Honeywell

ONEWIRELESS

RELEASE 323

Wireless Device Manager User's Guide

OWDOC-X254-en-323A

June 2022

DISCLAIMER

Table of contents

About this guide

This document describes the procedures to provision, configure, operate, and monitor ISA100 Wireless and WirelessHART 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
A	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 and Installation Guide (OWDOC-X253-en)	This guide provides information about planning, designing, and setting up the OneWireless network using WDM, 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 Controller Configuration Guide (OWDOC-X255-en)	This guide provides information about planning, designing, setting up, and configuring a OneWireless network using 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 https://process.honeywell.com 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.

Table. 1. WDM 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.

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

Hardware description of WDM

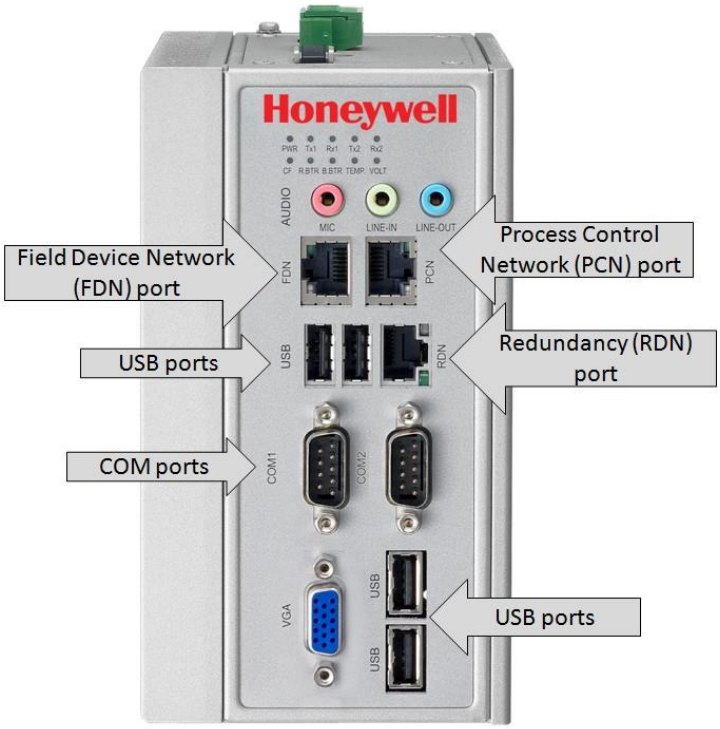


Fig. 1. WDMX hardware

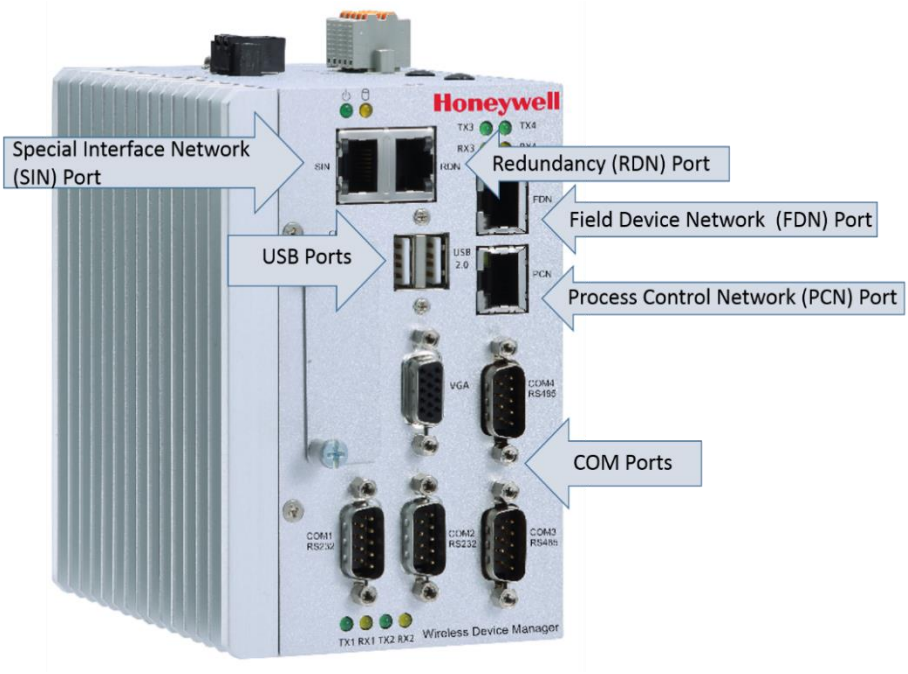


Fig. 2. WDMY hardware

Table. 2. Description of WDM ports

Port name	Description
Field Device Network (FDN) port	Used for connecting the WDM with FDAPs/Access points. ***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 embedded 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.

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.

Table. 3. LED indicators

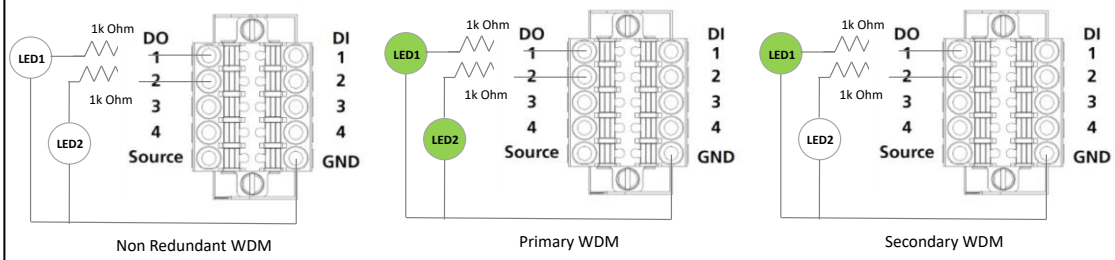
LED name	Status	Function
Power	Green	Power is on and the computer is functioning normally
	Off	Power is off
Storage 1 (CFast)	Yellow	Blinking: Data is being saved or retrieved
	Off	No data transmission
LAN 1/2/3/4	Green	Steady on: 100 Mbps Ethernet link Blinking: Data is being transmitted
	Yellow	Steady 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

Redundancy Status Identification of WDMY

The following image explains the redundancy status identification of WDMY.

WDMY

- Redundancy Status Identification using DO
- LED Connection Details



Non Redundant WDM | Primary WDM | Secondary WDM

- LED Status Indication
  - LED1 – Redundant Status
  - LED2 – Sync Status

Non Redundant WDM	LED1	LED2
	OFF	OFF

Primary WDM	LED1	LED2
	ON	ON

Secondary WDM	LED1	LED2
	ON	OFF

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.

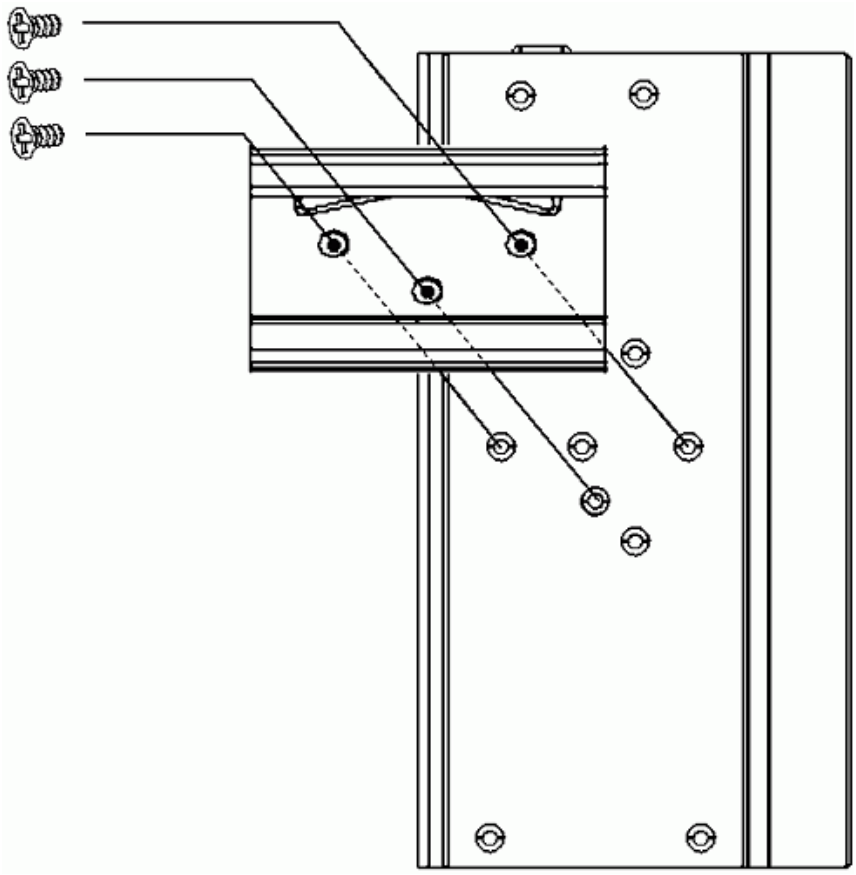
1. Install and configure the WDM.
2. Power up and provision all the Access Points (PCAP, FDAP2, FDAP Gen3).
3. Power up and provision all the FDAP routers.
4. Power up and provision all the field devices.

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.

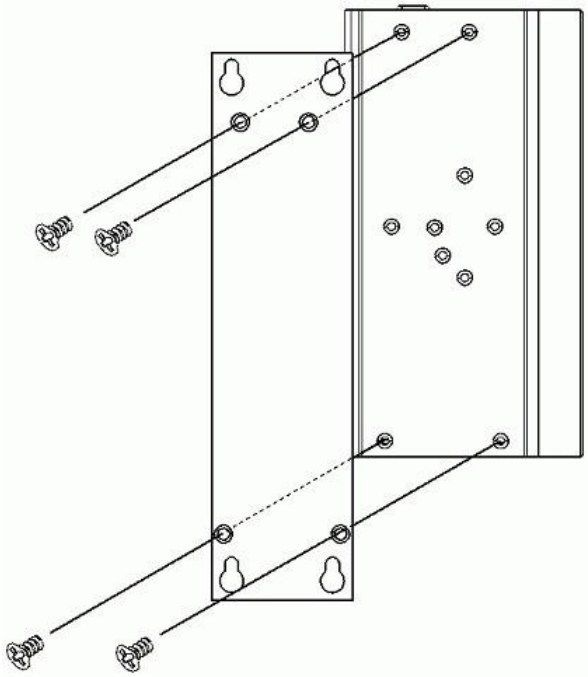


2. Hang the WDMX onto the DIN-Rail with an angle of inclination about 30 degrees.
3. Lower the WDMX straight down to slide over the Rail smoothly.

ATTENTION	**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 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.

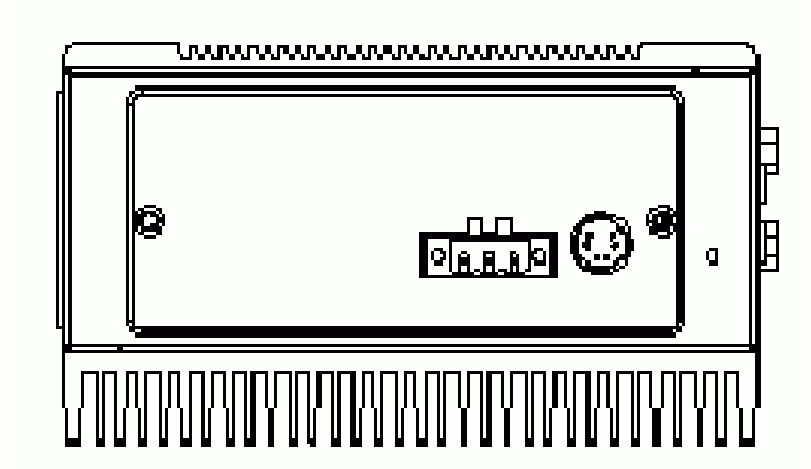


Fig. 3. Top view of the WDMX

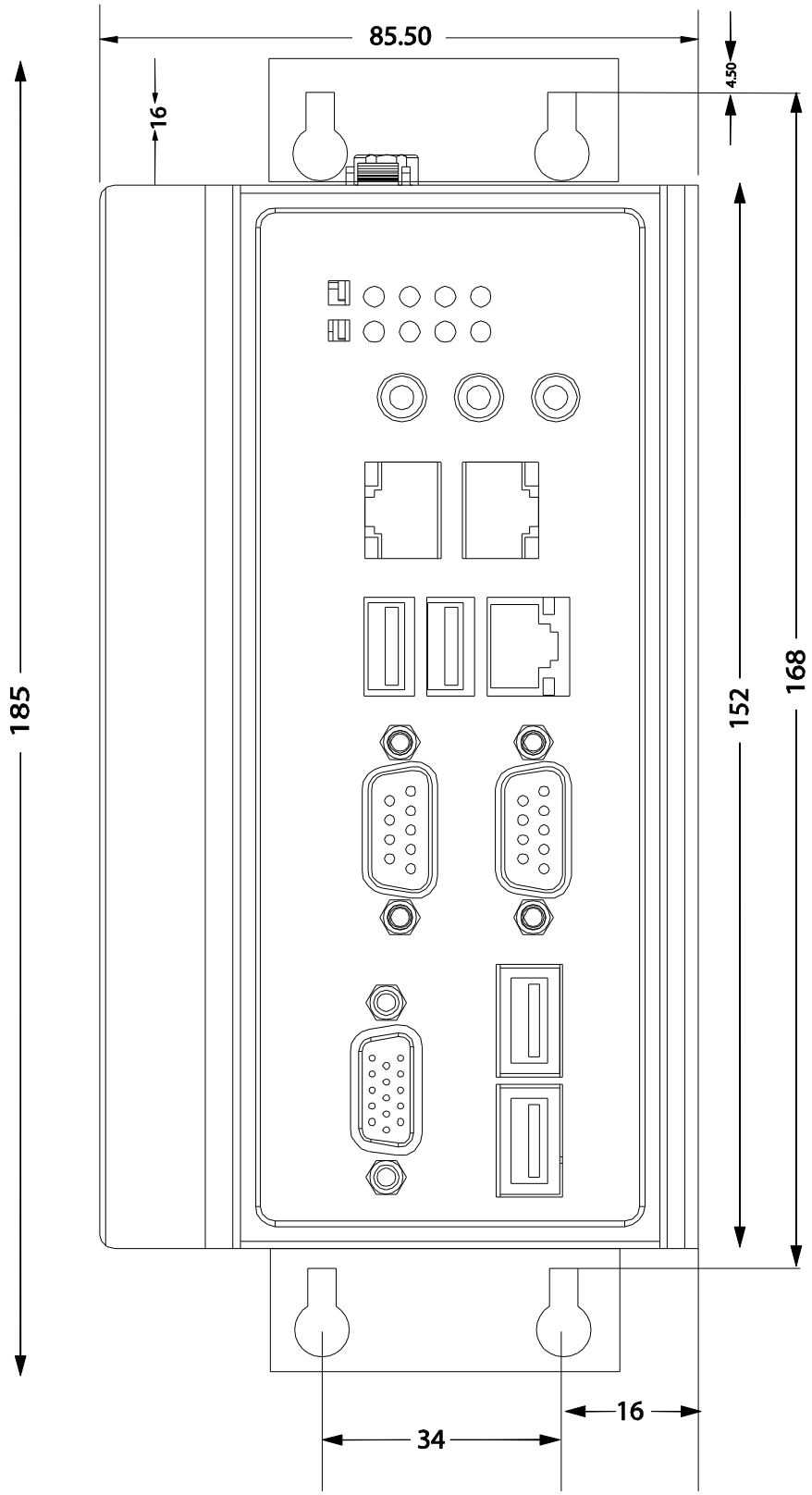


Fig. 4. Rear view of the WDMX

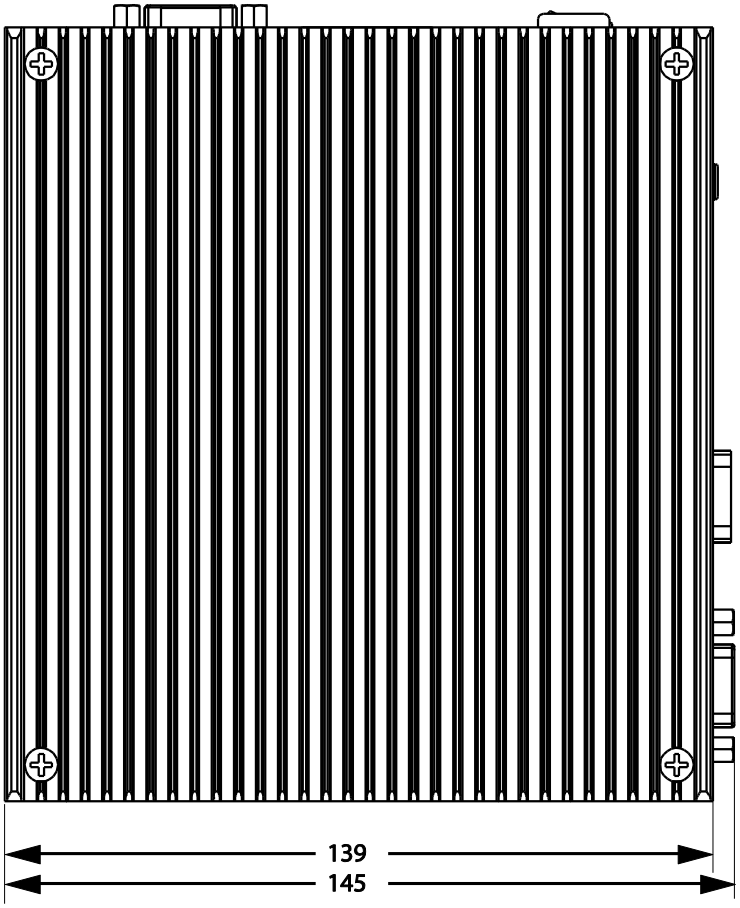
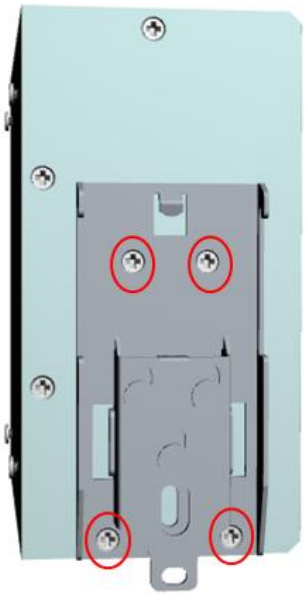


Fig. 5. Top view of the WDMX

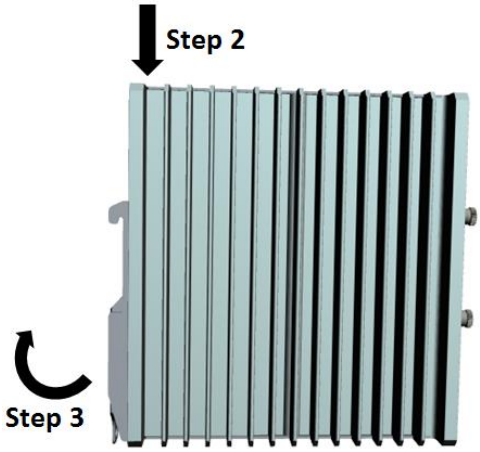
Mounting WDMY

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.



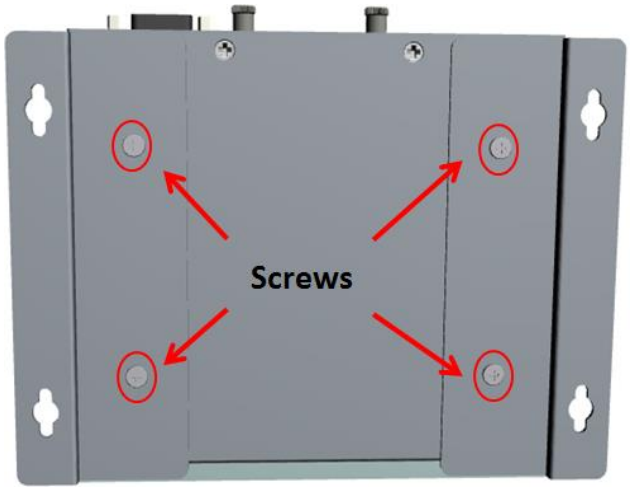
2. Insert the top of the DIN rail into the slot just below the upper hook of the DIN-rail mounting kit.



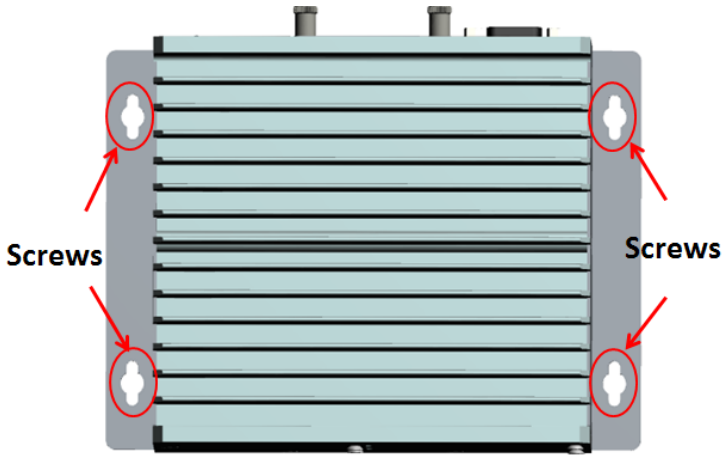
3. Press the WDMY towards the DIN-rail until it snaps into place.

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.



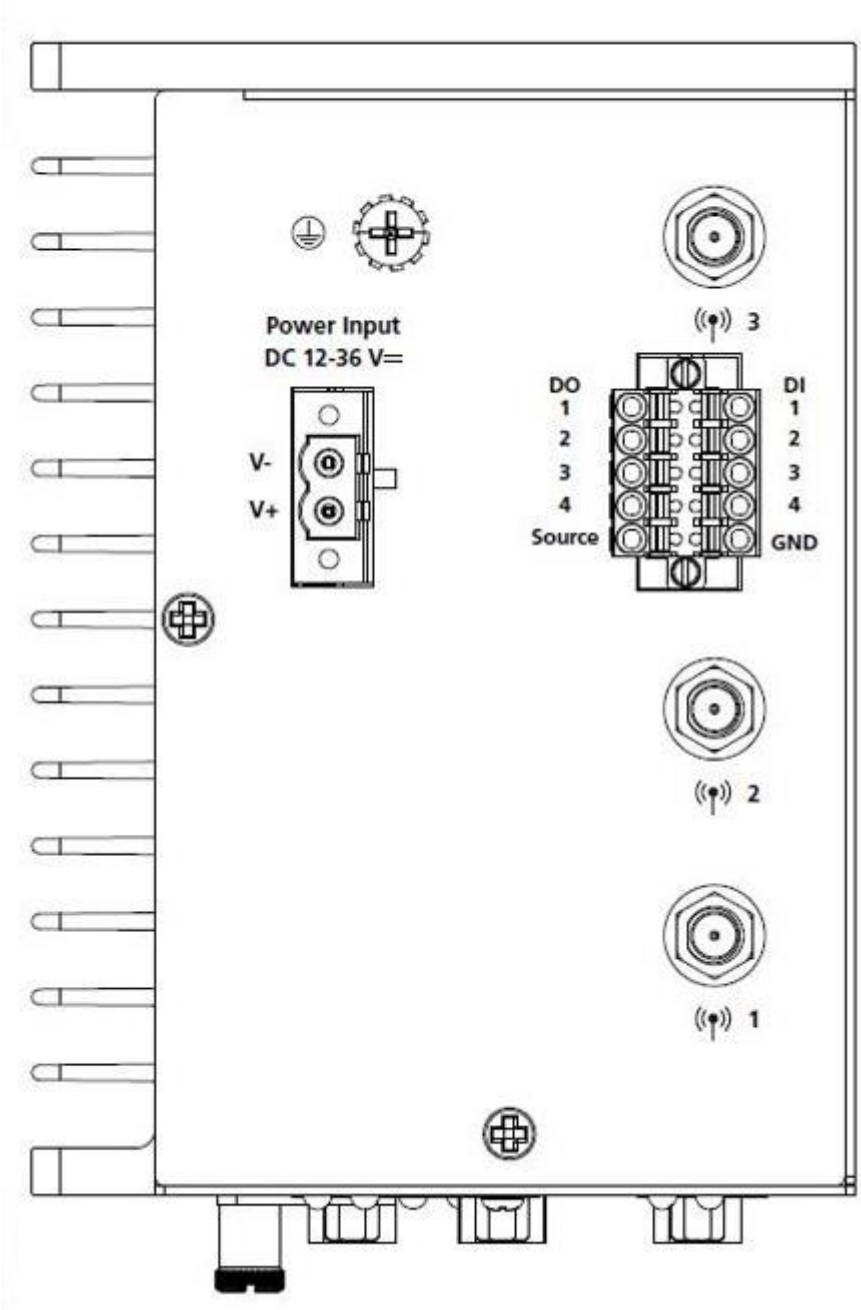


Fig. 6. Top view of the WDM

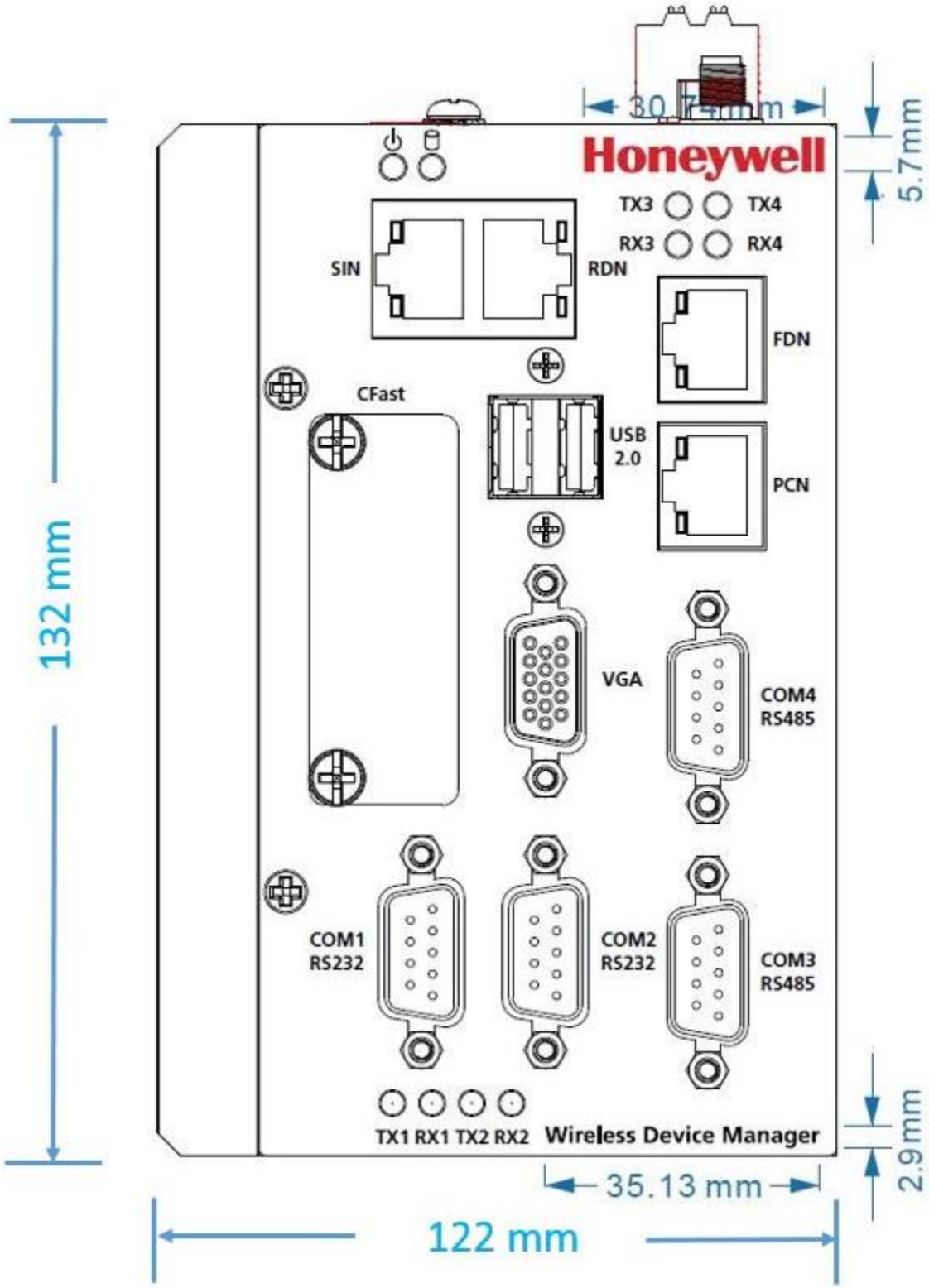


Fig. 7. Front view of the WDM

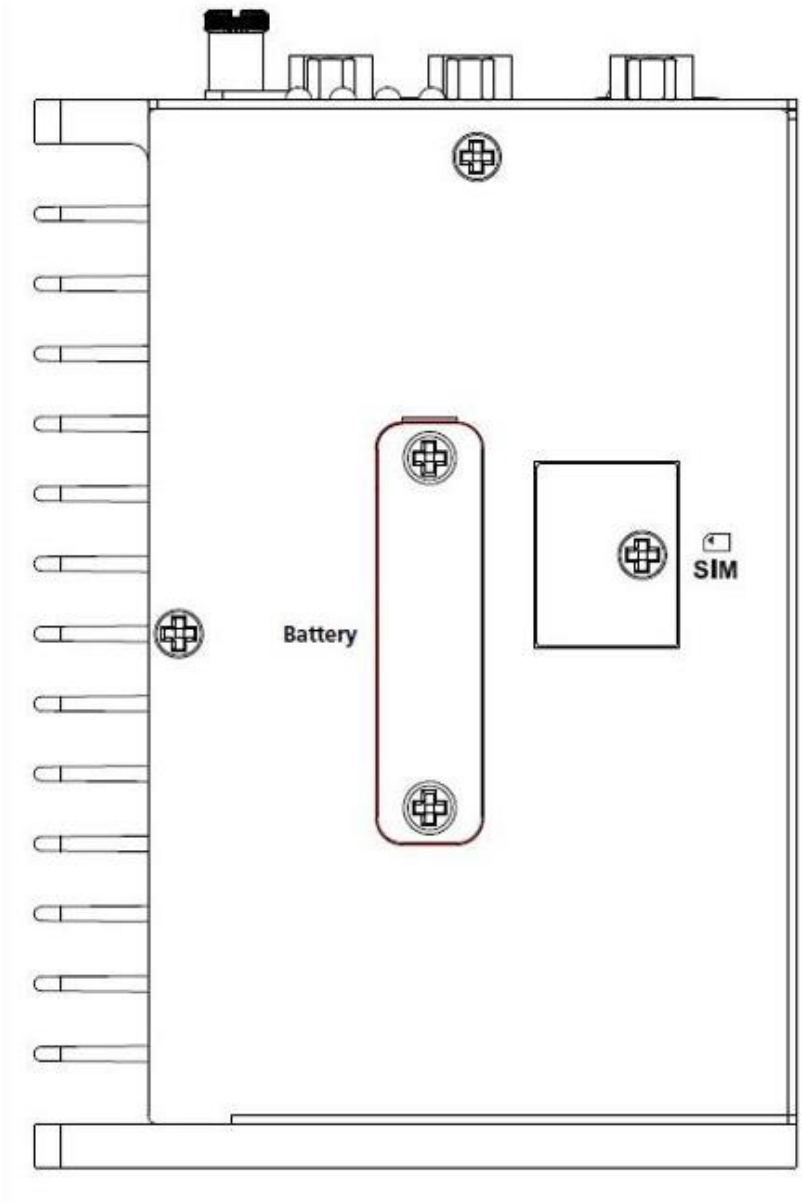


Fig. 8. Bottom view of the WDM

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.

ATTENTION	***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.

ATTENTION	*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 no IP address is assigned. To recover, you must resolve the duplicate IP address from the network.*

NOTE	**PHYSICAL ACCESS TO CRITICAL DEVICES** **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.

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

ATTENTION	***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**.

ATTENTION	***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.

ATTENTION	***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.

CAUTION	**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 address, https://192.168.1.1 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.

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

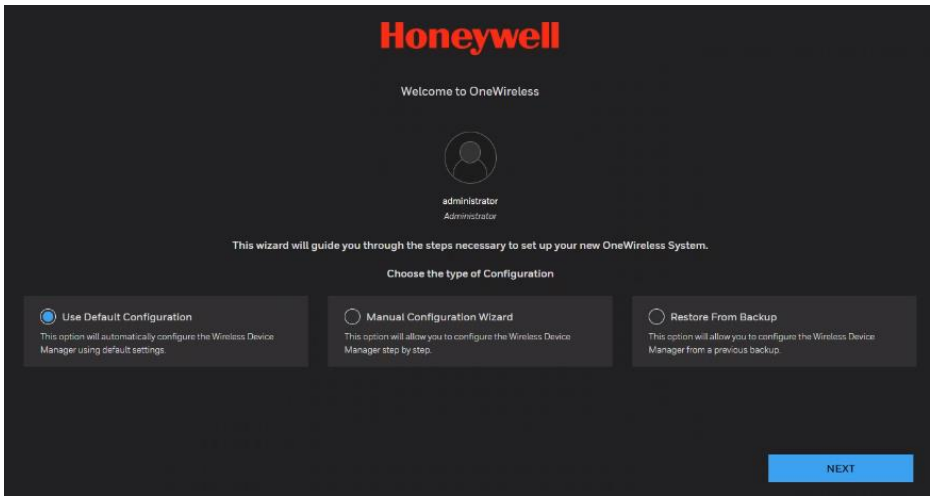
To configure WDM using the First Time Configuration Wizard

Use Default Configuration

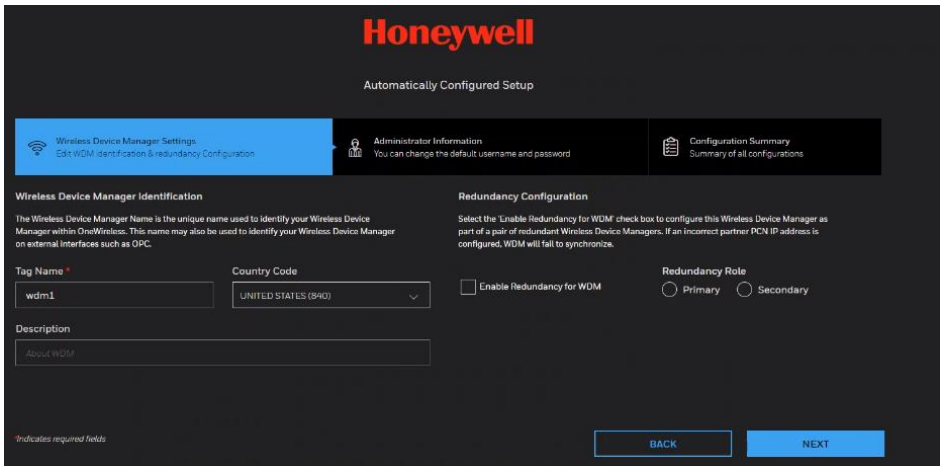
All the settings is configured with default values in this option.

1. 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**.

ATTENTION	**Default IP addresses are taken for FDN, PCN and SCN in Default Configuration**



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



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.

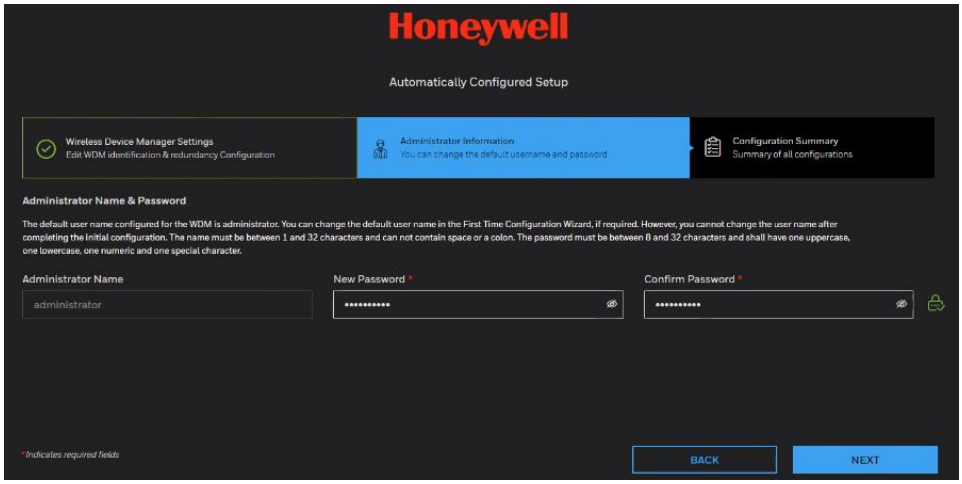
4. To configure redundant WDM, under **Redundancy Configuration**, configure the following:
   a. Select Enable redundancy for this Wireless Device Manager check box.
   b. Click the Redundancy Role, as required. You can select either Primary or Secondary option depending on the redundancy role.

ATTENTION	***Some of the settings may be disabled while configuring Secondary WDM as it follows the settings from the Primary WDM.***
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.**

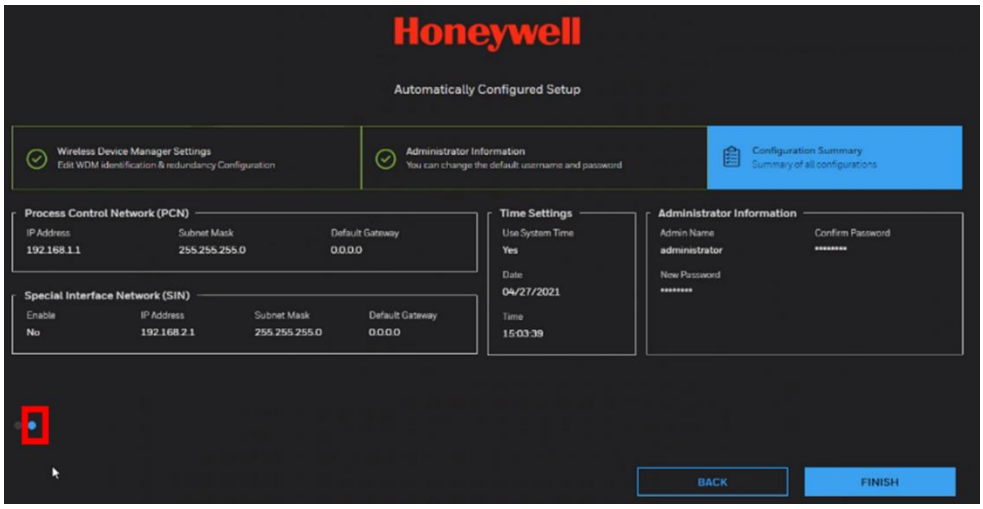
5. Under **Location**, select the **Country Code**. The country code is used to define any location-specific settings within the OneWireless Network. For example, radio frequency options are location dependent and vary depending on the country code settings. After completing the first time configuration,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

ATTENTION	*If an incorrect partner PCN IP address is configured, WDM does not synchronize. The incorrect PCN IP address can be reconfigured on WDM Property Panel.*

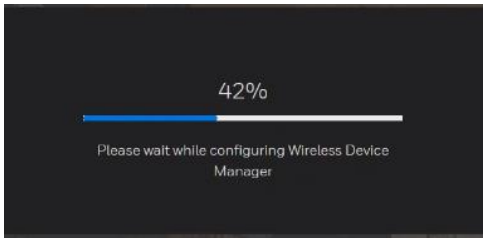
6. The **Administrator Information** page appears. Provide the Username, password and click **Next**.



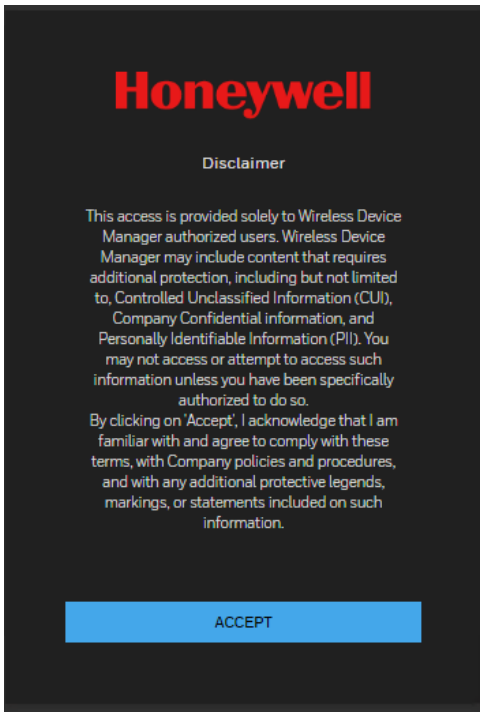
7. You can view the details in **Configuration Summary** page with default values.



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.

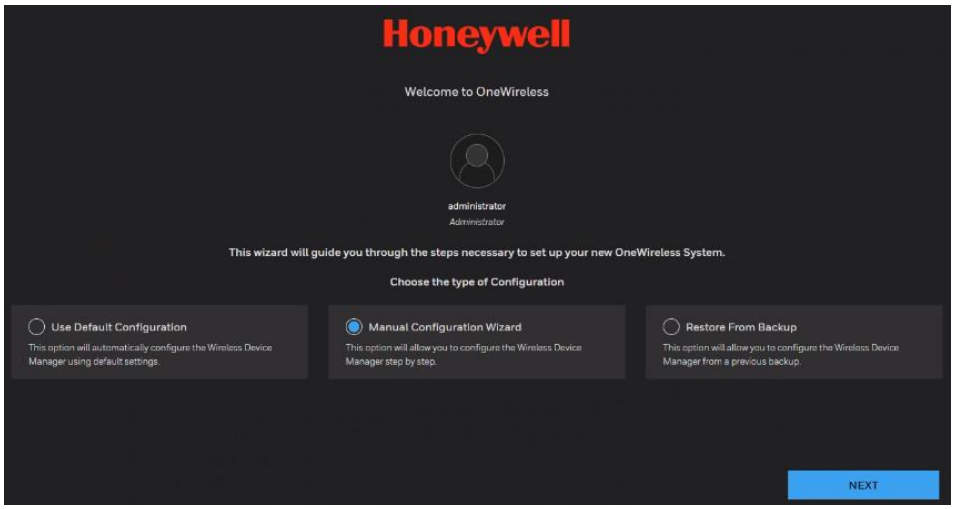


11. The following page appears after completion.

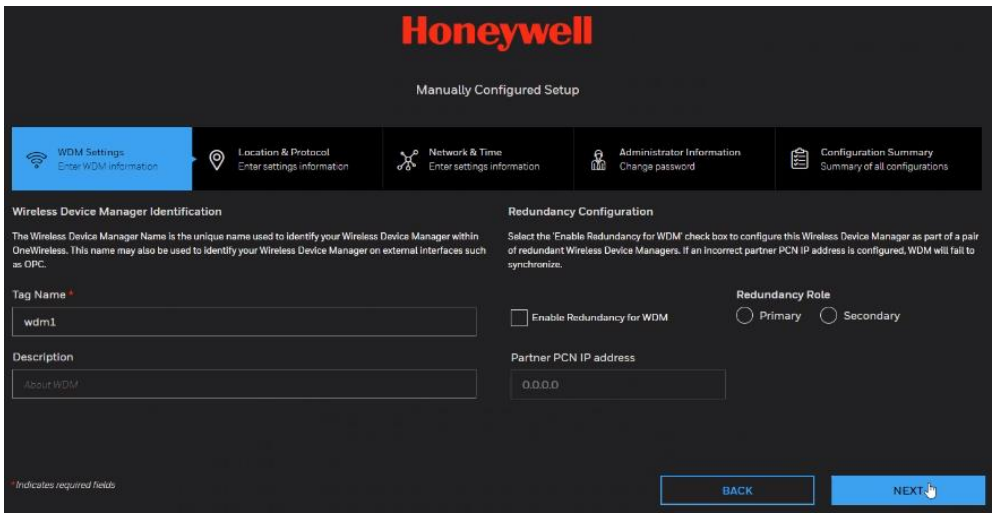


Manual Configuration Wizard

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



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

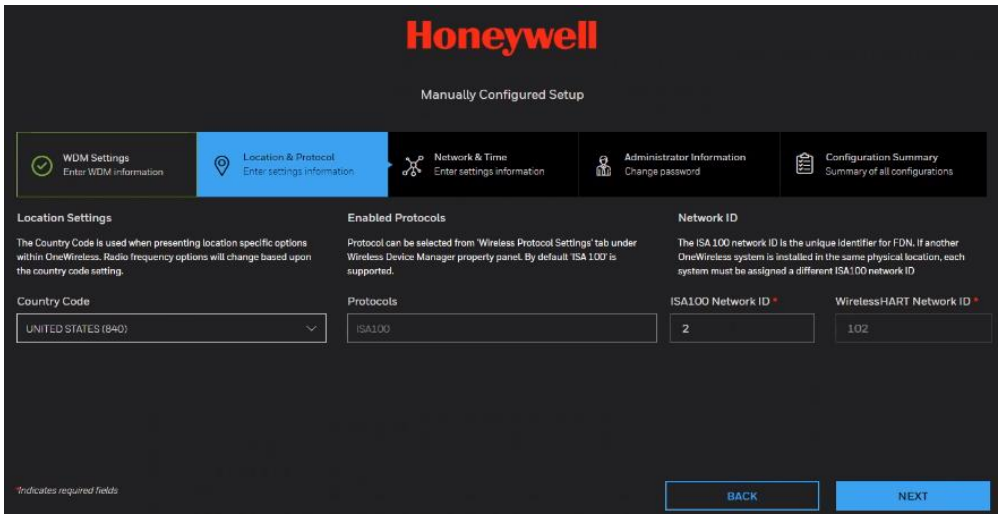
   c. In the Partner PCN IP Address box, type the PCN IP address of the partner WDM.

ATTENTION	***If an incorrect partner PCN IP address is configured, WDM does not synchronize. The incorrect PCN IP address can be reconfigured on WDM Property Panel.***

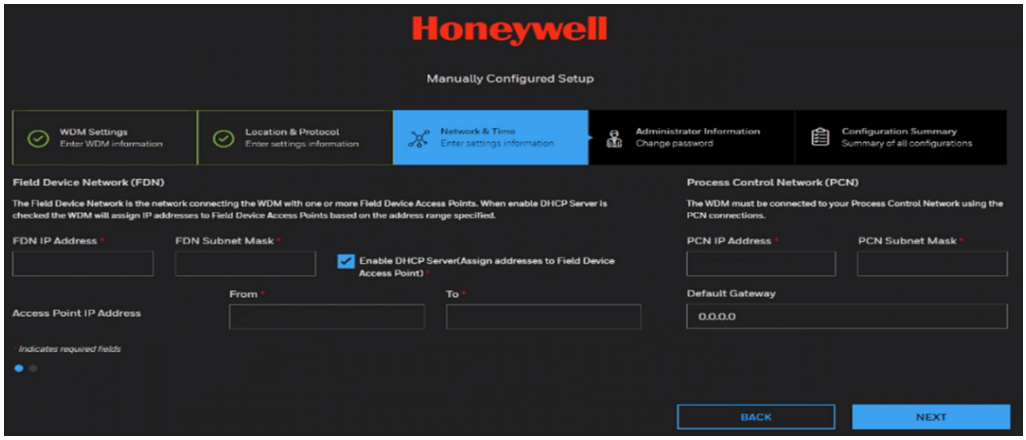
4. In the **Location and Protocol** page provide the **Country Code, Protocols, ISA100 Network ID** and **WirelessHART Network ID.**

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.

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



6. 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).**



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.

ATTENTION	• ***The IP address must be unique on the network, even if a redundant WDM pair is being configured.*** • ***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.

ATTENTION	***DHCP server configuration option is disabled on a secondary WDM.***

8. Under **Process Control Network (PCN)**, configure the process control network settings as follows.

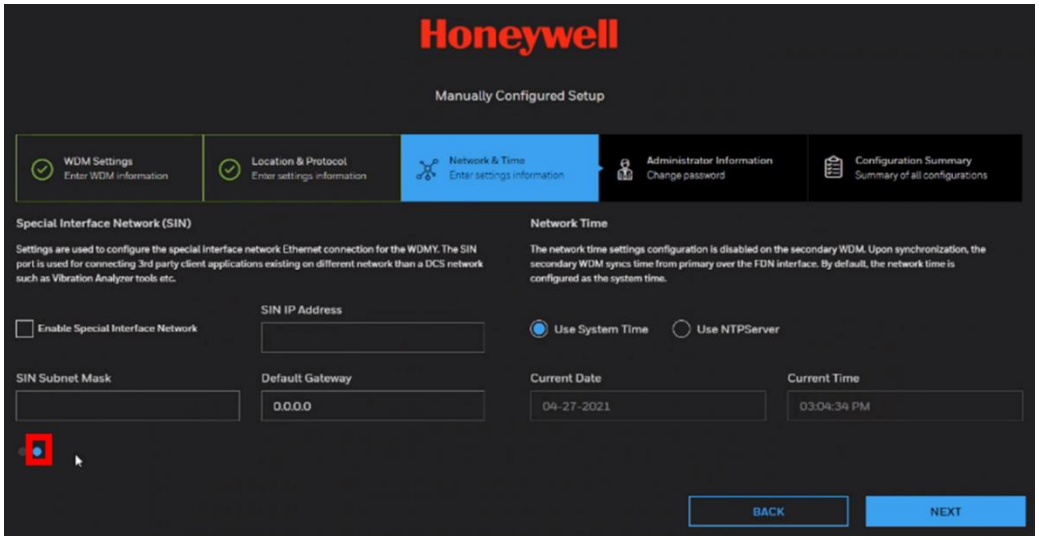
- **Process Control Network IP Address**: The process control network settings are used to configure the process control network Ethernet connections for the WDM. This is used for communication with monitoring applications and external controllers.

ATTENTION	***The IP address must be unique on the network, even if redundant WDM pair is being configured.***

- 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.**



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.

ATTENTION	***The IP address must be unique on the network, even if a redundant WDM pair is being configured.***

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

ATTENTION	***The network time settings configuration is disabled on the secondary WDM. Upon synchronization, the secondary WDM syncs time from primary over the FDN interface.***

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.

!	• ***By default, the network time is configured as the system time.***

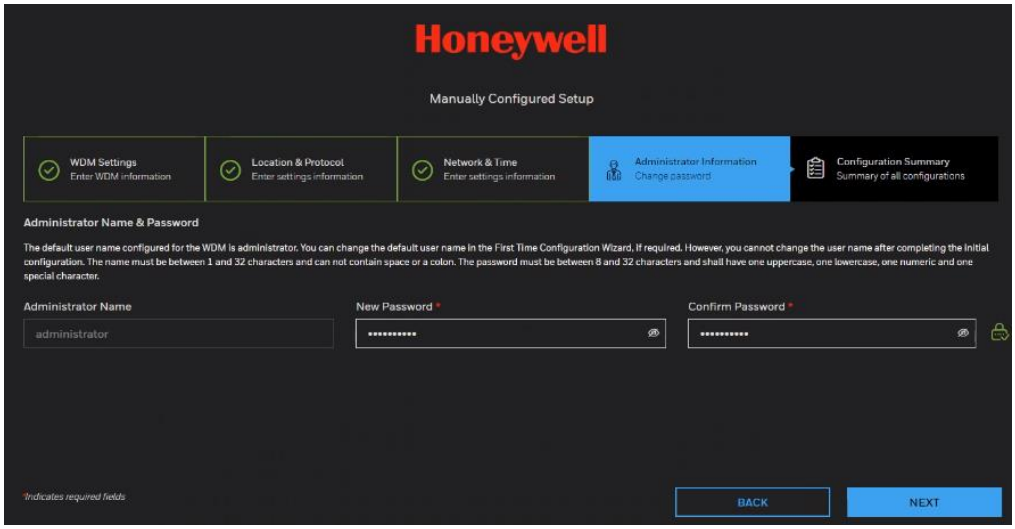
ATTENTION	• *Consider the following while configuring an external NTP server.* – *NTP server must be on the PCN or FDN.* – *NTP server IP address must be within FDN or PCN subnet unless a default gateway has been configured on the PCN subnet and the NTP server is accessible through the default gateway.* – *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.

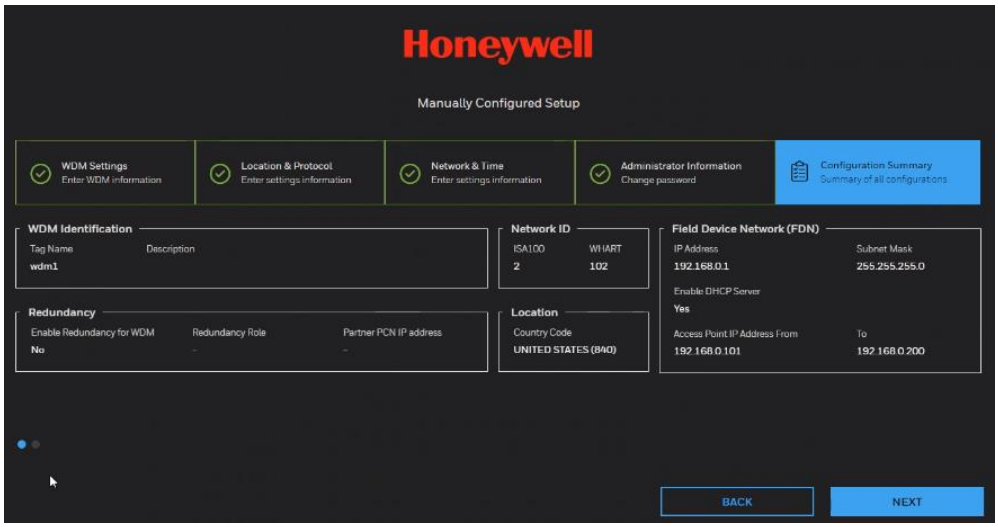
13. Type the user name and password in the **Administrator Name**, **New Password**, and **Confirm Password** fields.

    - 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.

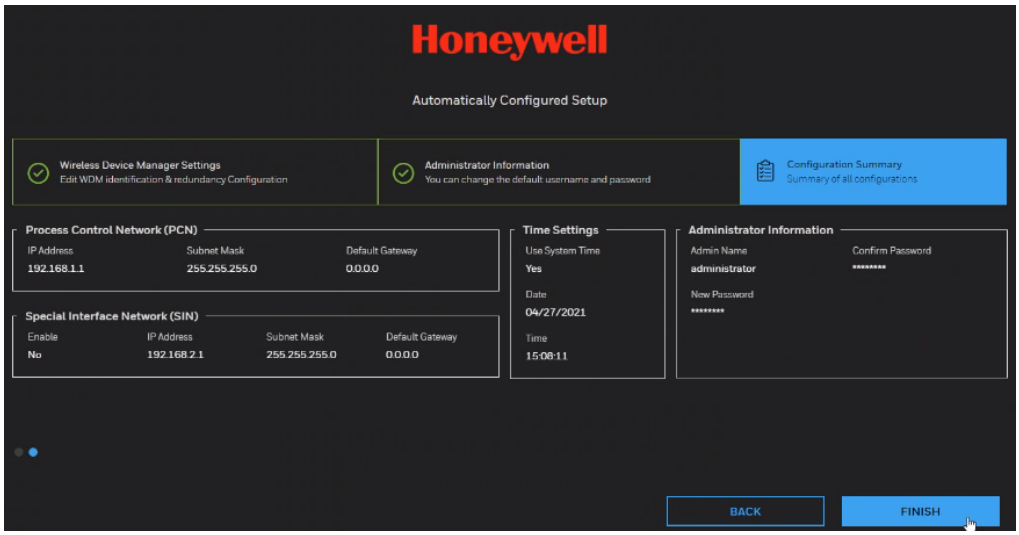
ATTENTION	*When setting up a redundant WDM pair, it is recommended that the same default username and password are configured on primary and secondary WDM. This is because when the primary and secondary WDMs synchronize, the secondary WDM's user account information is overwritten by the user accounts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



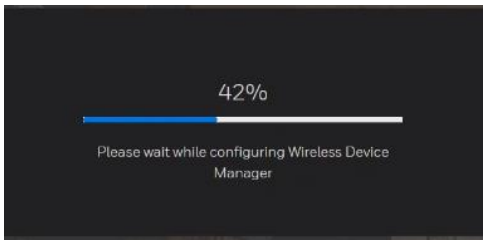
14. The Configuration Summary page appears which displays the summary of all the configuration information specified in the First Time Configuration Wizard. An incorrect entry is indicated by a warning icon.



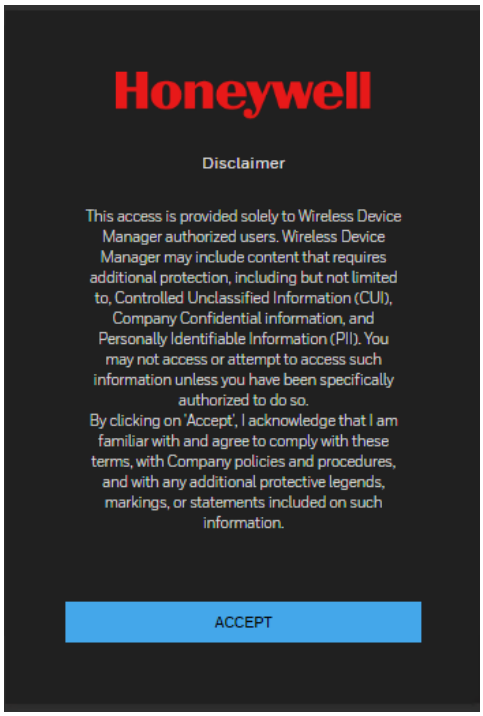
15. Verify the WDM settings, correct errors if any, and then click **Finish**. The Finish button is disabled if there are any errors in the configuration information that you have provided.



16. You can see the progress as shown below.

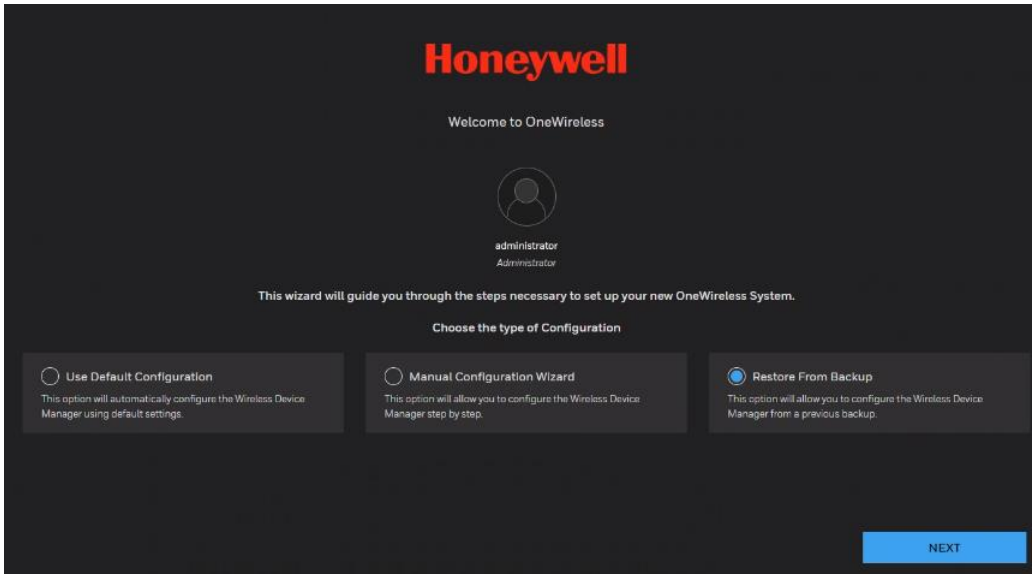


17. The following page appears after completion.



Restore from Backup

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

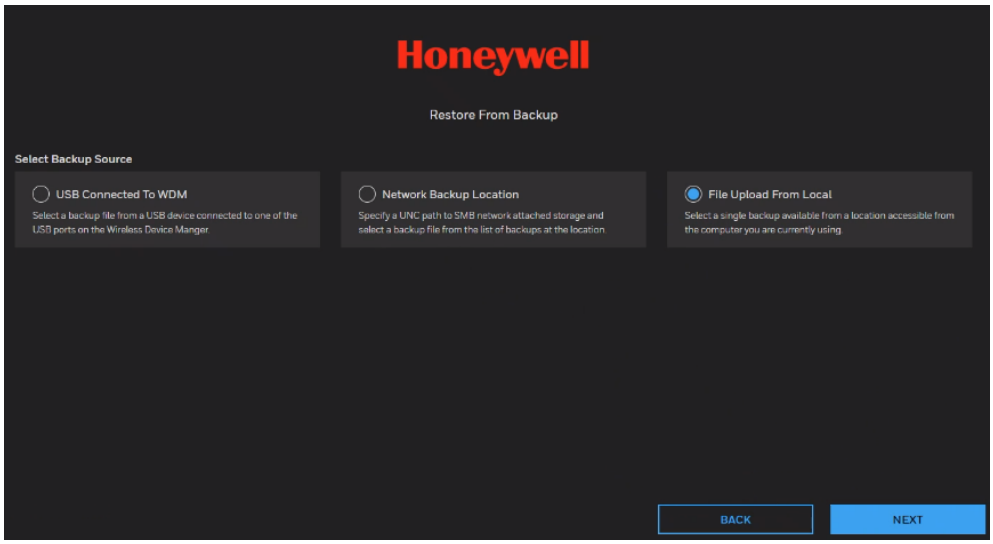


ATTENTION	**For R321.1 or prior releases, a conversion tool is required to update the backup file and make it compatible with R322.1**

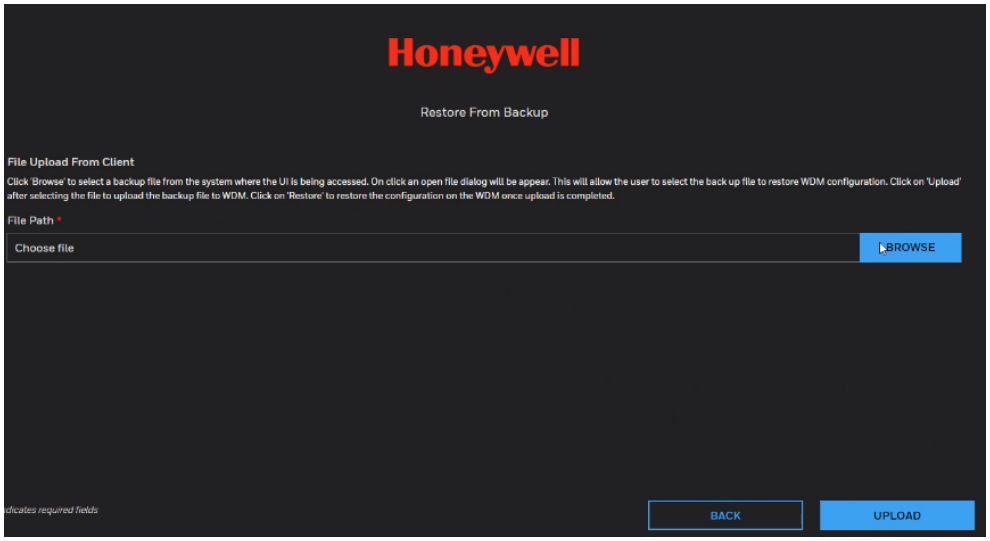
2. Restore from Backup can be done by the following ways:
   - **USB Connected To WDM**: Select a backup file from a USB device connected to one of the USB ports on the Wireless Device Manager.
   - **Network Backup Location**: Specify a UNC path to SMB network attached storage an select a backup file 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

1. Select **File Upload from Local** and click **Next.**



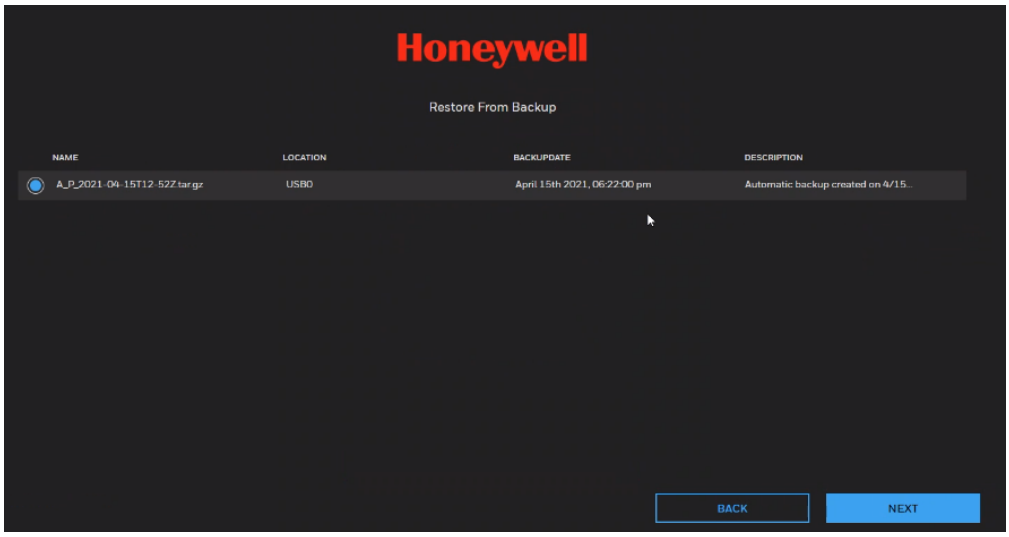
2. Browse the file and click **Upload**.



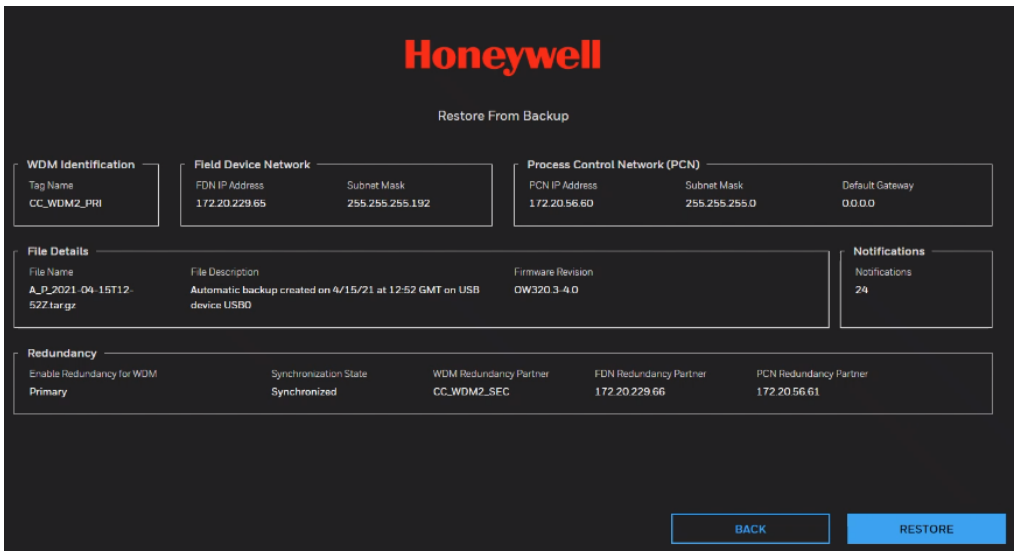
3. It will ask for encryption password

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

4. Click **Next**.

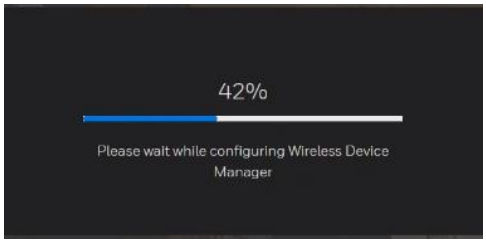


5. Click **Restore**.

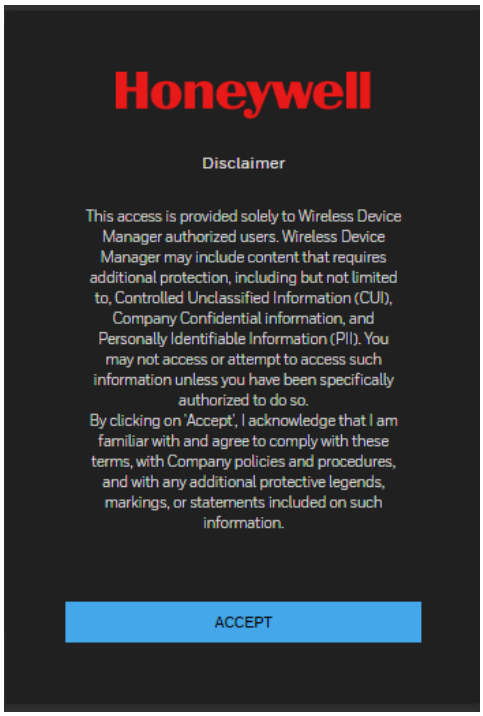


6. Verify the WDM settings, correct errors if any, and then click **Finish**. The Finish button is disabled if there are any errors in the configuration information that you have provided.

7. You can see the progress as shown below.

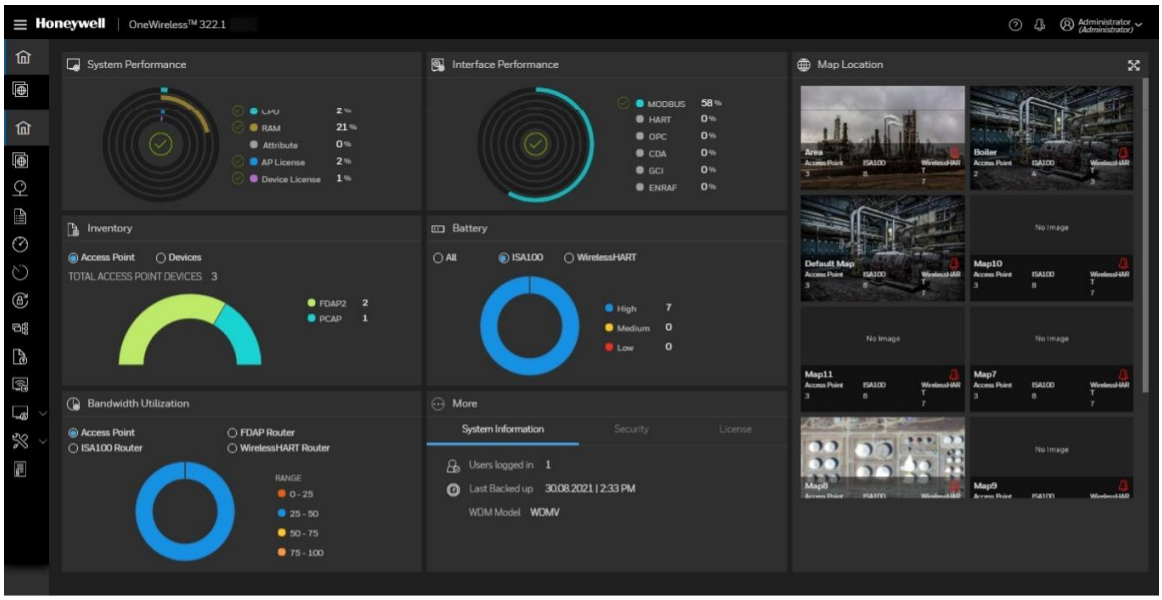


8. The following page appears after completion.


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 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

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.

