



FIELD DEVICE MANAGER

RELEASE 511.4

User's Guide

EP-FDM-11511C

August 2020

Disclaimer

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

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

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

Copyright 2020 - Honeywell International Sàrl

Contents	3
Chapter 1 - About this document	12
1.1 Prerequisite knowledge	12
1.2 Scope	12
1.3 Terms and definitions	14
1.4 References	17
1.5 Glossary	17
Chapter 2 - Introduction to Field Device Manager	24
2.1 Supported protocols	24
2.2 Enhancements to FDM R511	24
2.2.1 Enhancements in FDM R511.2	25
2.2.2 Enhancements in FDM R511.4	25
2.3 Enhancements in FDM R501	25
2.4 Enhancements in FDM R500	25
2.5 Enhancements in FDM R450	26
2.6 Enhancements in FDM R440	26
2.7 Enhancements in FDM R430	26
2.8 Support for Safety Manager SC	27
2.9 FF-EDDL support in FDM	27
2.10 ISA100 Wireless support in FDM	27
2.11 DE support in FDM	27
2.12 FDM functions and features	28
2.13 FDM features and supported devices	32
2.14 Supported technologies	35
2.14.1 Device Description files	35
2.14.2 FDT-DTM	36
2.14.3 FDI	37
2.15 Supported protocols	37
2.15.1 HART protocol	38
2.15.2 Foundation Fieldbus protocol	38
2.15.3 PROFIBUS protocol	38
2.15.4 ISA100 protocol	39
2.15.5 Honeywell Digitally Enhanced (DE) protocol	39

2.16 FDM software components and utilities	39
Chapter 3 - Getting started with FDM	41
3.1 Locale	41
3.2 Logging on to the FDM Server Management Tool	41
3.3 Updating FDM Server status	43
3.4 Updating the FDM license	43
3.4.1 Prerequisites	45
3.5 Logging on to the FDM Client	45
3.6 Changing the password	48
3.7 Logging on to FDT Comm Console	48
Chapter 4 - Configuring networks	50
4.1 Configuring RS-232 HART Modem	51
4.2 Configuring FDM for a Honeywell HART DE Modem	52
4.3 Configuring FDM for an RS-485 HART Multiplexer	53
4.4 Safety network configuration	54
4.4.1 Importing Safety Builder Export file	55
4.4.2 Configuring FDM for standalone Safety network	57
4.4.3 Online update of network configuration	59
4.5 OneWireless network configuration	62
4.5.1 Configuring FDM for standalone OneWireless network	63
4.6 Honeywell Experion network configuration	64
4.6.1 Configuring FDM for Honeywell Experion network	64
4.6.2 Configuring FDM for the Experion-integrated Safety network	65
4.6.3 Configuring FDM for Experion-integrated OneWireless network	66
4.7 Configuring Comm DTM network in FDM	67
4.8 Configuring FDM for HART-IP network	68
4.9 Configuring FDM for Honeywell ControlEdge RTU Network	69
4.10 Configuring FDM for Honeywell ControlEdge PLC/HC900 Network	70
4.11 Configuring FDM for Honeywell TPS network	71
4.12 Editing a network configuration	73
4.13 Deleting a network configuration	74
Chapter 5 - Understanding the FDM Client user interface	76

5.1 Online view	77
5.1.1 Network View	77
5.1.2 Device State View	83
5.1.3 Understand the icons	83
5.2 Offline View	85
5.2.1 DD library	85
5.2.2 Offline View Group	86
5.2.3 DTM library	88
5.2.4 FDI Package library	89
5.3 Device notifications	90
5.4 System notifications	91
5.5 Server poll status indication	91
Chapter 6 - FDM role-based user management	92
6.1 Roles and privileges	93
6.2 User management	97
6.2.1 Adding a new user in Classic Server Security	97
6.2.2 Adding a user in Windows Security	98
6.2.3 Modifying user details	100
6.3 Group management	101
6.3.1 Prerequisite to add a group in FDM	101
6.3.2 Assigning policies	102
6.3.3 Mapping Sentinel runtime user to FDM Server OPC Group	102
6.3.4 Adding a Windows group and associating a role	103
6.3.5 Editing roles and privileges of groups	104
6.4 Role management	104
6.4.1 Adding a role	104
6.4.2 Modifying a role	105
Chapter 7 - FDM settings	107
7.1 Customizing General settings	107
7.2 Customizing Network settings	111
7.3 Customizing Health settings	117
7.4 Customizing Security settings	120
7.5 Customizing Audit Trail settings	123
7.5.1 View Audit Trail	126
7.5.2 View Audit Trail from Database	126

7.5.3 View Audit Trail from the File	128
7.5.4 Automatic export and purge of audit trail	129
7.5.5 Manual export and purge of audit trail	131
7.6 Choosing DD/DTM load settings	132
7.7 Customizing the FDT health scan settings	133
7.8 Switching between FDM Servers	134
7.9 Customizing UAS settings	135
Chapter 8 - Device Description file management	137
8.1 Adding a DD file	137
8.2 Deleting a DD file	138
8.3 Synchronizing a DD based Template	138
Chapter 9 - DTM management	140
9.1 Installing DTMs	140
9.2 Managing DTMs that support proprietary protocols	141
9.3 Updating the DTM library	142
9.4 Adding DTMs to the DTM library	143
9.5 Removing DTMs from the DTM library	144
9.6 Upgrading DTM version	144
9.7 Uninstalling DTMs	145
Chapter 10 - FDI Device Package Management	146
10.1 Adding a Package	146
10.1.1 Package validation	147
10.2 Updating a Package	147
10.3 Deleting a Package	147
Chapter 11 - Synchronizing FDM Templates	149
Chapter 12 - About Offline Configuration	150
12.1 Creating a DD offline configuration for a specific device type	150
12.2 Creating a generic DD offline configuration	153
12.3 Creating a DTM offline configuration	155
12.4 Editing an offline configuration	156
Chapter 13 - Downloading bulk offline configurations	159

Chapter 14 - Build networks	164
14.1 Detecting devices on the network	164
14.2 Building FDT networks	165
14.2.1 Saving and restoring FDT networks	168
14.2.2 Resource consumption notifications in the FDT Comm Console	169
14.2.3 Configuring Gateway modules which do not support scan operation	171
14.3 Configuration of PROFIBUS masters	172
14.3.1 Configuration with both Class-I and Class-II Master	172
14.3.2 Configuration with only Class-I master	173
14.3.3 Configuring PROFIBUS Gateway Module in FDM	175
14.4 Building Safety networks	178
14.4.1 SM network redundancy handling in FDM	179
14.5 Building OneWireless networks	180
14.6 Building Experion networks	181
14.7 Building HART-IP networks	184
14.8 Building Honeywell ControlEdge RTU	185
14.9 Building Honeywell ControlEdge PLC/HC900	185
14.10 Building TPS networks	186
14.11 Soft resetting a multiplexer	187
Chapter 15 - Device access control	189
15.1 Explicit locking	189
15.2 Implicit locking	190
15.3 Exclusive locking	192
15.4 Unlock a device	193
15.4.1 Unlocking an explicitly locked device	193
15.4.2 Unlocking a process active device	194
15.4.3 Unlocking an exclusively locked device	198
15.4.4 Unlocking FHM locked device	198
15.5 Lock All/Unlock All	199
15.6 Dynamic Updates to Networks	199
Chapter 16 - FDM Tags	203
16.1 Considerations for FDM tags	209
Chapter 17 - Plant Area View	211

