ສຳໄJI	0 4G VoLTE 4:	22 pm	@ 🕫 🕸 43% 🔳
	Provisioning		
	Subnet ID		
	1015		
	UtcDrift		
	35		
	System Manager Eui64		
	0090E8FFFF6338	BF6	
	System Manager IP Add	ress	
	192.168.252.15		
	Join Key		
	2E766AA1	-	5CF1D9F5
	F96D03D5	-	1F83C528
	Provisi	on D	evice
	Reset Devi	ce to	Defaults
~			

Now the Access points with BLE successfully joined the network.

Reset Device to Defaults

Select **Reset Device to Defaults** to reset the Access Point from the current network. This drops the Access point connection from current network.

Tag name

- 1. Click **Tag name** to edit/update Tag name.
- 2. You can edit the tag name from the drop-down list or type in the device name as shown in the following image.

রীIJIO 4G Vo LTE 4:22 pm 🛞 তি 🕏 43% 💶)
\leftarrow Tag Name
Tag Name: T04084FFFF00FC20
Change Tag Name
T04084FFFF00FC63
OR Select From List
Device 1
Device 2
Device 3
Device 4
Device 5
Device 6
Device 7
Device 8
Write Tag Name
✓ □ ○

Radio Power Level

- 1. Click Radio Power Level to set the power.
- 2. A confirmation message appears after setting the power level.

៉ះដៀរiO 4G <i>VoLTE</i>	4:22 pm	@- [™] \$ 43%	ł
🗧 Radio P	ower Level		
Power Level : -	1 dBM		
Change Power l	_evel		
-2 dBM		~	
v	Vrite Power Lev	vel	
~			



It is not recommended to change the power level as it has direct implication with regulatory compliances.

ISA100 IR Devices

ISA100 - Access Points, and Devices with IR

Prerequisites:

• Ensure that you have ACT-BT5713U (BLE-to-Raw-IR Bridge) Adapter.

Bluetooth IR Bridge Device

This android application works with Bluetooth-IR Bridge device from ACTiSYS. ACT-BT5713U-v3 device has support for both battery and DC power. It has a power button to switch on /off the module in order to avoid burning of batteries too fast. ACTBT5713U-v3 provides a bridge solution between Bluetooth Low Energy (BLE) & Raw IR on data transmission. It tunnels data received through Bluetooth from Android Phone or Tablet to traditional RAW-IR data or vice versa.



Powering up ACTiSYS Device

Press "ON" switch to power on the device. When ACTiSYS device is powered on, the data LED starts blinking. This indicates that the device has powered on and started advertising for Bluetooth.

Provisioning Method



The ACT device acts as an intermediate bridge to Write/Read provisioning details and device parameters.

Prerequisites:

- Ensure ACT-BT5713U-v3 device is powered up and turned ON. This indicates the device can connect with Android Mobile.
- Ensure ACT-BT5713U-v3 device IR must be in line of sight with IR of Field device.

Provisioning Process for ISA100 IR Devices

1. In the OneWireless application, select ISA100 IR from the Choose Protocol drop-down list.

totudes vetre erz pri @ th € on ■	
Choose Protocol	
ISA100 IR 🗸 🗸	
Select Device to Connect 🖒	
Available Devices	
ATTENTION	oth permission when prompted e. This is mandatory for the

2. Select the ISA100 IR Device (ACTiSYS) from the Available Devices list.

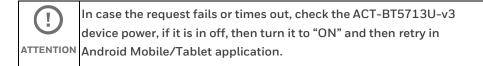
3. Once the device is successfully connected, it appears in connected device. Click **Continue** to proceed further.

thurs were ere	pm (8:01 8:50 ≡ ⊐) CE
Choose Protocol	
ISA100 IR	~
Connected Device	
ACT-BT5713U-v3	Disconnect
Cont	inue

4. The following options are available after pairing with the device.

154UJ0-46	Və LTIE	6:14 pm	æt9 ≵ 54% ■ ⊃			
\leftarrow A	ctions					
	Devi	ce Informat	ion			
	Device mornation					
	Provision Device					
	Tag Name					
	Radio Power Level					

The procedures are similar to those mentioned for ISA100 BLE.



WirelessHART Devices

Prerequisites

• Ensue that you have Viator[®] Bluetooth[®] HART Interface HM-MT-BT-EX-010041 (Bluetooth to WirelessHART Interface Bridge) Adapter.

Bluetooth to WirelessHART Interface Devices

This android application works with Bluetooth-WirelessHART Interface Bridge from Pepperl+Fuchs. This provides a bridge solution between Bluetooth and WirelessHART

Devices on data transmission. It tunnels data received through Bluetooth from Android Phone or Tablet to traditional WirelessHART devices or vice versa.

Viator[®] Bluetooth[®] Interface Modem is operated by replaceable AAA batteries. It attaches to a WirelessHART/HART field device with 18-inch leads & test clips. Android Phone host uses an internal Bluetooth interface to communicate with the modem. It has a power button to switch on /off the module to avoid burning batteries too fast.



Powering up Viator® Bluetooth®

Press "ON" to Power up the Modem. When Viator Modem is powered on, the data LED starts blinking. This indicates that the device has powered on and started advertising for Bluetooth.

Provisioning Method



As per the diagram, Viator Modem device acts as an intermediate bridge to Write/Read provisioning details and device parameters.

1. Ensure Viator Modem is powered up and it turns ON, which means Bluetooth is available to connect with Android Mobile.

NOTE

In general, the default password/PIN is "mactek", if it does not work, see the *Viator Modem User Guide* for the password/PIN.

2. Ensure Viator Modem test clips are connected to WirelessHART Device.

Provisioning Process for WirelessHART Devices

1. In the OneWireless application, select **WirelessHART** from the Choose Protocol dropdown list and discover MACTek Viator Bluetooth Device and provide the password/pin to pair with it.

IIO 4G Vo LTE	6:17 pm	@ 17 🕏 53% 🔳
Confi	gure Device	
Choose Prot	ocol	
Wireless	HART	~
Select Devic	e to Connect	φ
Available	Devices	
X MAC	TekViator5C7F	
	\bigcirc	\triangleleft

2. The following options are available after pairing with the device.

"ถิ่าไป	0 4G Volte	6:23 pm	🛞 😇 🕸 53% 💶 -
÷	Actio	ns	
		Device Informatio	
		Provision Device	•
		Tag Name	
		Radio Power Leve	el
		Dynamic Variable	25
		Device Status	
	Bur	st Message Inforn	nation
\sim		\bigcirc	\triangleleft

a. Device Information (Read Only).

EUI-64	: 26 63 2D C8 CC
HART Protocol Major Revision	: 99
Device Revision Level	: 5
Software Revision Level	: 7
Hardware Revision Level	: 1
Maximum Number Of Device Variables	: 4
Physical Signaling Code	: Bell 202 Voltage
Flags	EEPROM Control
Manufacturer Identification	: Rosemount
Private Label Distributor	: Rosemount
Device Profile	WirelessHART Process Automation Device
Long Tag	: Device_1
Read De	vice Information

	In case the request fails or times out, check the MACTek Viator device power and, if it is in off state, turn it to "ON" and then retry in Android
ATTENTION	Mobile/Tablet application."

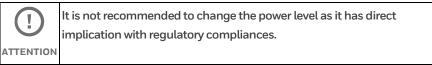
b. Provision device.

IU	0 4G VoLTE 4	.01 p	m ⊉⊛ ঊ≵36%[
←	Provisioning		
	Network ID		
	Max value 65536	5	
	Join Key		
	00000000	-	0000000
	00000000]-	00000011
	Provisi	ion	Device
	Provisi	ion	Device
			Device to Defaults

- c. Tag Name.
- Click **Tag name** to Edit/update Tag name.
- You can edit the tag name from the drop-down list or type in the device name.

: fal JiO 4G Vo LTE 4:02 pm 안 운 명 총 36% 💼
← Tag Name
Tag Name : Device_1
Change Tag Name
Enter Tag Name
OR Select From List
Device 1
Device 2
Device 3
Device 4
Device 5
Device 6
Device 7
Device 8
Write Tag Name
✓ □ ○

d. Update Power Level.



Click **Radio Power Level** to set the power. After setting the power level, it asks for a confirmation.

៉ះាlJIO 4G Vo LTE	6:24 pm	@• 17 🕸 53% 💶 ·
🔶 Radio Po	ower Level	
Power Level : 0	dBM	
Change Power L	.evel	
Select		~
w	/rite Power Lev	el
		1
× []		\triangleleft

៉ះាJJO 4G	VoLTE	6:24 pm	④ 행 \$ 53% ■
~ 1	Radio Powe	er Level	
Se	lect		
-5	dBM		
-4	dBM		
-3	dBM		
-2	dBM		
-1	dBM		
0	BM		
1	BM		
2 (BM		
3 (BM		
4	BM		
5	BM		
~			\triangleleft

e. Dynamic Variables.

The parameters that are configured as PV,SV,TV and QV can be viewed under this option.

filJIO 4G Vo LTE 6	6:24 pm
← Dynamic Var	iable Information
Primary Variable (PV)	: 0.00 Undefined
Secondary Variable (SV	0 : 25.10 °C
Tertiary Variable (TV)	: 25.00 °C
Quaternary Variable (Q	V) : 3.61 volts
Road Dura	amic Variables
Read Dyna	amic variables
× D	0 4

f. Device Status.

Status of the device is available in this option.

filJIO 4	G VoLTE 6:24 pm	، 🔁 🔁 🔁
←	Device Status	
De	vice Status	
De	vice Malfunction	•
Co	nfiguration Changed	•
Co	ld Start	•
Mo	ore Status Available	•
Lo	op Current Fixed	•
Lo	op Current Standard	•
No	n-Primary Variable Out of Limits	•
Pri	mary Variable Out of Limits	•
Ex	tended Device Status	
Ma	intenance Required	•
De	vice Variable Alert	•
Cri	tical Power Failure	•
Fa	ilure	•
Ou	t of Specification	•
Fu	nction Check	•
	Read Device Status	
	Read Device Status	
\sim		\triangleleft

g. Burst Message Information.

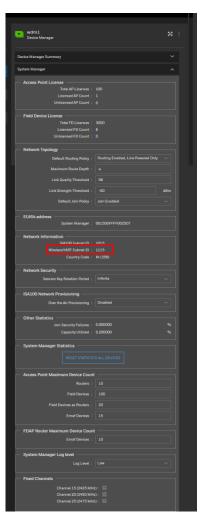
All the parameters required for publish configuration is available under this option.

JIO 4G Vo lte	6:24 pm	@• 10 🕸 53% 💻
Burst Me	essage Inforn	nation
Number of Burst	Msg : 3	
Burst Message (C	-2)	
0		~
Burst Control		
TDMA DLL o	only	~
Burst Period (in s	ecs)	
1		
Burst Max Period	(in secs)	
3001		
Burst Command		
33		~
Burst Trigger Mo	de	
Continuous		~
Rea	d Burst Messa	ige
Writ	te Burst Messa	ige
	\bigcirc	\triangleleft

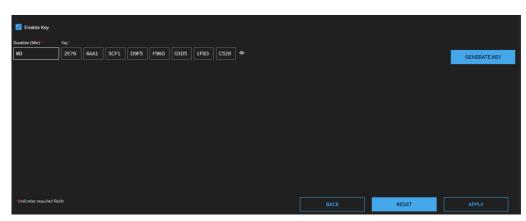
Provision Information from Honeywell WDM User Interface

WirelessHART Subnet ID & Join Key

• Get the common Join Key (Wireless HART provisioning) from Honeywell WDM user interface.



• Select the Enable Key checkbox to view the join key provisioning in WDM provide the Enabled Duration in between 60 to 600 minutes Range.



Provisioning Wireless HART Field Device using Values in Application

IJIO 4G VoLTE	4:01 prr	\$2⊛55≹361	
- Provisionin	a		
	<u> </u>		
Network ID			
Max value 655	36		
Join Key			
00000000		00000000	
00000000	-	00000011	
Prov	ision (Device	
		Device o Defaults	

You must provide network ID and Join key to join in the OneWireless application.

Configuring the WDM

Configure default routing policy

The default routing policy defines the routing behavior of a field device that is capable of operating as a router as well as an I/O device after it joins the network.

Considerations

The default routing policy is not applicable for the following devices.

- Devices capable of operating as access points (Access Points and FDAPs when connected to the backbone network).
- Devices capable of operating only as routers (FDAPs when not wired to the backbone network).
- Devices capable of operating only as I/O devices.

To configure default routing policy

- 1. Select Manage Devices from Left Navigation Menu bar.
- 2. Select the **WDM** from the selection panel.
- 3. Expand the property panel for WDM and expand System Manager.
- 4. Under Network Topology, select Default Routing Policy, as appropriate.

System Manager			^
— Access Point License —			
Total	AP Licenses :	100	
Licens	ed AP Count :		
Unlicens	ed AP Count :		
- Field Device License -			
Total	FD Licenses 🗧	3000	
License	ed FD Count :		
Unlicense	ed FD Count:		
Network Topology			
Default Ro	outing Policy :	Routing Enabled, Line Powered Only	
Maximum	Route Depth :		
Link Quali	ty Threshold :	96	
Link Strengt	th Threshold :	-90	dBm
Defaul	It Join Policy :	Join Enabled	
EUI64 address			
Syste	em Manager :	001500FFFF002507	

The following are the routing policy options available.

- **Routing Enabled** Enables all the routing field devices to function as a router and an I/O device.
- Routing Enabled, Line Powered Only Enables all the line-powered routing field

devices to function as a router and an I/O device. In this case, the battery powered routing field devices function only as I/O devices.

- **Routing Disabled** Disables the ability of the routing field devices to function as routers. The field devices with routing capability can function only as I/O devices.
- 5. Type the Maximum Route Depth, as appropriate.

The **Maximum Route Depth** parameter specifies the maximum number of hops. Hops are defined as the number of routing devices through which the data must pass to reach its destination. By default, this parameter is set to four.

6. Type the Link Quality Threshold, as appropriate.

This corresponds to the RSQI value between the devices. The link between the devices is established only if RSQI is equal to or greater than the **Link Quality Threshold** limit. By default, **Link Quality Threshold** is set to 96.

A Honeywell recommends that you set the Link Quality Threshold as 96. To set the Link Quality Threshold to any other value other than 96, you must contact a Honeywell technical support representative for assistance.

The Link Quality Threshold does not apply if the device has only one primary link.

- 7. Type the **Link Strength Threshold**, as appropriate. This corresponds to the RSSI value between the devices. By default the value is set to -90dBm. Honeywell recommends this value to be between -80 and -90.
- 8. Select one of the following **Default Join Policy** options, as required.

The **Default Join Policy** specifies the system-wide join policy for the routing devices (FDAP/FDAP Gen3 routers and routing field devices). The system – wide join policy can be overridden by the join policy of the device.

By default, the join policy for the devices is configured as **Join Enabled**.

- **Join Enabled** Enables the devices to join the network through FDAP routers and routing field devices.
- Join Enabled, Line Powered Only Enables the devices to join the network only through FDAP routers.
- 9. Click Apply.

The configured routing policy is applicable only for devices that are joining the network for the first time.

Configure key rotation period

To configure key rotation period

- 1. Select Manage Devices from Menu bar.
- 2. Expand the properties for WDM.
- 3. Expand System Manager in the property panel.
- 4. Select the Key Rotation Period under Network Security.

The following options are available for configuring the key rotation period.

- 8 Hours
- 1 Day
- 1 Week
- 1 Month
- Infinite The default setting, which implies that key rotation is disabled.

It is recommended to change the value to any value other than infinite.

5. Click Apply.

Configure Radio frequency Channel

The data communication in the OneWireless Network takes place through 15 channels of the wireless frequency spectrum. Each channel is of 5 MHz bandwidth, and with a center frequency starting from 2405 MHz to 2475 MHz of the 15 channels, three channels of frequency 2425 MHz, 2450 MHz, and 2475 MHz, are fixed and are not user configurable. The remaining 12 channels are user configurable and by default are available for data communication. You can determine and configure the channels that would be available for communication in the network.

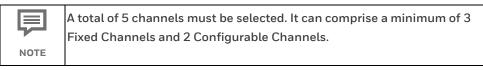
In a plant scenario, there can be various wireless devices communicating in specific channels, which may cause interference. In such situations, you can configure channel to avoid interference and have reliable data communication network.

To configure channel Radio frequency channel

- 1. Select Manage Devices from Menu bar.
- 2. Expand the properties for WDM.
- 3. Expand **System Manager** in the property panel.

wdm1 Device Manage		5
Fixed Channels		
	Channel 15 (2425 MHz) :	
	Channel 20 (2450 MHz) :	
	Channel 25 (2475 MHz) :	
Configurable C	hannels	
	Channel 11 (2405 MHz) :	
	Channel 12 (2410 MHz) :	
	Channel 13 (2415 MHz) :	
	Channel 14 (2420 MHz) :	
	Channel 16 (2430 MHz) :	
	Channel 17 (2435 MHz) :	
	Channel 18 (2440 MHz) :	
	Channel 19 (2445 MHz) :	
	Channel 21 (2455 MHz) :	
	Channel 22 (2460 MHz) :	
	Channel 23 (2465 MHz) :	
	Channel 23 (2405 MHz) .	

The fixed channels appear under **Fixed Channels** and the user configurable channels appear **under Configurable Channels**.



- 4. Select the check boxes for the channels, as required.
- 5. Click Apply.

It takes approximately 90 seconds for the changes to take effect.

Configuring the WDM redundancy

The OneWireless redundant system consists of two identical WDMs, one acts as a primary and the other acts as a secondary (redundant backup). In a redundant system, the secondary is actively linked to the primary (running), so that it can take control whenever the primary fails or is shut down. The primary and the secondary WDMs are connected to each other through the RDN Ethernet port.

Ę	
NOTE	

No WDM switchover happens when primary WDM is shutdown using the Power button present on WDM. This is an intentional user shutdown of the primary WDM and secondary WDM does not take over the primary WDM role in this case.

	Redundancy is supported for the following combinations:	
ATTENTION	WDMX and WDMY	
	WDMY and WDMY	

The following are the redundancy features:

- Provides an uninterrupted view to the field device network in the event of a hardware or a software failure.
- Synchronize process data, alarms and events, field device network databases, and WDM configuration in real time.
- Enables transparent switchover with no loss of view to the field device network across all external interfaces.
- Enables you to implement the network topology with no single point of failure, including the network switches. The following figure describes a dual switch network topology without a single point of failure.

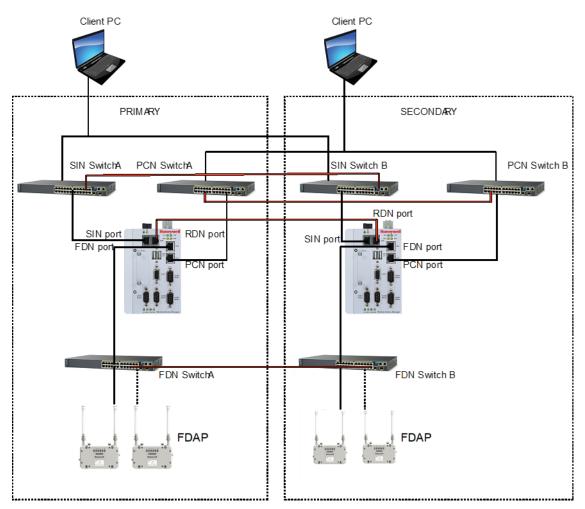
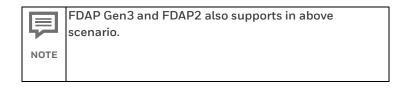


Fig. 12. Redundant Network Topology with FDAP



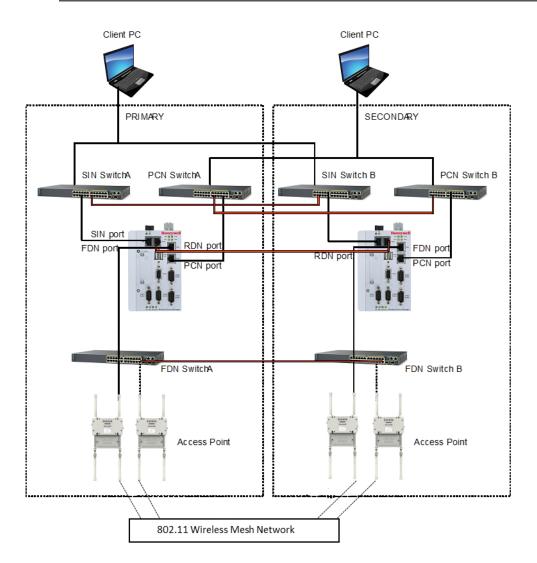


Fig. 13. Redundant Network Topology with Access Point

F	PCAP and Cisco 1552S also supports in the above scenario.
NOTE	

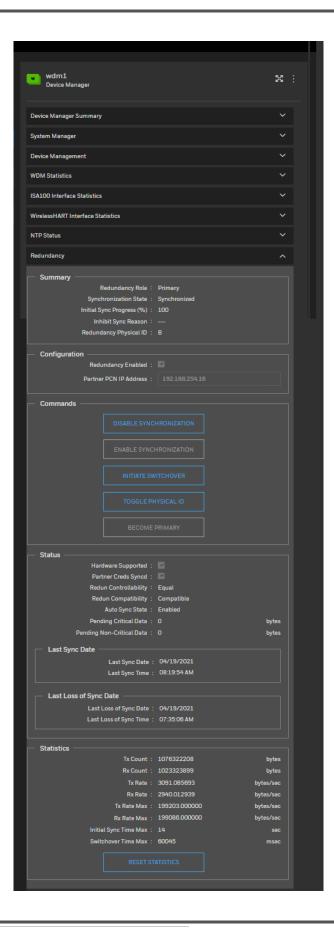
 Cisco Catalyst 2960 Series 8 port switches and Cisco Catalyst 2960X Series 24 port switches are the supported FDN switches. For more information, refer to the Cisco Catalyst 2960 Series documents. 		
• For information about Cisco Access Point configuration, see the OneWireless Wireless LAN Controller Configuration Guide.		
 You can use a single PCN/single FDN switch or dual PCN/dual FDN switches. Single switches are used for simple networks, less expensive, possible single point of failure. Dual switches are used for more robust networks, which are more expensive, but do not contain single point of failure. 		
In case you plan to set up a redundant WDM, ensure the following:		
 Cisco switch port, where the WDM is connected, is configured to operate in access mode. 		
2. Spanning-tree portfast feature is enabled.		
3. Speed is set to auto.		
4. Port is in full duplex mode.		
For an example of the Cisco switch configuration for WDM port, see the OneWireless Wireless LAN Controller Configuration Guide.		

Configure WDM redundancy from the First Time Configuration Wizard

You can configure the WDM redundancy from the First Time Configuration Wizard (FTCW). For more information, see the section **"Configuring WDM using the First Time Configuration Wizard**".

Configure WDM redundancy from the WDM Properties panel

Redundancy configuration may be enabled, disabled, or modified on-process from the WDM Properties List under Manage Devices. Changes performed to redundancy configuration from the WDM Properties list only apply to that WDM, and are not automatically cascaded to the redundant partner. For example, if redundancy is disabled on a primary WDM, the redundant partner remains in secondary role.



Enable redundancy from the WDM Properties list

To enable redundancy on a primary WDM:

- 1. Expand Redundancy in the Property panel of WDM from Manage Devices.
- 2. Select the **Redundancy Enabled** check box.
- 3. In the **Partner's PCN IP address**, type the partner's PCN IP address.

When the WDM redundancy is enabled, there is no need to specify a redundancy role since it is automatically set to primary. A non-redundant WDM may not be converted into a secondary on-process. To convert a non- redundant WDM into secondary WDM, reset it to defaults, and then configure it as a secondary WDM from the FTCW.

Disable redundancy from the WDM Properties Panel

The WDM redundancy can only be disabled from the WDM Properties list, if the WDM is in the primary role and synchronization is disabled. Secondary WDM may not be converted into non-redundant on-process.

To disable redundancy on a primary WDM:

- 1. Expand Redundancy in the Property panel of WDM from Mange Devices.
- 2. Clear the **Redundancy Enabled** check box.



To disable redundancy on a secondary WDM, reset it to defaults and then configure as non-redundant from FTCW.

Modify partner PCN IP address

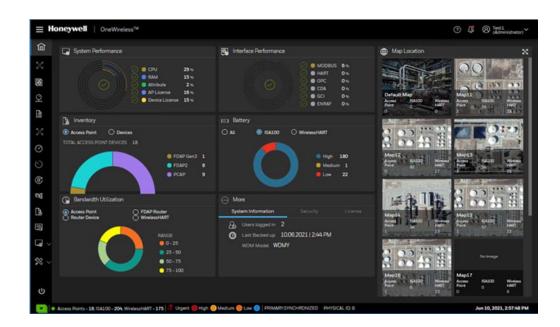
On a redundant WDM (primary or secondary), the partner's PCN IP address may be modified on-process if synchronization is disabled.

Redundancy operations

See the section "Perform redundancy-specific operations"

Primary view

The Primary WDM is used for monitoring field devices, initiating all the commands, and viewing alarms and events. The Primary WDM monitors and reports the communication configuration, performance, and operational status. The external interfaces such as MODBUS, HART, OPC, GCI, ENRAF and CDA are only available on the primary WDM. CDA interface is available on both the primary and secondary WDMs.



Secondary view

The secondary WDM has limited functionality and is used for monitoring redundancy parameters, initiating redundancy commands, and viewing the secondary WDM alarms and events. The access points, field devices, or external interfaces are not displayed on the secondary WDM. CDA external interface is not displayed on the secondary WDM. However, the secondary WDM can be accessed from the Experion through CDA interface.

The following are available in the Properties Panel of the secondary WDM.

- Device Manager Summary
- Device Management
- WDM Statistics
- NTP Status
- Redundancy
- Redundancy History
- Field Device Network (FDN)
- Process Control Network (PCN)
- Special Interface Network (SIN)

The external interfaces are only available on the primary WDM (except CDA). External clients cannot connect to the secondary WDM using Modbus, HART, OPC, GCI, and ENRAF. The CDA interface is available on both the primary and the secondary WDMs. The external clients are reconnected to the old secondary/new primary immediately after switchover, using the primary WDM configuration. Redundancy status parameters and commands are available when integrated with Experion R410 and later.

E Honeywell OneWireless	u l			⊙ 4 ® Shatana (Administrator)
HOME	Manage Devices The Secondary WDM is used for monitoring field devices, initiator	g all the commands, and viewing alarms and even	4 <u>5</u>	
MONTORNS	wdm2 Device Manager			
REPORTS	Device Manager Summary			
ACTIONS	Device Management			
O PROVISIONING	WDM Statistics			
MANAGEWOM	NTP Status			
B SINGLE SIGN ON	Redundancy			
CE OWNELS	Redundancy History			
FIRMWARE UPGRADE	Field Device Network (FDN)			
EXTERNAL INTERFACES	Process Control Network (PCN)			
SYSTEM V	Special Interface Network (SIN)			
	Alarms(1)	^		
	PRIORITY START TIME DE	SCRIPTION		
	Urgent 04/23/2021 8:30:35 PM Demon			
🕺 MAINTAINAINCE 🤍				
MANAGE LICENCES				
			RESET	APPLY
U LOGOUT				
💽 🕴 Urgent 📵 High 📀 Medium	Low O SECONDARYSYNCHRONIZED PHYSICALID:	4		Apr 23, 2021, 2:12:01

Monitoring the WDM redundancy status

The redundancy status is displayed on the Status Bar, Property panel and Reports of the OneWireless User Interface.

Status Bar

The Status Bar contains the overall redundancy and physical ID status.



Manage Devices

The WDM icon on the Manage Devices changes depending on the redundancy role. For information regarding the different WDM icons, see "**Understand the device icons**".

Monitor the redundancy status from the WDM Property panel

Follow the below procedure to monitor the redundancy status from the WDM Property panel:

- 1. Select Manage Devices from Menu bar.
- 2. Expand the properties for **WDM**.
- 3. Expand **Redundancy** in the property panel.



- 4. Under Summary, verify the Redundancy Role, Synchronization State, Initial Sync Progress, Inhibit Sync Reason, and Redundancy Physical ID.
- 5. Under Status, verify Hardware Supported, Partner Creds Synced, Redundant Controllability, Redundant Compatibility, and Auto Sync State, Pending Critical Data, and Pending Non-Critical Data.

The following table describes the attributes displayed in the Redundancy tab of the WDM Property panel.

Attributes	Description
Summary	
Redundancy Role	Indicates the current redundancy role - primary, secondary, or non- redundant.
Synchronization State	Indicates level of module synchronization with redundancy partner as follows: - Partner Visible, Initial Sync Progress, Synchronized, No Partner, and Incompatible.
	• Partner Visible: Communication is established over the RDN private path, but the WDMs are not yet synchronized.
	Initial Sync Progress: Initial sync is in progress.
	• Initial sync is complete and WDMs are in sync maintenance state.
	• No communication over RDN private path.
	• Redundant partner is not compatible for synchronization.
Initial Sync Progress (%)	Indicates the percentage of initial-sync completion. This is set to zero when initial sync is not in progress and it is set to 100 when initial sync is complete.
Inhibit Sync Reason	Indicates the current reason why initial sync is inhibited.
Redundancy Physical ID	Used to identify the physical hardware module.
	The Redundancy Physical ID attribute is used for identifying the physical hardware module. By default, when a WDM is configured in a primary role, the value of its attribute is set to A. When a WDM configured in a secondary role, the value of its attribute is set to B. These values are attached to the physical hardware and not the redundancy role. In other words, starting from a redundant synchronized WDM pair, where the WDM with a physical ID A is primary and the WDM with a physical ID B is secondary, if a switchover occurs, the WDM physical ID B is in primary role and the WDM with physical ID A reboots into secondary role. If the physical

	hardware is so labeled, it is possible to identify the WDM currently in Primary role.	
Status group		
Hardware Supported	Indicates whether redundancy is supported on current hardware. WDM redundancy is not supported on WDMS hardware.	
Partner Creds Synced	Indicates whether WDMs have synchronized at least once. On a lonely secondary, the	
	primary command is disabled if this check box is not selected.	
Redun Controllability	 Describes the module's ability to control relative to its redundant partner. For example, on an unsynchronized redundant WDM pair, if the primary's FDN/PCN/SIN cable is disconnected, but the secondary's FDN/PCN/SIN cables are connected, then the secondary has better control ability than the primary. And the primary WDM's control ability is worse than the secondary. Note that on such a redundant WDM pair, if synchronization is enabled, then the WDMs synchronize and immediately switchover since the secondary's control ability is better than that of the primary. Switchover can be initiated from primary or secondary WDM. The following conditions result in switchover: FDN/PCN/SIN Ethernet cable is disconnected on the primary WDM. Loss of power on the primary WDM. 	
Redun Compatibility	 Hardware failure on the primary WDM. Indicates whether redundant partner modules are compatible and if not compatible, provides a reason. Initial synchronization is disabled 	
Auto Sync State	on an incompatible WDM pair. Indicates whether auto synchronization is enabled or disabled. When disabled, you must explicitly issue the Enable Synchronization command to reset any persistent fault condition and (re)attempt initial synchronization.	
Pending Critical Data	Number of critical sync data bytes yet to be sent to partner. This value is usually 0. An increase may be observed during initial synchronization, which rapidly reduces to 0.	
Pending Non-critical dat	ta Number of non-critical synchronization data bytes yet to be sent to the partner. This value may increase to a large value during initial synchronization, and gradually reduce to zero.	

Last Sync Time	Time when the WDM completed initial synchronization.
Last Loss of Sync Time	Time when the WDM last lost synchronization.
	The attributes in this group indicate whether redundant WDMs are communicating over the RDN private path. A steadily increasing Tx count indicates that data is successfully being transmitted to partner. A steadily increasing Rx count indicates that data is successfully being received from the partner.

6. Expand Redundancy History in the Property panel to view the history details. The Redundancy History tab displays the 16 most recent redundancy events along with a reason why the event occurred. For example, in the following figure, the role change state is reported with reason Initiate Switchover Command indicating that a role change occurred at 3 PM on 4/19/2021 due to user- initiated switchover command.



Perform redundancy-specific operations

Enable Synchronization

The Enable Synchronization option enables auto synchronization and is used for initial synchronization. The maximum initial synchronization time is 180 seconds.

The following conditions result in loss of synchronization:

- Disable Synchronization command initiated from primary or secondary WDM.
- FDN or PCN Ethernet cable disconnected on the secondary WDM.
- RDN Ethernet cable disconnected.
- Loss of power on the secondary WDM.
- Software failure on the secondary WDM
- Hardware failure on the secondary WDM.
- Redundancy data communication failure (checksum, and so on).



Redundancy command buttons are disabled if they do not apply to the current redundancy state. For example, 'Enable Synchronization' is disabled when synchronized.

To enable synchronization

• Expand **Redundancy** in the Property panel and then click **Enable Synchronization**.

Disable Synchronization

The Disable Synchronization option disables auto synchronization and is used for drop synchronization. To disable synchronization

• Expand Redundancy in the Property panel and then click Disable Synchronization.

Initiate Switchover

The **Initiate Switchover** option enables immediate switchover of a synchronized WDM pair. The switchover time is 15 seconds.

Switchover can be initiated from the primary or the secondary WDM. The following conditions result in switchover:

- FDN/PCN/SIN Ethernet cable is disconnected on the primary WDM.
- Loss of power on the primary WDM.
- Software failure on the primary WDM.
- Hardware failure on the primary WDM

To initiate Switchover: Expand **Redundancy** in the Property panel and click **Initiate Switchover**.

• Redundancy data communication failure (checksum, and so on).