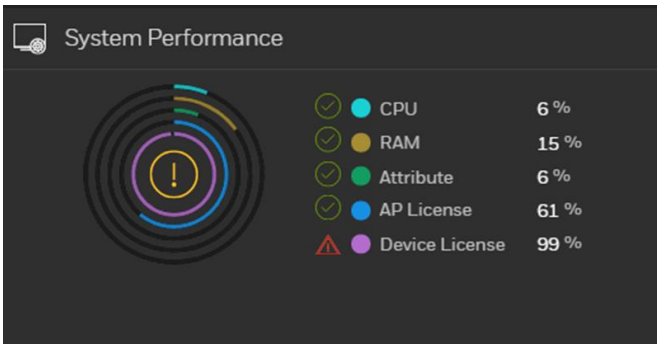
- **Left Navigation Menu bar:** Consists of Home, Main menu, Action menu and Logout. It gives an access to various functions for monitoring and maintaining the OneWireless Network. These user interface controls are contextual and are enabled based on user role and devices/channels selected in the Map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

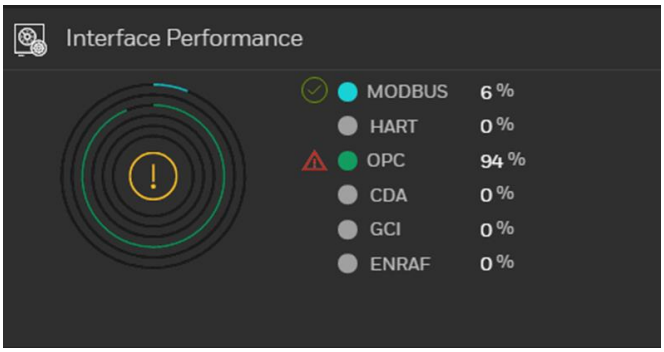
- System Performance:

  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.



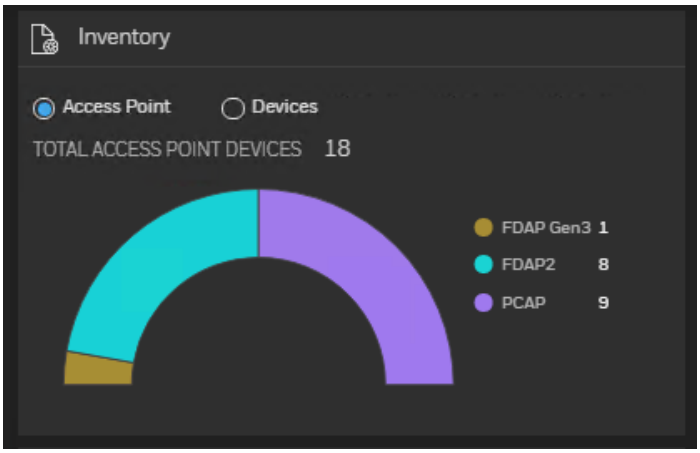
- Interface Performance:

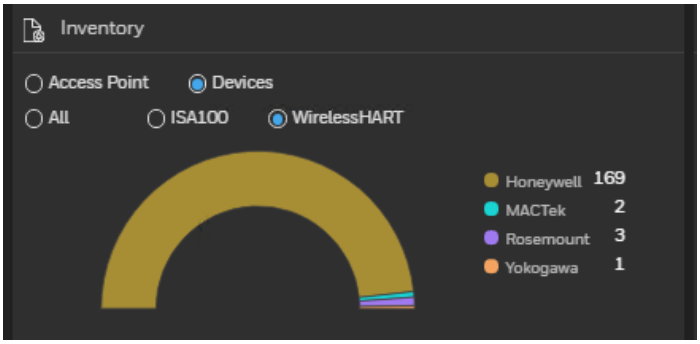
  Provides the information about individual external interface bandwidth utilization. Rate 0% means the interface might be disabled or no communication between client.



- Inventory:

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





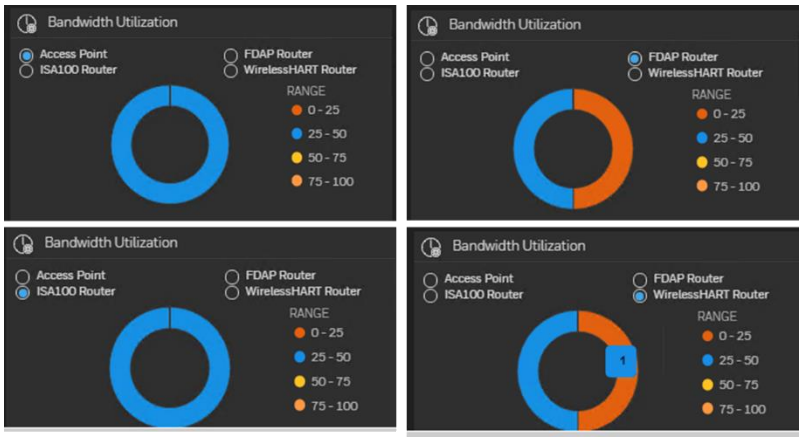
This page is read only, by default it is selected as Access Point.

- 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 WirelessHART Router connected to OneWireless network.

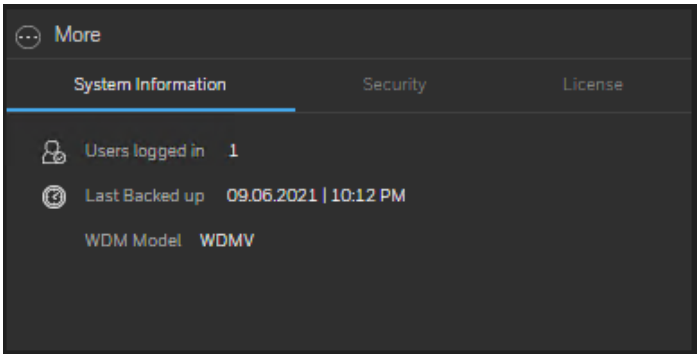


- More:

  Provides information on System Information. Security and License

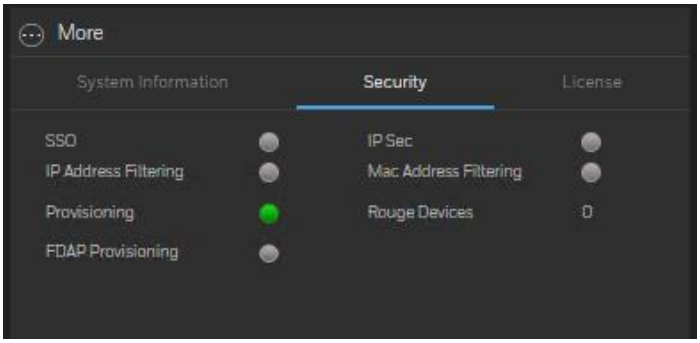
  System Information:

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



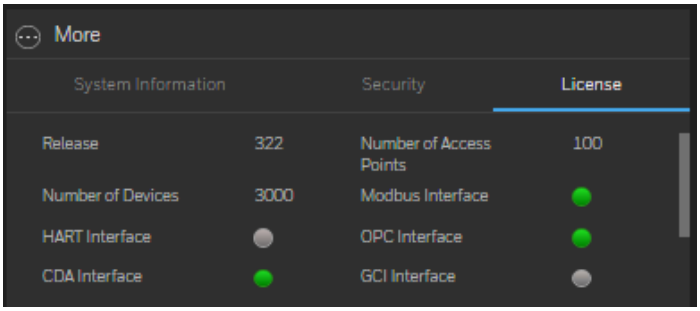
- Security:

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

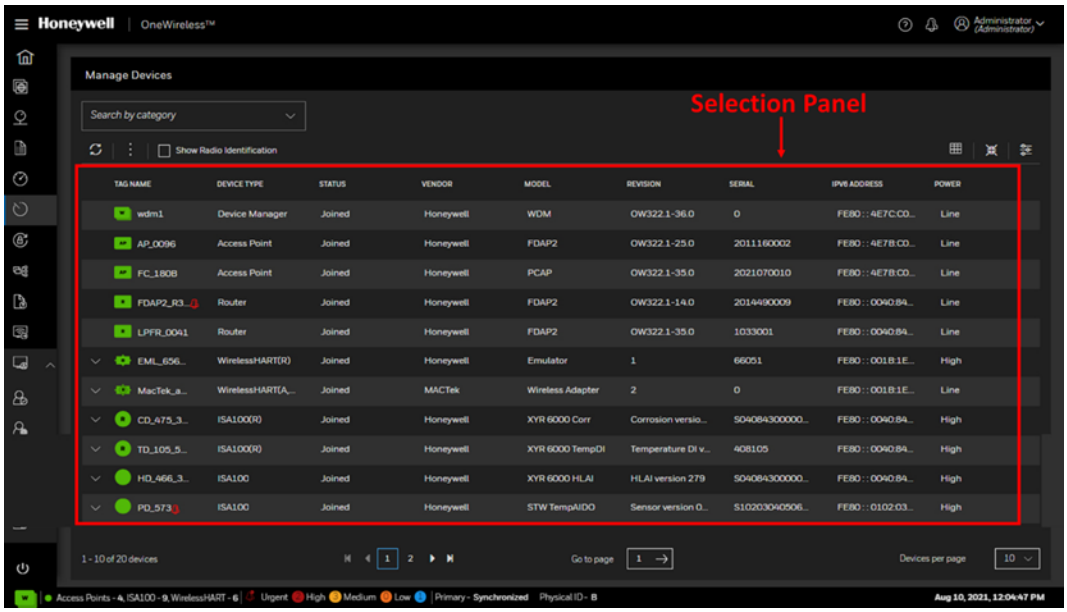


- License:

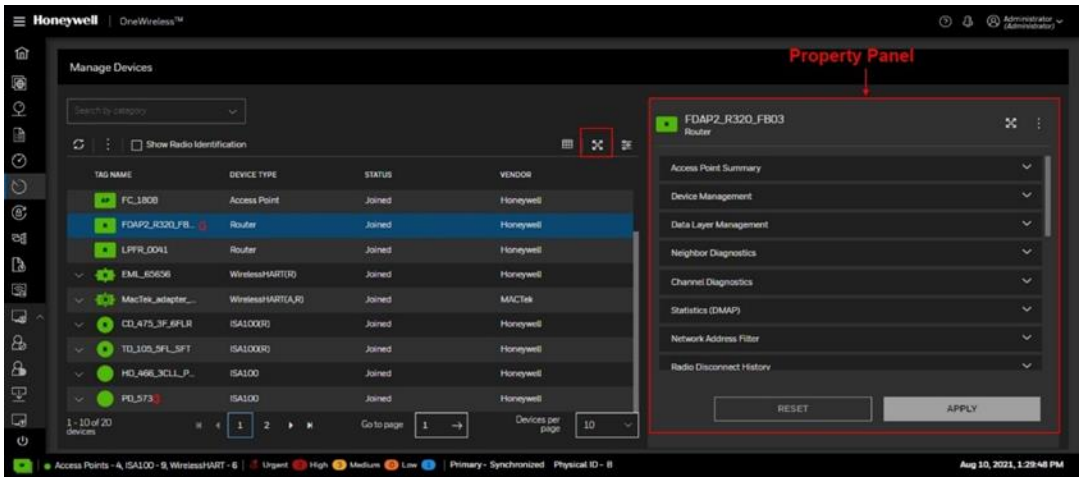
  Provide the information on license installed.



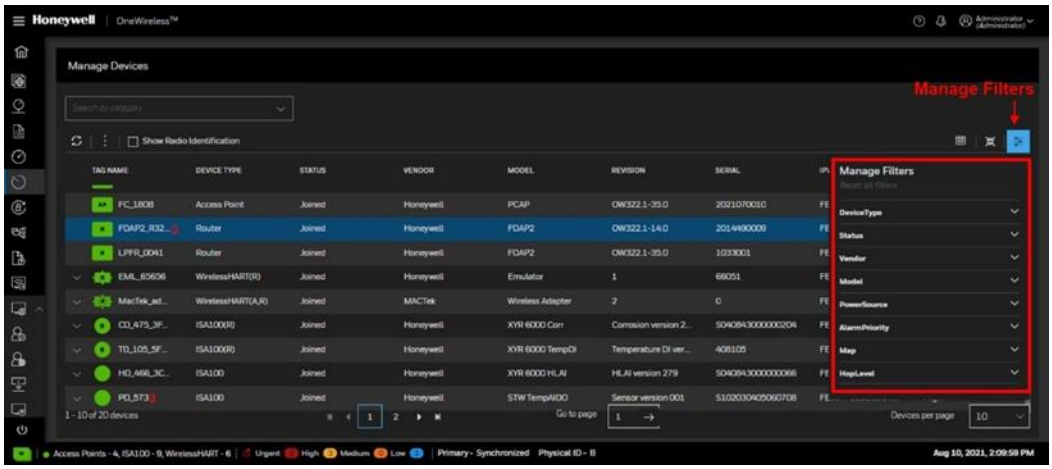
Selection Panel: The Selection Panel in the OneWireless user interface provides a list of all the devices configured in the OneWireless Network. See [Manage Devices] section for more information.



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.



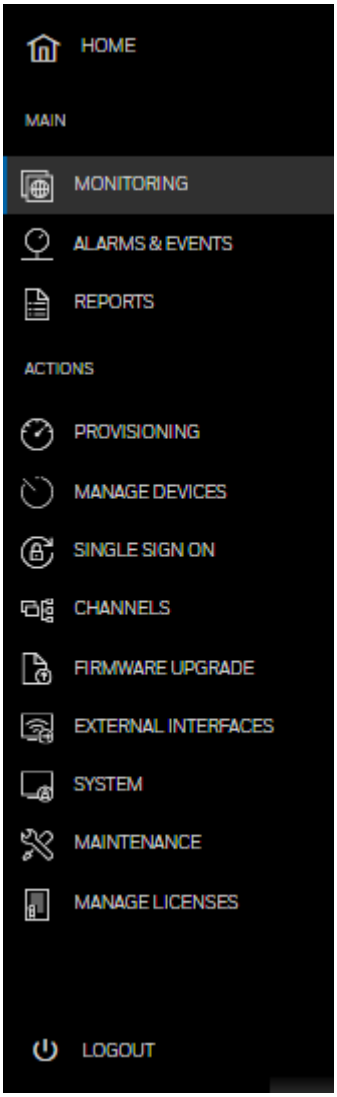
Manage Filters: The Filter option allows you to customize the device list by filtering the devices. By default, all the devices appear in the device list. You can filter by **Device Type**, **Device Status**, **Vendor, Model**, **Power Source**, **Alarm Priority**, **Hop Level**, and **Maps**.



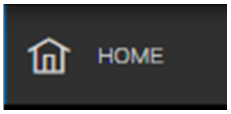
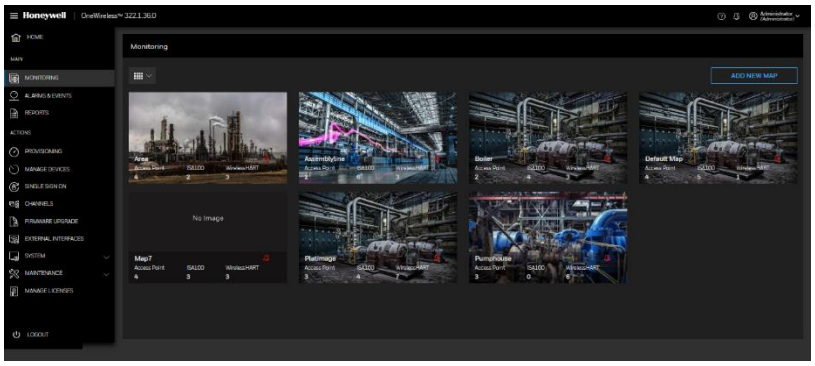
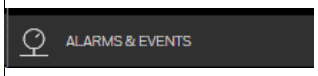
ATTENTION	When you set a filter, various system views are altered. For example, the map highlights only the devices for which the filter option is applied. Filter includes an option to filter by Map. This includes the Unplaced map so any device that has not been placed on a map can easily be detected. 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.

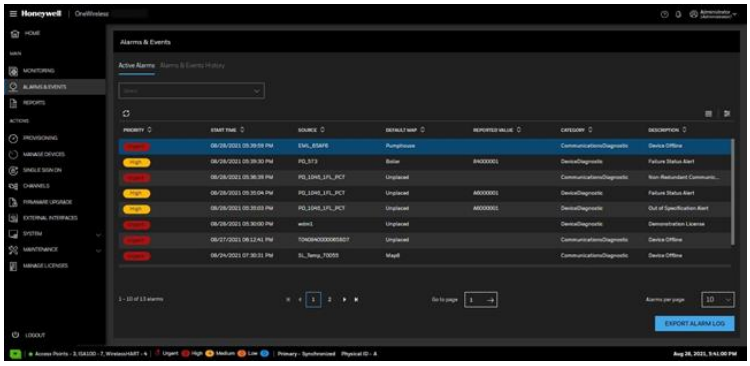
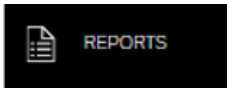
The following sections explain each element of the user interface in detail.

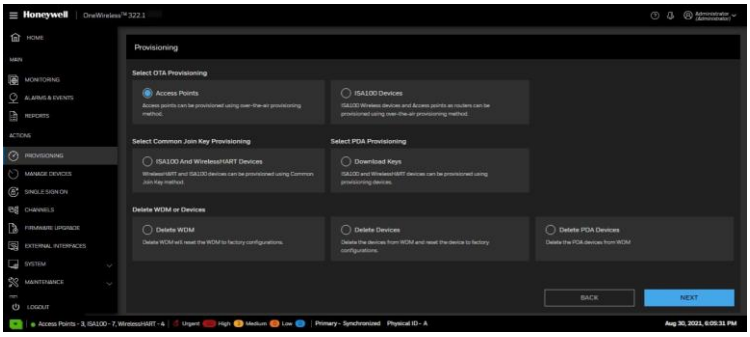
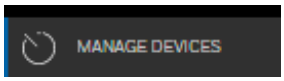
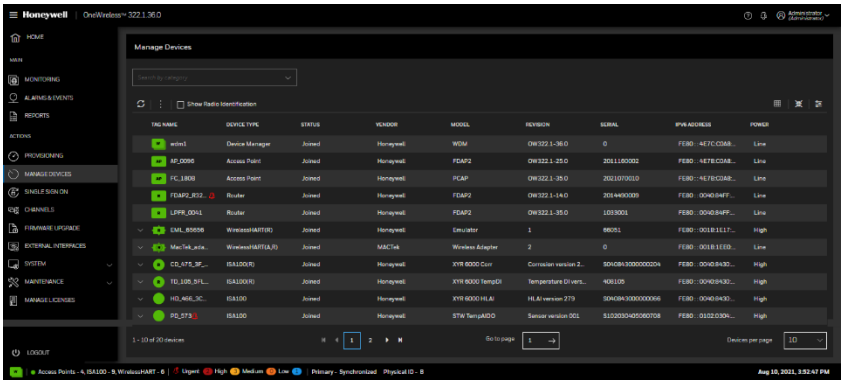
Left Navigation Menu bar

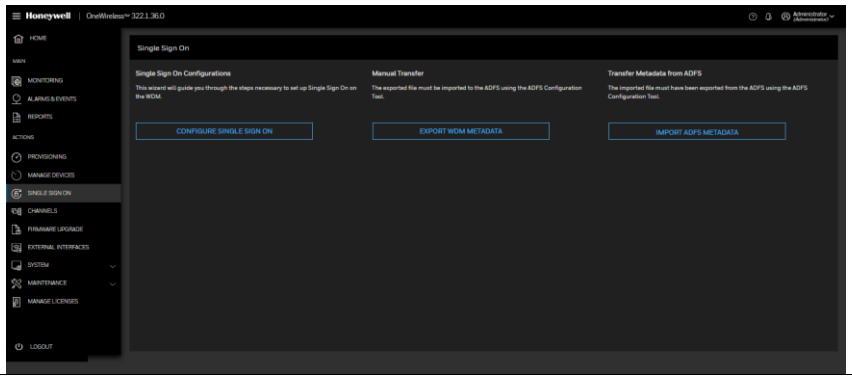
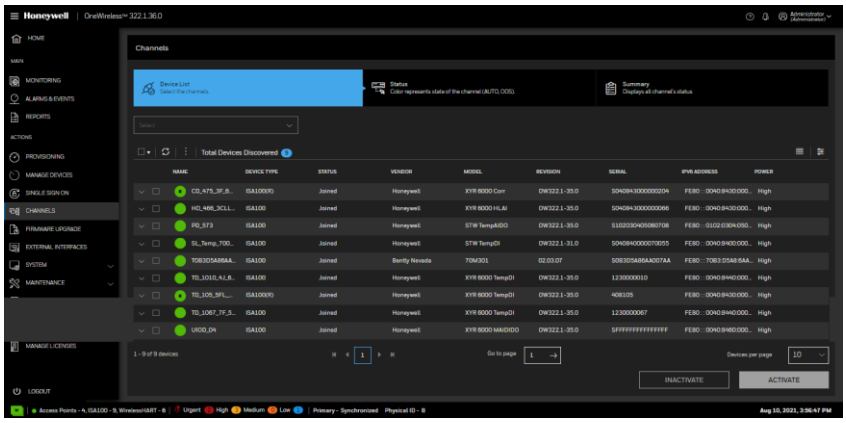
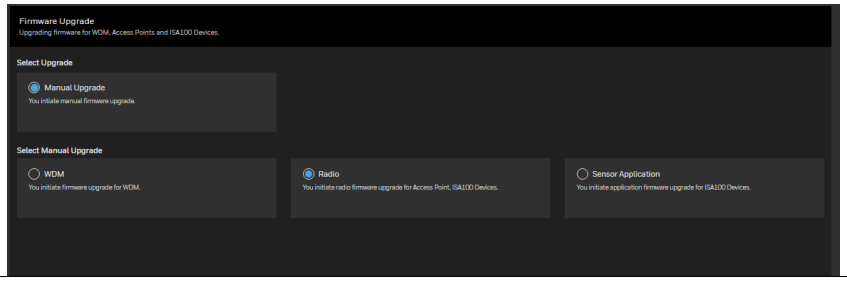


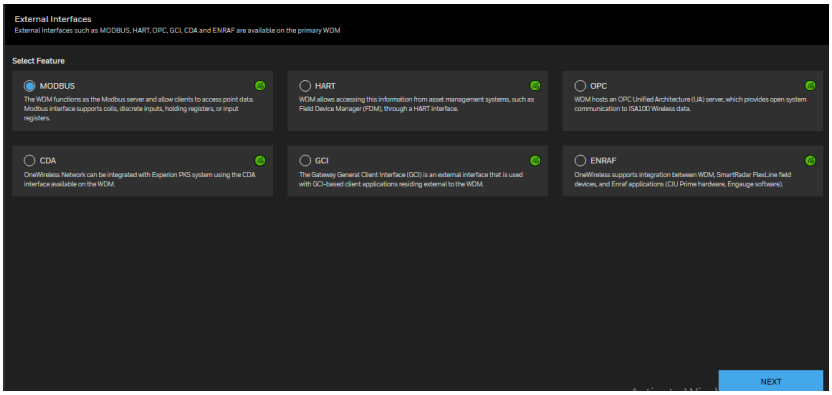
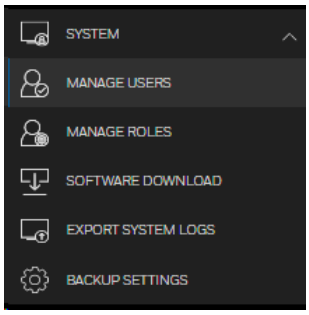
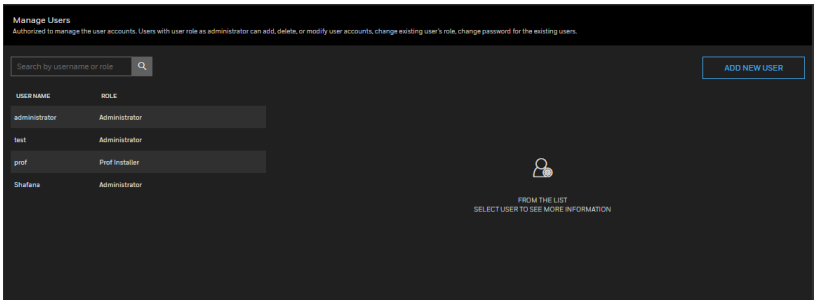
The Left Navigation Menu bar in the user interface is described in the following table.

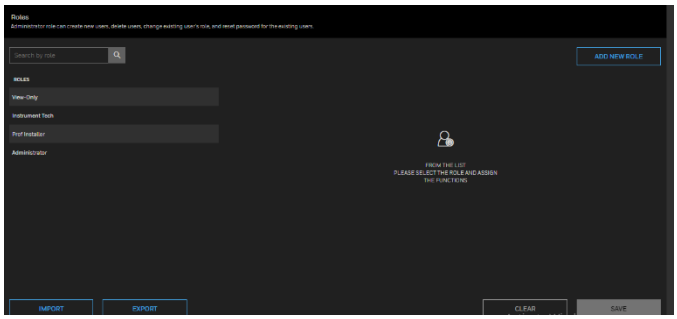
Tab/icon	Description
Home  	Home menu contains several dashboards for real time monitoring of OneWireless network health. It mainly contains status indicators like system performance, interface performance, inventory, battery, bandwidth utilization, system information, security and license. See section "Left Navigation Menu bar "for more details. 
Main Group	
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 About map view **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.  • The Alarms/Events History tab: Provides a tabular view of the events. It is possible to export the alarm log and the event log for a particular period.
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 • Device History • 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 "Provisioning " for more information.

	 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 of the device only from the WDM. 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  	Manage devices lists all the devices in the network (selection panel). You can read and write the properties, view alarms/events for all the devices. For more information, see "Manage devices" 

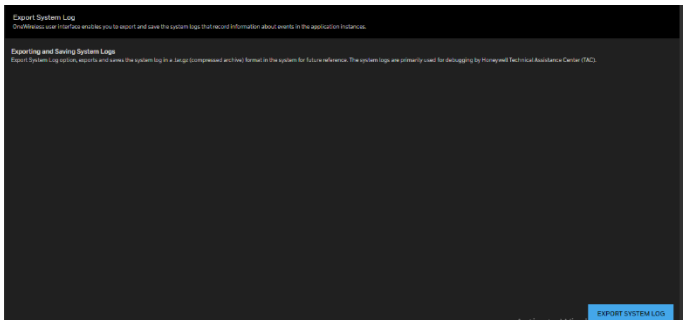
Single Sign On  	WDM supports single sign on feature. User can configure the WDM for single-sign on using this option. 
Channels  	 • **Activate**: Activates all the channels of the selected field device. Clicking the **Activate button** transitions the field device channel state from OOS to the currently configured Normal mode. • **Inactivate**: Inactivates all the channels of the selected field device. Clicking the **Inactivate** button transitions the field device channel state from AUTO to OOS. **ATTENTION** ***This group is disabled both on the secondary WDM and WirelessHART 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 "**Upgrading device firmware** "
External Interfaces  	External Interfaces such as MODBUS, HART, OPC, GCI, CDA and ENRAF are available on the primary WDM.  For more information, see section "**External Interfaces** "
System  	• **Manage Users**: Opens the **Manage Users** dialog box that contains the options to add, delete, or edit new user accounts.  • **Manage Roles:** Opens the Manage Roles dialog box that enables you to modify the configured user-permitted operations.

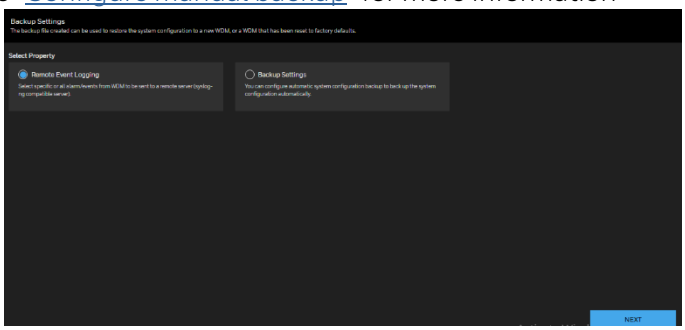
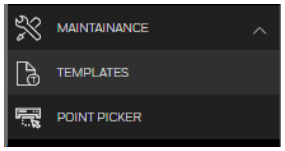
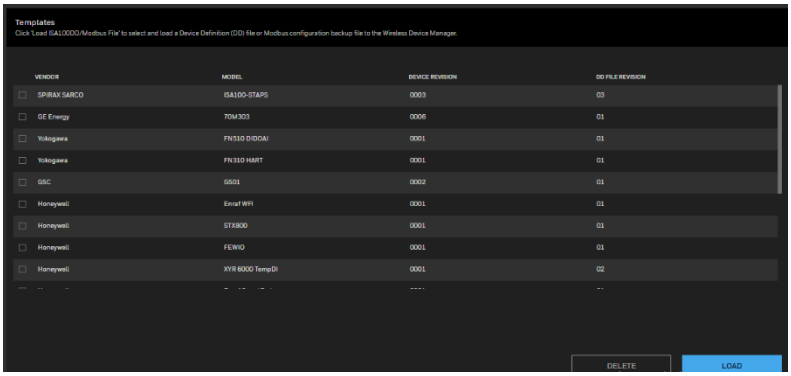
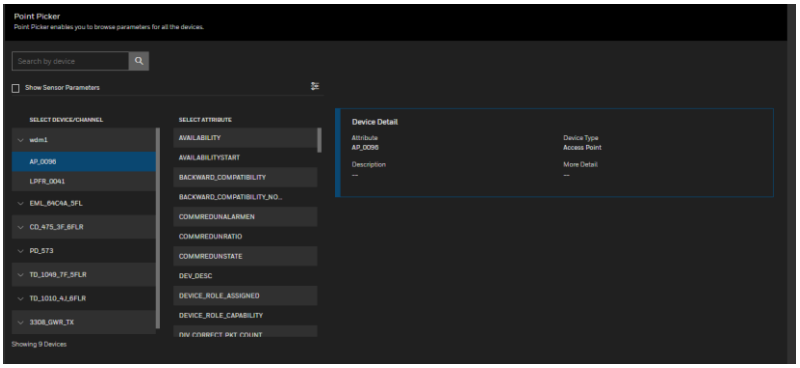
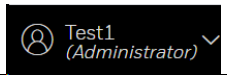


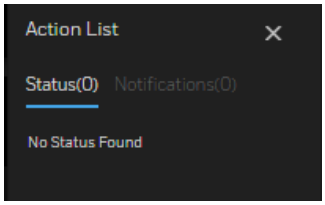
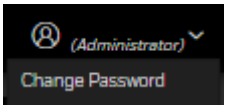
- Software **Download**: Enables you to download software provided on WDM.

- **Export System Log**: Enables you to export and save the system logs that record information about events in the application instances.



- **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 "Configure manual backup" for more information 
Maintenance  	• **Templates**: Uploads the vendor supplied ISA100 Wireless device DD file to the WDM. WirelessHART device DD files are not supported on WDM.  • **Point Picker**: Enables you to browse parameters on all devices and then drag and drop parameter into MODBUS coil or register configuration.  ***Attention*** ***This group is disabled on the secondary WDM.***
 	Displays the user who has currently logged on to the OneWireless user interface.

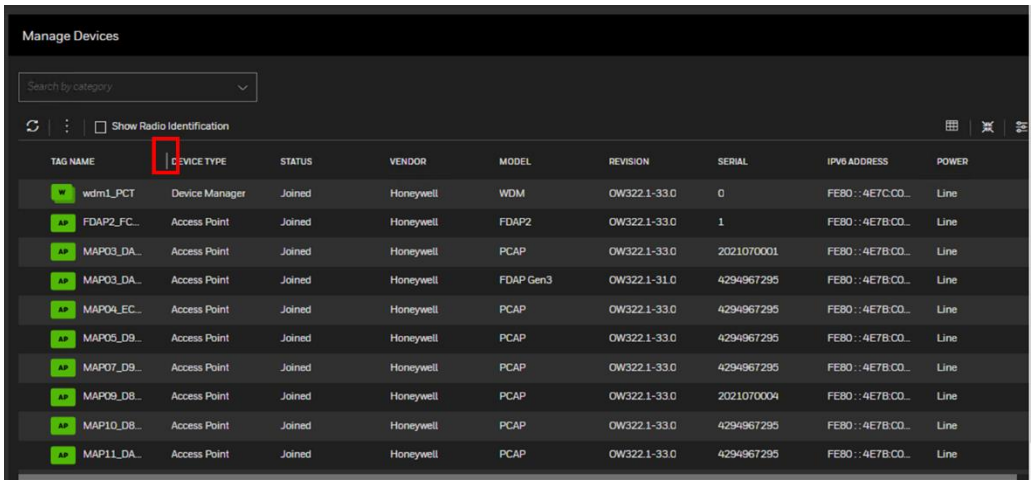
Action List 	Displays the status and notification. 
	Enables you to change the current user's password.

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.

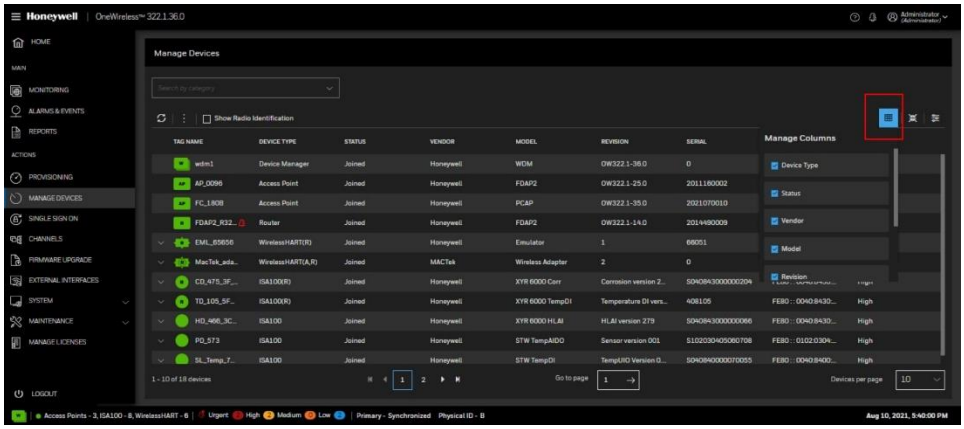
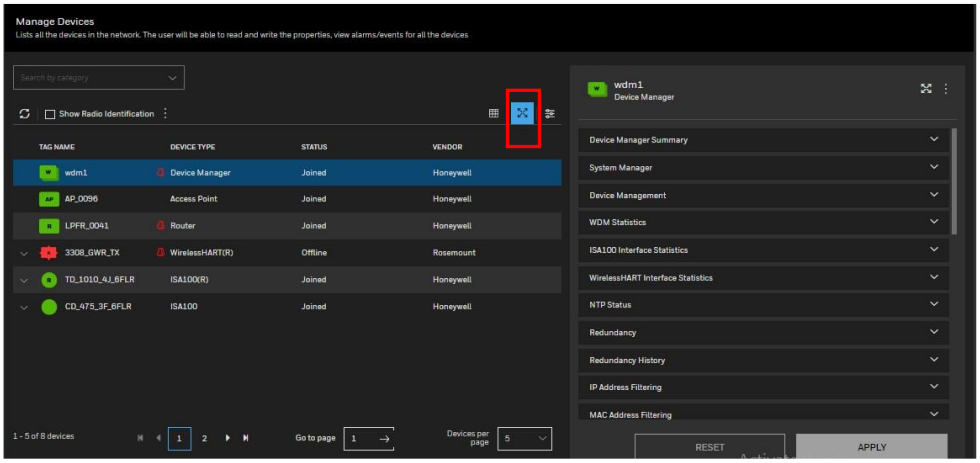
You can adjust the width of the column by adjusting the highlighted bar in the following image.

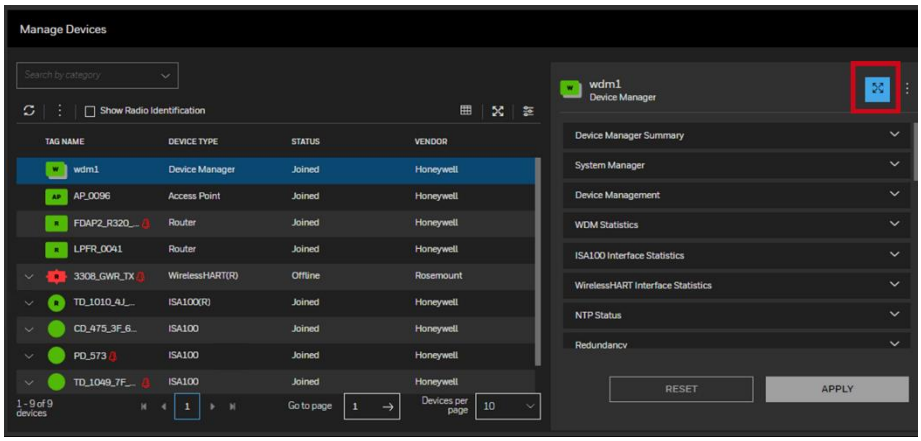
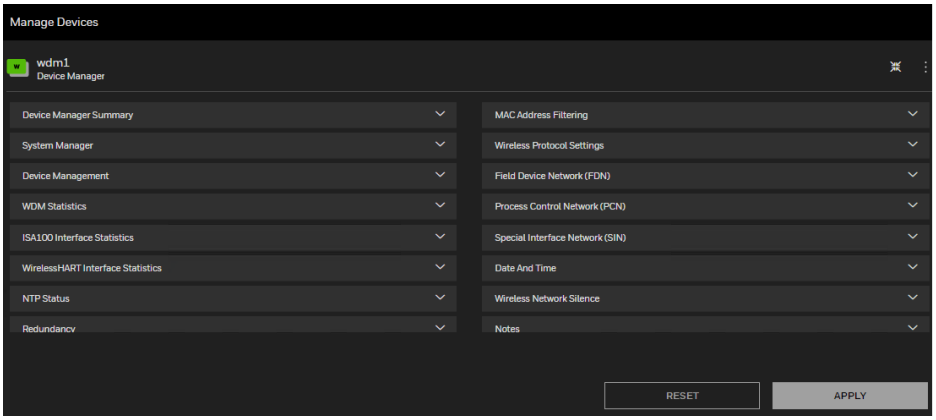
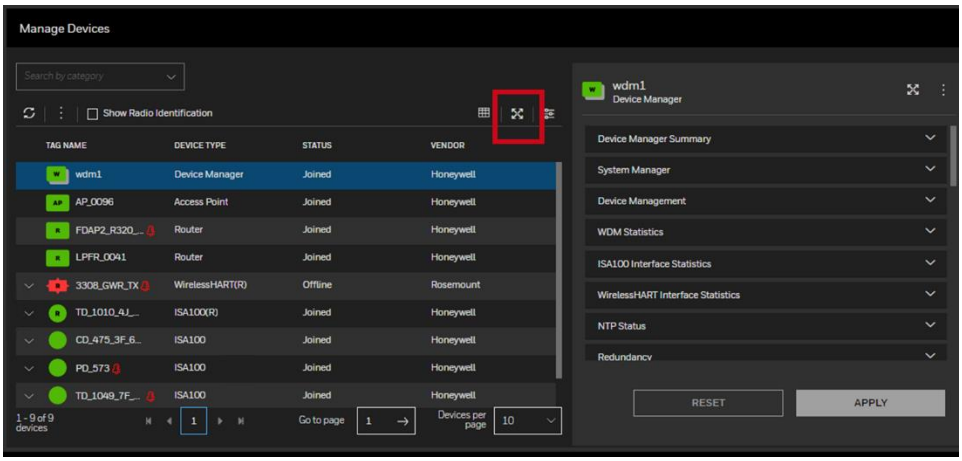


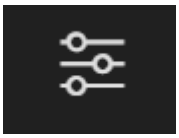
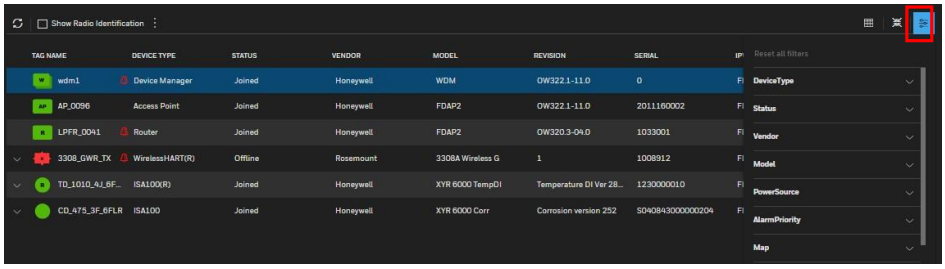
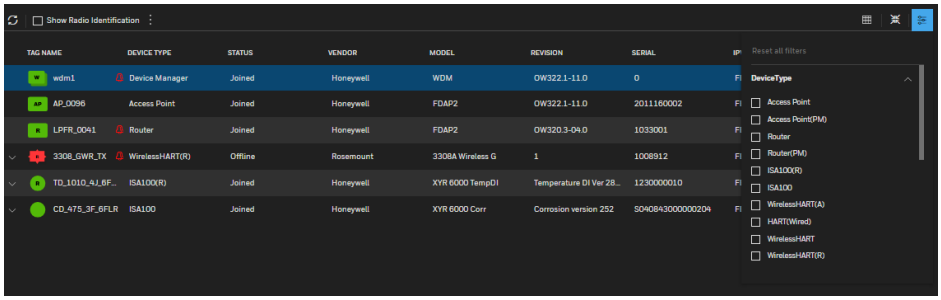
NOTE	**If any unprovisioned devices ae available in the selection panel, go to Provisioning from Left Navigation Menu and Accept the device for provisioning**

For more information see the section "selection panel"

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

Element	Function
Manage Columns 	Allows you to select the required attribute columns such as device type, status, vendor, model, serial number, and so on. 
Expand 	Select the device and click the highlighted icon to view the property panel. Click on individual property to expand the properties. For more information, see the "[Property panel](#)" section. 

	Further selecting the highlighted icon expands the property panel to a larger view.  
Collapse 	Select the collapse icon to collapse the propert panel. 

Manage Filters 	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.  

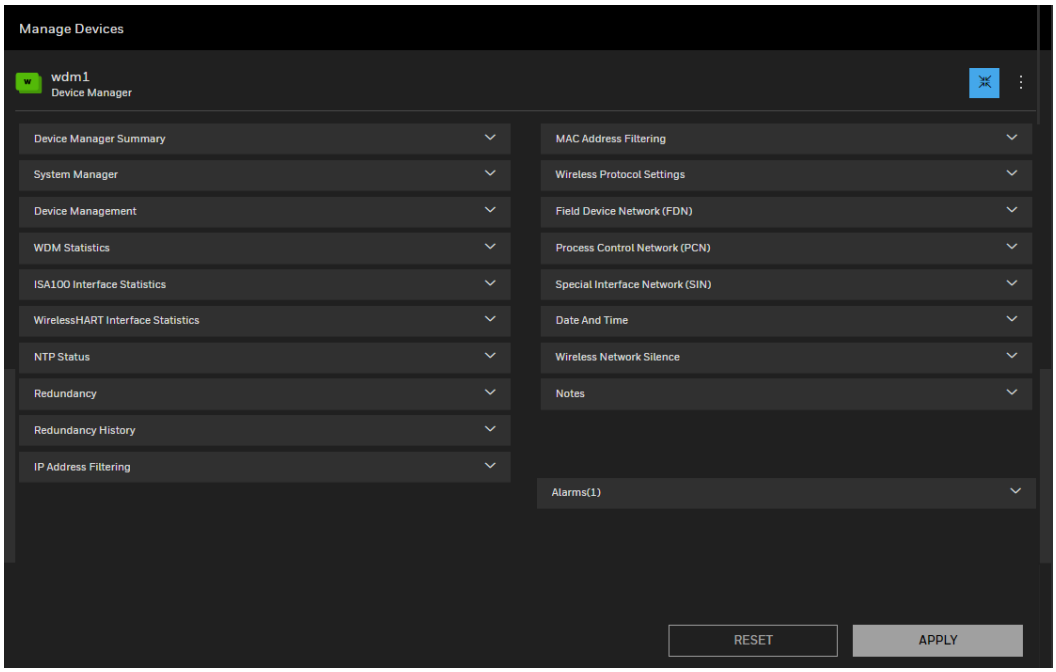
Property Panel

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.

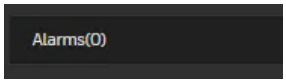
Selecting the required device in the Selection Panel displays all the configuration parameters of the devices that are accessible from the Property Panel. These configuration parameters are grouped into accordion panels that can be individually expanded or collapsed.

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



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

Table. 4. Property Panel elements

Element	Function
	Click to expand the Property Panel.
	Click to collapse the Property Panel.
	Click to save any configuration changes applied. This icon is enabled only if you have made any changes in the user interface.
	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.
	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...
	Non -Redundant WDM
	Redundant WDM
	FDAP router
	Access Point or FDAP access point
	Offline FDAP access point
	Offline FDAP router

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

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

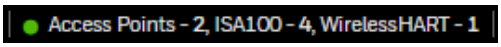
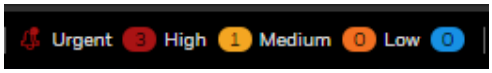
	For ISA100 Wireless device, Channel in Auto/MAN mode For WirelessHART Device, the variable status is Good.
	For ISA100 Wireless device, Channel in inactive/OOS mode.
	Channel becomes grey when the data is being fetched from the device. For a digital output channel, grey indicates the MAN mode, where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

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

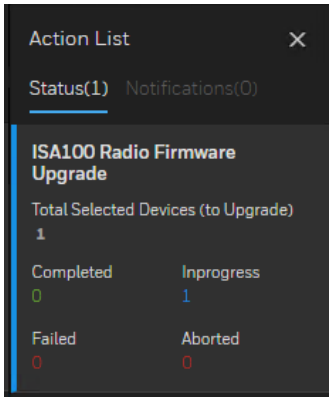
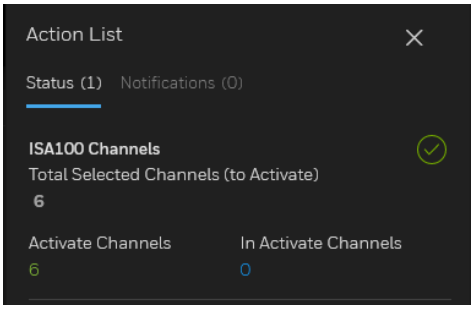
Status bar

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
	Number of online devices.
	Displays all the active alarms. Click the Alarms box to open the Active Alarms table in the **Alarm/Events** tab.
	Displays the redundancy role and synchronization status.
	Displays the date and time.

Notification List

Pane	Description
	Firmware upgrade status is displayed when you have initiated a firmware upgrade of any device. As the status bar displays the progress, you can close the **Firmware Upgrade** dialog box to allow the operation to run in the background. Click this box to open the **Firmware Upgrade** dialog box.
	Channel Activation/Inactivation

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 "Setting up the monitoring area".

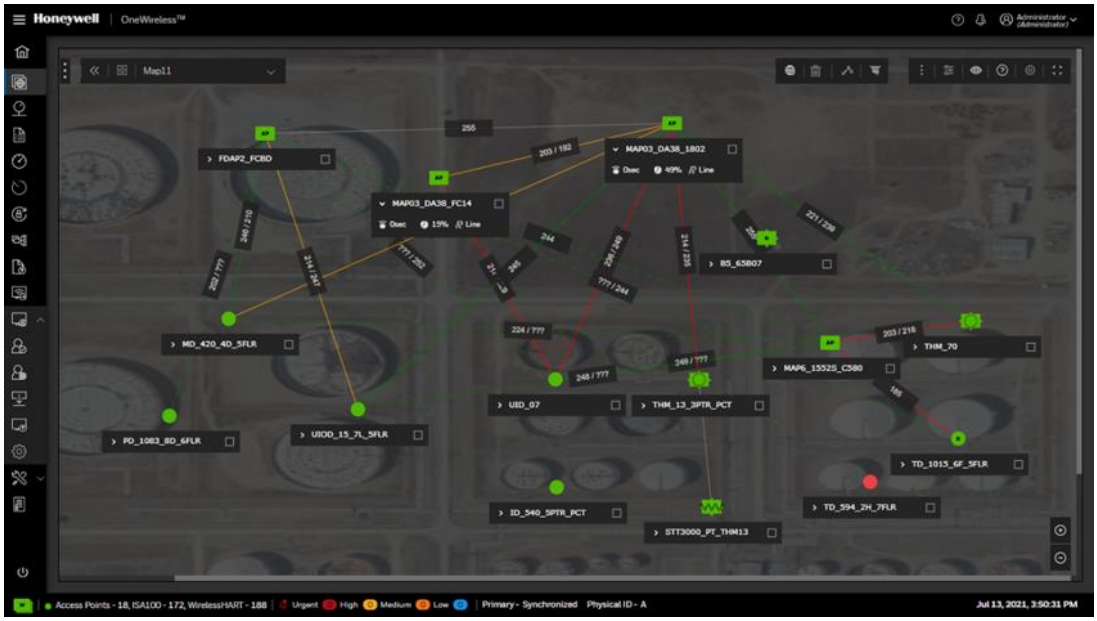
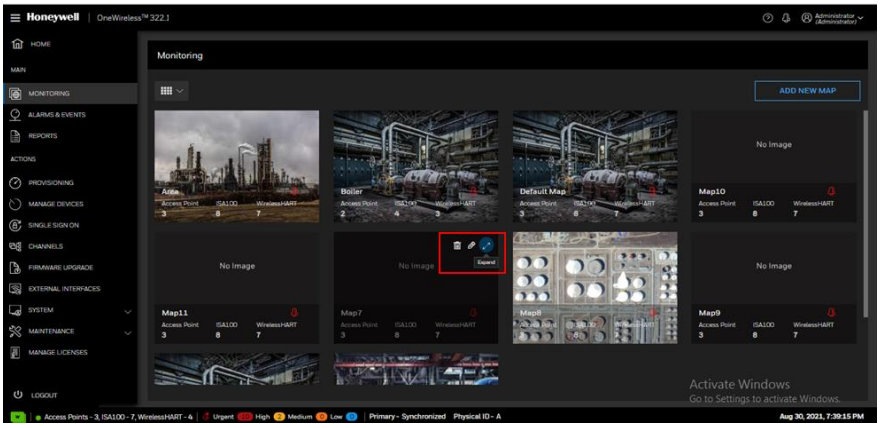


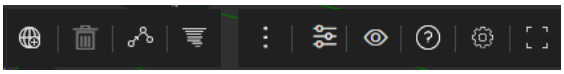
Fig. 10. Map view

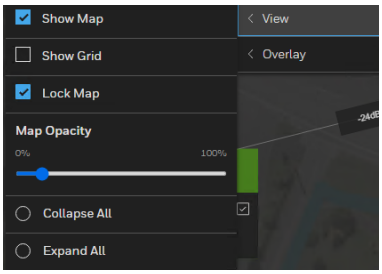
You can select individual devices by selecting the checkboxes near the device.

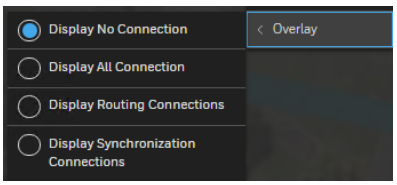
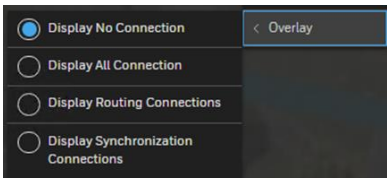
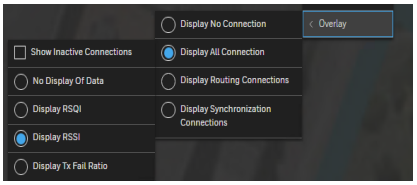
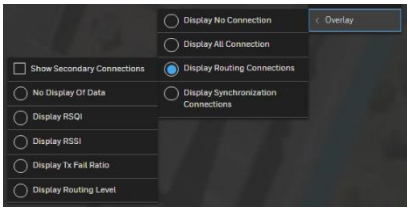
ATTENTION	**To display the map on the Monitoring page, click icon.**  **For more information about map controls, see the section, "About map view"**

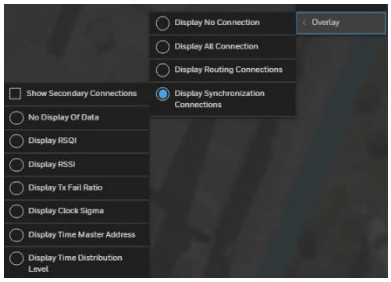
The following are the map navigation controls that are available in the map view.

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.
	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. 
	Allows to customize the device list by filtering the devices. See Section "Manage Filters" for more information
	Allows to add a Map.
	Allows to remove devices from Map.
	Displays the connection Status Options which enables you to define the quality thresholds for link quality. For more information about Connection Quality Configuring Connection
	Displays the property panel.

	Allows to select/ unselect devices.
	Allows to view the devices in the map.
	Displays the Device Replacement Help window.
	Displays Full screen.
	Following options displays: • View • Overlay
	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. • Expand All: Click the Expand All option to expand all collapsed 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 Routing Connections • Display Synchronization Connections ***Attention*** ***Depending on the Overlay option selected, the other options available are displayed.***
	Click the Display No Connections option for not displaying any connections on the map.
	Click the Display All Connections option for displaying all connection details on the maps. The following are the options: • Show Inactive Connections: Select the Show Inactive Connections check box to display inactive connections. • 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.
	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 secondary connections. • 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 Routing Level: Click Display Routing Level to display routing level.

	Click the Display Synchronization Connections option for displaying all clock connection details on the maps. The following are the options: • Show Secondary Connections: Select the Show Secondary Connections check box to display secondary connections. • 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 **"Verifying connectivity using maps"**

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.

Table. 7. Field device performance indicators

Device performance indicators	Description
	Displays the battery level as low, medium, high, or unknown.
	Displays the publishing rate at which the PV data is published.
	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.
	It represents that the device is line powered

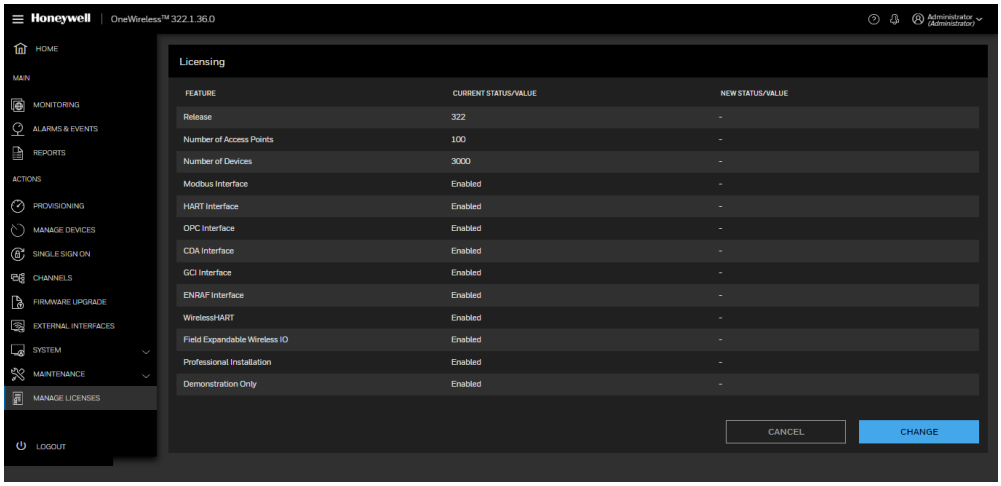
Installing the WDM license

Prerequisites

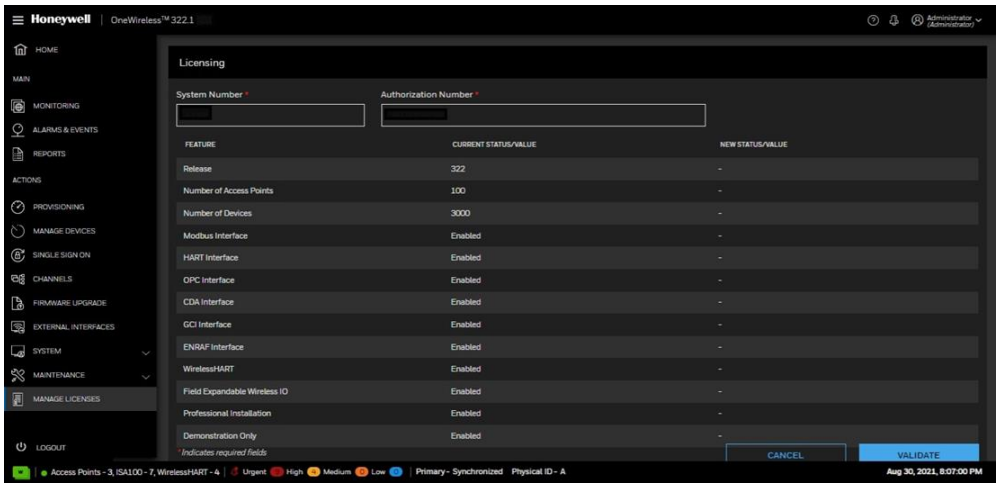
- Ensure that you have logged on to the OneWireless user interface.
- Ensure that you have a valid WDM license key. You can obtain the license key as a part of OneWireless ordering process.

To install a WDM license

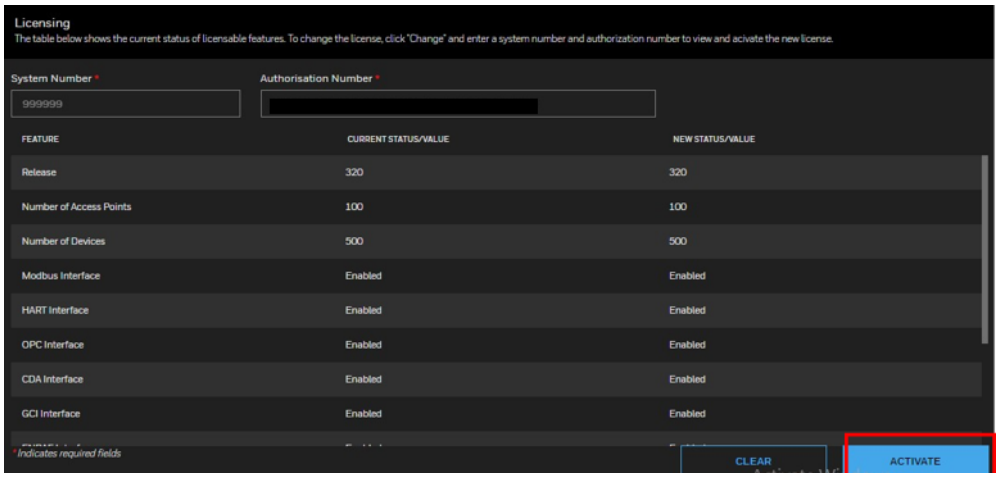
1. On the Left Navigation Menu bar, click **Manage Licenses**. The Licensing window appears and click **CHANGE**.



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



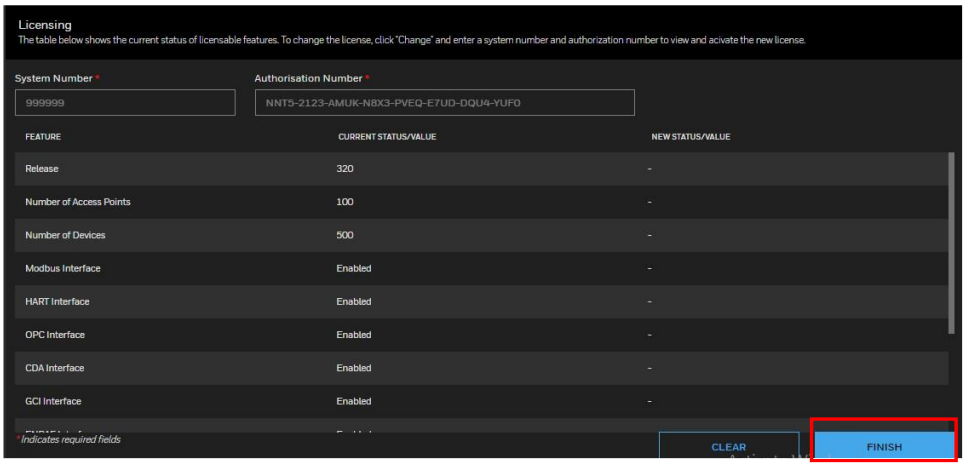
Based on the features enabled in the license, the **Licensing** window shows the difference in Status/Value.



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

ATTENTION	*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 Authorization Number and re-try.*

3. Click **ACTIVATE** and click **FINISH** when done.



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

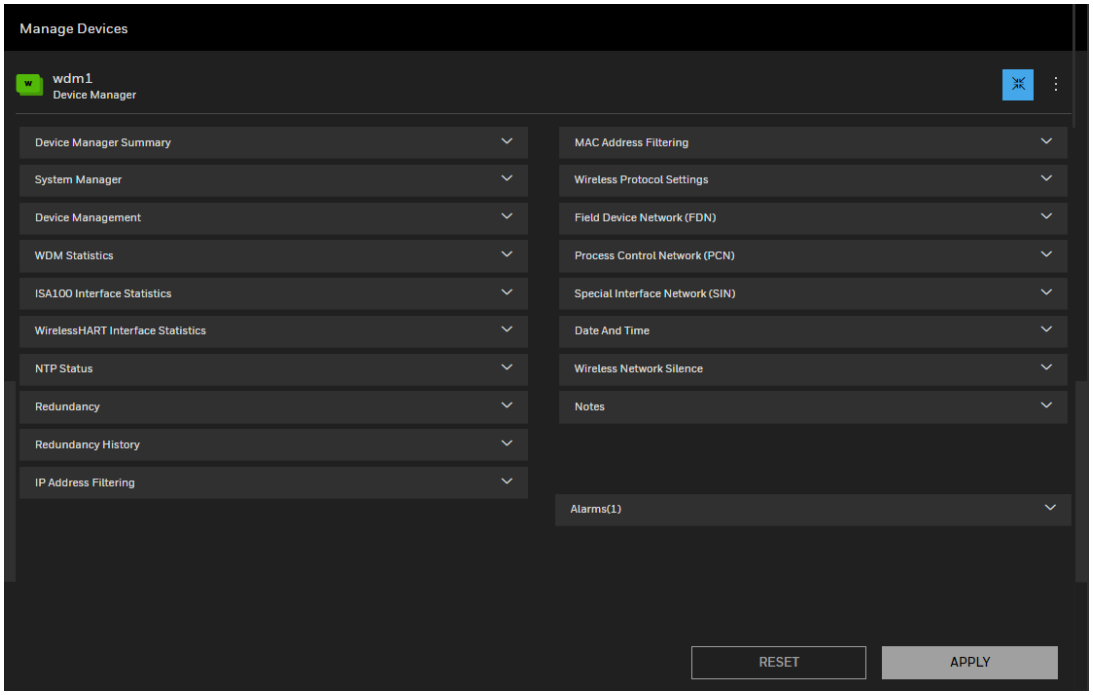
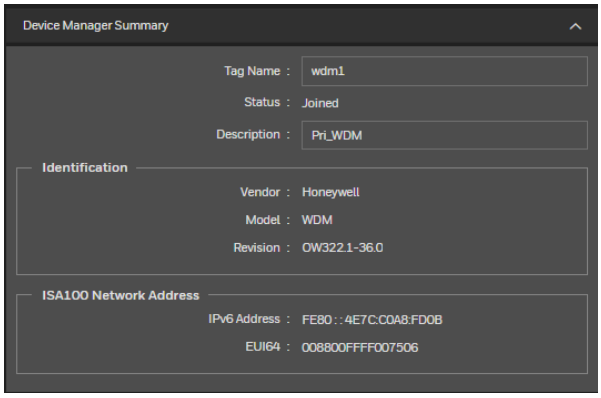
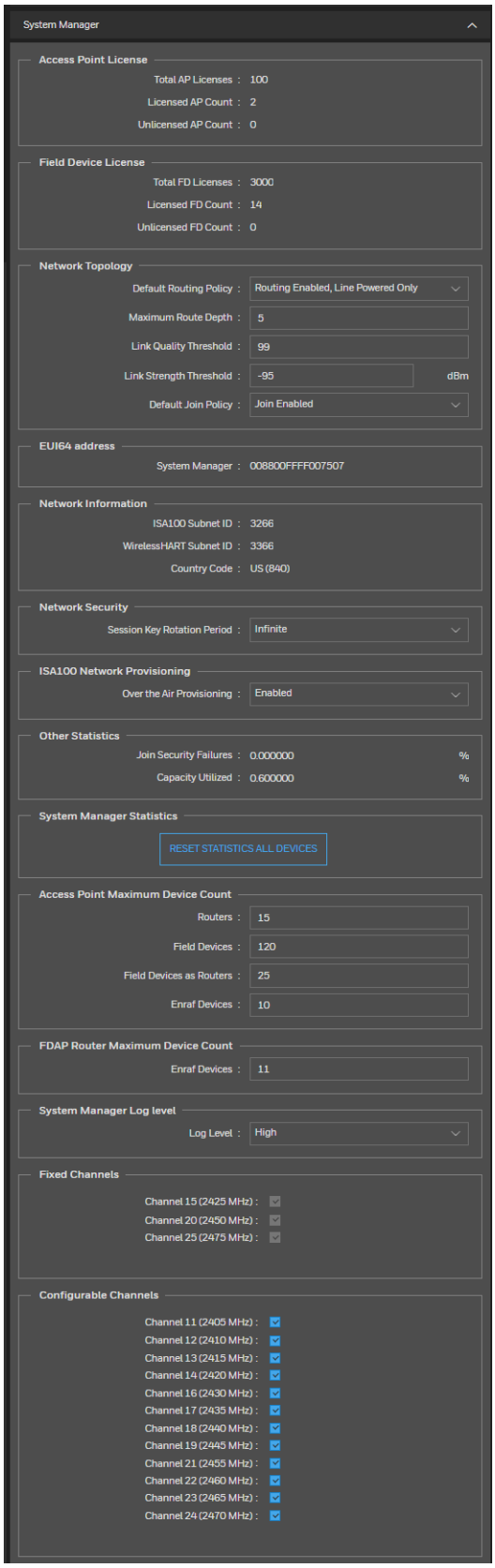


Fig. 11. WDM Property Panel

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

Property Panel	Description
Device Manager  	Device Manager summary information.

System Manager



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.

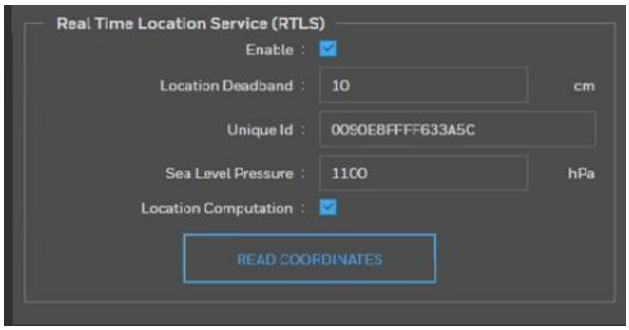
System Manager Log level

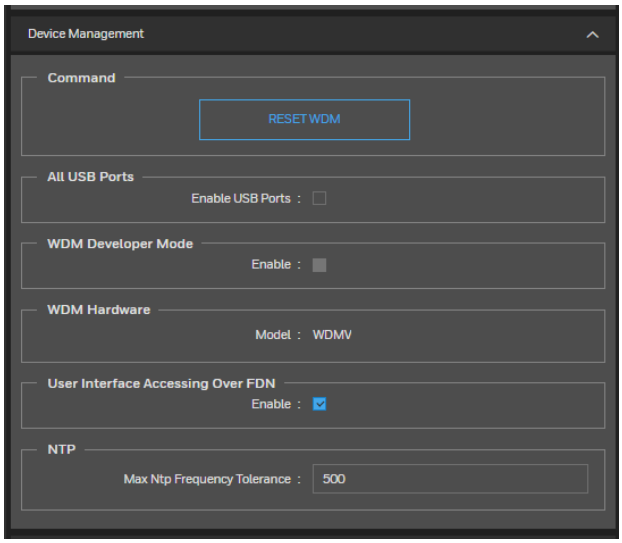
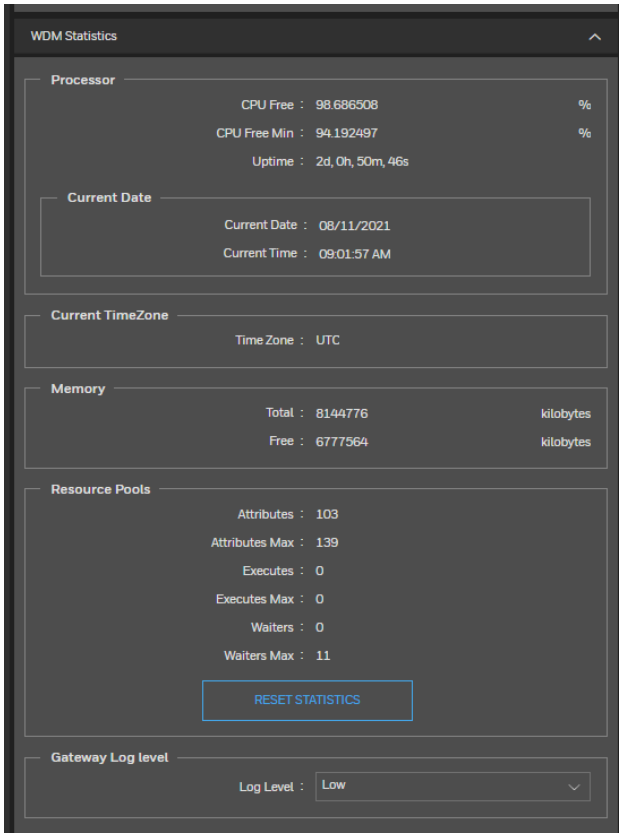
Log Level indicates the priority of the logs. For example, if multiple issues are reported during a short span of time, the Log Level is set to High to collect all the related logs.