17.1	Structure of the Plant Area View	211
17.1.1	Plant Area View - Edit Mode	211
17.1.2	Plant Area View - View Mode	214
17.2	Creating projects in Plant Area View	218
17.2.1	Adding a group	218
17.2.2	Deleting a group	219
17.2.3	Renaming a group	219
17.2.4	Adding/removing devices	219
17.3	Editing projects in Plant Area View	220
Chapter 18	- Device configuration using DD	222
18.1	Configuring a HART device using DD	223
18.1.1	Monitor the HART device status	228
18.1.2	Graphical data representation	229
18.2	Configuring a FF device using DD	232
18.2.1	Monitor the FF device status	236
18.3	Configuring an ISA100 Wireless device using DD	239
18.3.1	Monitor ISA100 Wireless device status	242
18.4	Executing methods	242
18.5	Editing device properties	244
18.6	Exporting online configuration	246
18.7	Saving history records	247
18.8	Saving an online configuration as an offline configuration using DD	249
18.9	Downloading a DD based offline configuration to an online device	250
18.10	Scanning dynamic parameters	252
Chapter 19	- Device Configuration Using FDI Package	254
19.1	Associating Package	254
19.2	Configure PROFIBUS PA devices using FDI package	256
19.3	Monitor PA device status	261
Chapter 20	- DE device configuration	262
20.1	Configuring a DE device	262
20.2	Editing DE specific system settings	266
20.3	Monitor process variables	267

20.4 Monitor DE device status	269
20.5 Monitor device information	270
Chapter 21 - Comparing configuration	271
Chapter 22 - Device configuration using DTM	279
22.1 Selecting DTM to device	279
22.2 Loading a device using DTM (online mode)	281
22.3 Loading a device using DTM (offline mode)	283
22.4 Configuring a device using DTM	284
22.5 Exporting online configuration using DTM	285
22.6 Saving history records using DTM	285
22.7 Saving an online configuration as an offline configuration using DTM	286
22.8 Downloading a DTM based offline configuration to an online device	287
22.9 Integrating ValveLink DTM for FF devices	287
22.10 PROFIBUS DP diagnostics	288
Chapter 23 - Import and export operations	290
23.1 Import and export device tags	290
23.1.1 Exporting device tags	290
23.1.2 Importing device tags	293
23.2 Import and export audit trail records	294
23.2.1 Exporting audit trail records	294
23.2.2 Importing audit trail records	297
23.3 Import and export offline device configuration	298
23.3.1 Exporting offline device configuration	298
23.3.2 Importing offline device configuration	300
23.4 Import and export device history	301
23.4.1 Exporting device history	302
23.4.2 Importing device history	304
23.5 Importing device configuration history from FDC into FDM	305
23.6 Importing DE device configuration history from MCToolKit into FDM	306
Chapter 24 - Viewing Device History	308
Chapter 25 - Bulk Operations	310

25.1 Saving bulk history	310
25.2 Saving bulk offline templates	314
25.3 Using advanced filter	315
Chapter 26 - FDM dashboard and QuickView	317
26.1 Dashboard	317
26.2 QuickView	317
26.3 Viewing information through dashboard	317
26.4 Viewing information through QuickView	320
Chapter 27 - Display filters	322
27.1 Creating a display filter from the Query View	322
27.2 Creating a display filter from the Device View	324
27.3 Searching for devices using advanced search	326
Chapter 28 - About FDM HART Multiplexer (FHM)	328
28.1 User role privileges	329
28.2 Enabling third party application for write access	329
28.3 Configure a device list	330
28.3.1 Creating a device list	330
28.3.2 Modifying a device list	332
28.3.3 Deleting a device list	332
28.4 Communicating third party application with HART devices	333
28.4.1 Updating the device list	334
28.4.2 Stopping the FHM	335
28.5 Device locks in FHM	336
Chapter 29 - Device documentation-related operations at system/device levels	337
29.1 Attaching device documentation at device-type level	338
29.2 Attaching device documentation at device instance level	339
29.3 Attaching device documentation at system level	339
29.4 Uploading an updated document	340
29.5 Detaching device documents	341
Chapter 30 - FDM application-related operations at system/ device levels	343
30.1 Attaching an application at device-type level	344

30.2 Attaching an application at system level	344
30.3 Launching an attached application	345
30.4 Detaching an attached application	345
Chapter 31 - FDM Operational Restrictions	347
Chapter 32 - Delete Records	350
32.1 Deleting device tags	350
32.2 Deleting offline device configuration	352
32.3 Deleting device history	353
32.4 Deleting PVST reports	355
Chapter 33 - FDM Station Maintenance View	357
33.1 Configuring relationship between Experion Server and FDM Server	358
33.2 Access rights for Station Maintenance View	361
33.3 Starting Maintenance View in Station	361
Chapter 34 - UAS Device View	365
Chapter 35 - FDM Data Backup-Restore utility	367
35.1 Taking a backup of the FDM database	367
35.2 Restoring the database	367
Chapter 36 - FDM diagnosis using Dr. FDM	369
36.1 Capturing diagnostics	369
36.2 Stopping/refreshing the device related services	372

ABOUT THIS DOCUMENT

This document provides information about using the Field Device Manager (FDM) for configuring and modifying the smart field device information using different network communication interfaces. It also covers the various features of FDM, including configuring network communication interfaces, editing device properties, executing device methods, parameter comparison, maintaining history log, importing/exporting tags, history, and offline configuration.