Convert a lonely unsynchronized secondary into a primary

The **Become Primary** option converts a lonely, unsynchronized secondary into a primary. The secondary WDM must have synchronized at least once with the primary WDM for this command to be enabled. This is indicated by the **Partner Credentials Synced** check box in the Status group.

As the secondary is not synchronized with the primary when this command is executed, it may have stale configuration data. You must manually check and re-configure devices and other settings as appropriate. The following data is preserved in the secondary WDM since the last sync drop event:	
٠	Primary WDM name.
•	Primary WDM FDN IP address.
•	Primary WDM PCN IP address.
•	Primary WDM external NTP server configuration.
•	Primary WDM DHCP server configuration.
•	DHCP leases given out by primary WDM.
•	Security keys already used by devices to join the network.
•	Country code.
•	Subnet ID.
•	TAI offset.
•	User accounts, their roles, and permissions.

NOTE

Reset of the configuration data such as Device Routing information, external interface configuration such as Modbus Points configuration, CDA device load configuration and so on are not preserved.

To convert a lonely, unsynchronized secondary into a primary:

• Expand **Redundancy** in the Property panel from **Mange Devices**, click **Become Primary**.

Toggle Physical ID

The **Toggle Physical ID** option allows to toggle physical ID from B to A or A to B.

When the redundant WDMs are communicating over the private path, the physical IDs of both the WDMs is toggled, regardless of whether the command was sent to the primary or

the secondary WDM. If redundant WDMs are not communicating over the private path, only the WDM to which the command was sent is affected.



When redundancy is enabled, the primary WDM is assigned physical ID A and the secondary WDM is assigned physical ID B. The physical IDs are displayed in the UI during normal operation. Tagging the physical hardware with matching labels makes it easy to distinguish the WDMs later.

To toggle the physical ID:

Expand Redundancy in the Property Panel and click Toggle Physical ID.

Configuring device communication redundancy

The OneWireless user interface displays the communication redundancy state of each device. A communication redundancy ratio statistic is provided to identify devices with frequent non-redundant connectivity over time, even if the device currently has redundant connectivity. In addition, devices may optionally alarm if a non- redundant connection is detected.

Property panel - device communication redundancy

The Property panel displays the communication redundancy information.

CD 475		user will be able to read	
ISA100	_3F_6FLR		
ISA100 Device Su	ummary		
Channel Configu	ration		
Device Managem	nent		
Power —			
Pow	ver Supply Status :	Battery, High	
Routing Ass			
	Fast Discovery :	Not Applicable	
	iting Assignment: Join Assignment:	Routing Disabled	
		Join Disabled	
Role Capab	ility		
	Routing Device :		
	I/O Device :		
Assigned R	ole		
	Routing Device :		
	D'O Device .		
Command			
	Join Command :	None	
	Join Command :	None	
— Uptime and	Join Command : Connectivity Uptime :		seconds
	Connectivity Uptime : Restart Count :	1816845 13	seconds
	Connectivity Uptime : Restart Count : e Drop Off Count :	1816845 13 0	seconds
	Connectivity Uptime : Restart Count :	1816845 13 0	seconds
Devic	I Connectivity Uptime : Restart Count : e Drop Off Count : RESET STJ	1816845 13 0 ATISTICS	seconds
Devic — Communica Co Co	I Connectivity Uptime : Restart Count : RESET STJ RESET STJ ation Redundancy mm Redun State : mm Redun Ratio :	1816845 13 0 ATISTICS , Redundant, SingleAP 100	seconds
Devic — Communica Co Co	I Connectivity Uptime : Restart Count : e Drop Off Count : RESET STA ation Redundancy mm Redun State :	1816845 13 0 ATISTICS , Redundant, SingleAP 100	
Devic — Communica Co Co	I Connectivity Uptime : Restart Count : Drop Off Count : RESET STJ ation Redundancy mm Redun State : mm Redun Atarm : tocol Version	1816845 13 0 ATISTICS Redundant, SingleAP 100	
Communica Co	I Connectivity Uptime : Restart Count : e Drop Off Count : RESET ST/ ation Redun data mm Redun Alarm : nm Redun Alarm : tocol Version Version :	1816845 13 0 ATISTICS Redundant, SingleAP 100	
Communica Co	I Connectivity Uptime : Restart Count : Drop Off Count : RESET STJ ation Redundancy mm Redun State : mm Redun Atarm : tocol Version	1816845 13 0 ATISTICS Redundant, SingleAP 100 STK-2.0	
Communica Co	I Connectivity Uptime : Restart Count : e Drop Off Count : RESET ST/ ation Redun data mm Redun Alatio : nm Redun Alatio : tocol Version Version : ghput Link Enable :	1816845 13 0 ATISTICS Redundant, SingleAP 100 STK-2.0	
Communica Co	I Connectivity Uptime : Restart Count : e Drop Off Count : RESET ST/ ation Redun data mm Redun Alatio : nm Redun Alatio : tocol Version Version : ghput Link Enable :	1816845 13 0 ATTISTICS Redundant, SingleAP 100 STK-2.0	
Communica Co	I Connectivity Uptime : Restart Count : e Drop Off Count : RESET ST. ation Redundancy mm Redun Atarm : mm Redun Alarm : tocol Version Version : ghput Link Enable : iscovery Frequency :	1816845 13 0 ATTISTICS Redundant, SingleAP 100 STK-2.0	percent
Device Communicat Ca Ca	I Connectivity Uptime : Restart Count : e Drop Off Count : RESET ST. ation Redundancy mm Redun Atarm : mm Redun Alarm : tocol Version Version : ghput Link Enable : iscovery Frequency :	1816845 13 0 ATISTICS Redundant, SingleAP 100 STK-2.0 1 hour	percent
Device Communica Co Cor ISA100 Prof High Throu Neighbor D Radio Diagr Time Sync	I Connectivity Uptime : Restart Count : e Drop Off Count : RESET ST. ation Redundancy mm Redun Atarm : mm Redun Alarm : tocol Version Version : ghput Link Enable : iscovery Frequency : nostics Radio Comm Fail : : Redundancy Fail :	1816845 13 0 ATISTICS Redundant, SingleAP 100 STK-2.0 1 hour	percent
Device Communica Co Cor ISA100 Prof High Throu Neighbor D Radio Diagr Time Sync	I Connectivity Uptime : Restart Count : e Drop Off Count : RESET ST. ation Redundancy mm Redun Atarm : tocol Version : ghput Link Enable : iscovery Frequency : nostics Radio Comm Fail : : Redundancy Fail : Sensor Comm Fail :	1816845 13 0 ATISTICS Redundant, SingleAP 100 STK-2.0 1 hour	percent
Device Communica Co Co ISA100 Prof High Throug Neighbor D Radio Diagr Time Sync	I Connectivity Uptime : Restart Count : e Drop Off Count : RESET ST/ ation Redun State : mm Redun State : mm Redun Alarm : tocol Version : Version : ghput Link Enable : iscovery Frequency : Radio Comm Fail : Redundancy Fail : Sensor Comm Fail :	1816845 13 0 ATISTICS Redundant, SingleAP 100 STK-2.0 1 hour	percent
Device Communicat Co Co	I Connectivity Uptime : Restart Count : e Drop Off Count : RESET ST/ ation Redun State : mm Redun State : mm Redun Alarm : tocol Version : Version : ghput Link Enable : iscovery Frequency : Radio Comm Fail : Redundancy Fail : Sensor Comm Fail :	1816845 13 0 ATISTICS Redundant, SingleAP 100 STK-2.0 1 hour	percent
Device Communica Co Co ISA100 Prof High Throu Neighbor D Radio Diagr Time Sync Battery Esti	I Connectivity Uptime : Restart Count : e Drop Off Count : RESET ST/ ation Redundancy mm Redun Atato : mm Redun Atato : mm Redun Alarm : tocol Version Version : ghput Link Enable : iscovery Frequency : Radio Comm Fail : Redundancy Fail : Sensor Comm Fail : EEPROM Fail : immetes	1816845 13 0 ATISTICS Redundant, SingleAP 100 STK-2.0 1 hour 1 hour 0	percent
Device Communica Co Co ISA100 Prof High Throu Neighbor D Radio Diagr Time Sync Battery Esti	I Connectivity Uptime : Restart Count : e Drop Off Count : RESET ST. ation Redundancy mm Redun Atarm : tocol Version : ghput Link Enable : iscovery Frequency : hostics Radio Comm Fail : censor Comm Fail : EEPROM Fail : iscort Remaining :	1816845 13 0 ATISTICS Redundant, SingleAP 100 STK-2.0 □ 1 hour 1 hour 0 79.512329	percent
Device Communica Co Co ISA100 Prof High Throu Neighbor D Radio Diagr Time Sync Battery Esti	I Connectivity Uptime : Perstart Count : Prop Off Count : Prop Off Count : RESET STJ ation Redun Atarn : tocol Version : Wersion : ghput Link Enable : iscovery Frequency : nostics Radio Comm Fail : Redundancy Fail : Sensor Comm Fail : EEPROM Fail : imates recent Remaining : Years Remaining :	1816845 13 0 ATISTICS Redundant, SingleAP 100 STK-2.0 □ 1 hour 1 hour 0 79.512329	percent

- Communication Redundancy State identifies if a device is having connectivity issues.
- Communication Redundancy Ratio provides ratio of redundant connectivity versus non-redundant connectivity, used to identify if a device is having connectivity issues over time.
- Communication Redundancy Alarm alerts if a device loses redundant connectivity, alarm may be disabled.

Report

The report displays the communication redundancy information. For example, Connection Summary report.

Honeywell OneWirel	e55 ^{%4}			③ (1) ④ Administratio (Administratio)
奋 HOME	Generating Reports			
44.N				Report Generated By Date and Time
MONITORING	Battery Life			administrator 17-May-21 1:34:26
ALARMS & EVENTS				
REPORTS	DEVICE NAME	BATTERY LIFE	DEFRUIT MAP	DESCRIPTION C
TIONS	wdm1		Unplaced	PILWOM
PROVISIONING	FC_1808	Line	Default Map	
MANAGE DEVICES	AP_0096		Boiler	
SINGLE SIGN ON	FDAP2_R320_F803	Line	Default Map	
CHANNELS	SL_Temp_70055		Default Map	
FIRMWARE UPGRADE	TD_105_SFL_SFT	High	Default Map	
EXTERNAL INTERFACES	TD_1010_4J_6FLR		Default Map	
ু হার্রার্চ্স	UI00_04	High	Default Map	
MAINTENANCE	HD_466_3CLL_PCT		Default Map	
MANAGELICENSES	EML_65891	High	Pumphouse	
			Go to page 1 →	Records per page 10
				PRINT
U LOGOUT				

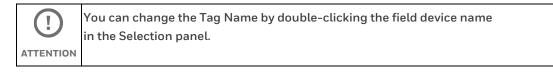
For more information, see section "Generating reports".

Configure field devices

Configure field device properties

To configure tag name and description

- 1. Select the **field device** in the Selection panel from **Manage Devices**.
- 2. Expand **Device Summary** in the Property panel for the selected device.
- 3. Type the required **Tag Name**.



- 4. Type the required **Description**.
- 5. Click **APPLY**.

Configuring routing assignment

After joining the network for the first time, a field device is capable of operating as a router and an I/O device initializes its routing assignment based on the current default routing policy. It is possible to override the default routing policy by configuring routing assignment for field devices. Configuring device routing assignment results in restarting the device with a new role.

Considerations

• Device routing assignment can be configured only for devices that are capable of operating as routers and I/O devices.

To configure routing assignment:

- 1. Select the field device in the Selection panel.
- 2. Expand Device Management in the Property panel.
- 3. Select Routing Assignment as appropriate.

The following are the Routing Assignment options available.

- **Routing Disabled** Disables the ability of a routing field device to function as a router. The field device can function only as an I/O device.
- **Routing Enabled** Enables the routing field device to function as a router and an I/O device. The default join policy configured is **Follow System Manager Policy**.
- Not Applicable
 - Does not apply to devices that are capable of operating as access points.
 - Does not apply to devices that are only capable of operating as routers.
- 4. Select one of the following **Join Assignment** options, as required.
- 5. The **Join Assignment** overrides the system manager join policy. This is applicable only for routing field devices.
 - Join Disabled Disables device-join through this device.
 - Join Enabled Enables device-join through this device.
 - Follow System Manager Policy Enables the device to follow the system manager join policy. Device-join through this device depends on the configured system manager join policy.

The Join Status is a read-only parameter that indicates the resultant join state for all the devices.

• Access Points, FDAP/PCAP access points, and FDAP routers have the **Join Assignment** permanently set to **Join Enabled**. • Non-routing field devices have the **Join Assignment** permanently set to **Join Disabled**.

Routing field devices have the default **Join Assignment** set to **Follow System Manager Policy**.

6. Click **Apply**.

Configure publication rate for ISA100 Wireless devices

The publication data for input and output field devices can be configured using the Input Publication and Output Publication panels in the Property panel. Depending on the device type, a field device can have an Input Publication panel, or an Output Publication panel, or both. This is determined by the DD file for the field device.

The Input/Output Publication panel for ISA100 Wireless devices contains the following configuration options.

- **Contract Status** A contract is a communication resource (bandwidth) allocation between two devices on the ISA100 Wireless network. The following are the status values that are displayed depending on the status of the contract.
 - Not Configured No contract established due to incorrect configuration of the device.
 - Activating Contract establishment is in progress.
 - Active- Contract is active.
 - Active, Negotiated Down If a device requests a contract for periodic publications at a fast rate (such as 1 second) and if the communication resources are not available, the contract is negotiated down to a slower publication period (such as 5 seconds).
 - Terminating Contract termination is in progress.
 - Failed Contract establishment has failed.
 - Inactive Contract is inactive.
- Rate Rate at which a source node (field device or gateway) publishes.
- **Stale Limit** Defines the maximum number of stale input values that can be received before the input status is set to Bad. The recommended stale limit is as stated in the following table.

Stale Limit	
120	
60	
30	
12	
6	
5	
5	
5	
	Stale Limit 120 60 30 12 6 5 5

- **Destination** Destination is the target device where publications must reach.
- **Channel** The list of channels for which the publication configuration applies.
- Attribute Attribute is a parameter of a channel. It can be a process value, a measurement, a configuration or a statistic of the channel. For example MODE, PV, SCALE, and so on. You can publish multiple attributes.



When a device joins the network, the WDM automatically configures its publication period as 60 seconds.

To configure publication rate and stale limit

- 1. Select the field device in the Selection panel.
- 2. Expand Input Publication or Output Publication in the Property panel.

Input Publication		
Publication Group 1		
	Contract Status :	Active
	Rate :	1 minute \checkmark
	Stale Limit :	
	Destination :	wdm1
Attribute 1		
	Channel :	TemperatureDI AIO 1 V
	Attribute :	PV V
	Attribute :	
Attribute 2		
	Channel :	TemperatureDI BIO 2 🗸
	Attribute :	PV_B v
	Attribute .	
Attribute 3		
	Channel :	TemperatureDI BIO 3 🗸 🗸 🗸
	Attribute :	MODE
Attribute 4		
	Channel :	None
	Attribute :	None

- 3. In the **Rate** field, select the publication rate, as appropriate.
- 4. In the **Stale Limit** field, select the stale limit, as appropriate.
- 5. Select the **Channel** and then the preferred **Attribute**.
- 6. Click Apply.

Configure publication rate for WirelessHART devices

The publication data for input and output field devices can be configured using the Input Publication panel in the Property Panel.

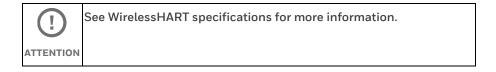
Burst Message 0	
Burst Status :	
Burst trigger mode :	
Actual burst rate :	
Minimum burst rate :	1/2 second 🗸
Maximum burst rate :	1/2 second 🗸
Stale limit :	
Burst mode control :	Disabled ~
Burst command :	Cmd 1 (Primary Variable) 🗸 🗸
Source device :	3308_GWR_TX ~
Device Variable Codes	
Slot 0 :	243 (Battery Life, Float in Days) 🗸 🗸
Slot 1 :	243 (Battery Life, Float in Days) 🗸 🗸
Slot 2 :	243 (Battery Life, Float in Days) 🗸 🗸
Slot 3 :	243 (Battery Life, Float in Days) 🗸 🗸
Slot 4 :	243 (Battery Life, Float in Days) 🗸 🗸
Slot 5 :	243 (Battery Life, Float in Days) 🗸 🗸
Slot 6 :	243 (Battery Life, Float in Days) 🗸 🗸
Slot 7 :	243 (Battery Life, Float in Days) 🗸 🗸
Statistics	
Messages Received :	
Messages Missed : Success Rate (%) :	
Average Update Time (sec) :	

The Input Publication panel for WirelessHART devices contains the following configuration options.

- **Burst status** Burst indicates the publishing feature of the WirelessHART devices. Depending on the configuration, the **Burst Status** is displayed.
 - **Disabled**: If the publishing is disabled for a device.
 - **Configures**: The device is getting configured to publish the data.
 - Active as configured 1 as 1: If the actual publishing rate for the device and WDM configured publishing rate are identical.
 - **Capacity adjusted 1 as 8**: If the actual publishing rate for the device and WDM configured publishing rate are not identical.
 - **Burst denied**: Publishing is not working, as intended.
- **Burst trigger mode** Indicates the trigger mode for publishing the data.
- Actual burst rate Configured rate at which a field device or gateway publishes.
- **Minimum burst rate** Minimum rate at which a field device or gateway publishes.
- **Maximum burst rate** Rate at which the device must publish though there is no change in process value.
- **Stale Limit** Defines the maximum number of stale input values that can be received before the input status is set to Bad. The recommended stale limit is stated here:

Publication period	Stale Limit	
1/2 second	120	
1 second	60	
2 seconds	30	
4 seconds	15	
8 seconds	10	
16 and 32 seconds	5	
1, 5, 15, 30 minutes	5	
1 hour	5	

- **Burst mode control** The mode of the field device on which the publication is active.
- **Burst command** Pre-specified commands that drive a specific action.
- **Source device** The source can be an adaptor or a field device.
- Device Variable Codes- command line refer to HART stats
- **Statistic** Burst message statistics



Calibrate Honeywell XYR6000 field devices

Calibration can be initiated either by manually setting the calibration parameters such as Cal Cmd, Cal Point High, Cal Point Low, and Cal Unit in the Calibration panel or by using the Invoke Method button. Invoke Method initiates the method manager, which guides you through the calibration process. All the field devices might not necessarily have the ability to calibrate. This is defined in the vendor supplied DD file.

Note: This option is applicable only for Honeywell XYR6000 ISA100 Wireless devices.

To calibrate field device using Invoke Method

1. Click **CHANNELS** from Left Navigation Menu Bar.

1 HOME	Channels									
MONITORING	Device List Select the channels.			Status Color represents state o			Summary Displays all channel's			
ALARMS & EVENTS	Select the channels.			- 🗞 Color represents state o	f the channel (AUTO, OOS).		Displays all channel's	s status		
REPORTS										
TIONS										
PROVISIONING	□ • S : Total Device	es Discovered 🕚								
) MANAGE DEVICES	NAME	DEVICE TYPE	STATUS	VENDOR	MODEL	REVISION	SERIAL	IPV6 ADDRESS	POWER	
SINGLE SIGN ON	∨ 🗆 🛑 CD_475_3F_6_	ISA100	Joined	Honeywell	XYR 6000 Corr	OW322.1-20.0	\$040843000000204	FE80 :: 0040:8430:000.	High	
CHANNELS	✓ □ ● P0_573	ISA100	Joined	Honeywell	2012	OW240.2-02.0	\$102030405060708	FE80::0102.0304:050.	High	
FIRMWARE UPGRADE	✓ □ • T0_1010_4J_6	ISA100(R)	Joined	Honeywell	XYR 6000 TempDI	OW320.2-11.0	1230000010	FE80::0040.8440:000.		
EXTERNAL INTERFACES	✓ □	ISA100	Joined	Honeywell	XYR 6000 TempDI	OW320.1-15.0	1230000049	FE80 :: 0040:8440:000.		
SYSTEM 🗸										
MANAGE LICENSES										
				1) H	Go to page	$1 \rightarrow$		Devices	ser page	10

- 7. Select the field device channel from the selection list and click **Inactivate**.
- 8. Ensure you inactivate the channels before starting calibration. You cannot perform calibration when the channel is online.
- 2. Click Apply.
- 3. In the Property Panel, expand **Calibration**.

TD_1010_4. Channel	I_6FLR.Tempera	tureDI AIO 1	:	X	
	Cal Cmd :	None			
	Cal Status :	None			
	Cal Point High:	871.000000			
	Cal Point Low :	-18.000000			
	Cal Source :	Factory			ŀ
	Cal Unit:	°C			
	Temperature	Calibration			
	RESET		APPLY		

4. Click **Invoke Method** to open the method dialog box.

	-≻́[ure	Calibration	×
Select the unit:		Select ~	
	I	NEXT	

- 5. Select the unit (°C or °F) and click **Next** and follow on-screen instructions to complete calibration.
- 6. Select **Yes** or **No** and click **Next**.

	-j Temperatur	e Calibration	×
-	ower Calibration point value = 18.00000 °C Do you want to le the lower calibration value? :	No A]
		NEXT	

To cancel the calibration process at any stage of method execution, click **Abort**.

You can close the method dialog box while the method execution is in progress.

After completion, a message appears indicating that the calibration process completed successfully.

- 7. Select the field device channel from the selection list under **CHANNELS** from Left Navigation Menu bar and click **Activate**.
- 8. Click Apply.
 - You can run only one method at a time for a field device using the current login session.
 - If you close the Web browser while a method is running and logon as another user, you can start another method on the same device only after a few minutes.

To calibrate field device by setting the calibration parameters:

 Select the field device channel from the selection list under CHANNELS from Left Navigation Menu bar and click Inactivate. Ensure you inactivate the channels before starting calibration. You cannot perform calibration when the channel is online.

- 2. Click Apply.
- 3. In the Property Panel, expand **Calibration**.

TD_ Chai	_1010_4J_6FLR.Tempera nnel	tureDI AIO 1	5	2	
	Cal Cmd :	None			
	Cal Status :				
	Cal Point High :	871.000000			
	Cal Point Low :	-18.000000			
	Cal Source :				
	Cal Unit:	℃			
	Temperature	Calibration			
	RESET		APPLY		

- 4. Set the following calibration parameters:
 - Cal Cmd The options available are None, Cal Lower (to calibrate device with lower calibration limit), Cal Upper (to calibrate device with higher calibration limit), Cal Restore (to restore calibration setting), and Cal Clear (to clear calibration setting).
 - Cal Point High
 - Cal Point Low
 - Cal Unit
- 5. Click Apply.
- 6. Select the field device channel from the selection list under **CHANNELS** from Left Navigation Menu bar and click **Activate**.
- 7. Click Apply.

Configuring field device channels for ISA100 Wireless devices

Configure Mode and Scale

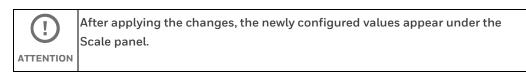
To configure Scale

- 1. Select the field device channel in the Selection Panel.
- 2. Expand **Process Variable** in the Property Panel to view the following read-only parameters in the OneWireless user interface.

TD_1049_7F_5FLR.TemperatureDI AIO 1 Channel	X :
Channel Summary	
Process Variable	
Process Value Value : 15.54 Status : Good Good EU at 100% : 871.000000 EU at 0% : -18.000000 Units Index : °C	
Mode	
Scale	
Calibration	
Sensor	
Values and Trends	

- EU at 100%: Specifies the high range PV value in Engineering Units.
- EU at 0%: Specifies the low range PV value in Engineering Units.
- Units Index: Specifies the unit of the measurement value. The value varies according to the sensor type selected for a channel. For example, in a temperature device, when the sensor type changes to a thermocouple (TC-J) or mV-50 range, the transducer block sets the Units Index to °C or mV.

3. Click Apply.



To configure Mode:

1. Select the channel from the **Selection Panel** and expand **Mode** in the Property Panel.

TD_1049_7F_5FLR.TemperatureDI AIO 1 Channel	8
Channel Summary	
Process Variable	
Mode	
Mode Actual/Target : Auto Normal : Auto Permitted OOS : Man : Auto : Auto :	
Scale	
Calibration	
Sensor	
Values and Trends	

2. Select the mode as required in the **Actual/Target** list.

The mode types available are **Normal**, **OOS**, and **Auto**. If the device type is Digital Output (DO), an additional mode **Man** is also available in the **Target** list.

3. Click Apply.

Add channels to publication groups

Perform the following steps to enable/disable the PV publication capability of field devices.

To add channels to publication groups:

- 1. Select the field device channel in the Selection Panel.
- 2. Expand Input Publication or Output Publication panel in the Property Panel.
- 3. Select the channels for which data publication needs to be enabled in the **Channel** drop-down list. After you select a channel, use the **Attribute** drop-down list to select the preferred measurement value.

Publication Group 1			
Contract Statu		Active	
Rat	te :	1 minute	
Stale Lim	nit :		
Destinatio	on :	wdm1	
Attribute 1			
Channe	el :	TemperatureDI AIO 1	
Attribut	te :	PV	
Attribute 2			
Channe	el :	TemperatureDI BIO 2	
Attribut	te :	PV_B	
Attribute 3			
Channe	-1 ·	TemperatureDI BIO 3	
		MODE	
Attribut	te :	MODE	
Attribute 4			
Channe	el :	None	
Attribut	te :	None	

4. Click Apply.

Configure channel instantiation

ATTENTION

OneWireless Network supports block instantiation for field device channels. You can add, remove, and reconfigure channels on supported field devices. An individual channel can be configured for one of the several roles, such as an analog temperature input, an analog current input, or a discrete input.

You can instantiate channels, only for the following supported field devices from Honeywell.

- XYR 6000 Multi AI DI
- XYR 6000 Multi AI DI DO
- XYR 6000 Temp DI

You can add, remove, and reconfigure channels on a supported field device using the user interface.

To inactivate channel:

- 1. Select the field device channel in the Selection Panel.
- 2. On the Property Panel, expand Mode and then in the Target list, click OOS
- 3. Click Apply.

The channel icon appears as blue indicating the inactive mode.

To remove channel from publication group:

- 1. Select the field device channel in the Selection Panel.
- 2. Expand Input Publication in the Property Panel.
- 3. Click **None** in the **Channel** drop-down list to remove the channel from the publication group.

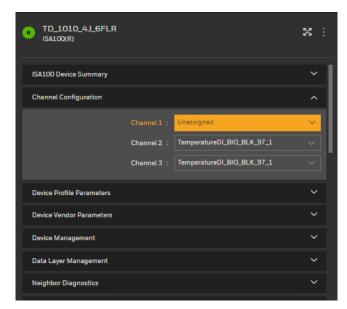
Input Publication			
Publication Group	ı ———		
	Contract Status :	Active	
	Rate :	1 minute	
	Stale Limit :		
	Destination :	wdm1	
Attribute 1			
	Channel :	TemperatureDI AIO 1	
	Attribute :		
Attribute 2 _			
	Channel :	TemperatureDI BIO 2	
	Attribute :	PV_B	
Attribute 3			
		TemperatureDI BIO 3	
	Channel :	Temperatureor Bio S	
	Attribute :	MODE	
Attribute 4			
	Channel :	None	
		Nee	
	Attribute :	None	

4. Click Apply.

Wait for a few seconds to save the changes.

To delete (un-instantiate) channel:

1. Expand **Channel Configuration** and click **Unassigned** in the drop-down list for the channel to be deleted.



2. Click Apply.

The channel disappears from the map view and the **Selection Panel**.

To instantiate channel

1. Expand **Channel Configuration** and click the respective instantiable object type for the channel to be instantiated.

In the following example illustration, the temperature DI field device has three instantiable channels. Each channel can be instantiated as an analog input channel or a binary input channel.

R TD_1010_4J_6FLR ISA100(R)			2
ISA100 Device Summary			~
Channel Configuration			^
	Channel 1 : Channel 2 : Channel 3 :	Unassigned Unassigned TemperatureDI_AIO_BLK_99_1 TemperatureDL_BIO_BLK_97_1 TemperatureDI_BIO_BLK_97_1	~ ~
Device Profile Parameters			~
Device Vendor Parameters			~
Device Management			~
Data Layer Management			~
Neighbor Diagnostics			~

2. Click Apply.

To add channel to publication group:

- 1. Expand Input Publication panel in the Property Panel.
- 2. Click the channel for which data publication needs to be enabled In the **Channel** drop-down list.
- 3. Click Apply.

Remove channels from publication groups

To remove channels from publication groups:

- 1. Select the field device channel in the Selection Panel.
- 2. Expand Input Publication in the Property Panel.
- 3. Click **None** in the **Channel** drop-down list to delete the channel from the publication group.
- 4. Click Apply.

Delete (un-instantiate) channels

Prerequisites

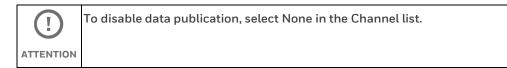
- Ensure that the channel is set to OOS mode.
- Ensure that the channel is not configured for publication in any of the Input/Output Publication groups. If configured, remove the channel from the Publication group.

To delete channels

- 1. Select the field device channel in the Selection Panel.
- 2. Expand Channel Configuration in the Property Panel.

The **Channel Configuration** panel displays a list of instantiated channels.

- 3. Select the channel to delete and select **Unassigned** in the corresponding drop-down list.
- 4. Click **Apply**.



5. Click Apply.

Enable Device Network System (DNS)

NOTE

DNS can be enabled either on PCN or on SIN, but not on both.

To enable Device Network System (DNS) in Process Control Network (PCN)

- 1. Select Manage Devices from Left Navigation Menu bar.
- 2. Select the **WDM** from the selection panel.
- 3. Expand the property panel for WDM.
- 4. Under **Process Control Network (PCN)**, to enable Device Network System (DNS), select the **Enable DNS** check box.
- 5. Provide DNS details such as **Preferred DNS Server** and **Alternate DNS Server**.



To enable Device Network System (DNS) in Special Interface Network (SIN)

- 1. Select Manage Devices from Left Navigation Menu bar.
- 2. Select the **WDM** from the selection panel.
- 3. Expand the property panel for WDM.
- 4. Under **Special Interface Network (SIN)**, to enable Device Network System (DNS), select the **Enable DNS** check box.
- 5. Provide DNS details such as **Preferred DNS Server** and **Alternate DNS Server**.

	Special Interfac	e Network (SIN)		ŝ	^	
	IP Address				-1	
		IP Address :	192.168.2.1			
_		Subnet Mask :	255.255.255.0			
		Default Gateway :	0.0.0			
	DNS -					
			192.168.2.20			
_		Alternate DNS Server :	0.0.0.0			
Ţ	To enal	ole DNS, mal	ke sure that	SIN is er	abled.	
NOTE						

Enable Single Sign On

See Single Sign On-User's-Guide-OWDOC-X742-en for more information.

Adding notes for devices

You can add device notes for WDM, FDAPs, PCAPs, Access Points or field devices. These notes can be used as a logbook for the device.

Perform the following steps to add notes for any configured device. Note that the notes added for devices are saved on the WDM and not on the device.

To add notes

- 1. Select the required device in the Selection Panel.
- 2. Expand **Notes** in the Property Panel.
- 3. Click the **Add note** icon. A text box appears.

Notes		^
notes	by	

4. Type the note and click **Apply**.

\bigcirc	All users can view all the notes added by other users.
(!)	
ATTENTION	 To delete any note, click the delete icon adjacent to the note.
ATTENTION	 Users with User role can delete only notes added by them.
	 Users with Administrator role can delete other users' notes.
	Notes are not restored during a replace operation.

5. To edit a note, double-click the note, make the necessary changes, and then click **Apply**.

Operations

Setting up the monitoring area

About site-specific monitoring

The OneWireless user interface enables you to create multiple maps for setting up sitespecific monitoring areas. After the initial configuration, WDM creates a default map. Based on the plant topology, you can create multiple site maps and place the devices under these maps. This enables site-specific monitoring of the devices that are placed in different locations of a plant. In addition, a site map of that particular location can be uploaded to the map. You can position the devices on the site map in such a way that it reflects the real plant topology.

You can create a map of entire plant and maps of smaller areas, each containing the same devices. The FDAPs and devices can be placed on multiple maps.

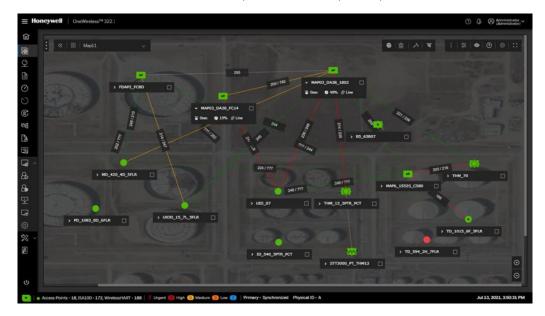


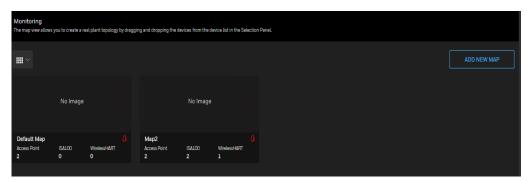


Fig. 14. Site-specific monitoring

Configure site maps

To add new map:

1. From Left Navigation Menu bar, click **Monitoring** to view the Maps.

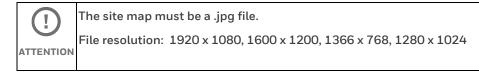


2. Click ADD NEW MAP

- 3. Type the name of the map in the **Map Name** box.
- 4. Type the description for the map in the **Description** box.