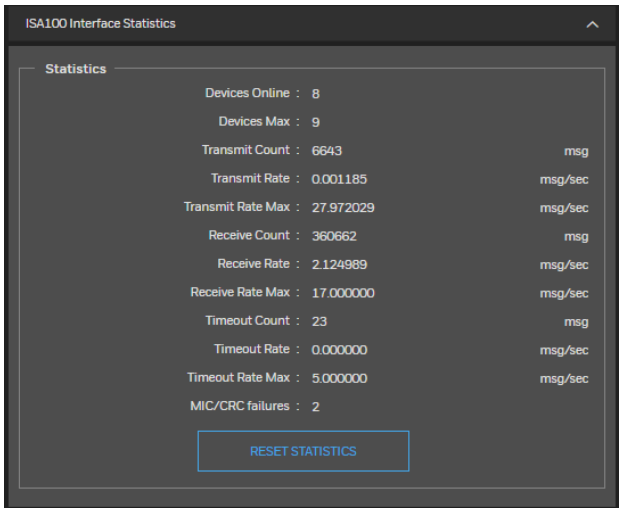
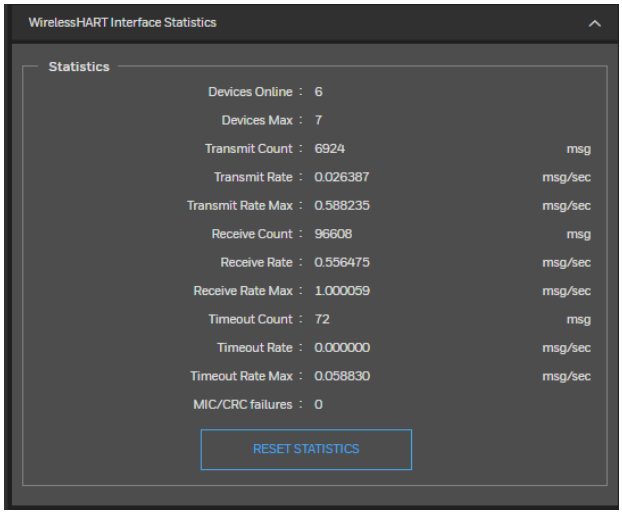
Channel Configuration

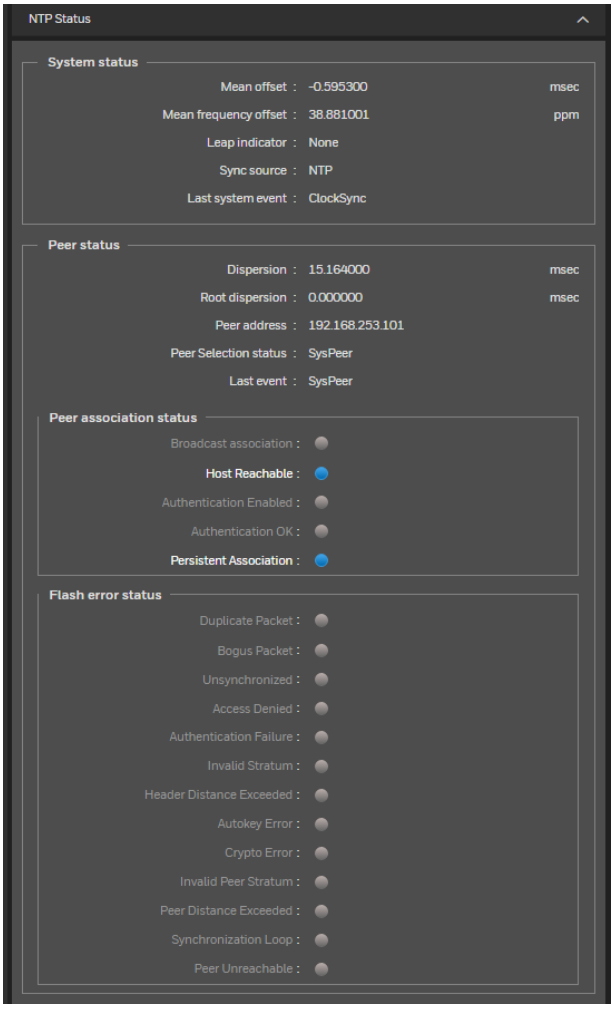
A minimum of 5 channels must be configured including Fixed and Configurable channels.

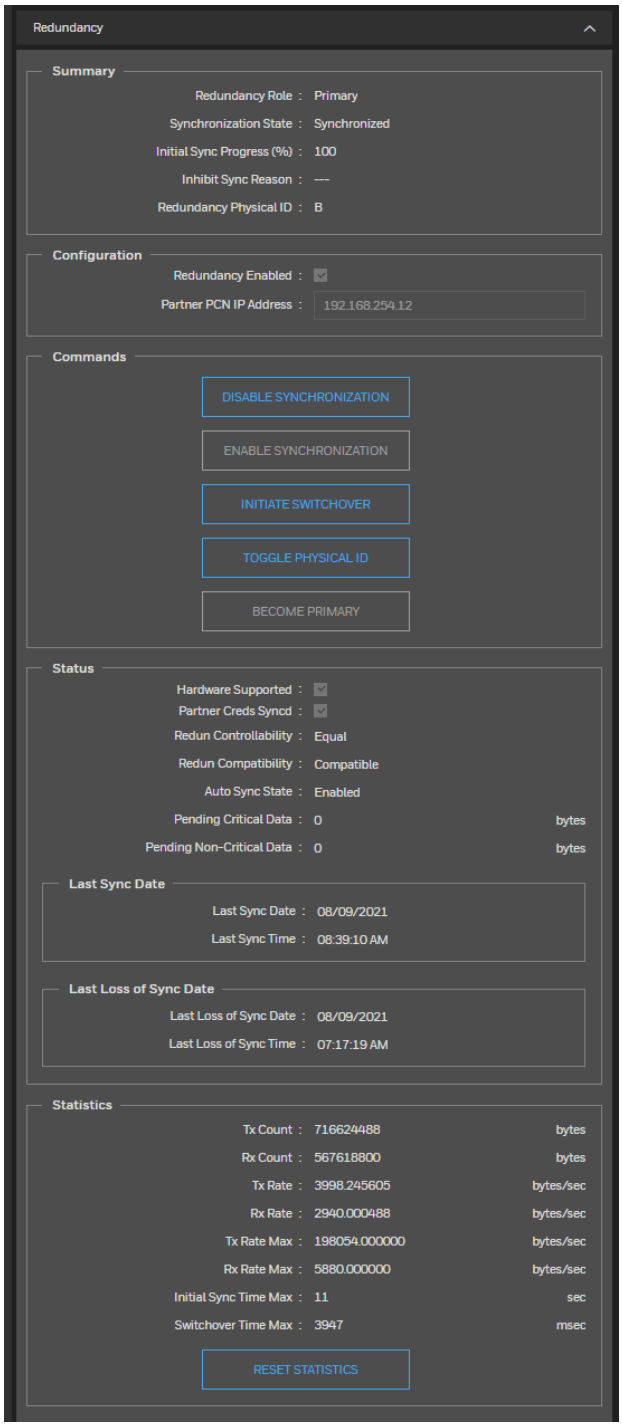
Access Point Maximum Device Count indicates the maximum capacity of Access Point with respect to different device types.

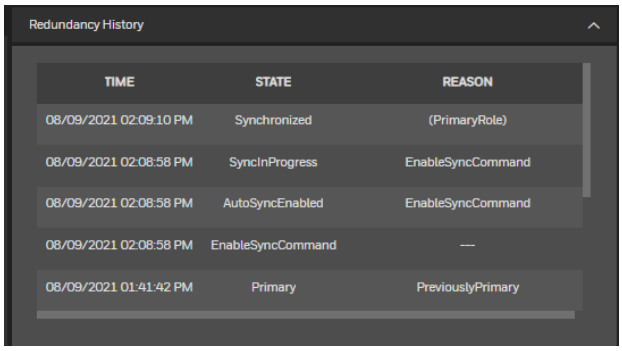
RTLS  	**Router Maximum Device Count** indicates the list of maximum capacity of FDAP as Router with respect to different device types. If a specific device type is not mentioned here it falls into generic field device type. **Real Time Location Service (RTLS)** You can enable the RTLS on the WDM for real time location monitoring using tag. **Location Deadband** indicates the minimum distance offset or minimum difference in distance computed between two consecutive ranging sequences required for 3 anchors for location computation. **Unique ID** indicates unique identification code per RTLS installation. **Sea Level Pressure** indicates sea level pressure at installation site used to determine the absolute altitude of anchor / tag. **Location Computation:** To enable or disable the Location Computation. **READ COORDINATES:** On clicking "**READ COORDINATES"**, WDM will read the current coordinates values from the Anchors.

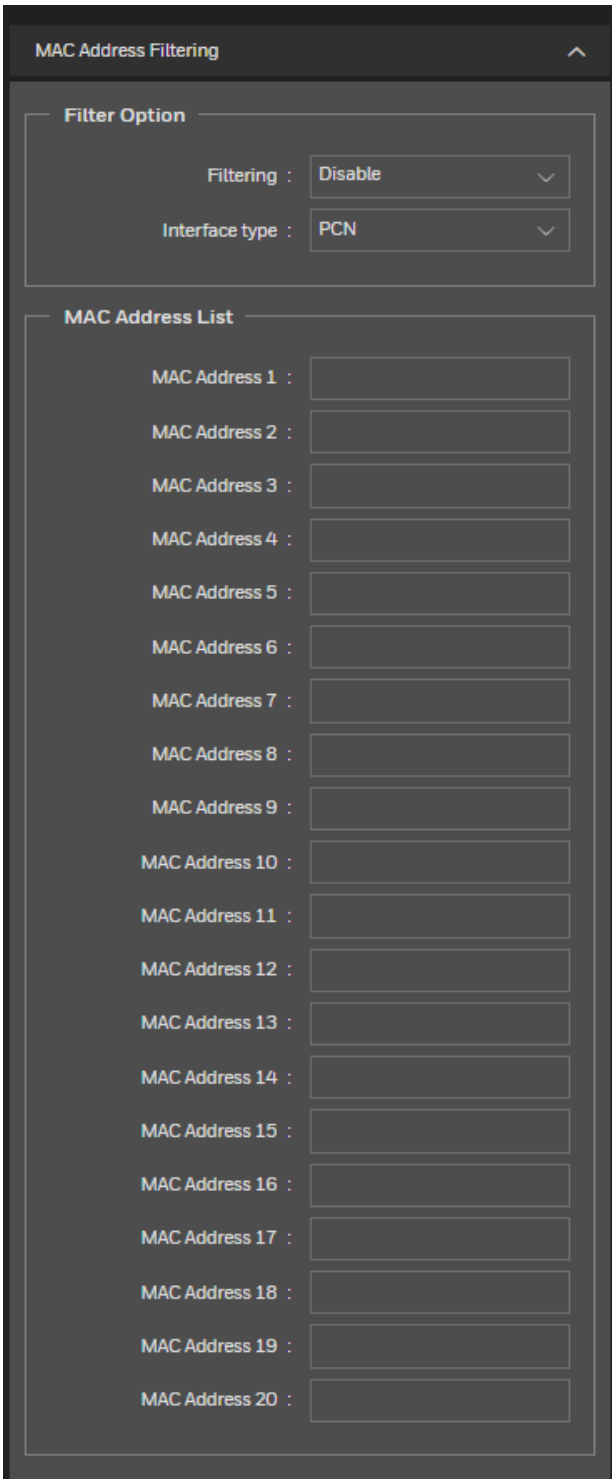
Device Management  	Command to reset the WDM and enable/disable the USB ports present on the WDM. You can disable the physical USB ports present on the WDM for security reasons. It provides the WDM Model. Allows to enable the User Interface Accessing Over FDN. You can provide the NTP frequency Tolerance.
WDM Statistics  	Hardware statistics of WDM.

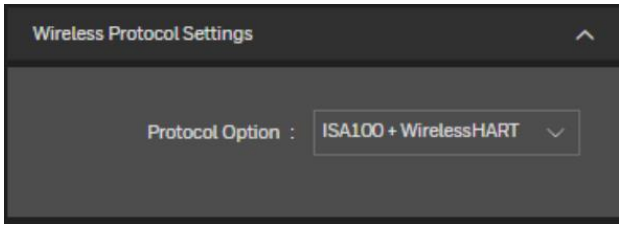
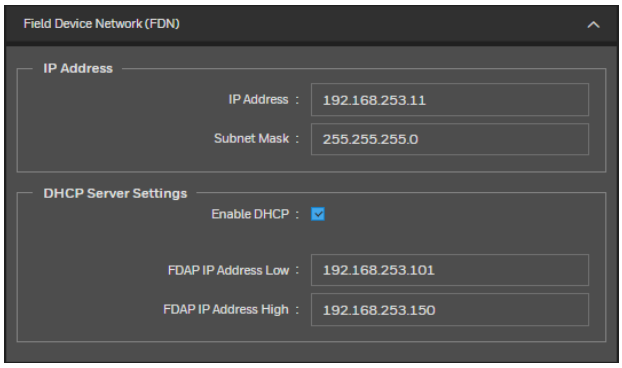
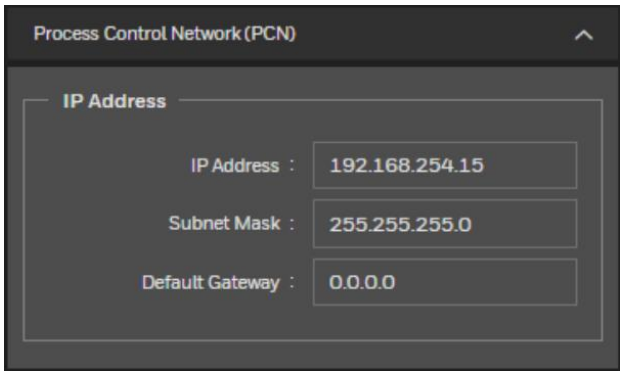
ISA100 Interface Statistics  	Statistics of ISA100 Wireless device connected to WDM.
Wireless HART Interface Statistics  	Statistics of WirelessHART device connected to WDM.

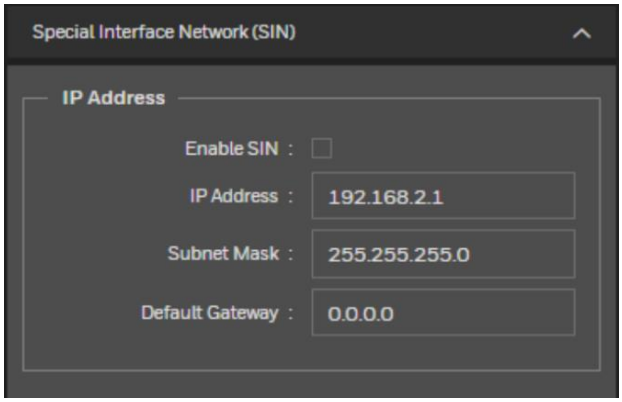
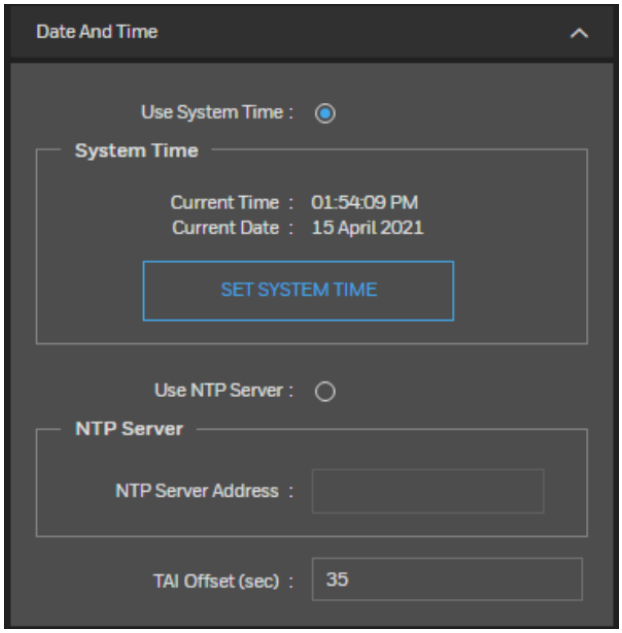
NTP Status  	Network Time Protocol (NTP), a networking protocol for clock synchronization between a server and other devices. WDM uses NTP for clock synchronization. The NTP time source could be an external NTP server or it could be an Access Point present in the network.

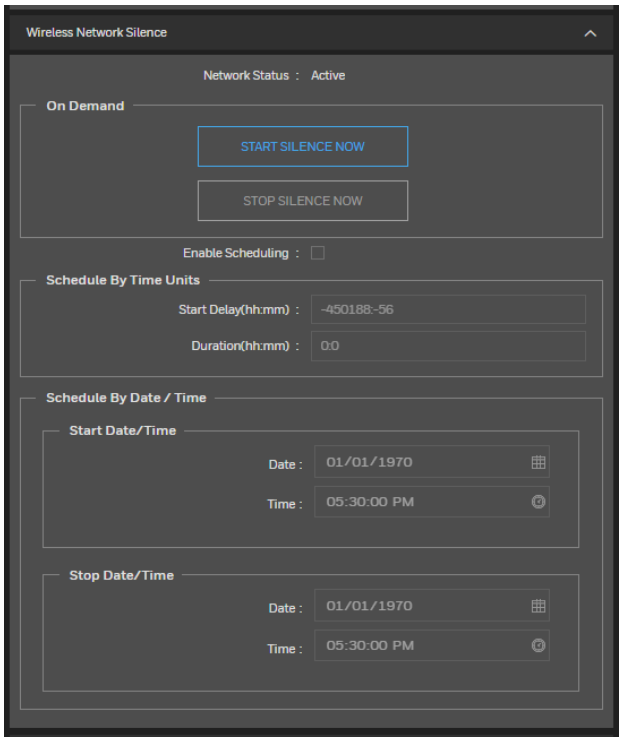
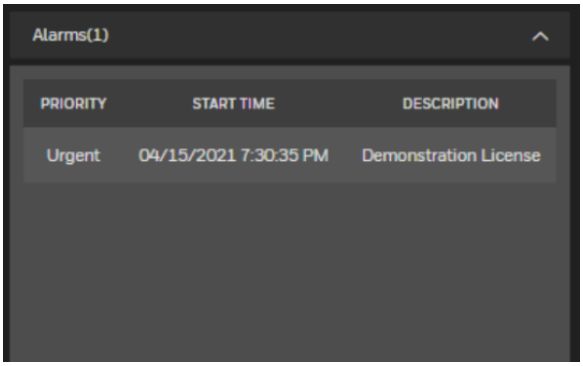
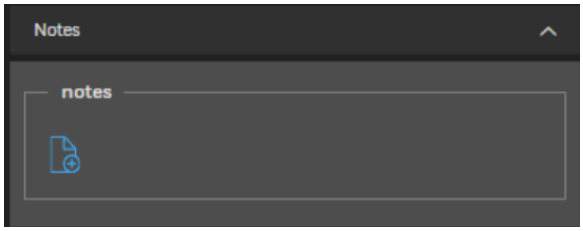
Redundancy  	Details of Primary and Secondary WDMs. Includes synchronization state & time, IP for secondary WDM, various commands to initiate synchronization and switchover, and so on.

Redundancy History  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	Time stamped WDM redundancy events.
IP Address Filtering  IP Address Filtering Filter Option Filtering : Disable Interface type : PCN IP Address List IP Address 1 : IP Address 2 : IP Address 3 : IP Address 4 : IP Address 5 : IP Address 6 : IP Address 7 : IP Address 8 : IP Address 9 : IP Address 10 : IP Address 11 : IP Address 12 : IP Address 13 : IP Address 14 : IP Address 15 : IP Address 16 : IP Address 17 : IP Address 18 : IP Address 19 : IP Address 20 :	**IP Address Filtering:** PCN and SIN ports on WDM are protected with IP address filtering. An administrator can allow or deny a client access to PCN and SIN ports on WDM by filtering his machine IP address. **NOTE:** **Make sure that you do not enter your own machine IP Address to be denied, as this may lead to blockage of access to WDM interface.** **NOTE:** Configure all IP addresses before enabling the Filtering Option.

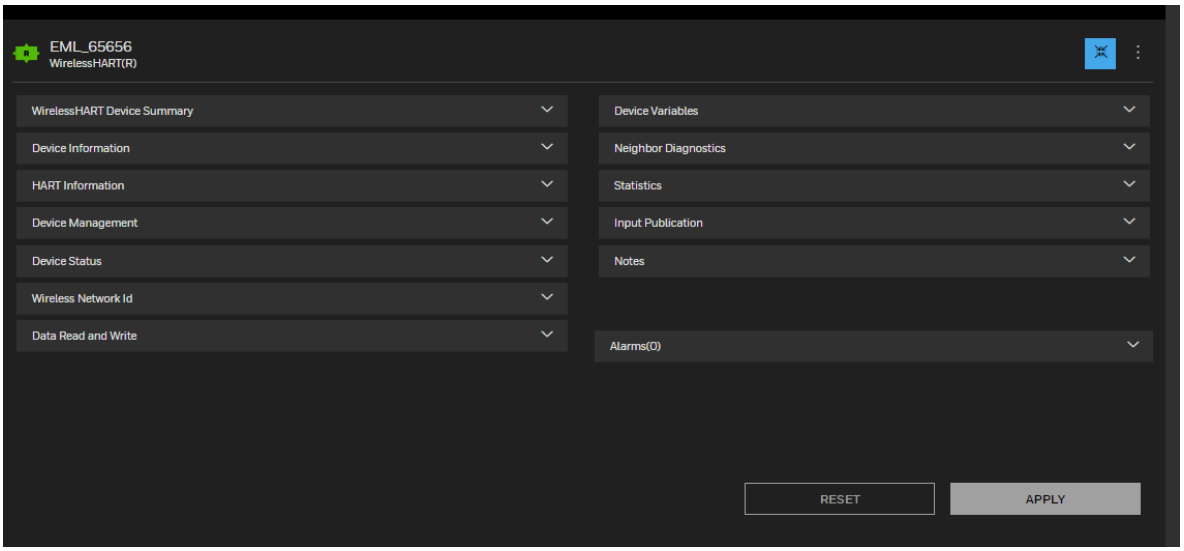
MAC Address Filtering	
	**MAC Address Filtering:** PCN and SIN ports on WDM are protected with MAC Address filtering. An administrator can allow or deny a client access to PCN and SIN ports on WDM by filtering his machine IP address. **NOTE:** **For a host computer, if MAC is denied and IP is allowed or vice versa, the settings may not work as intended.** **NOTE:** **Make sure that you do not enter your machine MAC Address to be denied, as this may lead to blockage of access to WDM interface.** **NOTE:** **Configure all MAC addresses before enabling the Filtering Option.**

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  	FDN details
PCN  	PCN details

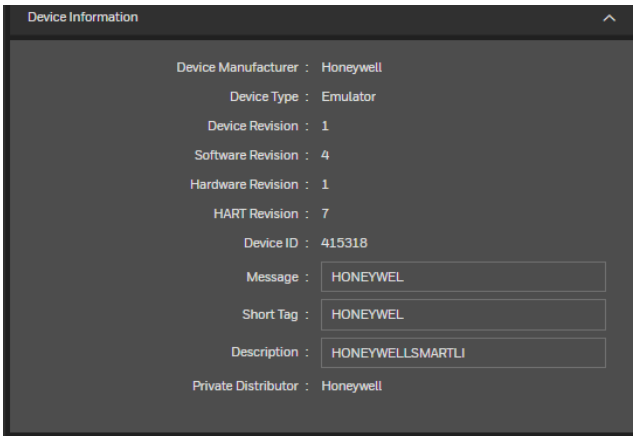
SIN  	SIN details **ATTENTION:** • *Make sure SIN IP address is not in same series of PCN or FDN IP address* • *WDM must reboot after SIN IP address is changed*
Date and Time  	Data and time information. You can either manually set the date and time or synchronize your WDM with the NTP server.

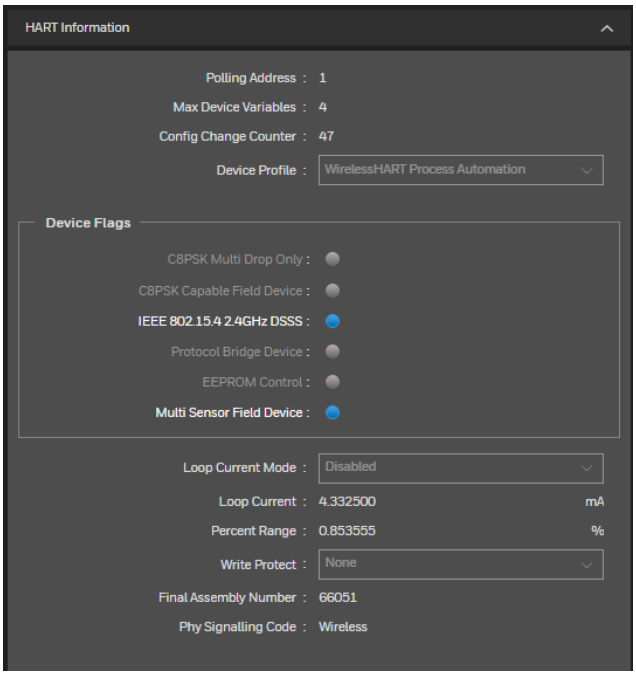
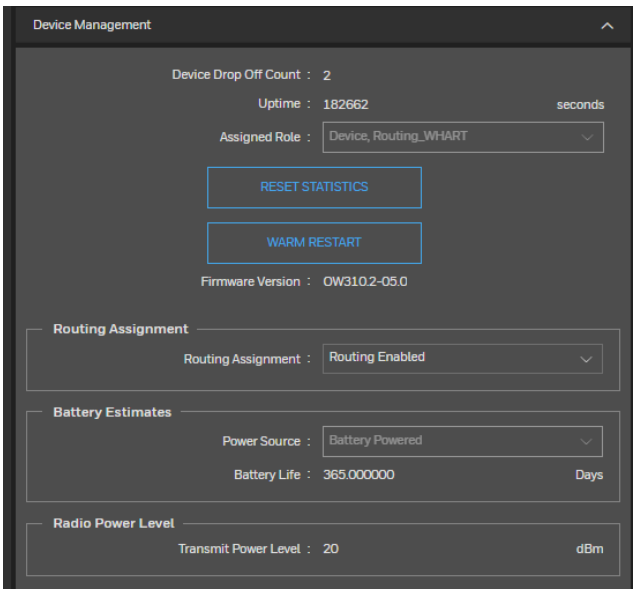
Wireless Network Silence  	In this state, only the access points are available while all the other devices are offline. Network Silence can be enabled in 3 ways. • On Demand: by manually starting or stopping this feature. • Enable Scheduling: by scheduling network silence for a later time along with the duration. • Schedule by Date/Time: by scheduling network silence for a later date or time along with the start and stop time.
Alarms  	Provides the information on Alarms which consists of Priority, Start time and description of the event.
Notes  	Add notes specific to WDM, if any.

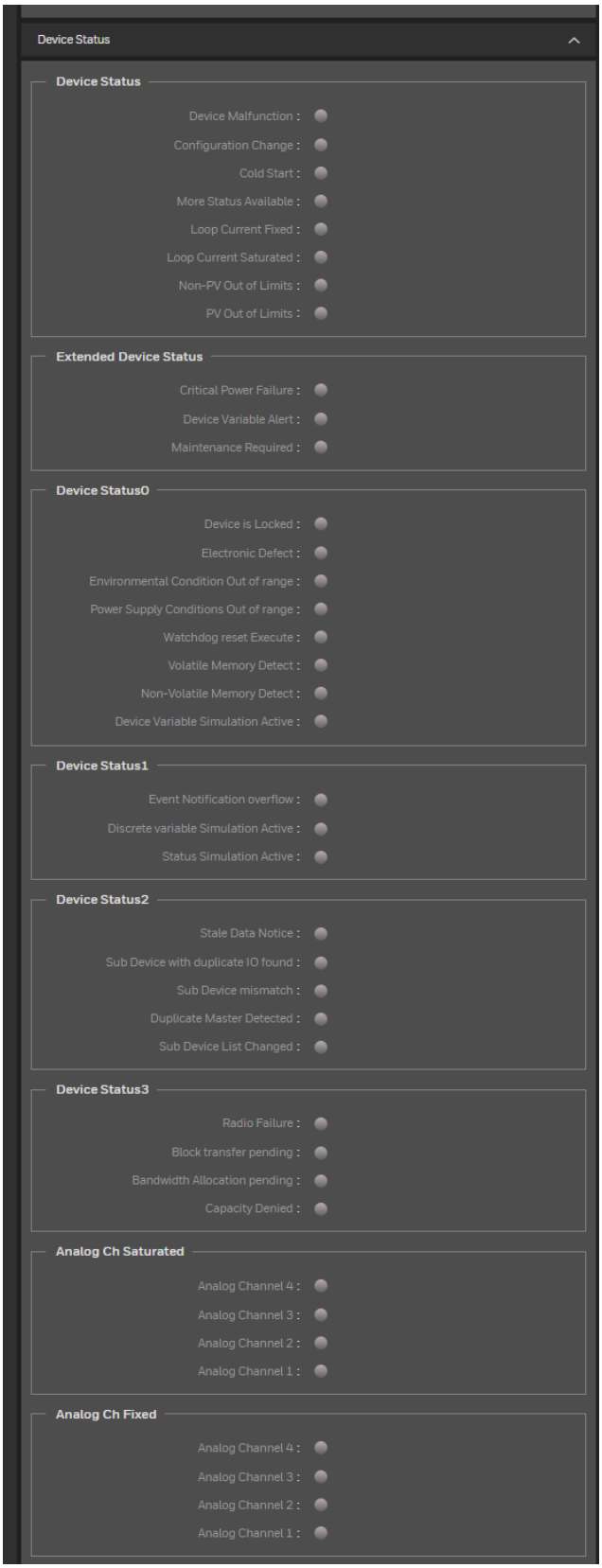
WirelessHART Devices

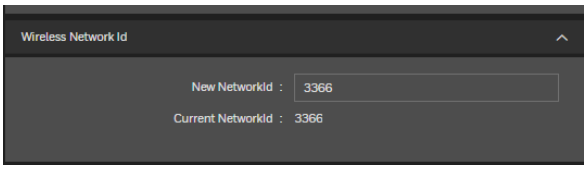
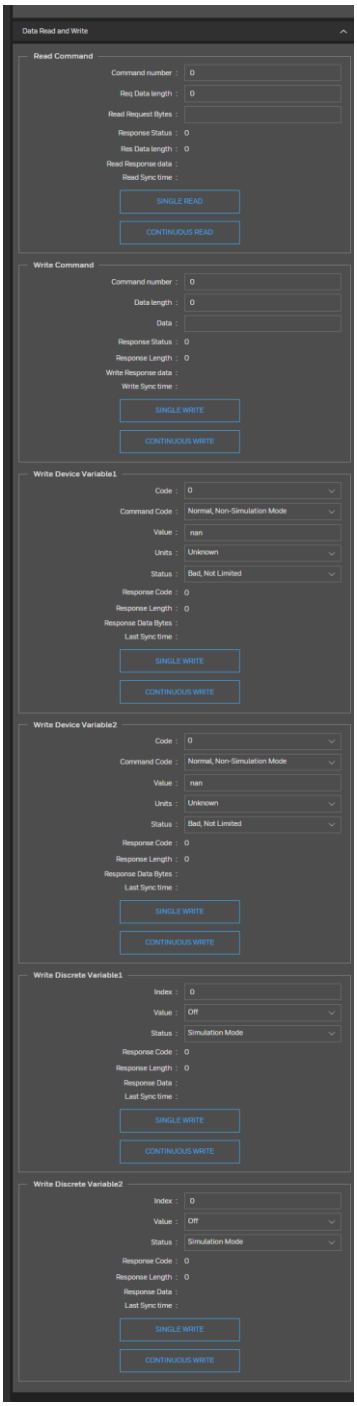


The following table describes the different properties available in the property Panel.

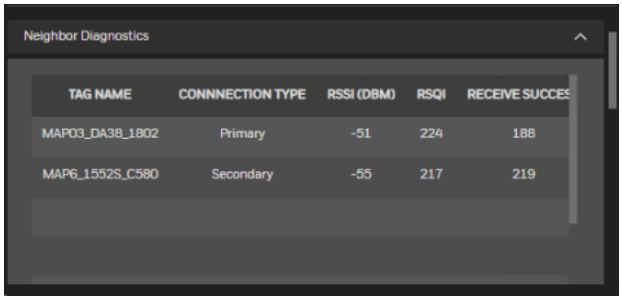
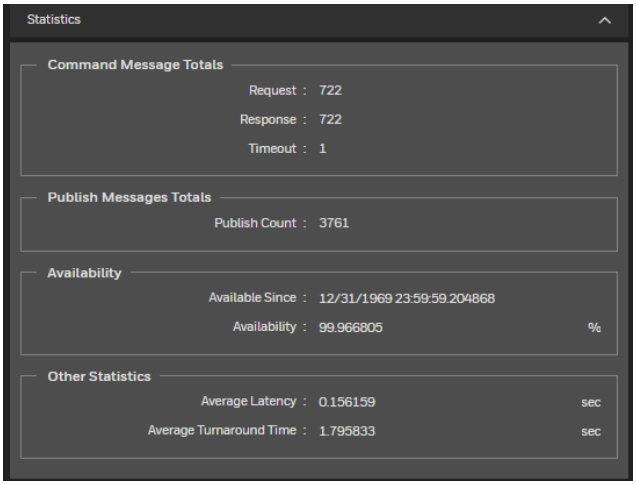
Property Panel	Description
Wireless HART Device Summary  	Device Summary of the selected device. The node manufacturer identification and network identification information and time synchronization information are displayed for both primary and secondary parent.
Device Information  	Overall health of the device. This data is fetched using command 48.

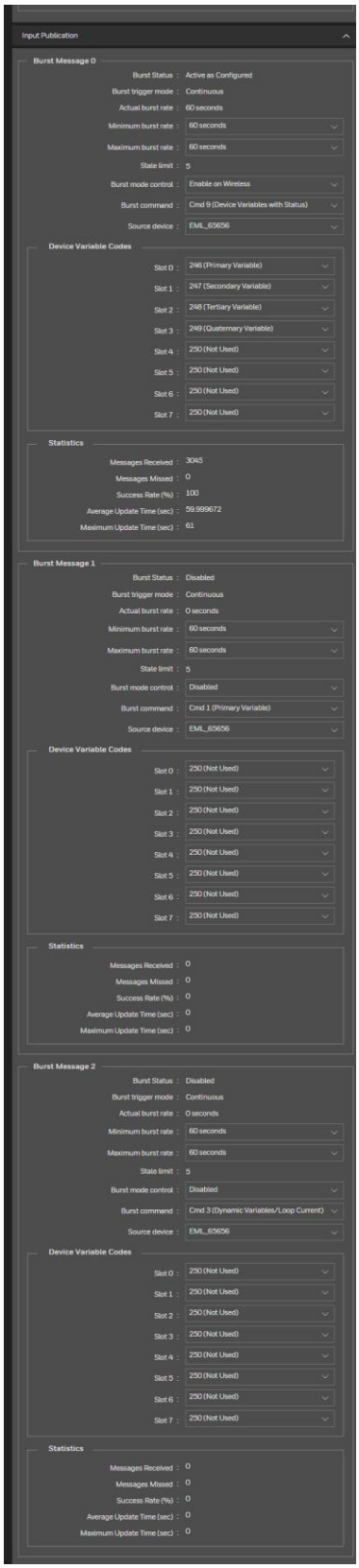
HART Information  	Common HART parameters
Device parameters  	Common device parameters

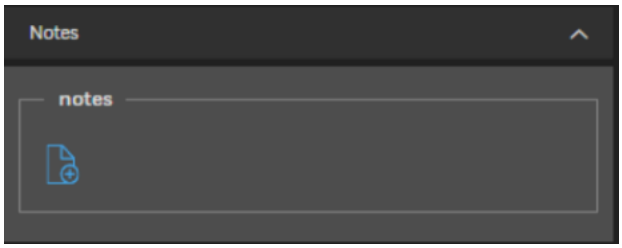
Device Status  	Overall health of the device. This data can be fetched by command 48.

Wireless Network ID  	Network ID details
Data Read and Write  	Data Write and Read To read and write the parameters of wireless HART device through custom commands For more information See "Sending control commands to WirelessHART devices"

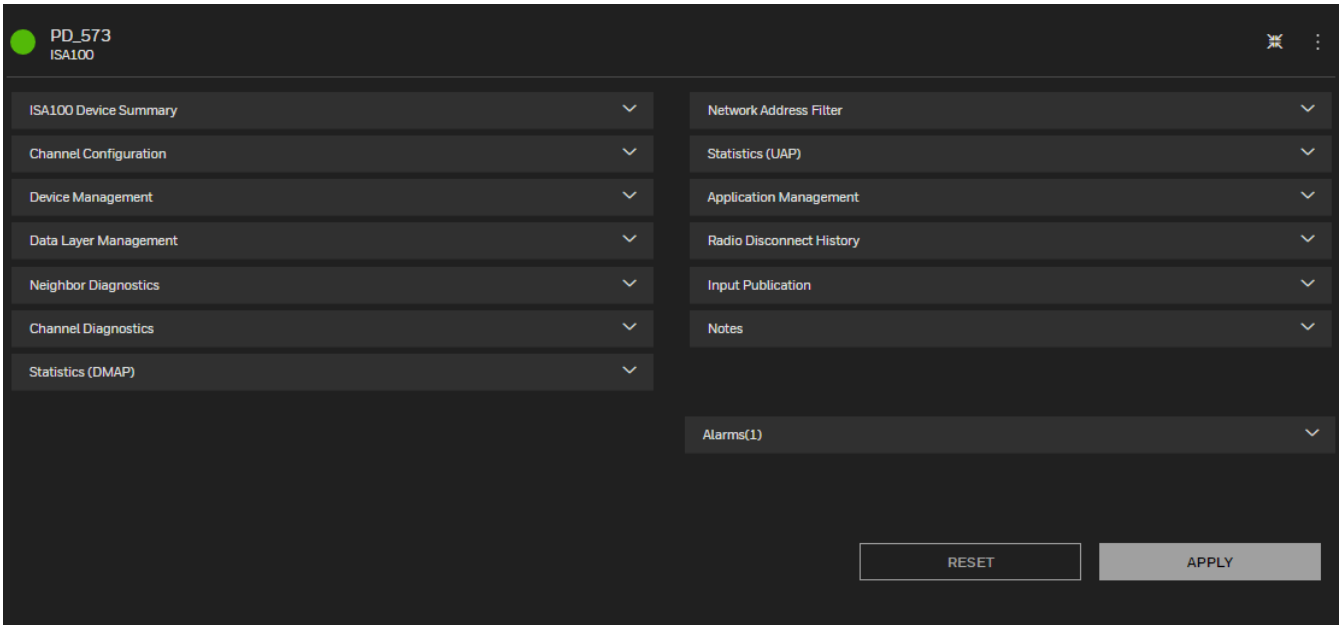
Device Variables	Device variables. The required slot variables are configured in one of the burst messages by selecting command 9 for period burst.

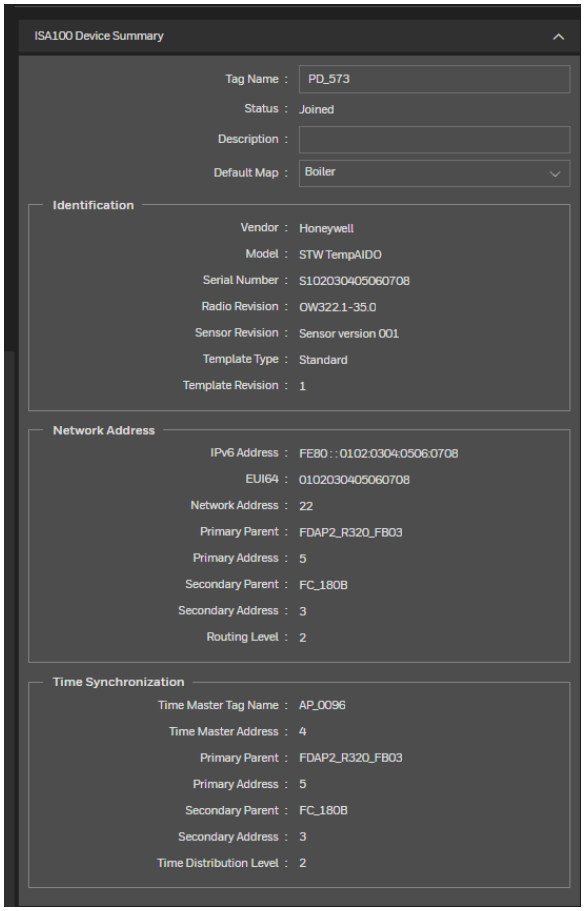
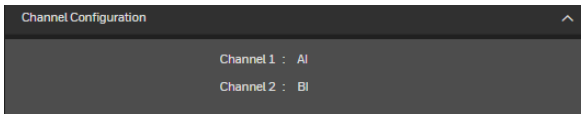
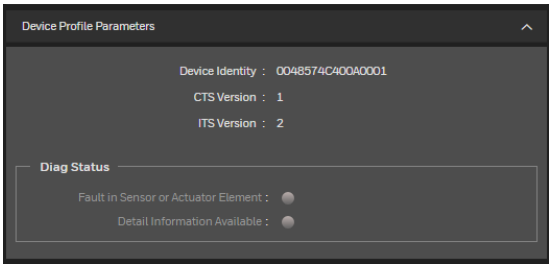
Neighbor Diagnostics  	Neighboring devices in the same network. These are the devices with which the selected device can communicate. The table displays the signal strength, packet transfer rate, receive and transmit success rate, and connection type of these devices.
Statistics  	Publication statistics of WDM. The commands sent by WDM, the response time for each command, and total messages that were published since the device is online. 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. 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.

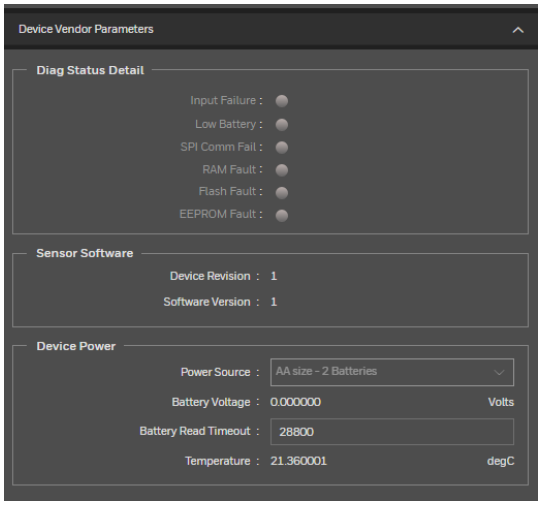
Input Publication  	Publishing (Burst message) feature of WirelessHART devices. The burst configuration can be defined for each device. There would be multiple burst messages for each device. Only one burst message is eligible to configure 8 seconds or lesser. All other burst messages can be configured for 16 seconds or greater only.

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

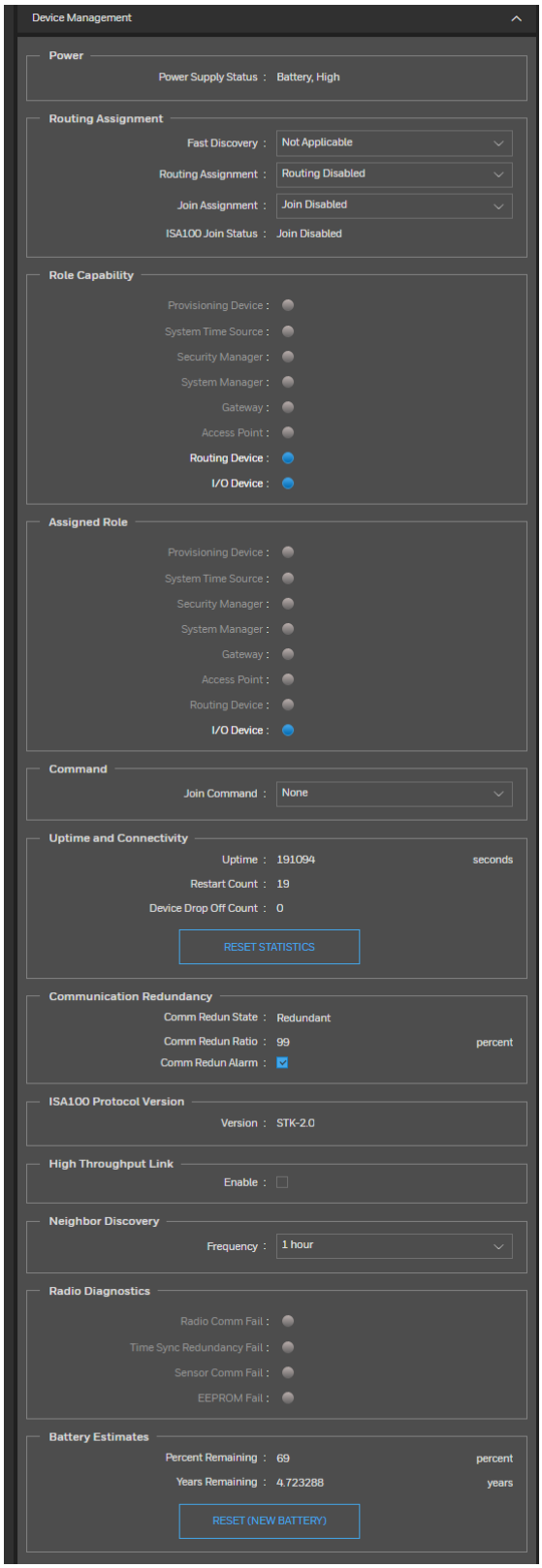
ISA100 Wireless Devices



Property Panel	Description
ISA100 Device Summary  	Device summary for the selected device. The node information and time synchronization information are displayed for both primary and secondary parent.
Channel Configuration  	List of channels (objects) supported for the selected device.
Device Profile parameters  	Standard device parameters.

Device Vendor Parameters  	This information is dependent on the vendor of the ISA100 Wireless device.

Device Management



Device specific information.

Routing Assignment: Role of the device currently - routing device or I/O device.

Role Capability: Roles the device can play.

Assigned Role: Role assigned to the device by WDM.

Join Command: Specifies applicable restart action.

Uptime indicates the duration for which it has been online since the last join.

Restart Count is the number of times the device has been restarted, whatever the reason.

Device Drop Off Count is the number of times that a device has dropped off from the network.

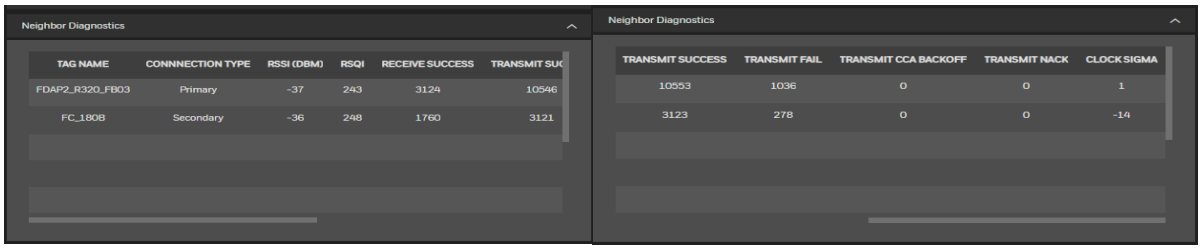
By enabling **HighThrough Put Link** feature, ISA 100 wireless devices communication improves, and they do not go to the sleep mode. This feature can be enabled only for Line Powered Devices.

If you are using an Enraf Flexline/WFI devices and Engauge Tool to talk to devices, you need to enable this setting for the Flexline/WFI Device you are reading the information from. If you are using to scan all Flexline/WFI devices using Engauge tool, please enable this setting for all Flexline/WFI devices in the network.

Neighbor Discovery: Device discovers new neighbors as per the configured frequency. Do not change these settings unless you really want the device to discover routers nearby faster. Making faster discovery reduces battery life of the device.

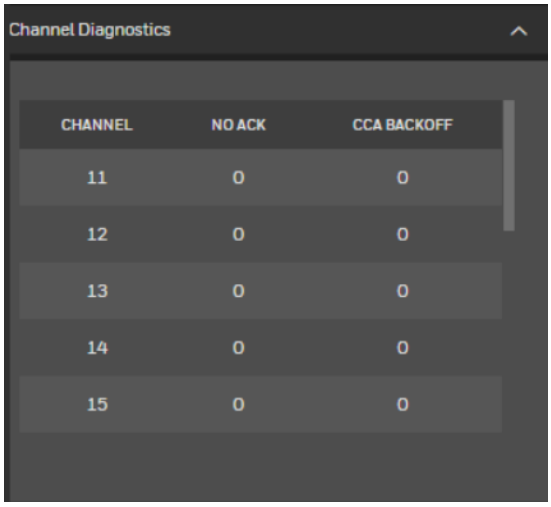
Data Layer Management  	Wireless transmit power level.

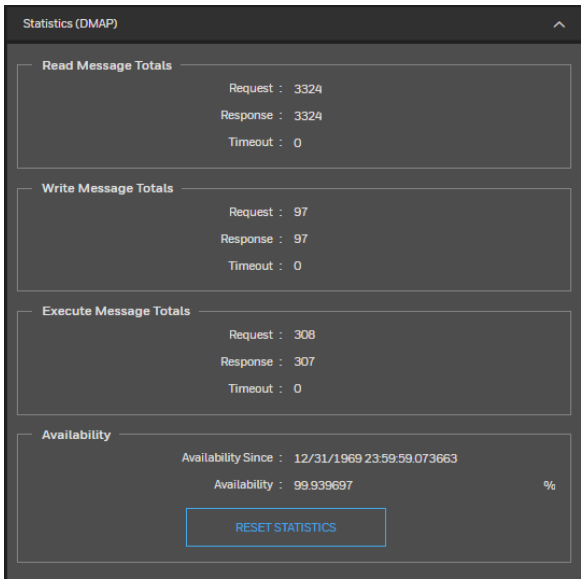
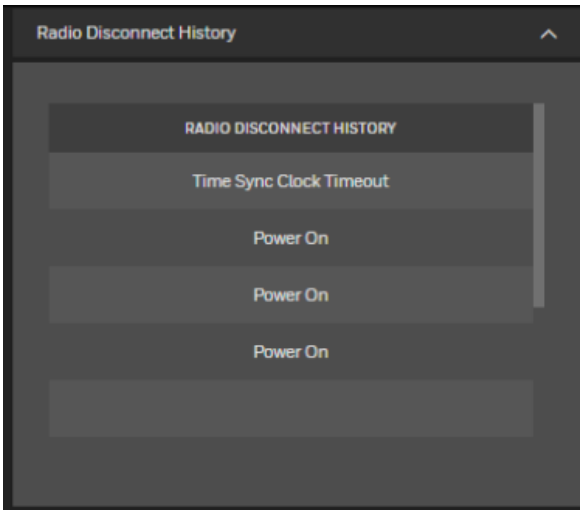
Neighbor Diagnostics

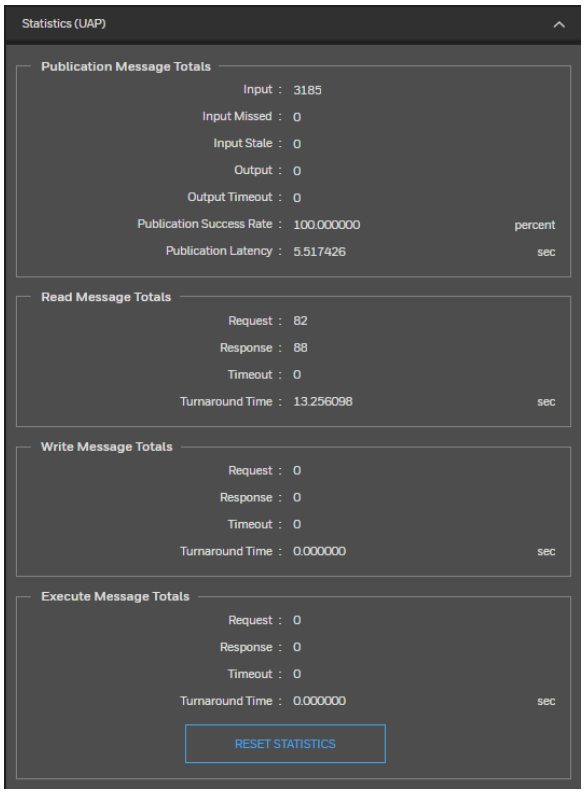
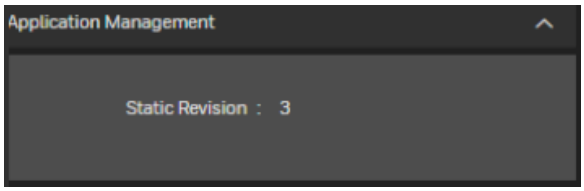
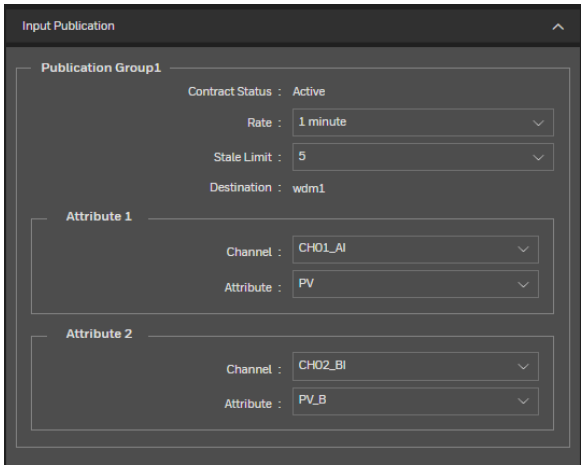


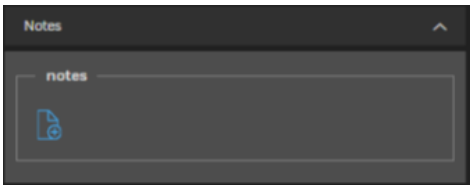
Displays neighboring devices in the same network. These are the devices with which the selected device can communicate.

This table displays the signal strength, packet transfer rate, receive and transmit success rate, and connection type of these devices.

Channel Diagnotics  	Channel information. No ACK & CCA Backoff indicate the noise levels present in a channel.

Statistics (DMAP)  	Read/Write/Execute requests sent by WDM.
Radio Disconnect History  	The history of last 5 disconnect reasons from the network.

Statustics UAP  	Statistics related to WDM communication with the field device. Statistics includes publications sent between the device and the WDM, This table captures the number of requests sent by WDM and the responses given by the device for Read/Write/Execute messages.
Application Management  	Static revision number.
Input Publication  	Attributes (objects) of the device selected for publication. Some devices have only Input Publication attributes while others have Output Publication attributes.

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

NOTE	**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.

ATTENTION	• ***The Device Description (DD) files are available only for ISA100 Wireless devices.*** • ***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.

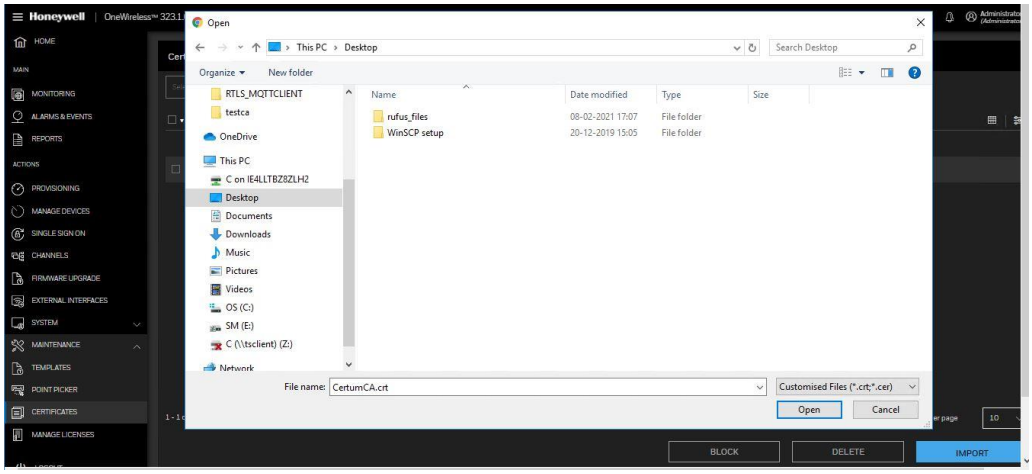
Loading the Certificate

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.

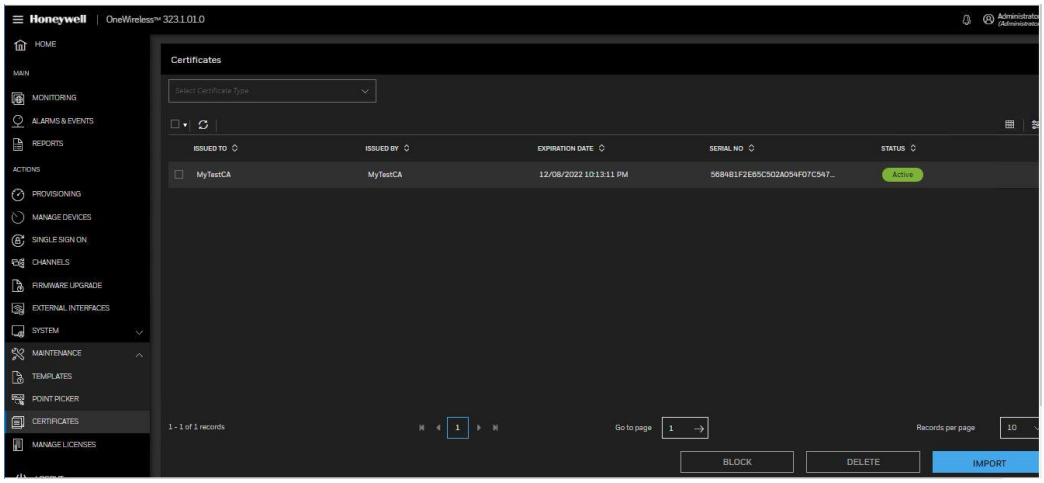
The client will send a certificate to the server only if the server requests one. This is known as client authentication. Using the certificate(s), cipher parameters are passed between the client and server to set up the secure connection. Even though the handshake is performed after the connection is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

To load the Certificate

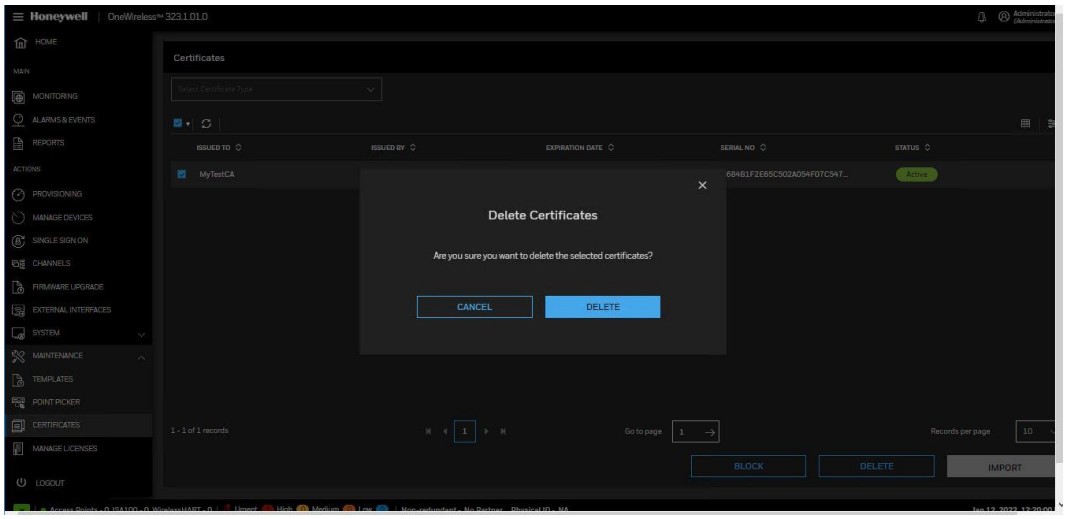
1. Click **Certificates** from Left Navigation Menu bar.
2. Click **Import** from the **Certificates**.



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.

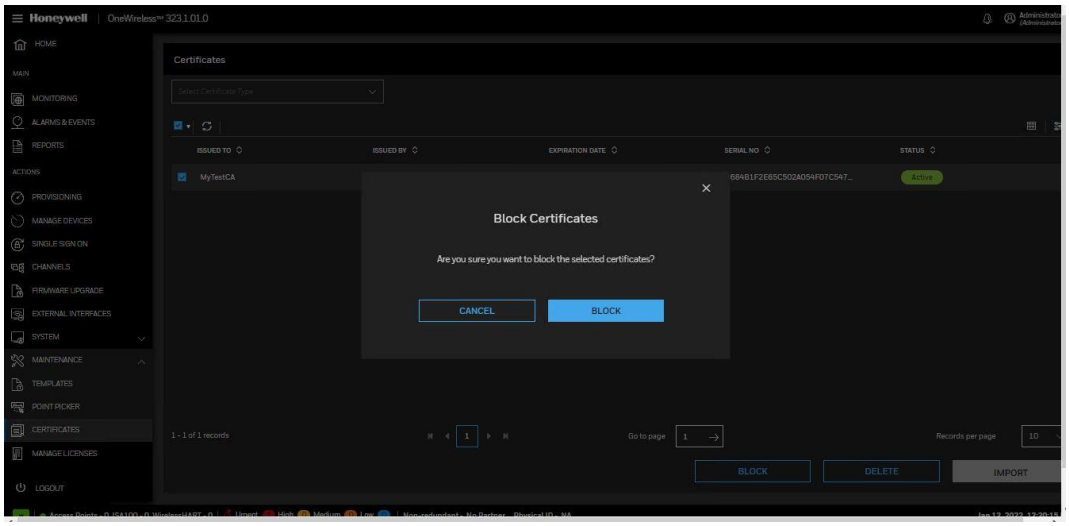


5. To delete the existing certificate, select **MytestCA** and click **DELETE**.
6. A pop -up window appears for the confirmation, click **DELETE.**

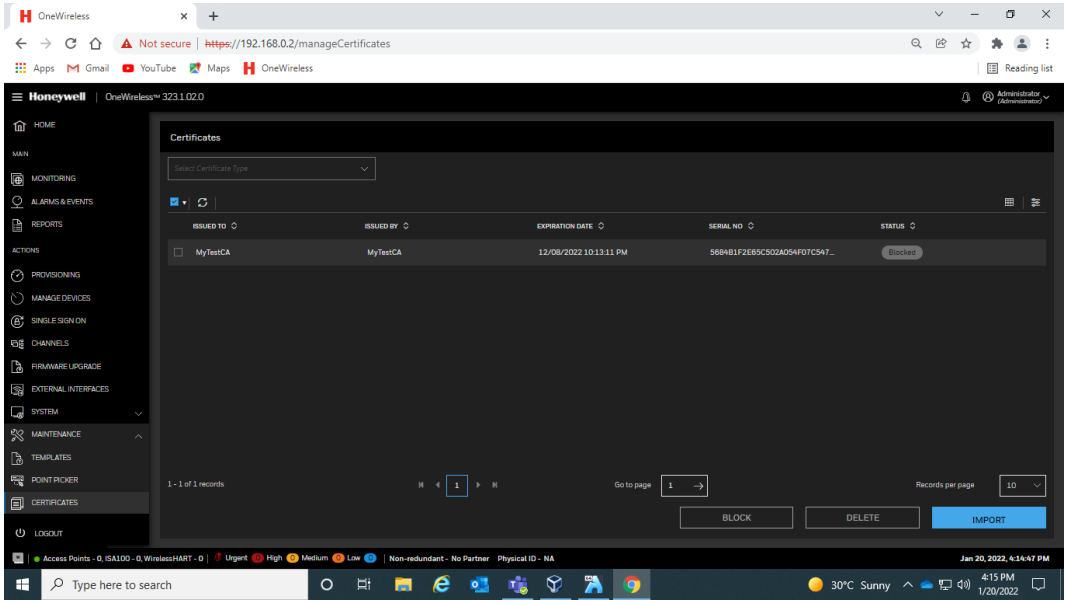


7. To block the existing Certificate, select **MytestCA** and click **BLOCK**.

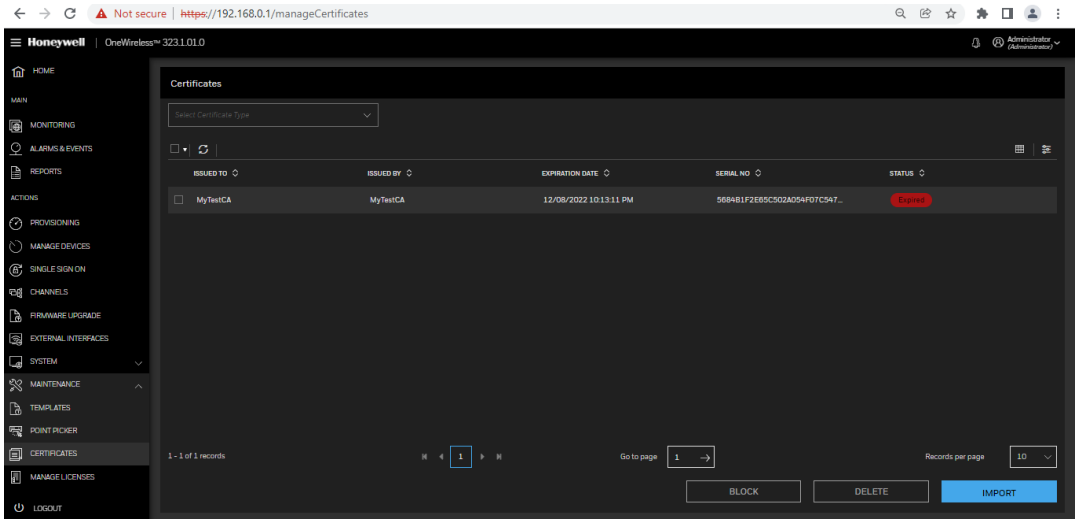
8. A pop -up window appears for the confirmation, click **BLOCK.**



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



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

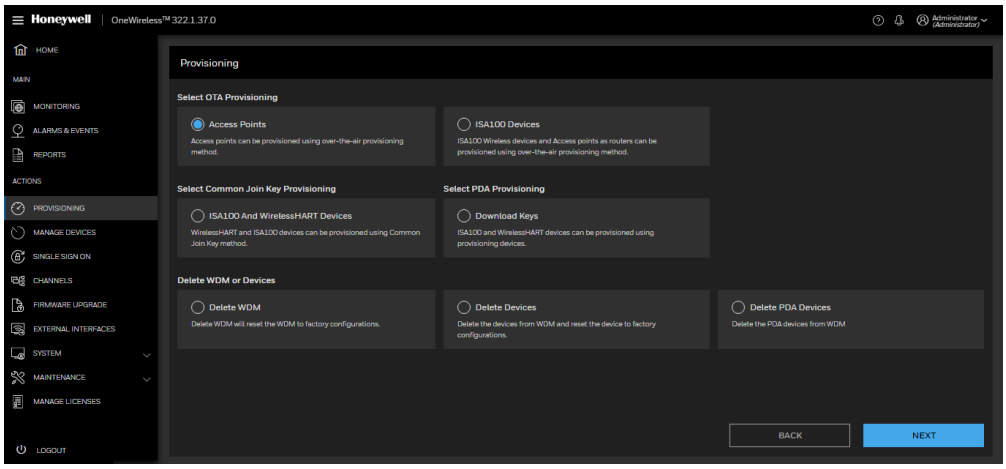


Provisioning

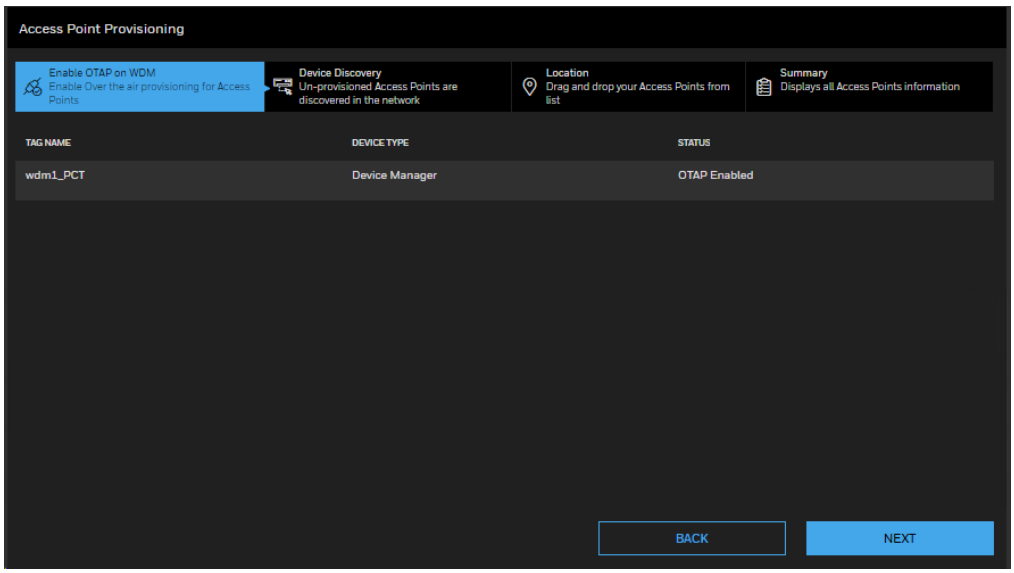
To provision the access points using over-the-air provisioning method

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

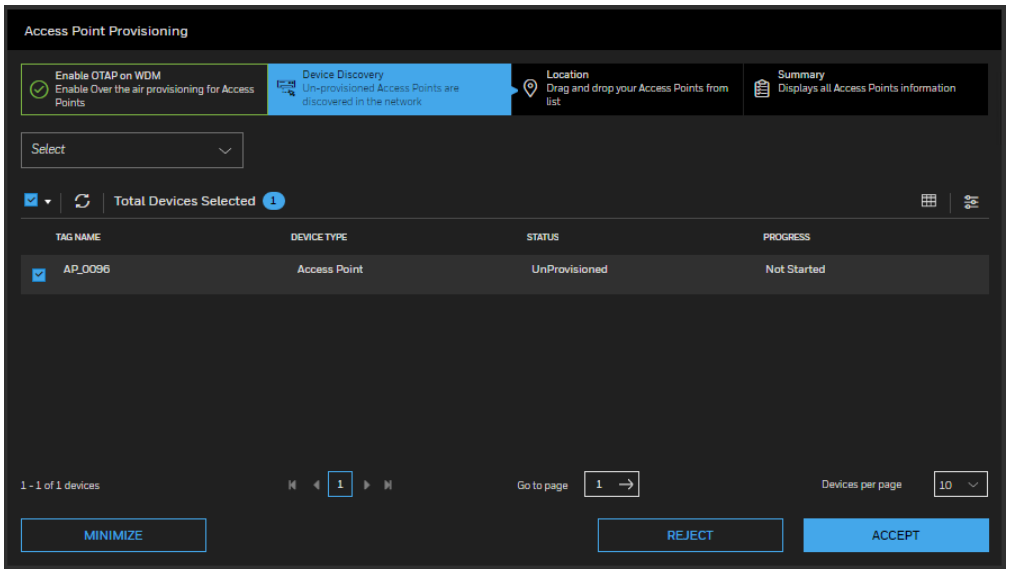
1. Click **Provisioning** from Left Navigation Menu bar.
2. Select **Access Points** from **Select OTA Provisioning** and click **Next.**



3. Click **Next** in **Enable OTAP on WDM** page.



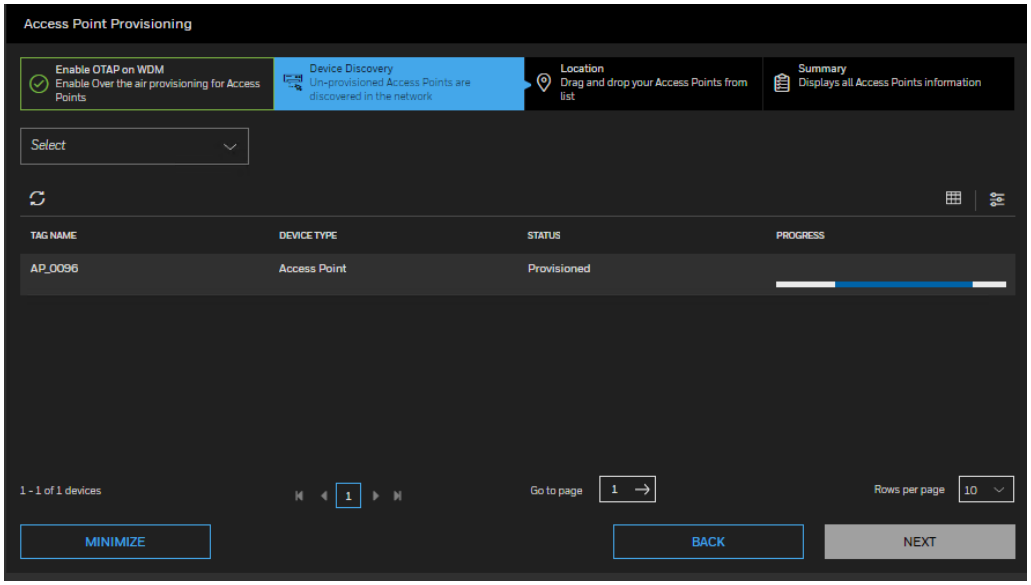
4. Select the required access point in the Selection Panel and then click **Accept.**



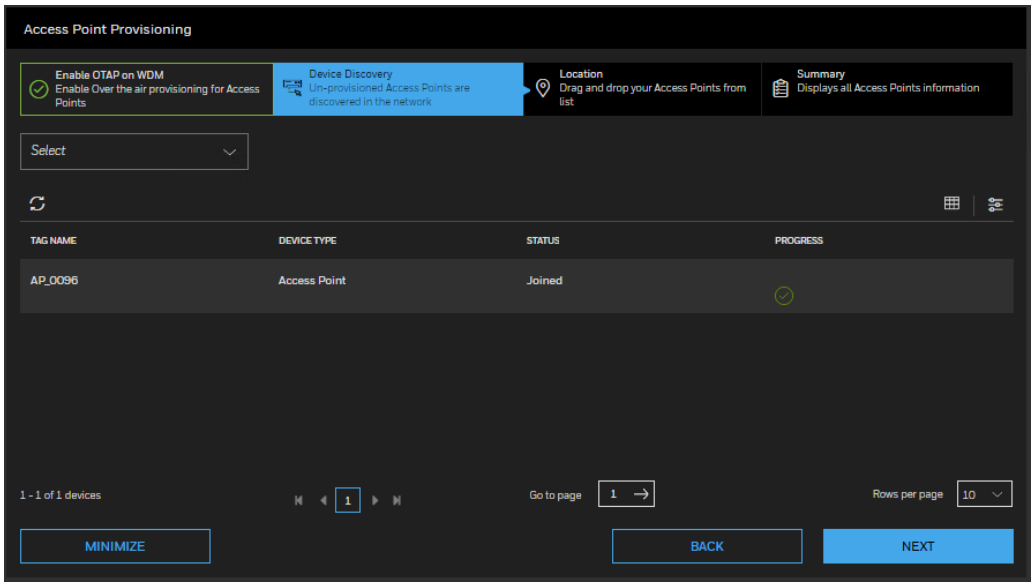
5. Reject all unintended devices till the devices that you want to appear in the OneWireless user interface. The unintended devices must not be deleted and must remain in rejected state. This is to make sure that the rejected devices are available for you to provision them in future.
6. For rejecting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

ATTENTION	• *You can select multiple access points from the Selection list,* • *It is recommended that you select and accept only 10 devices at a time.*

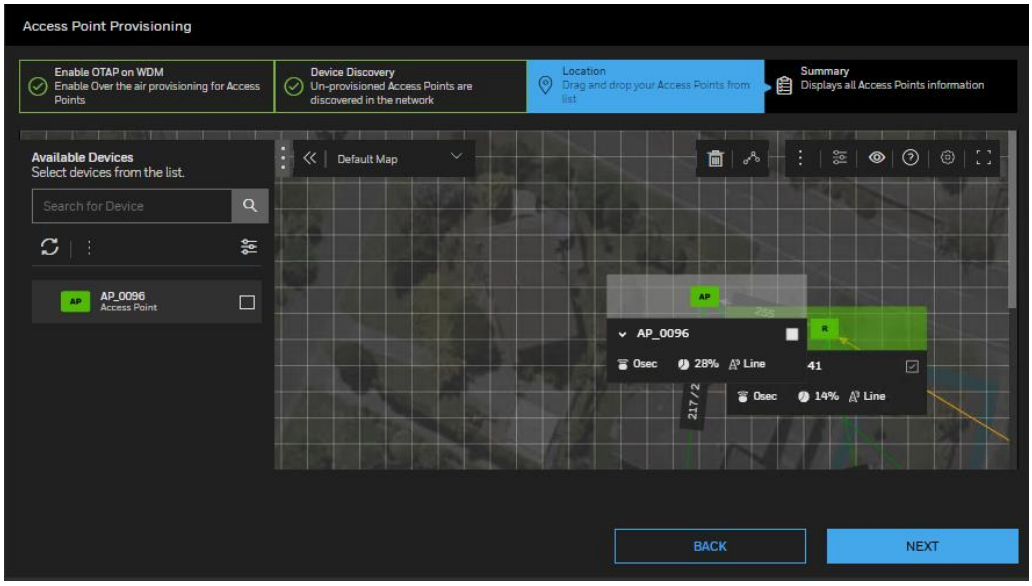
7. The confirmation window appears. Click **Accept.**
8. The **Progress** column displays the status as **In Progress**, **Provisioning**, and then **Joined** after completion. Do not close the window when over-the-air provisioning is initiated for devices.