1.1 Prerequisite knowledge

It is expected that you are familiar with the following:

- Field devices
- Network Communication interfaces like Modem, Multiplexer, Experion network, Safety network, OneWireless network, Honeywell TPS network
- HART protocol
- FF protocol
- PROFIBUS protocol
- ISA100 protocol
- Honeywell DE (Digitally Enhanced) protocol
- DTMs
- Basic features of Microsoft Windows user management

1.2 Scope

This document provides procedural steps for performing the tasks related to configuring and monitoring HART, FF, PROFIBUS, ISA100 Wireless, and DE devices using FDM. It also contains information about the following:

- HART 5/6/7 support
- FF, ISA100, PROFIBUS, and DE support
- Device DD/EDDL support for HART, Fieldbus, and ISA100 Wireless devices
- Station Maintenance View
- Windows Authentication
- FDT (Field Device Tool) or Frame Application in FDM
- Device DTM/Communication DTM support
- MUX Monitoring Solution: For more information about MUX monitoring solution, refer to the MUX Monitoring User Guide.
- Gateway DTM support
- Device DTM configuration support for HART and FF devices in Experion Station

- Device DTM Configuration support for PROFIBUS devices in FDT Network
- Device Access Control
- FDM integration with Safety Manager through Universal Safe Modules
- Plant Area View
- FDM integration with OneWireless network
- FDM integration with ControlEdge RTU
- FDM integration with Honeywell TPS (Total Plant Solutions) network (for DE devices)
- FDM PVST Planner

1.3 Terms and definitions

Term	Definition
Comm DTM	Communication DTM
ControlEdge RTU	Remote Terminal Unit
COTS	Commercial-off-the-Shelf
CSV	Comma Separated Variable
DD	Device Description Files (These files are in binary format. This contains the device description of HART field devices.)
DDL	Device Description Language
DE	Digitally Enhanced
DocTool	Documentation Tool
DTM	Device Type Manager
EDD	Electronic Device Description Files (These files are in binary format)
EDDL	Electronic Device Description Language
ESD	Emergency Shutdown
EPKS	Experion Process Knowledge System
ESVT	Experion Server-TPS
EST	Experion Station-TPS
FCH	Field Communication Handler
FDC	Field Device Configurator
FDM	Field Device Manager
FF	Foundation Fieldbus
FHM	FDM HART Multiplexer
FIM	Fieldbus Interface Module
GCI	Gateway General Client
HART	Highway Addressable Remote Transducer
HCF	HART Communication Foundation
HMI	Human Machine Interface

Term	Definition
HM	History Module
HoP	HART over PROFIBUS
HPM	High-Performance Process Manager
IDE	Integrated Development Environment
IOTA	Input/Output Termination Assembly
ISA	International Society of Automation
LCN	Local Control Network
MC Toolkit	Multi Communication Toolkit
MODEM	Modulator and Demodulator
MUX	Multiplexer
NIM	Network Interface Module
OPC	OLE for Process Control
PDA	Personal Digital Assistant
PGM	PROFIBUS Gateway Module
PAV	Plant Area View
PMIO	Process Manager I/O
PROFIBUS DP	Process Field Bus Decentralized Peripherals
PROFIBUS PA	Process Field Bus Process Automation
PLC	Programmable Logic Controller
PVST	Partial Valve Stroke Testing
RCI	Remote Communication Interface
RUSLS	Remote Universal Safe Logic Solver
SM	Safety Manager
SDC	Smart Device Configurator
STIM	Smart Transmitter Interface Module
TPS	Total Plant Solutions

Term	Definition
TPS DocTool	TPS Documentation Tool
UAS	Uniformance Asset Sentinel
UCN	Universal Control Network
UIO	Universal Input/Output
UIO-2	Universal Input/Output Phase 2
USIO	Universal Safe I/O
WDM	Wireless Device Manager

1.4 References

The following list identifies all documents that may be sources of reference for material discussed in this publication.

Document Title	Doc ID
FDM Installation and Configuration Guide	EP-FDM-02511
FDM PVST Planner User's Guide	EP-FDM-15511
HART I/O Implementation Guide in Experion Documentation	EPDOC-XX51-en-511A
Series C I/O User's Guide in Experion Documentation	EPDOC-X126-en-511A
Control Building User's Guide in Experion Documentation	EPDOC-XX19-en-511A
MUX Monitoring Solution User's Guide	EP-FDM-14511
Integrated Experion-TPS User's Guide	EX23
Smartline Transmitter Integration manual	PM12

1.5 Glossary

This section defines the terms and acronyms used in the FDM user's guide.

Term	Definition
B	
Build Network	Feature to populate a network after starting or re-starting the FDM Server, or to force an update of actual device status for any reason.
C	
Connected Device	A device that is physically connected to FDM through the network communication interface.
Commissioned Device	A device that is registered with FDM and available for use.
ControlEdge RTU	ControlEdge RTU is modular and scalable controller capable of all remote automation and control applications.
Network Communication Interface	A device that helps to communicate between FDM and the field devices. Example: RS-232 HART Modem, Honeywell HART DE Modem, RS-485 HART Multiplexer, and Honeywell Experion PKS Multiplexer.
D	
Database	A set of related files that is created and managed by a database management system (DBMS).
Decommissioned Device	A device that is permanently disconnected from the field.
Device	An instrument that measures or controls the process variables.
Device Configuration	A set of parameters specific to the device and that needs to be configured.
Device Description (DD)	A file that contains the device information such as commands and parameters. Device vendors develop DD file for each device they develop. These DDs are required to qualify the HART device against the configuration tool. The DD files can be identified with the help of its manufacturer ID, device type, and device version number. A set of instructions written in the HART device description language that defines the parameters, commands, and methods that a host application uses to communicate with a HART field device.

Term	Definition
Device History	A single time-stamped snapshot of all parameters from a device stored in the FDM database. Any number of device histories can be stored for a device.
Documentation Tool	The Documentation Tool (DocTool) is a TDC 3000x Engineering Personality function that allows you to retrieve data from the following sources. Online databases of LCN nodes Process-connected devices like UCN, Data Highways, and so on. Files from the History Module and removable media
E	
Experion Integrated Safety Network	It refers to Experion network along with Safety Manager with Universal Safe Modules in which Safety network is integrated with Experion to configure HART devices.
Experion Server-TPS (ESV-T)	ESV-T is an Experion Server-T node, which is connected to both Experion and LCN systems and primarily used for accessing the TPN data. It provides support for initial Experion configuration and also supports functions such as collection, archiving, and reporting TPN data.
Experion Station-TPS (ES-T)	An Experion Station – TPS (ES-T) provides a common operator interface for both TPS and Experion. In addition, it provides the Native Window application that emulates a Universal Station and optionally supports GUS displays. The Native Window and GUS runtime connect to a locally installed LCNP (LCN processor) board, providing a user interface with access to all TPS/LCN operations, engineering, and maintenance functions.
H	
HART Protocol	Highway Addressable Remote Transducer is an industry standard protocol for digitally enhanced 4-20 mA communications with field devices.
HART Device	A device that communicates information using the HART protocol.
HART DE Modem	HART DE Modem is a Honeywell product that communicates with HART protocol devices.
HART Modem	A HART Modem is a more general term for third party single-purpose modems that communicate with HART