5. Click **BROWSE** to load the image. Browse to the location where the site map is saved, and then select the site map.

	me Q			
MAP NAME	DESCRIPTION	Map Name *	Description	
Default Map	Default map	МарЗ		
Map2		File Name •		
		Choose file		BROWSE
		Image size should be in 1920*1080px with formet as jpeg		
		' Indicates required fields		



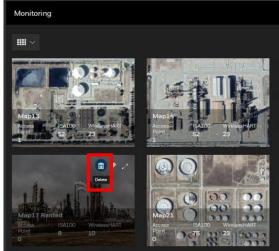
- 5. Click **Open** to upload the site map.
- 6. Click Save.

To edit map

- 1. From Left Navigation Menu bar, click **Monitoring.**
- 2. Click the edit icon to edit the site map details.
- 6. Click **Save** to save the changes.

To delete map

- 1. From Left Navigation Menu bar, click Monitoring.
- 2. <u>Click the delete icon to remove any previously loaded site map.</u>

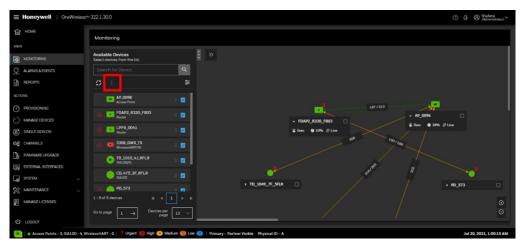


Position the devices on the map

After uploading the site map for a particular location, you can position the devices on the map to reflect the physical design and structure of your plant. The devices do not appear on the map view, by default.

To position the devices on the map:

- 1. On the Selection Panel, select the device to be positioned on the map.
- 2. Click i icon to expand the **Available Devices** menu.
- 3. You can refresh the selection by clicking the **refresh** button.
- The Filter option allows you to customize the device list by filtering the devices. By default, all the devices appear in the device list. You can filter by Device Type, Device Status, Vendor, Model, Power Source, Alarm Priority, Hop Level, and Maps.
- 5. Click the highlighted icon and **Select all devices** to select all the devices together.



6. You can also select individual devices as shown below.



7. Drag the device and drop it on the required location on the map.

Available Devices Select devices from the list.	1	K BB Boiler V		● 亩 ∧ च	: ≊ ∞ 0 © ::
Search for Device	¢.	> FC_1808 254/238	235 AP_0096		
AP_0096 Access Point		105_5FL_SFT 067_7F_5FLR C	0_475_3F_6FLR		
FDAP2_R320_FB03 Router	. 2		→ PD_573		
EML_65656 WirelessHART(R) MacTek_sdapter_11 WirelessHART(A.R)	Dreg Davice On Mag	* acTek_adapter_11 > EML_65656	*		
CD_475_3F_6FLR ISALDO(R) TD_105_5FL_SFT					
(R) (SA100(R)	н 1 н	love 1 devices on the map			
Go to page 1 \rightarrow	Devices per 10 ~				

- 8. Repeat steps 1 and 2 to place other devices.
- 9. Click $\stackrel{\text{N}}{\longrightarrow}$ icon in the top left of map view for the Map options.

10. On the top-right of Map view, click icon > View.

11. Select **Lock Map** check box to the lock the map.

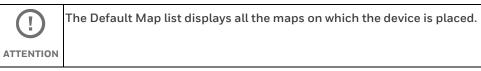
You must lock the map to prevent device locations from being accidentally modified.

Change the default map for a device

From the Property Panel, you can only change the default map for an FDAP/PCAP or a field device. This has no effect on the actual current placement of a device on any map. The default map is only used for display purposes in reporting alarms, reports, and so on. You cannot change any physical placement of a device from the property panel. In fact, only maps on which the device is currently placed appears in the drop down for default map.

To change the default map for a device

- 1. Select the required device from the Selection Panel under Manage Devices.
- 2. Expand the **Device Summary** in the Property Panel.
- 3. From the **Default Map** list, select the required map on which the device must be placed.



Remove device from the map

To remove a device from the map:

- 1. Click the **Monitoring** from left navigation menu to view the map view.
- 2. From the **Selection Panel** or map view, select the device.

- 3. Click icon in the top left of map view for the Map options.
- 4. Click icon to remove selected devices from the current map.

Configuring Connection Quality Options

Connection quality is based on the Receive Signal Strength Index (RSSI), Receive Signal Quality Index (RSQI), and Transmit Fail Ratio (TxFailRatio). Using the Connection Status Options, you can configure thresholds for RSQI, RSSI, and TxFailRatio. The overall quality of an active connection is based on RSQI, RSSI, or TxFailRatio. If RSQI, RSSI, or TxFailRatio is poor, connection quality is poor. Connection quality is displayed as good (green), fair (orange), or poor (red).

To configure connection quality options

- 1. Click icon in the top left of map view for the Map options.
- 2. Click contoview the Connection Status. The Connection Status Options dialog box appears.



- 3. In the boxes near the separator bars, type the RSSI, RSQI, and TxFailRatio values.
- 4. Click **APPLY**, and then click **OK**.



Verifying connectivity using maps

Perform the following steps to verify mesh connectivity and device connectivity.

To verify mesh connectivity and device connectivity

- 1. Click the **Monitoring** tab to view the map view.
- 2. Visually inspect network topology map and connectivity.
- 3. Navigate to the device in the topology map and check the link signal quality and connectivity.

The RSSI range is displayed in the format -xx/-yy dBm, where -xx and -yy represent the link strength of the devices connected to each other. When the difference between -xx and -yy is less than 5, the lowest of the two values is displayed.

The RSSI range is displayed in the format xx/yy, where xx and yy represent the link quality index of the devices connected to each other. When the difference between xx and yy is less than 10, the higher of the two values is displayed.

For example, in the following illustration, the value -55 represents RSSI of the device (EML_65656) and the value -62 represents the RSSI of the device (AP_0096).



- 4. Verify the device communication statistics information such as RSQI, RSSI, and TxFailRatio as follows:
 - a. Click $\stackrel{}{\longrightarrow}$ icon in the top left of map view for the Map options.
 - b. Click icon to select **View** and **Overlay** settings option.
 - c. Select **Overlay > Display All Connection >** Select the required device communication statistics information such as **RSQI**, **RSSI**, and **TxFailRatio**.

	⊕ 💼 🕹 ≒	: 💿 🧿 💿
	Display No Connection	< Overlay
Show Inactive Connections	Display All Connection	
No Display Of Data	Display Routing Connections	
Display RSQI	Display Synchronization	
O Display RSSI	Connections	
Display Tx Fail Ratio		

A green line between the devices in the map view indicates strong signal quality, whereas a red line indicates weak signal quality. A solid line between the devices represents an active connection between the devices and a dotted line represents an inactive connection.

The connection quality details are displayed as tool tip when you hover the mouse over the connection.



You can modify connection quality ranges.

Option	Description
RSQI range	192 to 255: Excellent
	128 to 192: Good
	64 to 128: Fair
	0 to 64: Poor
RSSI range	-75 to -25: Good
	-85 to -75: Fair
	-100 to -85: Poor
TxFailRatio	0 to 25: Good
	25 to 50: Fair
	50 to 100: Poor

Configuring alerts for Honeywell ISA100 Wireless field devices

You can configure to enable or disable the following alerts for Honeywell field devices if the DD files for the devices are loaded to the WDM.

- **Maintenance Required alerts**: Generated to indicate low battery or low external power condition.
- **Out of Specification Status alerts**: Generated for calibration errors, thermocouple condition warning, or indeterminate discrete input state.
- **Failure Status alerts**: Generated for fault conditions such as input failure, output failure, or electronic failure.
- Function Check Status: Generated for conditions such as device channel out of service.

To configure alerts for field devices

- 1. On the Selection Panel, select the field device.
- 2. On the Property Panel, expand **Device Vendor Parameters**.
- 3. For the type of alert to be configured, perform one of the following.
 - To enable alert generation, clear the **Alert Disable** check box.
 - To disable alert generation, select the **Alert Disable** check box.

	While configuring the network, ensure that the lowest RSQI on each
$\mathbf{\cdot}$	active link is greater than 180 and the lowest RSSI on each active link is
ATTENTION	greater than -80 dBm. An active link with RSQI/RSSI values higher than
	the specified values protects the signals when the signal strength/quality
	degrades due to transient environmental conditions.

- 4. Set the Alert Priority. The **Alert Priority** can contain the following values.
 - 0-2: Journal (only events are reported)
 - 3-5: Low
 - 6-8: Medium
 - 9-11: High
 - 2-15: Urgent
- 5. Click Apply.

Monitoring the network and the devices

You can monitor the performance of the network and the devices that have joined the network. All the devices that have joined the network are accessible from the Selection Panel. The extended Selection Panel allows you to view the details about the devices in the network.

Color of the channel represents the state of the channel (AUTO, OOS). Device specific attributes are shown in the Property panel when a device is selected in Selection panel. Channel specific attributes are shown in the Property panel when channel is selected in the Selection panel.

For a WirelessHART device, the Process Variables such as PV, SV, QV and TV are shown as children. The color of the channel represents the status of the process variables (Good or Bad). Device specific attributes are shown in the Property panel when device is selected in selection panel from Manage Devices. Process variable specific attributes are shown in the Property panel when channel is selected in the Selection panel.

	wdm1	Device Manager	Joined	Honeywell	WDM	OW322.1-40.0	0	FEB0::4E7C:COA8:	Line
	AP_0096	Access Point	Joined	Honeywell	FDAP2	OW322.1-25.0	2011160002	FE80::4E78:C0A8	Line
	FC_180B	Access Point	Joined	Honeywell	PCAP	OW322.1-35.0	2021070010	FE80::4E7B:C0A8:	Line
	FDAP2_R32_ 🦓	Router	Joined	Honeywell	FDAP2	0W322.1-14.0	2014490009	FE80::0040:84FF:	Line
~	EML_65656	WirelessHART(R)	Joined	Honeywell	Emulator		66051	FE80::001B:1E17:	High
	Name	(i	Channel	N	Mode	Value		Status	
	O PV	1	4A	N	۸A	25.000 °C		Good, Not Limited	
	o sv	(1	44	N	AN.	5.100 mbars		Good, Not Limited	
	עד 🥥		۹A	N	NA.	59.270 Perce	nt	Good, Not Limited	
	ov ov	81	44	N	NA.	5.150 mA		Good, Not Limited	
~	CD_475_3F	ISA100(R)	Joined	Honeywell	XYR 6000 Corr	Corrosion version 2	S040843000000204	FE80 :: 0040:8430:	High
					ATR 0000 Coll	Corroatori veratori 2	304084300000204		nign
~	TD_105_5FL	ISA100(R)	Joined	Honeywell	XYR 6000 TempDI	Temperature DI vers	408105	FE80::0040:8430:	High
^	TD_105_5FL	ISA100(R)		Honeywell					
^		ISA100(R)	Joined	Honeywell	XYR 6000 TempDI	Temperature DI vers		FE80 : : 0040:8430:	
	Name	ISA100(R)	Joined Channel	Honeywell	XYR 6000 TempDi Mode	Temperature DI vers Value		FE80 : : 0040:8430: Status	
	Name	ISA100(R)	Joined Channel	Honeywell A	XYR 6000 TempDI Mode	Temperature DI vers Value 22.89 °C		FE80::0040:8430: Status Good	
	Name TemperatureDI AIO 1 TemperatureDI AIO 2	ISA100(R)	Joined Channel	Honeywell A	XYR 6000 TempDI Mode Nuto	Temperature DI vers Value 22.89 °C 22.92 °C		FEBD:::0040:8430; Status Good Good	
	Name TemperatureDI AIO 1 TemperatureDI AIO 2 TemperatureDI AIO 2	ISA100(R) 1 2 3 3	Joined Chennel	Honeywell N	XYR 6000 TempDI Mode Liuto	Temperature DI vers Value 22.89 °C 22.92 °C 22.92 °C	408105	FE80 :: 0040:8430 Status Geod Geod Geod	High
	Name TemperatureDI AIO 3 TemperatureDI AIO 3 TemperatureDI AIO 3 DED_573@	ISA100(F)	Joined	Honeywell A	XVR 6000 TempDI 40de Lutts STW TempAIDO	Temperature DI vers Value 22.89 °C 22.92 °C 22.92 °C Sensor version 001	408105	FEB0 :: 0040-8430 Status Good Good Good FE80 :: 0102-0304	High

Fig. 15. Monitoring the network using extended Selection Panel

The following tables explain the device and the channel attributes that are available in the extended Selection Panel.

Device	Description
Tag Name	Name of the device.
Туре	Device type, which can contain the following values.
	Device Manager for WDM
	Access Point for FDAP and Access Points
	Routing for FDAP routers
	Device, Routing for field devices
Status	Device status.
	The status can be Offline, Joining, or Joined.
Vendor	Device vendor name.
Model	Device model.
	For example, XYR 6000 HLAI is the device model for Honeywell HLAI devices.
Revision	Device sensor firmware revision number.
	To view the radio firmware revision, select the Show Radio Identification check box.
Serial	Serial number of the device.
IP6 Address	IPv6 address of the device.
Power	Power source of the device, which can contain the following values.
	Line for line powered FDAPs or WDM.
	High, Low, or Medium for battery powered field devices.
Name	Channel name.
Channel	Channel number.
Mode	Device channel mode, which contains the values AUTO, OOS, or MAN.
Value	Process Value.
Status	PV status.

Table, 8.	Device attributes in the extended Selection Panel
Table. o.	Device altributes in the extended Selection Panel

You can view the PV trend in the **Values and Trends** panel of the channel's Property Panel.

Alarm and event management

Understand alarms and events

The following table provides a summary of the various alarms and events generated by the OneWireless devices and the recommended corrective action to handle the alarms and events.

Source	Alarm/Event notification	Possible cause	Consequence s	Recommended corrective action	Response time	Parameter/ Reported value	Defaul value
WDM	Bad Join Key	FDAP or field device is attempting to join the network with an invalid key.	the join	Locate the devices and re-provision the devices with valid join keys.	N/A	None	N/A
WDM	Expired Join Key	FDAP or field device is attempting to join the network with an expired key.	the join	Locate the devices and re-provision the devices with valid join keys.	N/A	None	N/A
WDM	Key Authenticatio n Failed	FDAP or field device security confirmation failed due to an invalid master key.	WDM rejects the join request by the FDAP or the field device.	None	N/A	None	N/A
WDM	Offline	FDAP or field device is offline.	None	None	N/A	EUI64 of the device	N/A
WDM	Joining	FDAP or field device is joining the network.	None	None	N/A	EUI64 of the device	N/A
WDM	Joined	FDAP or field device has joined the wireless network.	None	None	N/A	EUI64 of the device	N/A

Source	Alarm/Event notification	Possible cause	Consequence s	Recommended corrective action	Response time	Parameter/ Reported value	′ Default value
WDM	Not Synchronized	Redundancy enabled, but sync not yet enabled or completed. Error occurred during communication between redundant WDMs over the RDN private path. Sync is disabled.	of view and/or	Reconnect RDN private path communication cable. If redundancy is no	N/A	N/A	N/A
WDM	Switchover	Switchover can be initiated from primary or secondary WDM. The following conditions result in switchover: FDN or PCN Ethernet cable is disconnect on the primary WDM. Loss of power on the primary WDM. Software failure on the primary WDM. Hardware failure on the primary WDM.	WDM role change.	If switchover occurred due to FDN and/or PCN cable disconnect on original primary, verify connections. Reason for switchover is available in the redundancy history section in the redundancy tab in the WDM Properties Panel Take appropriate corrective action to restore WDM redundancy based on this reason. In case of hardware or software failure in the original primary, contact customer support.	N/A	N/A	N/A

Source	Alarm/Event notification	Possible cause	Consequence s	Recommended corrective action	Response time	Parameter/ Reported value	' Default value
WDM	Redundant Partner Visible on Redundant Link	Redundant WDM sync state changes to partner visible.	None	None	N/A	N/A	N/A
WDM	Redundancy Sync Maintenance	Redundant WDM sync state changes to sync maintenance.	None	None	N/A	N/A	N/A
WDM	Redundancy Sync In Progress	Redundant WDM sync state changes to sync in progress.	None	None	N/A	N/A	N/A
WDM	Redundant Non- Redundant	During role determination, the WDM configuration is changed from non-redundant to redundant.	None	None	N/A	N/A	N/A
WDM	Redundant No Partner	Sync state changes to no partner when WDM is configured as redundant.	None	None	N/A	N/A	N/A
WDM	Redundant Incompatible Partner	Redundant WDM sync state changes to incompatible partner.	None	None	N/A	N/A	N/A
WDM	Sync Hardware Failure	Redundant WDM serial port initialization fails.	Restart WDM.	Re-enable redundancy, restart WDM	N/A	N/A	N/A

Source	Alarm/Event notification	Possible cause	Consequence s	Recommended corrective action	Response time	Parameter/ Reported value	′ Default value
WDM	Redundant Physical ID A	Redundant WDM physical ID changes to A due to startup/ change.	None	None	N/A	N/A	N/A
WDM	Redundant Physical ID B	Redundant WDM physical ID changes to B due to startup/ change.	None	None	N/A	N/A	N/A
WDM	Redundant Partner not visible on PCN	Primary or secondary WDM communicating with compatible partner and partner is not visible across PCN.	Sync is inhibited	Ensure that primary and secondary are connected to the PCN network. Verify PCN switch connections.	N/A	N/A	N/A
WDM	Redundant Partner not visible on FDN	Primary or secondary WDM communicating with compatible partner and partner is not visible across FDN	Sync is inhibited	Ensure that primary and secondary are connected to the FDN network. Verify FDN switch connections.	N/A	N/A	N/A

Source	Alarm/Event notification	Possible cause	Consequence s	Recommended corrective action	Response time	Parameter/ Reported value	Default value
WDM	failed to connect to	If MQTT connection to the server not established successfully or dropped	publish to MQTT Broker will fail	Verify the configured interface (SIN/PCN) connections. Ensure the valid MQTT Broker certificate is imported to WDM. Ensure the WDM certificate is added to trust store of the MQTT Broker	N/A	N/A	N/A
WDM	Certificate Expires	The Certificate is about to expire in seven days	Applications which are using the certificate for secure communicatio n will fail.	Review the Certificate and Import.	N/A	N/A	N/A
FDAP, field device	Power Status Changed	The power status of FDAP or field device is changed.		Replace the field device battery	Immediate	POWER_ SUPPLY_ STATUS	N/A
FDAP, field device	Device Restarted	FDAP or field device radio is restarted.	None	None	N/A	RESTART _COUNT	0

Source	Alarm/Event notification	Possible cause	Consequence s	Recommended corrective action	Response time	Parameter/ Reported value	Default value
FDAP, field device	Clock Drift	 FDAP clock has drifted 200 msec or greater from the WDM clock. FDAP corrects its clock automatically over a period of time. If the difference between the FDAP clock and the WDM clock is too high, the FDAP may drop from the network. 	Loss of communicatio n with the field device and the associated channels.	encountered when installing a	N/A	None	N/A
FDAP, field device	Illegal Use of Port	FDAP received a message (TPDU packet) over the wireless network on an unexpected port.	None	Remove uncertified or incompatible Wireless devices from the Wireless network.	N/A	16-bit TL port number	N/A

Source	Alarm/Event notification	Possible cause		Recommended corrective action	Response time	Parameter/ Reported value	Default value
FDAP, field device	TPDU Does Not Match Security Policies	 FDAP received a message (TPDU packet) that does not match the current security policy. Unavailability of session key or configuration of an unsupported security algorithm, or configuration of an unsupported security mode. 		Remove uncertified or incompatible Wireless devices from the Wireless network.	N/A	TPDU	N/A
FDAP, field device	TPDU Received on Unregistered Port	FDAP received a message (TPDU packet) over the wireless network on an unexpected port.	None	Remove uncertified or incompatible Wireless devices from the Wireless network.	N/A	TPDU	N/A
FDAP, field device	Illegal Use of Port	FDAP received a message (TPDU packet) over the wireless network on an unexpected port.	None	Remove uncertified or incompatible Wireless devices from the Wireless network.	N/A	16-bit TL port number	N/A

Source	Alarm/Event notification	Possible cause	Consequence s	Recommended corrective action	Response time	Parameter/ Reported value	′ Default value
FDAP, field device	TPDU Received on Unregistered Port	FDAP received a message (TPDU packet) over the wireless network on an unexpected port.	None	Remove uncertified or incompatible Wireless devices from the Wireless network.	N/A	TPDU	N/A
FDAP, field device	TPDU Does Not Match Security Policies	 FDAP received a message (TPDU packet) that does not match the current security policy. Unavailability of session key or configuration of an unsupported security algorithm, or configuration of an unsupported security mode. 		Remove uncertified or incompatible Wireless devices from the Wireless network.	N/A	TPDU	N/A

Source	Alarm/Event notification	Possible cause C s		Recommended corrective action	Response time	Parameter/ Reported value	Defau value
FDAP, field device	DL Connectivity	transmission between wireless field devices, at 90% packet failure rate or	oss of communicatio h with the field device and the associated channels.	 Reposition the device or the antenna to minimize interference Reposition the antenna if the directional antenna is installed. Remove any strong interference sources near the Wireless device or reposition the Wireless device to 	N/A	Neighbor Diag	N/A
FDAP, field device	Neighbor Discovery	Discovery of a new neighbor near the FDAP or the field device in the wireless network.	Vone	None	N/A	DLMO_C ANDIDA TES	NZA
FDAP, field device	Alarm Recovery Start	Initiation of Nalarms recovery for FDAP or field device radio.	None	None	N/A	None	N/A
FDAP, field device	Alarm Recovery End		None	None	N/A	None	N/A

Source	Alarm/Event notification	Possible cause	Consequence s	Recommended corrective action	Response time	Parameter/ Reported value	Default value
FDAP, field device	MPDU Failure Rate Exceeded	 Occurrence of FDAP or field device security authentication failure for five packets per minute or greater, at the data link layer. A poor link or strong interference due to frequent packet security failures. 	Loss of communicatio n with the field device and the associated channels.	sources near the wireless field	N/A	Number of failures	N/A
FDAP, field device	TPDU Failure Rate Exceeded	 Occurrence of FDAP or field device security authentication failure for five packets within five minutes at the transport layer. Invalid or mismatched session key in the wireless field device. 	Loss of communicatio n with the field device and the associated channels.		N/A	Number of failures	N/A

Source	Alarm/Event notification	Possible cause		Recommended corrective action	Response time	Parameter/ Reported <u>value</u>	Defau value
FDAP, field device	Malformed APDU Received	FDAP or field device received a message (APDU) with an incorrect length, invalid read/ write/execute/ publish service, or invalid parameters for the specified service.	None	None	N/A	Device address generating Malformed APDU's	N/A
Field device	Device Offline	Field device is offline.	Loss of communicatio n with the field device and the associated channels.	communication between the WDM	Immediate	EUI64 of the device	N/A
Field device	Begin Alert Recovery	Initiation of alarms recovery of field device sensor radio.	None	None	N/A	None	N/A
Field device	End Alert Recovery	Completion of alarms recovery of field device sensor radio.	None	None	N/A	None	N/A

Source	Alarm/Event notification	Possible cause	Consequence s	Recommended corrective action	Response time	Parameter/ Reported value	Default value
Field device	Device Restart	Field device sensor is restarted.	None	None	N/A	RESTART _COUNT	0
Field device	Maintenance Alert	Critically low battery power or external power is detected by the field device sensor.	Loss of communicatio n with the field device and the associated channels.	Check the	 For battery powered devices replace the batteries within two to four weeks after initial alert. For externall y powered devices immediate action is required. 	DIAG_ST ATUS, DIAG_ST ATUS_D ETAIL	0
Field device	Out of Specification Alert	Invalid or unreadable calibration data.	Channel may report incorrect PV value.	Perform user calibration.	Immediate	DIAG_ST ATUS, DIAG_ST ATUS_D ETAIL	0

Source	Alarm/Event notification	Possible cause		Recommended corrective action	Response time	Parameter/ Reported value	′ Default value
Field device	Failure Status Alert	 An electronics failure, including NVM fault, RAM fault, program memory fault, or A/D failure is detected by the field device sensor. Cold junction failure. 	 Loss of communi cation with the field device and the associate d channels. Channel reports incorrect PV value. 	 Restart the field device radio and sensor. If condition persists, replace the sensor module. Check the connectors on the terminal board and sensor module. Replace the terminal board. 	Immediate	DIAG_ST ATUS, DIAG_ST ATUS_D ETAIL	0
Field device Al Channel	Out Of Service	Field device Al channel is out- of-service.	None	None	N/A	MODE.A CTUAL	OOS
Field device AI Channel	Sensor Over Temperature	The meter body exceeded the maximum temperature as defined by the meter body characterizatio n data.	Channel may report incorrect PV value.	Determine cause of excessive temperature.	Immediate	DIAG_ST ATUS, DIAG_ST ATUS_D ETAIL	0
Field device Al Channel	Out Of Service	Field device DI channel is out- of-service.	None	None	N/A	MODE.A CTUAL	OOS

Source	Alarm/Event notification	Possible cause		Recommended corrective action	Response time	Parameter/ Reported <u>value</u>	Default value
Field device Al Channel	Input Failure	Cold junction failure.	Channel reports incorrect PV value.	 Check connectors on the terminal board and the sensor module. Replace the terminal board. 	Immediate	DIAG_ST ATUS, DIAG_ST ATUS_D ETAIL	0
Field device AI Channel	Out Of Service	Field device DO channel is out- of-service.	None	None	N/A	MODE.A CTUAL	OOS
Field device Al Channel	Fault Alert	Number of consecutively missed data publication exceeds the stale count limit. The configured output value is not received by the output channel on the field device.	 Output channel may shed to fault state value. Change s to the Change output value would reflect on the 	Determine the cause of missing the published data or verify the stale count limit.	Immediate	DIAG_ST ATUS, DIAG_ST ATUS_D ETAIL	0

In addition to the alarms and events listed in the above table, the following user-initiated events are also recorded in the events history.

Table. 9.	User actions logged in the Alarms/Events History tab
-----------	--

Login/logout	DHCP server configuration change	Device replacement	Perform manual WDM backup
Failed login attempt	change	Firmware upgrade operation when initiated, completed, aborted, or failed.	Publication period change
Create/delete user account	PCN subnet mask change	DD load	Publication stale limit change

Password change	PCN default gateway change	Device deletion	PD deletion
User role change	Disable/enable external NTP server	Channel instantiation	Security key transfer to the PD for field devices/ infrastructure devices
FDN subnet mask change	External NTP server change	Channel deletion	Channel activation/ inactivation
Enable/disable publication channel	Enable/disable automatic backup	Channels rename	Attributes write (data may be truncated. Maximum reported size = 308. Maximum old size = 256)
Enable/disable DHCP server	Automatic backup configuration change	Method initiation	Method completion/ abortion (data may be truncated; maximum size = 114)
Add/remove role permission	Set system time	Accept/reject over- the-air provisioning	Restore WDM from backup
Failure in restoring WDM from backup	Configure a new WDM	Reset WDM to factory defaults	Restart WDM
FDN IP address changed	Write protect/unprote ct.	-	Redundant partner PCN IP changed

Monitor alarms and events

The Active Alarms tab displays the category, description, priority, default map, source, reported value, and time. The Alarms/Event History tab provides a tabular view of the events, displays event class, event category, priority, event start time, event source, location, and description. You can also export the alarm log and event log for a particular period.

Whenever a new alarm is triggered, a pop-up window appears in the user interface displaying the details of the alarm such as source, time, description, and priority. When multiple alarms are reported at the same time, the pop-up displays the message "You have multiple new alarms". Hovering the mouse over the window changes the appearance of the text displayed to that of a hyperlink. Click on the link to open the alarm display.

To monitor alarms and events

- 1. Click the Alarm/Events tab. The Alarm/Events page displays.
- 2. Click the Active Alarms tab. The Active Alarms page displays details about the active

alarms.

- 3. To view the alarm details, click on any alarm and expand **Alarm Detail** at the bottom of the pane.
- 4. Click the **Alarms/Events History** tab. The **Alarms/Events History** page displays details about all the alarms (active and inactive) and events.

Active Alarms Alar	ms & Events History										
S										⊞	
PRIORITY 🗘	EVENT CLASS	EVENT CATEGORY 🗘	EVENT START TIME 🗘	EVENT SOURCE	DEFAULT MAP 🗘	REPORTED VALUE	STARTED VALUE	DESCRIPTION \$	USER 🗘		
	Alarm J	DeviceDiagnostic	04/25/2021 7:30	wdm1	Unplaced			Demonstration Li			
Journal	Event	Security	04/25/2021 7:13	wdm1	Unplaced	127.0.0.1		Login	shafana		
Journal	Event	Security	04/25/2021 7:13	wdm1	Unplaced			Logout	shafana		
	Alarm J	DeviceDiagnostic	04/25/2021 6:30	wdm1	Unplaced			Demonstration Li			
	Alarm 🤰	DeviceDiagnostic	04/25/2021 5:30	wdm1	Unplaced			Demonstration Li			
	Alarm 4	DeviceDiagnostic	04/25/2021 4:30	wdm1	Unplaced			Demonstration Li			
	Alarm J	DeviceDiagnostic	04/25/2021 3:30	wdm1	Unplaced			Demonstration Li			
	Alarm 🧃	DeviceDiagnostic	04/25/2021 2:30	wdm1	Unplaced			Demonstration Li			

When an alarm is reported, the **Event Class** column displays a red alarm symbol. When the alarm returns to normal, the alarm symbol changes to black.

The following are the events that are reported in the Alarms/Events History.

- **Communications Diagnostic**: Reported for events such as device offline, device joining, device online, alarm recovery start, alarm recovery end, and so on.
- **Device Diagnostic**: Reported for events such as device restart, alarm recovery start, and alarm recovery end.
- Security: Reported for security-based events.
- User actions: Reported for user actions that are captured as events. For a list of user actions that are captured as events, refer to "Table 11: User actions logged in the Alarms/Events History tab" on page 119.

The **Alarms/Events History** page is not updated automatically. Click **Refresh** to manually update the **Alarms/Events History** page.

- 1. To export an alarm or event log:
 - a. Click Export Alarm Log or Export Event Log.
 - b. On the Export Logs window, click the Select export option, which the log needs to be exported. The following are the available export options.
 - Entire log
 - From last hours: Specify the number of hours for which the log needs to be exported.
 - From time period: Specify the From Date and To Date to export the log for that particular time period. Note that this is different from the time

when an event is detected which is reported in the **Event Start Time** column in the **Alarms/Events History** page.

- **Filter Logs**: Filter results is exported in the selected format.
- 2. Click **EXPORT ALARM LOG**. The alarm or event log is exported in the .csv format.

	Export to PDF is not supported
NOTE	

Viewing time synchronization parameters

Time synchronization parameters provide the details of the network clock master which distributes time to all the nodes within the time synchronization cluster.

To view the time synchronization parameters

- 1. On the Selection Panel, select an Access point/field device.
- 2. On the Property Panel, expand **Device Summary/Access Point Summary** for the respective device.
- 3. Under **Time Synchronization**, review the following time synchronization parameters.
 - **Time Master Tag Name**: The tag name of the device acting as the clock master in the time synchronization cluster.
 - Time Master Address: The short address of the clock master.
 - **Primary Parent**: The name of the primary node.
 - Primary Address: The network address of the primary parent.
 - Secondary Parent: The name of the secondary node.
 - Secondary Address: The network address of the secondary parent.
 - **Time Distribution Level**: The clock hop level in which the device is present.

A time master device (access point) is always at a Time Distribution level of O. A device that joins directly to this master is always be at level 1 and the devices joining through the level 1 devices are at level 2 and so on. Other access points in the network, synchronize its time from the clock master directly or indirectly through other access points. Hence they can be at time distribution level of 1, 2, or so on.

Viewing license agreement files

Honeywell End User License Agreement (EULA) and third-party licenses are available at the following locations.

Honeywell EULA: <u>https://<WDM IP Address>/licenses/Third_Party_Licenses.txt</u>

Third-party licenses: <u>https://<WDM IP</u>
 <u>Address>/licenses/Honeywell_End_User_License_Agreement.txt</u>

Configuring radio power level

Users with Professional Installer role can change the radio power level on an FDAP/PCAP or field device. You must have a valid WDM license to create a Professional Installer User.

Note that this option is available only for ISA100 Wireless devices.

	Contact GTAC to get the professional installer license.
ATTENTION	

To modify the radio power level:

- 1. On the Selection Panel, select the field device.
- 2. On the Property Panel, expand **Data Layer Management**.
- 3. Type the required Transmit Power Level.
- 4. Click **Apply**. The Confirm Transmit Power Level Change dialog box appears.
- 5. Click **OK** and confirm.

Activate process control interfaces

Establishing connection between WDM and external interfaces

Perform the following steps to connect OPC, Modbus, SmartRadar FlexLine (ENRAF), and HART interfaces to the PCN port of the WDM.

To connect OPC, Modbus, SmartRadar FlexLine (ENRAF), and HART interfaces to the PCN port or the COM1/COM2 of the WDM

Connect the external interface client to the PCN port of WDM.

You can use a switch if you have multiple interfaces to connect to the WDM.

Serial interface connection

For serial interface connection, connect a serial cable from the interface client to the serial port on the WDM.

RS-232

For RS-232, select the serial port on which the serial cable is connected as COM1.