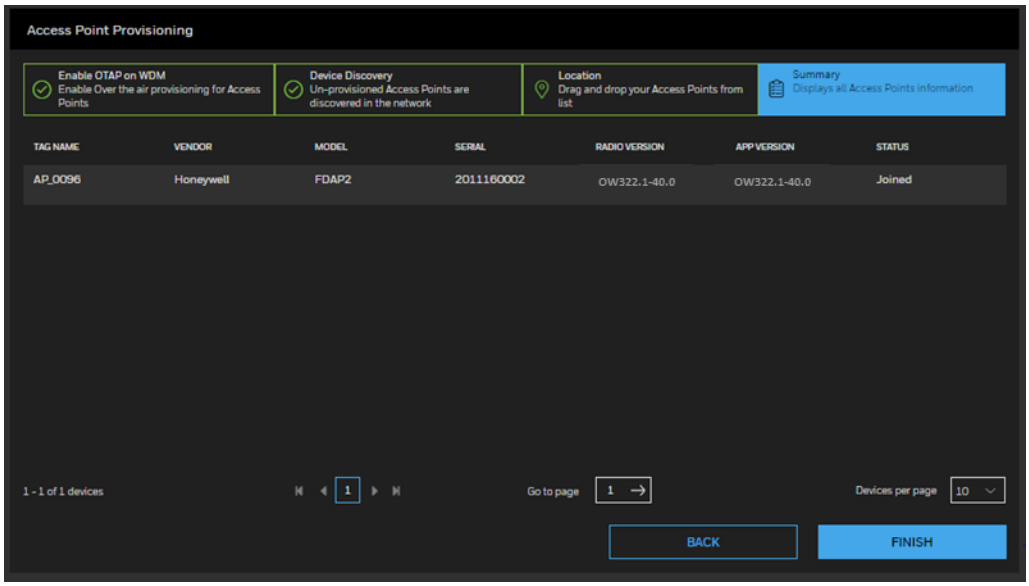
9. Device joins once the progress is completed and click **NEXT.**



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

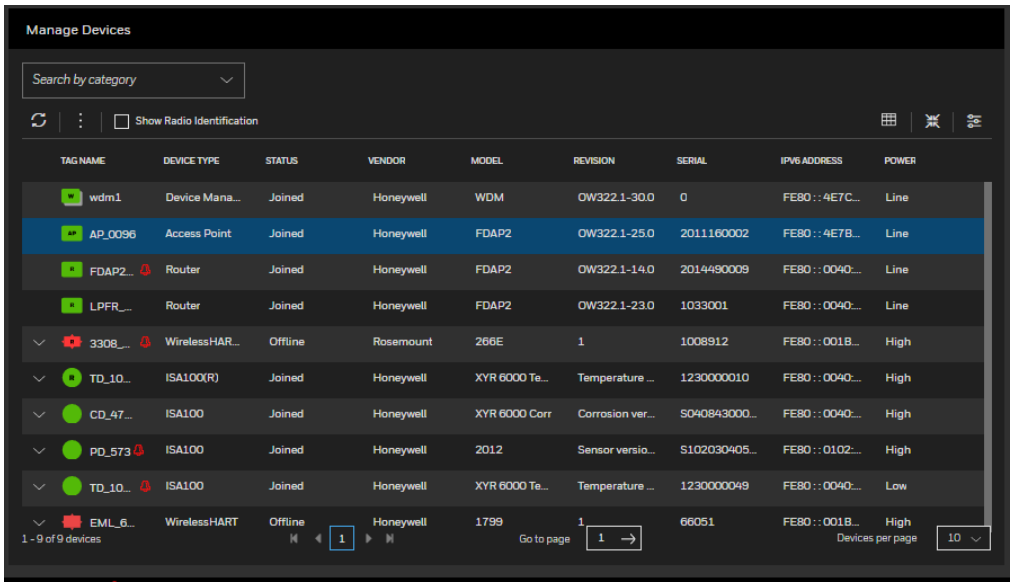


11. In the **Summary** page you can see all the Access points information. Click **FINISH**.



12. A confirmation message appears to disable OTAP.

13. After confirmation, the Access Point is displayed in the selection Panel.



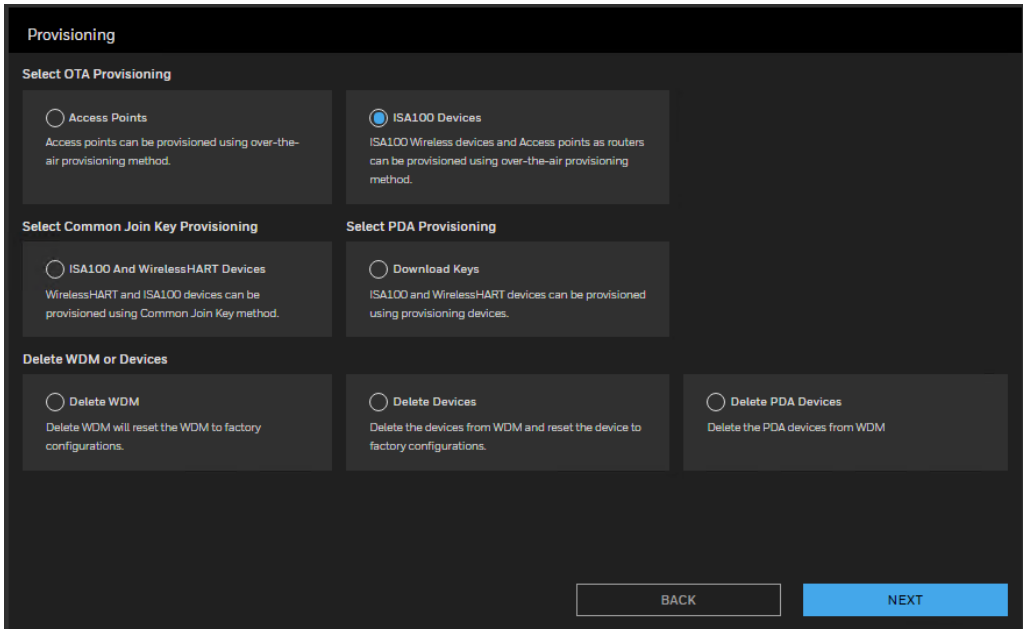
To provision the ISA100 Devices using over-the-air provisioning method

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.

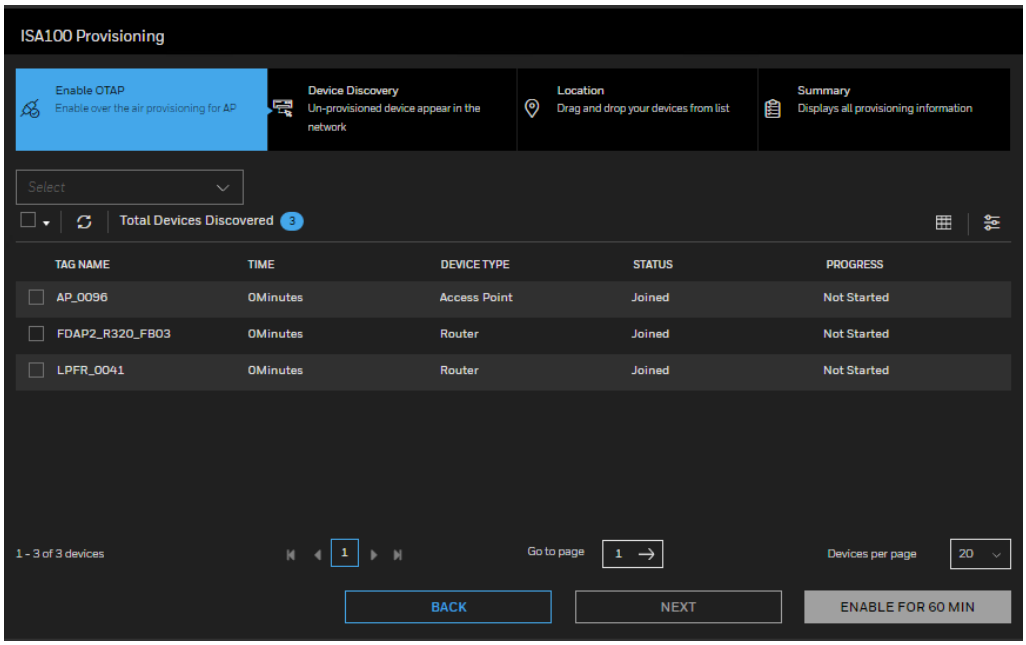
Any access point that is in the factory default state, when connected to the OneWireless Network can join the network as an Non-provisioned device. In this state, the WDM contains only the basic details about the device such as the Tag Name, EUI64, and Radio Revision. Also, there is no active data communication 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.
2. Select **ISA100 Devices** and click **Next**.

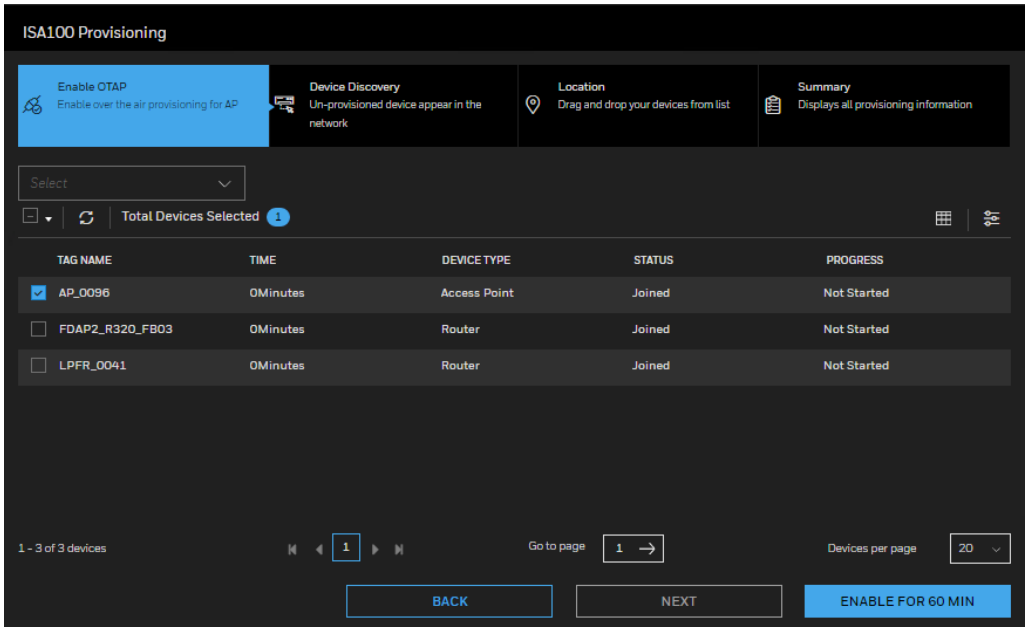


3. ISA100 provisioning window appears.

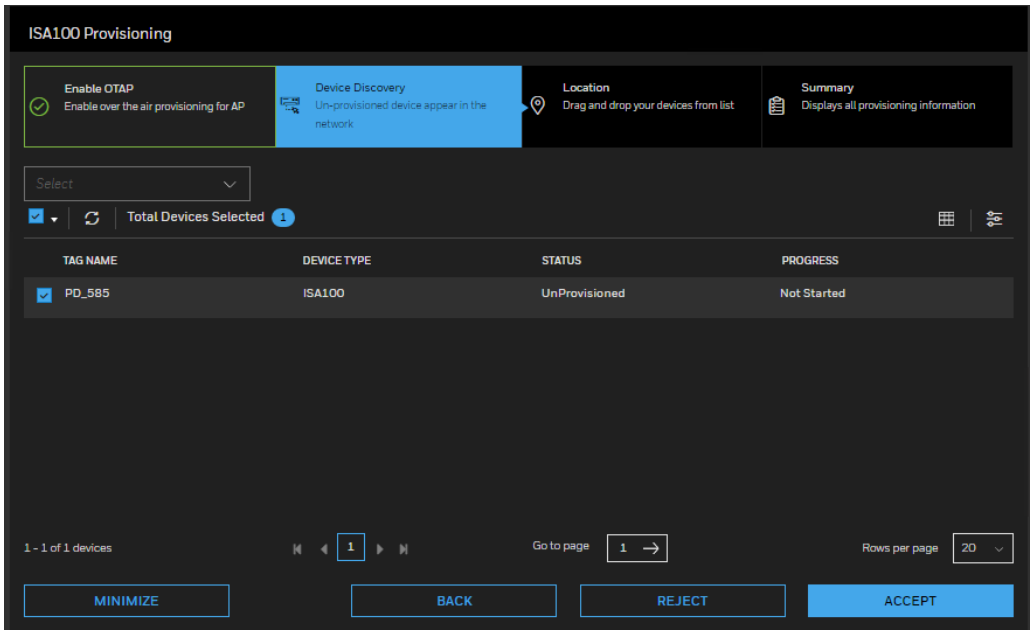


Here you can Manage Filters, manage columns and select the required device for the air provisioning method.

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



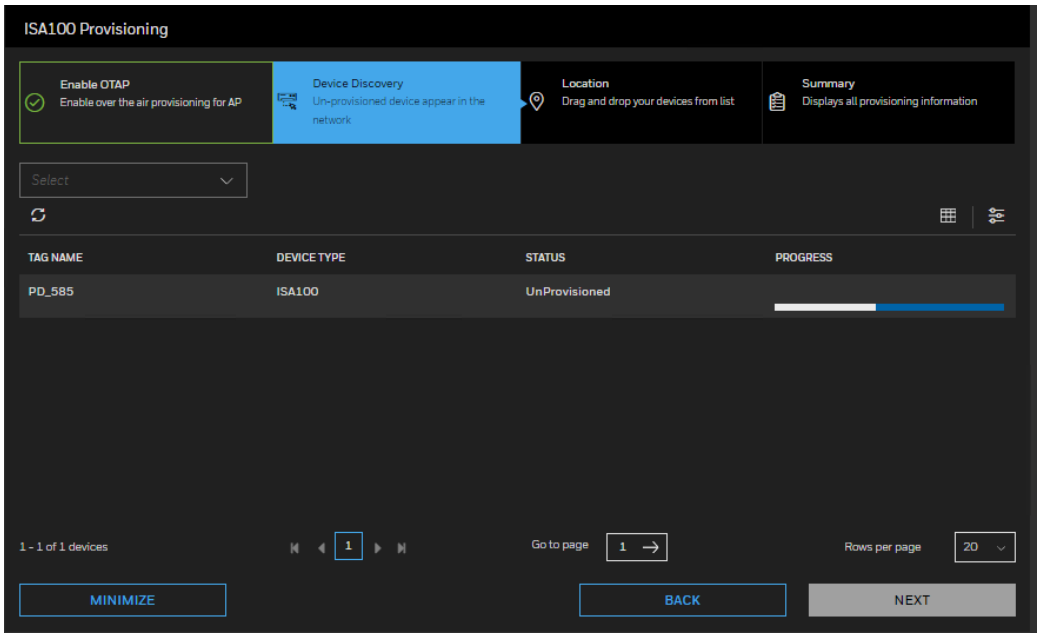
5. Select the **Tag Name** and click **Accept** in **Device Discovery** page.



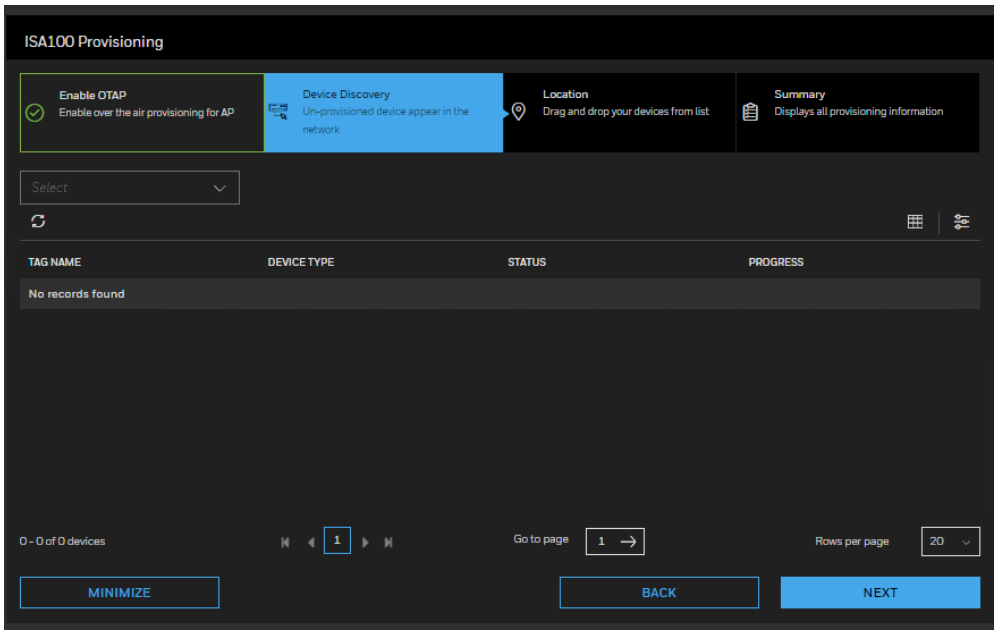
You can accept or reject devices.

6. A pop -up window appears for the confirmation, click **Accept.**

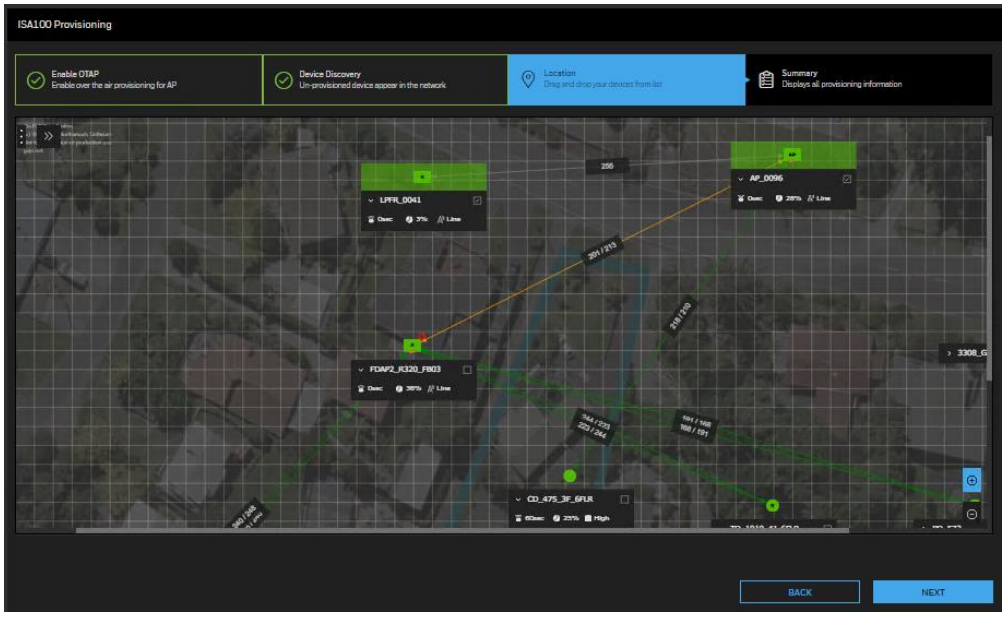
7. It takes time to discover and accept the device.



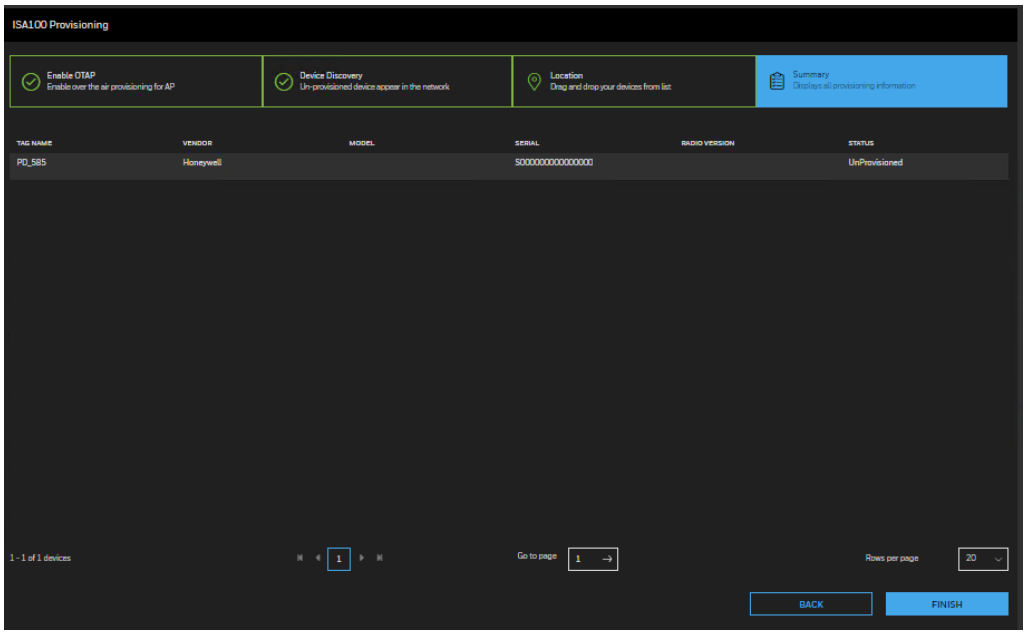
8. After the device is accepted, click **Next.**



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.

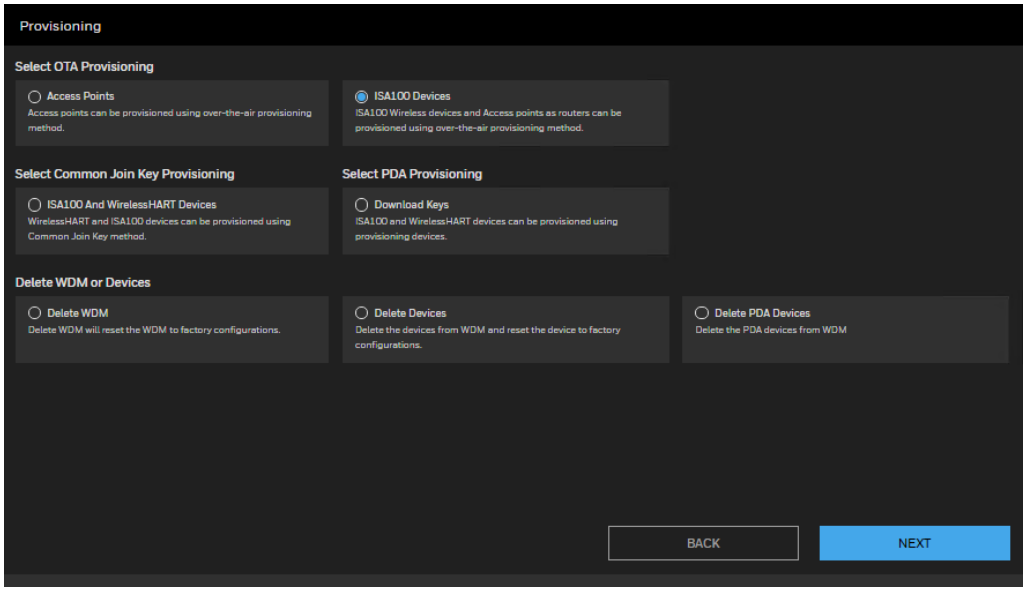


11. After completion, click **Finish.**

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

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

1. Select **ISA100 Devices** from **Select OTA Provisioning.**

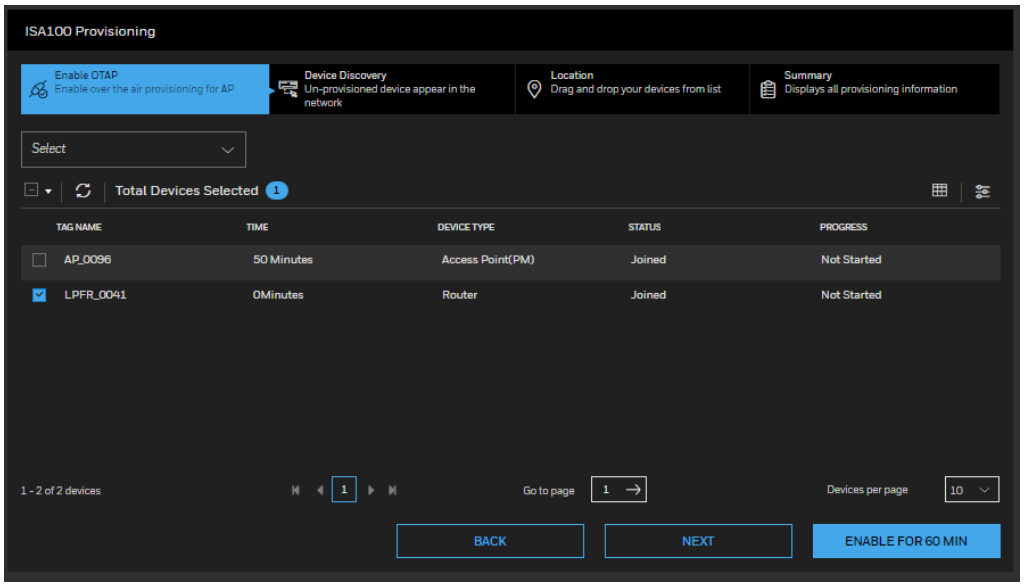


2. Select the Access Point and click **Next**.

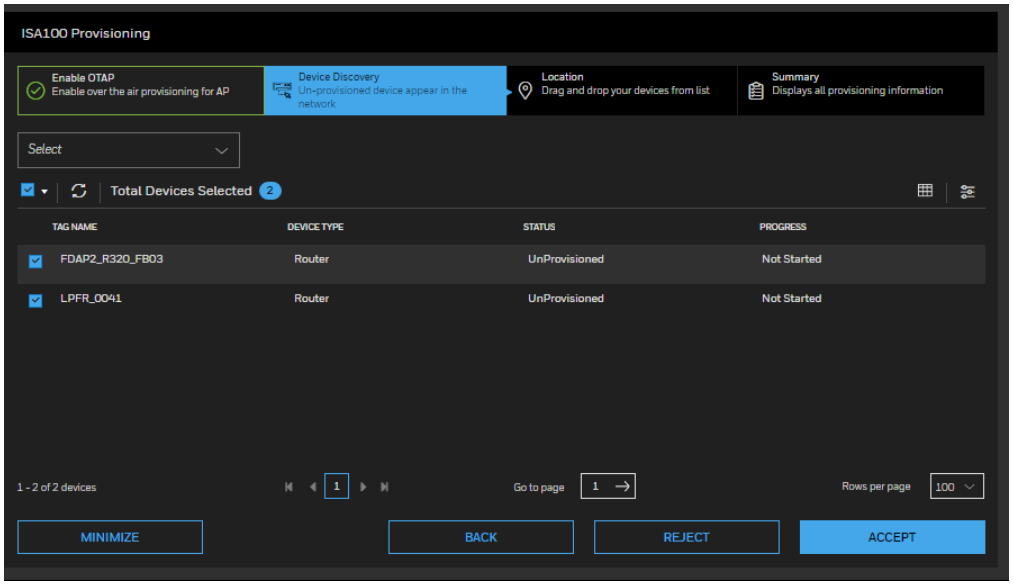
3. Select **Enable for 60 Minutes** if it is not enabled through WDM from property panel.

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

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.

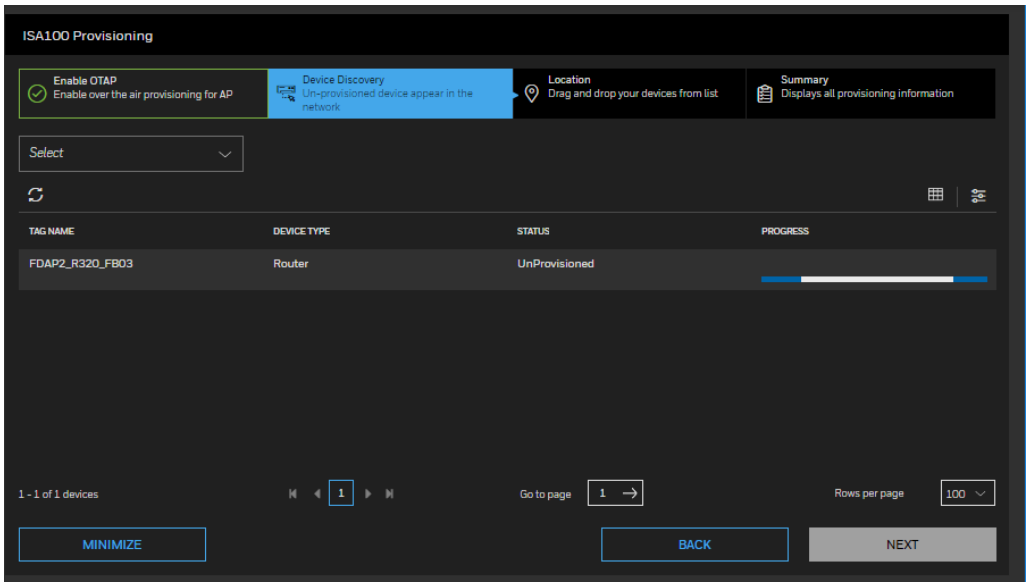


4. The **Device Discovery** page appears. This page displays all the Unprovisioned devices that you have selected for enabling over-the-air provisioning.

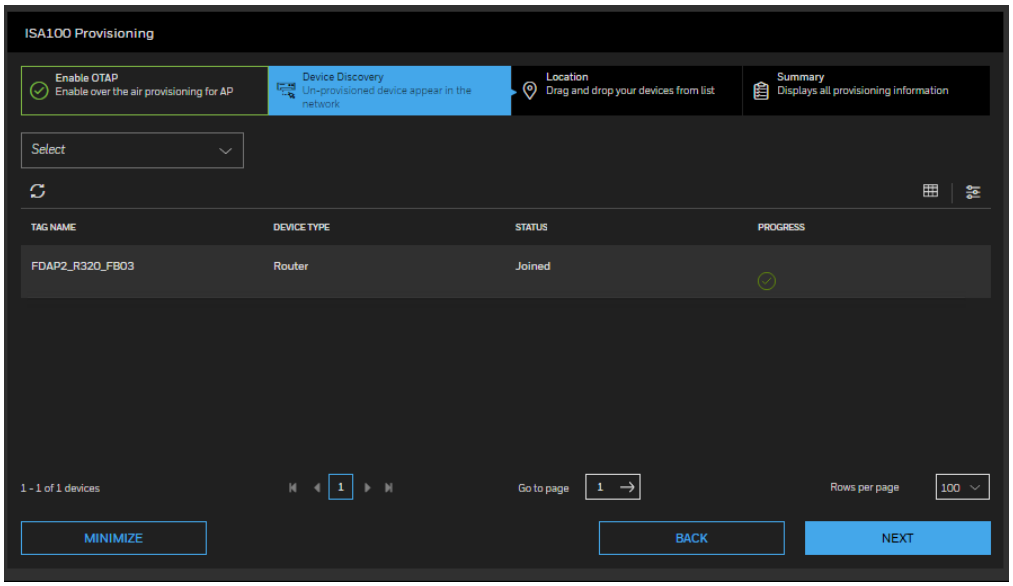


5. To reject a device from joining the network using over-the-air provisioning method.
   - Select the required device and click Reject. The Reject Over the Air Devices window displays.
   - Click Reject. The Progress column displays the status as In Progress, and then Completed, when complete.

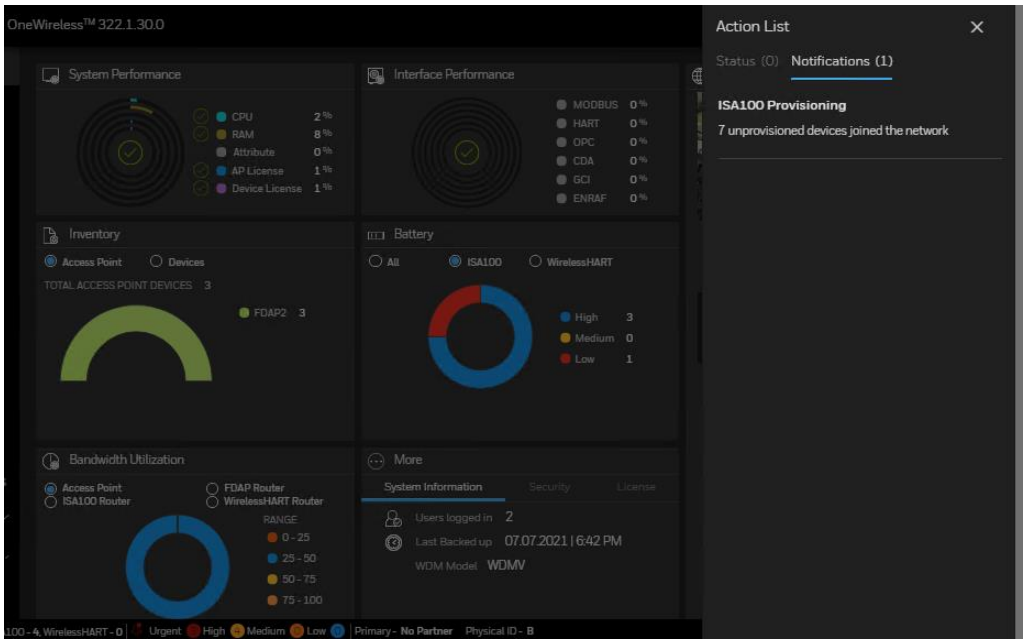
6. Click **Accept**. The **Progress** column displays the status as **In Progress**, **Provisioning**, and then **Joined**, when complete. Do not close the window when over-the-air provisioning is initiated for devices.



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

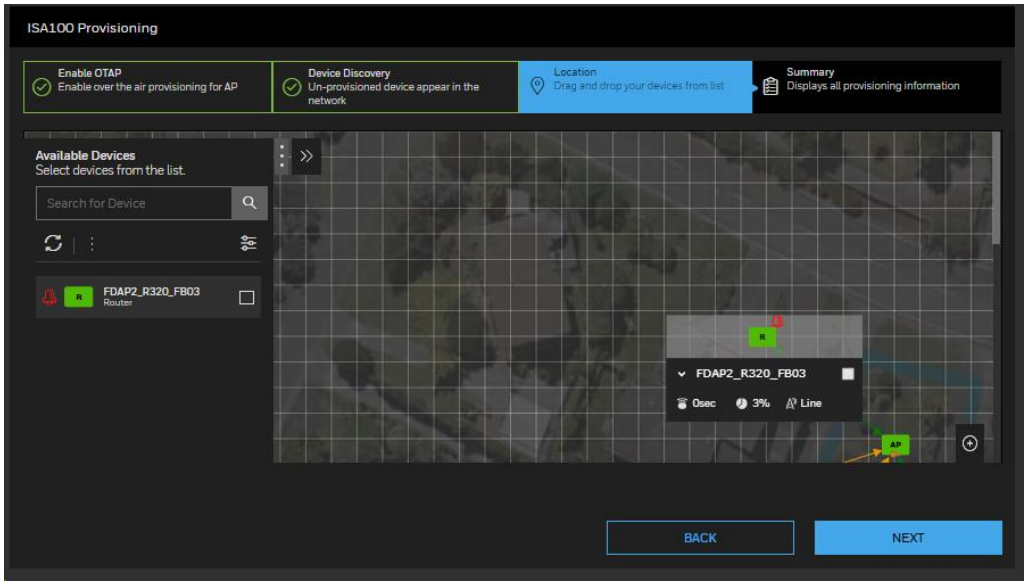


Also, you can minimize the screen by selecting **MINIMIZE** button and you can view it in the notification bar.

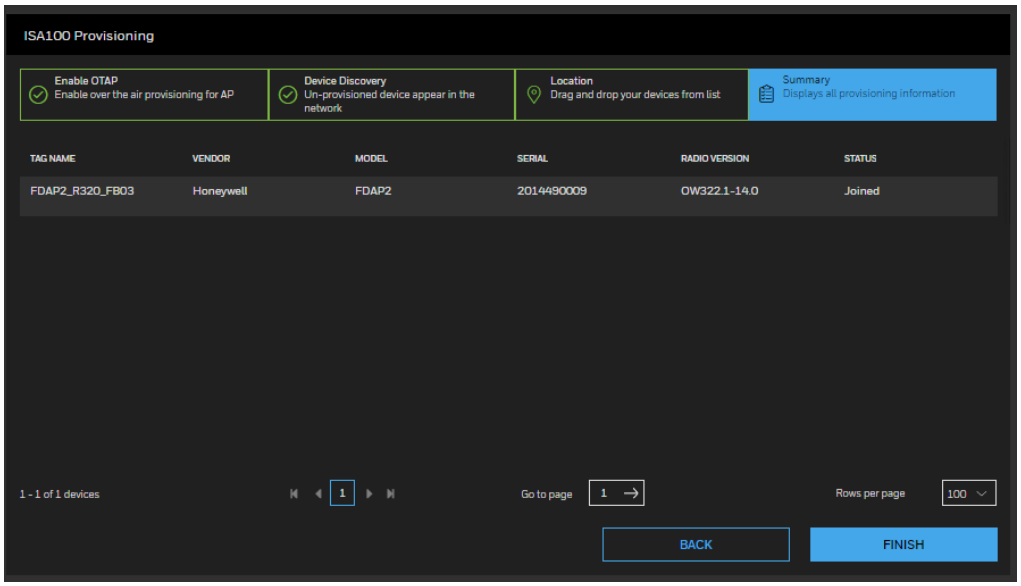


ATTENTION	*Repeat the procedure to enable over-the-air provisioning capability in line-powered FDAP routers. This enables the line powered FDAP routers to provision distant nodes in the network.*

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**.



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.

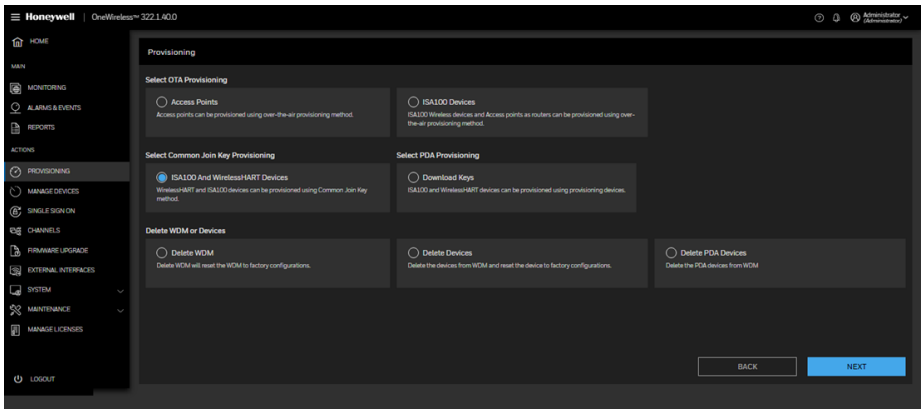
The device establishes a communication link with the access point after it attains the Non-provisioned state. This link persists even if the device is not provisioned using the connected access point. If the device needs to be provisioned using a different access point, reject the device and then delete 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.

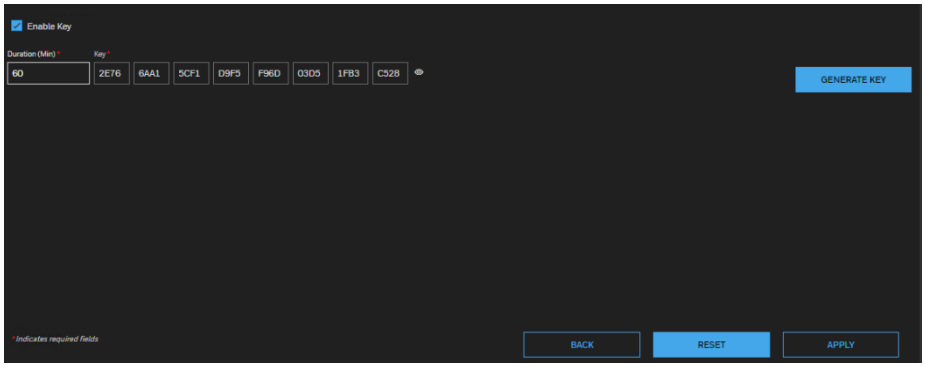
To provision the ISA100/WirelessHART devices using Common Join Key

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



ATTENTION	**Download keys is not supported in R22.1**

3. Click **Next.**
4. 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.



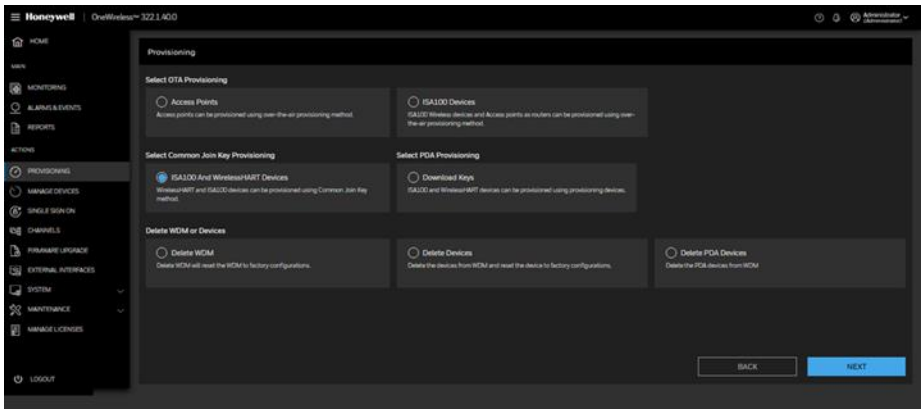
6. In the **Enabled Duration (min)** box, enter the duration in minutes and click **Apply**.
7. The device joins the network using the configured network ID and the Common Join Key.
8. Click **OK** on the confirmation message.

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

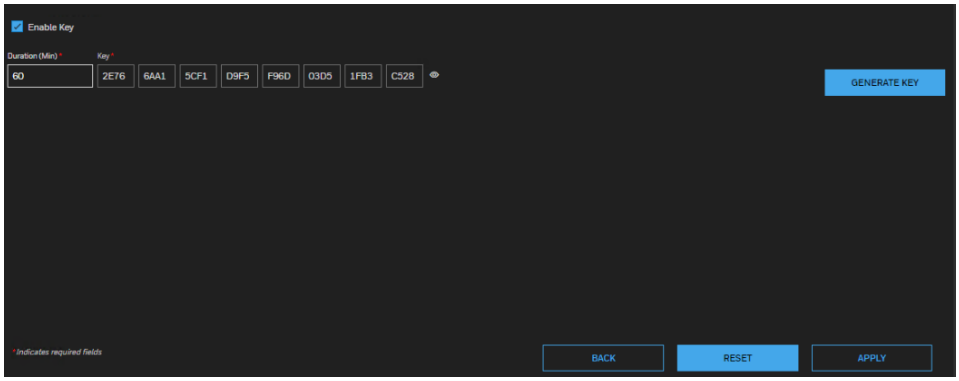
WirelessHART devices can be provisioned in the OneWireless Network using Over-The-Air (RE)-Provisioning method as described below. Any WirelessHART device which is factory delivered or provisioned for different network can be re-provisioned into this network over the air without using any specific OEM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

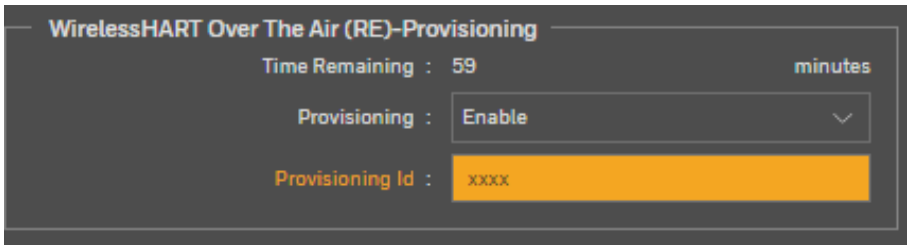


3. Click **NEXT.**
4. In the **Key** box, type the key details of the WirelessHART device provided by the manufacturer or key present/stored in the device.

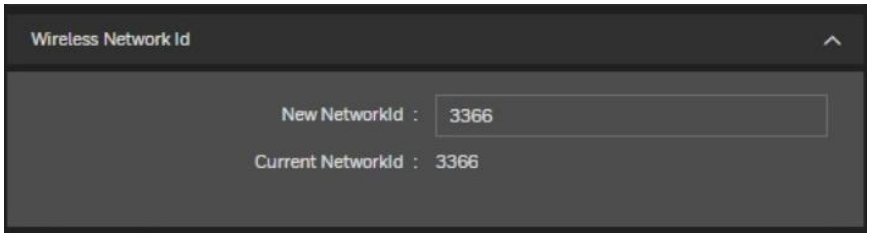


5. Enter duration in minutes and click **APPLY**.
6. Select **Manage Devices** from Menu bar.
7. Select the required field device access point. The selected Access point must be in the vicinity of the device to be re-provisioned to this network.
8. Expand **Device Management** in the Property panel.

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.

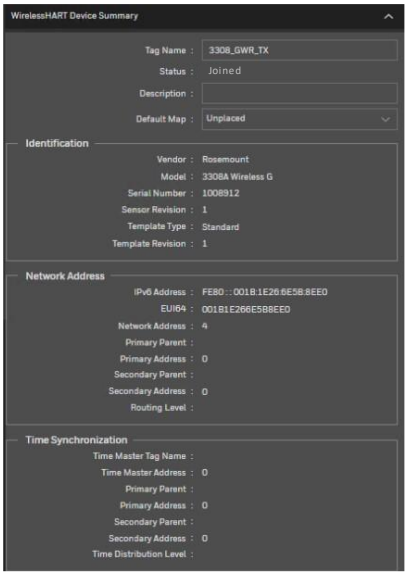


10. Click **APPLY**.
11. After a few minutes, the WirelessHART device joins the network through the FDAP on which Over-The-Air (RE)- provisioning is enabled.
12. Select the Wireless HART device from **Manage Devices**.
13. Expand **Wireless Network ID** in the Property panel. In the **New Network Id**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



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.

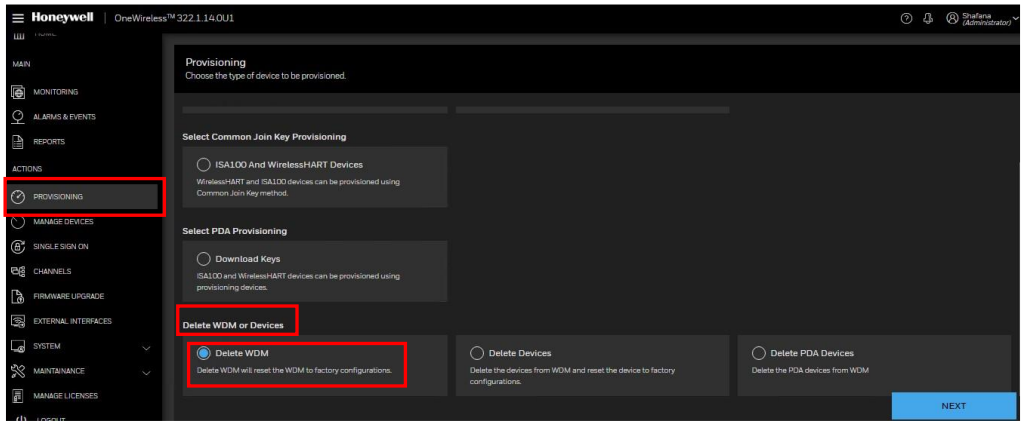


16. Disable Over-The-Air (RE)-provisioning in FDAP and Common join key in WDM.

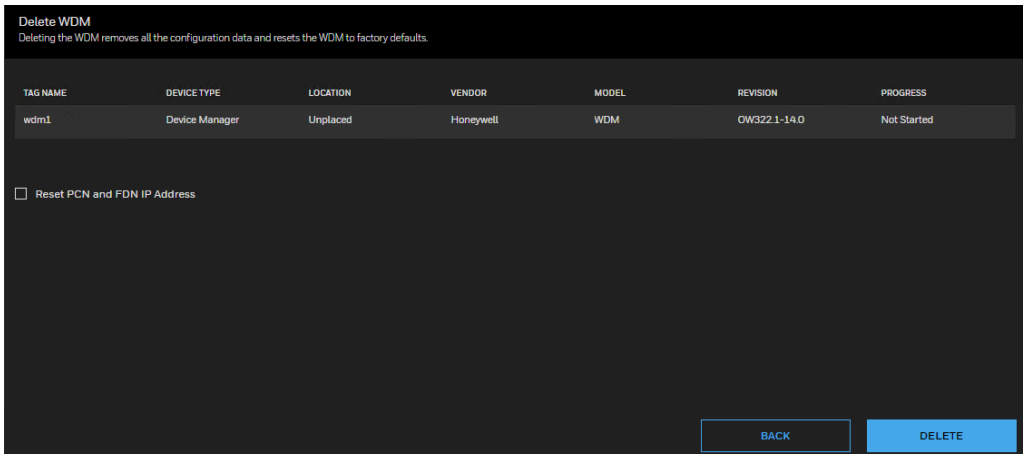
Remove Device

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.



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



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

Delete devices

See section To remove a device: for more information.

Delete PDA Devices

See section To remove a device: 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.

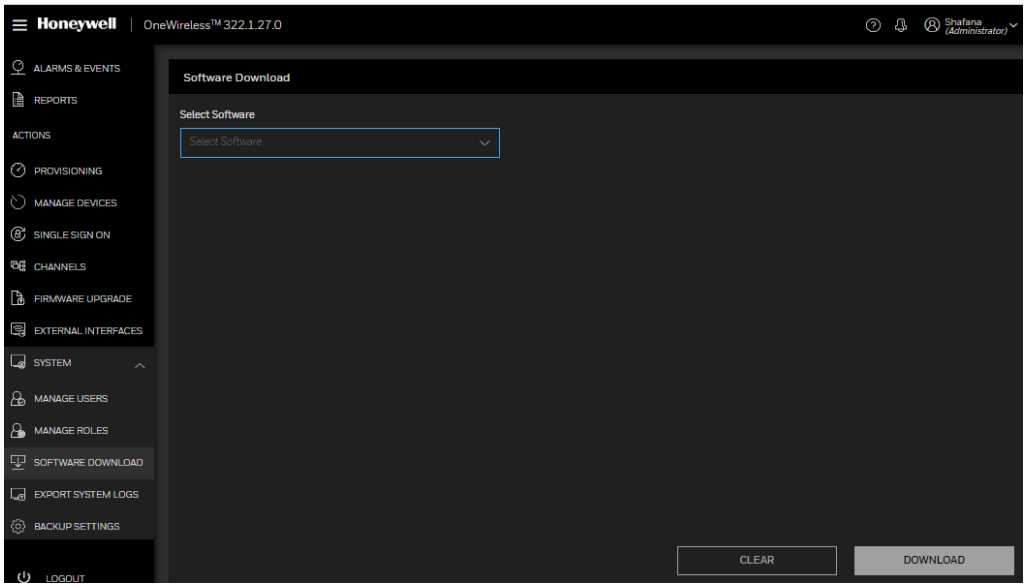
Prerequisites

- 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.

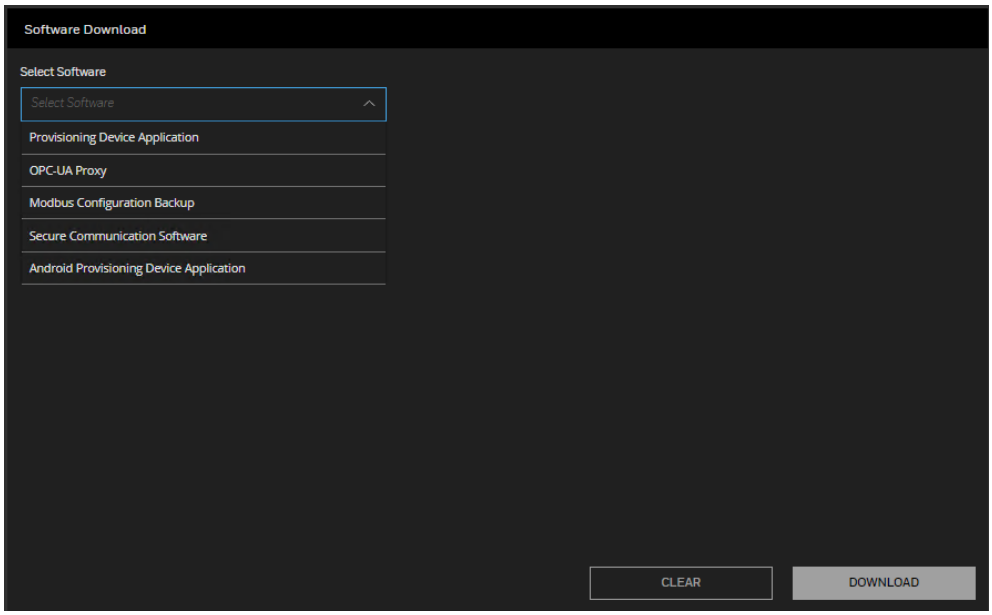
Install Android Provisioning Device Application from WDM

Perform the following procedure to Install Android Application from WDM.

1. Click **System** from left navigation menu and select **Software Download.**



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



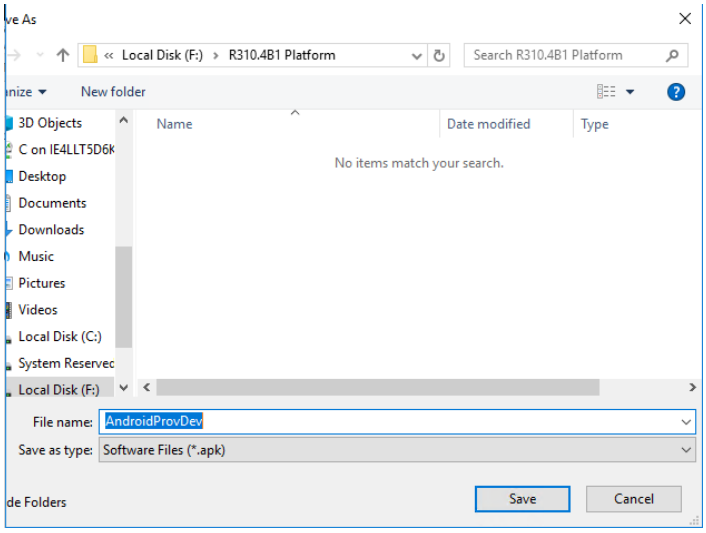
3. Software downloaded successfully message appears after downloading the software.

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

- Save AndroidProvDev.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

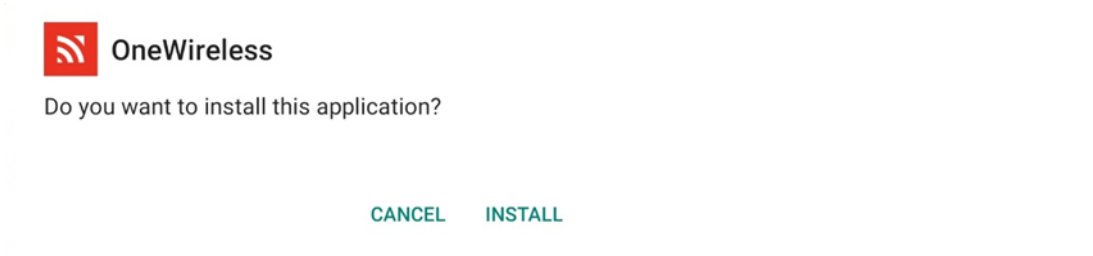
1. Install the application “AndroidProvDev” file in android device.



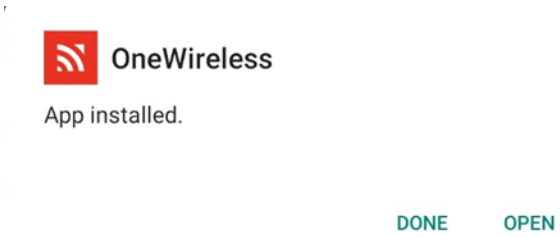
2. Download the application “AndroidProvDev” file to computer/laptop (Local Machine).
3. Transfer “AndroidProvDev” file from computer/laptop to Android mobile like any other file transfer.

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.



5. After a successful installation, click **OPEN** to launch the application.



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

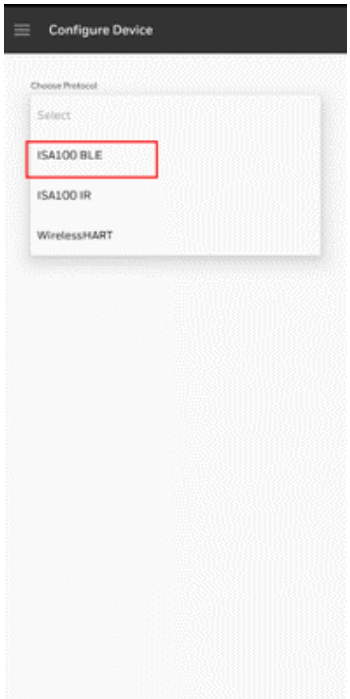
You can see these protocols while launching the application.

NOTE	**FDAP Gen3 and PCAP are provisioned using Bluetooth, all other Access points and devices use IR for provisioning.**

ISA100 BLE

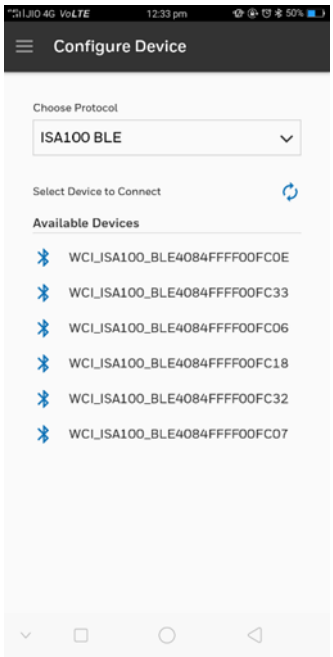
Provisioning Process for ISA100 BLE Devices

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



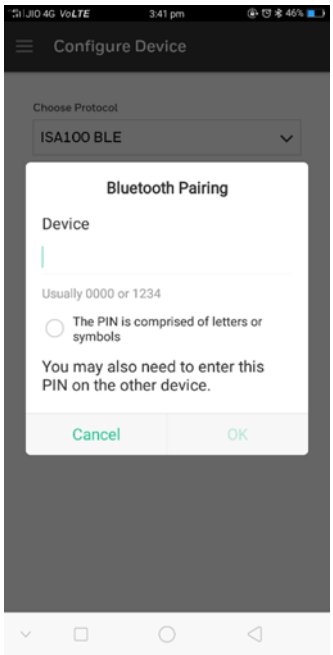
ATTENTION	**Allow Bluetooth permission when prompted by the device. This is mandatory for the application.**

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

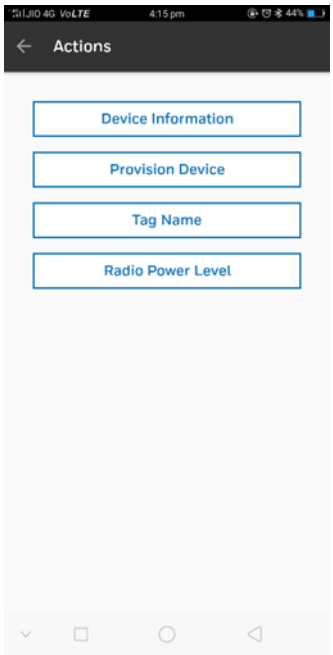


NOTE	**If the PCAP or FDAP Gen3 is in Reset to factory default state, use the default PIN "192021" to pair the device.** **If the PCAP or FDAP Gen3 is provisioned to a WDM and default pin is changed, see "BLE options" in Table. 7 *in Process Control Access Point (PCAP) User's Guide* / FDAP User's Guide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



Device Information:

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

NOTE	Read Device Information button is activated only when the BLE device is connected otherwise the button is disabled. This behavior is common for other screens.

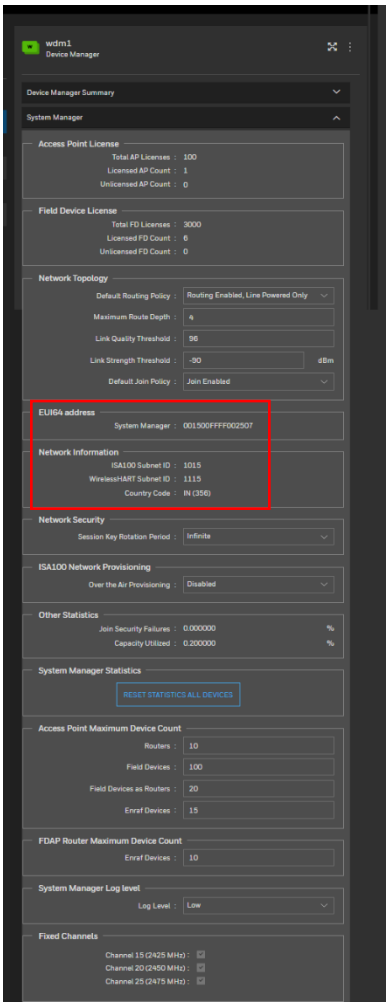
Provision Device

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

Provision information from Honeywell WDM User Interface

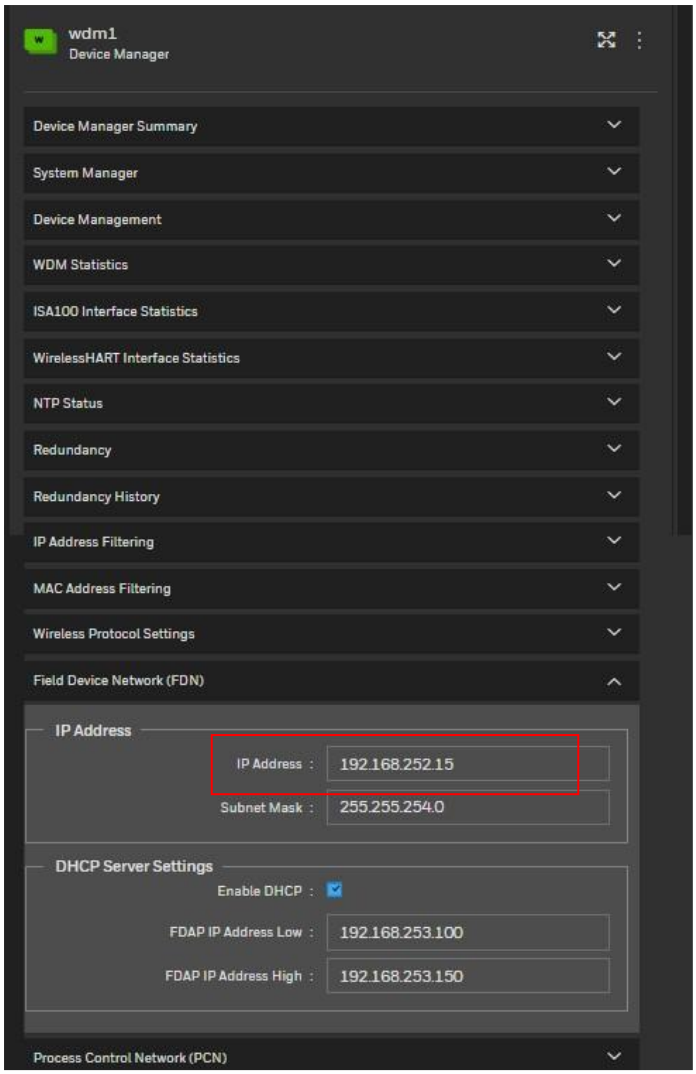
1. Get the SMEUI64 and Subnet ID from WDM to update it in mobile application.