Term	Definition
	devices.
Hardware Multiplexer	Hardware Multiplexer refers to hardware which enables the communication to multiple HART devices though same physical wiring to the system.
High-Performance Process Manager	High-Performance Process Manager is a process-connected device on the UCN that provides regulatory control and sequence operations.
Honeywell DE Protocol	The Smartline Transmitter can be set in Digital Enhanced (DE) mode and it offers bidirectional communication (read/write capability) between the system and the transmitter. In DE mode, it is possible to monitor and manipulate the transmitter from the Universal Station.
F	
FDM Client	Client is a workstation that runs FDM program and accesses the server for device information.
FDT Comm Console	User interface to configure the Communication and Gateway DTMs, and to build the complete network using only DTMs.
FDM Server	It refers to the node that runs FDM program and allows multiple clients to access it for the device information.
FF Protocol	Foundation Fieldbus is an enabling technology for dynamically integrating dedicated field devices with digitally based control systems. It defines how all smart field devices are to communicate with other devices in the control network.
FIM	FIM serves as the bridge between the control environment and the smart device control functions. It supports both publish/subscribe and the client/server communication methods to communicate with fieldbus function blocks.
I	
IOTA	IOTA (Input Output Termination Assembly), is an Experion term for I/O backplanes used with Series C and Safety Manager Universal Safe I/O.
K	
K2LCN	K2LCN is a LCN module printed circuit board that contains a 68020 microprocessor, memory, and LCN interface.

Term	Definition
K4LCN	K4LCN is a LCN module printed circuit board that contains a 68040 microprocessor, memory, and LCN interface.
L	
Local Control Network	The Local Control Network (LCN) is a coaxial and a fiber optic network that provides the data path for communication between the TPS network-based control modules and TPS system nodes.
Locate Device	An option to find the devices in the FDM network.
M	
Method	A Method is a script or procedure embedded in a Device Descriptor (DD) file which executes a series of steps to simplify a task for the end user. Methods can range from very simple to exceedingly complex.
Modem (Modulator – Demodulator)	A device which converts a signal of one type to other and vice-versa. In context of FDM, it refers to a HART modem which enables communication to a HART device through RS232/USB interface on PC. A modem is an analog-to-digital and digital-to-analog converter.
Multiplexer	Multiplexer is a communication device that multiplexes (combines) several signals for transmission over a single medium. The multiplexers are called as “MUX.”
Multiplexer Network	A network that connects several multiplexers to connect to multiple field devices.
MUX Monitoring	A unique FDM option that makes non-Experion HART device information available to the Experion system.
N	
NE107	NAMUR (international process industry end-user association) recommendation for self- monitoring and diagnosis of field devices.
NIM	The Network Interface Module (NIM) provides the interface between the Local Control Network and the Universal Control Network (UCN) in TPS system.
Offline Configuration	Editing and saving the device parameter values, when the device is not loaded. The changes in offline configuration can be transferred to the device using offline download.

Term	Definition
Offline Template	FDM template representing the parameters of the device. It is used for offline configuration and the device parameters are initialized with default values.
OPC Client	An OPC client requests and uses the data provided by an OPC Server.
OPC Server	An OPC server is an application, which collects data, generally directly from a physical device, and makes it accessible through the OPC interface.
P	
Parameter	In the context of a field device, a single value or measurement contained in that device.
Process Variable (PV)	The primary measured process parameter of interest in a field devices, such as temperature, flow, or level.
Protocol	Protocol is a set of rules that govern transmitting and receiving of data. The protocol is intended to provide a reliable, transaction oriented communication path to and from slave devices such as field instruments, for digital data transfer.
PLC	PLC is modular and scalable controller capable of flexibly interface with inputs and outputs devices at industrial scale.
R	
Registered Device	A registered device is one that has been tested and registered with a protocol-specific standards organization, such as the Fieldbus Foundation. FDM product is shipped with a library of DD files that are registered.
S	
Spare Device	A device that is connected with FDM, but not assigned for operation. These devices appear in the Spare Device folder.
Series C I/O	Series C I/O modules are an expanding family of traditional and special function input/output signal interface devices. These I/O modules share the same form factor as the C300 Controller and reside on the same type of common mounting system as other Series C components.
Safety Builder	Safety Builder is the client used for configuring Safety

Term	Definition
	Manager network (SMs, IOTAs, and Channels).
Safety Network	Safety Network with Universal Safe Modules (RUSIO/RUSLS).
Standalone Safety Network	It refers to a network having Safety Manager with Universal Safe Modules without Experion configured as standalone to configure HART devices.
Smart Transmitter Interface Multivariable Input/Output Processor	STIM IOP is an I/O Processor in the Process Manager (PM) to which smart device transmitters can be connected in Honeywell TPS network.
T	
Tag	Tag is the label that is assigned to each device to represent the device type, area under which the device is connected.
U	
UCN	The communication from the control room to the controllers (such as PM, APM, HPM, LM, and SM) is established through a coaxial cable system. This system and its protocol are designated as the Universal Control Network (UCN).
Universal Safe Modules	Common classification used for USIO (Universal Safe I/O) or RUSLS (Remote Universal Safe Logic Solver).
USB Modem	A network communication interface that establishes the physical connection between the system and the devices. The USB Modem helps to configure a single device at a time.
V	
Vendor	Manufacturer of the field devices.
W	
Workstation	Refers to the PC that runs the FDM tool.

INTRODUCTION TO FIELD DEVICE MANAGER

Field Device Manager is a complete instrument asset management system that can range from a single self-contained server/client node to a very distributed architecture, such as the Experion system. In fact, when it is installed as part of an Experion system, there are multiple nodes that are shared in common, such as the Experion Flex Station. FDM is used for configuration, commissioning, and maintenance of smart field devices based on HART, PROFIBUS, Foundation Fieldbus, ISA100 Wireless, and Honeywell DE (Digitally Enhanced) protocols.

FDM inherently supports Experion-connected devices along with non-Experion networks. FDM supports a large number of devices through FDM Clients connected to multiple and distributed FDM Servers.

FDM conforms to industry open standards for HART, PROFIBUS, Foundation Fieldbus, and ISA100 Wireless protocols and does not require additional files or programming to support devices or to access device-specific features. This includes unrestricted use of both Device Description (DD) and Device Type Manager (DTM) technologies as provided by the device vendors. FDM also supports Honeywell's own Digitally Enhanced (DE) protocol devices connected to TPS systems. FDM uses a unique remote communication infrastructure that allows widely distributed devices to communicate over a local or a wide area network, providing anytime, anywhere access in the plant environment. FDM does not require engineering or database building. Once the communication networks are configured, FDM automatically detects the smart devices and adds them to the database. This saves considerable time for commissioning, troubleshooting or performing routine maintenance.