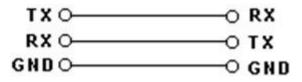


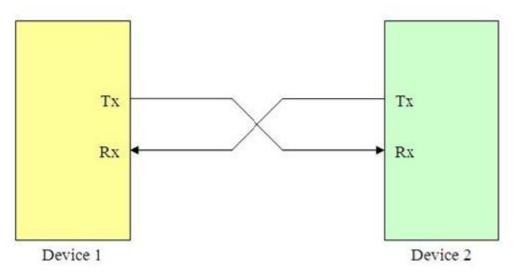
Fig. 16. RS-232

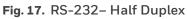
Table. 10.	RS-232 pi	in connection
------------	-----------	---------------

Pin number	Signal Name
1	DCD
2	RXD
3	TXD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI

For R240, the RS-232 – Half Duplex is supported.

RS232-Half Duplex

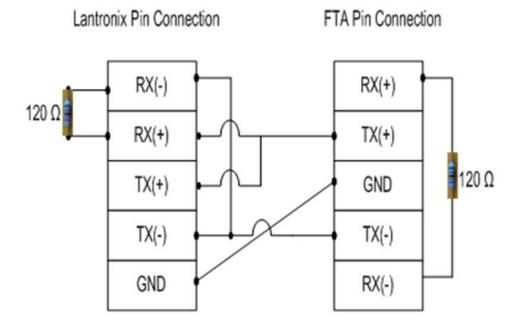




RS-485

The Modbus, HART, and SmartRadar FlexLine (ENRAF) interfaces supports RS-485. For RS-485, select the serial port on which the serial cable is connected as COM2.

Install the Lantronix DeviceInstaller software on the HART client machine using the documentation and media packaged with the device. For more information, see "Install and configure the Lantronix device".



SI FTA Pin Connection

1	RX(+)
2	TX(+)
3	GND
4	TX(-)
5	RX(-)

Fig. 18. Serial pin out diagram - RS-485

Table. 11.	RS-485	pin	connection	WDMX
------------	--------	-----	------------	------

Pin number	Signal Name
1	DATA-
2	DATA+
3	NC
4	NC
5	GND
6	NC
7	NC
8	NC

Table. 12. RS-485 pin connection WDMY

Signal Name Pin number NC 1 NC DataB⁺ 3 DataA⁻ 4 GND 5 NC 6 NC 8 NC

For R240, the RS-485 – Half Duplex is supported.

RS485-Half Duplex

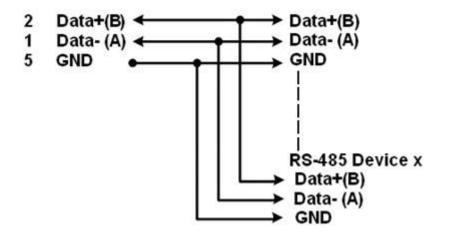


Fig. 19. RS-485 – Half Duplex

Activating HART in OneWireless Network

The ISA100 Wireless field devices maintain a database of process configuration, identification, and diagnostic information in memory. WDM allows accessing this information from asset management systems, such as Field Device Manager (FDM), through a HART interface. This enables monitoring the ISA100 Wireless field devices like any other HART device. OneWireless Network uses serial communication interface to support data transmission between the asset management systems and the WDM.

It also uses Ethernet/UDP interface for data transmission. Ethernet/UDP communication allows users to tunnel serial communication to Ethernet. Serial communication can be tunneled to Ethernet by using a Lantronix device or serial-to-Ethernet/UDP driver on the asset management system.

Configure HART serial interface

To configure HART serial interface:

- 1. Select **EXTERNAL INTERFACES** in the Left Navigation Menu bar.
- 2. Select **HART** and click **NEXT**.
- 3. Click Serial Interface in the Interface list from the Configuration tab.

Configuration Statistics Vendor and Model	Table oon Index Table
Interface	
Interface :	Disabled V
Licensing :	Licensed
Serial Interface Options	
Serial Port :	Сом1 ~
Baud Rate :	9600 ~
Dauu Rate.	
Parity :	None ~
Ethernet Interface Configuration	
Port Configuration :	PCN V
Ethernet/UDP Interface Options	
UDP Port:	55599
HART/IP Interface Options	
TCP Port:	5094
UDP Port:	20001
HART Polling Address Options	
Serial Polling Address :	0
HART/IP Polling Address :	63
HART Log level	
- Log Level:	Low

- 4. Configure the following under **Serial Interface Options**.
 - Serial Port: Select the serial port on which the serial cable is connected. For RS-232, select the serial port as COM1. For RS-485, select the serial port as COM2.
 - Baud Rate: Configure 9600 as the baud rate for HART serial interface.
 - Parity: Configure the parity as Odd.
- 5. In the **Serial Polling Address** box, type the required polling address value. This represents the polling address of the emulated HART MUX on the HART interface.
- 6. Click Apply.
- 7. Expand Vendor and Model Table tab.

The Vendor and Model Table is used to configure mapping between ISA100 Wireless vendor and model strings with HART manufacturer ID and device type bytes. This mapping is required for native ISA100 Wireless devices functioning as HART devices. The HART protocol uses a manufacturer ID byte and device type byte when identifying a device. This table is used to configure a lookup table that maps the ISA100 Wireless vendor and model strings with HART manufacturer ID and the device type bytes. The Vendor and Model Table contains the following columns.

- **Vendor String**: The ISA100 Wireless vendor string of the native ISA100 Wireless device.
- **Model String**: The ISA100 Wireless model string of the native ISA100 Wireless device.
- **Manufacturer ID**: The HART manufacturer ID byte used to represent the native ISA100 Wireless device.
- **Device Type**: The HART device type byte used to represent the native ISA100 Wireless device.

The Vendor and Model Table is pre-configured for Honeywell field devices. No configuration is required if your device vendor and model is pre-configured. Native HART devices connected using the OneWireless Adapter do not use the Vendor and Model Table.

Configure HART Ethernet/UDP interface

You can configure HART Ethernet/UDP interface by using a Lantronix device or a serial-to-Ethernet/UDP driver. Following are the high-level tasks to be performed for configuring the HART Ethernet/UDP interface using a Lantronix device.

- Install and configure the Lantronix device.
- Assign an IP address to the Lantronix device.
- Install the Standard Serial Tunnel firmware on the Lantronix device.
- Configure the Standard Serial Tunnel firmware settings on the Lantronix device.
- Activate HART Ethernet/UDP interface on the OneWireless user interface.

Install and configure the Lantronix device

Install the Lantronix Device Installer software on the HART client machine using the documentation and media packaged with the device. After installing the DeviceInstaller software, perform the following tasks to configure it.

- Assign an IP address to the Lantronix device.
- Install Standard Serial Tunnel firmware on the Lantronix device.
- Configure the Standard Serial Tunnel firmware settings on the Lantronix device.

Assign IP address to the Lantronix device

Perform the following steps to assign or reassign an IP address to the Lantronix device.

To assign or reassign an IP address to the Lantronix device:

- 1. From the Start menu, open Lantronix DeviceInstaller.
- 2. Click Device > Assign IP Address.

- 3. When prompted for device identification, enter the MAC address of the Lantronix device and click **Next**. The MAC address is located on a sticker on the side of the device.
- 4. When prompted for the assignment method, choose **Assign a specific IP address to assign a static IP address to the Lantronix device** and click **Next**.
- 5. Enter the IP address, subnet mask, and default gateway for the Lantronix device and click **Next**.
- 6. Click Assign.

The device now uses the new IP address and has network access.

Install Standard Serial Tunnel firmware on the Lantronix device

The Xpress-DR-IAP Device Server supports different protocols using different firmware images installed on the device. Perform the following procedure to install the Standard Serial Tunnel firmware on the device.

To install the Standard Serial Tunnel firmware on the Lantronix device:

- 1. From the Start menu, open Lantronix DeviceInstaller.
- 2. In the Lantronix Devices tree on the left pane, select Lantronix Xpress-DR-IAP device name.
- 3. Do one of the following:
 - On the menu bar, click **Device** > **Upgrade**.

Or

- Click the **Upgrade** icon on the toolbar.
- 4. To select the firmware files, click Create a custom installation option and click Next.
- 5. Browse and select the firmware file available for Standard Serial Tunnel protocol and click **Next**.
- 6. If there are no additional firmware files to install, select **No other files to install** option and click **Next**.
- 7. If you want to save this installation for a later use, select **Save Installation**.
- 8. To start firmware upgrade, click **Next**.

Configure Standard Serial Tunnel settings on the Lantronix device

Configure Standard Serial Tunnel firmware to enable it to properly tunnel HART messages from the RS-232 serial port to the Ethernet port of the WDM.

To configure Standard Serial Tunnel settings on the Lantronix device:

1. From the Start menu, open Lantronix DeviceInstaller.

- 2. In the Lantronix Devices tree on the left pane, select Lantronix Xpress-DR-IAP device name.
- 3. On the **Telnet Configuration** tab, click **Connect**.
- 4. When prompted, press **Enter** to go to the setup mode.
- 5. On the Main menu, press 1 on the keyboard to configure channel 1 and set the configuration parameters as follows:
 - Baud Rate = 9600
 - I/F Mode = 5C
 - Flow = 00
 - Port Number = 34568
 - Connect Mode = CC
 - Datagram Mode = 01
 - Remote IP Address = IP Address of the WDM
 - Remote Port = 55599
 - Packet Control = 00
 - Send Character 1 = 00
 - Send Character 2 = 00
- 6. Click **Save**.
- 7. Press **9** on the keyboard, to save and exit the **Lantronix** main menu.

Configure HART/IP interface

To configure HART serial interface:

- 1. Select **EXTERNAL INTERFACES** in the Left Navigation Menu bar.
- 2. Select **HART** and click **NEXT**.
- 3. Click HART/IP TCP Interface in the Interface list from the Configuration tab.

Configuration Statistics Vendor and Mo	del Table – Loop Index Table
Interface	
Interface :	HART/IP TCP Interface V
Licensing :	Licensed
Serial Interface Options	
Serial Port:	сом1 ~
Baud Rate :	9600 ~
Parity :	Odd ~
Ethernet Interface Configuration	
Port Configuration :	PCN ~
Ethernet/UDP Interface Options	
UDP Port :	55599
HART/IP Interface Options	
TCP Port:	5094
UDP Port:	20001
HART Polling Address Options	
Serial Polling Address :	10
HART/IP Polling Address :	63
HART Log level	
Log Level :	Low V

- 4. Configure the following under **Serial Interface Options**.
 - Serial Port: Select the serial port on which the serial cable is connected. For RS-232, select the serial port as COM1. For RS-485, select the serial port as COM2.
 - Baud Rate: Configure 9600 as the baud rate for HART serial interface.
 - **Parity:** Configure the parity as **Odd**.
- 5. Under **Ethernet Interface Configuration**, in the **Ethernet Interface** list, click the required option. The following are the interface options available.
 - FDN
 - PCN
 - SIN
- Note: The HART/IP TCP and HART/IP UDP are functional only on the enabled Interface

port.

- 6. In the **Serial Polling Address** box, type the required polling address value. This represents the polling address of the emulated HART MUX on the HART interface.
- 7. Click Apply.

Monitor performance of HART interface

To monitor performance of HART interface:

- 1. Select EXTERNAL INTERFACES in the Left Navigation Menu bar.
- 2. Select **HART** and click **NEXT**.
- 3. Click **Statistics** tab.

Configuration Statistics		
Serial Interface ———		
Message Rate :	0.000000	msg/sec
Message Rate Max :	0.000000	msg/sec
Ethernet/UDP Interface		
Message Rate :	0.000000	msg/sec
Message Rate Max :	0.000000	msg/sec
HART/IP Interface ——		
Message Rate :	0.000000	msg/sec
Message Rate Max :	0.000000	msg/sec
RESET STATISTICS		

- 4. Verify the following attributes to monitor the performance of the HART interface.
 - **Message Rate**: Number of messages processed by the interface, per second.
 - **Message Rate Max**: Maximum number of messages processed by the interface, per second.
 - **Reset Statistics:** Resets all HART interface statistics.

Monitor field devices from an asset management system

FDM supports both ISA100 Wireless and WirelessHART device templates using DD files. FDM communicates with ISA100 wireless devices using GCI interface. FDM communicates with OWA/HART devices using HART/IP interface.

Integration with FDM	Licenses to be enabled in WDM
ISA100 Wireless only	GCI

Integration with FDM	Licenses to be enabled in WDM
ISA100 Wireless and wired HART device connected through OWA	GCI+HART
WirelessHART only	WirelessHART
Both ISA100 Wireless and WirelessHART integration	GCI + HART + WirelessHART

The following procedure describes the steps to access the field devices using FDM. The steps in this procedure provide only an overview of the tasks that you need to perform. For detailed information on the tasks that you need to perform using FDM, see the FDM user documentation.

GCI and HART Interface licenses must be enabled in WDM for FDM to detect the wired HART devices connected to OW Adapter.

To access the field devices using FDM via Serial Interface:

- Log on to the FDM server and configure the following using the FDM Server Management Tool.
 - a. Configure RS-485 HART Multiplexer for enabling communication between HART client and the wireless field devices.
 - b. Configure the Network Interface Name and Remote Communication Interface Server Name.
- 2. Configure the following network specific parameters.
 - COM Port: COM port on the WDM to which the serial cable is connected.
 - BAUD Rate: 9600
 - Start Poll Address and End Poll Address: 0 to 127
- 3. Start the FDM server using the FDM Server Management Tool.
- Log on to the FDM Client and scan for the field devices. Once the FDM Client scans the devices, the WDM and the devices appear on the FDM Client as shown in the following illustration.

0 🕒 🗗 🔁 🖋	Search Device:	Advanced Searc
Online View		
Display Filter		
No Filter Apply		
Network View Device State View		
End Server (OWFDM)		
📥 💼 OWFDM		
📥 🥽 WDM_ISA10011a		
UIOD_533		
SS3_HL_C3		
Unhealthy devices		
⊥ Disconnected Nodes		
2 PD_497		

5. For accessing the field device parameters, add DD files for the field devices. After accessing the parameters, the HART Client displays the device details as follows.

0 🕞 🕞 🖴 🛃 🍠	Search Device: O Advanced Search
O <u>n</u> line View	CD 474
Display Filter No Filter Apply	Entry Points Device Setup
Network View Device State View □ Image: State View Image: State View Image: State View	Radio UAPMO CH01_AI_CORROSION

Configuring FDM for HART-IP network

FDM supports HART-IP networks and connected devices, including the Honeywell RTU2020 controller. Before using FDM with any HART-IP connected device, it is recommended (but not necessary) that the devices are commissioned first. Once

commissioned, the HART-IP network can be configured using the FDM Server Management tool. To configure a HART-IP network, you must specify the IP address range of all connected devices in that network. The Build Network operation is used for discovering all controllers and available HART devices.

Prerequisites

- Ensure that all HART-IP connected devices are commissioned.
- Ensure to enable the HART-IP interface from the HART-IP connected devices.

To configure the HART-IP network

- On the FDM Server computer, click Start > All Programs > Honeywell FDM > FDM Server Management Tool.
- 2. Log on to the FDM Server Management Tool. The **FDM Server Management** dialog box appears.
- 3. In the left pane, click **Network Configurator**. The **Network Configuration** page appears.
- 4. Click Add New to add a new network. The Add Network page appears.
- 5. In the Network Type drop-down list, click HART-IP Network.
- 6. Under IP Address Configuration,
 - If you want to configure a HART-IP connected device (example, RTU2020), then click Add IP and type the IP address.
 - If you want to configure multiple HART-IP connected devices (example, RTU2020 nodes) at a time, click Add IP Range(s) and enter the range of IP addresses for those devices.
- 7. In the Port No box, default port number is displayed as 5094 from the RTU2020. If the different port number is set in the RTU2020, you need to enter that port number in this box.
- 8. Click Add IP.

The specified IP address appears under HART-IP Configuration.

If you want to change the IP address or to delete the existing IP address, click Delete IP. The IP address is deleted under HART-IP Configuration and you can enter the new IP address.

9. Type the name of the RCI Server in **RCI Server Name** box. The configured network is connected to the RCI Server.



By default, FDM populates RCI Server Name with LOCALHOST. If you do not change this, FDM considers the local host as the RCI Server.

10. Click **OK**.

Activating Modbus in OneWireless Network

Using any Modbus application, you can read any standard measurement or status of field devices. The WDM functions as the Modbus server and allow clients to access point data. The Modbus interface within the WDM supports Modbus TCP and Modbus RTU. Modbus interface supports coils, discrete inputs, holding registers, or input registers. It can associate only standard measurement and status of field device within the network with a coil, discrete input, holding register, or input register.

The coil and discrete input are used for digital input and output SIGNALS/VALUES. The holding register and input register are used for analog input SIGNALS/VALUES.

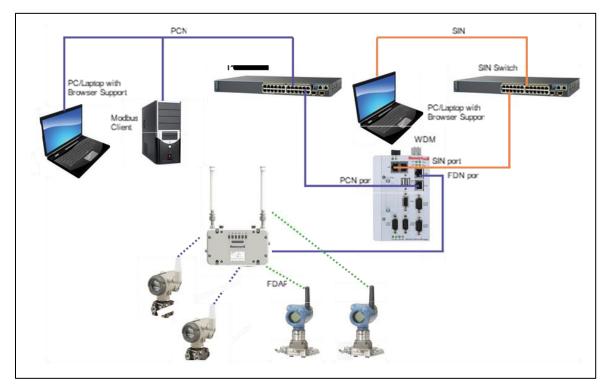


Fig. 20. Modbus TCP communication

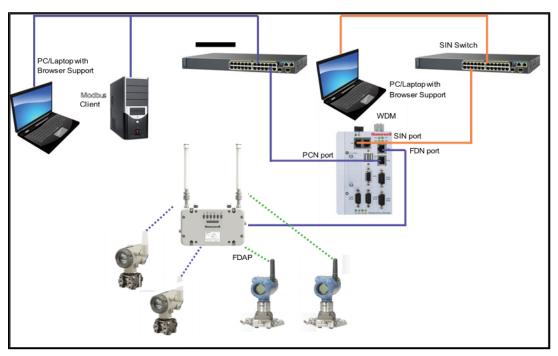


Fig. 21. Modbus RTU communication

Enable Modbus in OneWireless Network

Prerequisites

• Ensure that you have installed the Modbus client.

To enable Modbus in OneWireless Network:

- 1. Select **EXTERNAL INTERFACES** in the Left Navigation Menu bar.
- 2. Select **MODBUS** and click **NEXT**.
- 3. Click the required option in the **Interface** list under **Interface** from the **Configuration** tab.

The following are the available interface options.

- Modbus TCP Interface
- Modbus RTU Interface

MODBUS	
Configuration Statistics Coil Table Discrete I	
r Interface	Modbus TCP Interface V
Interface :	wooduda i Ce internace
Licensing :	Licensed
Modbus RTU Options	
Serial Port:	СОМ1 У
Baud Rate :	9600 ~
Parity :	None
Serial Unit ID/Address :	1
Ethernet Interface Configuration	
Port Configuration :	PCN ✓
Modbus TCP Options	
TCP Port:	502
r Byte Order	
Byte Order :	Big Endian V
Unconfigured Register Response	
Read Response :	Zero ~
With Bernand L	Ignare V
Write Response :	
Read Register Error Response	
Float Error Response :	NaN
Float Error Value :	0.000000
Integer Error Response :	Zero 🗸
Integer Error Response Value :	0
Modbus Log level	
Log Level :	Low

4. 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 Options**.
- TCP Port: The TCP port number used for the configuring the Modbus TCP interface.
- If you have selected **Modbus RTU Interface**, configure the following under **Modbus RTU Options**.
- Serial Port: The serial port used for the Modbus RTU interface. The available options are COM1 and COM2. For RS-232, select the serial port as COM1. For RS-485, select the serial port as COM2.
- Baud Rate: The baud rate used for the Modbus RTU serial port.
- **Parity**: The parity used for the Modbus RTU serial port.
- Serial Address: The serial address used for the Modbus RTU serial port. The serial address may be referred to as the unit ID in your MODBUS client.
- 5. Under **Byte Order**, in the **Byte Order** list, click the byte order for 32-bit holding register and input register values.

You must select a byte order that matches the expected byte order of the Modbus client. Options include **Big Endian, Big Endian Byte Swapped, Little Endian, and Little Endian Byte Swapped.**

6. Under Unconfigured Register Response, click Read Response and Write Response.

If you select the Read Response as "Zero", for unmapped registers the Modbus client displays zero. If you select Read Response as "Illegal Exception", then the server sends an exception response and returns no values.

- 7. Configure the following under **Read Register Error Response**.
 - Float Error Response
 - Float Error Value
 - Integer Error Response
 - Integer Error Response Value

If you have selected the Float Error Response as NAN and if the floating PV is not available, then the client displays "NAN".

If you have selected the **Float Error Response** as **Float Error value** and input any value in the **Float Error Value**, it displays the float error value in the client when the floating PV is not available in the client.

If you select the **Integer Error Response** as **Zero** and if the integer PV is not available, then the client displays "Zero".

If you have selected the **Integer Error Response** as **Integer Error value** and input any value in **Integer Error Response Value**, it displays the integer error value in the client when the Integer PV is not available in the client.

- Using the Coil Table, Discrete Input Table, Holding Register Table, and Input Register Table panels, you can configure standard measurement like PV or status of field devices.
 - **Coil Table** and **Discrete Input Table**: These two registers are used to configure the input/output and the status of the Boolean modules as well as the status of the analog devices.

MODBL	JS			
	ation Statistics Coil Table Discret			
S		Point Picker Point Picker enables you to browser parame		the second second second second second
COIL	ATTRIBUTE	Modules table.	ters on all devices and then comig	ure the parameters in the
	TD_111_3CLL_PCT.CH01	Search by device Q		how Sensor Parameters 📔 🌫
	TD_03_3S2.CH01_ALPV	SELECT DEVICE OR CHANNEL	SELECT ATTRIBUTE	
	TD_03_3S2.CH02_BLPV_B	V FCT2_vWDM_Pri	AVAILABILITY	Ø
		T04084FFFF22D098	AVAILABILITYSTAR	T
	TD_03_3S2.CH03_BI.PV_B	T04084FFFF22D099	BACKWARD COMP	
4		Showing 3037 Devices		
		BA	ICK RESET	APPLY

Fig. 22. Coil Table

Configurati	on Statistics Coil Table	Discrete Input Tabl	e Holding Register Table	Input Register Table	Alarms(0)	
S						
REGISTER	ATTRIBUTE					
0	FCT2_vWDM_Pri.CHANNE		▶			
1	FCT2_vWDM_Pri.GATEWA					
2						
3						
4						
				ВАСК	RESET	APPLY

Fig. 23. Discrete Input Table Table

• Holding Register Table and Input Register Table: These two registers are used to configure the input of the analog modules and Diag status of the device.

For an Analog input module, you must configure the PV and PV Status as follows:

• PV - TAGNAME.CHANNELNAME.PV

After configuring PV in Modbus registers in the user interface, the PV data starts appearing in the Modbus client. The PV value for a device received at the client is in

decimal or hexadecimal format and is displayed in two adjacent registers in the Modbus client.

- If the PV value received is in the hexadecimal format, you need to convert the data in to a float value to read the PV value as displayed in the user interface.
- If the PV value received is in the decimal format, you need to convert the data in to hexadecimal and then to a float value to read the PV value as displayed in the user interface.
- PV STATUS TAGNAME.CHANNELNAME.PV_B.STATUS

Note the following while configuring a Boolean module.

- For a Boolean input module, you must configure the PV and PV Status as follows:

 - PV STATUS TAGNAME.CHANNELNAME.PV_B.STATUS
- For a Boolean output module, you must configure the PV and PV Status as follows:
 - PV TAGNAME.CHANNELNAME.OP_B
 - PV STATUS TAGNAME.CHANNELNAME.OP_B.STATUS

Similarly, you can configure the device status as TAGNAME.DIAG_STATUS.

After configuring DIAG_STATUS in Modbus registers in the user interface, the DIAG_STATUS data starts appearing in the Modbus client. The DIAG_STATUS data received at the client is in decimal or hexadecimal format and is displayed in two adjacent registers in the Modbus client.

- If the data received is in the hexadecimal format, you need to convert the data in to binary format and then map each bit of the binary data to diag_status bits.
- If the data received is in the decimal format, you need to convert the data in to binary format and then map each bit of the binary data to diag_status bits.

Use the following table as a reference to map the binary data received in the Modbus client.

Diagnostic status detail	Bits	Diagnostic status detail	Bits
FAILURE_STATUS	BIT31	WCI_RESERVED_15	BIT15
FUNCTION_CHECK_STATUS	ВІТЗО	WCI_RESERVED_14	BIT14
OUT_OF_SPEC_STATUS	BIT29	WCI_RESERVED_13	BIT13
MAINTENANCE_REQD	BIT28	WCI_RESERVED_12	BIT12
FAULT_IN_ELECTRONICS	BIT27	WCI_RESERVED_11	BIT11
FAULT_IN_SENSOR_ACTUATO	BIT26	WCI_RESERVED_10	BIT10
INSTALLATION_CALIBRATION _ PROBLEM	BIT25	WCI_RESERVED_9	BIT9
OUT_OF_SERVICE	BIT24	WCI_RESERVED_8	BIT8
OUTSIDE_SENSOR_LIMITS	BIT23	DATABASE_ERROR	BIT7

Table. 13. DIAG_STATUS for all XYR 6000 field device types

ENVIRON_CONDITIONS_OUT	BIT22	RADIO_IPC_ERROR	BIT6
_O F_SPEC			
FAULT_PREDICTED	BIT21	HEAP_ERROR	BIT5
POWER_CRITICALLY_LOW	BIT20	DEVICE_FIRMWARE_MISMATCH	BIT4
POWER_LOW	BIT19	WATCHDOG_ERROR	BIT3
SOFTWARE_UPDATE_INCOM	BIT18	OUTPUT_AT_FAILSAFE	BIT2
PL ETE			
SIMULATION_ACTIVE	BIT17	FW_DOWNLOAD_ERROR	BIT1
WCI_RESERVED_16	BIT16	DETAIL_INFO_AVAILABLE	віто

You can read device vendor parameters (DEVICE_TAG.DIAG_STATUS_DETAIL_1) from Modbus client.

Use the following table as a reference to interpret the data received in the Modbus client.

Table. 14. DIAG_STATUS_DETAIL_1 for XYR 6000 temperature/Temp DI/Multi DI/HLAI

d	evices	
^u	CVICCS	

Diagnostic status detail	Bits	Diagnostic status detail	Bits
DEV_ST_ELEC_FAIL	BITO	DEV_ST_NVM_FAULT	BIT18
DEV_ST_INPUT_FAIL	BIT2	DEV_ST_AD_FAULT	BIT19
DEV_ST_LOW_BAT	BIT4	DEV_ST_INPUT_FAIL1	BIT21
DEV_ST_STACK_ERR	BIT5	DEV_ST_INPUT_FAIL2	BIT22
DEV_ST_CONF_ERR	BIT6	DEV_ST_INPUT_FAIL3	BIT23
DEV_ST_CAL_ERR	BIT7	DEV_ST_SUSP_IP1	BIT24
DEV_ST_RADIO_ERR	BIT8	DEV_ST_SUSP_IP2	BIT25
DEV_ST_WDT_ERR	BIT11	DEV_ST_SUSP_IP3	BIT26
DEV_ST_LOW_EXT_PWR	BIT12	DEV_ST_CAL_ERR1	BIT27
DEV_ST_FAILSTATE	BIT13	DEV_ST_CAL_ERR2	BIT28
DEV_ST_ROM_FAULT	BIT16ba	DEV_ST_CAL_ERR3	
DEV_ST_RAM_FAULT	BIT17		

Table. 15. DIAG_STATUS_DETAIL_1 for XYR 6000 corrosion devices

Diagnostic status detail	Bits	Diagnostic status detail	Bits
DEV_ST_ELEC_FAIL	BITO	DEV_ST_RAM_FAULT	BIT17
DEV_ST_INPUT_FAIL	BIT2	DEV_ST_NVM_FAULT	BIT18
DEV_ST_LOW_BAT	BIT4	DEV_ST_AD_FAULT	BIT19
DEV_ST_STACK_ERR	BIT5	DEV_ST_SHORT_PROBE	BIT20
DEV_ST_CONF_ERR	BIT6	DEV_ST_OPEN_PROBE	BIT21
DEV_ST_CAL_ERR1	BIT7	DEV_ST_EXCESS_CAL	BIT24
DEV_ST_RADIO_ERR	BIT8	DEV_ST_HDM_NOT_PO	BIT25
DEV_ST_HEAP_ERR	BIT9	DEV_ST_ASM_RESPONSE	BIT26
DEV_ST_IPC_ERR	BIT10	DEV_ST_DAC_ERROR	BIT27
DEV_ST_WDT_ERR	BIT11	DEV_ST_CAL_CLEAR	BIT28
DEV_ST_LOW_EXT_PWR	BIT12	DEV_ST_CJ_FAULT	BIT31
DEV_ST_ROM_FAULT	BIT16		

Table. 16. DIAG_STATUS_DETAIL_1 for XYR 6000 pressure devices

Diagnostic status detail	Bits	Diagnostic status detail	Bits
DEV_ST_ELEC_FAIL	BITO	DEV_ST_ROM_FAULT	BIT16
DEV_ST_INPUT_FAIL	BIT2	DEV_ST_RAM_FAULT	BIT17
DEV_ST_LOW_BAT	BIT4	DEV_ST_NVM_FAULT	BIT18
DEV_ST_EXT_PWR	BIT5	DEV_ST_AD_FAULT	BIT19
DEV_ST_CONF_ERR	BIT6	DEV_ST_CHAR_FAULT	BIT20
DEV_ST_CAL_ERR	BIT7	DEV_ST_MB_OVT	BIT24
DEV_ST_RADIO_ERR	BIT8	DEV_ST_MB_OVL	BIT25
DEV_ST_HEAP_ERR	BIT9	DEV_ST_EXCESS_ZERO	BIT26

Diagnostic status detail	Bits	Diagnostic status detail	Bits
DEV_ST_IPC_ERR	BIT10	DEV_ST_EXCESS_SPAN	BIT27
DEV_ST_WDT_ERR	BIT11	DEV_ST_EXCESS_CAL	BIT28
DEV_ST_LOW_EXT_PWR	BIT12	DEV_ST_CAL_CLEARED	BIT29
DEV_ST_STACK_ERR	BIT15		

Table. 17. DIAG_STATUS_DETAIL_1 for XYR 6000 Multi AI DI/Multi AI DI DO devices

Diagnostic status detail	Bits	Diagnostic status detail	Bits
DEV_ST_ELEC_FAIL	віто	DEV_ST_RAM_FAULT	BIT17
DEV_ST_INPUT_FAIL	BIT2	DEV_ST_NVM_FAULT	BIT18
DEV_ST_LOW_BAT	BIT4	DEV_ST_AD_FAULT	BIT19
DEV_ST_STACK_ERR	BIT5	DEV_ST_INPUT_FAIL1	BIT21
DEV_ST_CONF_ERR	BIT6	DEV_ST_INPUT_FAIL2	BIT22
DEV_ST_CAL_ERR	BIT7	DEV_ST_INPUT_FAIL3	BIT23
DEV_ST_RADIO_ERR	BIT8	DEV_ST_SUSP_IP1	BIT24
DEV_ST_HEAP_ERR	BIT9	DEV_ST_SUSP_IP2	BIT25
DEV_ST_IPC_ERR	BIT10	DEV_ST_SUSP_IP3	BIT26
DEV_ST_WDT_ERR	BIT11	DEV_ST_CAL_ERR1	BIT27
DEV_ST_LOW_EXT_PWR	BIT12	DEV_ST_CAL_ERR2	BIT28
DEV_ST_FAILSTATE	BIT13	DEV_ST_CAL_ERR3	BIT29
DEV_ST_ROM_FAULT	BIT16	DEV_ST_CJ_FAULT	BIT31

Table. 18. DIAG_STATUS_DETAIL_1 for OWA devices

Diagnostic status detail	Bits	Diagnostic status detail	Bits
DEV_ST_ELEC_FAIL	BITO	DEV_ST_FAILSTATE	BIT13
DEV_ST_INPUT_FAIL	BIT2	DEV_ST_ROM_FAULT	BIT16
DEV_ST_LOW_VOLT	BIT3	DEV_ST_RAM_FAULT	BIT17
DEV_ST_LOW_BAT	BIT4	DEV_ST_NVM_FAULT	BIT18
DEV_ST_STACK_ERR	BIT5	DEV_ST_AD_FAULT	BIT19
DEV_ST_CONF_ERR	BIT6	HART_LOOP_ERROR	BIT20
DEV_ST_CAL_ERR	BIT7	NO_HART_DEV	BIT21
DEV_ST_RADIO_ERR	BIT8	HART_DEV_MAINT_REQ	BIT22
DEV_ST_HEAP_ERR	BIT9	HART_DEV_VAR_ALERT	BIT23
DEV_ST_DEV_FW_ERR	BIT10	HART_DEV_BURST_MODE	BIT24
DEV_ST_WDT_ERR	BIT11	DEV_ST_CAL_ERR1	BIT27
DEV_ST_LOW_EXT_PWR	BIT12		

- 9. Expand **Statistics** panel, to monitor the performance of the Modbus interface. Following are parameters available in the **Statistics** panel.
- Under Modbus RTU Interface and Modbus TCP Interface,
 - **Message Count**: Total number of messages processed by the interface. The count must increase with every message sent by a Modbus client. If the count is not incrementing, it indicates that the Modbus interface on the WDM is not receiving messages from the client.
 - **Message Rate**: Number of messages processed by the interface per second.
 - Message Rate Max: Maximum number of messages processed by the interface per second.
 - **CRC Error Count**: Total number of CRC errors recorded by the Modbus RTU interface. The count must increase if any CRC errors are detected when receiving a message sent by the Modbus RTU client.
 - **CRC Error Rate**: Number of CRC errors recorded by the Modbus RTU interface per second.
 - **CRC Error Rate Max**: Maximum number of CRC errors recorded by the Modbus RTU interface per second.
- Under Coils, Discrete Inputs, Holding Registers, Input Registers, and Exceptions,
 - **Read**: Total number of read messages processed by the interface.
 - Write: Total number of write messages processed by the interface.
 - **Exception**: Total number of exceptions, such as invalid request messages.
 - **Timeout**: Total number of timeouts.