.

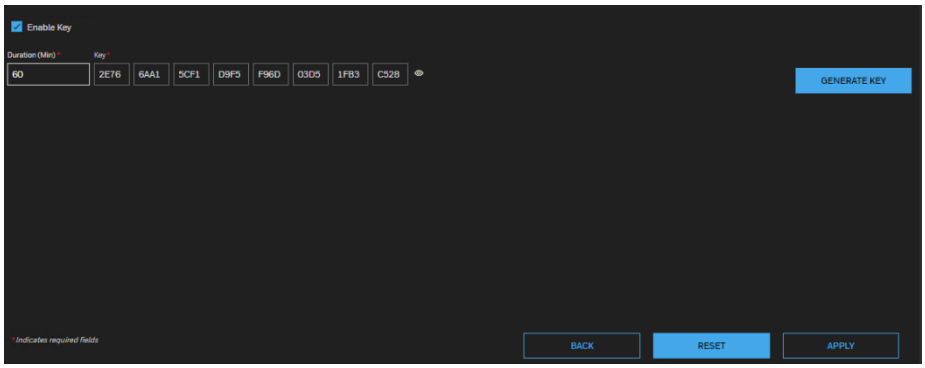


- SMEUI64 Address: Get the EUI64 address from Honeywell WDM User Interface as highlighted in blue color and the same must be used in SMEUI64 address in the Android Mobile Application.
- Subnet ID: Get the ISA100 Subnet ID from Honeywell WDM User Interface which is highlighted in red and the same must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

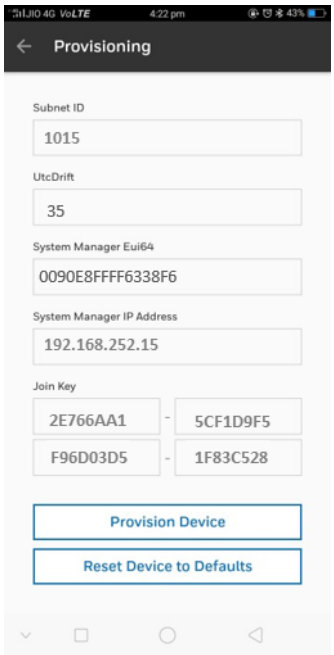
2. Get the IPv4 Address from WDM and Joining Key.



- 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.



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



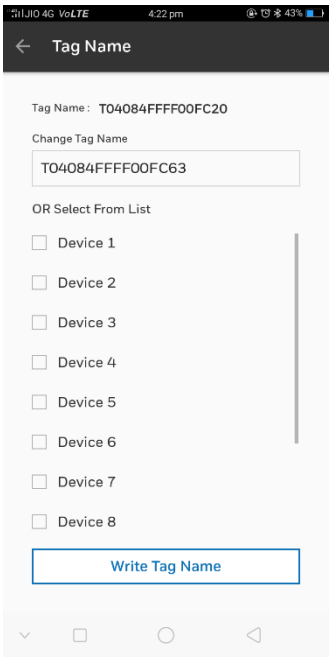
Now the Access points with BLE successfully joined the network.

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.

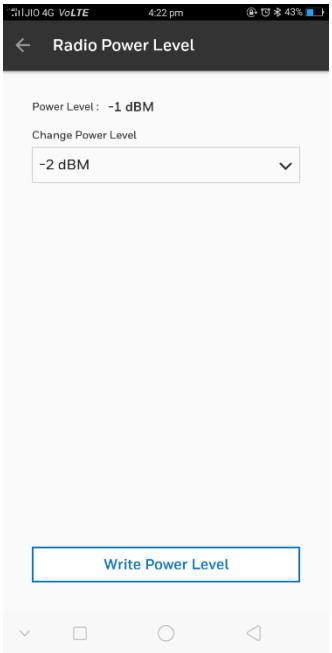
Tag name

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.



Radio Power Level

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



ATTENTION	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.

ATTENTION	**ACT-BT5713U-v3 cannot be used in hazardous area.**

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

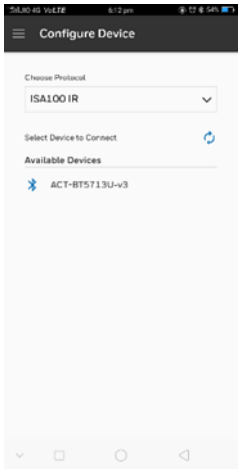
The ACT device acts as an intermediate bridge to Write/Read provisioning details and device parameters.

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.

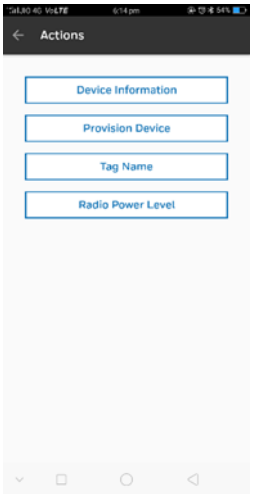


ATTENTION	**Allow Bluetooth permission when prompted by the device. This is mandatory for the application.**

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.

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



The procedures are similar to those mentioned for ISA100 BLE.

ATTENTION	**In case the request fails or times out, check the ACT-BT5713U-v3 device power, if it is in off, then turn it to "ON" and then retry in Android Mobile/Tablet application.**

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.

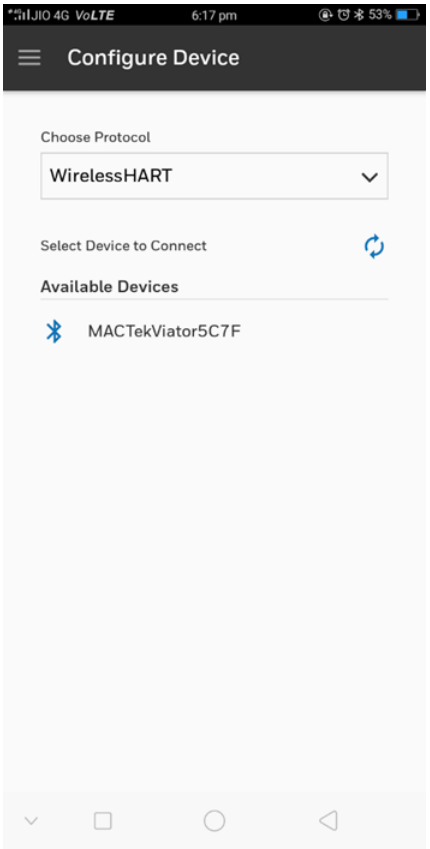
1. Ensure Viator Modem is powered up and it turns ON, which means Bluetooth is available to connect with Android Mobile.

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

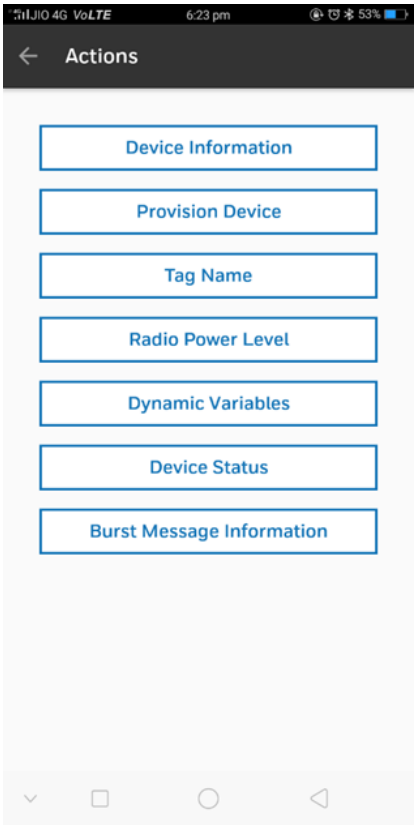
2. Ensure Viator Modem test clips are connected to WirelessHART Device.

Provisioning Process for WirelessHART Devices

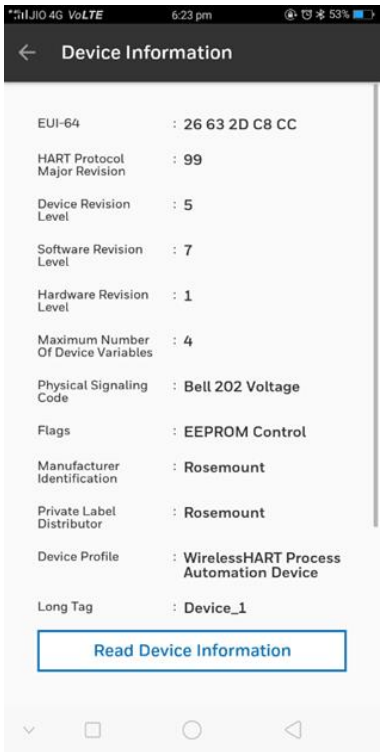
1. In the OneWireless application, select **WirelessHART** from the Choose Protocol drop-down list and discover MACTek Viator Bluetooth Device and provide the password/pin to pair with it.



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



a. Device Information (Read Only).



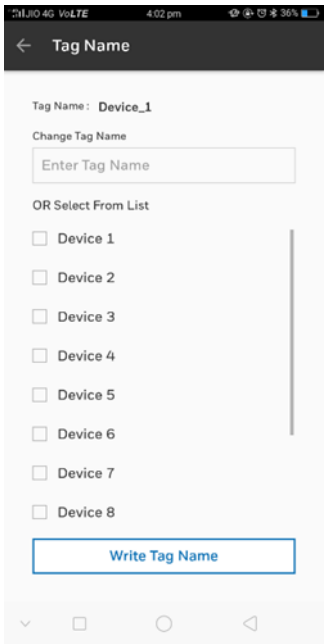
ATTENTION	In case the request fails or times out, check the MACTek Viator device power and, if it is in off state, turn it to “ON” and then retry in Android Mobile/Tablet application.”

b. Provision device.

c. Tag Name.

— Click **Tag name** to Edit/update Tag name.

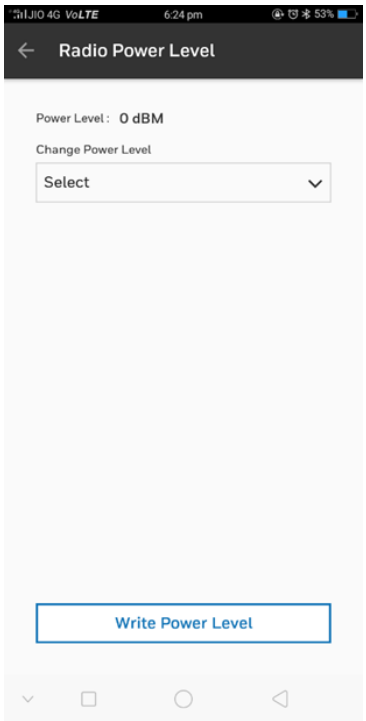
— You can edit the tag name from the drop-down list or type in the device name.

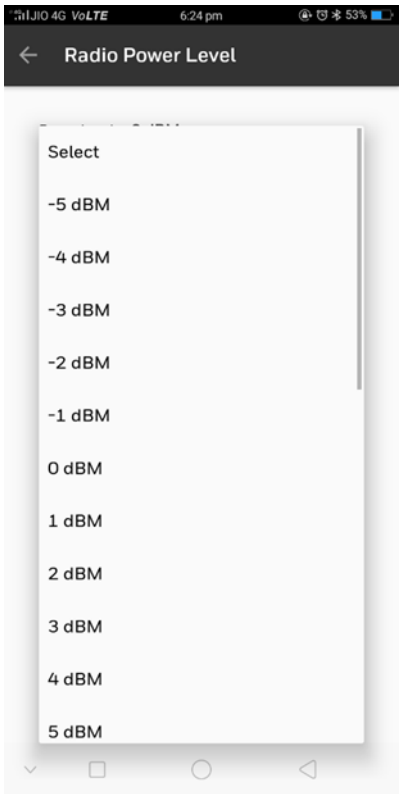


d. Update Power Level.

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

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



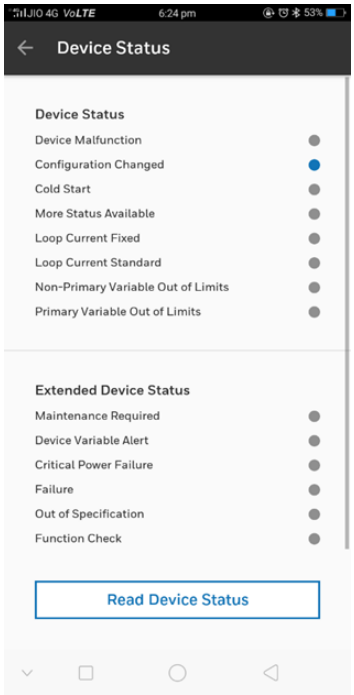


e. Dynamic Variables.

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

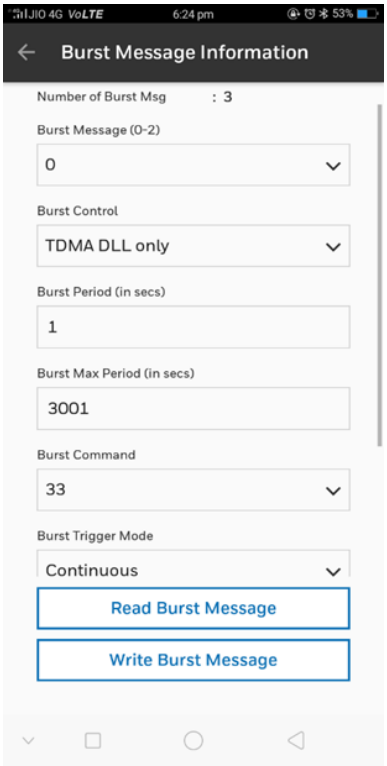
f. Device Status.

Status of the device is available in this option.



g. Burst Message Information.

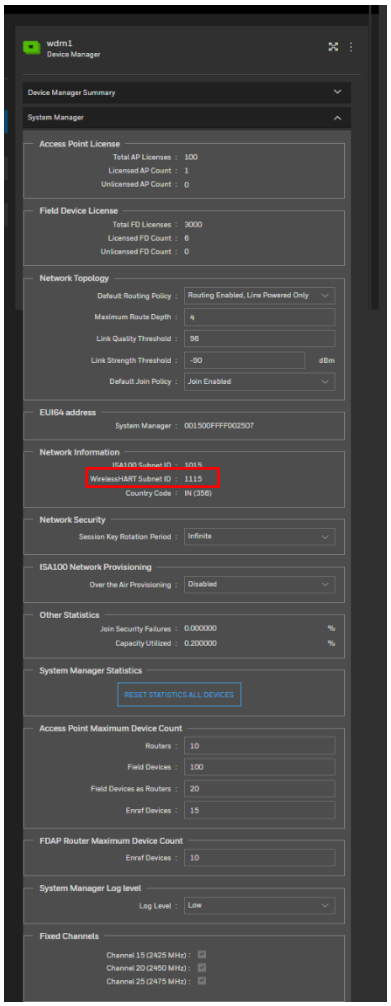
All the parameters required for publish configuration is available under this option.



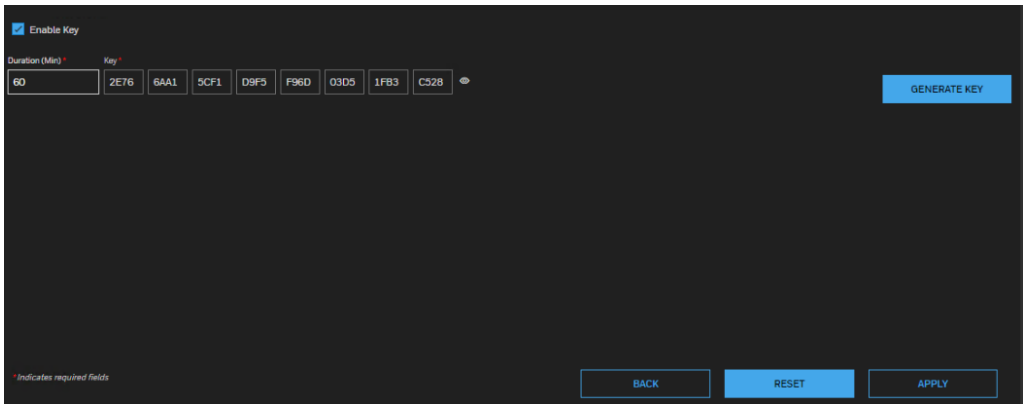
Provision Information from Honeywell WDM User Interface

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 WirelessHART Field Device using Values in Application

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.

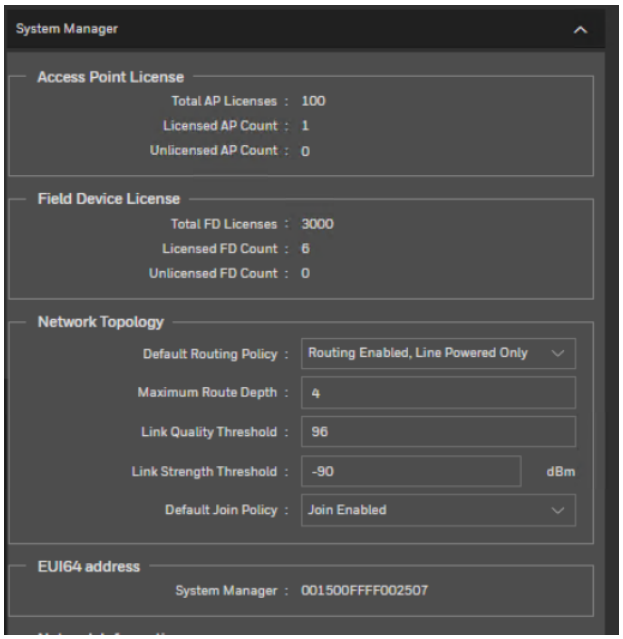
Considerations

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.



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.

CAUTION	**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.

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

5. Click **Apply**.

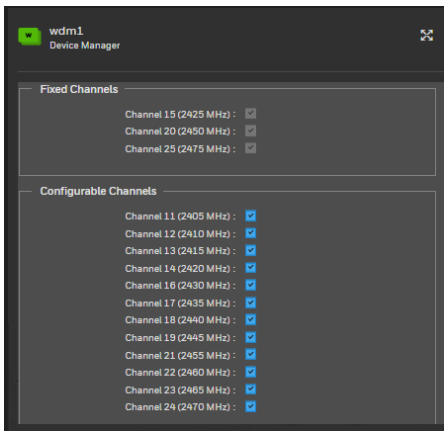
Configure Radio frequency Channel

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.



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

NOTE	**A total of 5 channels must be selected. It can comprise a minimum of 3 Fixed Channels and 2 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.

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.**

ATTENTION	***Redundancy is supported for the following combinations:*** • ***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.

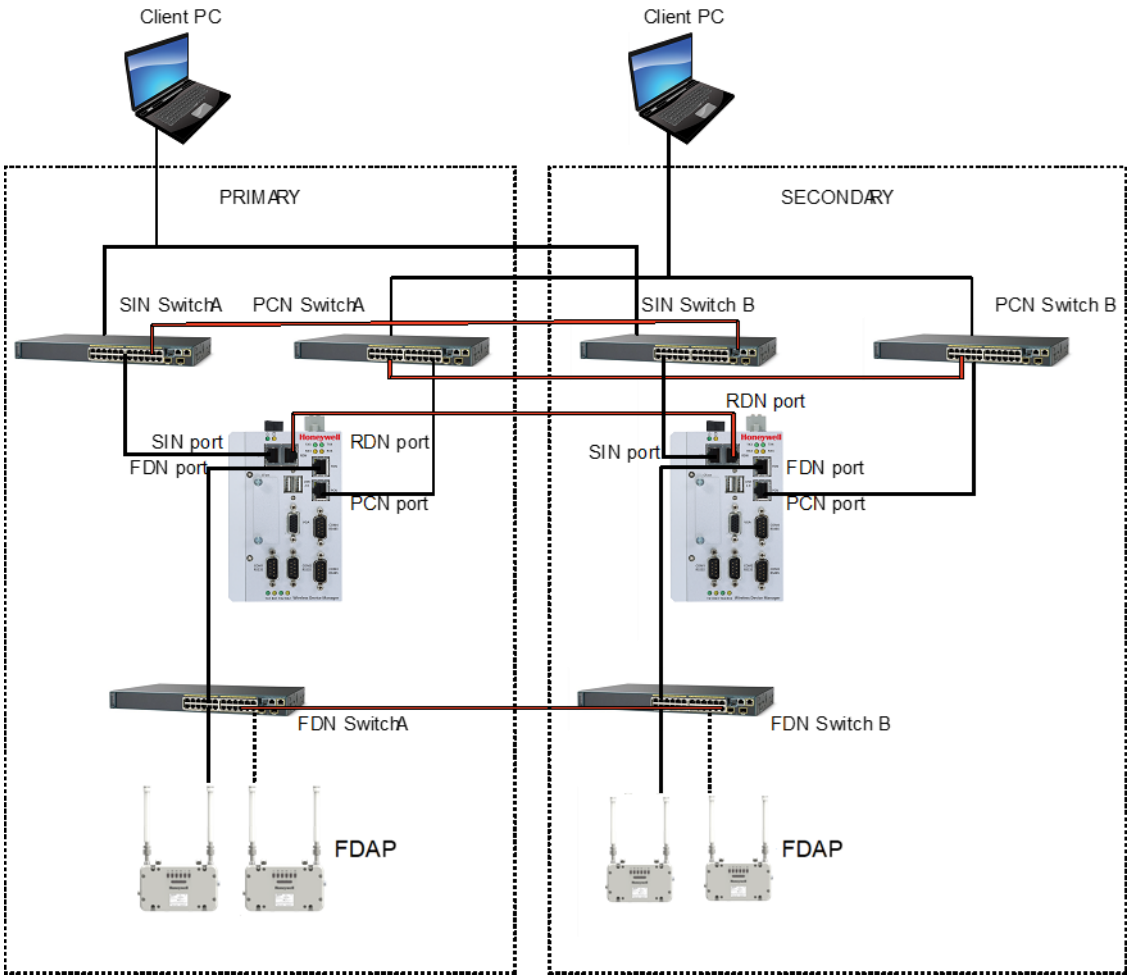


Fig. 12. Redundant Network Topology with FDAP

NOTE	FDAP Gen3 and FDAP2 also supports in above scenario.

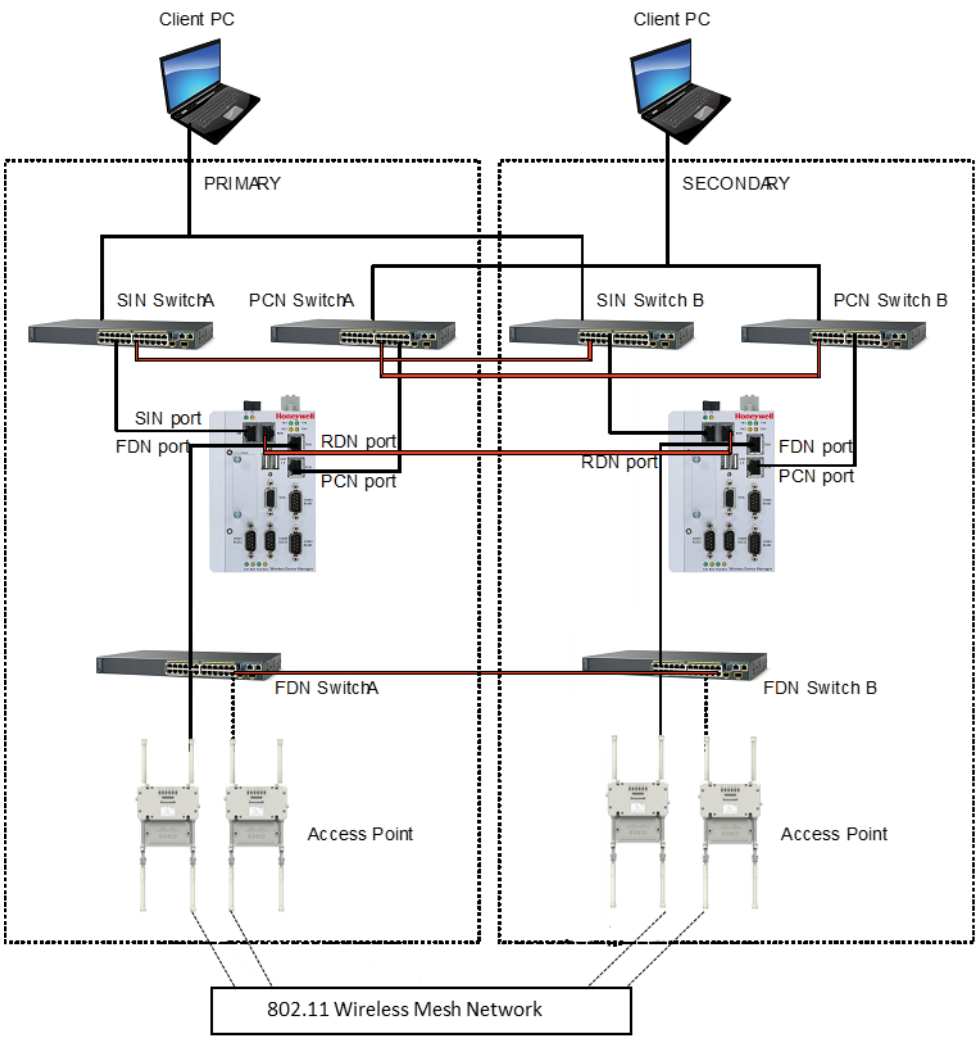


Fig. 13. Redundant Network Topology with Access Point

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

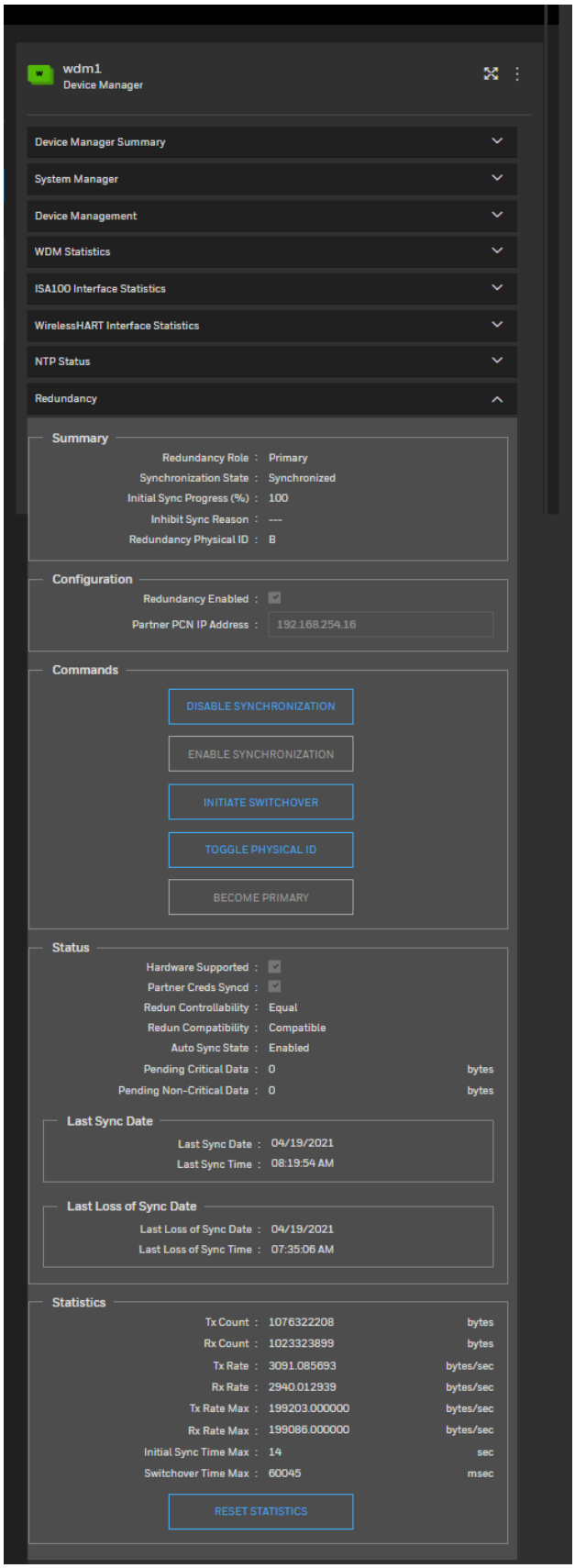
ATTENTION	• Cisco Catalyst 2960 Series 8 port switches and Cisco Catalyst 2960X Series 24 port switches are the supported FDN switches. For more information, refer to the Cisco Catalyst 2960 Series documents. • For information about Cisco Access Point configuration, see the OneWireless Wireless LAN Controller 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: 1. *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.


wdm1
Device Manager
Device Manager Summary
System Manager
Device Management
WDM Statistics
ISA100 Interface Statistics
WirelessHART Interface Statistics
NTP Status
Redundancy
Summary
Redundancy Role : Primary
Synchronization State : Synchronized
Initial Sync Progress (%) : 100
Inhibit Sync Reason : ---
Redundancy Physical ID : B
Configuration
Redundancy Enabled :
Partner PCN IP Address : 192.168.254.16
Commands
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 Date
Last Sync Date : 04/19/2021
Last Sync Time : 08:19:54 AM
Last Loss of Sync Date
Last Loss of Sync Date : 04/19/2021
Last Loss of Sync Time : 07:35:06 AM
Statistics
Tx Count : 1076322208 bytes
Rx Count : 1023323899 bytes
Tx Rate : 3091.085693 bytes/sec
Rx Rate : 2940.012939 bytes/sec
Tx Rate Max : 199203.000000 bytes/sec
Rx Rate Max : 199086.000000 bytes/sec
Initial Sync Time Max : 14 sec
Switchover Time Max : 60045 msec
RESET STATISTICS

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.

NOTE	**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.

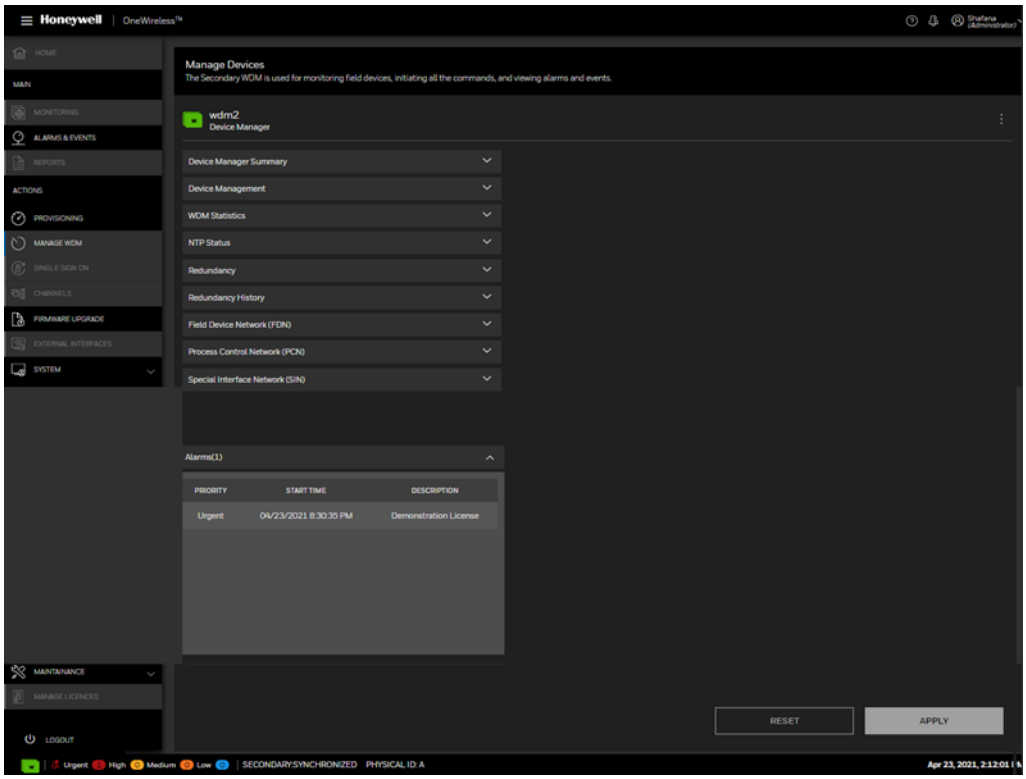
Secondary view

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.

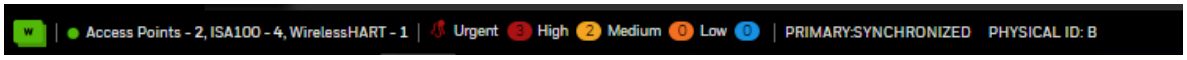

Honeywell
OneWireless™
Shafana (Administrator)
HOME
MAIN
MONITORING
ALARMS & EVENTS
REPORTS
ACTIONS
PROVISIONING
MANAGE WDM
SINGLE SIGN ON
CHANNELS
FIRMWARE UPGRADE
EXTERNAL INTERFACES
SYSTEM
MAINTAINANCE
MANAGE LICENCES
LOGOUT
Manage Devices
The Secondary WDM is used for monitoring field devices, initiating all the commands, and viewing alarms and events.
wdm2
Device Manager
Device Manager Summary
Device Management
WDM Statistics
NTP Status
Redundancy
Redundancy History
Field Device Network (FDN)
Process Control Network (PCN)
Special Interface Network (SIN)
Alarms(1)
PRIORITY
START TIME
DESCRIPTION
Urgent
04/23/2021 8:30:35 PM
Demonstration License
RESET
APPLY
Urgent
High
Medium
Low
SECONDARY:SYNCHRONIZED
PHYSICAL ID: A
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.



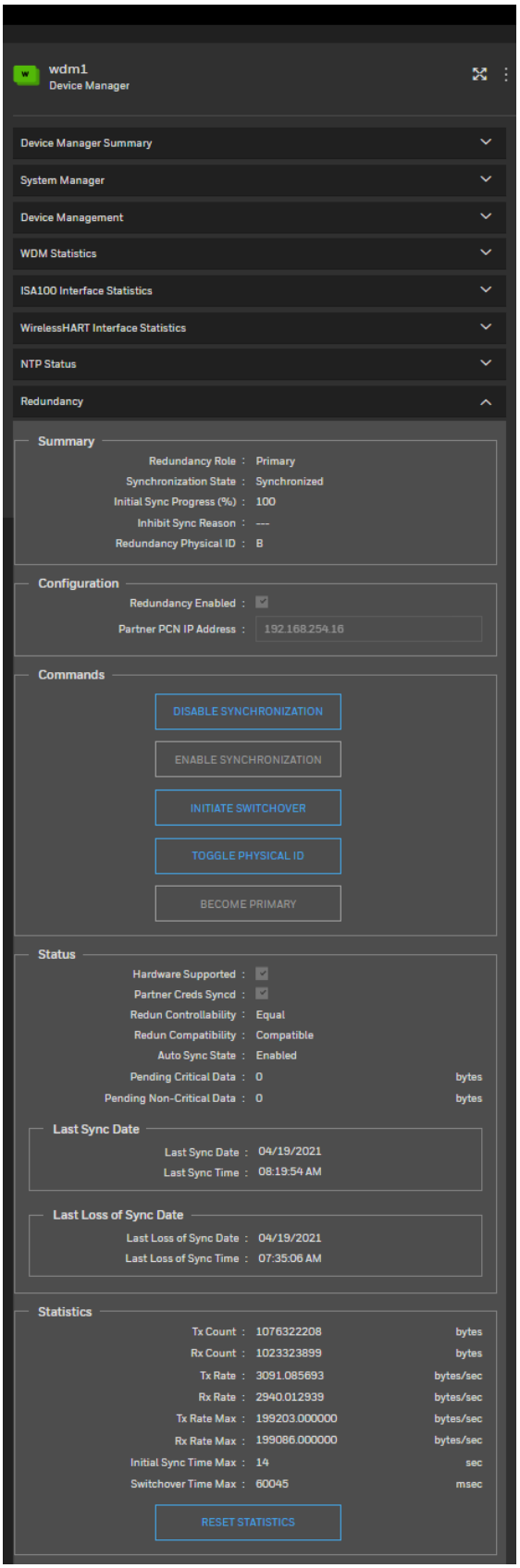
Manage Devices

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.


wdm1
Device Manager
Device Manager Summary
System Manager
Device Management
WDM Statistics
ISA100 Interface Statistics
WirelessHART Interface Statistics
NTP Status
Redundancy
Summary
Redundancy Role : Primary
Synchronization State : Synchronized
Initial Sync Progress (%) : 100
Inhibit Sync Reason : ---
Redundancy Physical ID : B
Configuration
Redundancy Enabled :
Partner PCN IP Address : 192.168.254.16
Commands
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 Date
Last Sync Date : 04/19/2021
Last Sync Time : 08:19:54 AM
Last Loss of Sync Date
Last Loss of Sync Date : 04/19/2021
Last Loss of Sync Time : 07:35:06 AM
Statistics
Tx Count : 1076322208 bytes
Rx Count : 1023323899 bytes
Tx Rate : 3091.085693 bytes/sec
Rx Rate : 2940.012939 bytes/sec
Tx Rate Max : 199203.000000 bytes/sec
Rx Rate Max : 199086.000000 bytes/sec
Initial Sync Time Max : 14 sec
Switchover Time Max : 60045 msec
RESET STATISTICS

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.

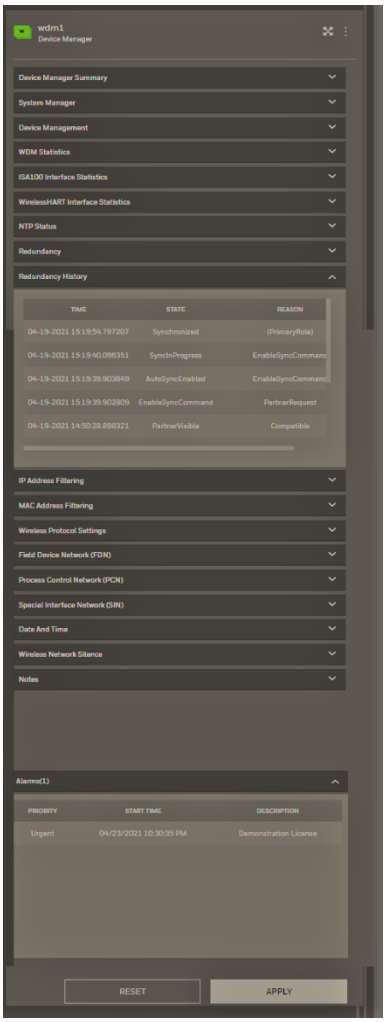
The following table describes the attributes displayed in the Redundancy tab of the WDM Property panel.

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. • Software failure on the primary WDM. • Hardware failure on the primary WDM.
Redun Compatibility	Indicates whether redundant partner modules are compatible and if not compatible, provides a reason. Initial synchronization is disabled on an incompatible WDM pair.
Auto Sync State	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 data	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.
Statistics	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).

ATTENTION	• **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.

ATTENTION	**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:** • **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.

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.**

To toggle the physical ID:

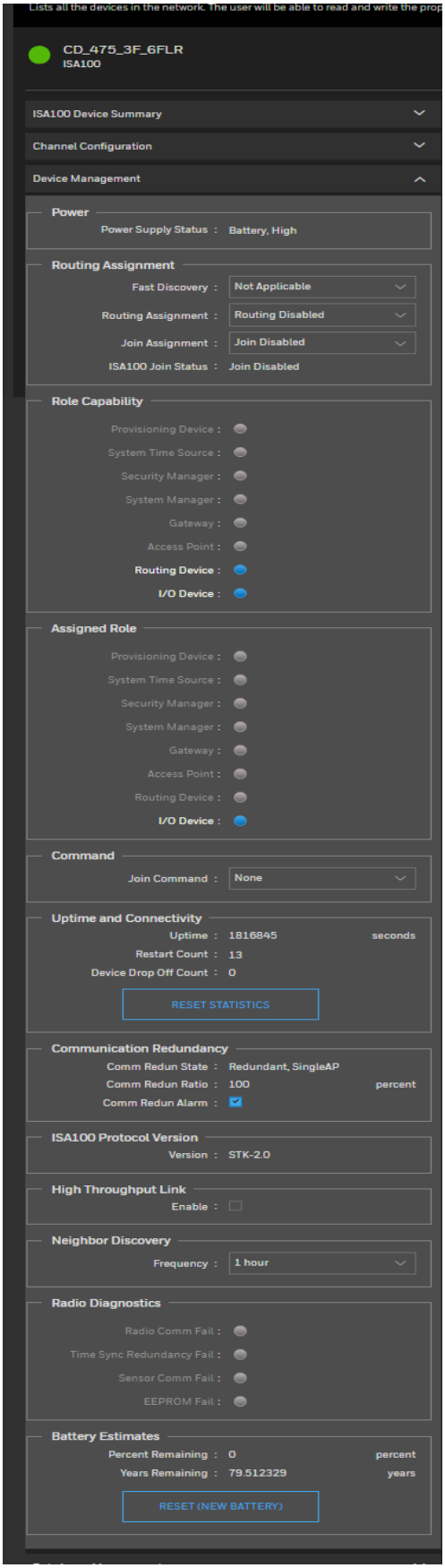
Expand **Redundancy** in the **Property Panel** and click **Toggle Physical ID**.

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

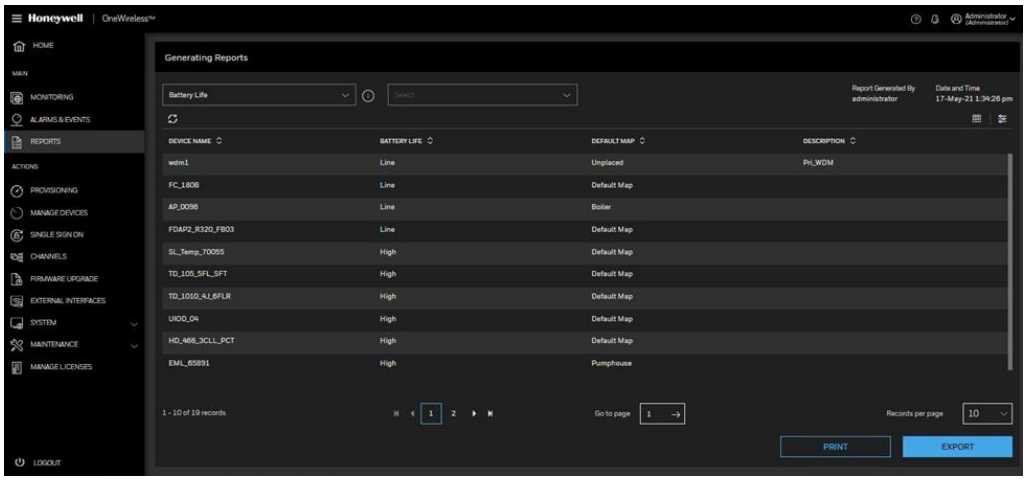
The Property panel displays the communication redundancy information.


Lists all the devices in the network. The user will be able to read and write the prop
CD_475_3F_6FLR
ISA100
ISA100 Device Summary
Channel Configuration
Device Management
Power
Power Supply Status : Battery, High
Routing Assignment
Fast Discovery : Not Applicable
Routing Assignment : Routing Disabled
Join Assignment : Join Disabled
ISA100 Join Status : Join Disabled
Role Capability
Provisioning Device :
System Time Source :
Security Manager :
System Manager :
Gateway :
Access Point :
Routing Device :
I/O Device :
Assigned Role
Provisioning Device :
System Time Source :
Security Manager :
System Manager :
Gateway :
Access Point :
Routing Device :
I/O Device :
Command
Join Command : None
Uptime and Connectivity
Uptime : 1816845 seconds
Restart Count : 13
Device Drop Off Count : 0
RESET STATISTICS
Communication Redundancy
Comm Redun State : Redundant, SingleAP
Comm Redun Ratio : 100 percent
Comm Redun Alarm :
ISA100 Protocol Version
Version : STK-2.0
High Throughput Link
Enable :
Neighbor Discovery
Frequency : 1 hour
Radio Diagnostics
Radio Comm Fail :
Time Sync Redundancy Fail :
Sensor Comm Fail :
EEPROM Fail :
Battery Estimates
Percent Remaining : 0 percent
Years Remaining : 79.512329 years
RESET (NEW BATTERY)

- 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.



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**.

ATTENTION	**You can change the Tag Name by double-clicking the field device name in the Selection panel.**

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.

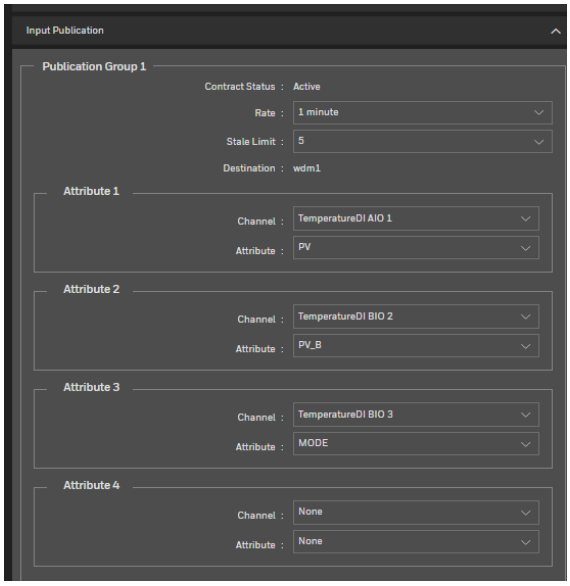
Publication period	Stale Limit
½ second	120
1 second	60
2 seconds	30
5 seconds	12
10 seconds	6
30 and 60 seconds	5
1, 5, 15, 30 minutes	5
1 hour	5

- **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.

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

To configure publication rate and stale limit

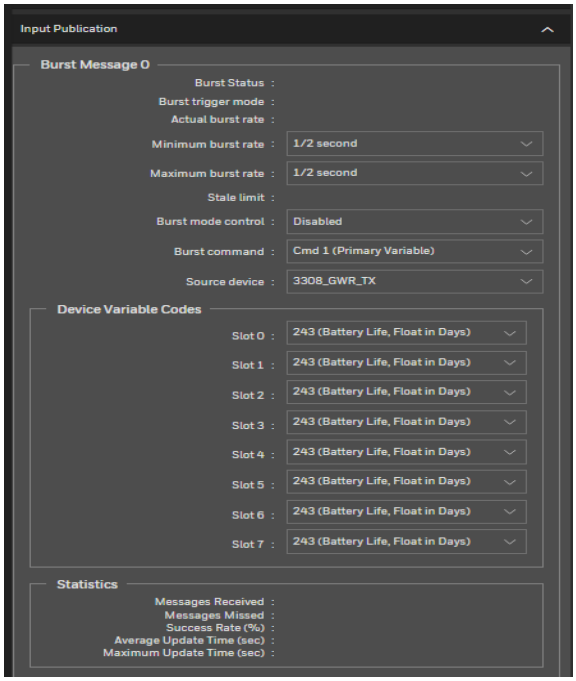
1. Select the field device in the Selection panel.
2. Expand Input Publication or Output Publication in the Property panel.



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.



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
½ 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

ATTENTION	**See WirelessHART specifications for more information.**

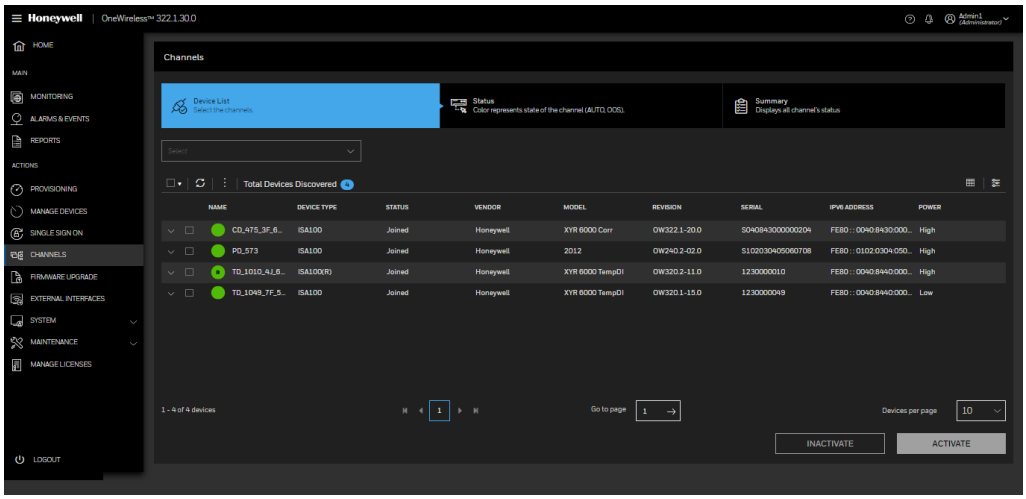
Calibrate Honeywell XYR6000 field devices

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.

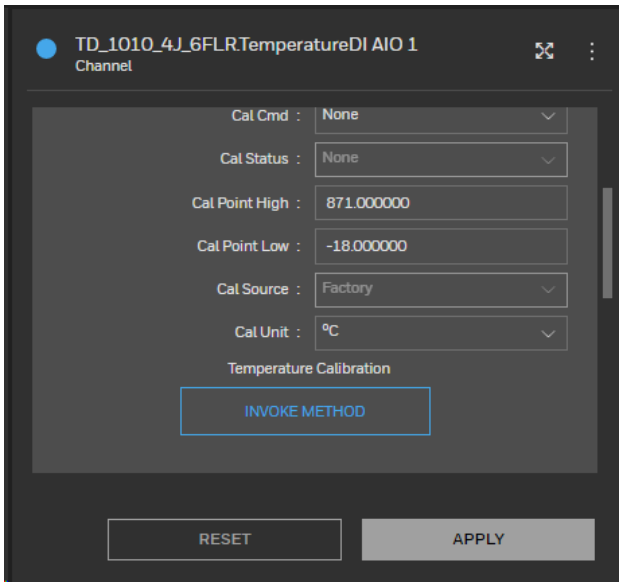


7. Select the field device channel from the selection list and click **Inactivate.**

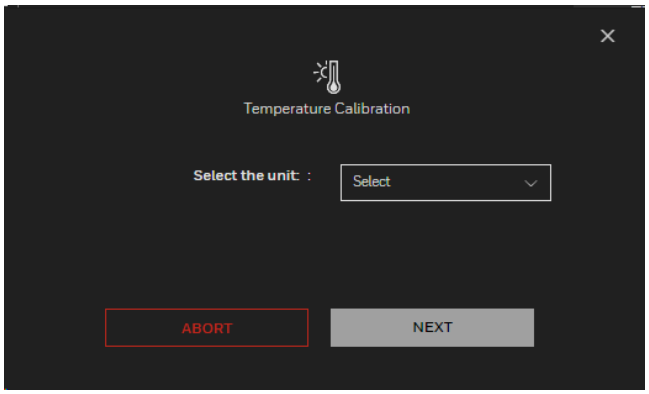
8. Ensure you inactivate the channels before starting calibration. You cannot perform calibration when the channel is online.

2. Click **Apply**.

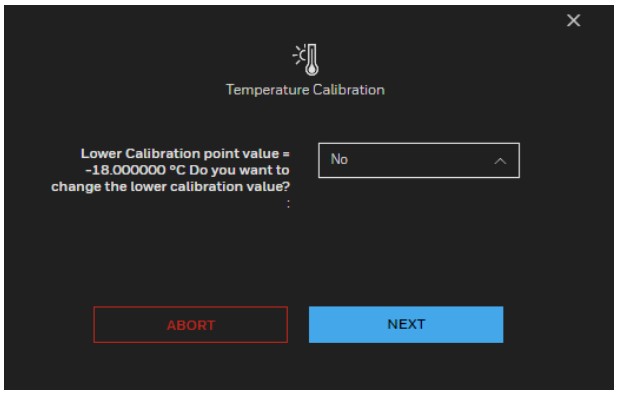
3. In the Property Panel, expand **Calibration**.



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



5. Select the unit (^{0}C or ^{0}F) and click **Next** and follow on-screen instructions to complete calibration.
6. Select **Yes** or **No** and click **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.

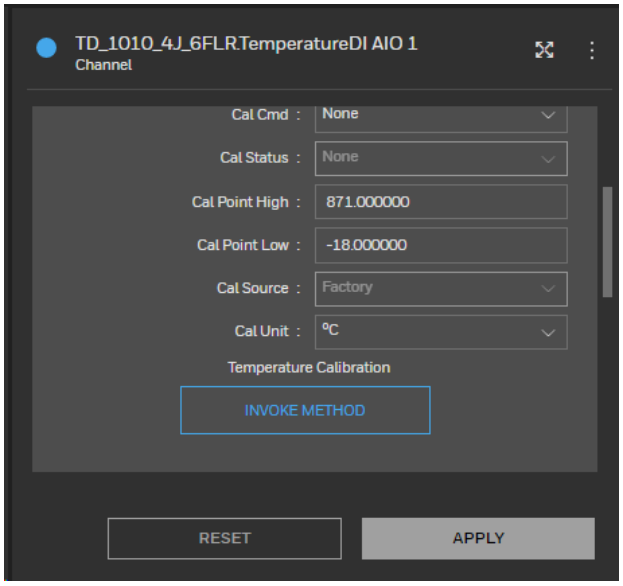
7. Select the field device channel from the selection list under **CHANNELS** from Left Navigation Menu bar and click **Activate**.
8. Click **Apply**.
    - You can run only one method at a time for a field device using the current login session.
    - If you close the Web browser while a method is 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:

1. 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**.



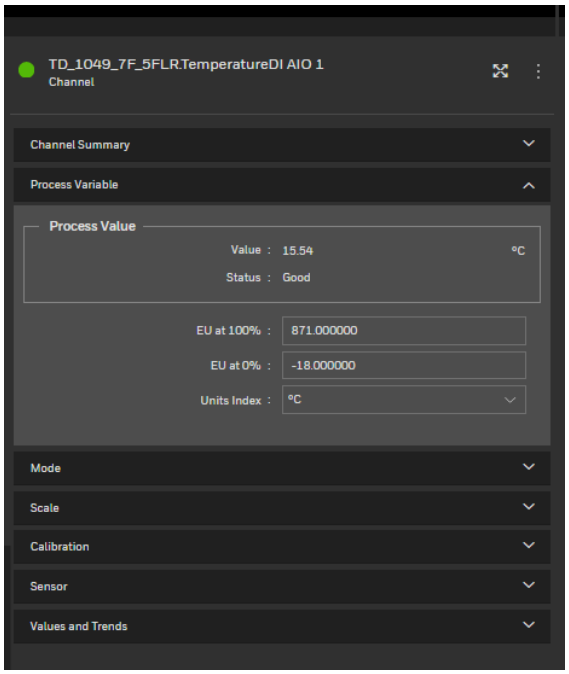
4. Set the following calibration parameters:
   - **Cal Cmd** – The options available are **None**, **Cal Lower** (to calibrate device with lower calibration limit), **Cal Upper** (to calibrate device with higher calibration limit), **Cal Restore** (to restore calibration setting), and **Cal Clear** (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.

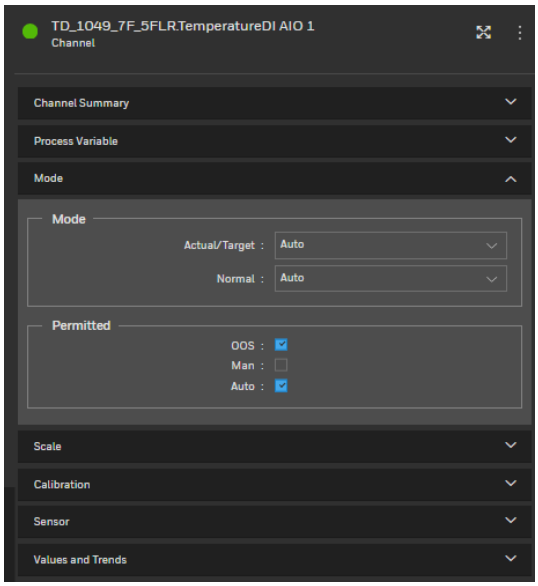


   - **EU at 100%**: Specifies the high range PV value in Engineering Units.
   - **EU at 0%**: Specifies the low range PV value in Engineering Units.
   - **Units Index**: Specifies the unit of the measurement value. The value varies according to the sensor type selected for a channel. For example, in 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**.

ATTENTION	**After applying the changes, the newly configured values appear under the Scale panel.**

To configure Mode:

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



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.

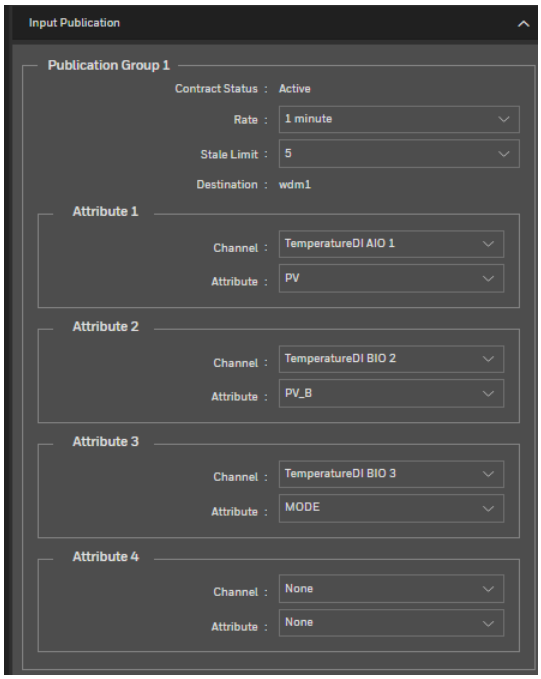
3. Click **Apply**.

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.



ATTENTION	**To disable data publication, select None in the Channel list.**

4. Click **Apply**.

Configure channel instantiation

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.

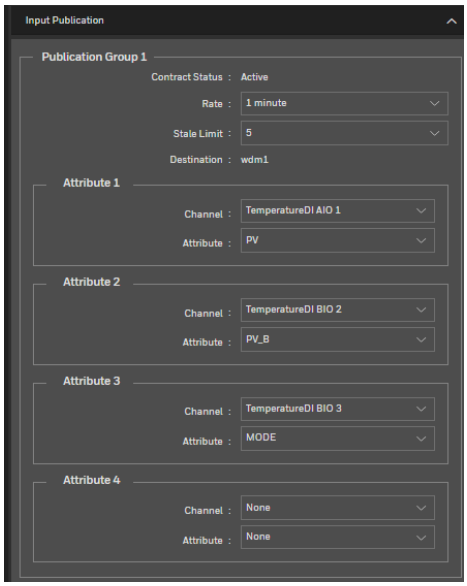
To inactivate channel:

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.

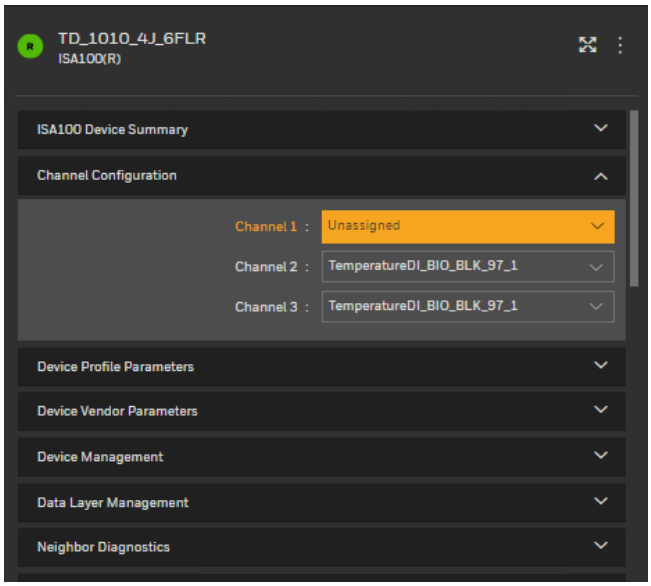


4. Click **Apply**.

   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.



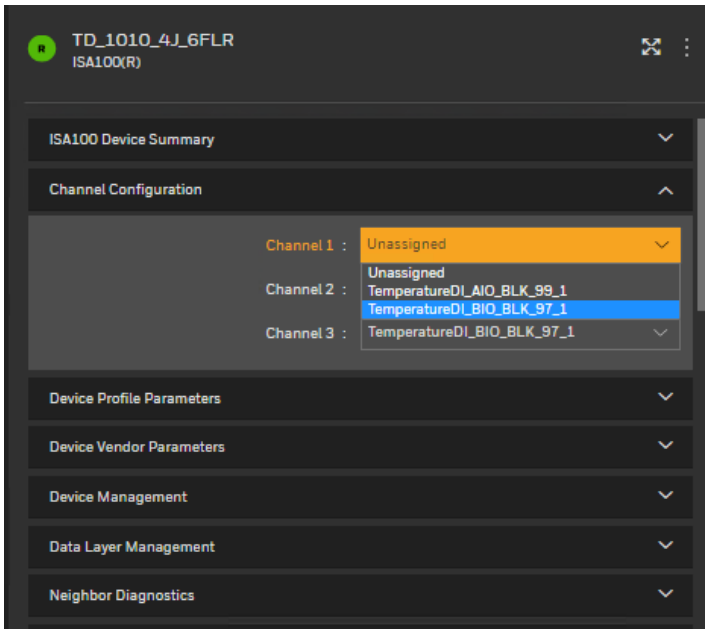
2. Click **Apply**.

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.



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**.

ATTENTION	**To disable data publication, select None in the Channel list.**

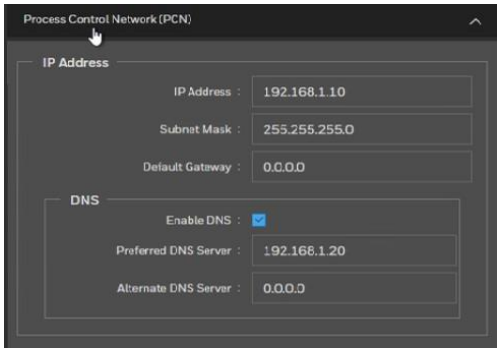
5. Click **Apply**.

Enable Device Network System (DNS)

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

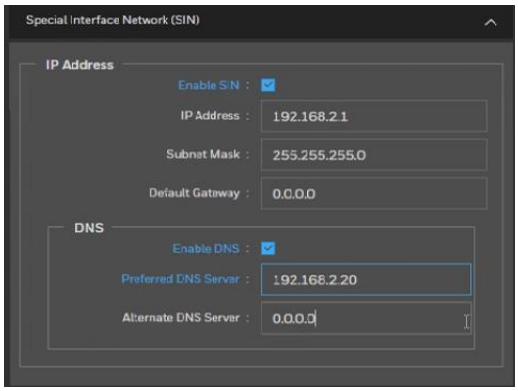
To enable Device Network System (DNS) in Process Control Network (PCN)

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**.



NOTE	**To enable DNS, make sure that SIN is enabled.**

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.

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

ATTENTION	• All users can view all the notes added by other users.
	• To delete any note, click the delete icon adjacent to the note.
	  – 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 site-specific 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.

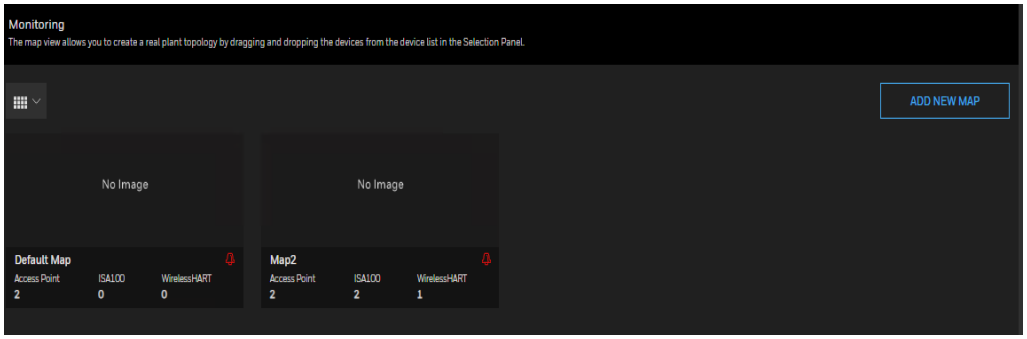
You can create a map of entire plant and maps of smaller areas, each containing the same devices. The FDAPs and devices can be placed on multiple maps.

Fig. 14. Site-specific monitoring

Configure site maps

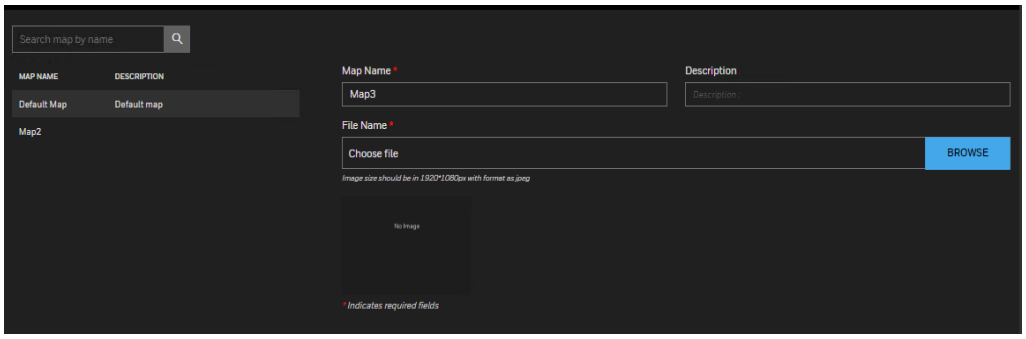
To add new map:

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.



ATTENTION	**The site map must be a .jpg file.** **File resolution: 1920 x 1080, 1600 x 1200, 1366 x 768, 1280 x 1024**

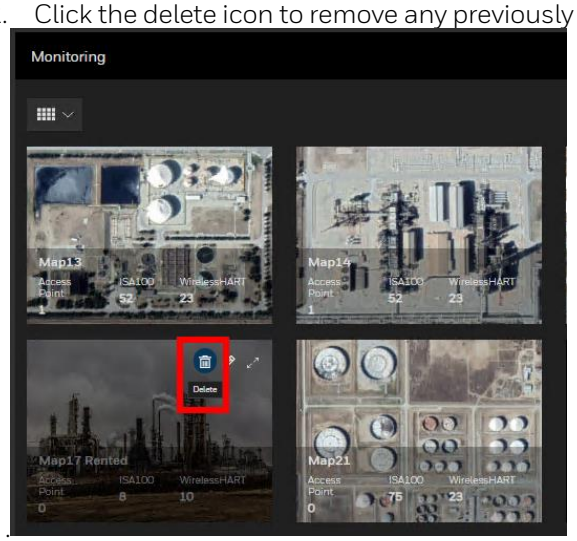
5. Click **Open** to upload the site map.
6. Click **Save**.

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. Click the delete icon to remove any previously loaded site map.

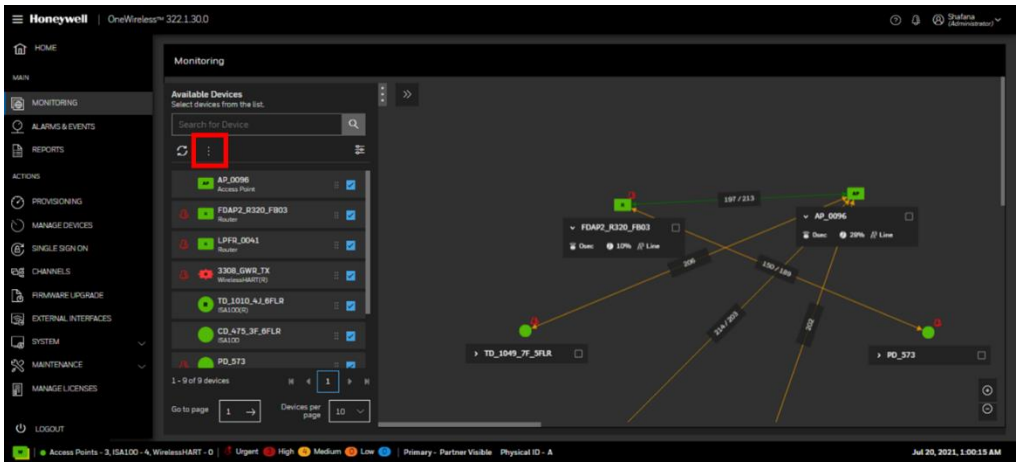


Position the devices on the map

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.