2.1 Supported protocols

- HART devices through Experion and Safety Manager, Safety Manager SC HART I/O
- HART devices through non-Experion-connected RS-485 HART multiplexers and modems
- HART devices and ISA 100 wireless devices through Honeywell RTU network
- HART devices, Wireless HART devices, and ISA 100 wireless compliant field devices through OneWireless network
- PROFIBUS devices using PROFIBUS communication and Device Type Managers (DTMs)
- HART devices connected to PROFIBUS networks through HART-over-PROFIBUS gateway devices
- Foundation Fieldbus devices through Experion-connected Fieldbus I/O
- HART devices through HART-IP network
- Honeywell DE (Digitally Enhanced) devices through Honeywell Total Plant Solution (TPS) network

2.2 Enhancements to FDM R511

In FDM R511, the following enhancements were added:

- Platform enhancement to support compatibility with Experion R510 and R511.x.
- Auto rebuild network.
- Auto export and purge of audit trail records.

FDM R511 is also enhanced to support the following features for FDM and UAS Integration:

- HART diagnostics bits in addition to the command 48 for HART devices.
- Communication fault for device connection and disconnection status.
- Rebuild network in FDM when instruments are monitored in sentinel.

2.2.1 Enhancements in FDM R511.2

Starting with R511.2, FDM has the following enhancements:

- PUIO
- UIO-16
- UAS integration to support monitoring for 10K HART instruments

2.2.2 Enhancements in FDM R511.4

Starting with R511.4, FDM has the following enhancements:

- HART configuration from FDM to EHPPM HART IOPs
- C300- Series A HART IO Modules
- Support for HC900

2.3 Enhancements in FDM R501

Starting with R501, FDM has the following enhancements:

- Support for ControlEdge UOC
- Support for Safety Manager SC
- IAMS with Instrument Sentinel integration
- Enhanced user experience for offline configuration of HART devices

2.4 Enhancements in FDM R500

Starting with R500, FDM has the following enhancements.

- PROFIBUS Gateway Module – Native integration
- Support for HART over PROFIBUS (HoP) devices
- HART EDDL enhancements
- Support for PROFIBUS EDDL
- Station Maintenance View
- Support for UIO-2
- OneWireless R300 integration
- Honeywell ControlEdge RTU integration
- Support for Uniformance Asset Sentinel device view

2.5 Enhancements in FDM R450

In FDM R450, the following enhancements were added.

- FDM integration with TPS (Total Plant Solutions) network to manage Digitally Enhanced (DE) devices
- through Experion-T nodes like ESVT (Experion Server-TPS) and EST (Experion Station-TPS)
- Support for importing and exporting MCToolKit DE device history

ATTENTION

You can only export MCToolKit DE device history for the records which were imported to FDM from MCToolKit.

- Support for PVST (Partial Valve Stroke Testing) Planner, which supports scheduling Partial Valve Stroke Tests of selected HART ESD devices. This feature increases confidence in safety instrumented systems by periodically testing safety shutdown valves. The feature also helps in automatically testing safety and control valves to detect failure modes. Testing can be done automatically, semi-automatically, or manually, with test results stored for documentation purposes.

For more information on PVST Planner, refer to the FDM PVST Planner User's Guide.

2.6 Enhancements in FDM R440

In FDM R440, the following enhancements were added.

- Support for parameterization and maintenance of FF devices using DD/EDDL
- FDM integration with the OneWireless network to manage ISA100 Wireless devices and HART devices connected through the OneWireless adapters
- FDM integration with RTU2020 to manage the HART devices connected to the RTU2020 using HART-IP network
- Improved support for EDDL

2.7 Enhancements in FDM R430

In FDM R430, the following enhancements were added.

- Support for HART 7 protocol
- Integration with Safety Manager through Universal Safe Modules to maintain the HART devices connected to safety systems
- FDT Comm Console to manage the networks and devices integrated in FDM through the FDT Communication and Gateway DTMs
- Support for Experion Series 8 HART I/O modules
- Provision for device access control, where write access to devices can be configured with password protection
- Plant Area View feature, which allows you to group the available devices based on their geographical locations
- Soft reset of a multiplexer feature, which facilitates resetting the multiplexer internally and removes the invalid device status if any, on the multiplexer device status page

- Support for Series C Universal Input/Output module. This module is used for viewing the HART devices connected to the HART enabled channels of UIO. The UIO has 32 configurable input or output channels. Each channel can be configured as an analog input or an analog output. All FDM features supported for the HART I/O are also supported for the UIO module.

2.8 Support for Safety Manager SC

FDM solution provides the capabilities of management of HART devices connected to Safety Manager. The Safety Manager SC is new offering which provide a cost effective/competitive, scalable, flexible and suitable SIL2/SIL3 Safety solution. The FDM R511 needs to support the management of HART devices connected to Safety Manager SC HART IO modules (USIO).

2.9 FF-EDDL support in FDM

FDM communicates with FF devices connected to Experion FIMs using DD files or vendor-supplied DTMs. You can use the primary features like save history, compare configurations, detailed view of advanced diagnostics during maintenance. For a list of FDM tasks that you can perform during maintenance after commissioning an FF device in Experion, see the following table.

For a complete list of supported features, see FDM features and supported devices FDM features and supported devices.

- Detailed view of advanced diagnostics: If you configure any alarm in Experion, the detailed parameters and bit-level information can be viewed in FDM device status page from the FF device configuration page. However, in Experion Station, you can view only the alarms.

2.10 ISA100 Wireless support in FDM

FDM communicates with ISA100 Wireless devices connected to WDMs using DD files. You can use primary features like save history, compare configurations, diagnostics during maintenance. For a list of FDM tasks that you can perform during maintenance after commissioning an ISA100 Wireless device using the OneWireless User Interface, see the following table.

For a complete list of supported features, see FDM features and supported devices FDM features and supported devices.

2.11 DE support in FDM

FDM communicates with Digitally Enhanced (DE) devices connected to the TPS system using the Honeywell TPS network. You can use primary features like save history, compare configurations, and diagnostics during maintenance. For a list of FDM tasks that you can perform during maintenance after commissioning TPS-connected DE devices in the TPS system, see the following table.

For a complete list of supported features, refer FDM features and supported devices.

The following DE device types are qualified with FDM.

- ST 3000 Pressure Transmitters
- STT3000 Temperature Transmitters
- ST 800 Pressure Transmitters
- ST 700 Pressure Transmitters
- Magnew 3000 Magnetic Flow Meter
- Magnew 3000 PLUS Magnetic Flow Meter
- SMV 3000 Smart Multivariable Transmitter

ATTENTION

Import history is not supported for SFM (Yamatake Magnetic flow meter) devices because MCToolkit record does not have point name information, Therefore, FDM is unable to identify the correct node to attach MCToolkit History record while importing history.