Configure the parameters in the Modbus tables

Point Picker enables you to browse parameters on all devices and then configure the parameters in the Modbus tables. You can drag and drop the information into the appropriate table. You can drag from the actual text next to the **Attribute** label, or dragged from the list of **Select Attribute**. You can drag and drop parameter into the Modbus coil or register configuration or copy and paste the parameter into the Modbus coil or register configuration.

To configure the parameters in the Modbus tables:

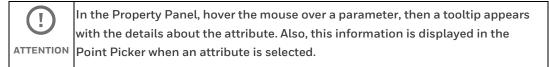
- From the Left Navigation Menu bar, expand Maintenance and click Point Picker. The Point Picker window appears.
- 2. From the **Select Device/Channel** list, select the required device or channel. The corresponding attributes appears under **Select Attribute** list.
- 3. From the **Select Attribute** list, select the required attribute.
- 4. Click Copy.
- 5. Select **EXTERNAL INTERFACES** in the Left Navigation Menu bar.
- 6. Select **MODBUS** and click **NEXT**.
- 7. In the Coil Table, Discrete Input Table, Holding Register Table, or Input Register Table, select the **Attribute** column, and then press Control V (Ctrl +V).

	MODBUS The WOM functions as the Modbus server and allow clients to access point data. Modbus interface supports colls, discrete inputs, holding registers, or input registers.						
	ion Statistics CoilTable Discrete Input Table Holdi						
S		Roint Picker					
COIL	ATTRIBUTE	Point Picker enables you to browser parameters on all device					
	AP_0096.DIV_CORRECTION_GAIN	Search by device Q	Show Sensor Parameters				
	wdm1.AVAILABILITY	SELECT DEVICE OR CHANNEL	SELECT ATTRIBUTE				
	wdm1_AVAILABILITY	✓ wdm1 AP 0096	ATTRIBPOOLMAX				
3	Enter Attribute	LPFR_0041 V EML.64C4A_5FL	ATTRIBPOOLTOTAL				
		✓ CD_475_3F_6FLR	ATTRIBPOOLUSED				
		V TD_1049_7F_5FLR					
		✓ TD_1010_4J_6FLR	AVAILABILITY				
		✓ 3308_GWR_TX	AVAILABILITYSTART				
			AVAILABILITYSTART				
		Showing 9 Devices					
IMF	PORT		BACK RESET APPLY				

8. Alternatively, the Point Picker option is available in the Coil Table, Discrete Input Table, Holding Register Table, or Input Register Table tabs in the **External Interface**.

	The entire set of attributes can be pasted from Excel. Also, you can copy and
<u> </u>	paste it to Excel. This helps you to save all the attributes in the Excel sheet.
ATTENTION	

9. Click Apply.



Import/Export Modbus register configuration

To export Modbus register configuration:

1. From the Left Navigation Menu bar, click **SYSTEM >SOFTWARE DOWNLOAD.** The Support Software window appears.

Software Download
Select Software
Select Software
Provisioning Device Application
OPC-UA Proxy
Modbus Configuration Backup
Secure Communication Software
Android Provisioning Device Application
HART DD To XML Converter

- 2. From the Select Software list, select the Modbus Configuration Backup. Click DOWNLOAD.
- 3. Click GO TO DASHBOARD after downloading the software.

To import Modbus register configuration:

1. From the Left Navigation Menu bar, click **Maintenance > Templates.**

The **Templates** window appears.

Templates Click Load ISAL00DD/Modbus File to select and load a Device	Definition (DD) file or Modbus configuration backup file to the W	reless Device Manager.	
VENDOR	MODEL	DEVICE REVISION	DD FILE REVISION
SPIRAX SARCO	ISA100-STAPS	0003	
GE Energy	70M303	0006	
Yokogawa	FN510 DIDOAI	0001	
🗌 Yokogawa	FN310 HART	0001	
GSC	GS01	0002	
Honeywell	Enraf WFI	0001	
Honeywell	STX800	0001	
Honeywell	FEWIO	0001	
Honeywell	XYR 6000 TempDI	0001	
			DELETE

- 2. Click Load.
- 3. Browse to the directory location of the ISA100 DD/Modbus file.

4. Select the ISA100 DD/Modbus file and click **Open**.

The ISA100 DD/Modbus file is uploaded to the WDM.

Activating OPC in OneWireless Network

WDM hosts an OPC Unified Architecture (UA) server, which provides open system communication to ISA100 Wireless data (current, historical and alarm/event data). OPC UA provides a Service Oriented Architecture (SOA) for industrial applications.

For the OPC-based applications that only support DCOM/COM based OPC (DA), WDM offers an OPC Proxy. OPC Proxy when installed on the client machine enables communication between a DCOM/COM-based OPC client and the WDM.

Several OPC clients are used to connect to the WDM which hosts an OPC server. Honeywell uses Unified Automation UaExpert as the sample client for configuring OPC UA and OPC Validator as the sample client for configuring OPC DA. The procedures to configure an OPC client (for OPC UA and OPC DA) in this document are based on Unified Automation UaExpert and OPC Validator.

Enable OPC interface

To enable OPC interface:

- 1. Select **EXTERNAL INTERFACES** in the Left Navigation Menu bar.
- 2. Select **OPC** and click **NEXT.**
- 3. Click **Enabled** in the Interface list from the **Configuration** tab.
- 4. Click Apply.

Configure OPC UA client system

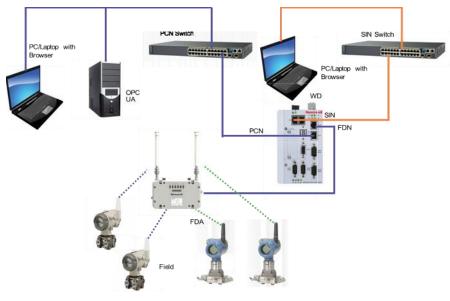


Fig. 24. OPC Interface

Prerequisites

• Install Microsoft .NET Framework 3.5 SP1 and OPC UaExpert Client in the client system.

To configure OPC UA client system:

1. On the desktop of the client system, double-click **Unified Automation UaExpert** icon. The **Unified Automation UaExpert** window appears.

🖉 Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject						
File Server Document Settings Help						
Project	₽×	Default DA View		Θ	Attribute Window	₽×
🖻 📁 🃁 Project		Server	Noce Id	Display	9	
🗁 💋 Servers					Attribute Value	
🖨 🃁 Documents					Attribute	
🛄 📁 📁 Default DA View						
Address Space	8×					
					Reference Window	5×
					😏 🥪 🏭 🏶 Forward 💌	
					Reference Target DisplayName	
		<		>		
Log Window						₽×
🗱 🕞						
		ready to use.				~
		renceplugin.dll.				1
		hodplugin.dll.				=
		oryplugin.dll. ntplugin.dll.				
		icesplugin.dll.				_
	ided dev					~

- On the Server menu, click Add to add the OPC server to be connected to the client. The Add Server dialog box appears.
- 3. Type the Configuration Name.

figur	ation Name
iscov	ery Advanced
Τ.	
• (Remote Couble click to Add Server >
G	- Q opc.tcp://wdm1:4840
	🖨 👰 opcuasrv-x86@wdm1
	🚆 None - None
	Basic128Rsa15 - Sign & Encrypt
	Basic256 - <u>Sion & Encrynt</u> Becently Used opc.tcp://wdm1:4840
🛨 ''' 🗸	
Auth	
Auth	Anonymous
	entication Settings
	Anonymous
•	entication Settings
•	Anonymous
•	Anonymous Username Password Store
 ○ ○ 	Anonymous Username Password Certificate Currently not supported by UaExpert
 ○ ○ 	Anonymous Username Password Store

- 4. Click the **Discovery** tab to view all the available servers. There is only one OPC UA server available for a WDM, and its port number is 4840.
- 5. Click the **Advanced** tab and then type the IP address of the WDM and the port number in the Endpoint URL field.

The OPC server IP address with port number is opc.tcp://WDM IP address: 4840. For example, if the WDM IP address is 192.168.1.1, then type, opc.tcp://192.168.1.1:4840.

- 6. Under Security Settings, ensure that Security Policy and Message Security Mode are selected as None. There is only one OPC UA server available for a WDM, but with multiple security modes. Multiple levels of security are allowed in configuring the OPC UA connection to the server.
- 7. Under Authentication Settings, click Anonymous.
- 8. Select the **Connect Automatically** check box.

Add 9	Server ? 🖻
onfigur	ation Name R200_OWserver
Discov	very Advanced
-Serv	er Information
Endp	opint Url opc.tcp://192.160.0.1:4040
Secu	irity Settings
Secu	urity Policy None 🗸
Mes:	sage Security Mode None 🗸
Auth	entication Settings
۲	Anonymous
	Username
0	Password Store
	Certificate Currently not supported by UaExpert
Conr	ect Automatically
	OK Cancel

9. Click **OK** and the server automatically connects.

The OPC server appears as connected under **Projects** > **Servers**.

10. Under **Projects**, expand **Project** > **Server** and select the added server.

🧮 Unified Autom	ation UaExpert	- The OP	C Unified Archite	ecture Client - N	ewPro je	ct*		
File Server Docu	iment Settings	Help						
i D 🥔 🖯 I	10 🛛	— Ø	🗙 🔦 🛛					
Project		₽×	Default DA View		Θ	Attribute Window		đΧ
🖻 📶 Project			Server	Node Id	Display	90		
🖻 🗂 Servers			berver	NODE IO	Dispiay		1.12	1029
R200	LOW					Attribute	Value	1
🖻 🎵 Documen						🕀 NodeId	Nodeld	
	ult DA View					Namespa	2	
Dera	UICDA VIEW					Identifier		
						Identifier NodeClass	ID_122 Object	
						BrowseName	2, "ID 122"	
						DisplayName	"" "ID 122"	
						Description	"", "ID_122" "", "ID_122"	
						WriteMask	0	
Address Space		₽×					0	V
C Root						Reference Window		đΧ
🖨 🛅 Objects								0 A
🕀 🚕 ID_122						😏 🧹 品 🐵 🛛	Forward 🔽	
🕀 🚕 MNBBR_B	33					Reference	Target DisplayName	^
🕀 🍰 53-TD-08						and the second se	and a second descent of the second	
🕀 🍰 53_MD_0	17					HasComponent HasComponent	CH01_AI CH02 BI	
🕀 🂑 53_TE_0:						HasComponent	CH02_BI	
B Server	•					HasComponent	CTS VERSION	
						HasComponent	DEVICE_ROLE_CAPABILI	TV
😟 🚕 wdm1						HasComponent	DIAG STATUS	
🕀 🧰 Types						HasComponent	DIAG STATUS DETAIL 1	
🗄 🫅 Views			<		2	HasComponent	DL_A.IAS_16_BIT	v
1 Sectored and						HacComponent	DLMG CHANNEL DIAG	
Log Window								₽×
😫 🕞								
	ypeCache		e = ComponentOf					~
	ypeCache		has bad statuscode:					
	ypeCache		e = 0:HasComponen					
	ypeCache		sions has bad status					
	ypeCache		as bad statuscode: 0					
	ypeCache		has bad statuscode:	0x80350000				~
16:25:25.562 T	ypeCache	DisplayNam	e = HasComponent					

11. To monitor the PV value of any field device,

- 12. In the Address Space pane, under Root expand Objects > Transmitter > Transmitter Channel.
- 13. Click **PV**.

The selected PV attributes appear in the Attribute Window pane.

🚟 Unified Automation UaExpert	- The OP	C Unified Archite	ecture Client - N	ewProje	ect*	
File Server Document Settings	Help					
🗋 🥔 🕞 🔀 💽 🜩	- Q	🛛 🗙 🔌 🛛 🖬) 🛛 🖉			
Project	5×	Default DA View		0	Attribute Window	8×
🖻 🗊 Project		Server	Node Id	Display	9	
🖨 📁 Servers		R200-OW	53 MD 07.CH01		Attribute Value	~
🖳 🚫 R200-OW					Attribute Value	
🖻 📁 Documents					- BrowseName 2, "PV"	
🔤 📁 📁 Default DA View					DisplayName "", "PV"	
					Description "", "Process Value"	
					WriteMask 0 UserWriteMask 0	
					Value 22,9781	
					DataType Float	
Address Cases					- Namespa 0	
Address Space	5×				Identifier Numeric	~
🖨 💑 CH01_AI_1_Temperatur	reDI 🖄				Reference Window	đ×
BREAK_DETECT						6 4
CAL_CMD					😏 🥪 🏭 🏶 Forward 💌	
🕀 🎯 CAL_POINT_HI					Reference Target DisplayName	
CAL_STATUS						
CAL_UNIT						
	NT					
De MODE						
	~	<		>		
Log Window						Β×
🗱 🕞						
16:26:22.828 DA Plugin				eueSize=1	, MonitoredItemId=1	~
16:26:22.828 DA Plugin		itoredItems succeede				_
16:26:22.828 DA Plugin		amplingInterval=-1, Q				
16:26:22.828 DA Plugin 16:26:22.828 DA Plugin		ues: Lirei imeCount=6 scription succeeded.	и, махкеернімесоц	INC=5, Pric	ority=0, PublishingInterval=1000	
16:26:22:828 DA Plugin			Handle=0. Publishing	Fnable=1	, LifeTimeCount=60, MaxKeepAliveCount=5	i. Pri
16:26:22.828 DA Plugin		ion for ServerId 0	riancio oj riabilorning	,6113610 1	jeronnocoane ooj naxeoop intocoane e	·) · · · · · · · · · · · · · · · · · ·

14. Drag any parameter from the **Address Space** pane to the **Default DA View** to increase the load of the network.

The OPC Statistics pane in the OneWireless user interface displays the following information about the loaded parameters.

- **Subscription Rate**: Current rate of OPC subscriptions/attributes/data points that the WDM provides every second. This must be less than or equal to 500 attributes per second.
- **Subscription Rate Max**: Maximum rate of OPC subscriptions/attributes/data points that the WDM provides in a second since OPC statistics reset due to WDM reboot. This can have a higher value because while launching the OPC client, the data rate might increase considerably.

Configure OPC DA client system

You can setup OPC proxies on a client machine so that an OPC DA client (a non-UA client) can connect to the OPC UA server on the WDM. The proxy files are available on the WDM.

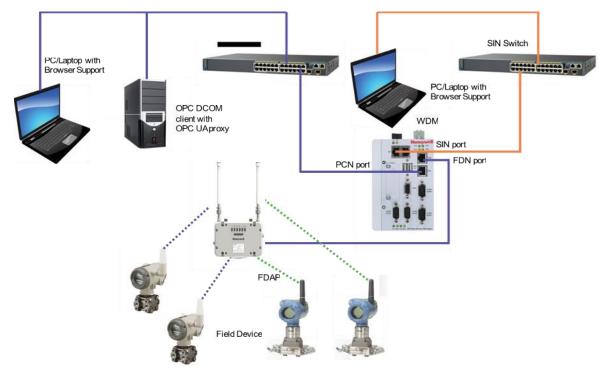


Fig. 25. OPC client with OPC DA

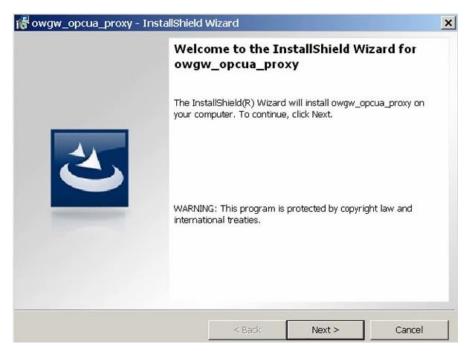
Prerequisites

- Connect the OPC DA client system to a switch or to a system connected to the PCN.
- Install the OPC Validator Client in the client system.

Install OPC proxies

- From the Left Navigation Menu bar, click SYSTEM > SOFTWARE DOWNLOAD. The Support Software window appears
- 2. From the **Select Software** list, select the **OPC UA Proxy** software.
- 3. Click **Download** to download the software to the computer.
- 4. Open the installer and click **Run**.

The InstallShield wizard appears.



- 5. Click **Next** to proceed with the installation. The **License Agreement** page appears.
- 6. Click I accept the terms in the license agreement and click Next. The Customer Information page appears.
- 7. Enter the **User Name** and **Organization** and click **Next**. The **Setup Type** page appears.
- 8. Click **Complete** and then click **Next**. The **Ready to Install the Program** page appears.
- 9. Click **Install** and click **Next** to proceed with the installation. The **OPC Gateway Server Host IP Address** page appears.
- 10. Type the OPC Gateway Server Host IP Address (WDM's IP Address) and click Next. The **OPC Gateway Server tcp Port** page appears.
- 11. Type the **TCP Port Value** as 4840 and then click **Next**. The **InstallShield Wizard Completed** page appears.
- 12. Click **Finish** to load the OPC proxies.

Access WDM using OPC DA

On the desktop of the client system, double-click OPC Validator icon. The OPC Validator window appears.

ACS	No Sci	ript - OF	C Vali	dator																							1			×
		Servers			ige	Alarms	Histori	ical	Batch	Va	lidate	Scr	ipt	Log	Tools	Hel	P										U			
8	В.	F F			7	• G	Ø C	76	7 C	e	e	卽	¢	¢	(]	2	-	ar i	VT	+	all i	-	ų!	닅	÷		4		E	ę
٦		3 G 6																												
																														_
				W	orksp	oace -						ſ	Ta	igs -	All		Alarr	ns	Т	Hist	orical		Bro	owse		Vali	date			-
<u> </u>					_			_					_					_	_	_	_		_	_		_		_	_	-
	Dutput	Sa	ipt	ScriptC	out	Lo	g	St	atus		Spec	c	Ţ	est C	ase															
For H	lelp, pre	ess F1									Tag	s: 0	-	A	arms: 0)	L	OG I	UTC	HE>	K AU	TO AI	CK 🗌	-		CA	LLBAC	KL	n 0	

2. Click Servers > Connect to Server (Listing). The OPC Server List dialog box appears.

OPC Server List		×
Node (computer, IP)	S-CEFA73DE011	Add
OPC Data Opc Clata Opc Clata Opc Data Opc Data Opc Data Opc Data	DE011 Access Servers Version 1.0 Access Servers Version 2.0 OneWirelessGW ComServer ComDaProxyServer.1 Access Servers Version 3.0 ackChange Servers Version 1.0 and Event Server Version 1.0 ical Data Access Servers Version 1.0 Servers Version 1.0 Servers Version 2.0	
Legend DA Servers DX Servers A&E Servers DA Servers Batch Servers Server Info Node T Node	Local Server CoCreate Options ALL C LOCAL C I Remote Server Location Manual Override Use this computer Honeywell Server Connection Restrictions Override connection restrictions	NPROC
	Connect Server Close	Help

- Double-click the OPC DataAccess Servers Version 2.0 and select
 OpcDa.OneWirelessGW.ComServer from the list, and then click Connect Server....
- 4. Once the server is connected, click **Close**. The **OPC Server List** dialog box closes.
- 5. In the OPC Validator window, select **OpcDa.OneWirelessGW.ComServer**.

Click Data > Browse Server Address Space, and then click Browse Server Address
 Space All. The Address Space appears on the lower pane.

« No Script - OPC Validator						[
File View Servers Data eXchange Alarms Historical E	Batch Validate So	ript Log Tools	Help				
8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	0 0 C C		9 - 4 -	[66 68 al	· + + +	' 로 로 로	
5 5 6 6 6 8 K R K K R 10	ਸਟੈ ਸਟੈ ਸਟੈ ਸਟੈ	тё тё					
🗐 DA1\\LOCAL\OpcDa.OneWirelessGW.ComServer							
Workspace - DA11\LOCAL\OpcDa.OneWirelessGW.Co	mServer	Tags - All	Alarms	Historical	Browse	Validate]
Address Space of DA1\\LOCAL\OpcDa.OneWirelessGW.0 G G Server G ID_122 F MNBBR 83	ComServer						(1) (1)
Output Script ScriptOut Log Stat	tus Spec	Test Case					
or Help, press F1	Tags: 0	Alarms: 0	LOG U	TC HEX AUTO	ACK	CALLBACK	LnO

7. In the upper pane, right-click **OpcDa.OneWirelessGW.ComServer**, and then click **Add Private Group**. The **Add Private Group** dialog box appears.

Group Name Group_	OW								
Active	\mathbf{V}								
Requested Update Rate	1000	(msee)							
Time Bias	0	(min) UTC							
Percent Deadband	0	(0-100)							
Locale ID	0								
Max KeepAlive, 0=Off	0	(msec)							
Requested Connection Auto Detect IOPCDataCallback. (2.0) IAdviseSink. (1.0) No Callback.									

- 8. Type the Group Name, and then click OK.
- 9. From the lower pane of the **OPC Validator** window, select the OneWireless Network, and then a device.

10. To add all the parameters of a device, right-click on the device and click Add All Items and SubItems to Group_OW.

🛤 No Script - OPC Validator						
File View Servers Data eXchange Alarms Historical Batch Va	alidate Script Log To	ols Help				<u>ار کار</u>
• • • • • • • • • • • • • • • • • • •				, , , , ,	🚽 🚽 🚽	E
B B B B B B B B B B B B B B B B B B B					<u> </u>	
□-■ ■ DA1\\LOCAL\OpcDa.OneWirelessGW.ComServer └-① Group_OW						
Workspace - Group_OW	ags - All	Alarms	Historical	Browse	Validate	
Workspace - Group_OW Image: Solution of the state of the		Alarms	Historical	Browse	Validate	

To add individual parameters for a device, expand the device, right-click on the parameter, and then click **Add Item to Group_OW**.

- 11. In the upper pane, expand **Group_OW** to view the items in your group.
- 12. Click **Tags All** to view all the tags.
- 13. Navigate to the desired value. Identify the OPC item that represents the desired value.

		אַ שָּׁ שָּׁ שָּׁ שָּׁ אָ שָּׁ דלי דלי דלי דלי דלי ד			<u> </u>	E
tem ID	Access Path	Value	Ouality	Гуре	Canonical Rights	Time
ns*2;s*53 MD 07.CTS VERSION		1	GOOD : NON SPECIFIC : LIMIT N		VT UI2 R	201
ns*2;s*S3 MD 07.DEVICE ROLE CA		3	GOOD : NON SPECIFIC : LIMIT N	-	VT UI2 R	201
ns*2;s*S3_MD_07.DIAG_STATUS		0	GOOD : NON_SPECIFIC : LIMIT_N	. ¥T_UI4	VT_UI4 R	201
ns*2;s*53_MD_07.DIAG_STATUS_DE		0	GOOD : NON_SPECIFIC : LIMIT_N	. YT_UI4	VT_UI4 R	201
ns*2;s*53_MD_07.DL_ALIA5_16_BIT		6	GOOD : NON_SPECIFIC : LIMIT_N	. VT_UI2	VT_UI2 R	201
ns*2;s*53_MD_07.DLMO_CHANNEL_D.		11; 22; 0; 12; 0; 0;	GOOD : NON_SPECIFIC : LIMIT_N	. VT_ARRA	VT_ARR R	201
ns*2;s*53_MD_07.DLMO_NEIGHBOR		77; 78; 66; 66; 82;	GOOD : NON_SPECIFIC : LIMIT_N	. VT_ARRA	VT_ARR R	201
ns*2;s*53_MD_07.DLMO_RADIO_TRA.		16	GOOD : NON_SPECIFIC : LIMIT_N	. VT_I1	VT_I1 R	201
ns*2;s*53_MD_07.DROP_OFF_COUNT		1	GOOD : NON_SPECIFIC : LIMIT_N	. VT_UI2	VT_UI2 R	201
ns*2;s*53_MD_07.EUI_64		0; 64; 132; 0; 0; 1;	GOOD : NON_SPECIFIC : LIMIT_N	. VT_ARRA	VT_ARR R	201
ns*2;s*S3_MD_07.FAILURE_STATUS		0; 10;	GOOD : NON_SPECIFIC : LIMIT_N	. VT_ARRA	VT_ARR RW	201
ns*2;s*53_MD_07.FUNCTION_CHECK		0; 10;	GOOD : NON_SPECIFIC : LIMIT_N	. YT_ARRA	VT_ARR RW	201
ns*2;s*53_MD_07.IDENT_NUMBER		0; 72; 87; 76; 32; 3	GOOD : NON_SPECIFIC : LIMIT_N	. VT_ARRA	VT_ARR R	201
ns*2;s*53_MD_07.IT5_VERSION		2	GOOD : NON_SPECIFIC : LIMIT_N	. VT_UI2	VT_UI2 R	201
ns*2;s*53_MD_07.JOIN_ATTEMPT_C		2	GOOD : NON_SPECIFIC : LIMIT_N	. VT_UI2	VT_UI2 R	201
ns*2;s*53_MD_07.JOIN_COMMAND		0	GOOD : NON_SPECIFIC : LIMIT_N	. VT_UI1	VT_UI1 RW	201
ns*2;s*53_MD_07.MAINTENANCE_AL		0; 10;	GOOD : NON_SPECIFIC : LIMIT_N	. YT_ARRA	VT_ARR RW	201
ns*2;s*53_MD_07.MODEL_ID		2618_242C_01	GOOD : NON_SPECIFIC : LIMIT_N	. VT_BSTR	VT_BSTR R	201
		254, 120, 0, 0, 0, 0	COOD - NON OFFICIERS - LIMIT N		UT 400 0	
*	aroup OW		Tags - All Alarms H	istorical Bro	owse Validate	

Perform the following steps to edit parameters from OPC DA client. Note that you can only edit the parameters whose access rights are displayed as **RW** in the **Rights** column of the OPC Validator.

- a. In the OPC DA client, click the **Tags All** tab.
- b. Right-click the parameter that you have added, and then click Async > Write Item. The Write Async Item Value dialog box appears.
- c. In the **Raw** field, type the required value. You can only edit the mode for all the device types and the output value of the Multi AI DI DO devices.
- d. Click **OK**.

Configuring OPC communication using Experion SCADA and OPC Validator with multiple WDMs in the same network

With Experion SCADA

1. In the Experion SCADA Machine, edit the HOSTS File with multiple WDMs hostnames.

	🗌 hosts - Notepad - 🗆	
F	ile Edit Format View Help	
#	Copyright (c) 1993-2009 Microsoft Corp.	
#	This is a sample HOSTS file used by Microsoft TCP/IP for Windows.	
	This file contains the mappings of IP addresses to host names. Each	
	entry should be kept on an individual line. The IP address should	
	be placed in the first column followed by the corresponding host name.	
	The IP address and the host name should be separated by at least one	
#	space.	
#		
	Additionally, comments (such as these) may be inserted on individual	
#	lines or following the machine name denoted by a '#' symbol.	
	For example:	
#	for example.	
#	102.54.94.97 rhino.acme.com # source server	
#	38.25.63.10 x.acme.com # x client host	
#	localhost name resolution is handled within DNS itself.	
1	92.168.15.15 wdm_pri	
1	92.168.15.16 wdm1	

2. Configure UA Server COM Proxies for multiple WDMs (PCN IP address of WDMs).

2 R510_NRSRV_KS on 10.79.214.225							<u> 100</u>	
File View VM	13 10 0 1	b						
File Help								
Manage Security Manage Application	Manage Certificates	Manage COM Interop H	TTP Access Rules					
	DA opcua	A Clients.	192.168.15.15		- 0	I X		
	Endpoint URL	opc.tcp://192.168.15.16	4840					
	ОК		Discove	r		Cancel		
Γ	No-							

🔡 Server Configur	ation			×
Protocol	opc.tcp [wdm1:4840]	~		
Security Mode	None	~		
Security Policy	None	~		
Message Encoding	Binary	~		
User Identity Type	Anonymous [Anonymous]	~		
lssued Token Type				
User Identity				
User Default Limits	Yes 🗸			
Configuration options a	are up to date.			
ОК	Refresh		Ca	ncel

🔛 COM	M Server Configura	tion	4 <u>-</u>		×
Protocol	DA	~			
CLSID	10730038-fa55-485	a-92a2-38b2555111e0			
Prog ID	OpcDa.opc.tcp.192	.168.15.16.4840			
OK				C	ancel

🔲 🕨 😋 🙆 🚳	13 🐶 (9 B9							
File Help					_				Ī
anage Security Manage Application	Manage Certifi	Cates Manage COM Int	erop HT	TP Access Rules					
		to COM Clients.							
Wrap COM Servers Make a C	OM Server visib	le to UA Clients.							
ProgID	Specification	Server	Protocol	Haet	Security			 	-
OpcDa.opc.tcp.192.168.15.16.4840		opcuasrv-x86@wdm1			-				
OpcAe One WirelessGW ComServer		opcuasrv-x86@wdm1							
OpcDa.OneWirelessGW.ComServer	DA						×		
		Restart the 'UA CON changes to take effe		/rapper' (Admin	istrative Tools -	Services) for a	ny		
		changes to take ene							
							_		
						OK			

Restart the UA COM Server Wrapper service using services.msc.