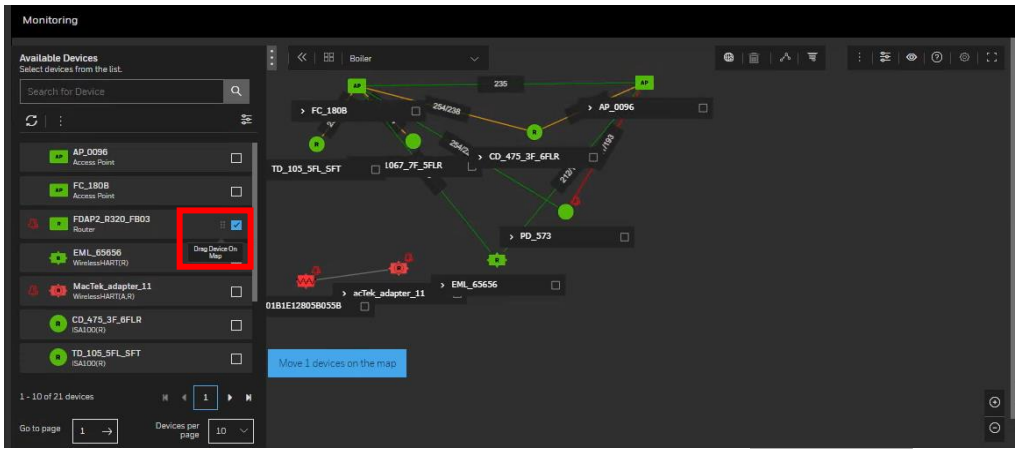
To position the devices on the map:

1. On the Selection Panel, select the device to be positioned on the map.
2. Click ⋮ icon to expand the **Available Devices** menu.
3. You can refresh the selection by clicking the **refresh** button.
4. 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.



8. Repeat steps 1 and 2 to place other devices.
9. Click 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.

ATTENTION	**The Default Map list displays all the maps on which the device is 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  icon to view 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**.

ATTENTION	**Click Restore Defaults to restore the Honeywell recommended default values.**

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).

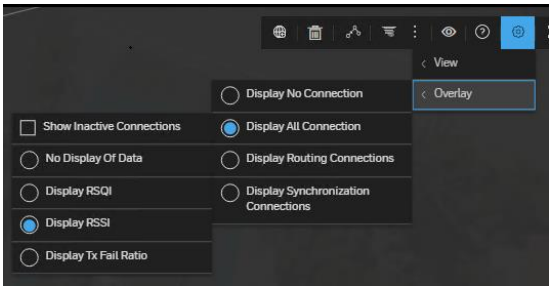
   

4. Verify the device communication statistics information such as RSQI, RSSI, and TxFailRatio as follows:

   a. Click icon in the top left of map view for the Map options.

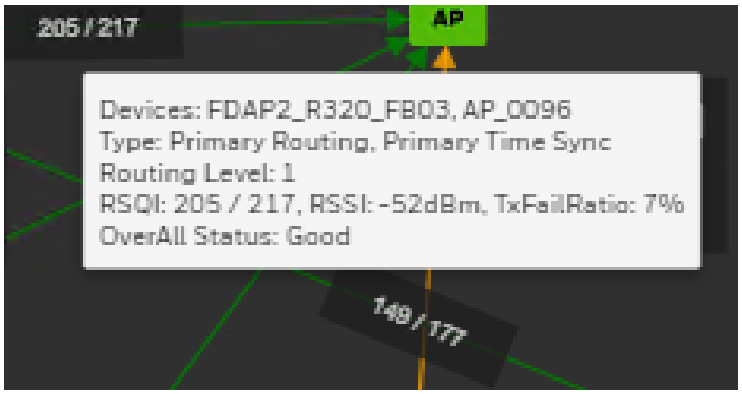
   b. Click icon to select **View** and **Overlay** settings option.

   c. Select **Overlay > Display All Connection >** Select the required device communication statistics information such as **RSQI**, **RSSI**, and **TxFailRatio**.

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.

ATTENTION	**While configuring the network, ensure that the lowest RSQI on each active link is greater than 180 and the lowest RSSI on each active link is 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.**

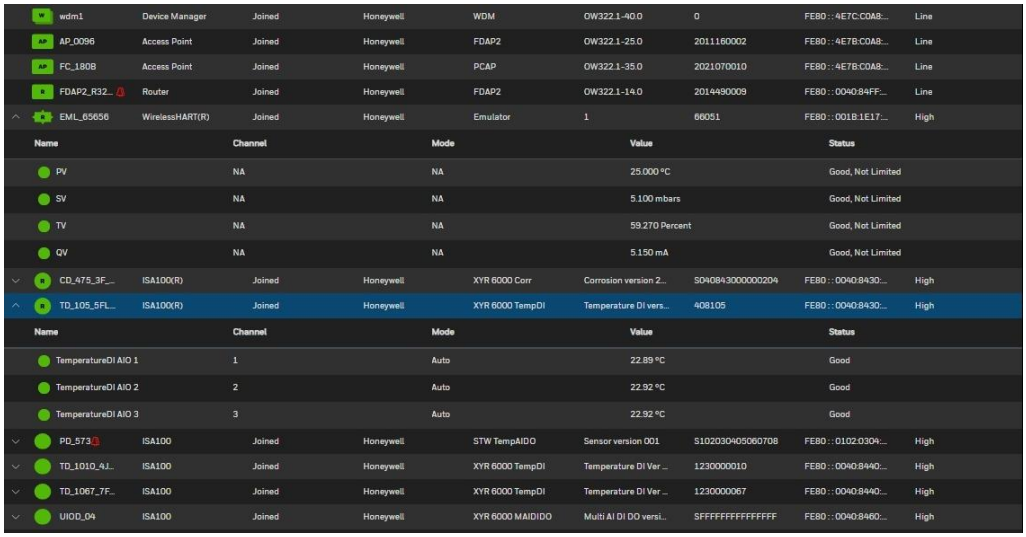
4. Set the Alert Priority. The **Alert Priority** can contain the following values.
   - 0-2: Journal (only events are reported)
   - 3-5: Low
   - 6-8: Medium
   - 9-11: High
   - 2-15: Urgent
5. Click **Apply**.

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	FE80::4E7C:C0A8:...	Line
AP_0096	Access Point	Joined	Honeywell	FDAP2	OW322.1-25.0	2011160002	FE80::4E7B:C0A8:...	Line
FC_180B	Access Point	Joined	Honeywell	PCAP	OW322.1-35.0	2021070010	FE80::4E7B:C0A8:...	Line
FDAP2_R32...	Router	Joined	Honeywell	FDAP2	OW322.1-14.0	2014490009	FE80::0040:84FF:...	Line
EML_65656	WirelessHART(R)	Joined	Honeywell	Emulator	1	66051	FE80::001B:1E17:...	High
Name		**Channel**		**Mode**	**Value**		**Status**	
PV		NA		NA	25.000 °C		Good, Not Limited	
SV		NA		NA	5.100 mbars		Good, Not Limited	
TV		NA		NA	59.270 Percent		Good, Not Limited	
QV		NA		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
TD_105_5FL...	ISA100(R)	Joined	Honeywell	XYR 6000 TempDI	Temperature DI vers...	408105	FE80::0040:8430:...	High
Name		**Channel**		**Mode**	**Value**		**Status**	
TemperatureDI AIO 1		1		Auto	22.89 °C		Good	
TemperatureDI AIO 2		2		Auto	22.92 °C		Good	
TemperatureDI AIO 3		3		Auto	22.92 °C		Good	
PD_573	ISA100	Joined	Honeywell	STW TempAIDO	Sensor version 001	S102030405060708	FE80::0102:0304:...	High
TD_1010_4J...	ISA100	Joined	Honeywell	XYR 6000 TempDI	Temperature DI Ver ...	1230000010	FE80::0040:8440:...	High
TD_1067_7F...	ISA100	Joined	Honeywell	XYR 6000 TempDI	Temperature DI Ver ...	1230000067	FE80::0040:8440:...	High
UIOD_04	ISA100	Joined	Honeywell	XYR 6000 MAIDIDO	Multi AI DI DO versi...	SFFFFFFFFFFFFFFF	FE80::0040:8460:...	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.

Table. 8. Device attributes in the extended Selection Panel

Device	Description
Tag Name	Name of the device.
Type	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.

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	Consequences	Recommended corrective action	Response time	Parameter/ Reported value	Default value
WDM	Bad Join Key	FDAP or field device is attempting to join the network with an invalid key.	WDM rejects the join request by the FDAP or the field device.	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.	WDM rejects the join request by the FDAP or the field device.	Locate the devices and re-provision the devices with valid join keys.	N/A	None	N/A
WDM	Key Authentication 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	Consequences	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.	WDM redundancy is not available and primary WDM failure results in loss of view and/or control.	Enable sync if disabled. Reconnect RDN private path communication cable. If redundancy is no longer required, disable redundancy.	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	Consequences	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	Consequences	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	Consequences	Recommended corrective action	Response time	Parameter/ Reported value	Default value
WDM	MQTT Server failed to connect to MQTT broker	If MQTT connection to the server not established successfully or dropped	Tag data 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 communication 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.	Loss of power to the field device	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	Consequences	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 communication with the field device and the associated channels.	• This issue may be caused by delays encountered when installing a wireless system with a third party Wi-Fi (TCP/IP) mesh network. • Connect the WDM and at least one FDAP directly to the same Ethernet switch. This allows the WDM and Ethernet-connected FDAPs to synchronize clocks over Ethernet. • Position additional FDAPs in such a way that a Wireless mesh network is formed between the nodes. Additional FDAPs can synchronize the clocks over the Wireless mesh network.	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	Consequences	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.	None	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	Consequences	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.	None	Remove uncertified or incompatible Wireless devices from the Wireless network.	N/A	TPDU	N/A

Source	Alarm/Event notification	Possible cause	Consequences	Recommended corrective action	Response time	Parameter/ Reported value	Default value
FDAP, field device	DL Connectivity	Failure in data transmission between wireless field devices, at 90% packet failure rate or greater. FDAP may have a poor communication link with another wireless field device on the wireless network.	Loss of communication 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.	None	None	N/A	DLMO_CANDIDATES	N/A
FDAP, field device	Alarm Recovery Start	Initiation of alarms recovery for FDAP or field device radio.	None	None	N/A	None	N/A
FDAP, field device	Alarm Recovery End	Completion of alarms recovery for FDAP or field device radio.	None	None	N/A	None	N/A

Source	Alarm/Event notification	Possible cause	Consequences	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 communication with the field device and the associated channels.	Remove any strong interference sources near the wireless field device or reposition the field device to limit interference.	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 communication with the field device and the associated channels.	None	N/A	Number of failures	N/A

Source	Alarm/Event notification	Possible cause	Consequences	Recommended corrective action	Response time	Parameter/ Reported value	Default 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 communication with the field device and the associated channels.	• Verify that there is no loss of communication between the WDM and the field device, specifically loss of power or connectivity to the FDAPs. • Physically check the field device. Replace failed battery or failed hardware, as appropriate.	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	Consequences	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 communication with the field device and the associated channels.	• Replace the batteries. • Check the external power 24V supply and wiring.	• For battery powered devices, replace the batteries within two to four weeks after initial alert. • For externally powered devices, immediate action is required.	DIAG_STATUS, DIAG_STATUS_DETAIL	0
Field device	Out of Specification Alert	Invalid or unreadable calibration data.	Channel may report incorrect PV value.	Perform user calibration.	Immediate	DIAG_STATUS, DIAG_STATUS_DETAIL	0

Source	Alarm/Event notification	Possible cause	Consequences	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 communication with the field device and the associated 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_STATUS, DIAG_STATUS_DETAIL	0
Field device AI Channel	Out Of Service	Field device AI channel is out-of-service.	None	None	N/A	MODE.ACTUAL	OOS
Field device AI Channel	Sensor Over Temperature	The meter body exceeded the maximum temperature as defined by the meter body characterization data.	Channel may report incorrect PV value.	Determine cause of excessive temperature.	Immediate	DIAG_STATUS, DIAG_STATUS_DETAIL	0
Field device AI Channel	Out Of Service	Field device DI channel is out-of-service.	None	None	N/A	MODE.ACTUAL	OOS

Source	Alarm/Event notification	Possible cause	Consequences	Recommended corrective action	Response time	Parameter/ Reported value	Default value
Field device AI 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_STATUS, DIAG_STATUS_DETAIL	0
Field device AI Channel	Out Of Service	Field device DO channel is out-of-service.	None	None	N/A	MODE.ACTUAL	OOS
Field device AI 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. • Changes to the configured output value would reflect on the	Determine the cause of missing the published data or verify the stale count limit.	Immediate	DIAG_STATUS, DIAG_STATUS_DETAIL	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	PCN IP address 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/unprotect.	Redundancy enabled/ disabled	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.

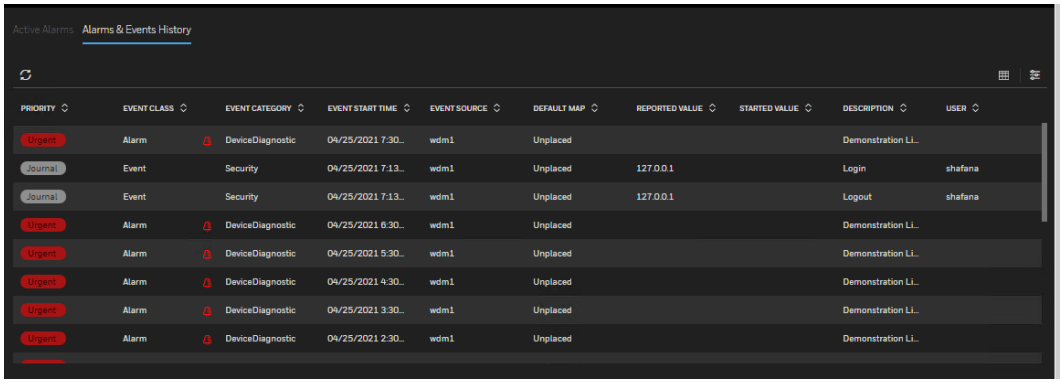
To monitor alarms and events

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.



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.

NOTE	**Export to PDF is not supported**

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 0. 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: https://<WDM IP Address>/licenses/Third_Party_Licenses.txt

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

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.

ATTENTION	**Contact GTAC to get the professional installer license.**

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.

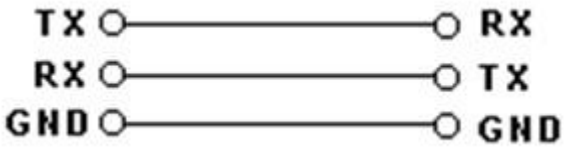


Fig. 16. RS-232

Table. 10. RS-232 pin 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.

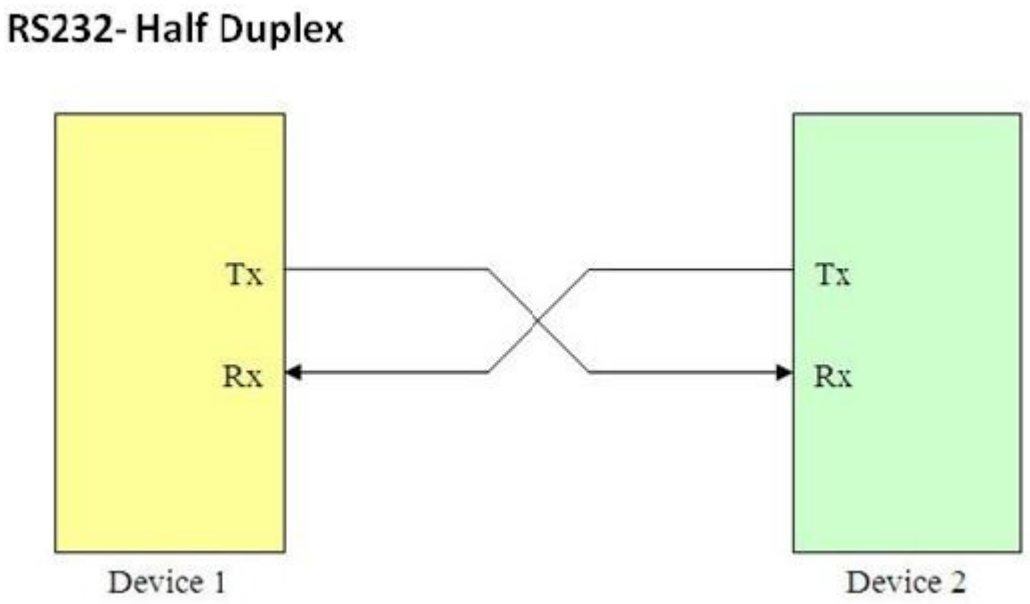
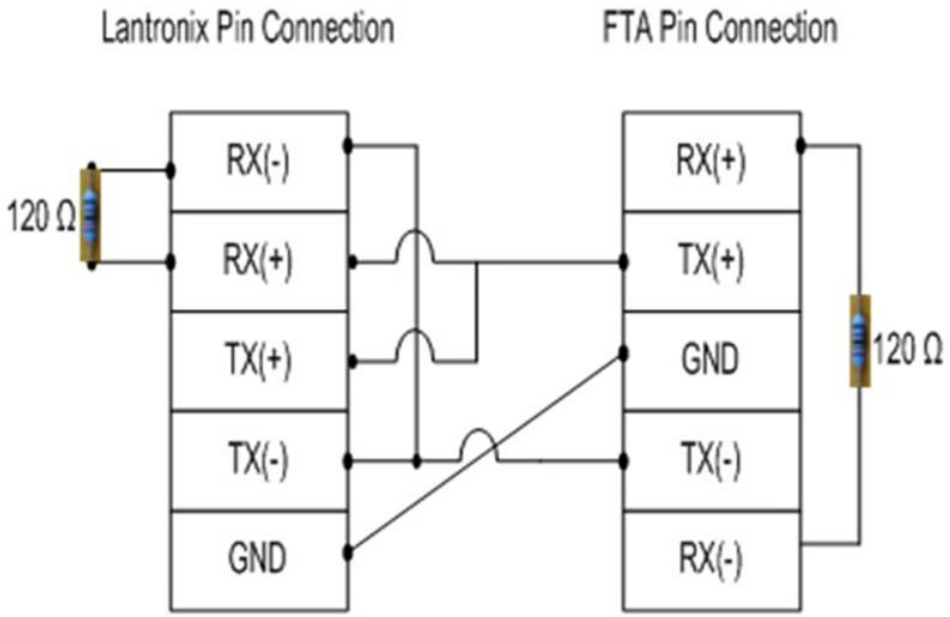


Fig. 17. RS-232– Half Duplex

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

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

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

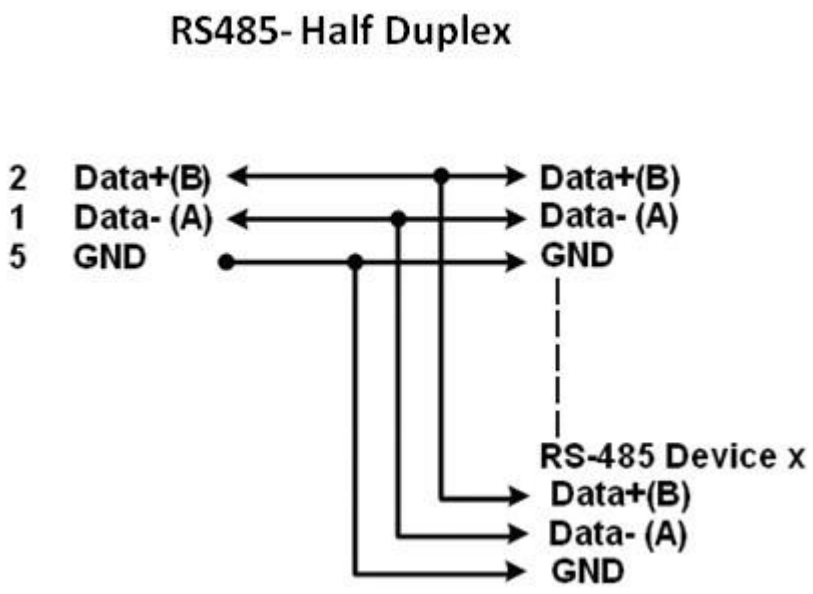


Fig. 19. RS-485 – Half Duplex

Activating HART in OneWireless Network

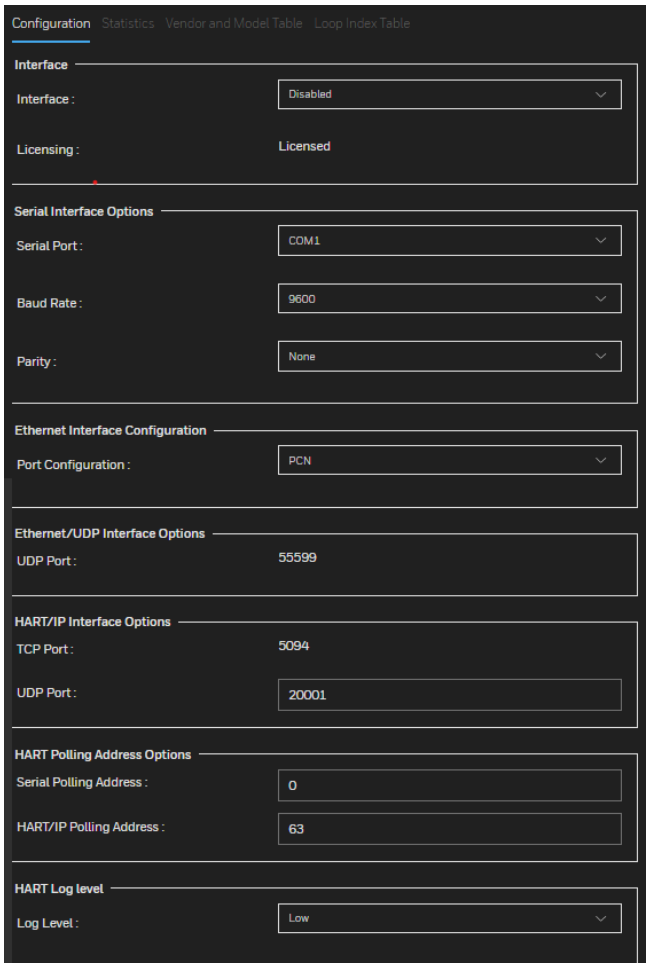
The ISA100 Wireless field devices maintain a database of process configuration, identification, and diagnostic information in memory. WDM allows accessing this information from asset management systems, such as Field Device Manager (FDM), through a HART interface. This enables monitoring the ISA100 Wireless 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.



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.

ATTENTION	**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:

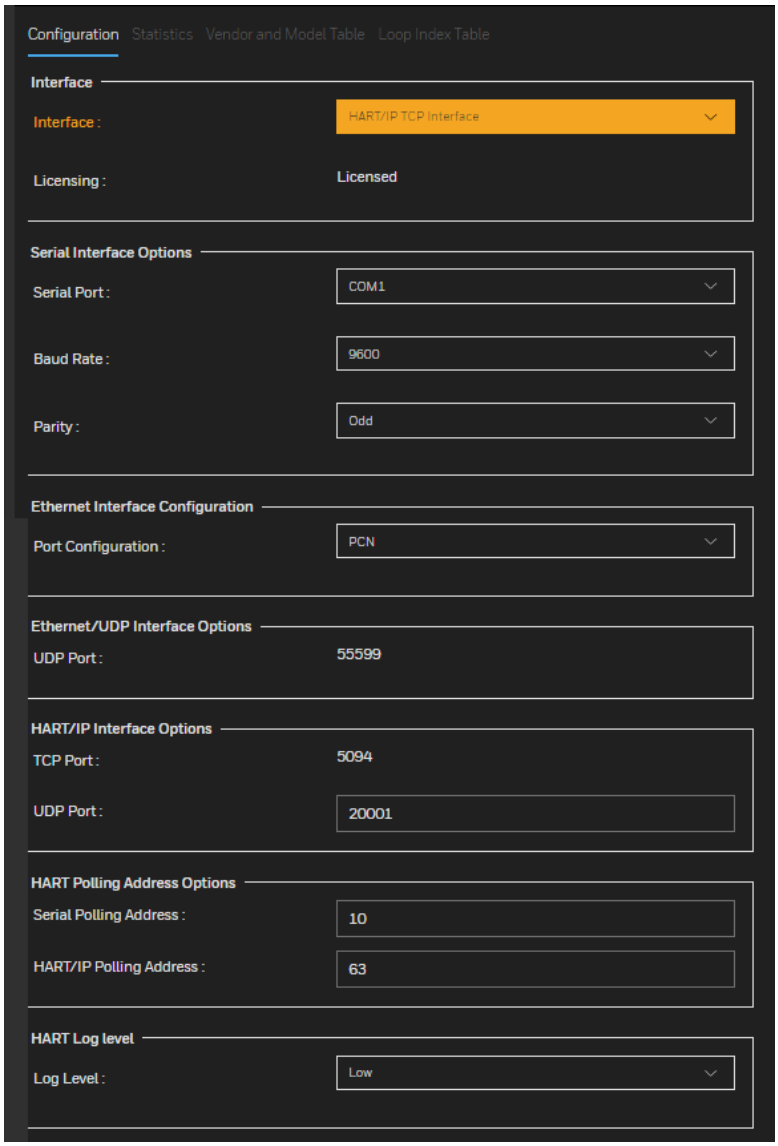
1. From the Start menu, open **Lantronix DeviceInstaller**.

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.



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

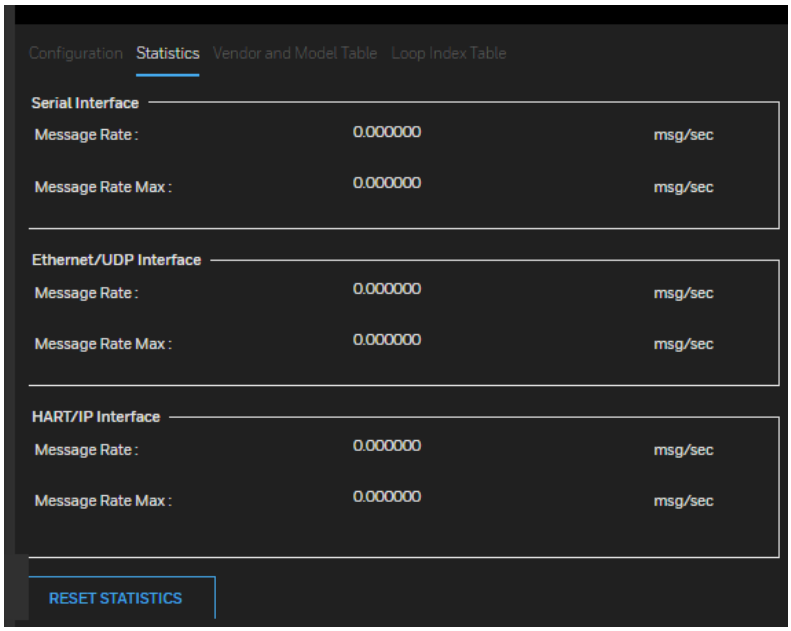
port.

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.



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

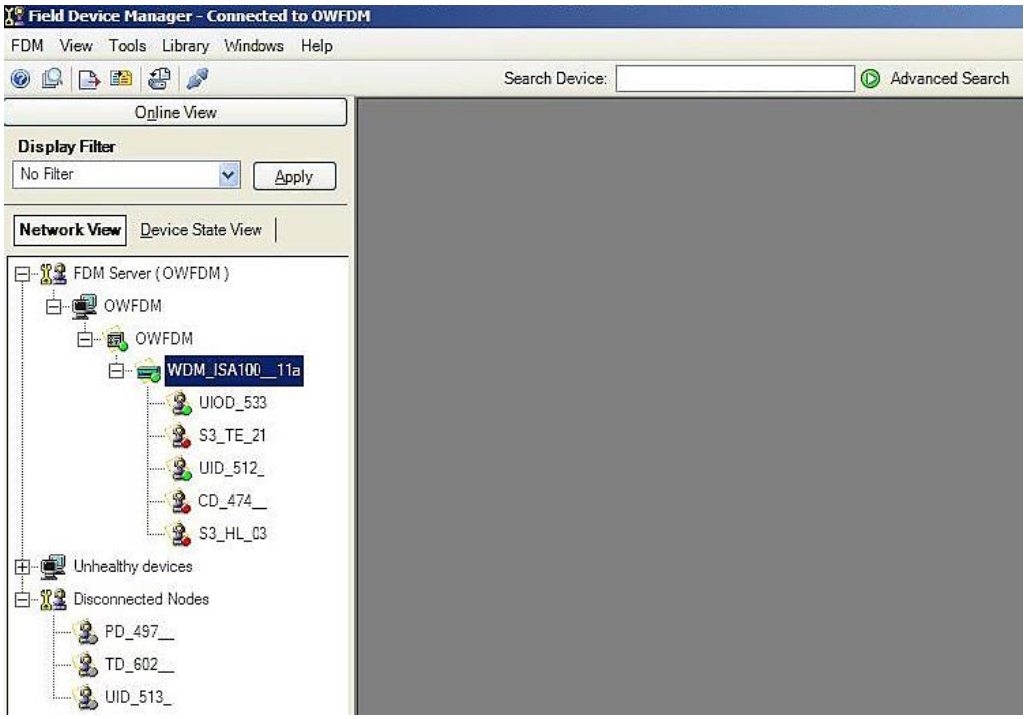
Integration with FDM	Licenses to be enabled in WDM
ISA100 Wireless and wired HART device connected through OWA	GCI+HART
WirelessHART only	WirelessHART
Both ISA100 Wireless and WirelessHART integration	GCI + HART + WirelessHART

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.

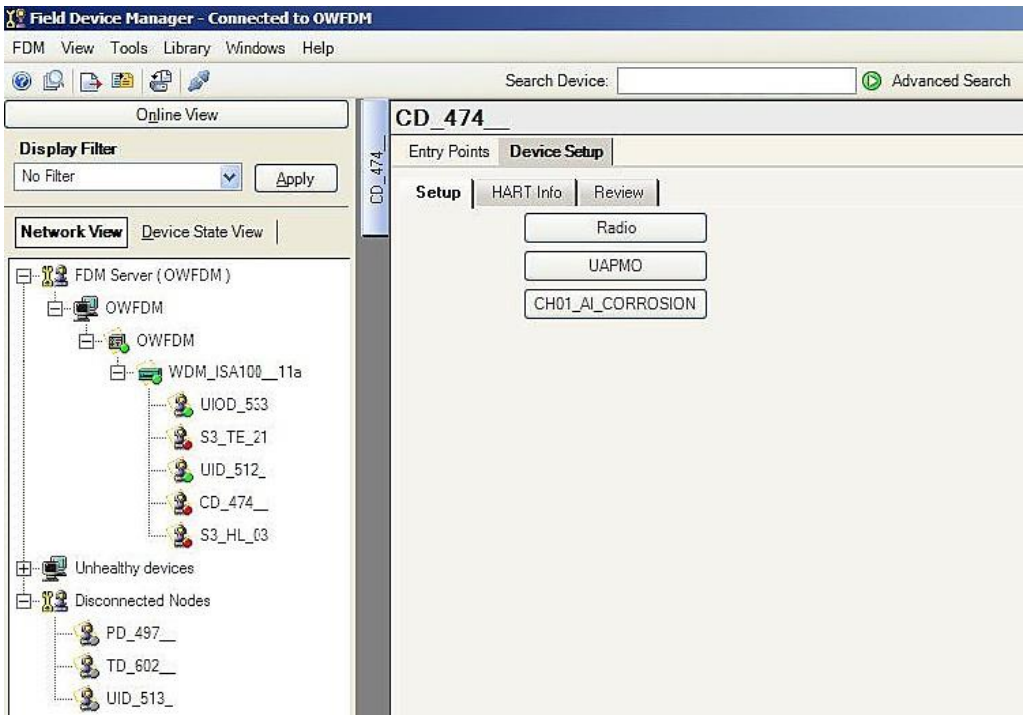
GCI and HART Interface licenses must be enabled in WDM for FDM to detect the wired HART devices connected to OW Adapter.

To access the field devices using FDM via Serial Interface:

1. 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**.
4. 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.



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.



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

1. 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.

ATTENTION	**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.

ATTENTION	**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.

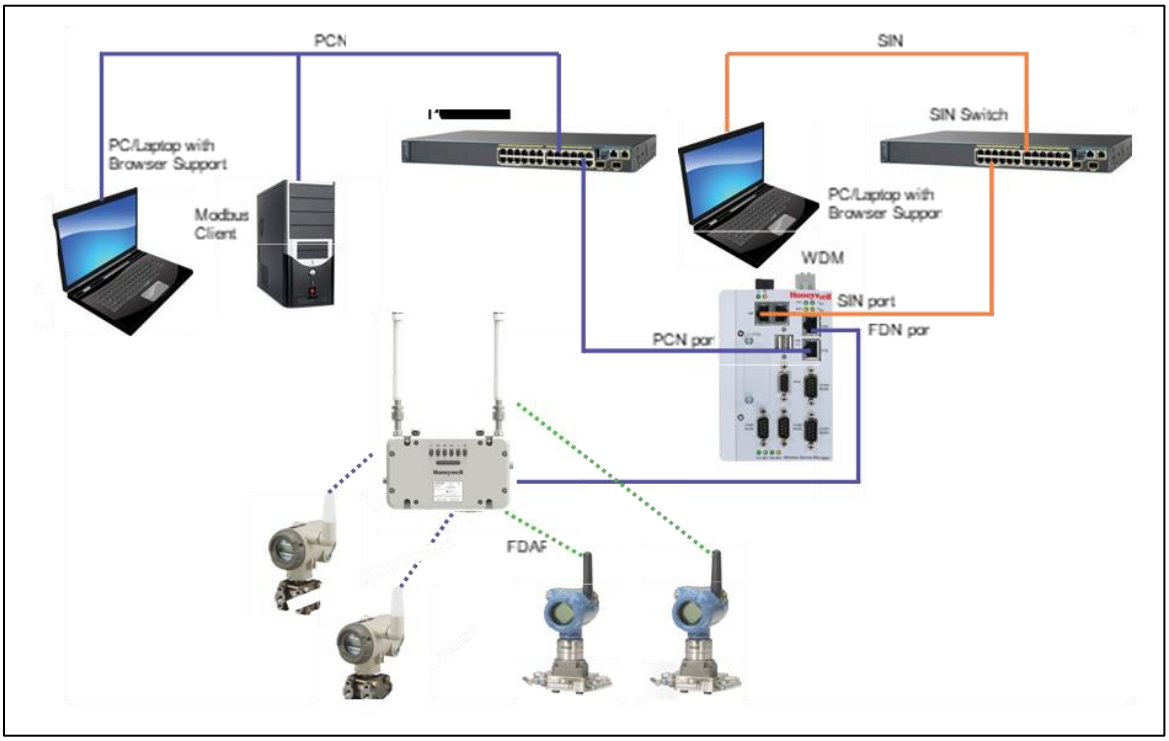


Fig. 20. Modbus TCP communication

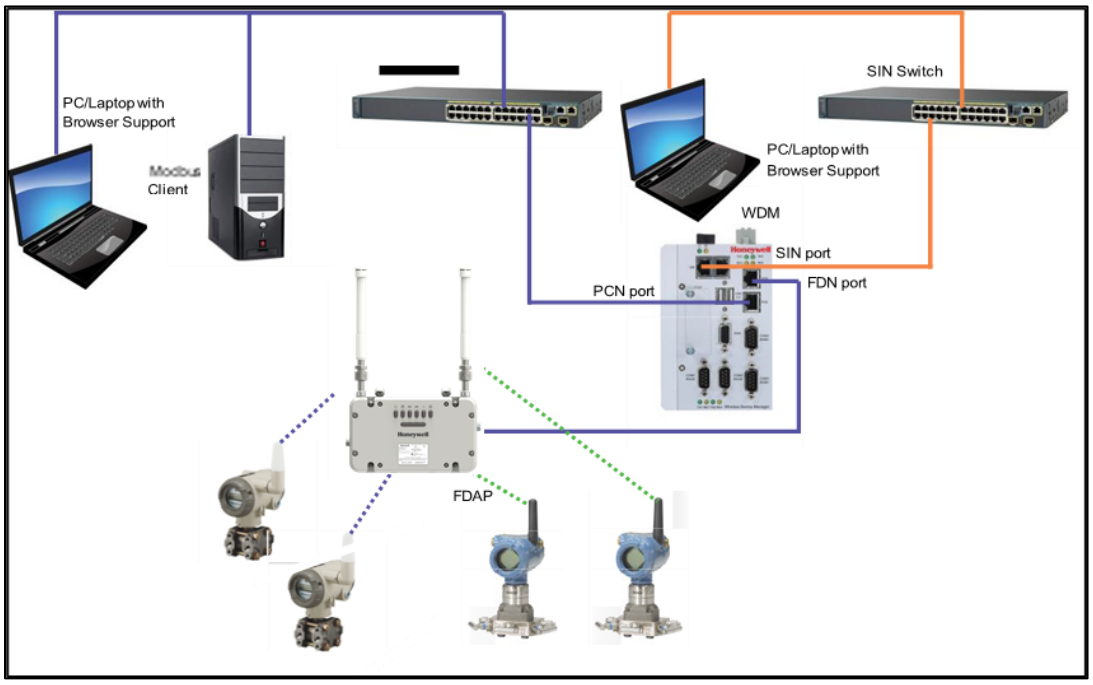


Fig. 21. Modbus RTU communication

Enable Modbus in OneWireless Network

Prerequisites

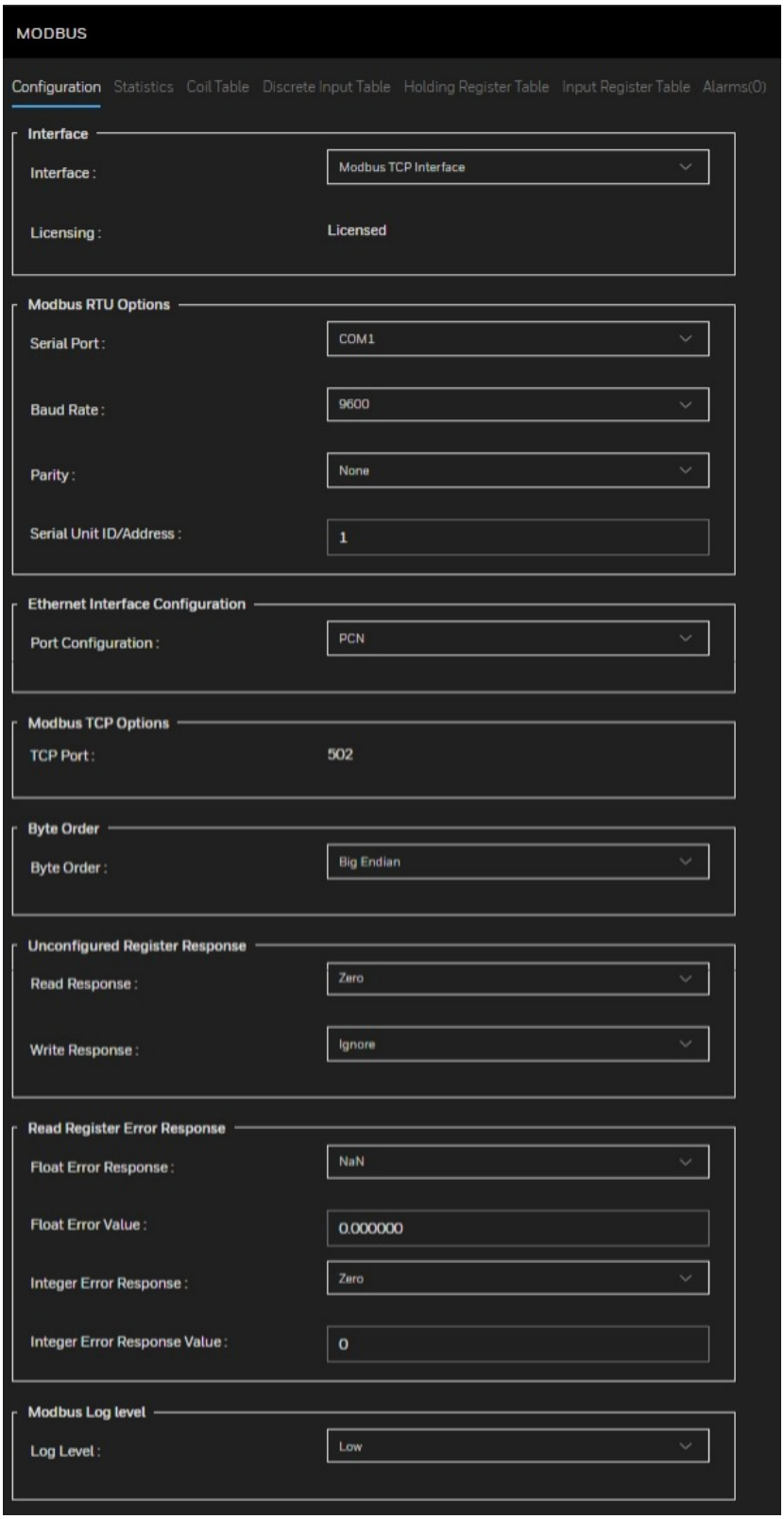
- Ensure that you have installed the Modbus client.

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



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.

8. 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.

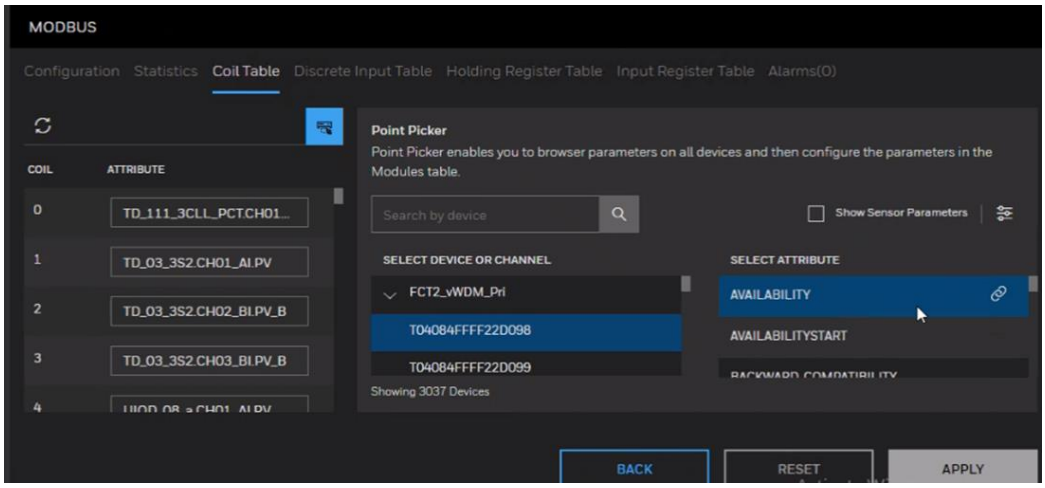


Fig. 22. Coil Table

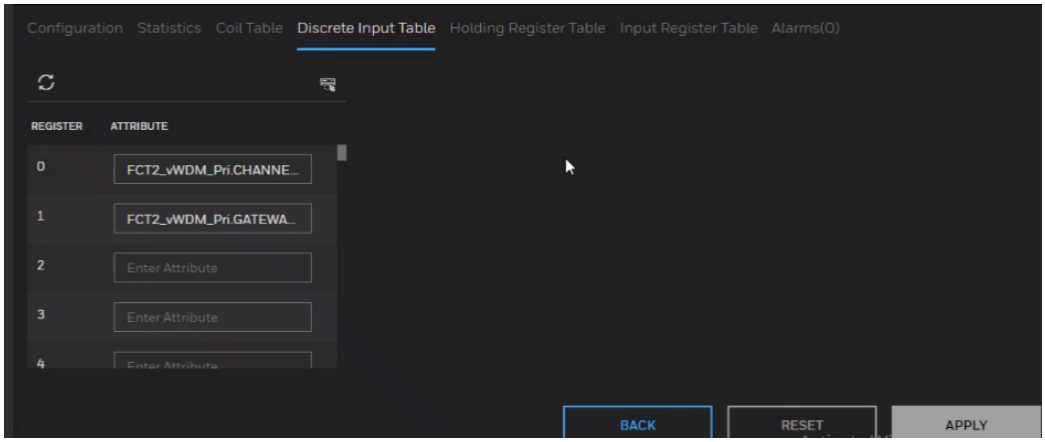


Fig. 23. Discrete Input Table Table

   - **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 - TAGNAME.CHANNELNAME.PV_B
  - 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.

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

Diagnostic status detail	Bits	Diagnostic status detail	Bits
FAILURE_STATUS	BIT31	WCI_RESERVED_15	BIT15
FUNCTION_CHECK_STATUS	BIT30	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

ENVIRON_CONDITIONS_OUT_O F_SPEC	BIT22	RADIO_IPC_ERROR	BIT6
FAULT_PREDICTED	BIT21	HEAP_ERROR	BIT5
POWER_CRITICALLY_LOW	BIT20	DEVICE_FIRMWARE_MISMATCH	BIT4
POWER_LOW	BIT19	WATCHDOG_ERROR	BIT3
SOFTWARE_UPDATE_INCOM PL ETE	BIT18	OUTPUT_AT_FAILSAFE	BIT2
SIMULATION_ACTIVE	BIT17	FW_DOWNLOAD_ERROR	BIT1
WCI_RESERVED_16	BIT16	DETAIL_INFO_AVAILABLE	BIT0

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 devices

Diagnostic status detail	Bits	Diagnostic status detail	Bits
DEV_ST_ELEC_FAIL	BIT0	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	BIT0	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	BIT0	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	BIT0	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	BIT0	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.

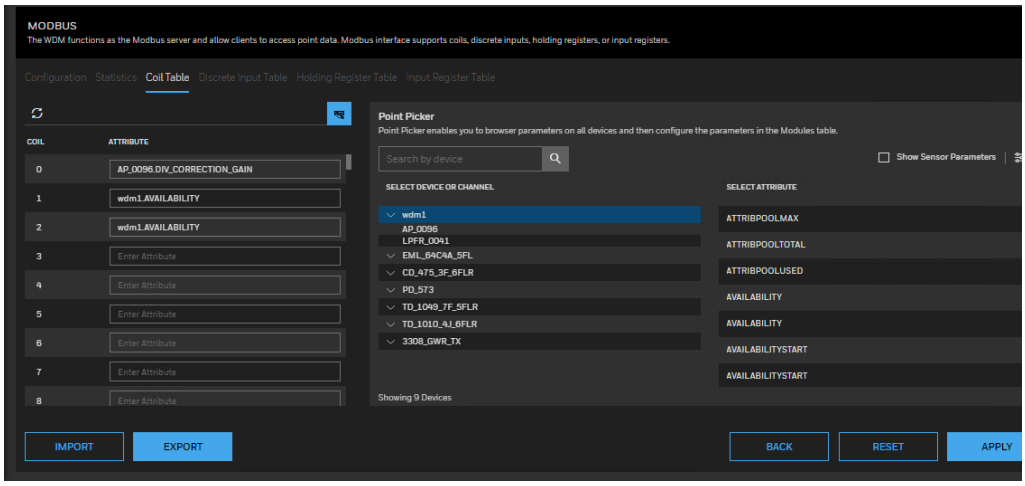
- Under Modbus RTU Interface and Modbus TCP Interface,
  - **Message Count**: Total number of messages processed by the interface. The count must increase with every message sent by a Modbus client. If the count is not incrementing, it indicates that the Modbus interface on the WDM is not receiving messages 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:

1. 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).



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**.

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

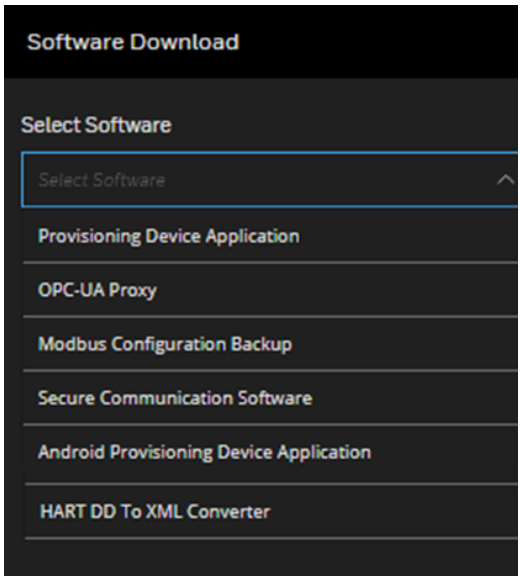
9. Click **Apply**.

ATTENTION	**In the Property Panel, hover the mouse over a parameter, then a tooltip appears with the details about the attribute. Also, this information is displayed in the Point Picker when an attribute is selected.**

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.

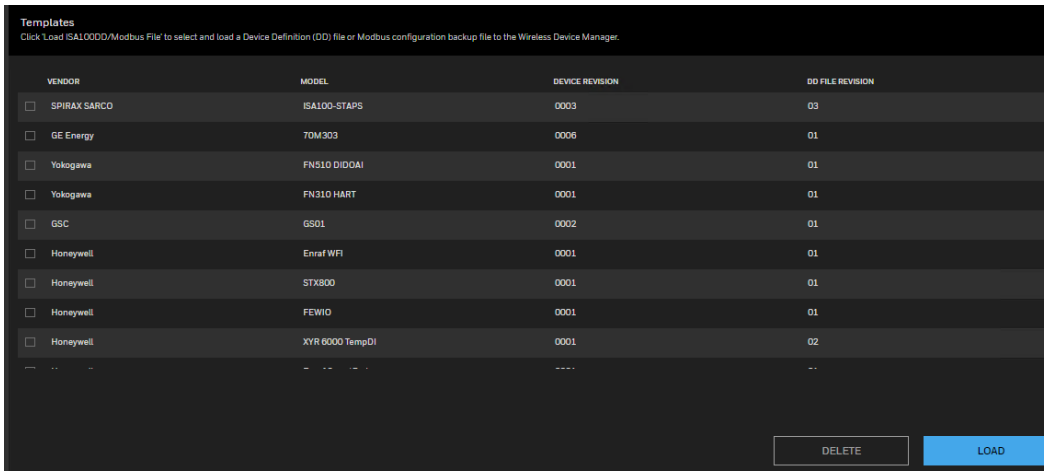


2. From the **Select Software** list, select the **Modbus Configuration Backup**. Click **DOWNLOAD**.
3. Click **GO TO DASHBOARD** after downloading the software.

To import Modbus register configuration:

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

   The **Templates** window appears.



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

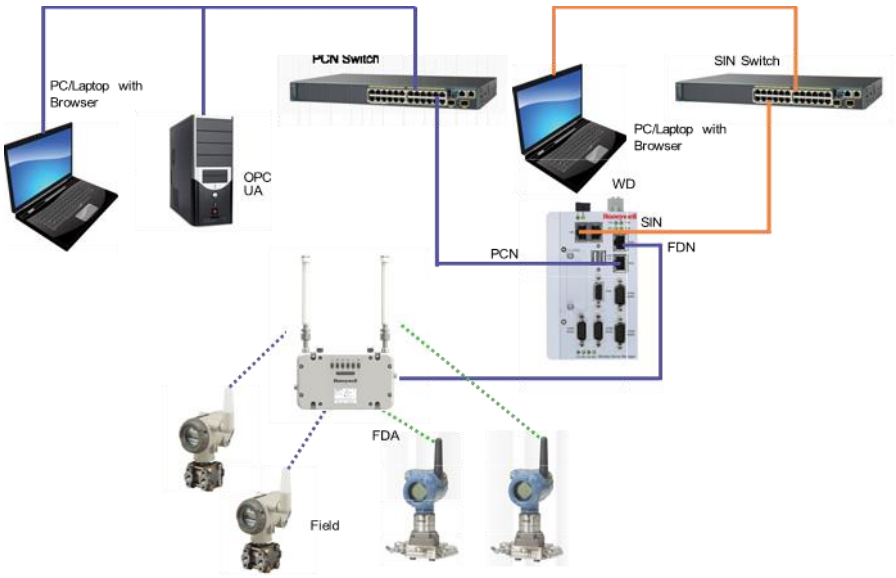


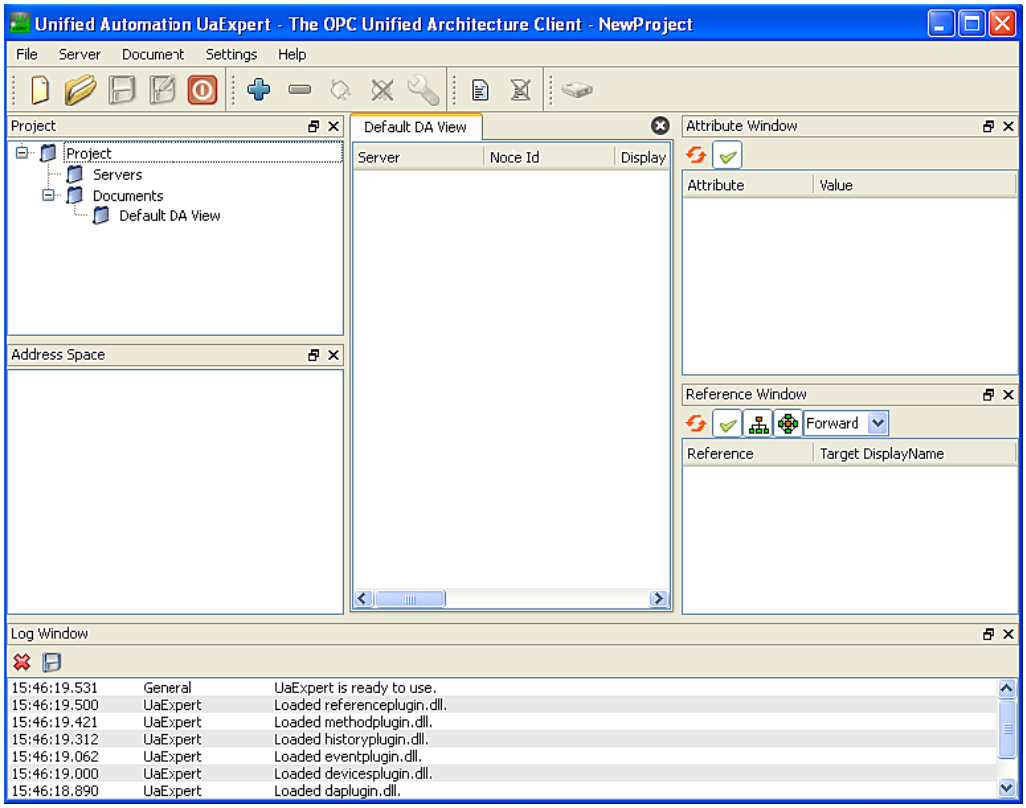
Fig. 24. OPC Interface

Prerequisites

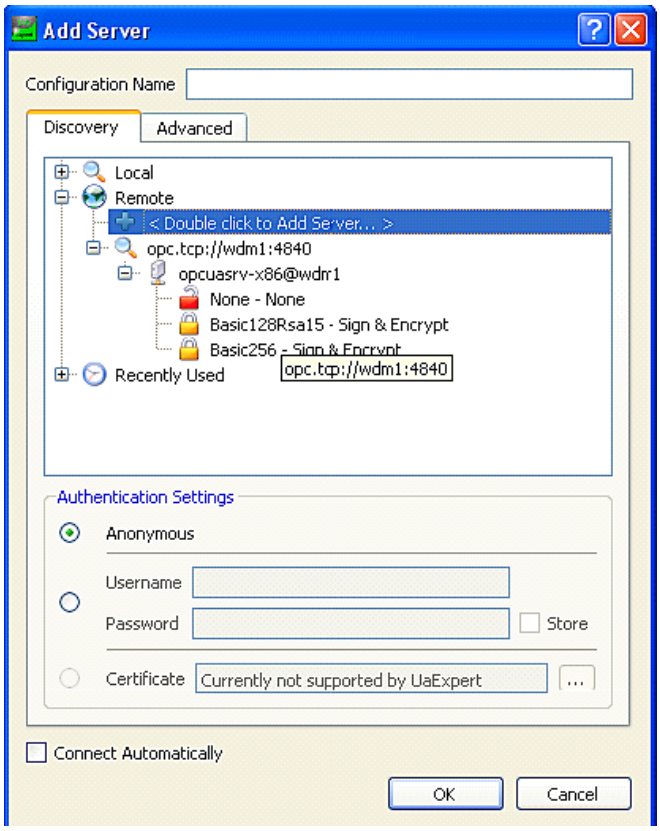
- Install Microsoft .NET Framework 3.5 SP1 and OPC UaExpert Client in the client system.

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.

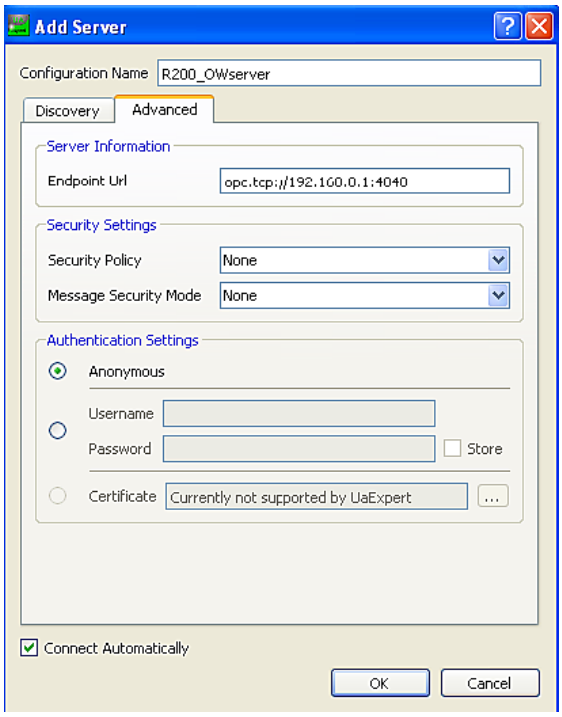


2. On the **Server** menu, click **Add** to add the OPC server to be connected to the client. The **Add Server** dialog box appears.
3. Type the Configuration Name.



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.

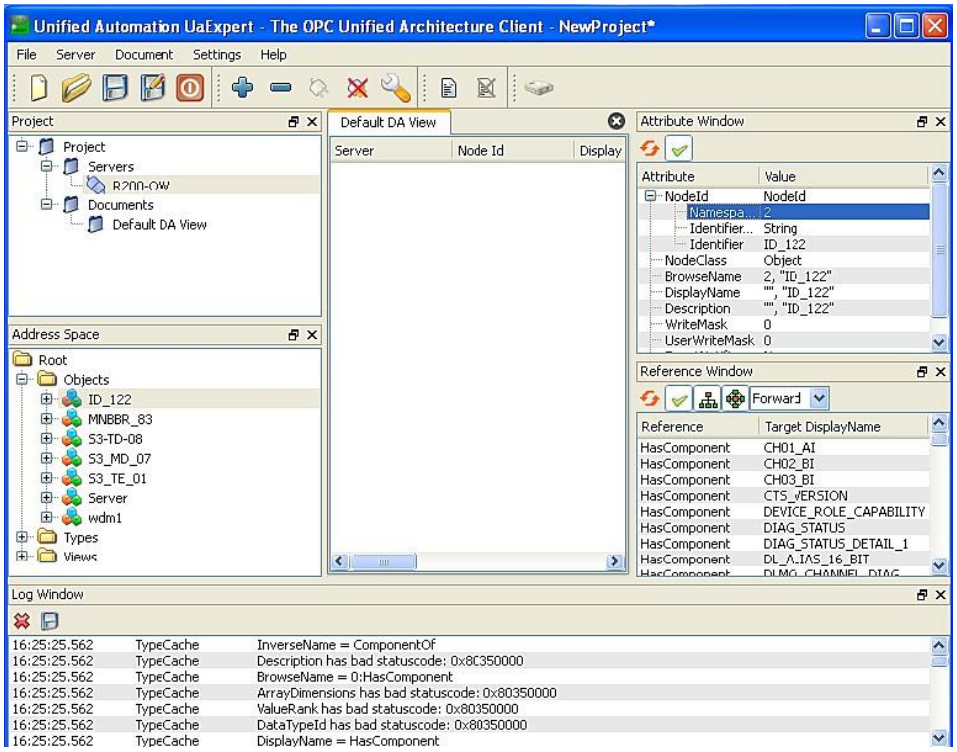
   The OPC server IP address with port number is opc.tcp://WDM IP address: 4840. For example, if the WDM IP address is 192.168.1.1, then type, opc.tcp://192.168.1.1:4840.
6. Under **Security Settings**, ensure that **Security Policy** and **Message Security Mode** are selected as **None**. There is only 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.



9. Click **OK** and the server automatically connects.

   The OPC server appears as connected under **Projects** > **Servers**.

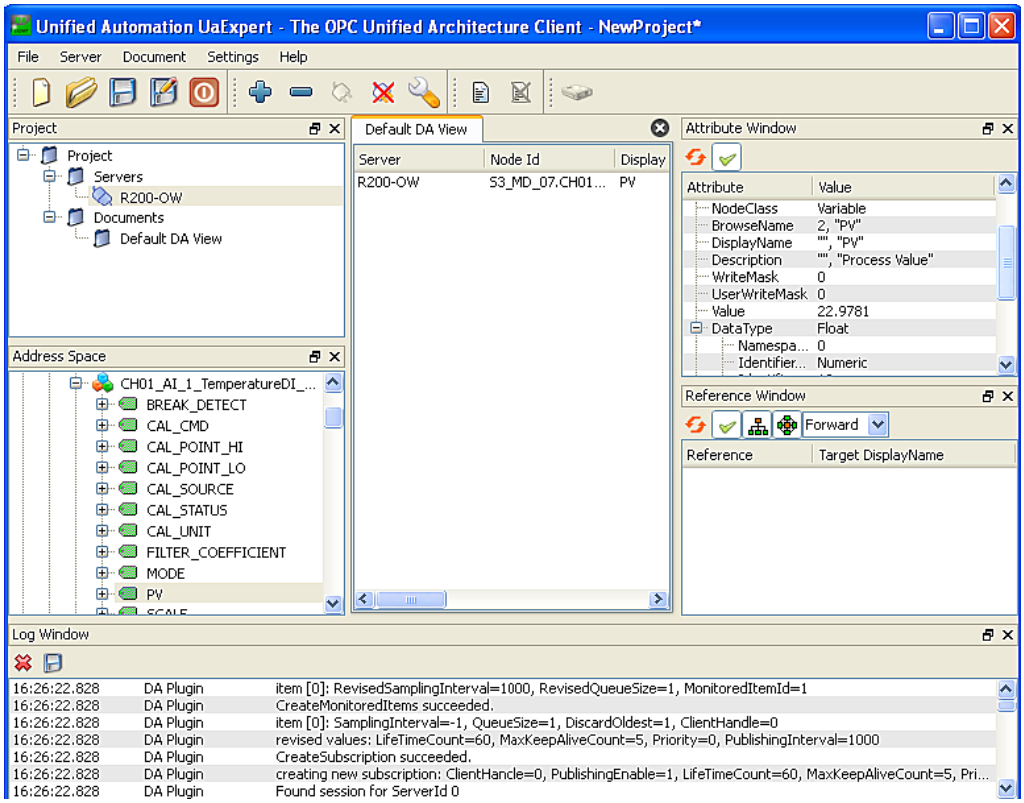
10. Under **Projects**, expand **Project** > **Server** and select the added server.



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.



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.

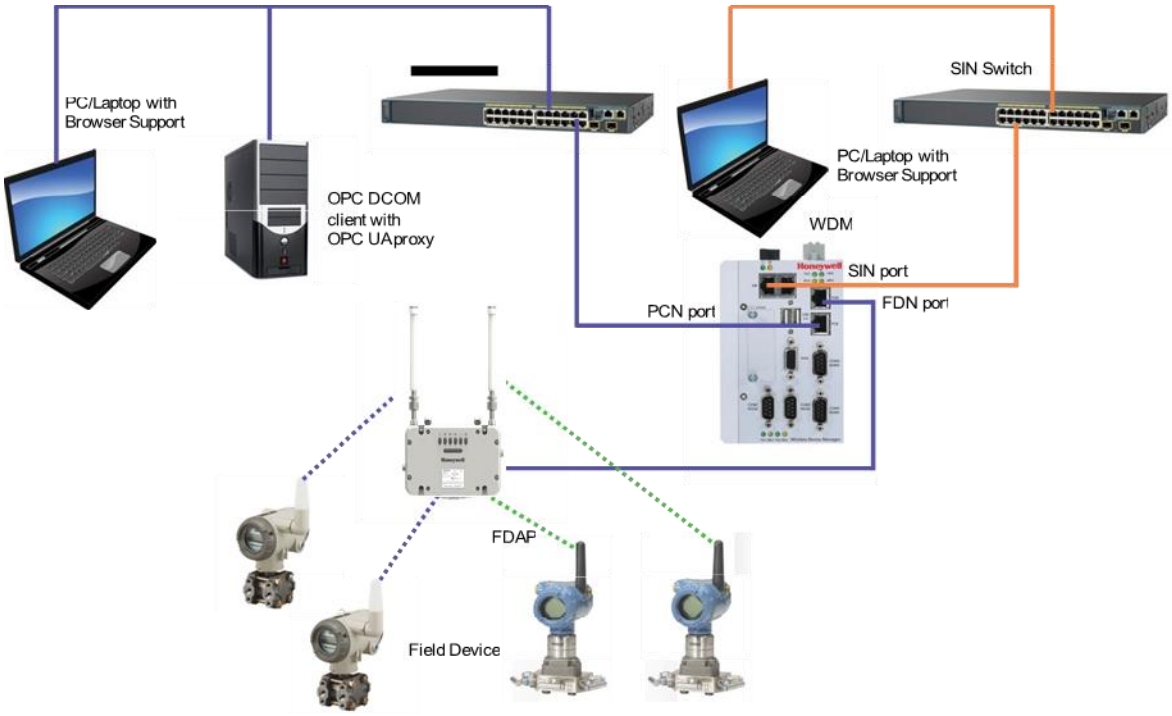


Fig. 25. OPC client with OPC DA

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

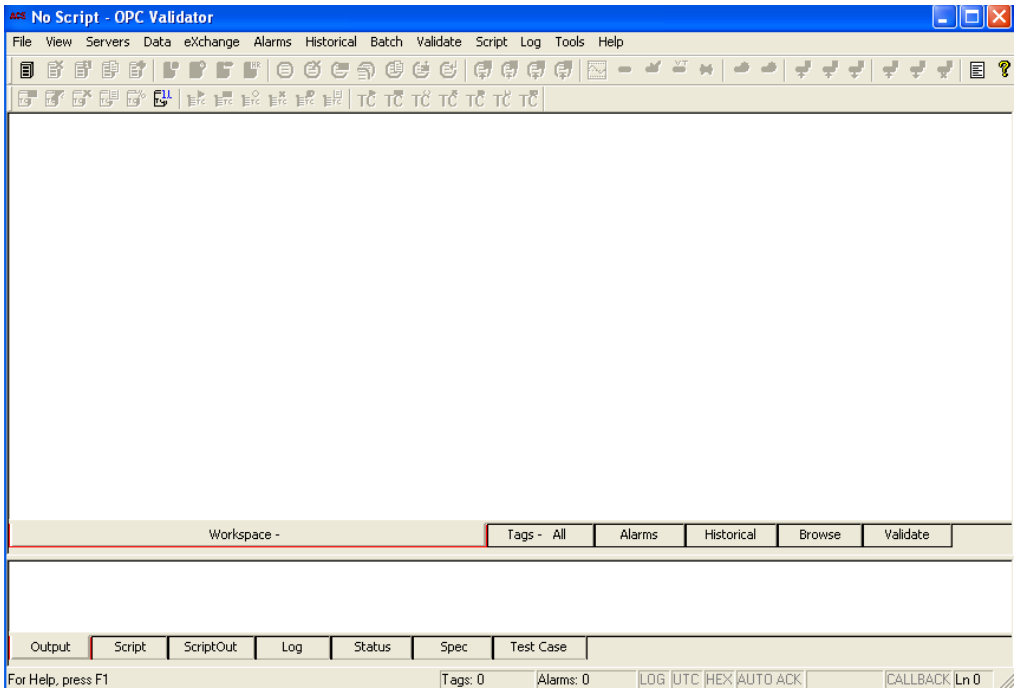
1. From the Left Navigation Menu bar, click **SYSTEM > SOFTWARE DOWNLOAD.** The Support Software window appears
2. From the **Select Software** list, select the **OPC UA Proxy** software.
3. Click **Download** to download the software to the computer.
4. Open the installer and click **Run**.

   The **InstallShield** wizard appears.

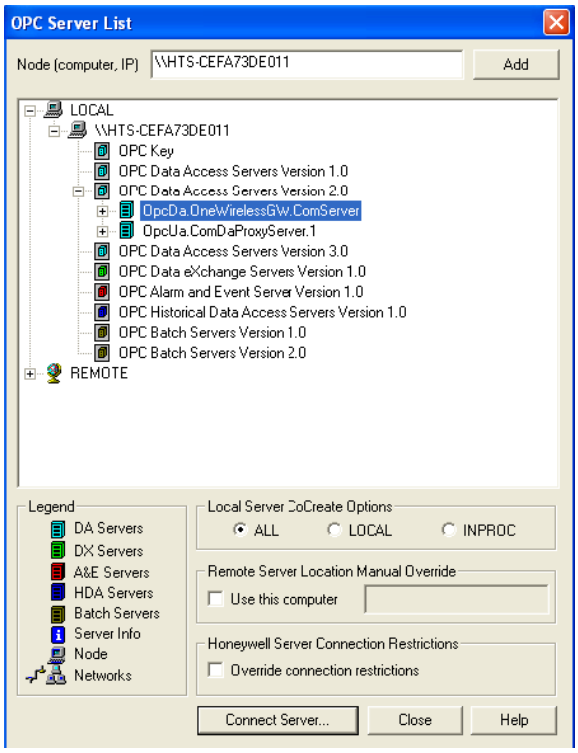
5. Click **Next** to proceed with the installation. The **License Agreement** page appears.
6. Click **I accept the terms in the license agreement** and click **Next**. The **Customer Information** page appears.
7. Enter the **User Name** and **Organization** and click **Next**. The **Setup Type** page 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

1. On the desktop of the client system, double-click **OPC Validator** icon. The **OPC Validator** window appears.



2. Click **Servers** > **Connect to Server (Listing)**. The **OPC Server List** dialog box appears.

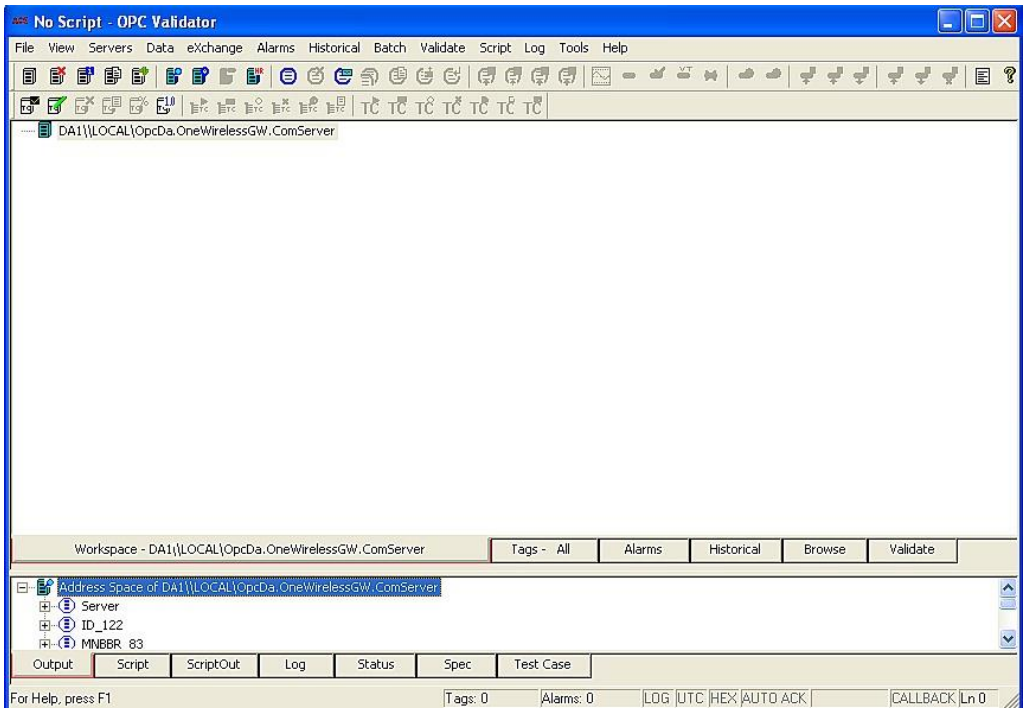


3. Double-click the **OPC DataAccess Servers Version 2.0** and select **OpcDa.OneWirelessGW.ComServer** from the list, and then click **Connect Server...**.