	FF-EDDL	ISA100 Wireless	DE
FDM tasks supported during Maintenance			
Edit the parameters and download to the device	✓	✓	✓
Calibrate the device or run other procedures using Methods	✓	✓	NA
Save the history and use this for troubleshooting where an alarm is displayed	✓	✓	✓
Compare the current history with the previous saved history	✓	✓	✓
Troubleshoot the devices based on the device health status	✓	✓	✓

2.12 FDM functions and features

FDM Server and FDM Client allow communication across the network throughout the plant area. It is possible to remotely accomplish device-monitoring, configuration, and setup from the operator center, maintenance shop, or relay room.

The key functions and features of FDM are listed here.

Advanced search

FDM allows you to easily locate specific devices in the network view using this feature. For more information, refer to the section [“Searching for devices using advanced search”](#).

Audit trail

FDM can maintain an audit log of predefined user actions, custom user-actions, and some implicit actions performed on the device, describing the action made, the user and the timestamp for each event. It can be viewed based on various filter criteria. This feature meets 21 CFR-11 standards. For more information, refer to [the section “Viewing audit trail”](#).

Dynamic network update

After the network is built for the first time, FDM automatically discovers any newly connected or disconnected nodes in the network view. For more information, refer to the section [“Dynamic network update”](#).

Bulk operations

Using this feature, you can create history records and offline templates for a large number of devices simultaneously. For more information, refer to the section [“Bulk operations”](#).

Client-Server architecture

FDM supports a distributed client-server architecture in which different components may be installed on different systems. In addition, it supports a multi-client, multi-server architecture, where multiple clients can connect to the same server and one client can connect to any server.

Compare configuration

FDM supports the compare configuration feature for DE devices and DD/EDD based devices. You can either compare the device data of two different devices belonging to the same device type or the device data of the same device history. For more information, refer to the section [“Comparing configuration”](#).

Device Access Control

FDM supports the following settings that are used for enhancing the security to the devices, with respect to “write access” to them.

- Automatic lock of devices as they are discovered on the network
- Password protection for access control of devices that are connected to a network
- Automatic lock of an unlocked device after a specified time period
- Exclusive access to unlocked devices
- Manual lock/unlock of all the devices connected to a network/hierarchy

All these settings can be configured individually. Hence, you can customize this function to your specific plant needs. For more information, refer to the section [“Device access control”](#).

Device history

FDM enables you to view the historized device configuration and compare it against historized or live configurations. For more information, refer to the section [“Viewing the device history”](#).

Device configuration

FDM supports configuration of HART and FF devices through DD and FDT-DTM technologies. It also supports configuration of ISA100 Wireless devices through DD, and PROFIBUS devices through FDT-DTM technology. DE device configuration is supported in FDM using the template-based approach. FDM provides an option to view the current configuration settings and downloads configurations from FDM to devices in the field.

Device documentation

FDM allows you to add documents such as user manuals and P&ID diagrams to the FDM database for quick reference. Documents associated with a device are easily invoked from the FDM Client. For more information, refer to the section [“Device documentation-related operations at system/device levels”](#).

Display filter

FDM enables you to create filters using various filtering criteria. Using this you can customize the view of the network. For more information, refer to the section [“Display filters”](#).

Dashboard

Using this feature, you can view all types of information related to the FDM Client, FDT Comm Console, devices, RCIs, gateways, networks and operations at a single place, and you gain quick, easy access to it. For more information, refer to the section [“Viewing information through dashboard”](#).

Experion redundancy support

FDM supports redundant Experion network connectivity. When required Experion services are unavailable, FDM automatically switches over to the redundant partner. No action is required to re-detect devices.

FDM integration with Experion

When integrated with Experion, FDM supports configuration, method execution and monitoring of the following devices.

- HART devices connected to a Series C I/O module, PMIO module, 1756 HART I/O module, S8 HART I/O module, Series C UIO module, Series C UIO-2 module, or WDM
- FF devices connected to FIM2, FIM4, and FIM8 modules
- ISA100 Wireless devices connected to WDM
- PROFIBUS devices connected to PROFIBUS Gateway Module

FDM integration with Experion LS

When integrated with Experion LS, FDM supports configuration and monitoring of HART devices. Refer to Experion LS R311 Product documentation for more information.

FDM integration with OneWireless network

FDM supports configuration and monitoring of ISA100 Wireless devices, and HART devices connected through OneWireless adapters that are connected to WDM using the OneWireless network.

Refer to OneWireless R220 documentation for more information.

FDM integration with Safety Manager through Universal Safe Modules

FDM supports configuration and maintenance of HART devices connected to Safety Manager through Universal Safe Modules (USIO/RUSLS). However, HART channels connected to local I/O network of SMs are supported through multiplexer network configuration in FDM.

FDM integration with HART-IP gateways

FDM supports configuration and maintenance of the HART devices connected to third-party HART-IP gateways over the HART-IP network.

FDM integration with Honeywell ControlEdge RTU

FDM supports configuration and maintenance of the HART and ISA devices connected to Honeywell ControlEdge RTU over the Honeywell ControlEdge RTU network.

FDM integration with Honeywell ControlEdge PLC/HC900

FDM supports configuration and maintenance of the HART devices connected to Honeywell ControlEdge PLC/HC900 over the ControlEdge PLC/HC900 network.

FDM integration with Honeywell TPS network

FDM supports configuration and maintenance of smart transmitter devices such as DE (Digitally Enhanced) devices connected to the Honeywell TPS network through Experion-T nodes like Experion Server-TPS (ESVT) or Experion Station-TPS (ES-T).

Refer to the Integrated Experion-TPS User's Guide in the TPN/TPS book set for more information.

FDM PVST Planner

FDM supports scheduling and executing PVST for different valves using FDM PVST Planner. You can perform the following using FDM PVST Planner.

- Create logical groups of devices and configure/assign a schedule to a group
- View the execution status of the PVST for the current set of valves using Execution view
- View/export the PVST status for the selected dates using Reports view
- Receive alerts/notifications for PVST status and schedule. For more information about PVST Planner, refer to the FDM PVST Planner User's Guide

Health scan on the device

FDM indicates device health status without opening the device configuration for the following devices. The device health is displayed when the device is discovered for the first time during the build network operation. A healthy device is indicated in green and if a device is found unhealthy, is indicated in red.

- HART devices connected to RS-485 HART multiplexer, Modem, Experion, HART-IP network, ControlEdge PLC/HC900, ControlEdge RTU
- HART and PROFIBUS devices connected to the COMM DTM interface (FDT network)
- FF, PROFIBUS devices connected to the Experion network
- HART devices (connected through OneWireless adapters/Wireless HART adapters), ISA100 Wireless devices, and Wireless HART devices connected to the OneWireless network
- DE devices connected to the Honeywell TPS network

Import and Export operations

FDM enables you to import and export device tags, audit trail records, offline configurations, and device history. You can also import MCToolKit DE device history from MCToolKit to FDM. You can also export MCToolKit DE device history, which was imported to FDM only from MCToolKit. For more information, refer to the section [“Import and export operations”](#).