3. Configuring OPC Channels, OPC Controllers, Analog Points in Experion Quick Builder.

R510_NRSRV_KS on 10.79.214.225	k.			
File View VM				
🖬 🖬 🕟 😋 🔯 🚳	13 6 📀 🄛			
	Спаннсіз	0× -×		
R510-NRESV	Name 🔺 D	escription	Item Number	🔝 Modbus Channel
Channels	CHAMODO		CHN0001	DPC Channel
(T) Equipment	CHAOPC1		CHN0002	
Points	CHAOPC2		CHN0003	1
Printers				1
- Stations				
- E Servers				
EFM Meters				
- 📅 Recycle Bin				4
	Main			
	Marginal Alarm Limit 10			
	Fail Alarm Limit 20			
	Connect Timeout 20	secs		
	Read Timeout 2	secs		
	Host Name (Preferred Data So	urce) R510-NRESV		
	Host Name (Alternate Data So	- Justo Hiteov	_	
		Server host time can drift (Asynchronous reads)	Controller
	🖵 Use	the "Last Known Value" su	bstatus to indicate a value as	Point
All items		the "Last Usable Value" su the OPC Server timestamp	ubstatus to indicate a value a: when raising alarms	EFM Data Export Format
SCADA Controllers	Diagnostic Scan Period 60	Backgrour		EFM Meter
g Assets	60	Scan Perio	od 60	EFM Meter Template
EFM Configuration		opc.tcp.192.168.15.16.4840		EFM Schedule
	Item Type OPC Char			Printer
Controller Integration	Last Downloaded 8/31/201	18 9:22:42 AM Item Numbe 18 9:22:47 AM	r JCHN0003	Station
*	<		~	Server

OPC Channel for wdm1 with ProgID: OpcDA.opc.tcp.192.168.15.16.4840

• • • • • • •			
R510-NRESV	Name Description	Item Number	🔢 Modbus Channel
Channels	CHAMOD0	CHN0001	OPC Channel
Controllers	CHAOPC1	CHN0002	
Points Printers Stations Servers EFM Meters	CHAOPC2	CHN0003	
└─ m Recycle Bin	Main In Marginal Alarm Limit 10 Fail Alarm Limit 20 Connect Timeout 20 Read Timeout 2 Host Name (Preferred Data Source) RS10-NRESV Host Name (Alternate Data Source) F		Controller
		n drift (Asynchronous reads)	- company
		lue" substatus to indicate a value as alue" substatus to indicate a value a:	Point
All items	Use the OPC Server time	stamp when raising alarms	EFM Data Export Format
SCADA Controllers	Diagnostic Scan Period 60 Sc	ckground 60	EFM Meter
Assets	I Sc	an Period 1	EFM Meter Template
EFM Configuration	Prog Id OpcDa.OnewirelessGW.Co Item Type OPC Channel	mserver	EFM Schedule
	Last Modified 8/22/2018 1:43:18 PM Item	Number CHN0003	Printer
Controller Integration	Last Downloaded 8/22/2018 1:49:37 PM	Number Jennouz	Station

OPC Channel for wdm_pri with ProgID: OpcDA.OneWirelessGW.Comserver

R510_NRSRV_KS on 10.79.214.	225					-	
File View VM	a 13 6 9 6	9					
Configuration Explorer 🛺 R	510-NRESV - Quick Builder	<u> </u>			×	Library	g
All items	Controllers	Υ.	٩		•	Channel	
B 🧮 R510-NRESV 🔚 Channels	Name 🔺	Description	Item Number	Controller Channel Name		Controller Modbus Controller	
Controllers	CONMOD0 CONOPC1		RTU00001 RTU00002	CHAMOD0 CHAOPC1		OPC Controller	
Points	CONOPC2		RTU00003	CHAOPC2			
🛲 🗑 Recycle Bin	Main				•		
	Name Description	[
	Associated Asset Channel Name	CHAOPC2 -					
	Marginal Alarm Limit Fail Alarm Limit	20					
	Background Scan	Disabled	•			Point	
All items	Deadband	0.000 -				EFM Data Export Format	
SCADA Controllers	Diagnostics Item]		EFM Meter	
g Assets	Failure Value	Zero 💌		_		EFM Meter Template	
EFM Configuration	Enable SOEs to	1				EFM Schedule	
	1ms resolution for digital input tags					Printer	
Controller Integration	Enable	Г				Station	
	» ControlLogix Integration				~	Server	

OPC Controller for wdm1

R510_NRSRV_KS on 10.79.214.225 File View VM					- 0
					1
En Esio-NRESV	Name 🔺	Description	Item Number	Controller Channel Name	Controller 🔤 Modbus Controller
Controllers	CONMODO		RTU00001	CHAMOD0	OPC Controller
-[T] Equipment	CONOPC1		RTU00002	CHAOPC1	OPC Controller
Printers Printers Servers FFM Meters Fervers Recycle Bin	CONOPC2		RTU00003	CHAOPC2	
	Main				
	Name Description Associated Asset				
	Channel Name Marginal Alarm Limit Fail Alarm Limit	CHAOPC1			
	Dackground Scan	Disabled	•		Point
All items	Deadband	0.000 🔹			EFM Data Export Format

OPC Controller for wdm_Pri

		÷		×	Library	G
Configuration Explorer	R510-NRESV - Quick Builder		۹.		Channel	4
R510-NRESV		Description	Area Code	Source Address PV	Controller Point	
Controllers	DUPLICATE	PV	ow	CONOPC1 ns*2;s*TD	Accumulator Point	
[f]:] Equipment 	POIANAO		OW	CONOPC2 ns*2;s*wd		
Points	POIOPC1		ow		Analog Point	
Stations Stations Servers EFM Meters Recycle Bin	TD_52_PV	PV	ow	CONMOD0 2 IEEEFPB	Container Point E IEC-870 Point OPC Advanced Point Status Point	
	Main Display	Alarms Control	Auxiliary Histo	ory Scripts ()		
	Point ID Enterprise Model Item Name Description	POIANAO				
	Parent Asset	ow				
		CONOPC2 ns*2;s*wdm1				
All items	Engineering Units				EFM Data Export Format	
SCADA Controllers	100% Range Value	100	0% Range Value 0		EFM Meter	
	Drift Deadband (%)	0.000 -			EFM Meter Template	
En Assets	PV Algo	NONE		•	EFM Schedule	
EFM Configuration	Action Algo	NONE		-	Printer	
Controller Integration	Action Algo	Scanning Enabled	Clamp PV		Station	

Analog Point for wdm1

ile View VM			-		
R510-NRESV Channels Controllers Controllers Controllers Printers Printers Stations Servers Printers Firef Metters	Name DUPLICATE POIANAD POIOPC1 TD_52_PV		Area Code OW OW OW OW	Source Address PV CONOPC1 ns*2;s*TD CONOPC2 ns*2;s*wd CONMOD0 2 IEEEFPB	Controller Point Accumulator Point Container Point Container Point EC-870 Point COPC Advanced Point
La	Parent Asset PV Source Address	Alarms Control DUPLICATE PV OW CONOPC1 ns*2;s*TD_52 PV Vpnamic Scannin	_3CLL_PCT.CH01_AI.PV	y Scripts ()	Status Point
All items	Engineering Units				EFM Data Export Format
SCADA Controllers	100% Range Value	100	0% Range Value 0		EFM Meter
Assets	Drift Deadband (%)	0.000 💌			EFM Meter Template
) EFM Configuration	PV Algo	NONE		•	EFM Schedule
crim conliguration	Action Algo	NONE		-	Printer

Analog Point for wdm_pri

Enable OPC Controllers and OPC channels from station

Launch the trend to display the values

le View Ultrained State	••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••• ••<		Image: wide wide wide wide wide wide wide wide			eriod: 1 Minute	Interval: 1 sec
9/ 100.0 80.1 60.1 40.1 20.1						eriod: 1 Minute	Interval: 1 sec
9 100.0 80.1 60.1 40.1 20.1	% 3: POIANA0.P					eriod; 1 Minute	r Interval: 1 sec 👤
100.0 80.0 60.0 40.0	.0		-		Pt	eriod: 1 Minute	r Interval: 1 sec
80.1 60.1 40.1 20.1	.0						
60.1 40.1 20.1	.0						
60.1 40.1 20.1	.0						
40.1 20.1	.0						
40.1 20.1	.0						
40.1 20.1	.0						
20.1							
20.1							
20.1							
	.0						
	.0						
0.0							
0.0							
	10:52:4	2 AM 10:52:48 AM	10:52:54 AM 10	:53:00 AM 10:53:06 AM	4 10:53:12 AM 10:53:	18 AM 8/31/2018	- 10:53:36 AM
	•				•		
Pen	Point ID	Parameter	Description	Low Scale (%)	High Scale (%)	Reference Value	Current Value
1 🗹	TD_52_PV	PV	PV	0.00	100.00		22222
2 🗹	DUPLICATE	PV	PV	0.00	100.00		25.08
3 🗹	POIANA0	PV	•	0.00	100.00		89.18
4							
5 🗆							
6							

Values from 2 different WDMs visible in Experion SCADA in same Experion Server.

Monitor OPC interface statistics

To monitor OPC interface statistics:

- 1. Select **EXTERNAL INTERFACES** in the Left Navigation Menu bar.
- 2. Select **OPC** and click **NEXT**.
- 3. Go to **Statistics** tab.

You can view the OPC interface messages totals and OPC interface message rates.

onfiguration Statistics Alarm	s(0)	
OPC Interface Messages		
Message Count :	8428	mag
Message Rate :	0.000000	msg/sec
Message Rate Max:	333.333344	msg/sec
OPC Interface Subscriptions		
Subscription Count :	1119	attr
Subscription Rate :	1011.183350	atto/sec
Subscription Rate Max:	1106.256226	atto/sec

4. Click **Reset Statistics** to reset all the OPC interface statistics.

Monitor OPC interface for multiple WDMs

To monitor OPC interface for multiple WDMs:

- 1. Download and install OneWireless UA proxy software. During the installation enter the Host ID and then complete the installation.
- 2. Open OPC UA configuration tool. Click Manage COM Interop and select Wrap UA Server.

UA Configuration Tool File Help						
lanage Security Manage Application I	Manage Certific	sates Manage COM Interop	HTTP Ac	cess Rules		
Wrap UA Server Make a UA	A Server visible	to COM Clients.				
Wrap COM Servers Make a CC) M Server visib	le to UA Clients.				
)M Server visib Specification		Protocol	Host	Security	
		Server	Protocol opc.tcp	Host 192.168.0.1	Security None/None	
ProgID	Specification DA	Server		192.168.0.1	None/None	
ProgID	Specification DA AE	Server opcuasrv-x86@AIMS-WDM	opc.tcp	192.168.0.1	None/None None/None	

3. Test UA Server COM proxies.

🖌 RSI - OPC Test Client - [~Op	cDa.opc.tcp.192.168.0.2]					
🗹 File Server Group Item I	Log View Window Help					_ 8 ×
📀 WDM2 (Actual Rate: 2000)	ItemID	Sub Value	Sub Quality	Sub Updates	Update Rate	Run. Avg
	Signer Contemporation (Contemporation of the contemporation of the	90.8306	Good	45331	1	0.499998
	•					
Ready					1	JUM ///
🚮 RSI - OPC Test Client - [~Op	cDa.opc.tcp.192.168.0.1]					_ 🗆 ×
😴 File Server Group Item I	Log View Window Help					_ 8 ×
🕘 WDM1 (Actual Rate: 2000)	ItemID	Sub Value	Sub Quality	Sub Updates	Update Rate	Run. Avg
	Sins*2;s*AIMS-WDM.CPUFRE	E 92.3614	Good	45329	0	0.499748
	•					Þ
Ready					1	JUM ///

4. Configure Channels using COM proxies.

All items	Channels	All items	Channels
C2-4-0-NRSERVER C2-4-0-NRSERVER	Name 🕗 Description Item Number	C2-4-0-NRSERVER	Name 🔺 Description Item Number
	CHAOPCWDM1 CHN02	Controllers	CHAOPCIVDM1 CHN02
Controllers	CHAOPCWDM2 CHN03	Points	CHAOPD/VDM2 CHN03
	Main		Main
🔤 🍿 Recycle Bin	Name CHAOPCWDM1	👘 Recycle Bin	Name CHAOPOWDM2
	Description		Description
	Associated Asset SUNASSIGNEDITEMS		Associated Asset SUNASSIGNEDITEMS
	Marginal Alarm Limit 10		Marginal Alarm Limit 10
	Fail Alarm Limit 20		Fail Alarm Limit 20
	Connect Timeout 20 secs		Connect Timeout 20 secs
	Read Timeout 2 secs		Read Timeout 2 secs
	Host Name (Preferred Data Source) localhost		Host Name (Preferred Data Source) localhost
	Host Name (Alternate Data Source)		Host Name (Alternate Data Source)
	OPC Server host time can drift (Asynchronous reads)		OPC Server host time can drift (Asynchronous reads)
	Use the "Last Known Value" substatus to indicate a value Use the "Last Usable Value" substatus to indicate a value		Use the "Last Known Value" substatus to indicate a value Use the "Last Usable Value" substatus to indicate a value
	Use the OPC Server timestamp when raising alarms	1	Use the OPC Server timestamp when raising alarms
	Diagnostic Scan Period 60 Scan Period 60		Diagnostic Scan Period 5 Background 5 T
	Progld OpcDa.opc.tcp.192.168.0.1.		Progid OpcDa.opc.tcp.192.168.0.2.
	Item Type OPC Channel		Item Type OPC Channel
	Last Modified 7/28/2015 10:00:10 AM Item Number CHN02		Last Modified 7/28/2015 10:00:12 AM Item Number CHN03
	Last Downloaded 7/28/2015 18:00:20 AM		Last Downloaded 7/28/2015 10:00:20 AM

5. Configure Controllers using Channels.

All items	Controllers				All items		Contro	ollers			
E- 🗮 C2-4-O-NRSERVER	Name 🛆 D	escription Nu	em Imber	Controller Channel		-4-0-NRSERVER Channels	Name	Δ.		tem Jumber	Controller Channel N
	CONOPC1	RTU	J00002	CHAOPCWDM1		Controllers	CONOPC1		R	TU00002	CHAOPCWDM1
	CONOPC2	RTU	100003	CHAOPC/VDM2		Points	CONOPC2		R	TU00003	CHAOPD/VDM2
🧮 Servers					🖻	Servers					
📅 Recycle Bin	Main				L. 6	Recycle Bin	Main				
	Name	CONOPCL	_					Name	CONOPC2		
	Description	CONOPUL						Description	CONOPUZ		
	Associated Asset	\$UNASSIGNEDITEMS					Assoc	tiated Asset	SUNASSIGNEDITEMS		
	Channel Name	CHAOPCWDM: -					Cha	annel Name	CHAOPOV/DM: -		
	Marginal Alarm Limit	10					Marginal	Alarm Limit	10		
	Fail Alarm Limit	20					Fail	Alarm Limit	20		
	Background Scan	Disabled	•				Back	ground Scan	Disabled	•	
	Deadband 0	0.000						Deadband	0.000		
	Diagnostics Item						Diag	nostics Item			
	Failure Value	Zero 🔻					Fa	ailure Value	Zero 💌		
	Enable SOEs to F 1ms resolution for digital input tags						1ms re:	ble SOEs to solution for al input tags			
	Item Type 0 Last Modified 7 Last Downloaded 7	/28/2015 9:56:54 AM	Item Numbe	r RTU00002				st Modified	OPC Controller 7/28/2015 9:57:02 AM 7/28/2015 9:57:08 AM		r RTU00003
	Last Downloaded 7	1/20/2013 3:57:08 AM					Last D	ownioaded	7/20/2015 9:57:08 AM		

6. Configure Points using Controllers and OPC Access Path (PV Source Address).

All items	Points				All items	Point	s					
E- E C2-4-0-NRSERVER	Name	A Description Area	a Code	Source Add	ss - C2-4-0-NRSERVER	Name		△ Descrip	tion Area	Code	Sou	urce Addres
- 🔚 Channels	PVVDM1CPUFREE	\$UN4	ASSIGNEDITEMS	CONOPC1 ns	Channels	PWDM1C	PUFREE		\$UN4	SSIGNEDITEM:	s con	IOPC1 ns*2;
Controllers	PWDM2CPUFREE	\$UN4	ASSIGNEDITEMS	CONOPC2 ns ¹	Controllers	PWDM20	PUFREE		\$UN4	SSIGNEDITEM	s con	10PC2 ns*2;
Points					Points							
Servers		r r	e e	6			1	5	Ϋ́.	í.	5	5
🦾 🍿 Recycle Bin	Main Display	Alarms Control	Auxiliary	History Scrip	The Recycle Bin	Main	Display	Alarms	Control	Auxiliary	History	Scripts
	Point ID	PWDMLCPUFREE					PointID	PWDM2CPI	IEDEE			-
	Enterprise Model	FUIDMEEPOINEE					rise Model		511166			-
	Item Name						Item Name	-				
	Description						Description	1				
	Parent Asset	SUNASSIGNEDITEMS				P	arent Asset	\$UNASSIG	VEDITEMS			
	PV Source Address	CONOPC1 ns*2;s*AIMS-	-			PV Sour	rce Address	CONOPC2 r	is*2;s*mywd	ī]		
		🔽 PV Dynamic Scannir	ng					🔽 PV Dyna	mic Scannir	ng		
	PV Scan Period	5 💌				PV S	Scan Period	5	-			
	Engineering Units					Engine	ering Units					
	100% Range Value	100	0% Range Value	0	1	100% R	ange Value	100		0% Range Val	lue 0	
	Drift Deadband (%)	0.000				Drift De	adband (%)	0.000	-			
	PV Algo	NONE		•			PV Al go	NONE			-]
	Action Algo	NONE		-			Action Algo	NONE			-]
		Scanning Enabled	🗌 Clamp PV					🔽 Scannir	ig Enabled	🗌 Clamp PA	/	
	Item Type	Analog					Item Type	Analog				
	Last Modified	7/29/2015 10:24:14 AM				La	st Modified	7/29/2015	10:24:10 AM			
	Last Downloaded	7/29/2015 10:24:24 AM				Last D	ownloaded	7/29/2015	10:24:24 AM			

7. Enable controllers:

🔅 Station - Default - Con	ntroller Summary(sysSEAL	DAControllers.	htm)								
	Control Action Configure										
♠ 🗛 🖉 🗔 🗆	V A O - O - 4	\circ \simeq III	▲ ▼ ✓ × ७ Q	Zoom T	o Fit 🔹	Command					
	_	_									
(filter applied)	Clear All Filters 🔀	Enable	Name	•	Stat	us	Description	Number 🗘	Server	Cha	nnel
Filter by Status	1	~	CONALL1			ок		1	mw-440-C2-4SRV	۲	SRVPNT1
Failed (0)		~	CONOPC1		۲	OK		2	mw-440-C2-4SRV	۲	CHAOPCWDI
Marginal (0)		~	CONOPC2			OK		3	mw-440-C2-4SRV	۲	CHAOPCWD
Disabled (0)		Showing 11	to 3 of 3 entries								N A
OK (3)		onowing 11	to 5 of 5 entities								
Unknown (0)											
Filter by Location	2										
San Assets											
🖃 💑 🛛 System Comp											
	2-4SRV [local server]										
Channel Channel CHAC											
CHAC											
SRVP	NT1										

8. Enable channels:

Station Edit View Control Action Configure	Help		
	$ \simeq \land \lor \checkmark \times 0$	り Q, Zoom To Fit ・ Command	
▼ System Status	Channel	2 Server: mw-440-C2-4S	RV CHAOPCWDM1
	SCADA Channel		
 System Hardware 	oon brit on annoi		0
 Controller Interfaces 	 Enable 	ок	Scope of
System Interfaces			Associated
SCADA Controllers	Connection type:	Direct	
OPC Integrator	Error statistics		Simulatio
+ Stations	Total requests:	1676	Enable s
Consoles	Total errors:	0	
Printers	% Errors:	0.0000	
Server Redundancy			
Distributed Servers	Barometer		
Experion Server Peer Responder	Current value:	0	

9. Call-up display for WDM OPC SCADA Point.

Station - Default - Analog Point Detail:PWDM1CPUFREE -	sysdtlana.htm(sysdtlana.htm)		Station - Default - Analog Point Detail/PWDM2CPU	FRFF - sysdtlana.htm(sysdtlana.htm)	
Station Edit View Control Action Configure Help	systematicity second activy		Station Edit View Control Action Configure		
♠ ▲ ≪ 등 □ ⊡ ⊡ ● • • • ¢ ×	111 ▲ ▼ ✓ X O Q Zoom To Fit •	Command	♠ 4 & ⊂ □ • • • • • • ≎	≫ [] ▲ ▼ ✓ X ᠿ Q Zoom To Fit ▪	Command
Analog Point Detail	/Assets/Unassigned Items/PWDM1	CPUFREE	Analog Point Detail	/Assets/Unassigned Items/PWDM	12CPUFREE
PWDM1CPUFREE	General Scanning	Alarms	PWDM2CPUFREE	General Scanning	Alarms
	Range			Range	
	Units:			Units:	
	100%:	100.00		100%:	100.00
	0%:	0.00		0%:	0.00
100.00	Bias and scaling Enable additional PV bias and scaling Bias:	0.00	100.00	Bias and scaling Enable additional PV bias and scaling Bias:	0.00
	Scale:	1.00	-	Scale:	1.00
0.00	Services Scanning and control enabled Sams enabled Journal only option Journal only option Hield value: Displays Scanning Field value:	92.31	0.00	Seam: Seaming and control enabled Alarms enabled Journal only option Manual PV Field value: Displays Associated display:	92.20
SP 0.00 EU PV 92.31 EU	Algorithms PV algorithm: Action algorithm:	0		Algorithms PV algorithm: Action algorithm:	0 0

About integrating OneWireless Network with Experion using the CDA interface

OneWireless Network can be integrated with Experion PKS system using the CDA interface available on the WDM. To establish communication between the Experion system and the OneWireless Network, you must connect the WDM to the Experion network. For more information about connecting WDM with the Experion system, see the section **"Establishing communication between OneWireless Network and Experion system**"

After connecting the WDM to the Experion network, configure the OneWireless Network components such as WDM and field devices using the Control Builder. For more information about configuring the OneWireless Network components using Control Builder, see the *Experion PKS OneWireless Integration User's Guide*.

After the communication between the Experion system and the OneWireless Network is established, the CDA parameters on the OneWireless user interface provides you information about the WDM state, CDA statistics, and the peer connections of the WDM. The following are the CDA parameters that are available on the user interface.

Selection P	anel element	Parameters and their descriptions
Configurati	ion	WDM State parameter indicates the WDM state in an
CDA OneWireless Network can be integrated	d with Experion PKS system using the CDA interface available on the WD	Experion system. This parameter displays the state as
Configuration Statistics Connec		Online , when the WDM is loaded in an Experion system.
Licensing :	Licensed	WDM Command parameter on the CDA interface consists
Experion PKS Database		of the following commands.
WDM State :	Not Loaded	– None
WDM Command :	rune	– Clear CDA Database: This command is used to
CDA Log level	Low	clear the CDA interface database from a running
		WDM. You must clear the CDA interface database
		when moving the WDM from one Experion PKS
		system to another. If you do not clear the CDA
		interface database, you may get an "invalid EEC"
		error when attempting to load the WDM on a
		different Experion PKS system.

atistics	Displays the CDA statistics used for maintenance and
	performance monitoring of the WDM. For the
DA environment of the second	specifications for peer responder rate and display
allaurstian Statistics Connections	
Peer Responder Rate	responder rate, refer to the Technical Specifications
Request Rate : 0.000000 req/sec	document available at the Honeywell Process Solutions
Request Rate Max : 0.000000 reg/sec	website.
Display Responder Rate	website.
Request Rate : 1.110954 req/sec	
Request Rate Max : 5.000000 req/sec	
Total Responder Rate	
Total Responder Rate	
	Displays the number of peer and display connections
Request Rate: 1.110954 reg/sec Request Rate Max: 5.000000 reg/sec	
Request Rate: 1110994 reg/sec Request Rate Max: 5000000 reg/sec	between the WDM and the controller CEEs. It also displays
Request Rate: 1110994 reg/sec Request Rate Max: 5000000 reg/sec Connections M Winking Network can be integrated with Experion PKS system using the CCM interface available on the WDM. Figure1Con: Statistics: Connections:	between the WDM and the controller CEEs. It also displays the details about incoming and outgoing connections
Request Rate: 1110954 reg/sec Request Rate: 5000000 reg/sec	between the WDM and the controller CEEs. It also displays
Request Rate: 1110594 reg/sec Request Rate Max: 5000000 reg/sec Donnectionss A Ministra Network can be integrated with Equation PVS system using the CDA interface available on the WDM. Figuretion: Subsidies: Connections annection Count	between the WDM and the controller CEEs. It also displays the details about incoming and outgoing connections
Request Rate: 1110994 reg/sec Request Rate: 5000000 reg/sec	between the WDM and the controller CEEs. It also displays the details about incoming and outgoing connections
Request Rate: 1110594 reg/sec Request Rate Max: 5000000 reg/sec Domnectionss A Workers Never can be introduced with Equation PCS system using the CDA interface available on the WDM. Figuration Statistics <u>Connections</u> parametrions: 0 and 0	between the WDM and the controller CEEs. It also displays the details about incoming and outgoing connections
Request Nate: 1110994 reg/sec Request Nate: 5000000 reg/sec	between the WDM and the controller CEEs. It also displays the details about incoming and outgoing connections
Request Rate: 1110994 reg/sec Request Rate: 5000000 reg/sec	between the WDM and the controller CEEs. It also displays the details about incoming and outgoing connections
Request Rate: 1110994 reg/sec Request Rate: 5000000 reg/sec	between the WDM and the controller CEEs. It also displays the details about incoming and outgoing connections

For more information about the CDA parameters, see the *OneWireless Parameter Reference Dictionary.*

Activating GCI interface on the WDM

The Gateway General Client Interface (GCI) is an external interface that is used with GCI-based client applications residing external to the WDM. GCI is a protocol that is used with client applications that communicate with the wireless field devices using ISA100 Wireless standard.

To activate GCI interface on the WDM

- 1. Select EXTERNAL INTERFACES in the Left Navigation Menu bar.
- 2. Select **GCI** and click **NEXT.**
- 3. Select **TCP Interface** In the Interface list from **Configuration** tab.

GCI The Gateway General Client Interface (GCI) is a	an external interface that is used with $\ensuremath{GC}\xspace^{-1}\ensuremath{based}\xspace$ client applications
Configuration Statistics	
_ Interface	
Interface :	TCP Interface 🗸 🗸
Licensing :	Licensed
Ethernet Interface Configuration —	
Port Configuration :	PCN ~
Ethernet/TCP Interface Options —	
TCP Port:	4901
GCI Log level	
Log Level :	Low ~

- 4. Under Interface Configuration,
 - In the **Ethernet Interface** list, click the required option. The following are the interface options available.
 - FDN
 - PCN
 - SIN

Note: GCI interface is enabled only on the Ethernet interface selected

- 5. Under Ethernet/TCP Interface Options,
 - In the **TCP Port** field, specify the default port number **4901**.
- 6. Click Apply.
- 7. Expand **Statistics** tab to monitor performance of GCI interface.
- 8. Verify the following attributes to monitor the performance of the GCI interface.
 - Message Rate: Number of messages processed by the interface, per second.
 - **Message Rate Max**: Maximum number of messages processed by the interface, per second.
- 9. Click **Reset Statistics** to reset all the GCI interface statistics.

Activate ENRAF Ethernet UDP interface on the OneWireless user interface

OneWireless supports integration between WDM, SmartRadar FlexLine field devices, and ENRAF applications (CIU Prime hardware, Engauge software). For more information, see the *ISA100 Wireless SmartRadar FlexLine User's Guide*.

To activate ENRAF Ethernet/UDP interface on the OneWireless user interface

- 1. Select **EXTERNAL INTERFACES** in the Left Navigation Menu bar.
- 2. Select **ENRAF** and click **NEXT**.
- 3. Select Ethernet/UDP Interface In the Interface list from the Configuration tab.

ENRAF OneWireless supports integration between WD	M, SmartRadar FlexLine field devices, and Enraf applications (CIU
Configuration Statistics Address Table	
_ Interface	
Interface :	Ethernet/UDP Interface 🗸 🗸
Licensing :	Licensed
Serial Interface Options	
Serial Port :	COM1 ~
Baud Rate :	9600 ~
Parity :	None
Ethernet Interface Configuration —	
Port Configuration :	PCN ~

- 4. The following options are available in the **Port Configuration** list under the **Ethernet Interface Configuration**.
 - FDN
 - PCN
 - SIN
 - The **UDP port number** of the port on which the WDM is connected is displayed.
- 5. Click Apply.

Configure ENRAF serial interface

To access the field device data, you need to configure the Enraf interface from the OneWireless user interface.

Prerequisites

- The SmartRadar FlexLine field devices are connected to the WDM using a serial cable.
- The SmartRadar FlexLine field devices are joined in the ISA100 Wireless network.
- The GPU address and the FlexConn address configured for a SmartRadar FlexLine field device must be unique for each device in the network.

For more information regarding the GPU address and the FlexConn address, see the section "Configure SmartRadar FlexLine field device interface".

• If RS-485 serial communication is required, then connect the RS-485 serial cable between the COM2 port of the WDM and the client.

To configure ENRAF serial interface

- 1. Select EXTERNAL INTERFACES in the Left Navigation Menu bar.
- 2. Select ENRAF and click NEXT.
- 3. Select **Serial Interface** in the Interface list from the **Configuration** tab.
- 4. Configure the following under **Serial Interface Options**.
 - **Serial Port**: Select the serial port on which the serial cable is connected. The available options are COM1 and COM2.
 - Baud Rate: Select 19200 as the baud rate for ENRAF serial interface.
 - **Parity**: This is a read-only parameter and displays the value as **None**.
- 5. Click **Apply**.

Monitor performance of ENRAF interface

To monitor performance of ENRAF interface

- 1. Select EXTERNAL INTERFACES in the Left Navigation Menu bar.
- 2. Select **ENRAF** and click **NEXT**.
- 3. Go to **Statistics** tab.

Configuration Statistics Addres	ss Table	
┌ Serial Interface ————		
Message Rate :	0.000000	msg/sec
Message Rate Max :	0.000000	msg/sec
Ethernet/UDP Interface		
Message Rate :	0.000000	msg/sec
Message Rate Max :	0.000000	msg/sec
RESET STATISTICS		

- 4. Verify the following attributes to monitor the performance of the ENRAF interface.
 - Message Rate: Number of messages processed by the interface, per second.
 - **Message Rate Max**: Maximum number of messages processed by the interface, per second.
- 5. Click **Reset Statistics** to reset all the ENRAF interface.

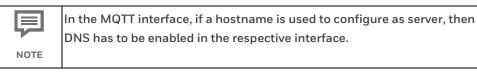
Activate MQTT in OneWireless Network

WDM supports Message Queuing Telemetry Transport Protocol (MQTT), where it acts as MQTT client to publish the topic data over the secured communication to MQTT Broker.

Enable MQTT interface

Prerequisites

- If the port configuration is selected as **SIN**, ensure that **SIN** is enabled in the WDM.
- MQTT communication is only supported in port **8883.**
- Ensure the WDM certificate is downloaded from the **Software Downloads** section and added to trust store of the MQTT Broker.
- Ensure the WDM certificates are downloaded and added to the trust store of the Broker. In case of redundant WDM, both primary and secondary WDM certificates need to be added to trust store of the Broker.
- MQTT Broker's CA Certificate must be imported to the WDM from the **Certificates** option.



To enable MQTT interface

1. Select **EXTERNAL INTERFACES** in the Left Navigation Menu bar.

2. Select **MQTT** and click **NEXT**.

HOME	External Interfaces					
MONITORING	Select Feature					
ALARMS & EVENTS	MODBUS The WDM functions as the Modbus server and allow of		HART WDM allows accessing this information from asset management sy		OPC OPC OPC OPC not activated. Please apply the license.	6
REPORTS	Modbus interface supports colls, discrete inputs, hold registers.		WUM allows accessing this internation from asset management sy Field Device Manager (FDM), through a HART interface.	soens, such as	UPC FOR ACTIVATION MAKAGE apply the scenae.	
PROVISIONING	⊖ CDA	6	() cCI	0	O ENRAF	
MANAGE DEVICES					OneWireless supports integration between WDM, Sma and Enral applications (OU Prime hardware, Engauge	
CHANNELS	🔘 матт					
FIRMWARE UPGRADE	The WDM acts as a MQTT client which connects to th					
	send data for the configured publish topics or receive topics.					
SYSTEM						
MAINTENANCE						
MANAGE LICENSES						
LOGOUT					BACK	NEXT

- 3. Configure the following under **Configuration** Option.
 - **Interface**: Select **Enabled** from the drop-down list to allow the MQTT connection. Select **Disabled** to disable the MQTT connection.
 - **Port configuration**: Port configuration can be configured in either **SIN** or **PCN** interface. Default interface is **SIN**.
 - Log level: Log level can be selected between Low and High.
- 4. Click Apply.

MQTT				
Configuration Servers & Topics Server S				
Interface				
Interface :	Enabled			
Licensing :	Licensed			
Ethernet Interface Configuration				
Port Configuration :	PCN ~			
MQTT Log level				
Log Level :	Low			
		BACK	RESET	AP

Configure MQTT Server

1. Select Servers and Topics and click ADD SERVER.

MQTT						
Configuration Servers & Topics Se						
Select Server Type						
□• S !						#
SERVER NAME	IP/HOSTNAME	PORT NUMBER	CONNECTION STATUS	CONNECTION	ACTIONS	
No records found						
0 - 0 of 0 records		1 > H	Go to page $1 \rightarrow$		Records per page	
			ВАСК	ADD SERVER	DELETE SE	RVER

2. Enter the details in **Add Server** Window as given below.

Note: Maximum 10 servers can be added.

- Server Name: Server name can be any user specified unique name.
- Select IP address and enter the IP address to connect to the MQTT Broker. Note: Hostname option is not supported.
- **Port Number:** Port Number should be configured as **8883**.
- Alive Interval (sec): Configure as the duration where the WDM MQTT client will ping the broker. Connection drop will be checked within this interval.
- **LWT Topic (optional parameter):** This topic message gets published when WDM connection is lost non gracefully from the MQTT broker. Default LWT topic is lost clients.

	×
Add Server	
Server Name *	
Server Name	
IP Address O Host Name	
IP Address *	
IP Address	
Port Number *	
8883	
Alive Interval(sec) *	
Alive Interval(sec)	
LWT Topic	
LostClients	
Indicates required fields	
CANCEL	

- 3. Click Save.
- 4. Once the server is successfully added, it appears in the **Servers and Topics** window as shown below.

MQTT					
Configuration Servers & Topics Se					
Select Server Type					
S :					₩ ₩
SERVER NAME	IP/HOSTNAME	PORT NUMBER	CONNECTION STATUS		ACTIONS
∽ □ Test	192 168 1 10	8883	Disabled	Disabled ~	
1 - 1 of 1 records			Go to page 1 → BACK	ADD SERVE	Records per page 10 V

5. To Edit Server, Click on **Edit** under **Actions.**

Note: Ensure the connection status is disabled.

MQTT Configuration Servers&Topics 9	Server Statistics Topic Statistics	Alarms(O)			
Select Server Type					⊞ \$
SERVER NAME	IP/HOSTNAME	PORT NUMBER	CONNECTION STATUS	CONNECTION	ACTIONS
∽ □ Test	192.168.1.10	8883	Disabled	Disabled \checkmark	Ø
			Go to page 1 → BACK	ADD SERVER	Records per page 10 DELETE SERVER

- 6. Enter the details in **Edit Server** Window as given below.
 - Server Name: Server name cannot be edited.
 - Select IP address and enter the IP address to connect to the MQTT Broker. Note: Hostname option is not supported.
 - Port Number: Port number should be configured as 8883.
 - **Alive Interval (sec):** Configure as the duration where WDM MQTT client will ping the broker. Connection drop will be checked within this interval.
 - **LWT Topic (optional parameter):** This topic message gets published when WDM connection is lost non gracefully from the MQTT broker. Default LWT topic is lost clients.
- 7. Click Save.

	×
Edit Server	
Server Name *	
IP Address O Host Name	
IP Address	
192.168.1.10	
Port Number *	
8883	
Alive Interval(sec) *	
5	
LWT Topic	I.
LostClients	
Indicates required fields	
CANCEL	

8. Enable/Disable MQTT Connection

Note: Ensure that certificates are properly imported and exported for MQTT secured connection to work and interfaces are accessible. To check the latest connection of MQTT, click on Refresh on Server and Topics Window.

- To enable the MQTT connection, select **Enabled** from the connection drop down list. If connection is successfully established with the MQTT Broker, the connection status shows as **Connected**.
- If connection is not established with the MQTT Broker, the connection status shows as **Disconnected**.

MQTT						
Configuration Servers & Topics Se						
Select Server Type						
						⊞ \$ĕ
SERVER NAME	IP/HOSTNAME	PORT NUMBER	CONNECTION STATUS	CONNECTION	ACTIONS	
∽ □ Test		8883	Connected	Enabled \checkmark		
1 - 1 of 1 records			Go to page 1 →		Records per page	10 ~
			BACK	ADD SERVER	DELETE SE	ERVER

• To disable the MQTT connection, select **Disabled** from the connection drop down list.

MQTT					
Configuration Servers & Topics Se					
Select Server Type					
S :					1 a
SERVER NAME	IP/HOSTNAME	PORT NUMBER	CONNECTION STATUS	CONNECTION	ACTIONS
∽ □ Test	192.168.1.10	8883	Disabled		
1 - 1 of 1 records			Go to page $1 \rightarrow$		Records per page 10 ~
			BACK	ADD SERVER	DELETE SERVER

9. To delete the server, select the server and click **DELETE SERVER**. Delete Server will delete the server configuration and all the topics configured for the server.

Note: Ensure the connection is disabled before deleting the server and deletion of multiple servers also supported.