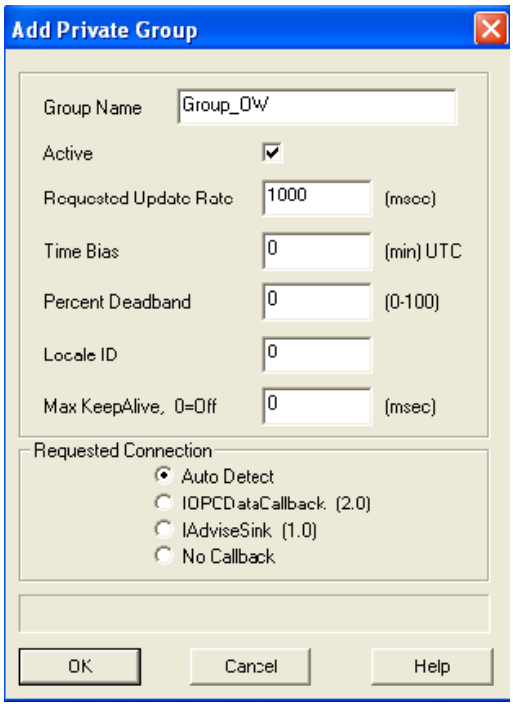
4. Once the server is connected, click **Close**. The **OPC Server List** dialog box closes.

5. In the OPC Validator window, select **OpcDa.OneWirelessGW.ComServer**.

6. Click **Data** > **Browse Server Address Space**, and then click **Browse Server Address Space All**. The Address Space appears on the lower pane.



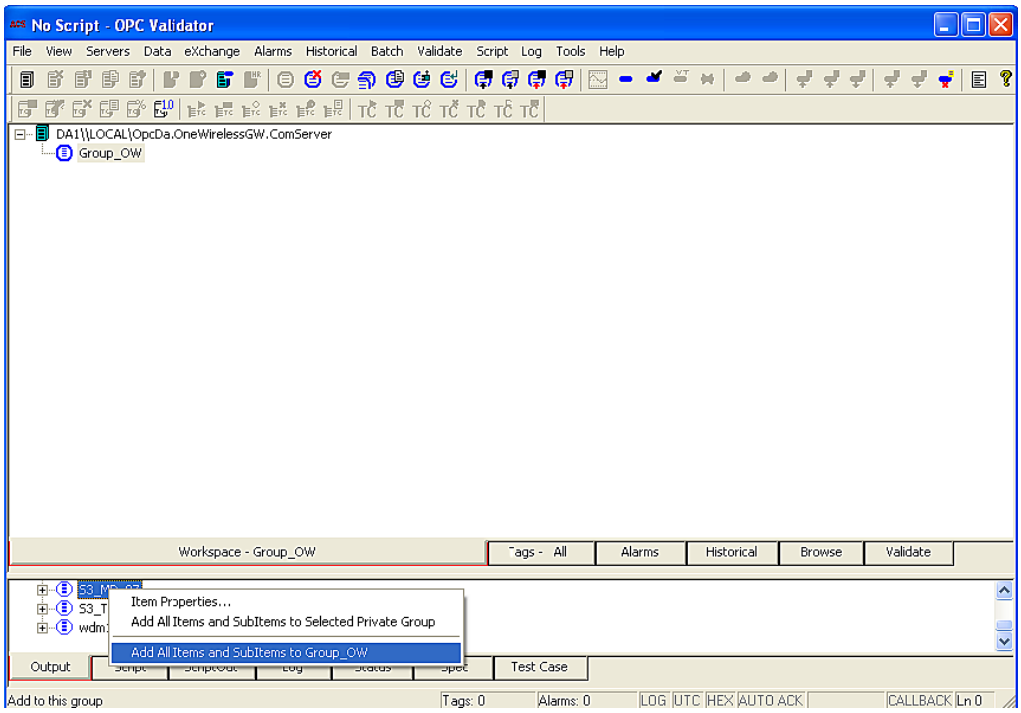
7. In the upper pane, right-click **OpcDa.OneWirelessGW.ComServer**, and then click **Add Private Group**. The **Add Private Group** dialog box appears.



8. Type the **Group Name**, and then click **OK**.

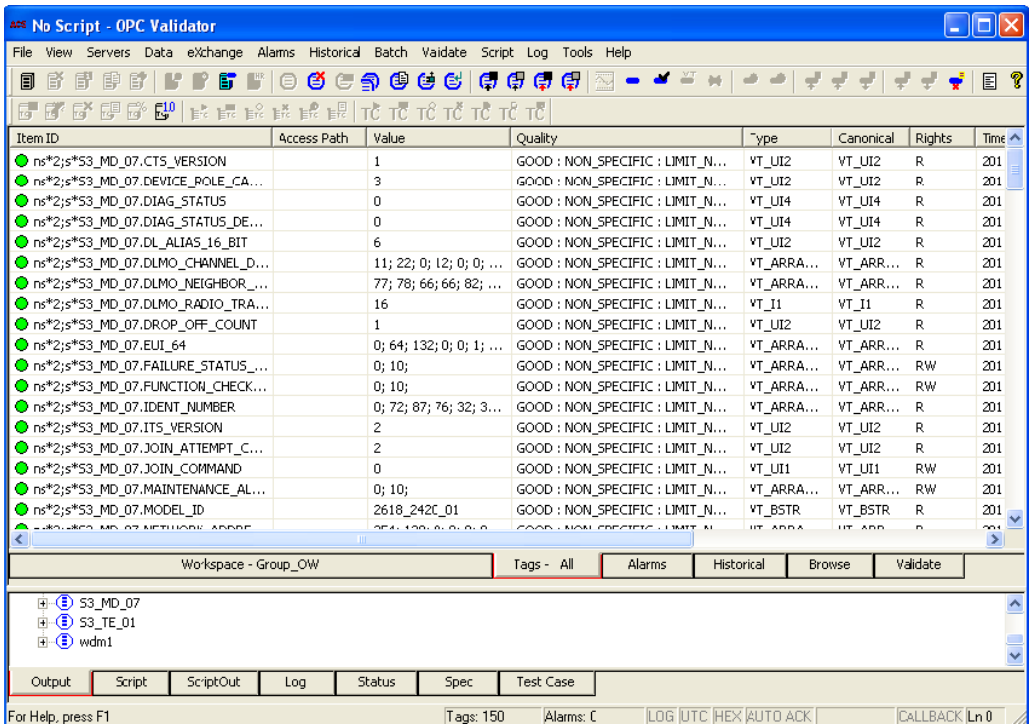
9. From the lower pane of the **OPC Validator** window, select the OneWireless Network, and then a device.

10. To add all the parameters of a device, right-click on the device and click **Add All Items and SubItems to Group_OW**.



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.



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.

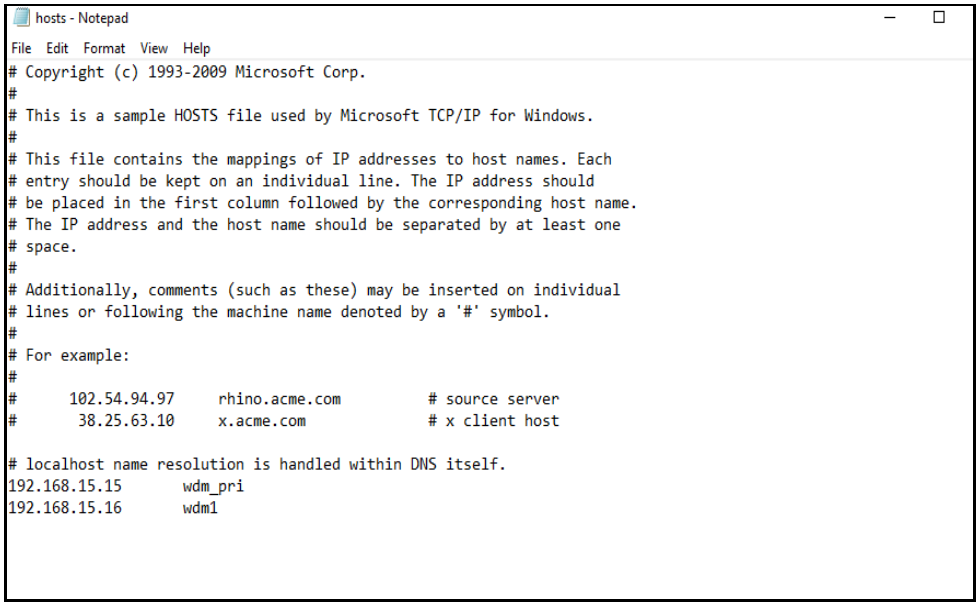
c. In the **Raw** field, type the required value. You can only edit the mode for all the device types and the output value of the Multi AI DI DO devices.

d. Click **OK**.

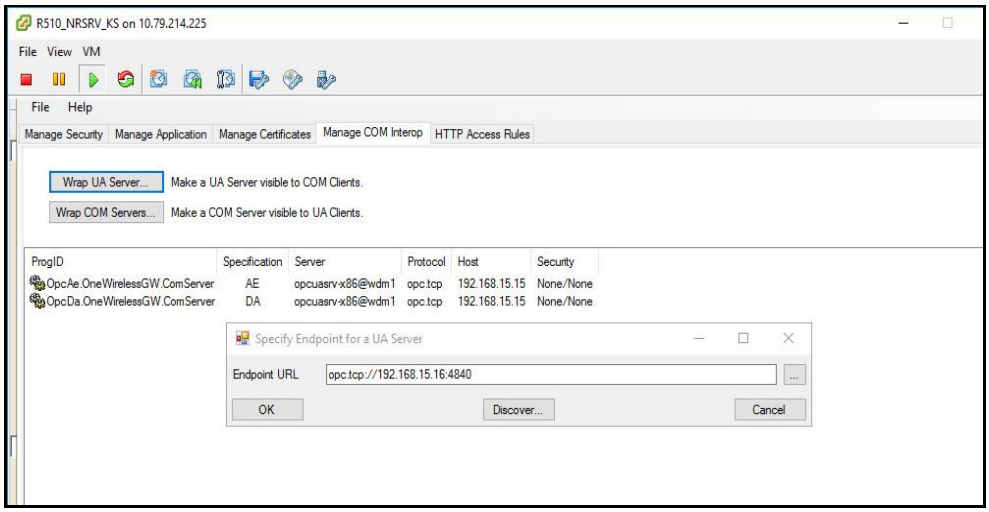
Configuring OPC communication using Experion SCADA and OPC Validator with multiple WDMs in the same network

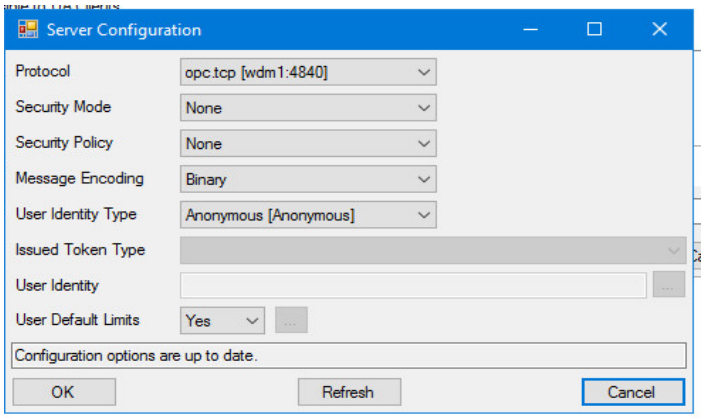
With Experion SCADA

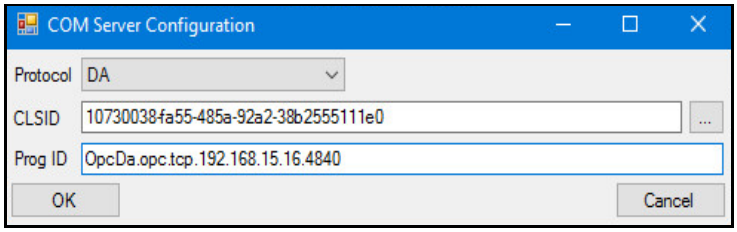
1. In the Experion SCADA Machine, edit the HOSTS File with multiple WDMs hostnames.

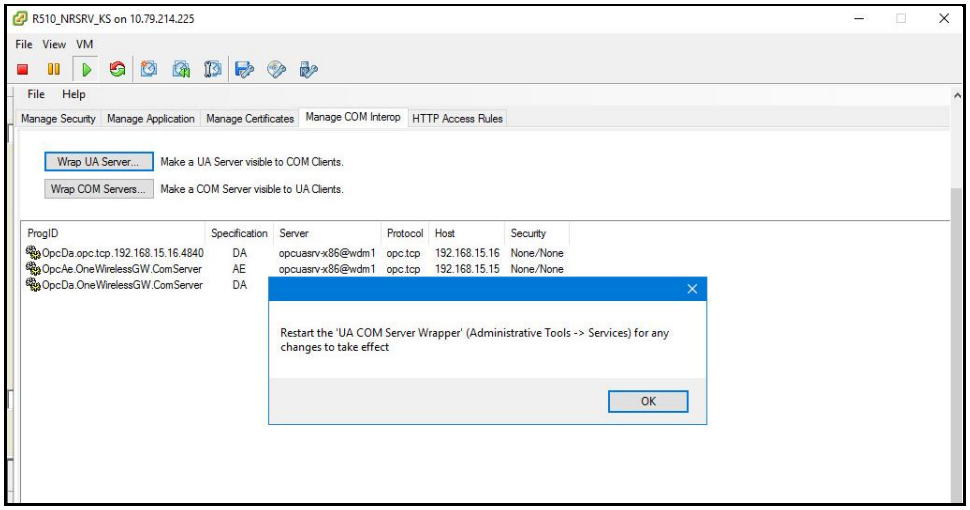


2. Configure UA Server COM Proxies for multiple WDMs (PCN IP address of WDMs).



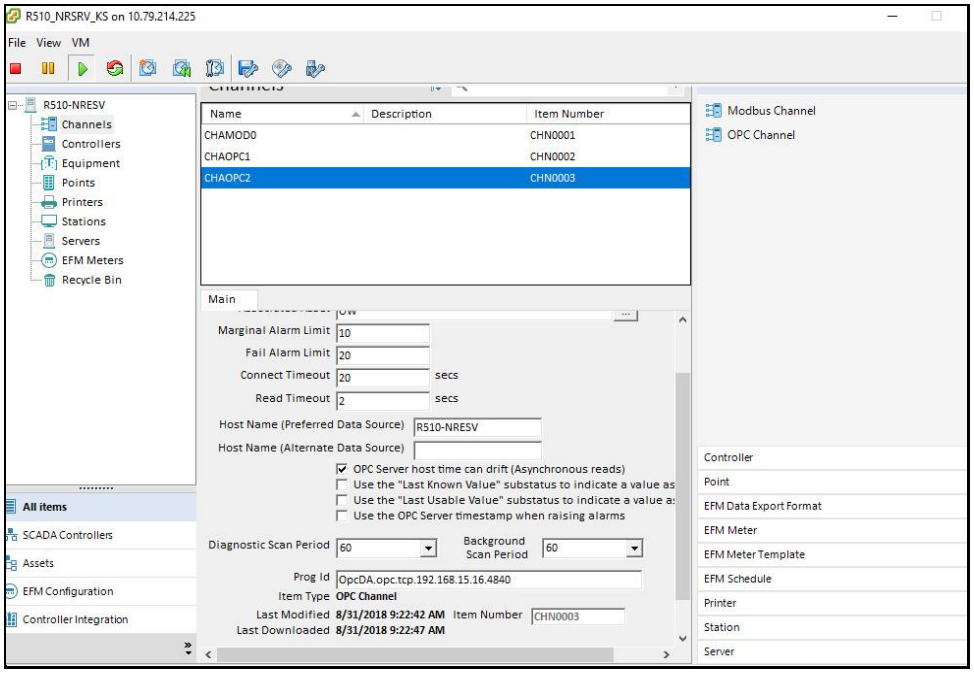




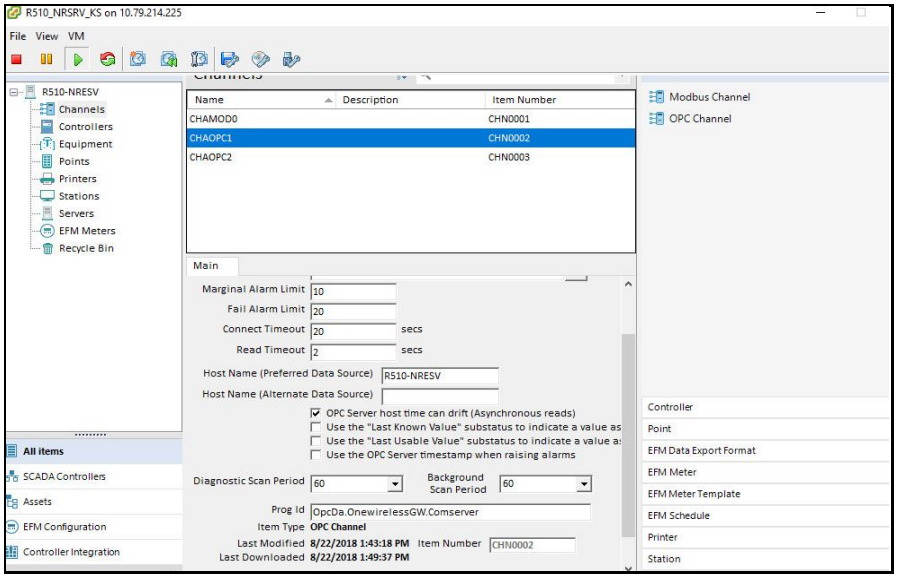


Restart the UA COM Server Wrapper service using services.msc.

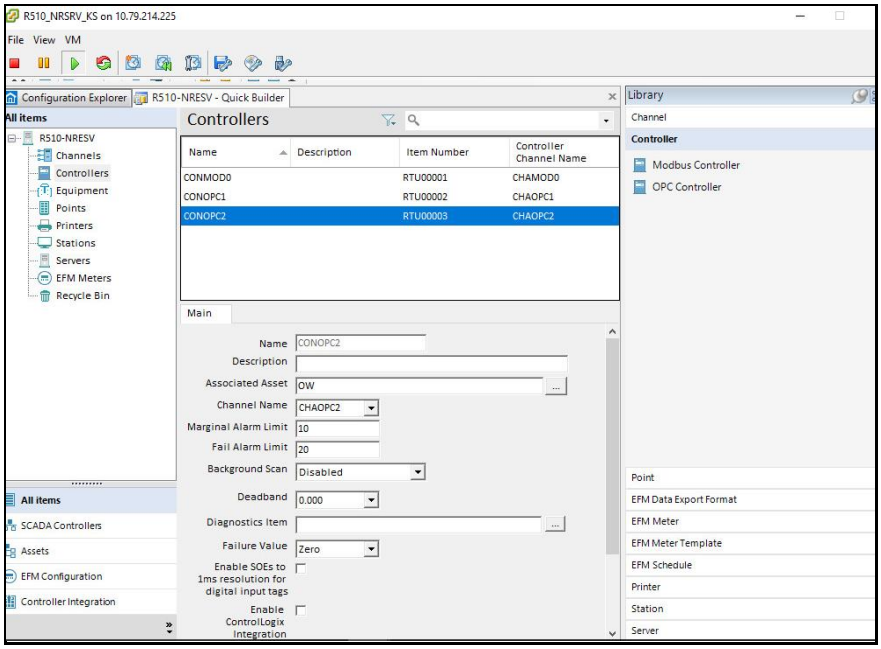
3. Configuring OPC Channels, OPC Controllers, Analog Points in Experion Quick Builder.



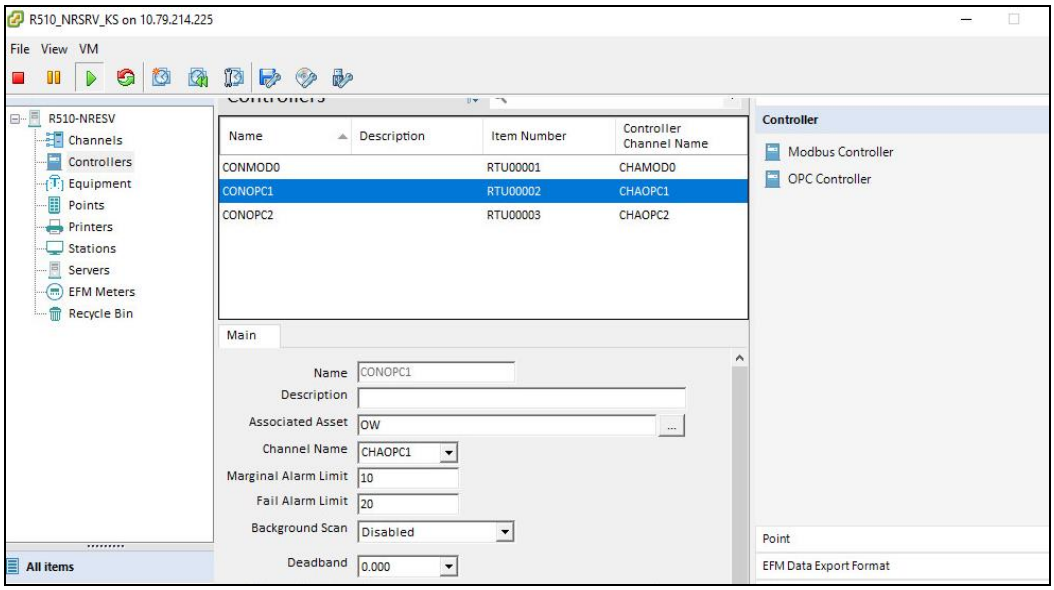
OPC Channel for wdm1 with ProgID: OpcDA.opc.tcp.192.168.15.16.4840



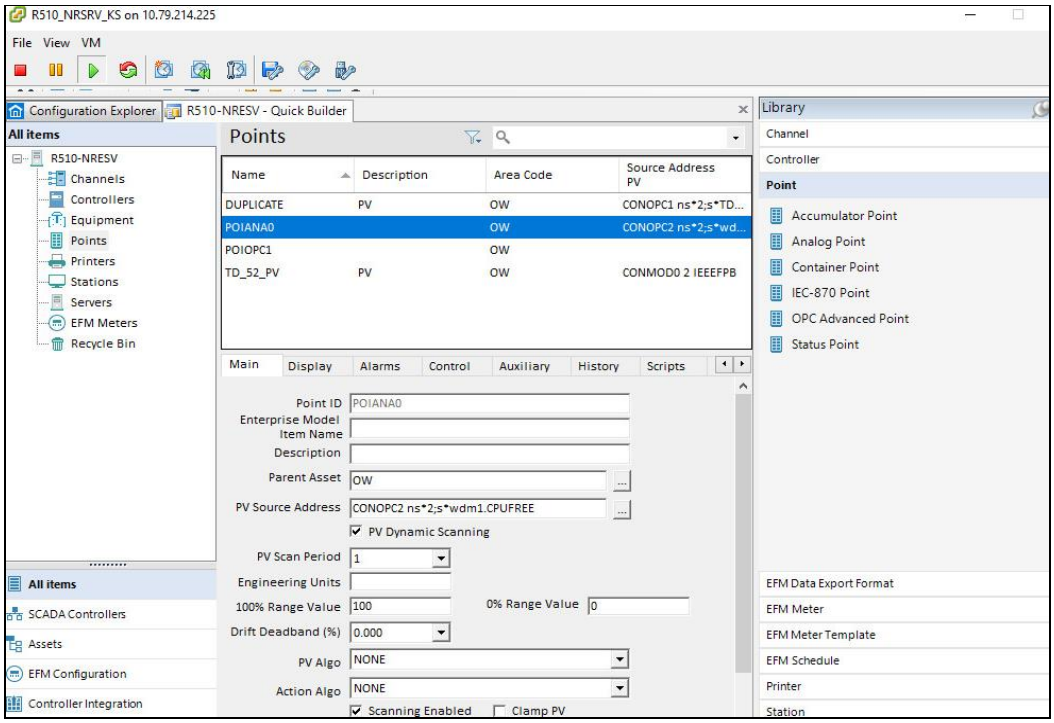
OPC Channel for wdm_pri with ProgID: OpcDA.OneWirelessGW.Comserver



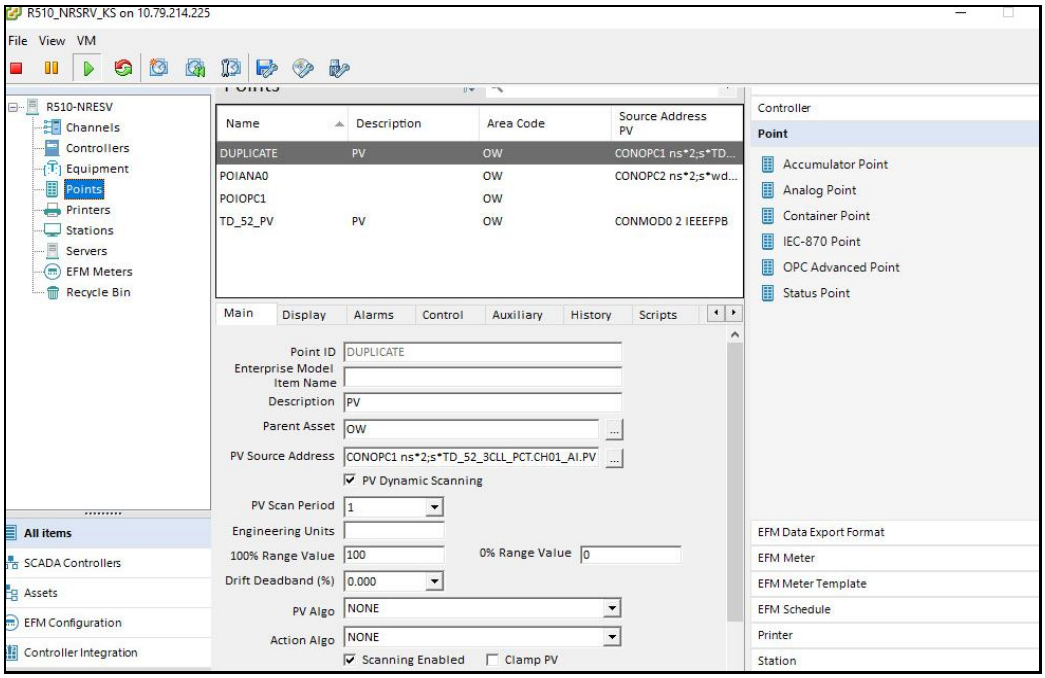
OPC Controller for wdm1



OPC Controller for wdm_Pri



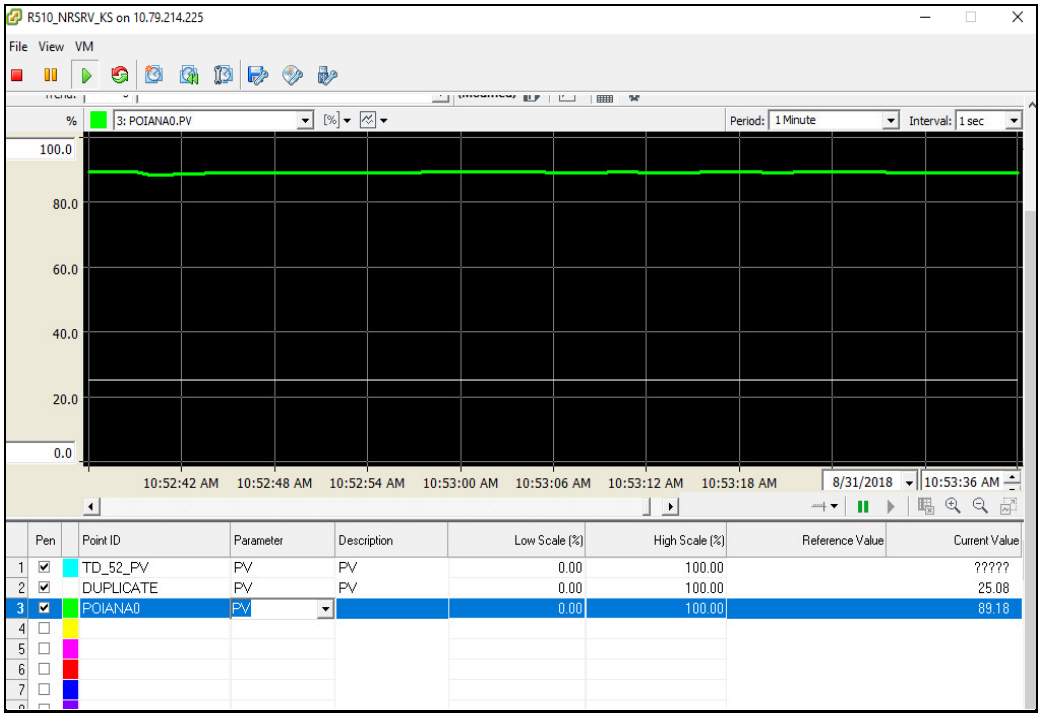
Analog Point for wdm1



Analog Point for wdm_pri

Enable OPC Controllers and OPC channels from station

Launch the trend to display the values



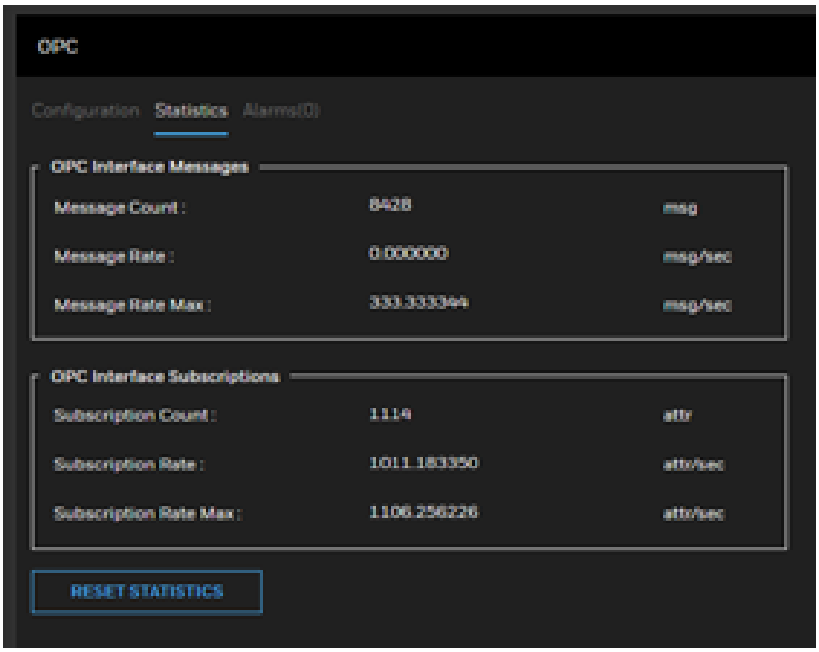
Values from 2 different WDMs visible in Experion SCADA in same Experion Server.

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.

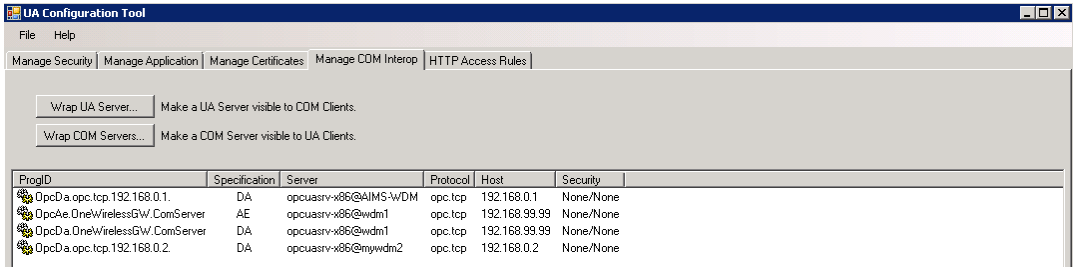


4. Click **Reset Statistics** to reset all the OPC interface statistics.

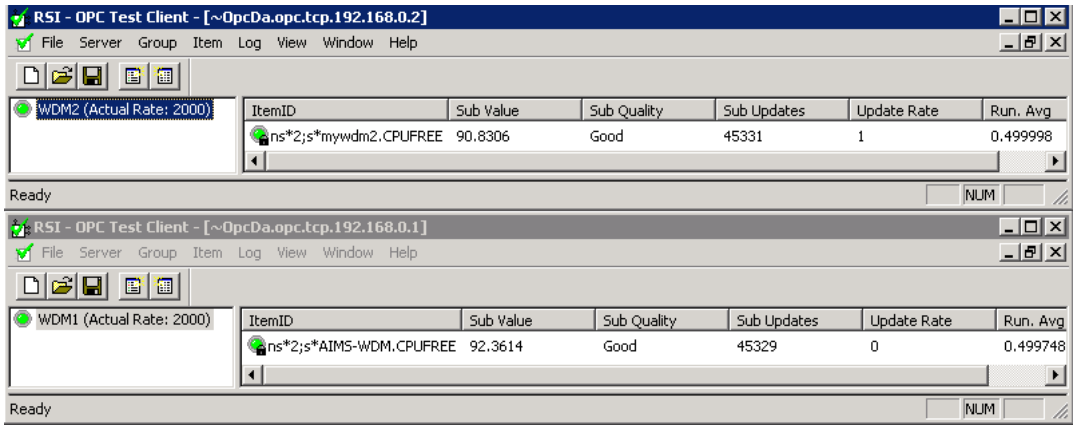
Monitor OPC interface for multiple WDMs

To monitor OPC interface for multiple WDMs:

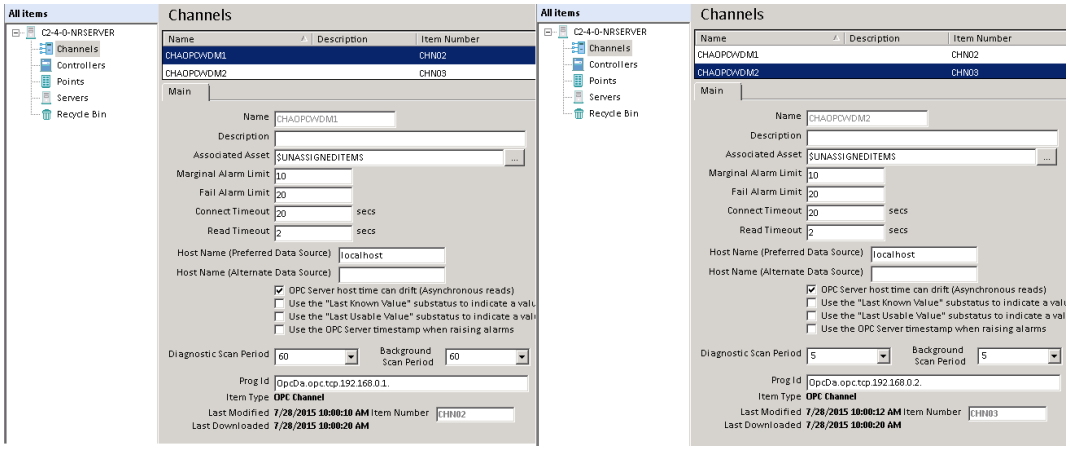
1. Download and install OneWireless UA proxy software. During the installation enter the Host ID and then complete the installation.
2. Open OPC UA configuration tool. Click Manage COM Interop and select Wrap UA Server.



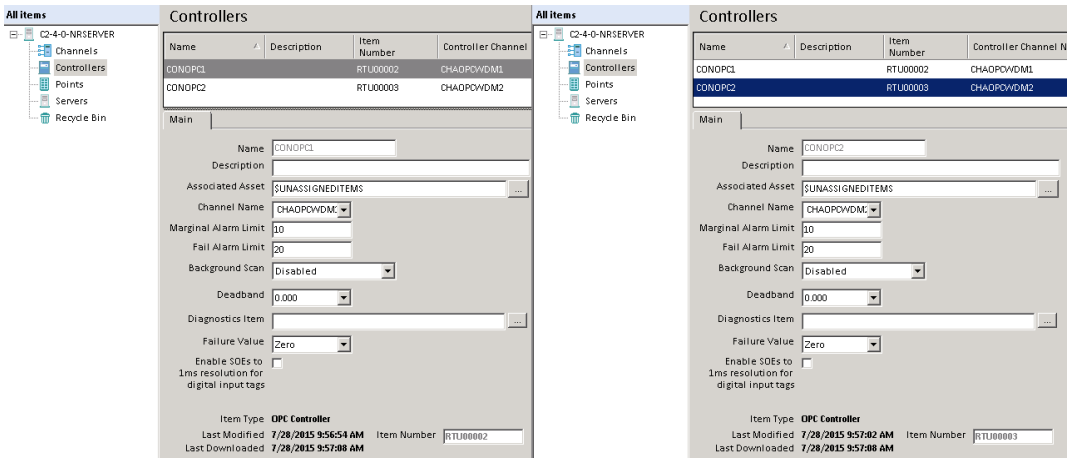
3. Test UA Server COM proxies.



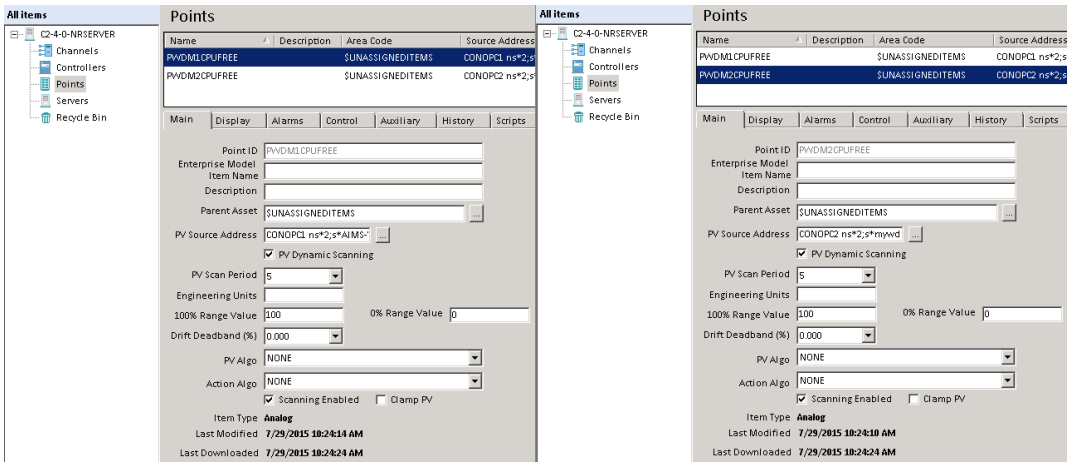
4. Configure Channels using COM proxies.



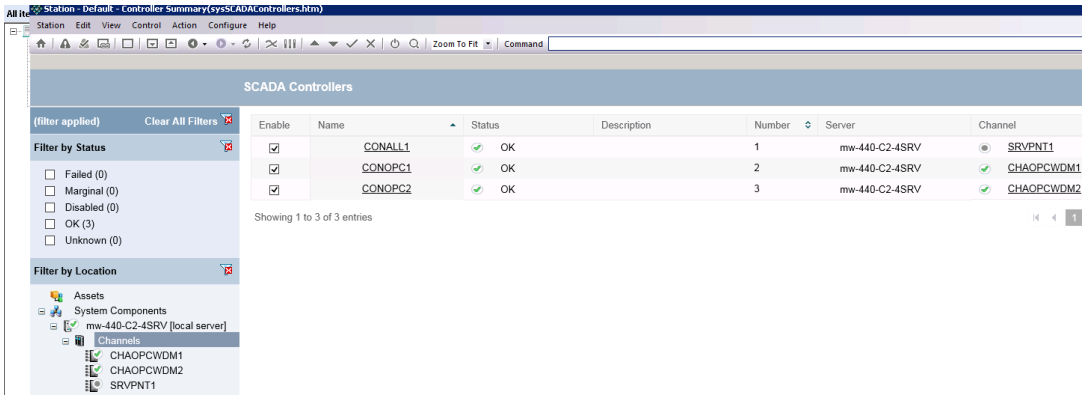
5. Configure Controllers using Channels.



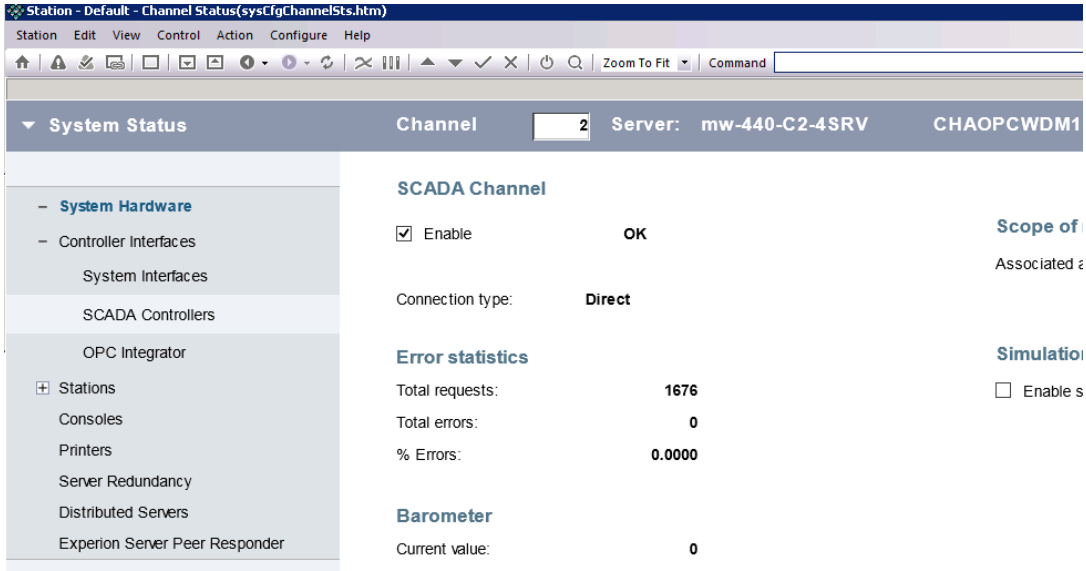
6. Configure Points using Controllers and OPC Access Path (PV Source Address).



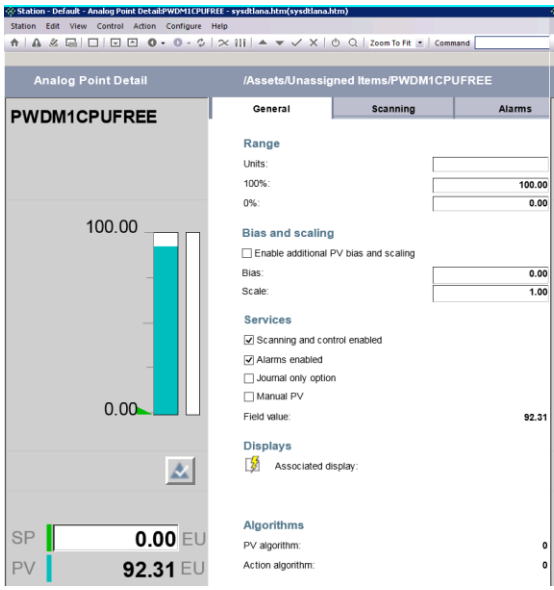
7. Enable controllers:

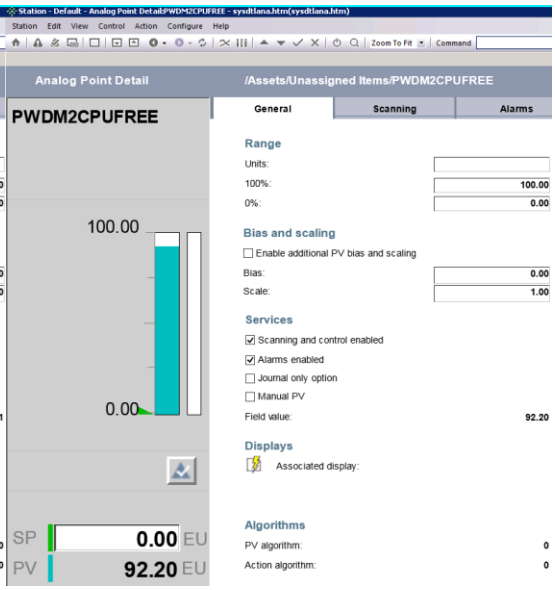


8. Enable channels:



9. Call-up display for WDM OPC SCADA Point.


Station - Default - Analog Point Detail:PWDM1CPUFREE - sysdtlana.htm(sysdtlana.htm)
Station Edit View Control Action Configure Help
Zoom To Fit
Command
Analog Point Detail
/Assets/Unassigned Items/PWDM1CPUFREE
PWDM1CPUFREE
General
Scanning
Alarms
100.00
0.00
Range
Units:
100%: 100.00
0%: 0.00
Bias and scaling
Enable additional PV bias and scaling
Bias: 0.00
Scale: 1.00
Services
Scanning and control enabled
Alarms enabled
Journal only option
Manual PV
Field value: 92.31
Displays
Associated display:
Algorithms
PV algorithm: 0
Action algorithm: 0
SP 0.00 EU
PV 92.31 EU

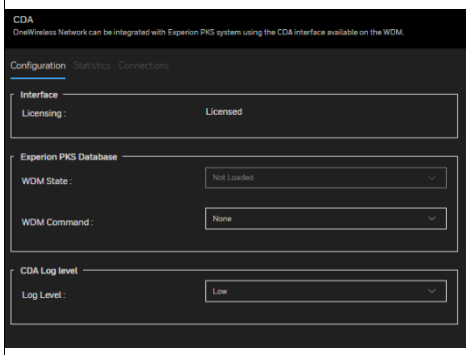

Station - Default - Analog Point Detail:PWDM2CPUFREE - sysdtlana.htm(sysdtlana.htm)
Station Edit View Control Action Configure Help
Zoom To Fit
Command
Analog Point Detail
/Assets/Unassigned Items/PWDM2CPUFREE
PWDM2CPUFREE
General
Scanning
Alarms
100.00
0.00
Range
Units:
100%: 100.00
0%: 0.00
Bias and scaling
Enable additional PV bias and scaling
Bias: 0.00
Scale: 1.00
Services
Scanning and control enabled
Alarms enabled
Journal only option
Manual PV
Field value: 92.20
Displays
Associated display:
Algorithms
PV algorithm: 0
Action algorithm: 0
SP 0.00 EU
PV 92.20 EU

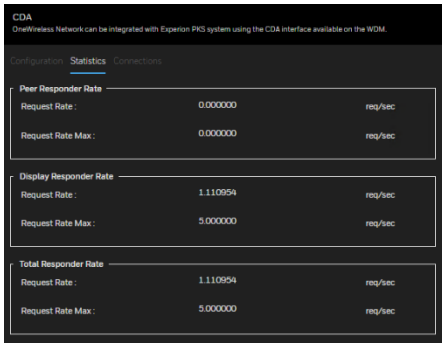
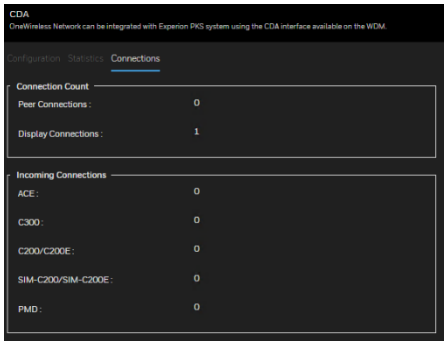
About integrating OneWireless Network with Experion using the CDA interface

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 Panel element	Parameters and their descriptions
Configuration  	**WDM State** parameter indicates the WDM state in an Experion system. This parameter displays the state as **Online**, when the WDM is loaded in an Experion system. **WDM Command** parameter on the CDA interface consists of the following commands. – **None** – **Clear CDA Database**: This command is used to 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.

Statistics  	Displays the CDA statistics used for maintenance and performance monitoring of the WDM. For the specifications for peer responder rate and display responder rate, refer to the Technical Specifications document available at the Honeywell Process Solutions website.
Connections  	Displays the number of peer and display connections between the WDM and the controller CEEs. It also displays the details about incoming and outgoing connections between the different CEEs.

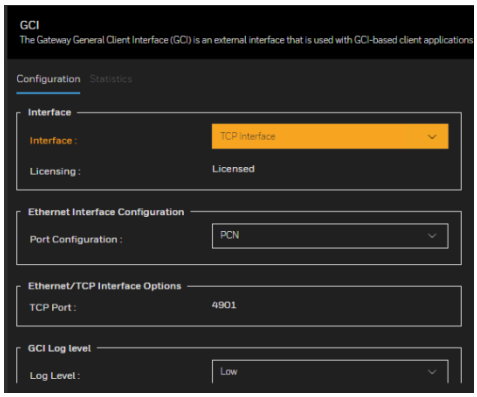
For more information about the CDA parameters, see the *OneWireless Parameter Reference Dictionary*.

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.



4. Under Interface Configuration,
   - In the **Ethernet Interface** list, click the required option. The following are the interface options available.
     - FDN
     - PCN
     - SIN

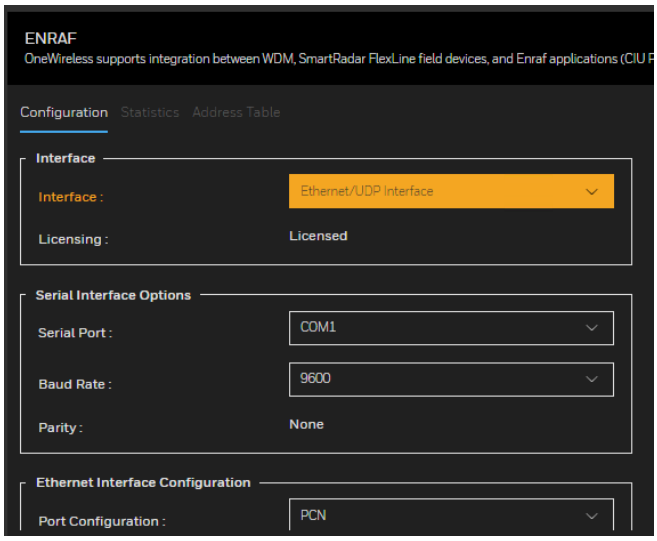
       Note: GCI interface is enabled only on the Ethernet interface selected
5. Under Ethernet/TCP Interface Options,
   - In the **TCP Port** field, specify the default port number **4901**.
6. Click **Apply**.
7. Expand **Statistics** tab to monitor performance of GCI interface.
8. Verify the following attributes 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.



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.

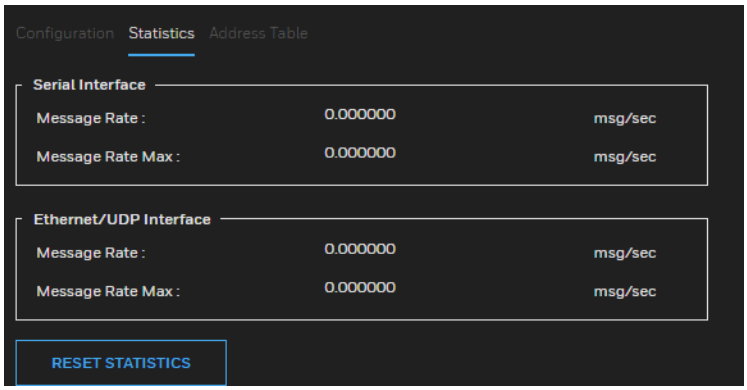
To configure ENRAF serial interface

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.



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

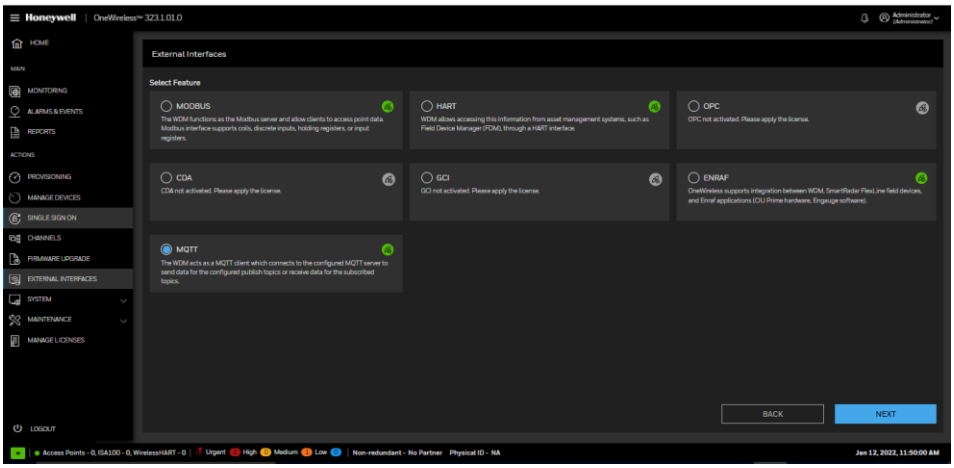
- If the port configuration is selected as **SIN**, ensure that **SIN** is enabled in the WDM.
- MQTT communication is only supported in port **8883.**
- Ensure the WDM certificate is downloaded from the **Software Downloads** section and added to trust store of the MQTT Broker.
- Ensure the WDM certificates 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.

NOTE	**In the MQTT interface, if a hostname is used to configure as server, then DNS has to be enabled in the respective interface.**

To enable MQTT interface

1. Select **EXTERNAL INTERFACES** in the Left Navigation Menu bar.

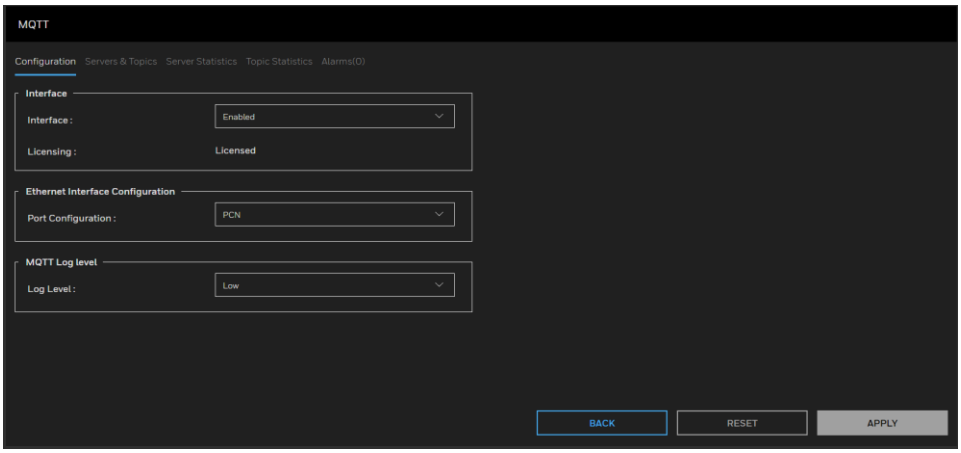
2. Select **MQTT** and click **NEXT.**



3. Configure the following under **Configuration** Option.

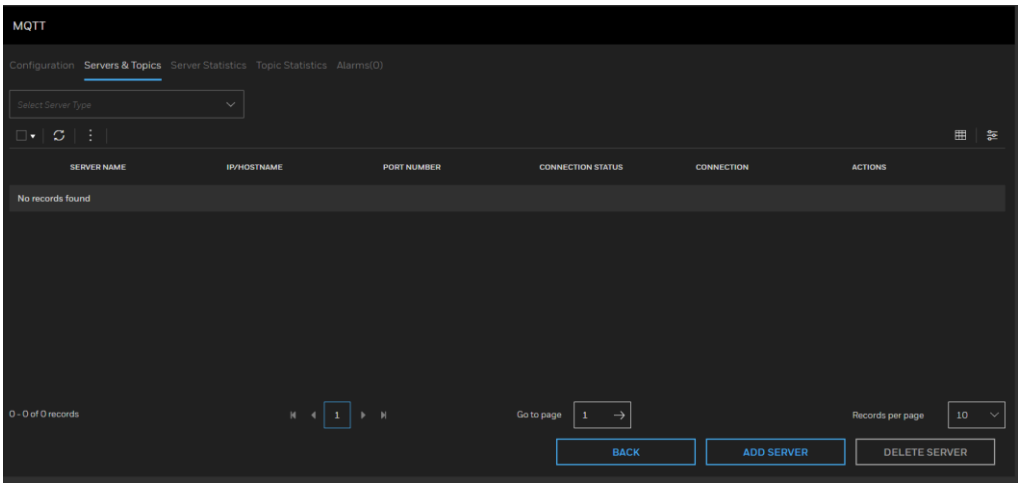
   - **Interface**: Select **Enabled** from the drop-down list to allow the MQTT connection. Select **Disabled** to disable the MQTT connection.
   - **Port configuration**: Port configuration can be configured in either **SIN** or **PCN** interface. Default interface is **SIN**.
   - **Log level**: Log level can be selected between **Low** and **High**.

4. Click **Apply**.



Configure MQTT Server

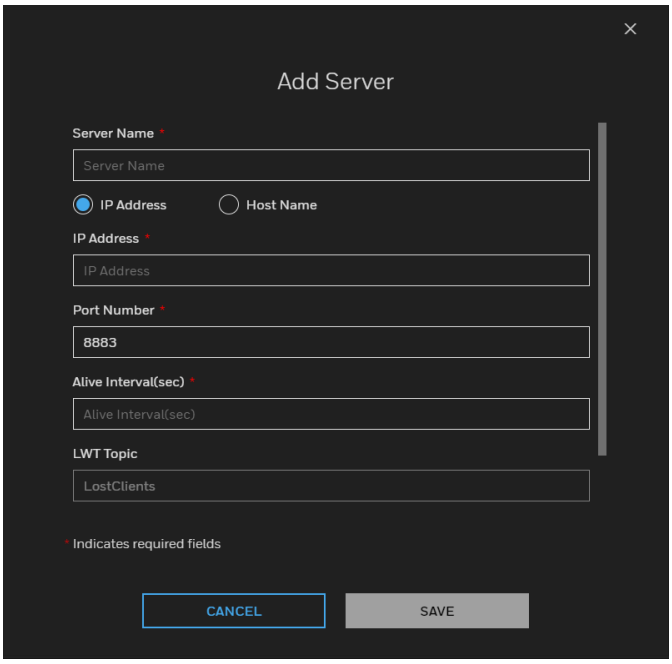
1. Select **Servers and Topics** and click **ADD SERVER.**



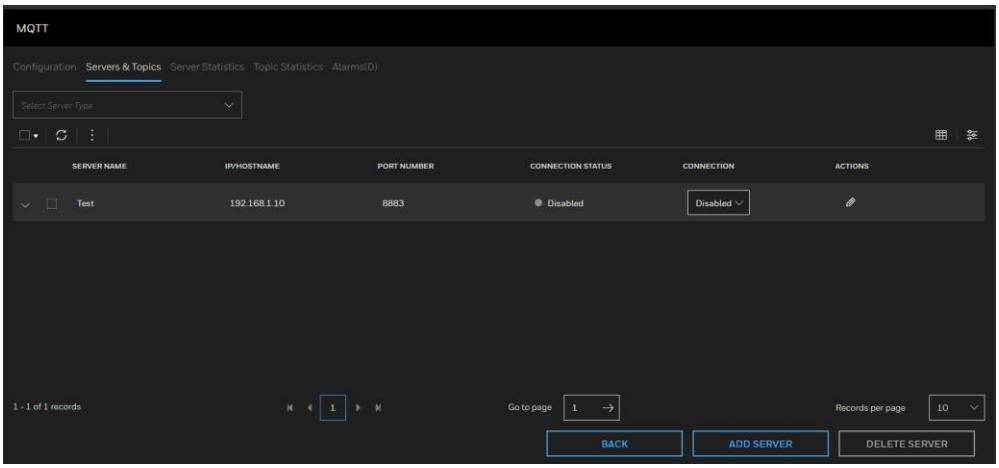
2. Enter the details in **Add Server** Window as given below.

   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.

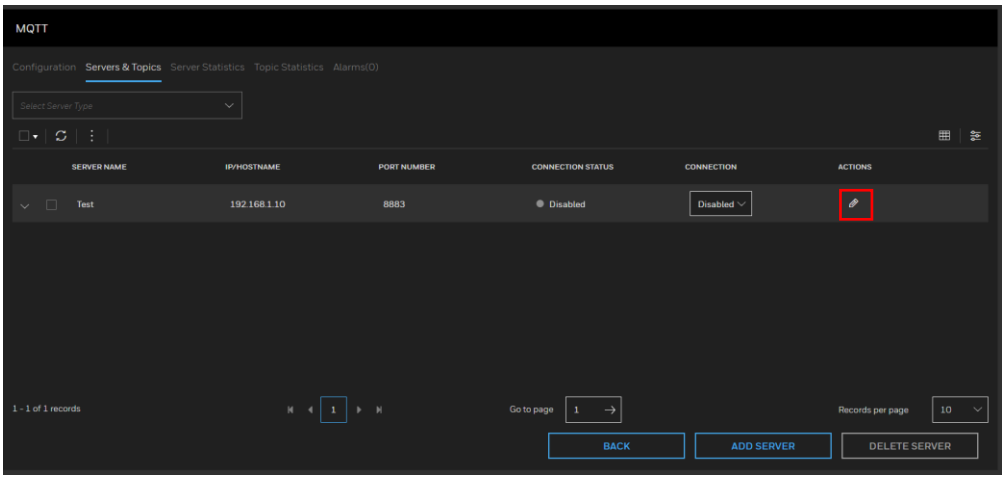


3. Click **Save.**
4. Once the server is successfully added, it appears in the **Servers and Topics** window as shown below.



5. To Edit Server, Click on **Edit** under **Actions.**

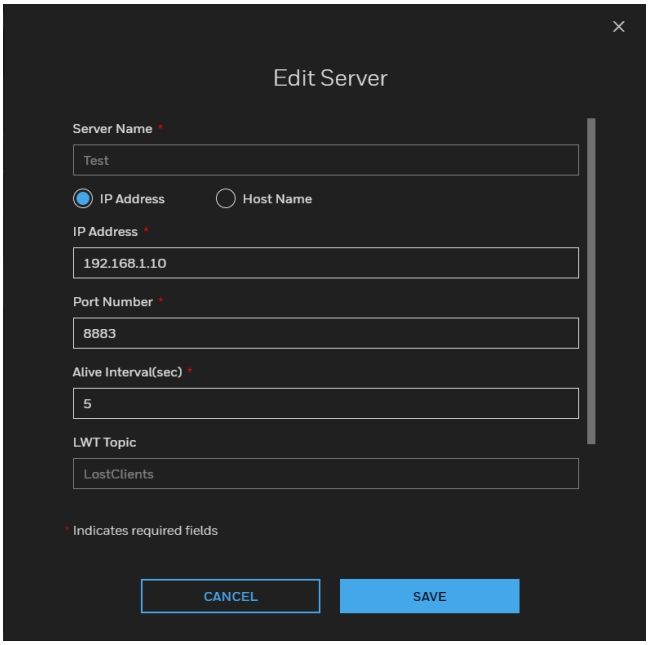
   Note: Ensure the connection status is disabled.



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.

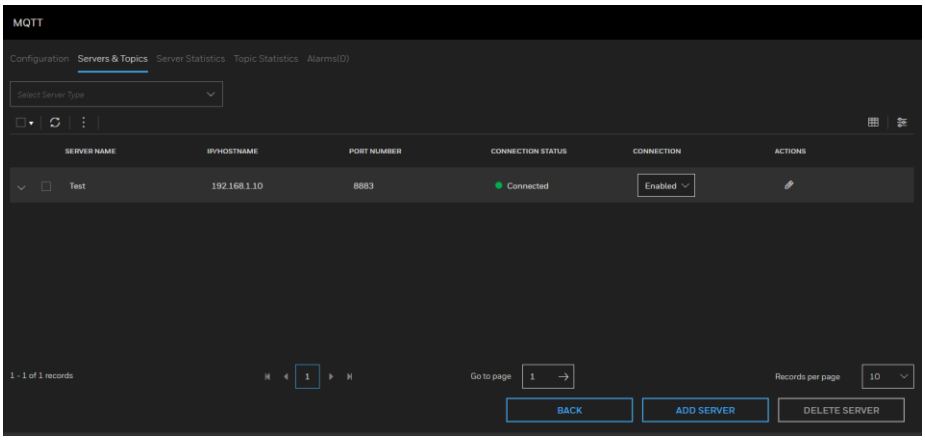
7. Click **Save.**



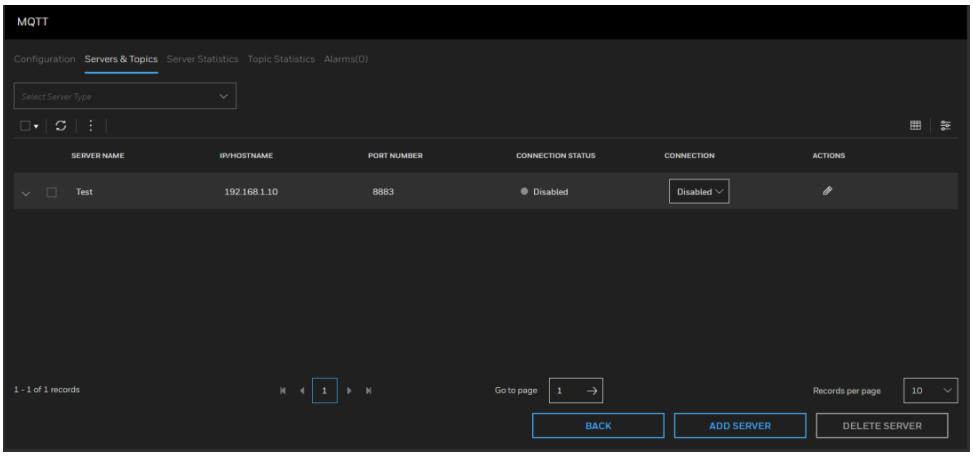
8. **Enable/Disable MQTT Connection**

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**.

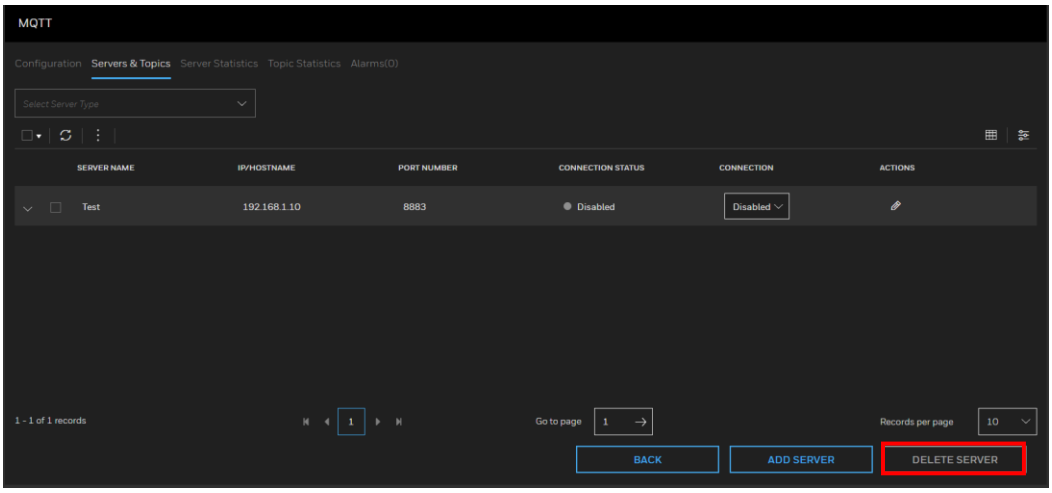


- To disable the MQTT connection, select **Disabled** from the connection drop down list.

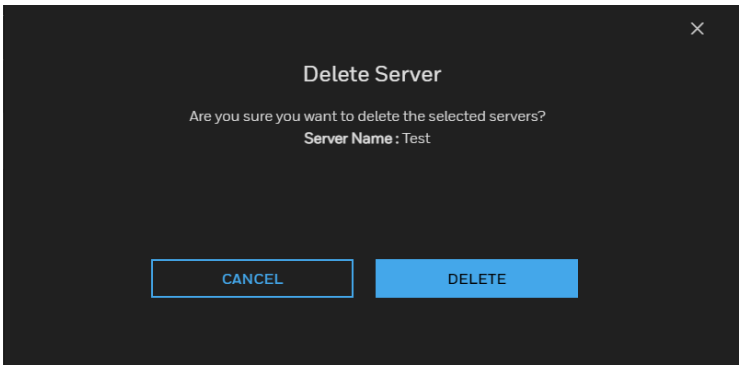


9. To delete the server, select the server and click **DELETE SERVER**. Delete Server will delete the server configuration and all the topics configured for the server.