MUX Monitoring Solution

FDM MUX Monitoring Solution allows Experion to access alarms and events from HART devices associated with FDM connected RS-485 HART Multiplexer networks, Experion-integrated Safety network, and Experion-integrated OneWireless network.

Offline configuration

FDM enables you to configure a set of device parameters without the need for a device to be available physically. These configurations are stored in the database or in separate files, and they can be downloaded to the devices when they are physically connected. This offline configuration can later be used for configuring an online device. For more information, refer to the section [“About Offline Configuration”](#).

Plant Area View

Using this feature, you can group the available devices based on their geographical locations or logical process associations, such as by unit or area. In addition, you can easily identify a device location and view, monitor the device directly by its location. The device grouping strategy followed in Plant Area View follows the ANSI/ISA-88.01-1995 standards. For more information, refer to the [section “Plant Area View”](#).

QuickView

Using this feature, you can view the information related to device status, device information, network information, device state information, lock state, and attached documents for all connected and disconnected devices. This information is available at a single place for easy access.

Role based user management

FDM provides robust role-based user management. You can create users with two mechanisms - FDM Classic Server Security and Windows Security. For more information, refer to the section “FDM role- based user management”.

Station Maintenance View

The Station Maintenance View feature allows access to the complete FDM device configuration from an Experion Flex Station point detail display. This unique capability enables operators and maintenance personnel to query device information and to take required actions. For more information, refer to the section “FDM Station Maintenance View”.

Support for UAS

Asset Sentinel integration with FDM provides Sentinel users with the required privilege with the Device View to view parameters and diagnostic information for HART devices. This solution provides a read-only view of field instruments connected to the Experion network only.

The data presented is dynamic and reflects current values in the devices. For configuration tasks, FDM Client is still required. The view provided by Asset Sentinel includes parameters and diagnostics data. It however, does not display images or EDD constructs that the FDM Client provides.

Support for device description files

FDM uses original unmodified device vendor DDs and EDDs to provide full configuration and setup for all Foundation Fieldbus registered (FF) devices and HCF registered HART devices. DDs or EDDs are available from the device vendors.

Third party application integration

The FDM HART Multiplexer (FHM) option allows third-party tools such as valve diagnostic applications to communicate with the HART devices connected to any network. For more information, refer to the section “About FDM HART Multiplexer (FHM)”.

Windows authentication® and Single Sign On

System Administrators can associate an existing Windows user to a particular role. Therefore, a System Administrator need not create a user using the FDM User Management utility. Single Sign On allows you to skip the login screen if you are logging on as an authorized Windows user.

2.13 FDM features and supported devices

The following table summarizes the functions and features of FDM with respect to each open device protocol supported - HART, PROFIBUS, FF, ISA100, and DE. It also presents a comparison of features as applied to DD/EDDL vs. FDT-DTM technologies.

FDM features	HART (Wired/Wireless)		PROFIBUS		FF		ISA100	DE
	DD	DTM	DTM	Package	DD	DTM	DD	
Audit trail	✓	✓	✓	✓	✓	✓	✓	✓
Save history ³	✓	✓	✓	✓	✓	✓	✓	✓
Offline configuration (template) ⁴	✓	✓	✓	✓	✗	✓	✗	✗
Bulk save history ⁵	✓	✗	✗	✓	✓	✗	✓	✓
Download offline configuration	✓	✓	✓	✓	✗	✗	✗	✗
Bulk offline templates	✓	✗	✗	✓ for HoP devices only	✗	✗	✗	✗
Bulk offline download	✓	✗	✗	✓ for HoP devices only	✗	✗	✗	✗
Device configuration (online)	✓	✓	✓	✓	✓	✓	✓	✓
Device health scan	✓	✓	✓	✓	✓	✓	✓	✓
Compare device configuration	✓	✗	✗	✓ [HoP & PA devices only]	✓	✗	✓	✓
Station Maintenance View	✓	✓	✓	✓	✓	✓	✓	✗
Import and Export of offline configuration	✓	✓	✓	✓	✗	✓	✗	✗

FDM features	HART (Wired/Wireless)		PROFIBUS		FF		ISA100	DE
	Advanced search	✓	✓	✓	✓	✓		✓
Attach documents to devices	✓		✓	✓	✓		✓	✓
Display filters	✓		✓	✓	✓		✓	✓
Connects to Experion	✓		✓	✓	✓		✓	NA
Connects to MUXs, modems, Safety Manager, and OneWireless Adapter	✓		NA	NA	NA		NA	NA
Import and Export (tags, audit trail, device history)	✓		✓	✓	✓		✓	✓
Import and Export MCToolKit DE device history	NA		NA	NA	NA		NA	✓
Dynamically device update ²	✓		NA	✓	✓		✓	✓
MUX monitoring ¹	✓		NA	NA	NA		NA	NA
Third-party application integration (FHM)	✓		NA	✓ [HoP only]	NA		NA	NA

ATTENTION

Note 1: Not supported for RTU2020.

Note 2: Not supported for Safety Manager Universal Safety I/O.

Note 3: The Save History for DTMs works only if the vendor has designed the DTM to perform the Save History operation.

Note 4: The Save Offline configuration (template) for DTMs works only if the vendor has designed the DTM to perform the Save Offline Configuration operation.

Note 5: Bulk Save History available only for PROFIBUS PA devices and HoP devices (excludes PROFIBUS DP devices) connected under PGM.

2.14 Supported technologies

FDM supports the following technologies to configure, commission, and maintain field devices.

- Device Description files
- FDT-DTM
- FDI

2.14.1 Device Description files

Devices that are supported through DD/EDDs are capable of providing functions and features far beyond the basic task of providing a process input or accepting a control output to manipulate process conditions.

Device vendors create a Device Description (DD) or (EDD) for every device that describes the functions and features specific to that device. The DD and EDD also contain information essential for the successful configuration and calibration of the device. FDM provides full support of HART, Foundation Fieldbus and ISA100 Wireless devices by interpreting DD and/or EDDL files. It utilizes all device features, irrespective of the vendor or manufacturer, the device version, and the release date. Support for DD and EDDL files includes device-specific commands, device-specific configuration, and diagnostics and status information.

Device Description (DD) file

It contains the electronic descriptions of device parameters and functions needed by a host application to communicate with devices. They are written according to the DD language specification. DD files are device-specific and are developed and made available by device vendors. Ensure that you use the latest DD for a particular device type and revision. Unlike other configuration tools, FDM does not require custom DD to be developed for the tool itself.