MQTT					
Configuration Servers & Topics S					
SERVER NAME	IP/HOSTNAME	PORT NUMBER	CONNECTION STATUS	CONNECTION	ACTIONS
∽ □ Test	192.168.1.10	8883	Disabled	Disabled ~	
		1 > H	Go to page $1 \rightarrow$		Records per page 10
			ВАСК	ADD SERVER	DELETE SERVER

10. A pop -up window appears for the confirmation, click **DELETE**.

		×
Delete	Server	
	lelete the selected servers? a me : Test	
CANCEL	DELETE	

Configure MQTT Topics

1. To add topic for a particular server, click (^) and then click Add Topic.

Note: Two topics with same name and same type cannot be added.

MQTT					
Configuration Servers & Topics Se					
Select Server Type					
□• S !					⊞ ‡
SERVER NAME	IP/HOSTNAME	PORT NUMBER	CONNECTION STATUS	CONNECTION	ACTIONS
Test	192.168.1.10	8883	Connected	Enabled ~	Ø
					IDD TOPIC DELETE TOPIC
1 - 1 of 1 records	н 4 🔤	.) N	Go to page 1 → BACK	ADD SERVE	Records per page 10 V

2. Enter the details in **Add Topic** Window as given below.

- Server Name: Server name cannot be edited.
- **Topic Name**: Select the topic name based on the nine predefined topics and type.

Topic Name	Торіс Туре		
RTLS_TELEMETRY	Publish		
RTLS_ANCHOR_CONFIG_WDM	Subscribe		
WDM_ANCHOR_CONFIG_RTLS	Publish		
RTLS_TAG_CONFIG_WDM	Subscribe		
WDM_TAG_CONFIG_RTLS	Publish		
WDM_TAG_CONFIG_WDM	Publish or Subscribe		
RTLS_ALARM	Publish		
RTLS_ DISTANCE	Publish		
RTLS_ DISTANCE	Subscribe		

- To publish tag telemetry data to Broker, select the topic name as **RTLS_TELEMETRY** and type as **Publish**.
- LWT QOS (Quality of Service): Can be configured between QOSO, QOS 1, and QOS2, where QOS2 is for best quality for transmission of respective topic data.
- **Retain Last Message**: Can be selected as **Yes** or **No.** If the retain message is configured as **Yes**, whoever subscribes to this topic receives the latest message from the broker on subscription.

	Add Topic
Server Nar	ne *
Topic Nam	e *
RTLS_TEL	emetry ~
Publis	h 🔘 Subscribe
LWT QOS	
QOS1	~
Retain Las	t Message 🔹 🔘 Yes 🚫 No
Indicates r	equired fields

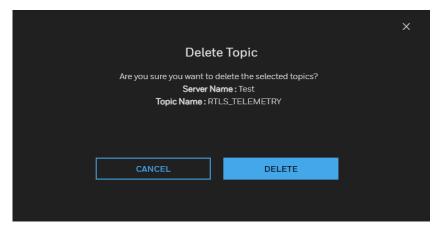
- 3. Click Save.
- 4. To edit the existing Topic, click on **Edit** under **Actions**.

MQTT						
	Servers & Topics Server S					
	Type					
□• S						\$\$ ⊞
s	SERVER NAME	IP/HOSTNAME	PORT NUMBER	CONNECTION STATUS	CONNECTION	ACTIONS
		192.168.1.10	8883	Connected	Enabled ~	
	Topic Name	Туре	Pub/Sub	QOS	RetainLastMessage	Actions
	RTLS_TELEMETRY	Fixed	Publish	QOS1		Ø }
					ADI	D TOPIC DELETE TOPIC
1 - 1 of 1 record			1 * M	Go to page 1 → BACK	ADD SERVER	Records per page 10 ~

- 5. Enter the details in **Edit Topic** Window as given below.
 - Server Name: Server name cannot be edited.
 - **Topic Name**: Select the topic name based on the four predefined topics. For tag telemetry data, select topic name as **RTLS_TELEMETRY** topic.
 - Topic type can be selected between **Publish** and **Subscribe**. For publishing **RTLS_TELEMETRY** topic data, select **Publish**.
 - LWT QOS (Quality of Service): Can be configured between QOSO, QOS 1, and QOS2, where QOS2 is for best quality for transmission of respective topic data.
 - **Retain Last Message**: Can be selected as **Yes** or **No.** If the retain message is configured as **Yes**, whoever subscribes to this topic receives the latest message from the broker on subscription.

		Edi	t Topic		
Server Nam	e *				
Topic Name					
RTLS_TELE	METRY				
Publisł	- O	Subscribe			
LWT QOS					
QOS1					
Retain Last	Message *	Yes			
Indicates re	quired fields				
		NCEL		SAVE	

- 6. Click Save.
- 7. To edit or delete Topic, server connection must be in **Disabled** state.
- 8. To delete the existing Topic, select the Topic and click **DELETE TOPIC**.
- 9. A pop -up window appears for the confirmation, click **DELETE**.



Monitoring MQTT statistics

Server Statistics

MQTT Statistics provides the following information:

General Statistics	Description
Total Number of Connections	Total number of configured MQTT Server
Number of Enabled Connections	Total number of configured MQTT Server which are enabled.

General Statistics	Description
Number of Active Connections	Total number of configured MQTT connections which are successfully connected.
Number of Inactive Connections	Total number of configured MQTT connections which are in disconnected state.

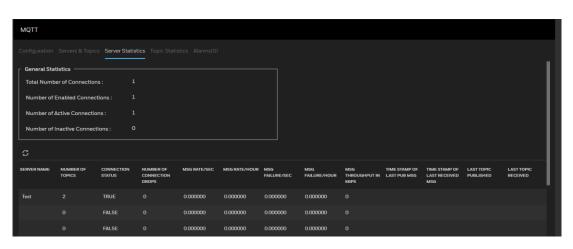


Fig. 26. Server Statistics

SERVER NAME: Name of Each Server.

NUMBER OF TOPICS: Total Number of Topics for each server.

CONNECTION STATUS: Status of Each Server. It will show "TRUE" if it is connected to Broker or else it will show "FALSE".

NUMBER OF CONNECTION DROPS: Total Number of times server is disconnected.

MSG RATE/SEC: Average rate of Publish and Subscribed messages per Second for each server.

MSG RATE/HOUR: Average Success rate of Publish and Subscribed messages per Hour for each server.

MSG FAILURE/SEC: Average Failure rate of Publish and Subscribed messages per Second for each server.

MSG FAILURE/HOUR: Average Failure rate of Publish and Subscribed messages per Hour for each server.

MSG THROUGHTPUT IN KBPS: Total length of Published and Subscribed message for each server.

TIME STAMP OF LAST PUB MSG: Time stamp of Last Published Topic for each server.

TIME STAMP OF LAST RECEIVED MSG: Time stamp of Last Subscribed Topic for each server.

LAST TOPIC PUBLISHED: Topic name of the latest published topic for each server.

LAST TOPIC RECEIVED: Topic name of the latest Subscribed topic for each server.

NUMBER OF INVALID TOPIC MSG RECEIVED: Msg received from invalid topics for each server.

Topic Statistics

MQTT								
Configuration Servers & Topics Server Statistics Topic Statistics Alarms(0)								
S								
SERVER NAME	TOPIC NAME	TOPIC TYPE	MSG RATE/SEC	MSG RATE/HOUR	MSG FAILURE/SEC	MSG FAILURE/HOUR	MSG THROUGHPUT IN KBPS	TIME STAMP OF LAST PULASUB MSG
Test	RTLS_TELEME	TRV2	0.000000	0.000000	0.000000	0.000000		
Test	RTLS_ANCHOR	CØNFIG_WDM	0.000000	0.000000	0.000000	0.000000		
			0.000000	0.000000	0.000000	0.000000		
			0.000000	0.000000	0.000000	0.000000		
			0.000000	0.000000	0.000000	0.000000		
			0.000000	0.000000	0.000000	0.000000		
			0.000000	0.000000	0.000000	0.000000		
		0	0.000000	0.000000	0.000000	0.000000	0	

Fig. 27. Topic Statistics

SERVER NAME: Server Name for each topic.

TOPIC NAME: Name of the Topic.

TOPIC TYPE: Topic Type either Pub/Sub. It will display "2" for Pub and "1" for Sub.

MSG RATE/SEC: Average rate of Publish and Subscribed messages per Second for each Topic.

MSG RATE/HOUR: Average Success rate of Publish and Subscribed messages per Hour for each Topic.

MSG FAILURE/SEC: Average Failure rate of Publish and Subscribed messages per Second for each Topic.

MSG FAILURE/HOUR: Average Failure rate of Publish and Subscribed messages per Hour for each Topic.

MSGTHROUGHTPUT IN KBPS: Total length of Published and Subscribed message for each Topic.

TIME STAMP OF LAST PUB/SUB MSG: Time stamp of Last Published or Subscribed Topic.

Administration

Administering users

About users and user roles

The WDM enables you to define user-specific settings by creating user accounts with the required user roles. The following are the user roles defined by the WDM.

- Administrator Authorized to manage the user accounts. Users with user role as administrator can add, delete, or modify user accounts, change existing user's role, change password for the existing users, upgrade firmware, and provision the infrastructure nodes. Only a user logged on with Administrator role has the ability to provision and upgrade a WDM.
- View Only Authorized only to read/view the device parameters and export the system logs, alarm and event logs, and the reports.
- Instrument Tech Authorized to configure operating mode for the field device channels and provision only the field devices. This role also has privileges to enable/disable write protection for the field devices.

By default, the WDM is configured with an administrator account. You can create multiple user accounts and assign the user role, as required. Users with Administrator role can create new users, delete users, change existing user's role, and reset password for the existing users.

The following table summarizes the default role-based access privileges enforced by the WDM for performing different operations. Note that a user logged on with Administrator role can override the default privileges, except for the operations that are grayed out in the following table.

Function	View Only	Instrument Tech	Professional Installer	Administrator
Read	Y	Y	Y	Υ
Upload DD	N	Y	N	Y
Calibrate Device	N	Y	N	Y
Instantiate/Delete Channel	N	Y	N	Y
Delete Device	N	N	N	Y
Provision Field Device	N	Y	Ν	Y

Table. 19. Default role-based access privileges

Function	View Only	Instrument Tech	Professional Installer	Administrator
Provision FDAP or Wireless Infrastructure Node	N	N	N	Y
Configure Device Publication	N	Y	Ν	Y
Replace Device	N	Y	N	Υ
Upgrade Device	N	N	N	Y
Device Write	N	Y	Y	Y
Write Protect Device	N	Y	Y	Ν
Channel In/Out of Service	N	Y	Y	N
Download Support Software	N	Y	N	Y
Export Logs/Generate Reports	Y	Y	Y	Y
User Management	N	N	N	Y
Configure WDM Backup	N	N	N	Y
Provision WDM	N	N	N	Υ
Configure WDM Network Settings	N	N	N	Y
Configure Transmit Power Level	N	N	Y	N
Data Change Allowed	N	Y	Y	Y
Enable WDM Developer Mode	N	N	Y	N
Field Expandable Wireless IO	N	N	Y	Y

TX power level can be configured for Honeywell devices only.

The Provision WDM function also enables you to configure the redundant related parameters. ATTENTION

Į.

Create user accounts

To create user accounts

- From the Left Navigation Menu bar, click System > Manage Users. The Manage Users window appears.
- 2. Click Add New User.
- 3. In the Manage Users window, provide the user name, password and role.

Manage Users Authorized to manage	ge the user accounts. Users with user role as admini	strator can add, delete, or modify user accounts, change existing user's role, ch	ange password for the existing users.	
Search by usern	ame or role Q			ADD NEW USER
USER NAME	ROLE	User Name *	Role *	
administrator	Administrator		Select Role	^
test	Administrator	Password *	Confirm Password *	
prof	Prof Installer			
Shafana	Administrator			
Admin	Administrator			
*Indicates required t	fields		CLEAR	SAVE

4. Click Save.

Edit user account

To edit user account

- From the Left Navigation Menu bar, click System > Manage Users. The Manage Users window appears.
- 2. From the list of users on the **Users** pane, select the user account to edit and click the **Edit** icon.
- 3. Edit the required account details, and then click **Save**.

Delete user account



Note that you cannot delete the default user account (administrator) configured by the WDM.

To delete user account

- From the Left Navigation Menu bar, click System > Manage Users. The Manage Users window appears.
- 2. From the list of users on the **Users** pane, select the user account to delete, and then click **Delete** icon.
- 3. Click **Delete** in the confirmation dialog box.

If you logged on simultaneously using the user account that you want to delete, then it is automatically logged off.

Change password

To change your own password

- Click Change Password from the top-right corner of the Home page. The Change User Password window appears.
- 2. In the **Current Password** box, type the current password and in the **New Password** and **Confirm Password** boxes, type the new password.
- 3. Click **Save.** The message Password has been successfully changed appears.
- 4. Click Cancel to close the Change User Password window.
- 5. Restart the Web browser and log on to the user interface using the new password.

Reset password

If you are logged on to the user interface with administrative privileges, you can reset the password of any user. For example, using an administrator account, it is possible to reset the password for a user who has forgotten the password.

To reset the password of any user

- From the Left Navigation Menu bar, click System > Manage Users. The Manage Users window appears.
- 2. From the list of users on the **Users** pane, select the user account for which you need to reset the password and click the **Edit** icon.
- 3. Type the new password in the **Password** and **Confirm Password** boxes.
- 4. Click Save.

Change user role

() ATTENTION

Note that you cannot change the user role for the default user account (administrator) configured by the WDM.

To change user role

- From the Left Navigation Menu bar, click System > Manage Roles. The Manage Roles window appears.
- 2. From the list of users on the **Users** pane, select the user account for which the user role needs to be changed.
- 3. Click the appropriate user role in the **Select User Role** list.
- 4. Click Save.

The user account is modified with the new user role. If you have logged on using the user account whose role is modified, then that user account is automatically logged off. You must log on to the system again.

Manage user roles

Roles Administrator role can create new u	isers, delete users, change existing us	er's role, and reset password for the existing users.			
Search by role	Q			ADD NEW ROL	
ROLES View-Only	_	Functions Creating user accounts with the required user roles.			
Instrument Tech					
Prof Installer					
Administrator					
IMPORT	EXPORT	Export Logs/Generate Reports	User ManaQleEnAARt	SAVE	

To add a new user role:

- From the Left Navigation Menu bar, click System > Manage Roles. The Manage Roles window appears.
- 2. Click Add New Role.

A new column is added to the list of users. The new user name is added as **New Role x** (x is the number of user being created). You can edit the name of the user role.

3. Click **Save**. A new user role is created.

To delete user roles:

1. From the Left Navigation Menu bar, click **System > Manage Roles.** The **Manage**

Roles window appears.

2. Select the role that to be deleted and click the **Delete** icon.

Roles		
Search by role Q		
ROLES		
View-Only		
Instrument Tech		
Administrator		
test5		
wesrwe	0 🖬	

A confirmation dialog appears, click **OK** to delete the role.

To import user roles:

- From the Left Navigation Menu bar, click System > Manage Roles. The Manage Roles window appears.
- 2. Click **Import** and browse to the xml file which contains the user roles to import. Click **Open**. All the user roles are imported to the existing WDM.
- 3. Click Save.

To export user roles:

- From the Left Navigation Menu bar, click System > Manage Roles. The Manage Roles window appears.
- 2. Click Export.
- 3. Browse to the location to save the existing user role information in an xml file.
- 4. Click Save.

Downloading support software

The Software Download option enables you to download software provided on the WDM.

To download support software:

 From the Left Navigation Menu bar, click System > Software Download. The Software Download window appears.

- 2. From the **Select Software** list, select the required software to be downloaded. The following software can be downloaded.
 - **Provisioning Device Application**: The Provisioning Device Application is a Windows Mobile PDA application that allows you to transfer network configuration and security keys from your WDM to your access points and field devices.
 - **OPC UA Proxy**: The OPC-UA Proxy is used to connect OPC-DA clients to the OPC-UA server running on your WDM.
 - Modbus Configuration Backup: The Modbus Configuration Backup is the running configuration of the Modbus interface, which includes all the points configured in input, coil, holding and discrete registers. This configuration can be restored using Templates under Maintenance from the Left Navigation menu Bar.
 - Secure Communication Software: The Secured Communication software is required to configure secure communications between the windows nodes and redundant WDM. Network Layer security is provided by employing IPSEC policies. For more information on Secure communications, see the *Wireless Device Manager Secure Communication Guide (OWDOC-X584-en).*

The Secured Communications software can be installed by following steps:

- 1. Save "SecureCommunication.msi" to your PC
- 2. Using your PC, open Windows Explorer and navigate to "SecureCommunication.msi". Click on MSI file
- 3. Follow on-screen prompts
- Android Provisioning Device Application: This application is developed to provision ISA100 and WirelessHART devices using an Android mobile phone or a tablet. It allows you to transfer network configuration and security keys to your access points and field devices. It also allows you to read identification and network state parameters directly from any device. It uses Bluetooth to communicate with access points and field devices

The Android Provisioning Device Application can be installed by following steps:

- 1. Save Android ProvDev.apk to your Android device.
- 2. Using your Android device, open File Explorer and navigate to AndroidProvDev.apk. Click on the apk file to start installation.
- 3. Follow any on-screen prompts
- 4. Click **Download** to download the software to the computer.

- HART DD to XML Converter: A windows-based tool to Change the HART channel names and convert the HART DD to XML. The HART DD to XML converter can be installed and used by following these steps:
 - 1. Save DDToXMLConverter.exe to your PC.
 - 2. Using your PC, open windows Explorer and navigate to DDToXMLConverter.exe.
 - 3. Click on the DDToXMLConverter.exe to open the application. Select the HART DD file through browse option provided by this application.
 - 4. Change the channel names (PV,SV,QV,TV) as per the user needs and click on the convert option. ZIP file will be created in the same location of the exe file.
 - **5.** This ZIP file can be loaded into WDM using the Template upload option in UI in order to modify the channel names of those particular HART device models.

Note: Use this application only in case you wanted to change the channel name of the WirelessHART devices.

Upgrading device firmware

	Firmware upgrade is supported only on ISA 100 devices.
OTE	

The FDAPs/PCAPs and field devices have radio firmware that can be upgraded. Some field devices may have a separate application firmware, which handles the functioning of the sensor in the device. This can also be upgraded over the wireless network. For more information about upgrading the firmware of field devices, refer to the field device vendor's documentation. Honeywell field devices usually have separate firmware files for radio firmware and application firmware. FDAPs have only radio firmware.

The firmware can support ISA2009, 2011, and WirelessHART.

Considerations

The following are some of the considerations for upgrading the device firmware.

- You can upgrade only the application firmware or radio firmware of a device at a time.
- You can upgrade only the firmware of five devices simultaneously.
- Starting the radio firmware upgrade operation of lower hop and upper hop devices simultaneously, results in the failure of upgrade operation of the lower hop device. When the devices are in different hops, it is recommended to perform the upgrade of only one device at a time.

Upgrading the radio firmware of a device, which routes communication between other devices, results in communication failure as well as firmware upgrade failure.

Upgrading the WDM firmware

Download the latest WDM firmware file from the Honeywell Process Solutions website.

|--|

The steps for upgrading the WDM from R202 to R210, from R210 to R220 and then from R220 to R230. or 230 to 240, R240.2/R300.2 to R310, R310.x to R320.x , R320.x to R321.x and R321.x to R323.x are common.

Prerequisites

Ensure that the speed/duplex setting for the network adapter of the computer is set to Auto.

To upgrade the WDM firmware:

- 1. From the Left Navigation Menu bar, click **FIRMWARE UPGRADE.** The **Firmware Upgrade** window appears.
- 2. Click NEXT.
- 3. Select **WDM** and click **NEXT.**
- 4. Click **NEXT**.
- 5. Click **UPLOAD FIRMWARE FILE** to navigate to the directory location of the firmware file and click **Open**. The WDM firmware file has a *.tar.gz* extension.

Manual Firmware Upgrade Initiate manual firmware upgrade operation for the WDM, access points and radio firmware of the ISA100 Wireles	s field devices.		
[
WDM Once initiated, you cannot abort the firmware upgrade operation.	Available Firmware Package Files Upload the latest WDM firmware file fro	om the Honeywell Process Solution	ns website.
FIRMWARE FILE NAME	ACTION		
Firmware Package is not available. Please Upload.			
UPLOAD FIRMWARE FILE			NEXT

The **WDM Update** dialog box displays the upload status. Once complete, the Firmware File box displays the uploaded firmware file.

6. Click Update.

The firmware upgrade starts and once complete, the user interface displays a message indicating the result of firmware upgrade operation.

At times, the update may take longer than expected and the result of the upgrade may not be displayed. Instead, a "Page not available" error may appear. In such cases, wait for a minute and then redirect the browser to "https://<ipaddress>/restartzfs.html" for viewing the result. Do not remove or reboot the WDM during the upgrade process.

After the WDM upgrade is complete, the WDM reboots automatically.

- 7. Close and restart the web browser.
- 8. Log on to the user interface again.
- 9. Verify the upgraded version of the WDM firmware as follows:

- a. Click Manage devices from Left Navigation Menu bar.
- b. Expand Device Manager Summary from WDM property panel.
- c. Under Identification, verify the Revision.

Upgrading the FDAP/access point firmware

Download the latest FDAP/access point firmware files from the Honeywell Process Solutions website.

To upgrade the FDAP/access point firmware:

- 1. From the Left Navigation Menu bar, click **FIRMWARE UPGRADE.** The **Firmware Upgrade** window appears.
- 2. Click NEXT.
- 3. Select **Radio** and click **NEXT**.
- 4. Provide the **Device Type** and **Radio Model** and click **NEXT**.

	nual Radio Firmware Upgrac ates firmware upgrade operation for t						
A	Select Device Choose device from the list.		i lable Firmware Package Files ilable firmware upgrade files are listed.	C Firmware Upgrade St Displays the progress of		Summary Displays all device's firmware in	nformation.
Devi	се Туре	Radio Me	odel				
Acc	ess Point	V FDAP2					
	S						⊞ ≋
	TAG NAME	LOCATION	VENDOR	MODEL	DEVICE TYPE	REVISION	
	AP_0096	Default Map	Honeywell	FDAP2	Access Point	OW322.1-11.0	
1-1	of 1 records			Go to page $1 \rightarrow$		Devices per page	
					Ĩ	ВАСК	NEXT

- 5. Select the device from the selection list and click **NEXT**.
- 6. Click **UPLOAD FIRMWARE FILE** to navigate to the directory location of the firmware file and click **Open**. The FDAP firmware file has a .bin extension"

Manual Radio Firmware Upgrade Initiates firmware upgrade operation for the Radio			
Select Device Choose device from the list.	Available Firmware Package Files Available firmware upgrade files are listed.	C Firmware Upgrade Status Displays the progress of the upgrade.	Summary Displays all device's firmware information
FIRMWARE FILE NAME		ACTION	
HON_FDAP2_Rev1_R322.1.14.0.bin		â	
HON_FDAP2_Rev81_R322.1.14.0 bin			
UPLOAD FIRMWARE FILE		[BACK

7. In the Available Firmware Files list, select the required firmware upgrade file.

By default, the firmware upgrade file appears in the list. If the file is not available in the list, perform the following steps to open the firmware file.

- a. Click **UPLOAD FIRMWARE FILE** to browse to the directory location of the firmware upgrade file.
- b. Click Open.

8. Click Upgrade.

The **Firmware Upgrade Status** dialog box appears. The **Progress** column displays the progress of the upgrade.

Ma	nual Radio Firr	mware Upgrade						
\bigcirc	Select Device Choose device fro	om the list.	Available Firmware Available firmware listed.		C Bisplays the progr	t Status ess of the upgrade.	Summary Displays all d	evice's firmware information.
S								# %
TAG	NAME	LOCATION	VENDOR	MODEL	REVISION	STATUS	PROGRESS	ACTION
PD	_495_4CLL	Map4	Honeywell	2618_2420_01	OW322.1-41.0	Progress	0%	
								Þ
1-10	of 1 records	E			Go to page 1	BACK	D.	evices per page 10 ~
!			, firmware u he upgrade:		eration, clic	k the Abor	rt Upgrade	icon
ATTENTION	• To	remove th	ne devices fo	or which th	ne firmware	upgrade h	nas been	

completed, click the Clear Upgrade icon adjacent to the upgrade status.

- 9. Verify the upgraded version of the FDAP / Access Point firmware as follows:
 - a) Click Manage devices from Left Navigation Menu bar.

- b) Expand Device Manager Summary from WDM property panel.
- c) Under Identification, verify the Revision.

Upgrading the ISA100 Wireless field device firmware

The devices at the farthest hop level must be upgraded first.

To upgrade the field device firmware

Follow the same procedure in section *"To upgrade the FDAP/access point firmware"* for ISA100 Wireless field device firmware. Select **Sensor Application** instead of **Radio** in step 3.

Sensor Application firmware must be upgraded before upgrading the radio firmware.
To initiate the firmware upgrade of the HCI-1WL (CAN-1WL) board using the Application firmware, the SD card must be inserted in the HCI-1WL (CAN-1WL)

ATTENTION board. Also, the SD card should not be write protected.

Closing the dialog box allows the upgrade operation to run in the background. The upgrade status is displayed in the Notification list. Click the firmware upgrade notification to open the dialog box again. If multiple users are simultaneously upgrading different device firmware, all the users can view the progress of all the device upgrades.

While upgrading the application firmware of a field device, the LCD display of the field device displays the firmware upgrade status. The status is displayed until the upgrade operation completes or aborts.

Once the upgrade is complete, the status column displays the status as complete. If firmware upgrade fails for a device, you can abort the upgrade and start again. To abort firmware upgrade for individual devices, click **Abort** next to the status indicator.

HCI-1WL (CAN-1WL) Firmware upgrade takes more time due to the larger size of the firmware download. Ensure that HT link option is enabled before starting the firmware upgradation.
 Post completion of HCI-1WL (CAN-1WL) firmware upgrade, sometimes the upgrade status shows as failed. In such cases, Warm restart the device and the device rejoin with the updated firmware. This can be verified by checking the firmware version in the device ISA100 Device Summary.

Configuring system configuration backup

About system configuration backup

OneWireless user interface enables you to configure system backup on a FAT32 formatted USB drive connected to one of the USB slots in the WDM. The backup file created can be used to restore the system configuration to a new WDM, or a WDM that has been reset to factory defaults. System configuration can be backed up manually or WDM can be configured to automatically backup system configuration whenever a configuration change is detected. All system configuration data is included in the backup file created.

In automatic system configuration backup, a USB flash drive must be connected to the WDM at all times. If automatic backup is enabled and the USB flash drive is disconnected from the WDM, automatic backup stops and resumes when a flash drive is connected to the same slot on the WDM. If the disk space on the backup drive is insufficient, you can replace the disk with a new one without any backup configuration changes.

WDM state, ISA100 Wireless network state, WirelessHART devices, WDM configuration changes, user actions, external interface configuration changes, and device topology changes are monitored every five minutes to initiate an automatic system backup, when enabled.

Configure manual backup

The **Manual Backup** option enables you to back up the system configuration manually. This option is disabled when automatic backup is enabled.

You can back up the data on a USB flash drive or on a specified server.



For network backup, windows machine password must not contain space.

To configure manual backup:

- 1. Connect a FAT32 formatted USB flash drive to any one of the USB slots on the WDM. Alternatively, share a network drive on which you want the backed up data.
- 2. From the Left Navigation Menu bar, click **SYSYTEM > BACKUP SETTINGS.**
- 3. Select Backup Settings.

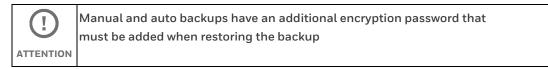
Backup Settings The backup file created can be used to restore	the system configuration to	a new WDM, or a WDM that has been reset to factory defaults.		
Select Property				
Remote Event Logging Select specific or all alarm/events from WDM t server (syslog-ng compatible server).		Backup Settings You can configure automatic system configuration backup to back up the system configuration automatically.		
Select Backup Method				
O Automatic Backup You can configure automatic system configure the system configuration automatically.		Manual Backup It enables you to back up the system configuration manually. This option is disabled when automatic backup is enabled.		
Latest Backup File NAME	SIZE	DATE	DESCRIPTION	
No Backup Taken	51212	UAIC	DESCRIPTION	
				NEXT

4. Under Manual Backup, the Destination drop-down list displays the USB slots (to which the flash drive is connected) and the Network Attached Storage. Select the required option.

Backup Settings The backup file created can be used to restore the system configuration to a new WDM, or a WDM that has been reset to factory defaults.						
r Manual Backup						
File Destination :	USB1 No Device Detected					
	USB1 No Device Detected					
	USB2 No Device Detected					
	USB3 No Device Detected					
	USB4 No Device Detected					
	Network Attached Storage (SMB)					
		ВАСК	RESET	BACKUP NOW		

- 5. If you select the Network Attached Storage (SMB) option, type the additional information.
 - **UCN Path**: Type the URL for the server location.
 - User Name: Type the user name to access the specified server.
 - **User Password**: Type the valid password.
- 6. Click BACKUP NOW.

The **Backup Status** dialog box displays the following information about the last successful backup.



- Name: Name of the backup file.
- **Size**: Size of the backup file.
- **Date**: Date and time of last backup.

• **Description**: The mode of backup configured (automatic or manual) and the USB drive/slot number where the backup file was created. It also displays any errors that occurred during a backup.

Configure automatic backup

You can configure automatic system configuration backup to back up the system configuration automatically. To configure automatic backup:

- 1. Connect a FAT32 formatted USB flash drive to any one of the USB slots on the WDM. Alternatively, share a network drive on which you want the backed up data.
- 2. From Left Navigation Menu bar, click SYSYTEM > BACKUP SETTINGS.
- 3. Select Backup Settings.

The **Destination** drop-down list displays the USB slot (to which the flash drive is connected) and the Network Attached Storage. Select the required option.

Backup Settings The backup file created c	an be used to restore the system configuration to	a new WDM, or a WDM that has	been reset to factory defaults.			
– Automatic Backup						
			15 Minutes			
File Destination :	USB1 No Device Detected	Frequency (for every):	15 Minutes	Status :	Auto Backup N	lot Configured
	USB1 No Device Detected					
	USB2 No Device Detected					
	USB3 No Device Detected					
	USB4 No Device Detected					
	Network Attached Storage (SMB)					
			BACK	RESE	T	APPLY
					·	

- 4. If you select the **Network Attached Storage (SMB)** option, type the additional information.
 - UCN Path: Type the URL for the server location.
 - **Username**: Type the username to access the specified server.
 - User Password: Type the valid password.
 - **Periodicity**: Select the required period.

The **Status** displays the current automatic backup status. Following are the different status values that are displayed.

- Idle when automatic backup is not in progress.
- In Progress when automatic backup is in progress.
- Error when an automatic backup fails.

- **No Device** when the backup device is not available on the destination USB slot even though backup is enabled.
- **Device Access Error** when an error is encountered while accessing the backup device on the destination USB slot.
- **Device Disk Space Low** when the disk space is low on the backup device.
- Auto Backup Not Configured when automatic backup is disabled.

The **Backup Status** displays the following details about the last successful backup.

- **Name**: Name of the backup file.
- **Size**: Size of the backup file.
- **Date**: Date and time of last backup.
- **Description**: The mode of backup configured (automatic or manual) and the USB drive/slot number where the backup file was created. It also displays any errors that occurred during a backup.

Restoring the system configuration from a backup

See section <u>Restore from Backup</u> for more information.

Control over wireless using OneWireless

Traditionally, industrial plants are use wireless technology for monitoring applications not for control or safety due to wireless technology being a shared medium prone to interference attacks.

OneWireless System has been designed considering these interferences, security, high reliability, redundancy and guaranteed latency. These qualities of the OneWireless system makes it suitable for control applications.

Typical OneWireless systems can be used for the following control applications such as Temperature, Pressure, Tank Level control, Loading/Down-loading gantry.

Туре	Class	Type Based on Industry	Recommendation
	1	Closed loop Regulatory Control (Critical control loops)	Not Recommended
Control 2 3	2	Closed Loop Supervisory Control (Set Point Change, Process Optimization)	Recommended
	3	Open Loop Control (Based on Requirement/ Operator In-Person)	Recommended
Monitoring	4	Event Action/ Sequence based (Based on Event /Small operation task)	Recommended
worntoring	5	Uploading/Downloading (Requirement based Task/ Action)	Recommended

Recommendation / Suitable control type for OneWireless system.

Deployment Topology:

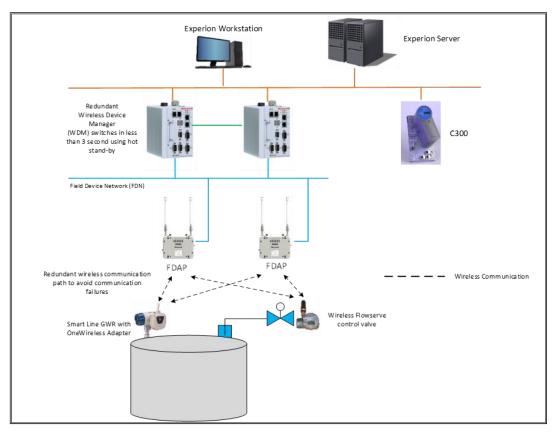
It is important to follow proper deployment rules for installing wireless devices for control applications to achieve the performance requirement needed.