   Note: Ensure the connection is disabled before deleting the server and deletion of multiple servers also supported.



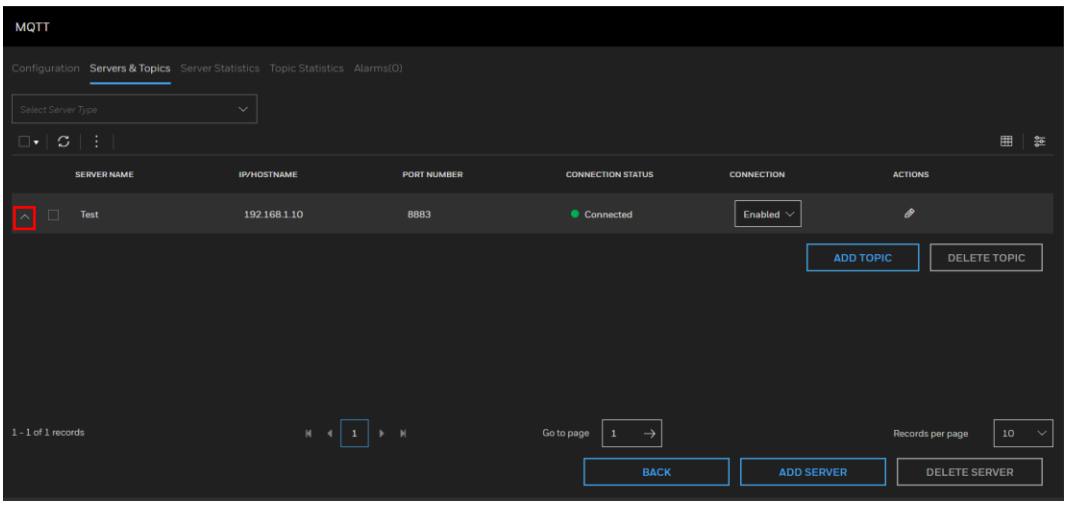
10. A pop -up window appears for the confirmation, click **DELETE**.



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.

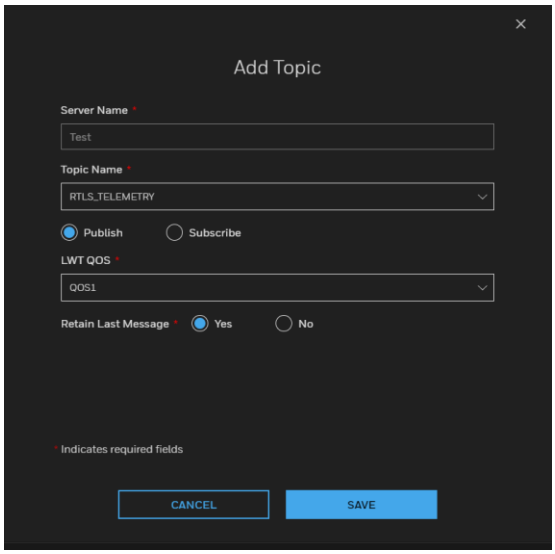


2. Enter the details in **Add Topic** Window as given below.

- **Server Name:** Server name cannot be edited.
- **Topic Name**: Select the topic name based on the nine predefined topics and type.

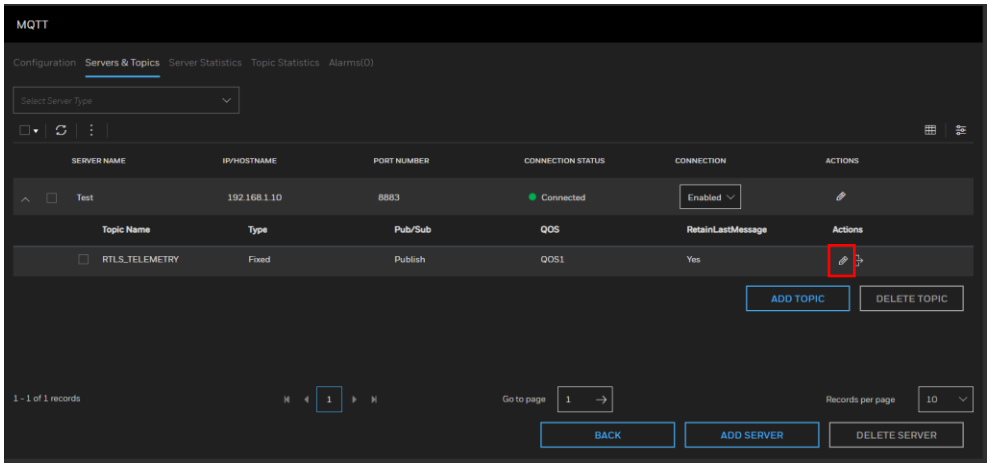
Topic Name	Topic Type
RTLS_TELEMETRY	Publish
RTLS_ANCHOR_CONFIG_WDM	Subscribe
WDM_ANCHOR_CONFIG_RTLS	Publish
RTLS_TAG_CONFIG_WDM	Subscribe
WDM_TAG_CONFIG_RTLS	Publish
WDM_TAG_CONFIG_WDM	Publish or Subscribe
RTLS_ ALARM	Publish
RTLS_ DISTANCE	Publish
RTLS_ DISTANCE	Subscribe

- 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 QOS0, 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.



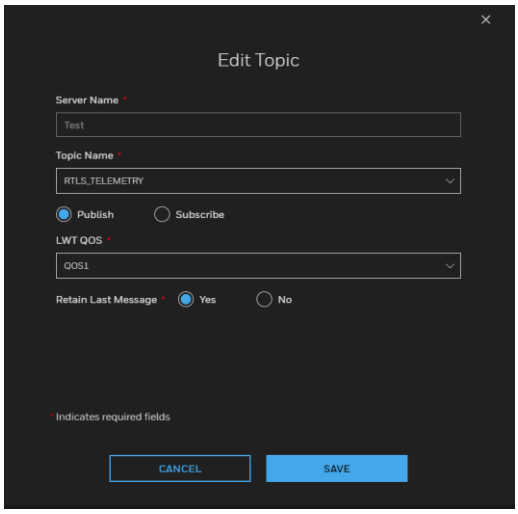
3. Click **Save**.

4. To edit the existing Topic, click on **Edit** under **Actions**.

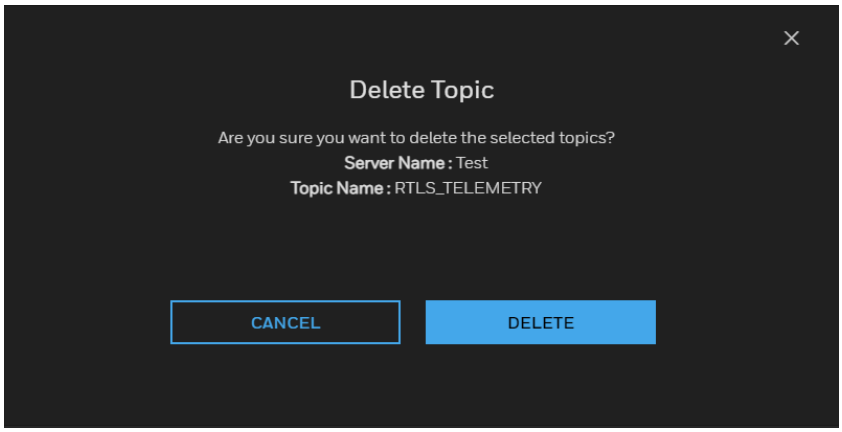


5. Enter the details in **Edit Topic** Window as given below.

   - **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 QOS0, 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.



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.

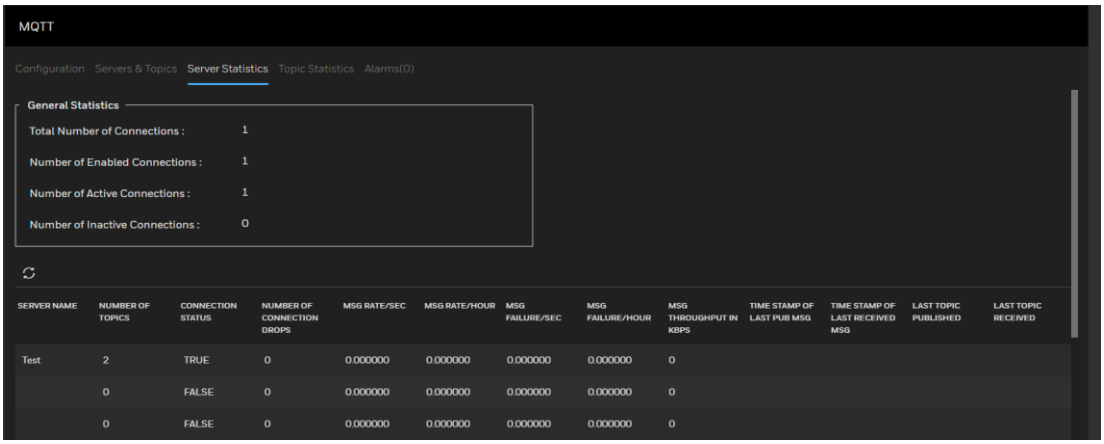


Fig. 26. Server Statistics

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.

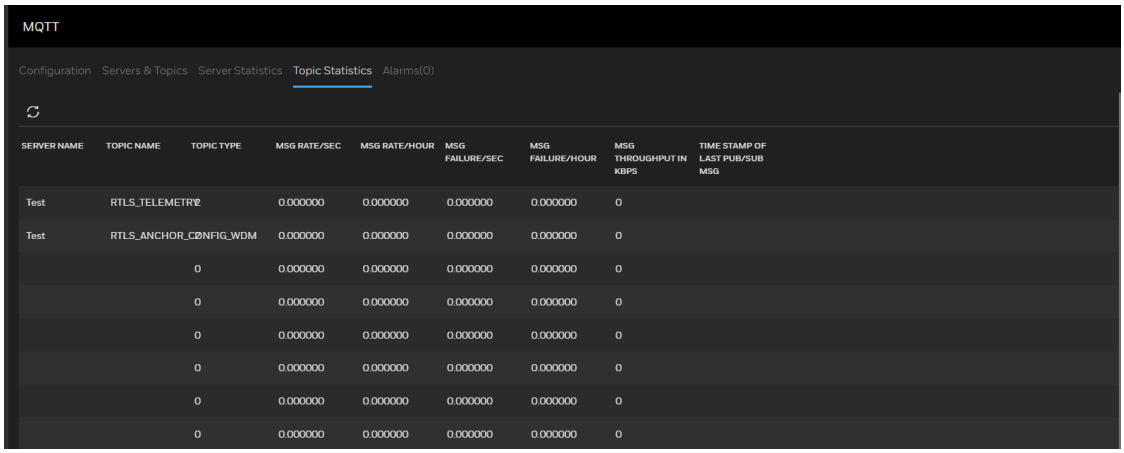
TIME STAMP OF LAST RECEIVED MSG: Time stamp of Last Subscribed Topic for each server.

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



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 PUB/SUB MSG
Test	RTLS_TELEMETRY	2	0.000000	0.000000	0.000000	0.000000	0	
Test	RTLS_ANCHOR_CONFIG_WDM	0	0.000000	0.000000	0.000000	0.000000	0	
		0	0.000000	0.000000	0.000000	0.000000	0	
		0	0.000000	0.000000	0.000000	0.000000	0	
		0	0.000000	0.000000	0.000000	0.000000	0	
		0	0.000000	0.000000	0.000000	0.000000	0	
		0	0.000000	0.000000	0.000000	0.000000	0	
		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.

Table. 19. Default role-based access privileges

Function	View Only	Instrument Tech	Professional Installer	Administrator
Read	Y	Y	Y	Y
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	N	Y

Function	View Only	Instrument Tech	Professional Installer	Administrator
Provision FDAP or Wireless Infrastructure Node	N	N	N	Y
Configure Device Publication	N	Y	N	Y
Replace Device	N	Y	N	Y
Upgrade Device	N	N	N	Y
Device Write	N	Y	Y	Y
Write Protect Device	N	Y	Y	N
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	Y
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

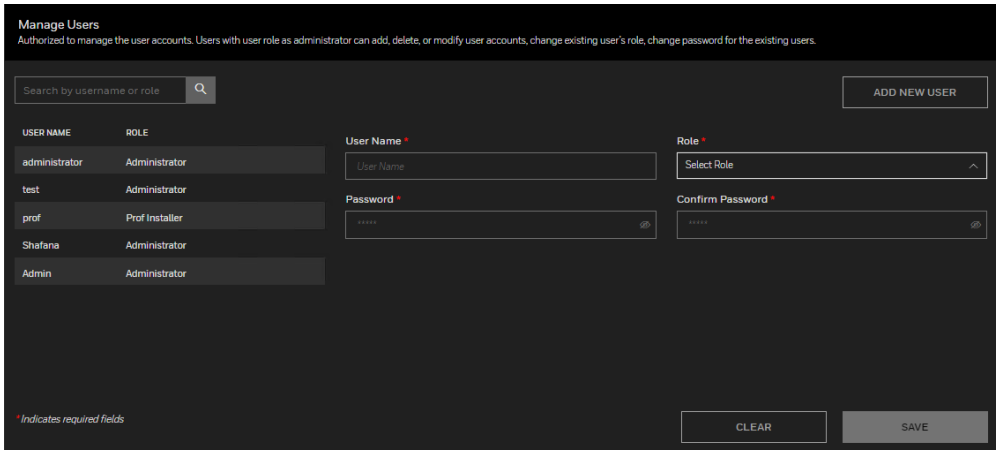
TX power level can be configured for Honeywell devices only.

ATTENTION	**The Provision WDM function also enables you to configure the redundant related parameters.**

Create user accounts

To create user accounts

1. 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.



4. Click **Save**.

Edit user account

To edit user account

1. 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

ATTENTION	**Note that you cannot delete the default user account (administrator) configured by the WDM.**

To delete user account

1. 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

1. 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

1. 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

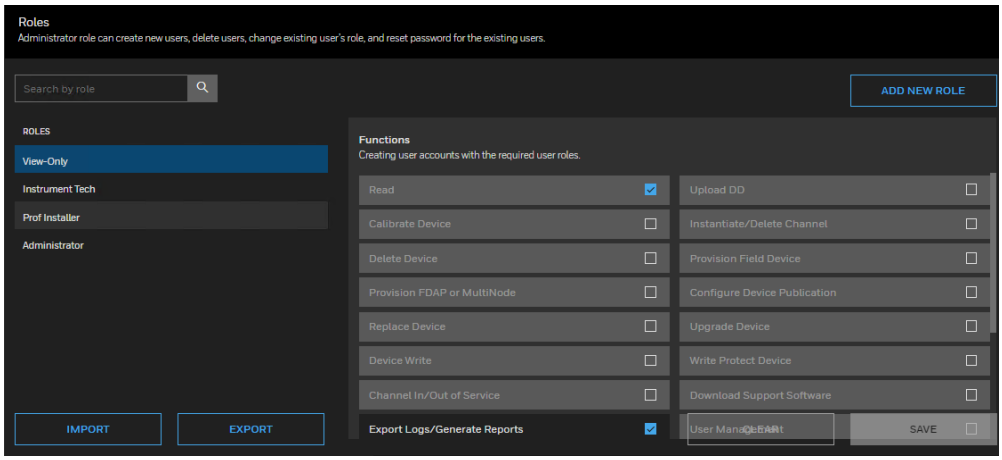
ATTENTION	**Note that you cannot change the user role for the default user account (administrator) configured by the WDM.**

To change user role

1. 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



To add a new user role:

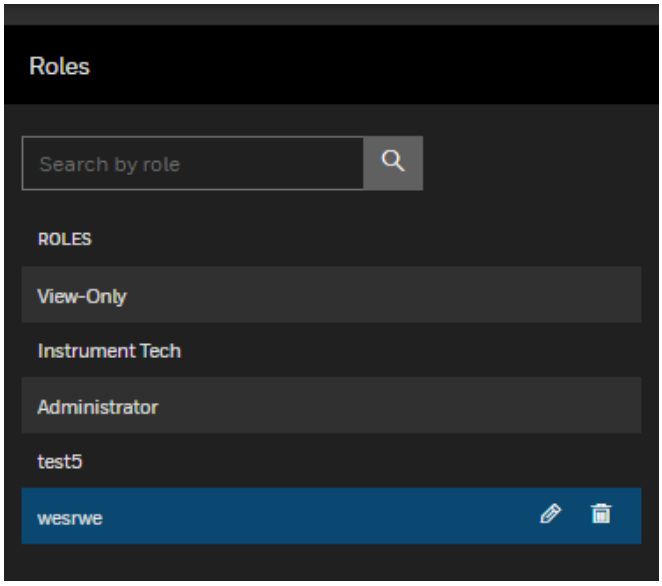
1. From the Left Navigation Menu bar, click **System > Manage Roles.** The **Manage Roles** window appears.
2. Click **Add New Role**.
   A new column is added to the list of users. The new user name is added as **New Role x** (x is the number of user being created). You can edit the name of the user 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.



A confirmation dialog appears, click **OK** to delete the role.

To import user roles:

1. 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:

1. 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:

1. 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 AndroidProvDev.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

NOTE	**Firmware upgrade is supported only on ISA 100 devices.**

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.

CAUTION	• **Upgrading the WDM firmware makes the WDM offline for some time. During this operation, all the devices drop and join the network again.** • **Once initiated, you cannot abort the firmware upgrade operation.** • **The WDM should not be turned off while the upgrade is in progress.**

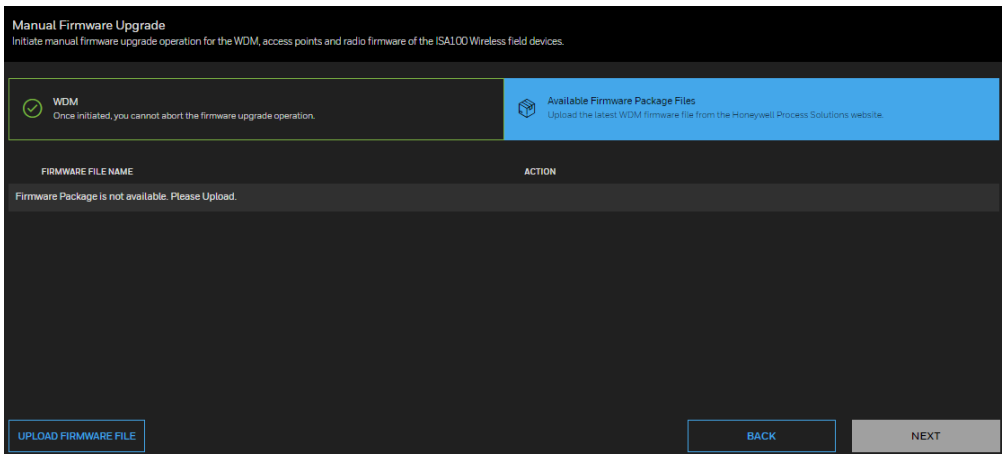
The steps for upgrading the WDM from R202 to R210, from R210 to R220 and then from R220 to R230. or 230 to 240, R240.2/R300.2 to R310, R310.x to R320.x , R320.x to R321.x and R321.x to R323.x are common.

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.



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.

ATTENTION	**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.

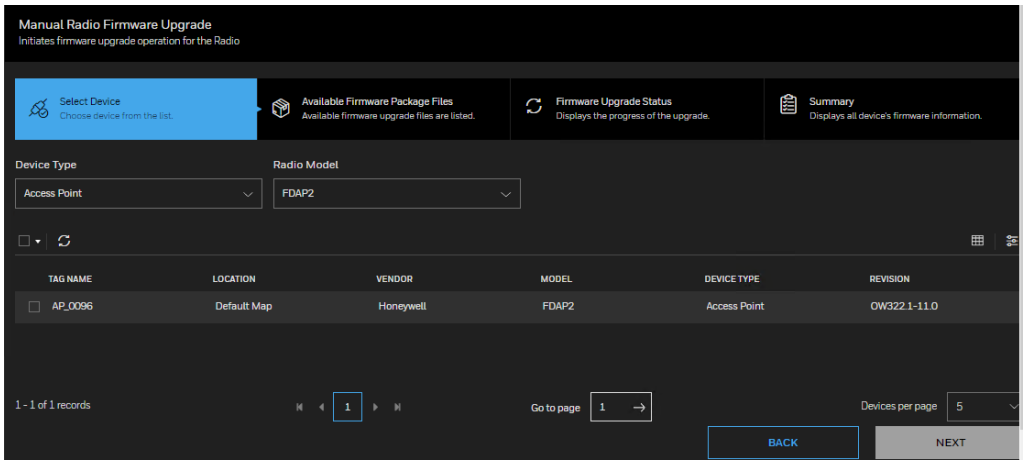
c. Under Identification, verify the Revision.

Upgrading the FDAP/access point firmware

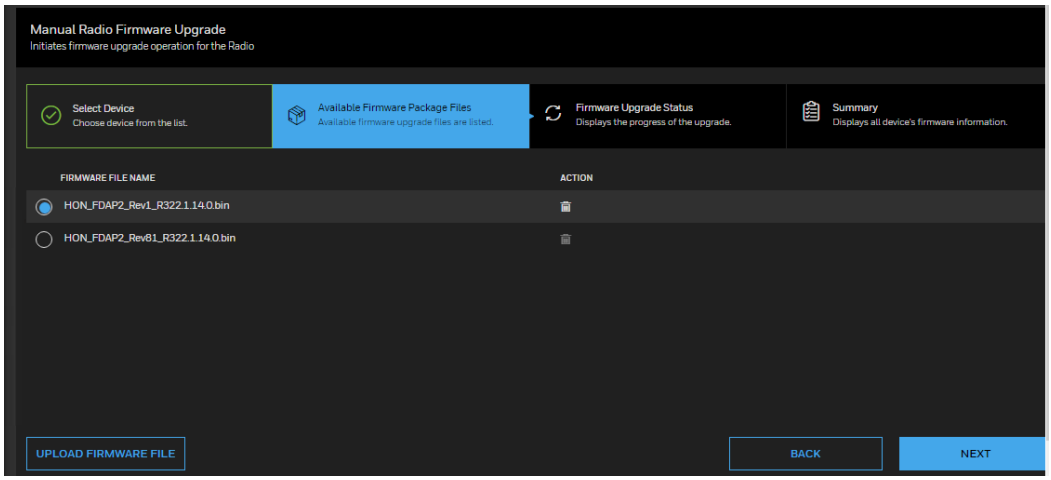
Download the latest FDAP/access point firmware files from the Honeywell Process Solutions website.

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**.



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"



7. In the **Available Firmware Files** list, select the required firmware upgrade file.

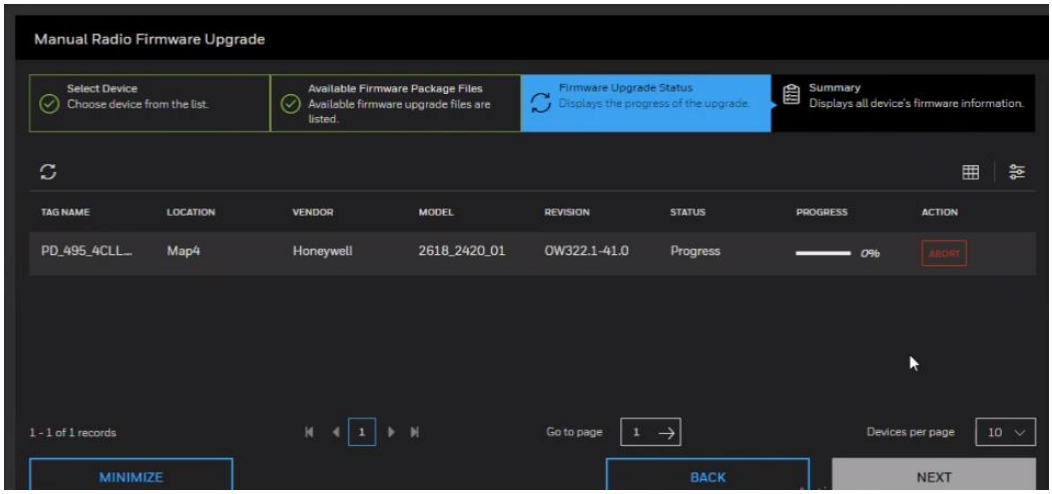
By default, the firmware upgrade file appears in the list. If the file is not available in the list, perform the following steps to open the firmware file.

   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.



ATTENTION	• **To abort any firmware upgrade operation, click the Abort Upgrade icon adjacent to the upgrade status.** • **To remove the devices for which the firmware upgrade has 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.

ATTENTION	**Sensor Application firmware must be upgraded before upgrading the radio firmware.**
ATTENTION	**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) 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.

ATTENTION	• **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

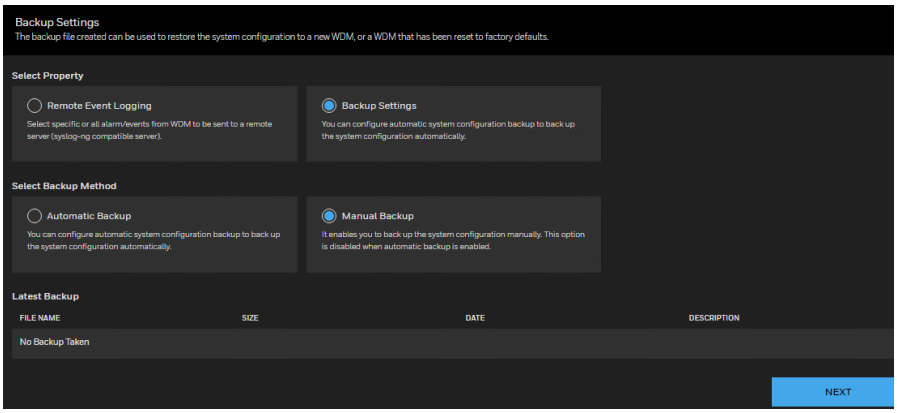
The **Manual Backup** option enables you to back up the system configuration manually. This option is disabled when automatic backup is enabled.

You can back up the data on a USB flash drive or on a specified server.

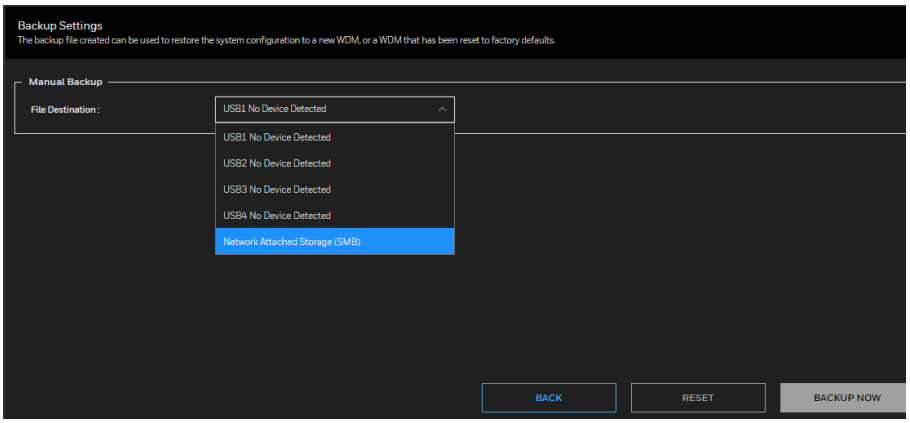
ATTENTION	**For network backup, windows machine password must not contain space.**

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.**



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.



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.

ATTENTION	**Manual and auto backups have an additional encryption password that must be added when restoring the backup**

   - **Name**: Name of the backup file.
   - **Size**: Size of the backup file.
   - **Date**: Date and time of last backup.

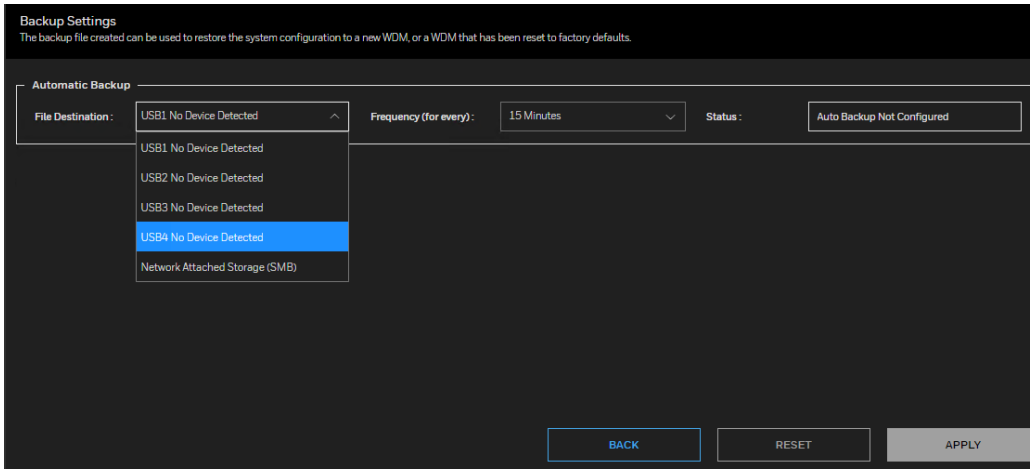
- **Description**: The mode of backup configured (automatic or manual) and the USB drive/slot number where the backup file was created. It also displays any errors that occurred during a backup.

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.



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 Restore from Backup 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.

Recommendation / Suitable control type for OneWireless system.

Type	Class	Type Based on Industry	Recommendation
Control	1	Closed loop Regulatory Control (Critical control loops)	Not Recommended
	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
	5	Uploading/Downloading (Requirement based Task/ Action)	Recommended

Deployment Topology:

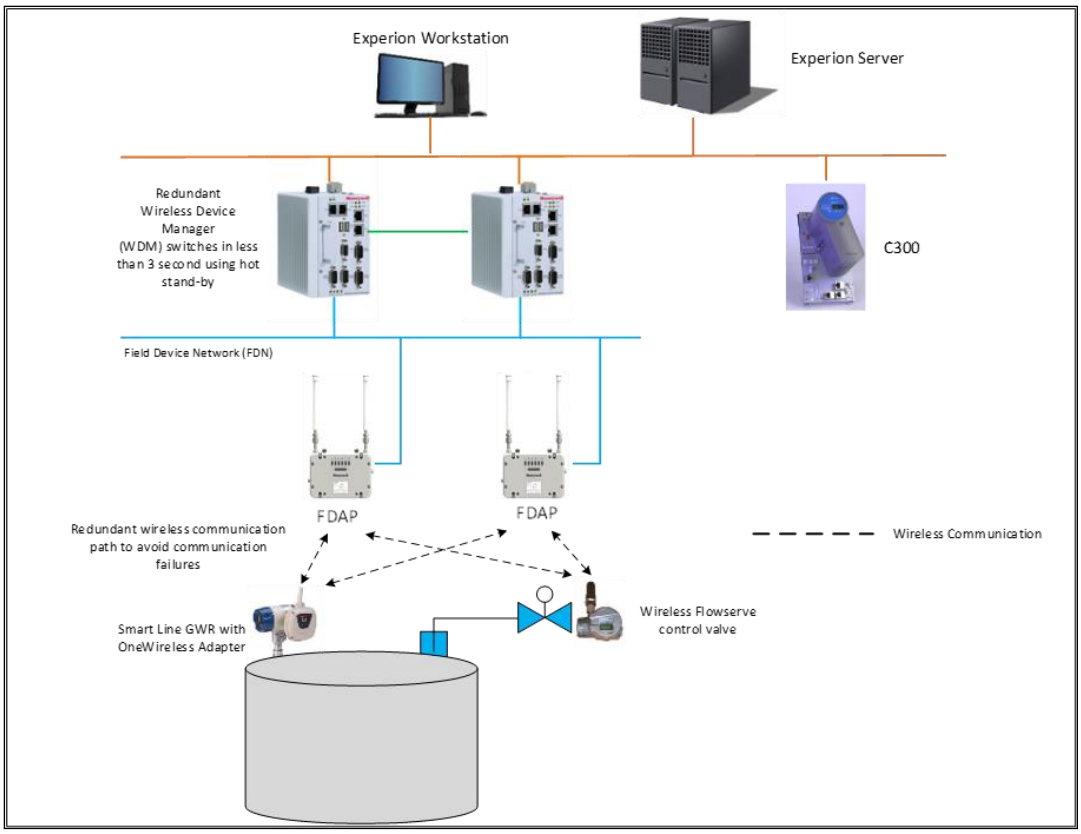
It is important to follow proper deployment rules for installing wireless devices for control applications to achieve the performance requirement needed.

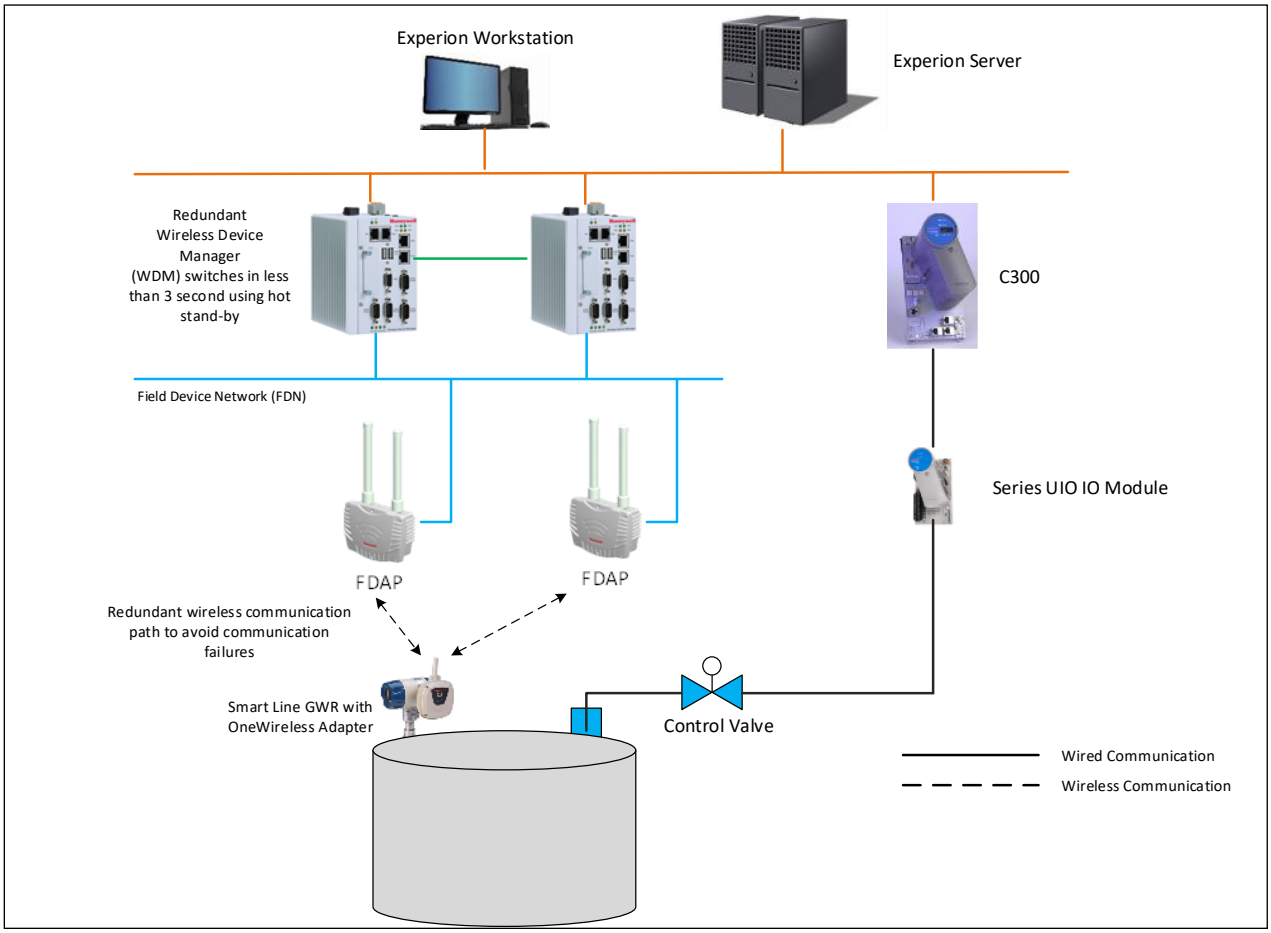
Wireless devices are installed at site based on their initial survey to ensure reliable communications with each device through redundant network connectivity, at least two communication paths are needed for each device from a wireless gateway. Each communication link must be good.

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

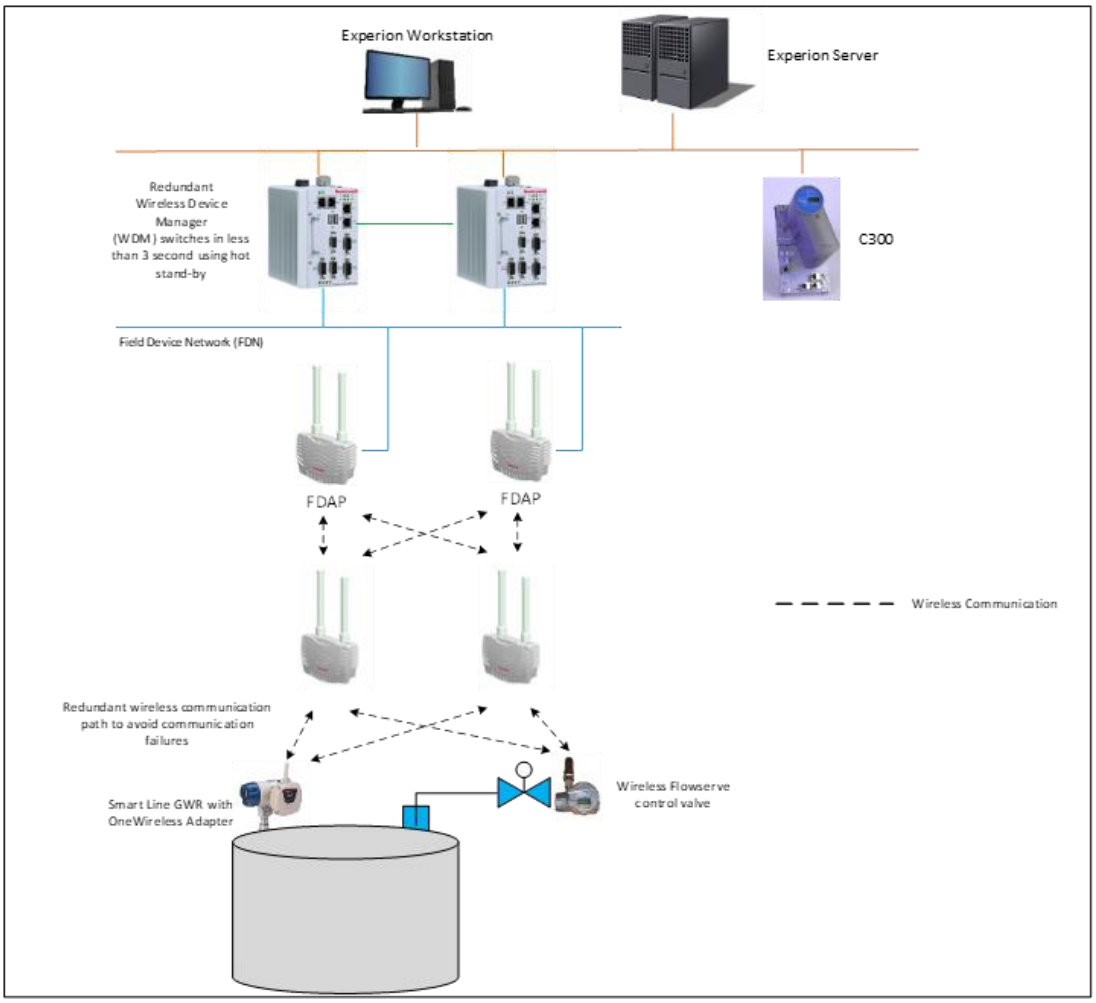
Wireless device deployments are completely based on loop criticality or data update to control system. 1 sec or faster (500 msec) update rates are difficult to achieve over a multi-hop mesh network due to routing delays. For such response times, it is recommend to deploy wireless devices communicating 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.




Experion Workstation
Experion Server
Redundant Wireless Device Manager (WDM) switches in less than 3 second using hot stand-by
C300
Field Device Network (FDN)
Series UIO IO Module
FDAP
FDAP
Redundant wireless communication path to avoid communication failures
Smart Line GWR with OneWireless Adapter
Control Valve
Wired Communication
Wireless Communication

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.



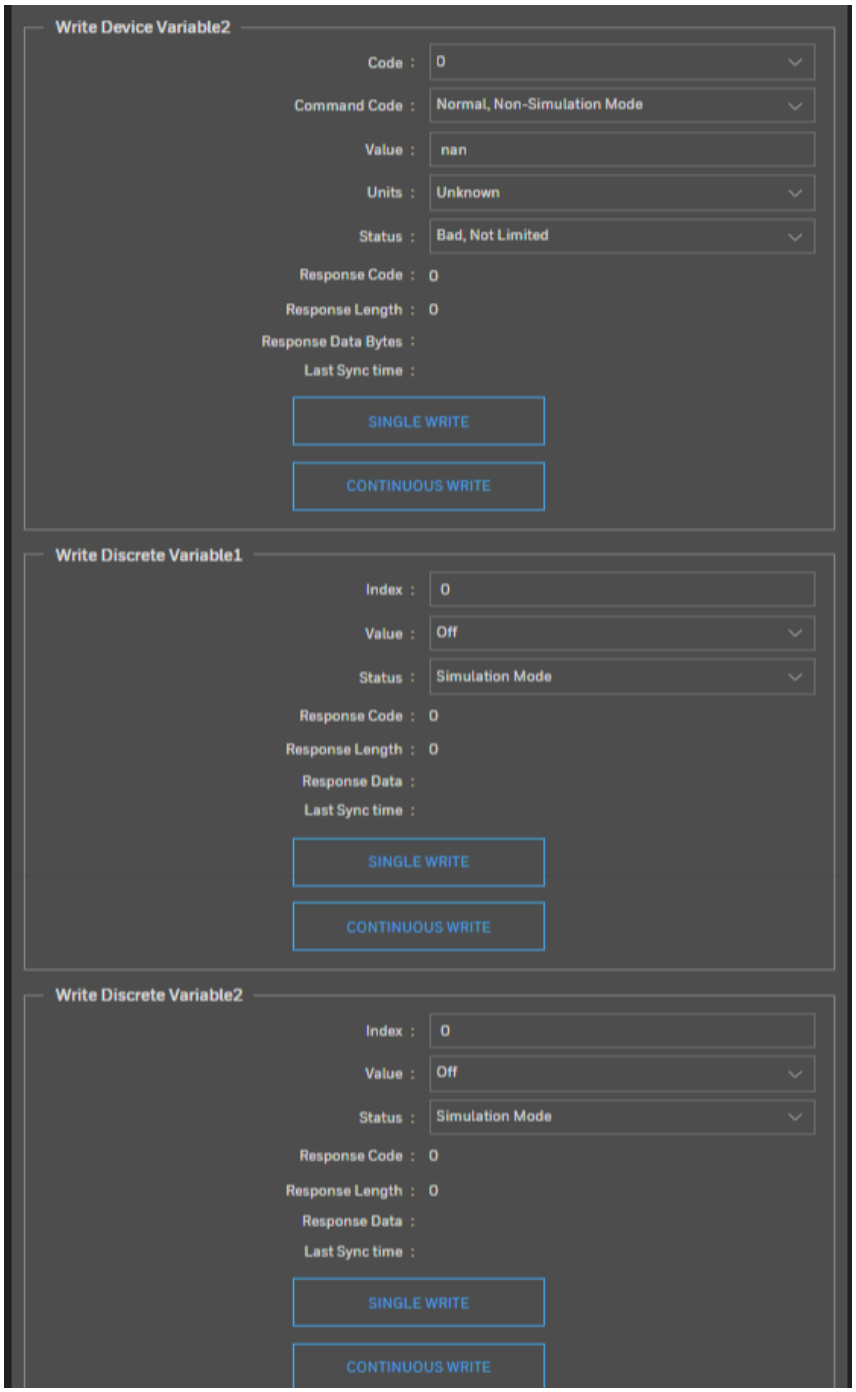
Sending control commands to WirelessHART devices

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 WirelessHART.

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 :
SINGLE READ
CONTINUOUS READ
Write Command
Command number : 0
Data length : 0
Data :
Response Status : 0
Response Length : 0
Write Response data :
Write Sync time :
SINGLE WRITE
CONTINUOUS WRITE
Write Device Variable1
Code : 0
Command Code : Normal, Non-Simulation Mode
Value : nan
Units : Unknown
Status : Bad, Not Limited
Response Code : 0
Response Length : 0
Response Data Bytes :
Last Sync time :
SINGLE WRITE
CONTINUOUS WRITE



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.

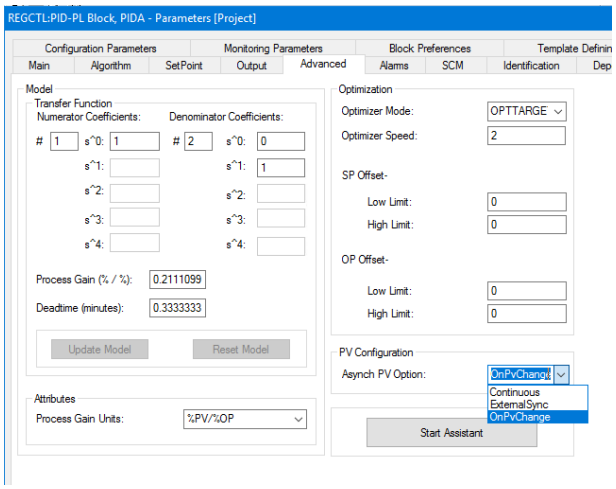
Features: Range and Dual Range control, handles complex dynamics, Predictive alarming, Handles Asynchronous PV input & Profit Loop Assistant

- 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.



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.

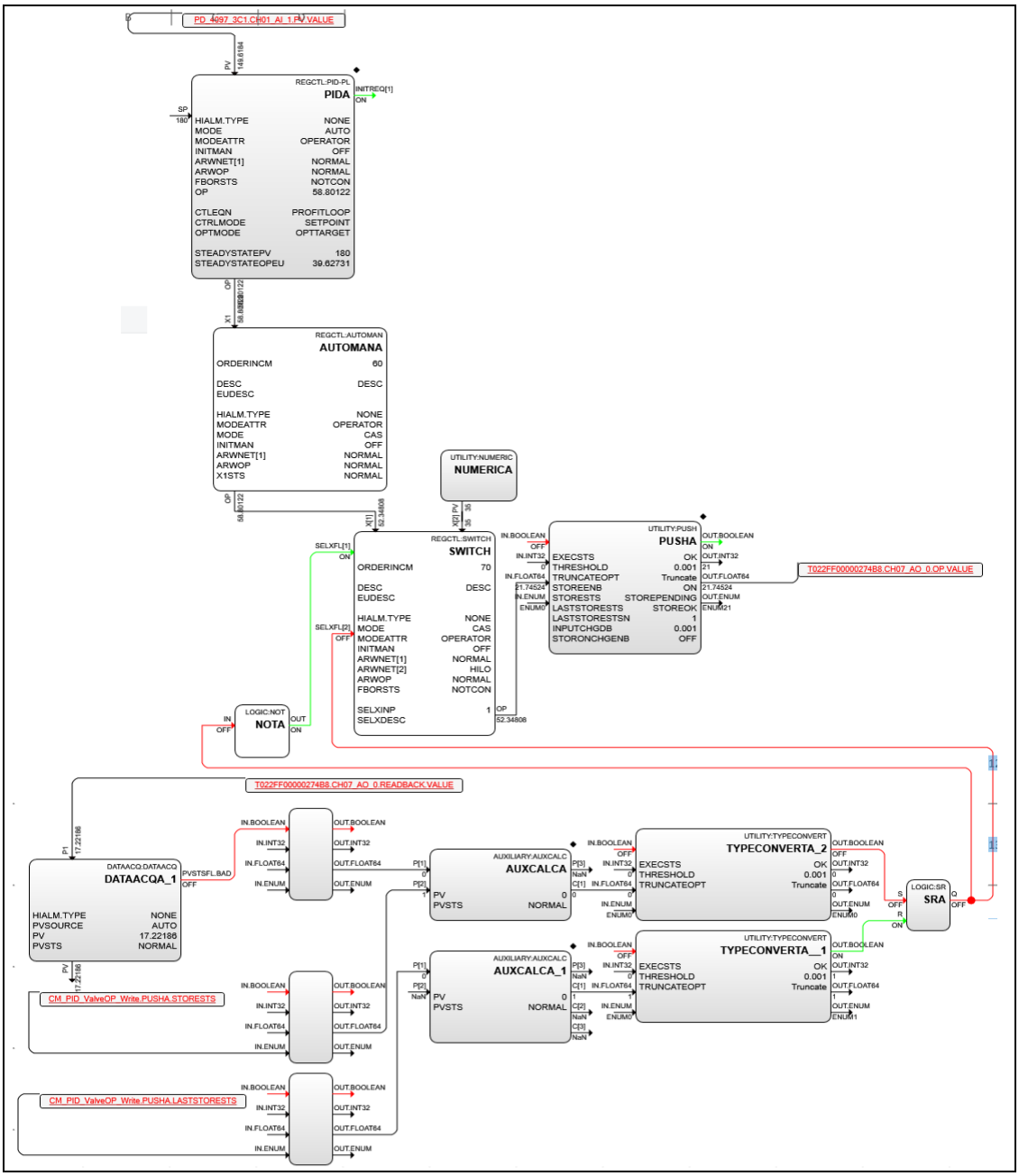
AUXILIARY CALCULATION(AUXCALCA) blocks: Used where logic is written such that a flag has been raised if either push blocks OP write failure or Readback of Output device failure is triggered. This flag is linked with SWITCH block such that it triggers failover and back initializes PID-PL block through 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)

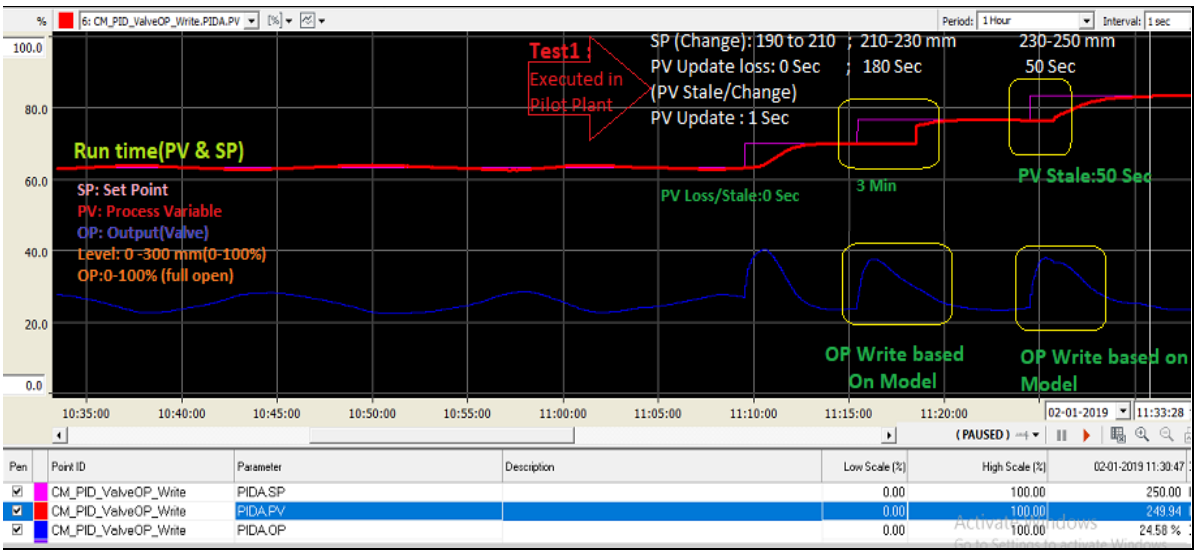
Control Element (OP): Flowserve PMV D3 Positioner with Valve assembly- ISA100 Wireless

Control System: EPKS R510.1 with C300 Controller

WDM: OW320 Release; Setup: 2 FDAP, 2 LPFR, 6 FDs

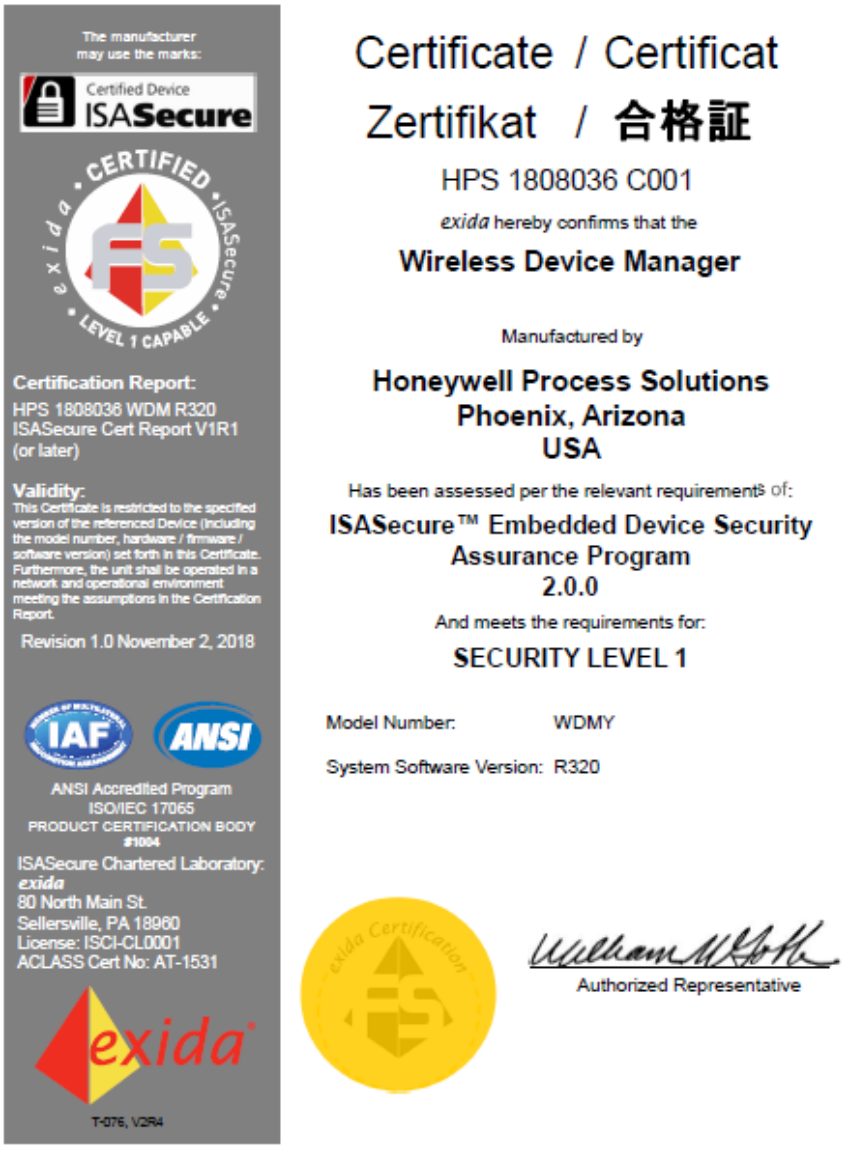
- Test

- 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.



The manufacturer may use the marks:

Certified Device ISASecure

exida CERTIFIED ISASecure LEVEL 1 CAPABLE

Certification Report:
HPS 1808036 WDM R320 ISASecure Cert Report V1R1 (or later)

Validity:
This Certificate is restricted to the specified version of the referenced Device (including the model number, hardware / firmware / software version) set forth in this Certificate. Furthermore, the unit shall be operated in a network and operational environment meeting the assumptions in the Certification Report.

Revision 1.0 November 2, 2018

IAF ANSI

ANSI Accredited Program
ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004

ISASecure Chartered Laboratory:
exida
80 North Main St.
Sellersville, PA 18960
License: ISCI-CL0001
ACLASS Cert No: AT-1531

exida

T-076, V2R4

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

Model Number: WDMY

System Software Version: R320

exida Certification

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.
5. 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.

ATTENTION	**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

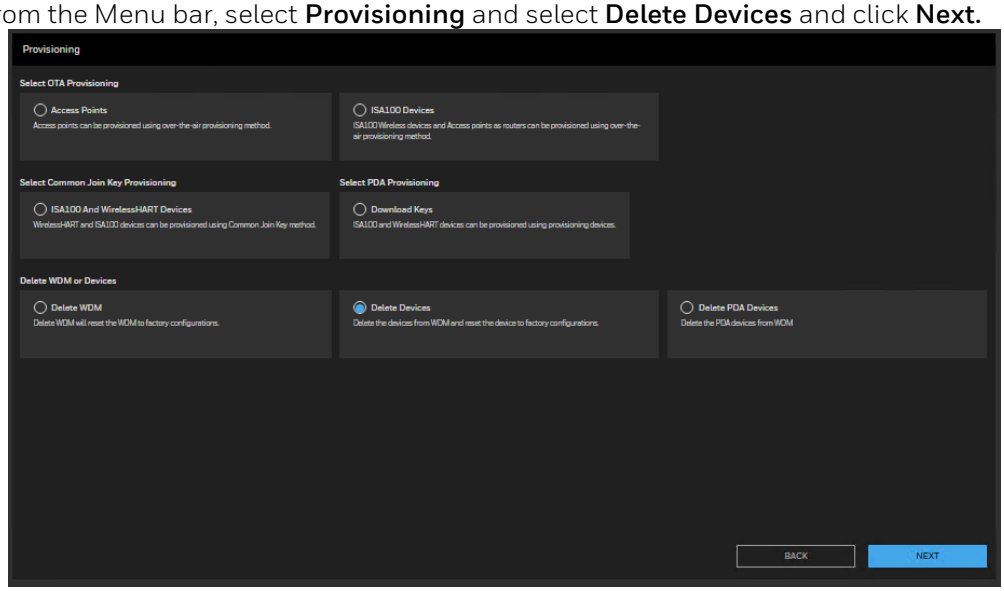
- Removing an online device resets the device configuration to factory defaults. This results in the loss of provisioning data from the device.
- Removing an offline device makes the security information of the device invalid, but retains the provisioning data in the device. Though the device retains the provisioning data, it must be authenticated again to allow it to join the network.

To remove a device:

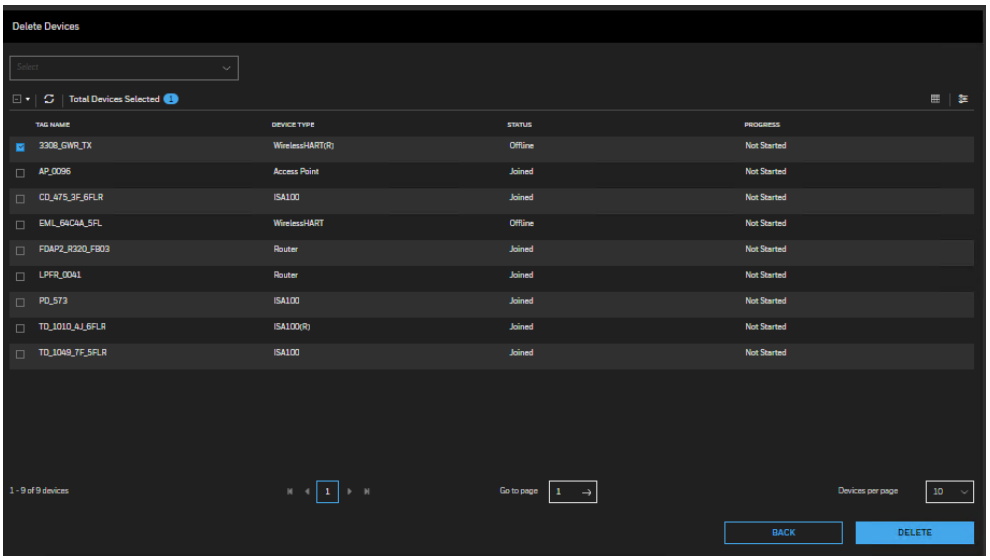
1. On the Selection Panel, select the devices that you want to delete.

   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.**



3. Select the device you need to delete and click **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.

CAUTION	**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:

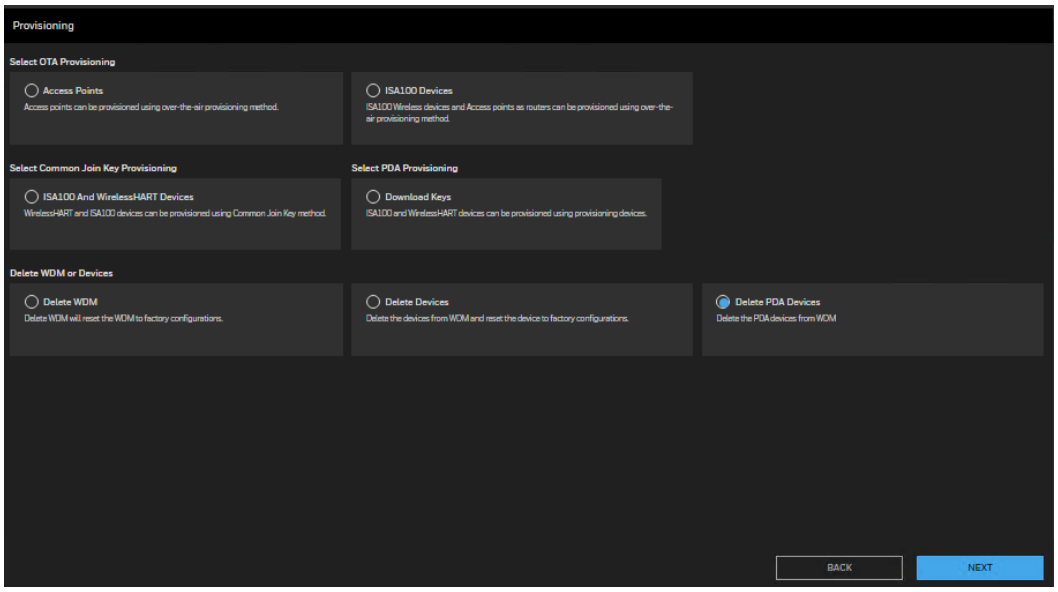
1. From the Menu bar, select **Provisioning** and select the devices or WDM from **Delete WDM or Devices** option and click **Next**.
2. Click **Delete**.

   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**.

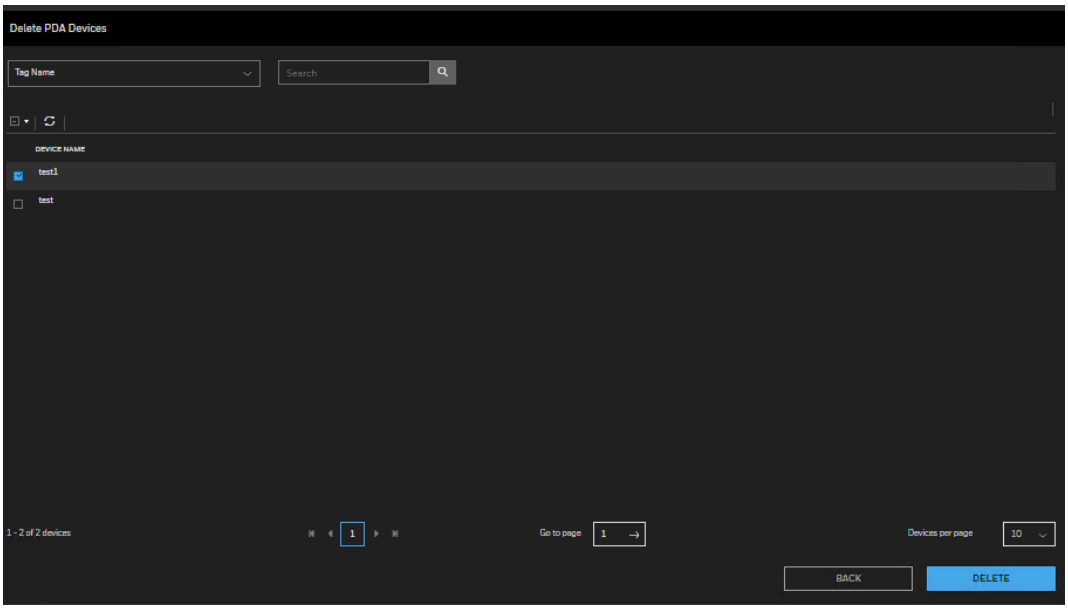
   You can either configure the WDM using the **First Time Configuration Wizard** or restore the system configuration using the latest available backup. If you are configuring the WDM using the **First Time Configuration Wizard**, you need to transfer new provisioning keys to the provisioning device and 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.**



2. Select the device you need to delete and click **Delete.**

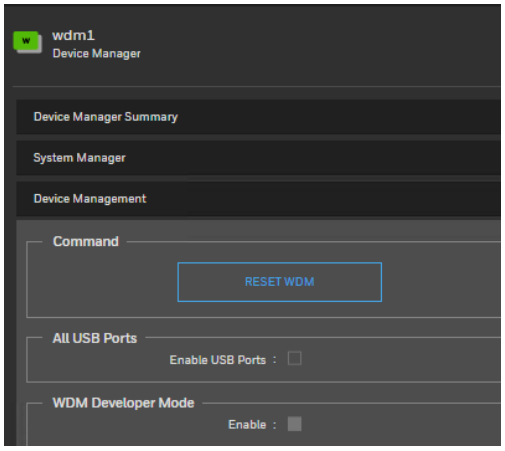


3. A window appears to provide the confirmation.

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.



3. Click **Reset WDM**. The WDM restarts.

To restart FDAP/Access Point/field device

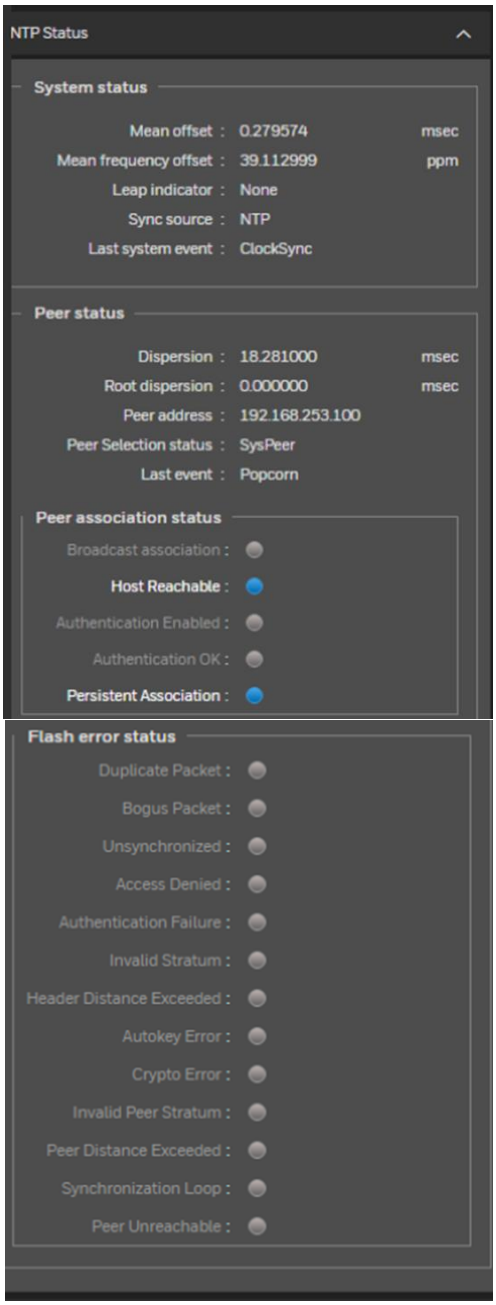
1. From **Manage Devices**, select the device to be restarted.
2. Expand **Device Management** in the Property Panel.
3. In the **Join Command** list, select one of the following options.
   - **None**
   - **Warm Restart** — preserves static and constant attributes data.
   - **Restart as Provisioned** — 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.



NTP server unreachable

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 reachable

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

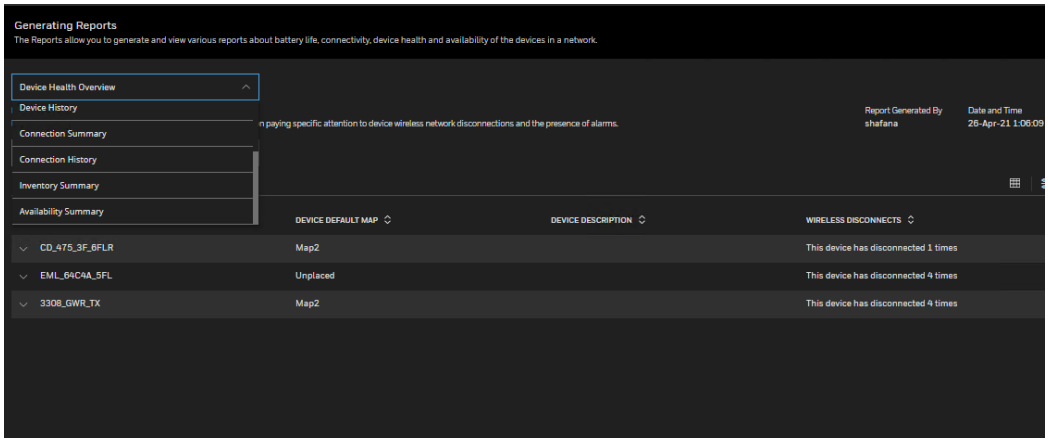
In the NTP Status panel, under the **System status** section, the Mean frequency offset field indicates the periodic correction applied to the system clock. Positive values make the clock go faster while negative values slow it down. When the NTP process starts synchronizing with a server, depending 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.



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).

ATTENTION	**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:

1. 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
OTAP	Over the Air Provisioning
PCAP	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.
PCAP	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
OTAP	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	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	Note that in this document, a reference to WDM includes WDMX and WDMY unless otherwise mentioned. Specific WDM is mentioned as and 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 feedback

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: hpsdocs@honeywell.com

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell 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, https://process.honeywell.com/us/en/contact-us.

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 http://www.automationcollege.com.

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

Honeywell