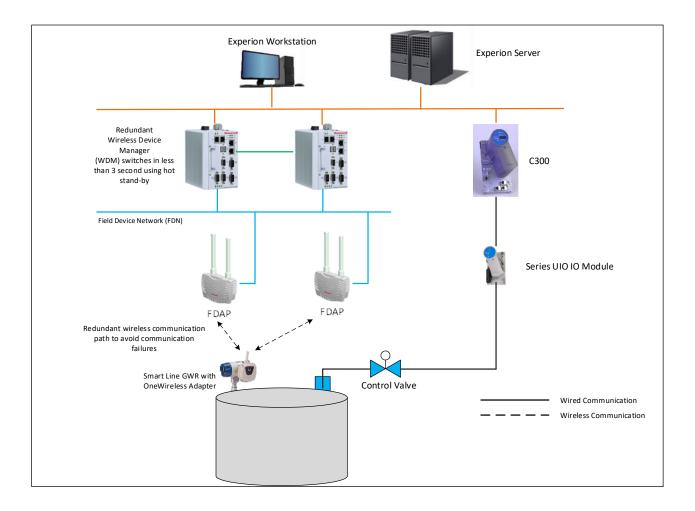
Wireless devices are installed at site based on their initial survey to ensure reliable communications with each device through redundant network connectivity, at least two communication paths are needed for each device from a wireless gateway. Each communication link must be good.

The deployment topologies depend on the control loop latency requirements. Single deployment topology does not work for all types of control loops. OneWireless system supports two types of topology based on the control loop latency/response time.

Topology for 1 sec or faster loops

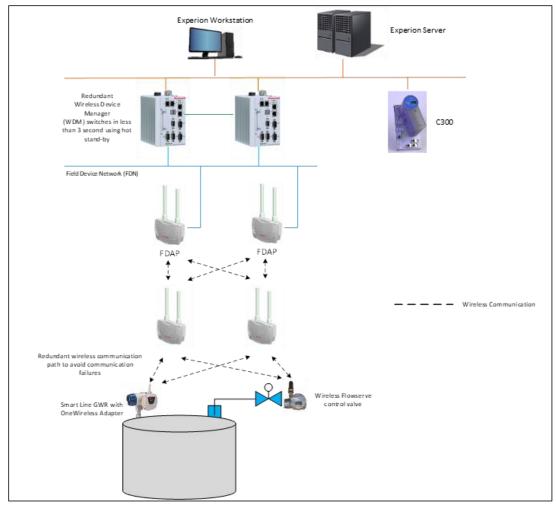
Wireless device deployments are completely based on loop criticality or data update to control system. 1 sec or faster (500 msec) update rates are difficult to achieve over a multi-hop mesh network due to routing delays. For such response times, it is recommend to deploy wireless devices communicating directly to FDAP instead of going through a mesh network. The following figures show such topologies. Figure 1 shows both the measuring element and control element are wireless; Figure 2 shows measuring element is wireless and control element is wired to the control system.





Topology for 4 sec or above loops

Wireless device deployments are completely based on loop criticality or data update to control system. 4 sec or above update rates are achievable over a multi-hop mesh network. The following diagram shows one such topology.



Sending control commands to WirelessHART devices

Any WirelessHART device variable command can be written to the device. WirelessHART device variable command can be Read or Write through Modbus and OPC interface. Two Wireless HART device variable commands can be written parallelly.

OneWireless system can send control commands through **Data Read and Write functionality** in Wireless HART.

Elements	Description
Command number	2 byte
	Need to enter the command number in decimal format
Req data length:	1 byte
	Need to enter the command number in decimal format
Read Req Bytes:	initially this is blank, you can enter whenever sending request, it must be in hexadecimal format
	for example, if you need to enter 0x01, 0xf2 then you need to enter 01f2.
Response status	success or failure status
Res data length	Number of bytes of response data
Read sync time:	time by when the WDM get response from WirelessHART device
Read command:	only read parameters
Write command:	to write parameters for WirelessHART
Read Response	It is a hexadecimal string
	Read response is updated when it has response data length
Write Response	It is a hexadecimal string
	Write response is updated when it has response data length
Write device variable 1	You can write device variable of wireless HART provided the respective device variable is in input mode
Write discrete variable 1	You can write discrete variable

Data Read and Write
Read Command
Command number : 0
Req Data length : 0
Read Request Bytes :
Response Status : 0
Res Data length : 0
Read Response data :
Read Sync time :
Write Command
Command number : 0
Data length : 0
Data :
Response Status : 0
Response Length : 0
Write Response data :
Write Sync time :
Write Device Variable1
Code : 0 V
Command Code : Normal, Non-Simulation Mode 🗸 🗸
Value : nan
Units : Unknown V
Response Code : 0 Response Length : 0
Response Lengtri : 0 Response Data Bytes :
Last Sync time :

Write Device Variable2	
Code : 0	
Command Code : Normal,	Non-Simulation Mode V
Value : nan	
Units : Unknow	n 🗸
Status : Bad, Not	: Limited 🗸 🗸
Response Code : 0	
Response Length : 0	
Response Data Bytes :	
Last Sync time :	
Write Discrete Variable1	
Index : 0	
Value : Off	
Status : Simulati	
Response Code : O	
Response Length : 0	
Response Data : Last Sync time :	
Last sync time :	
Write Discrete Variable2	
Index : 0	
Value : Off	
Status : Simulati	on Mode 🗸 🗸
Response Code : 0	
Response Length : O	
Response Data :	
Last Sync time :	

Control over wireless using OneWireless integrated with Experion

Wireless control can be implemented using PID OR PID Profit Loop (PID-PL) blocks in Experion by integrating the wireless data from OneWireless to Experion either through CDA/Modbus.

Honeywell OneWireless is tightly integrated with Experion PKS system. See the *OneWireless Experion PKS Integration Guide* for more information.

PID - Profit Loop

Honeywell's patented algorithm that represents a SISO (Single Input Single Output) -Profit Loop PKS Control Algorithm belongs to a class of controller known as "Model Predictive control". These controllers rely on a dynamic model to predict future movement in the process variable. If this predicted PV does not meet the control objectives [maintain a set point], control action is taken to realign the PV with its objectives and can increase process stability.

By definition, PID Profit Loop offers advantages over the traditional PID control techniques.

Features: Range and Dual Range control, handles complex dynamics, Predictive alarming, Handles Asynchronous PV input & Profit Loop Assistant

- Profit Loop Assistant can be launched from Point detail page
- Modeling wizard
 - Model by loop type
 - Model from loop tuning
 - Model by step testing
 - Model by direct entry

See the PID-PL document.

In contrast, a PID controller uses past and current error trajectories to restore the PV to its SP within one control move, regardless of the long-term consequences of the move.

Using Wireless transmitter for control applications, control strategy must compensate for Asynchronous measurement updates. PID-PL has a configuration where it handles the Asynchronous Process value updates. Configuring "OnPVChange" makes sure PID PL handles the non-continuous measured values through wireless. Below figure shows the Asynchronous mode configuration required for wireless control using PID-PL.

Config	uration Parameter	rs	Monitoring Par	ameters	s Block Preference		Template	e Defin
Main	Algorithm	SetPoint	Output	Advanced	Alams	SCM	Identification	De
/odel				Optin	nization			
Transfer				Ontin	mizer Mode:	[OPTTARGE V	
Numerat	or Coefficients:	Denomin	ator Coefficients:			L.		
# 1	s^0: 1	# 2	s^0: 0	Opti	mizer Speed:	l	2	
	s^1:		s^1: 1	SPO	Offset-			
	s^2:		s^2:		Low Limit:	r	0	
	s^3:		s^3:		High Limit:	L	0	
	s^4:		s^4:		riigir cinit.	L	•	
				OP	Offset-			
Process	Gain (% / %):	0.2111099						
					Low Limit:	l	0	
Deadtim	e (minutes):	0.3333333			High Limit:		0	
L	Jpdate Model		Reset Model	PVC	onfiguration			
				Asyr	- nch PV Option:	[OnPvChange 🗸	
Attributes							Continuous	
	, Gain Units:	* PV	/%OP	~			ExternalSync OnPvChange	
11000000	cidin Onics.	Yet V.	/ 401	~	Ch-	rt Assistant	on ronongo	

Control Over Wireless Network- Wireless Input & Output device variables are dependent on Wireless Network, Signal Quality or Device placement and so on. The following are the details of both parameters that are handled by Profit Loop.

Wireless Input device delayed in receiving PV: Wireless process variable (Input) Communication fail OR Input Device Drop, Profit loop Model optimizes the impact based on process configurations set for the loop. Once wireless PV restore it continues. Control actions have minimal impact (No such abrupt valve movements) as output is being corrected based on PID-PL model.

Stale limit on wireless input must be configured where in case of any wireless communication failure last good value are sent or used for the configured stale limit. Have 1 to 120 Seconds of stale configuration available in OneWireless

Wireless Output: Wireless Output device delay in writing output (Valve Output)-

Control loop operation, if any wireless Output Write communication fails OR Device Drops, PID PL block output goes to defined fail safe state which is based on engineering solution in control strategy.

Fail safe state in wireless output device:

For additional safety to Device / Process operation User must configure failsafe value on Wireless Output device to ensure complete safety of process / plant.

Wireless control loop example using PID-PL in Experion

PID-PL block: Used for actual control with Measured value from wireless transmitter is been connected to the PV pin of PID-PL loop and SP configured to the required setpoint value. The OP pin is connected to the AUTOMAN block and then through SWITCH block is finally written to the wireless transmitter through a PUSH block.

PUSH block: Used where the Wireless output value from PID-PL is pushed from controller to wireless gateway which writes the value to the device. Failure in writing to device through wireless gateway can be detected based on the STORESTS and LASTSTORESTS flag of this block.

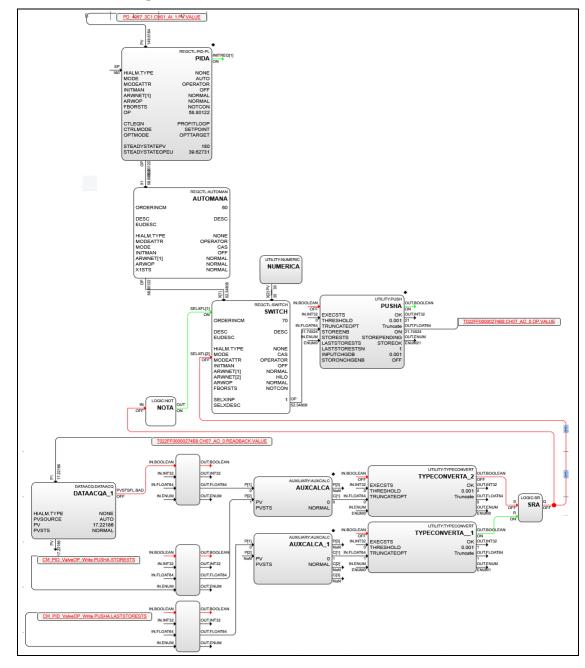
DATA ACQA block: Used to detect if there is any failure in communication from Output device to controller or any BAD process value from the output device. This can be used if we have a readback value available for the output device.

AUXILIARY CALCULATION(AUXCALCA) blocks: Used where logic is written such that a flag has been raised if either push blocks OP write failure or Readback of Output device failure is triggered. This flag is linked with SWITCH block such that it triggers failover and back initializes PID-PL block through AUTOMAN block. Such that control loop can be sent to failover state in case of communication failure.

The following example shows where failsafe is detected based on any disruption of wireless output readback or when wireless output cannot be written to the device, due to device disconnected from wireless or device is in configuration state.

ISA100 Wireless DP Level Transmitter: PD_4097 is pressure device and which is used to detect the level of the tank. The PV of this device is connected as the input of PID-PL block

ISA100 Wireless Flow Serve PMV D3 Positioner Valve: T022FF00000274B8 is the valve and the PID-PL output is finally driving the position of this value.



Control over wireless using both input and output transmitters are wireless

Tank Level Control Over Wireless (Test Results)

Measuring Elements (PV): Differential Pressure Transmitter for level – XYR6000 (ISA100 Wireless)

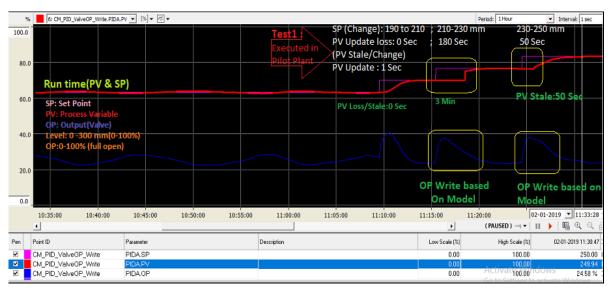
Control Element (OP): Flowserve PMV D3 Positioner with Valve assembly- ISA100 Wireless

Control System: EPKS R510.1 with C300 Controller

WDM: OW320 Release; Setup: 2 FDAP, 2 LPFR, 6 FDs

• Test

- Set Pont/Process Operational Run Time (Packet loss OR PV Stale :0) –
- SP change: 190 to 210 mm (Packet Loss or PV Stale: 0) –
- SP Change: 210 to 230 mm (Packet Loss OR PV Stale: 180 Sec) OP Write as per Model
- SP Change: 230 to 250 mm (Packet Loss OR PV Stale: 50 Sec)- OP Write as per Model and Once PV resumed it continued OP write, No impact on loop.



ISA Secure Level1 Certification

WDMY model with R320 release as passed the ISASecure EDSA Level1 certification.



Certificate / Certificat

Zertifikat / 合格証

HPS 1808036 C001

exida hereby confirms that the

Wireless Device Manager

Manufactured by

Honeywell Process Solutions Phoenix, Arizona USA

Has been assessed per the relevant requirements of: ISASecure [™] Embedded Device Security Assurance Program 2.0.0 And meets the requirements for: SECURITY LEVEL 1

WDMY

Model Number:

System Software Version: R320



William MK

Authorized Representative

Secure Communications

For more information on Secure communications, see the Secure Communication Guide (OWDOC-X584-en).

Troubleshooting and maintenance

Replacing devices

You can replace a failed FDAP, Access Point, or a field device with a new device. Replace operation restores all the configuration information to the new device. This includes the position of the device on the map, device name, channel names, publication, configuration, and so on. Note that device notes from a failed device are not restored to the new device.

Considerations

- A failed device can be replaced with a new device, only if the new device specification is identical to the failed one.
- Device role must be identical for the devices that are undergoing replacement operation. That is, a field device can be replaced only with a field device and a routing field device can be replaced only with a routing field device.
- Device to be replaced must not be part of another replacement operation.
- For FDAP and field device, the radio vendor and radio model of the failed device and the new device must be identical.
- For field devices, the application vendor and application model of the failed device and the new device must be identical.
- For field devices, the number of channels and the channel types of failed device and the new device must be identical.

Prerequisites

- Ensure that the failed device is offline and that it is not deleted.
- Ensure that the new device's tag name, type, radio vendor, and radio model is read by the WDM.
- Ensure that methods are not running for any of the channels of the new field device.
- Ensure that new device's firmware is not undergoing any upgrade operation.
- Ensure that new device's channels have been read by the WDM.

To replace devices:

- 1. Provision the new device to allow it to join the network.
- 2. Perform one of the following:
 - For replacing a field device with instantiable channels, verify that the new

device's instantiable channels are identical to that of the failed device.

Or

- If not, perform channel instantiation to make the channel configuration identical to the failed device. For more information, see the section **"Configure channel instantiation**".
- 3. To replace a field device, set the channel to OOS mode as follows:
 - a. From the Menu bar, select the field device channel.
 - b. Expand **Mode** in the Property Panel.
 - c. In the **Target** list, click **OOS** and then click **Apply**.

The channel icon appears as blue indicating the OOS mode.

- 4. On the Selection Panel, select the newly added device.
- Drag the new device icon and drop it on the failed device on the map. The Device Replacement dialog box appears.
- 6. Click Replace failed device <device name> with <new device name>.
- 7. Click **OK**

The **Device Replacement Status** dialog box appears indicating the progress of replace operation. The status bar also displays the status. If you close the **Device Replacement Status** dialog box, click the **Device replacement in progress** pane in the status bar to open the dialog box.

8. After the device replace operation is complete, the **Device Replacement Status** dialog box displays the result.

If a device replace operation completes with errors, it implies that one or more attributes of the device is not restored successfully. In this case, manually inspect the device and channel configuration from the Property Panel and correct any incorrectly configured attribute.

9. Click **Clear List** to clear the list of device replace operations.

Removing devices

You can remove a failed device from the network. A device that is removed can rejoin the network only if it is assigned a new provisioning key.

Considerations

- Removing an online device resets the device configuration to factory defaults. This results in the loss of provisioning data from the device.
- Removing an offline device makes the security information of the device invalid, but retains the provisioning data in the device. Though the device retains the provisioning data, it must be authenticated again to allow it to join the network.

To remove a device:

1. On the Selection Panel, select the devices that you want to delete.

If you are deleting an online device, change the channel mode to **OOS** for all the channels.

2. From the Menu bar, select **Provisioning** and select **Delete Devices** and click **Next**.

Provisioning			
Select OTA Provisioning			
Access Points Access points can be provisioned using over-the-sir provisioning method.	SAL00 Devices SAL00 Weekees devices and Access paints as nuters can be provisioned using sam-the- air provisioning method.		
Select Common Join Key Provisioning	Select PDA Provisioning		
O ISA100 And WiredessHART Devices WirelessHART and EA100 devices can be provisioned using Common Join Key method.	O Download Keys SALCO and WindowsHART devices can be provisioned using provisioning devices.		
Delete WDM or Devices			
O Delete WDM Delete WDM will reset the WDM to factory configurations.	Delete Devices Delete the devices from WOM and reset the device to factory configurations.	O Delete PDA Devices Delete the PDA devices from WDM	
		BACK	NEXT

3. Select the device you need to delete and click **Delete**.

Delete Devices				
Select 🗸				
• C Total Devices Selected (1)				≡ ≇
	DEVICE TYPE	STATUS	PROGRESS	
2308_GWR_TX	WirelessHART(R)	Offline	Not Started	
AP_0096	Access Point	Jained	Not Started	
C0_475_3F_6FLR	ISA100	Joined	Not Started	
EML_64C4A_5FL	WirelessHART	Offline	Not Started	
D FDAP2_R320_FB03	Router	Joined	Not Started	
LPFR_0041	Router	Joined	Not Started	
□ P0_573	ISA100	Joined	Not Started	
TD_1010_4J_6FLR	ISA100(R)	Joined	Not Started	
TD_1049_7F_5FLR	ISA100	Joined	Not Started	
1 - 9 of 9 devices		Go to page $1 \rightarrow$	Devices per pa	age 10 V
			BACK	DELETE

4. Click **Delete** when the confirmation dialog appears..

Resetting/removing WDM

Like any other device, you can reset/remove a WDM using the **Delete Selected Device** icon on the Property Panel. Resetting or removing WDM is possible only if WDM sync is disabled. Resetting the WDM removes all the system and configuration data and resets the WDM to factory defaults.



This operation results in significant changes in the system configuration. Honeywell recommends you to perform this operation only when there is a definite requirement.

To delete/reset a WDM:

- From the Menu bar, select Provisioning and select the devices or WDM from Delete WDM or Devices option and click Next.
- 2. Click Delete.

This resets/removes the WDM.

- 3. Use default FDN or PCN IP address to access WDM after the WDM is reset to defaults.
- 4. Restart the Web browser to run the First Time Configuration Wizard.

You can either configure the WDM using the **First Time Configuration Wizard** or restore the system configuration using the latest available backup. If you are configuring the WDM using the **First Time Configuration Wizard**, you need to transfer new provisioning keys to the provisioning device and provision all the devices in the network.

Delete PDA Devices

1. From the Menu bar, select **Provisioning** and select **Delete PDA Devices** and click **Next.**

Provisioning			
Select OTA Provisioning			
C Access Points Access points can be provisioned using over the eir provisioning method.	 ISA100 Devices ISA100 Weekees and Access points as nouters can be provisioned using over-the- air provisioning method. 		
Select Common Join Key Provisioning	Select PDA Provisioning		
O ISAL00 And WirelessHART Devices WrelessHART and EAL00 devices on be provisioned using Common Join Key method.	O Download Keys SA100 and WindexsHART devices can be provisioned using provisioning devices.		
Delete WDM or Devices			
O Delete WDM Delete WDM will react the WDM to factory configurations.	O Delete Devices Delete the devices from WOM and reset the device to factory configurations.	Delete PDA Devices Delete the PDA devices from WDM	
		BACK	NEXT

OWDOC-X254-en-323A

2. Select the device you need to delete and click **Delete**.

elete PDA Devices					
		-			
Tag Name		Q			
- S					
DEVICE NAME					
a testl					
test					
2 of 2 devices	н (1)		Go to page $1 \rightarrow$		Devices per page 10
				BAC	K DELETE

3. A window appears to provide the confirmation.

Restarting devices

To restart a WDM:

- 1. Click Mange Devices from the Menu bar and select WDM.
- 2. Expand **Device Management** in the Property Panel.

wdm1 Device Manager		
Device Manager Summary		
System Manager		
Device Management		
Command		
	RESET WDM	
All USB Ports Enable US	18 Ports : 🗌	
WDM Developer Mode	Enable :	

3. Click **Reset WDM**. The WDM restarts.

To restart FDAP/Access Point/field device

- 1. From Manage Devices, select the device to be restarted.
- 2. Expand Device Management in the Property Panel.
- 3. In the **Join Command** list, select one of the following options.
 - None
 - Warm Restart preserves static and constant attributes data.
 - **Restart as Provisioned** corresponds to the provisioned state of the device in which the device only retains the data received during its provisioning.
- 4. Click Apply.

About NTP status

The NTP Status panel in the WDM Properties Panel displays a number of NTP process attributes, which are mostly useful for debugging purposes.

To view the NTP Status Display:

- 1. Select WDM from Manage Devices.
- 2. Expand **NTP Status** in the Property Panel.

and the second se		
NTP Status		^
- System status		
Mean offset :		msec
Mean frequency offset :	39.112999	ppm
Leap indicator :		
Sync source : Last system event :	NTP	
Last system event :	ClockSync	
- Peer status		
Peerstatus		
Dispersion :	18.281000	msec
Root dispersion :		msec
Peer address :	192.168.253.100	
Peer Selection status :	SysPeer	
Last event :	Popcorn	
Peer association status		
	•	
Host Reachable :		
	•	
Authentication OK :		
Persistent Association :		
Flash error status		
	•	
	•	
	•	
	•	
	•	
	•	
	•	
	•	
	•	
Peer Distance Exceeded :		
	•	

NTP server unrea	chable
	When the NTP server is not responding to NTP communication from the WDM, the WDM raises the NTP server not reachable alarm. In the NTP Status panel, under Flash error status section, the Peer Unreachable appears in blue color and indicates as ON, and under Peer association status section, the Host Reachable appears in grey color and indicates as OFF. Depending on the internal state of the NTP process, it takes 8.5 minutes or more to detect that the server is not reachable.
NTP server reach	able
	The NTP server unreachable alarm returns to normal when the server is reachable again. In the NTP Status panel, under Flash error status section, the Peer Unreachable appears in grey color and indicates as OFF, and under Peer association status section, the Host Reachable appears in blue color and indicates as ON. Depending on the internal state of the NTP process, it takes 8.5 minutes or more to detect that the server is not reachable.
Peer rejected	
	The NTP process determines the time quality of the server over several communication packets based on various time and frequency measurements. Based on these measurements, the NTP process may reject a server but still continue to communicate with it and perform the time measurements. Until the server's time quality improves, the NTP process keeps the server marked as rejected. In the NTP Status panel, under Peer status section, the Peer Selection status is set to Reject . When a server is in rejected state, the NTP process does not try to sync time from the server.
Peer selected	
	The NTP process may reject a server for several reasons. For example, the server itself may not yet have synchronized to the root time server. While the server is rejected, the NTP process keeps performing the time and frequency measurements with the data received from the server. When the reference time quality improves, the NTP process selects the server as a system peer and starts synchronizing time with the server. In the NTP Status panel, under Peer status section, the Peer Selection status is set to SysPeer .
Mean offset	
	The NTP process monitors time from a server selected as a system peer and calculates how much correction must be made to the system time. In the NTP Status panel, the Mean offset indicates the additional remaining correction to the system clock. A positive value indicates that the system clock is behind the reference clock. As the NTP process slowly corrects the system time, the system clock slowly approaches the reference clock and the mean offset reduces.

Time synchronization

In the NTP Status panel, under the System status section, the Mean frequency offset field indicates the periodic correction applied to the system clock. Positive values make the clock go faster while negative values slow it down. When the NTP process starts synchronizing with a server, depending on how far the two clocks are, it may set the frequency offset to the maximum value (+/-500 ppm). This is unusually high for a good clock and is an intermediate value. ISA100 Wireless network devices correct their clocks at a maximum rate of 60 ppm. If the WDM's clock is corrected at a higher rate, the ISA100 Wireless network devices may further apart in time, resulting in devices reporting a clock drift alarm. The WDM generates an NTP frequency error alarm when the frequency offset is > 60 ppm. As the WDM's system time converges and the offset reduces, the frequency offset gradually reduces to a more realistic value. The NTP frequency error alarm returns to normal when the frequency offset reduces to below 30 ppm. The NTP process adjusts the clock in small steps so that the time-scale is effectively continuous and without discontinuities. This makes clock correction slow. In a system with a redundant or backup WDM, the backup WDM uses the primary WDM as its time server. If the primary WDM is configured to use an external NTP server, it may take some time for the primary WDM to synchronize with the NTP server and then the secondary WDM synchronizes, after some more time, with the primary WDM's time.

Generating reports

The OneWireless user interface enables you to generate and view various reports about connectivity, device health, and battery life of the devices in a network.

You can generate and view the following reports:

- **Battery Life**: Lists all devices that require battery replacement and lists the devices with battery level less than 50%.
- **Device Health Overview**: Lists all the devices with wireless network disconnection and alarms.
- **Device Summary**: Provides a summary of each of the device that is configured in the network. The report does not display the details of the devices that are filtered out using the **Filter** option.
- **Device History**: Lists all the device status changes. For example, status change from online to offline device, routing to time synchronization, non-redundant connection to redundant connection.
- **Connection Summary**: Provides a summary of current status of device connections in the network, redundancy state, and lists all connections with a poor or unacceptable signal strength and quality. The RSQI value when less than 64 results in poor or unacceptable signal quality.
- **Connection History**: Lists all the history of connection changes. For example, change of RSQI, RSSI, transmit fail ratio.
- **Inventory Summary**: Provides a count of all the different devices connected to the OneWireless network, including the vendor make and the model.
- Availability Summary: Provides the summary of Device Name, Short Address, Availability, Latency, Turnaround time, Publication Success Rate, Uptime, and Device Drop Count of the devices. See the following table and the illustration for more information.

Connection Summary Mediate State Med	Device Health Overview ^ Device History	n paying specific attention to device wireless network di	isconnections and the presence of alarms.	Report Generated By	Date and Time 26-Apr-21 1:06:0
Device beraulti Mup 0 Device becaulti Mup 0 Device becaulti Mup 0 WeeLess becoments 0 CD_475_3F_6FLR Map2 This device has disconnected 1 times EML_64CAL_SFL Unplaced This device has disconnected 4 times	Connection Summary Connection History				
EML_DACAA_SFL Unplaced This device has disconnected 9 times	Availability Summary	DEVICE DEFAULT MAP 💲	DEVICE DESCRIPTION \$	WIRELESS DISCONNECTS 🗘	
	CD_475_3F_6FLR	Map2		This device has disconnected 1 times	
v 3308_GWPLTX Map2 This device has disconnected 4 times	V EML_64C4A_5FL	Unplaced		This device has disconnected 4 times	
	V 3308_GWR_TX	Map2		This device has disconnected 4 times	

Field Names	Description
Device Name	Name of the device
Short Address	Short address of the device
Availability (%)	Device availability from the time it was provisioned to the network
Latency (secs)	Average time taken to publish by wireless sensor to the WDM for the configured publish rate
Turnaround time (secs)	Average time taken for WDM requests for measurement data through the wireless gateway to the target wireless sensor and the wireless sensor acquires a measurement and responds to the WDM request
Publication Success Rate (%)	Percentage of number of publish received from the wireless sensor vs the expected number, based on the publish rate configured
Uptime (secs)	Device uptime from the time it joined the network
Device Drop Count	Number of times the device dropped from the network
Note: Latency, Turnaround time and Publication Success Rate is not applicable for Access Point and Access point as Router.	

.

Exporting and saving system logs

OneWireless user interface enables you to export and save the system logs that record information about events in the application instances. Export System Log option exports and saves the system log in a .tar.gz (compressed archive) format in the system for future reference. The system logs are primarily used for debugging by Honeywell Technical Assistance Center (TAC).



For WDMs configured as redundant, export the system logs from both WDMs when reporting an anomaly or requesting clarification.

To export and save system logs:

- Click Export System Log under System from Left Navigation Menu. The Export System Log dialog box appears.
- 2. Click OK.

The Save As dialog box appears.

3. Save the log file.

The system log files are saved in *.tar.gz format. The **Export System Log in Progress** message appears. After the system log is saved, **Export System Log completed successfully** message appears indicating that system log has been saved successfully.

4. Click OK.

Reporting anomalies

If you encounter any errors in the OneWireless Network that you cannot resolve, contact TAC. The following are required while contacting TAC for assistance.

- Export and collect system logs. For information on exporting system logs, refer to the section "Exporting and saving system logs"
- Take a system configuration back up. For information on taking a backup, see the section **"Configuring system configuration backup"**.
- Contact TAC and provide the following.
 - System logs from both WDMs, if configured for WDM redundancy.
 - The system configuration backup, if required
 - Affected device tag name and the exact description of the anomaly
 - Time when the anomaly occurred
 - To export the System Events history

Terms and definitions

Terms	Definition
DD files	Device Description files
DSSS	Direct Sequence Spread Spectrum
FDAP	Field Device Access Point (FDAP) is a wireless infrastructure node that acts as an ISA100.11 and WirelessHART I/O access point and a mesh node member. FDAP can communicate with ISA100 2009 version, ISA100 2011 version, and WirelessHART field devices.
FDAP Gen3	Field Device Access Point
FDN	Field Device Network
FEWIO	Field Expandable Wireless IO
Field device	A general term for process sensor (input) or process actuator (output) device.
GCI	Gateway General Client Interface
HART	Highway Addressable Remote Transducer
ΟΤΑΡ	Over the Air Provisioning
РСАР	Process Control Access Point (PCAP) is a wireless infrastructure node that acts as an ISA100.11 and WirelessHART I/O access point and a mesh node member.
PCN	Process Control Network
Provisioning handheld device	Includes Personal Digital Assistant (PDA), mobile PCs and so on.
RSQI	Receive Signal Quality Index
RSSI	Receive Signal Strength Index
SIN	Special Interface Network
TXFR	Transmit Fail Ratio
WDM	Wireless Device Manager (WDM) is a device that manages both the ISA100.11a and WirelessHART field device network and all the ISA100.11a and WirelessHART related components connected to the OneWireless network.

Terms	Definition
WDM	Wireless Device Manager (WDM) is a device that manages both the ISA100.11a and WirelessHART field device network and all the ISA100.11a and WirelessHART related components connected to the OneWireless network.
FDAP	Field Device Access Point (FDAP) is a wireless infrastructure node that acts as an ISA100.11 and WirelessHART I/O access point and a mesh node member. FDAP can communicate with ISA100 2009 version, ISA100 2011 version, and WirelessHART field devices.
РСАР	Process Control Access Point (PCAP) is a wireless infrastructure node that acts as an ISA100.11 and WirelessHART I/O access point and a mesh node member.
FEWIO	Field Expandable Wireless IO
ΟΤΑΡ	Over the Air Provisioning
Field device	A general term for process sensor (input) or process actuator (output) device.
Provisioning handheld device	Includes Personal Digital Assistant (PDA), mobile PCs and so on.
DD files	Device Description files
DSSS	Direct Sequence Spread Spectrum
FDN	Field Device Network
PCN	Process Control Network
SIN	Special Interface Network
HART	Highway Addressable Remote Transducer
RSSI	Receive Signal Strength Index
RSQI	Receive Signal Quality Index
TXFR	Transmit Fail Ratio
GCI	Gateway General Client Interface

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 is mentioned as and when applicable.

	Note that in this document, a reference to WDM includes WDMX and
	WDMY unless otherwise mentioned. Specific WDM is mentioned as and
NOTE	when applicable.

Notices

Trademarks

	Experion®, PlantScape®, SafeBrowse®, TotalPlant®, and TDC 3000® are registered trademarks of Honeywell International, Inc.
	ControlEdge™ is a trademark of Honeywell International, Inc.
	OneWireless™ is a trademark of Honeywell International, Inc.
	Matrikon® and MatrikonOPC™ are trademarks of Matrikon International. Matrikon International is a business unit of Honeywell International, Inc.
	Movilizer® is a registered trademark of Movilizer GmbH. Movilizer GmbH is a business unit of Honeywell International, Inc.
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.
Documentation feed	back
	You can find the most up-to-date documents on the Honeywell Process Solutions support website at:
	https://process.honeywell.com
	If you have comments about Honeywell Process Solutions documentation, send your feedback to: <u>hpsdocs@honeywell.com</u>
	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 Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC).

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 Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC).

Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, <u>https://process.honeywell.com/us/en/contact-us</u>.

Training classes

Honeywell holds technical training classes that are taught by process control systems experts. For more information about these classes, contact your Honeywell representative, or see <u>http://www.automationcollege.com</u>.

Honeywell Process Solutions

1250 W Sam Houston Pkwy S #150, Houston, TX 77042

Honeywell House, Skimped Hill Lane Bracknell, Berkshire, RG12 1EB

Building #1, 555 Huanke Road, Zhangjiang Hi-Tech Park, Pudong New Area, Shanghai, China 201203 https://process.honeywell.com

OWDOC-X254-en-323A June 2022 © 2022 Honeywell International Sàrl