ATTENTION

FDM supports all devices that have their DDs registered with the HART Communication Foundation (HCF) and Fieldbus Foundation. FDM also supports currently available ISA100 standard and continues to follow the emerging standard.

Electronic Device Description Language (EDDL)

Representing an extension to the DD language specification, EDDL provides clear and structured text description that specifically describes the field device data to host systems. It includes the following enhancements.

- Graphical elements and waveforms
- Standardized access to historic measurements and device performance information
- Vendor-specified organization of device parameters
- Enhanced tools for high-level information display and control system use

EDDL enhancements provide for an improved user interface compared with the DD specification. It further standardizes the user interface for managing intelligent devices and eliminates the need for Windows resource files, supplemental files, and other modifications.

Methods execution

Methods are predefined sequences of steps that can be executed by a host. The device vendors develop these methods and supply them as a part of the device's DD file/EDD file or device DTM. Some examples of methods are:

- Commanding the device to complete a calibration operation
- Commanding an advanced diagnostic test procedure
- Executing tests to gather information on device operation

FDM supports the following:

- Method execution through DD/EDD file or device DTM for HART/FF protocol
- Method execution through device DTM for PROFIBUS protocol
- Method execution through DD/EDD file for ISA100 protocol

2.14.2 FDT-DTM

FDM supports the Field Device Tool (FDT)-Device Type Manager (DTM) technology to configure HART and PROFIBUS devices.

Field Device Tool is a standard interface defined by the FDT group for integration with field devices. Host applications like FDM use it to integrate with devices and provide configuration and maintenance capabilities. Any host application which implements the FDT-DTM technology is referred to as an FDT Frame.

It has three primary functions:

- Interface with the Device DTM for device configuration
- Interface with the Gateway and Communication DTMs to communicate with devices
- Manage the DTM Catalog

Device Type Manager: This is analogous to a device driver that is developed by device vendors for a particular device type. DTM enables the usage of devices in all the asset management and device configuration software like FDM, with the help of the FDT-DTM technology.

The DTM provides:

- Graphic User Interface for device configuration
- Device configuration, calibration, and management features for a device

There are three types of DTMs:

- **Device DTM:** Represents a field device and contains the details of the user interface, device parameters, DTM documentation for configuration and calibration of devices and diagnostic functions for the device.
- **Communication DTM:** A Communication DTM is a software that represents a communication device, such as an Ethernet to PROFIBUS gateway. Its salient features are listed here:

- Is provided by the communication device vendor.
 - Can be loaded in an FDT Frame in a host application.
 - Is responsible for the communication between the FDT host application and the physical communication device.
 - Implements the standard interfaces specified by the FDT Group.
 - Allows for browsing the complete network and to configure to work with a different network type.
 - Has its own UI, which allows for configuring the communication device for proper communication with the network.
 - Has its own installations that take care of registering the DTMs.
- **Gateway DTM:** The Gateway DTM is a software that represents a gateway device. Its salient features are listed here.
 - Uses the communication DTMs or other communication drivers for communicating with the devices. Requests from devices connected to the Gateway are sent to the Gateway DTM, which is then sent to the Communication DTMs.
 - Has its own UI, which allows for configuring the Gateway device for proper communication with the network.
 - Has its own installations that take care of registering the DTMs.

For example, HART-over-PROFIBUS Gateway DTM represents the HART-over-PROFIBUS Gateway device that is used to connect HART devices on PROFIBUS networks.

ATTENTION

PROFIBUS PA devices can be configured in FDM through DTMs and FDI packages, while PROFIBUS DP devices can be configured only using DTMs.

2.14.3 FDI

FDI technology combines the advantages of FDT and EDDL to provide a simple, effective solution to configure, commission, diagnose, and calibrate simple and complex devices.

The FDI package for any model or type of device is provided by its manufacturer. The core of the FDI package is the Electronic Device Description (EDD) that provides a complete description of the device. The EDD contains device-specific information that is used for interpreting the responses received from the device. FDI device packages are able to be processed in both FDI hosts and FDT2 frame applications. You can add and delete FDI packages from the client. The FDI device package feature is supported for PROFIBUS PA profile v3.01 and later versions.

In the FDM R500 release, FDM uses only EDD content in the package for PROFIBUS. Future releases may have full support for all FDI package specifications.

2.15 Supported protocols

FDM supports the following protocols to configure, commission, and maintain field devices.

- HART
- Foundation Fieldbus
- PROFIBUS
- ISA100
- Honeywell Digitally Enhanced (DE)

2.15.1 HART protocol

In a process control environment, field devices such as pressure, level, and temperature transmitters and valve positioners provide the physical connection to the process. These devices allow the control system to monitor and manipulate process conditions. The smart field devices, such as HART (wired) devices, HART wireless devices configured on the OneWireless network maintain a database of process configuration, identification, and diagnostic information in memory. These devices use the HART digital protocol (governed and maintained by the FieldComm Group) to communicate with the control and asset management system. The FieldComm Group has a membership of over 150 vendors (including Honeywell), offering over 500 different HART devices. HART is an open smart field device protocol available for use by all member companies.

For more details about HART and HCF, visit the website at:

<https://www.fieldcommgroup.org/technologies/hart>.

FDM supports HART devices conforming to HART 5.x, 6.x and 7.x (wired and wireless) versions of the HART protocol. It also supports HART devices connected to a number of I/Os, using both DDs and DTMs.

2.15.2 Foundation Fieldbus protocol

Foundation Fieldbus is an enabling technology for dynamically integrating dedicated field devices with digitally based control systems. It defines how all smart field devices must communicate with other devices in the control network. The technology is based upon the International Standards Organization's Open System Interconnection (OSI) model for layered communications. Foundation Fieldbus is a sophisticated, object-oriented protocol that uses multiple messaging formats and allows a controller to recognize a rich set of configuration and parameter information (device description) from devices that have been plugged into the bus. Foundation Fieldbus even allows a device to transmit parameters relating to the estimated reliability of a particular piece of data. Foundation Fieldbus uses a scheduler to guarantee the delivery of messages. Therefore, the issues of determinism and repeatability are solidly addressed (determinism means knowing the absolute worst-case response times with 100% certainty). Each segment of the network contains one scheduler.

For more details about FF, visit the website at:

<https://www.fieldcommgroup.org/technologies/foundation-fieldbus>.

FDM supports all FF devices connected to Experion using both DDs and DTMs. These devices are connected to the Fieldbus Interface Module. All FIM versions - FIM2, FIM4, FIM8, are supported.

2.15.3 PROFIBUS protocol

PROFIBUS is a powerful and versatile two-wire digital fieldbus system. It is mainly used in the field with interfacing capabilities downward towards the sensor/actuator level and upwards towards the production and enterprise levels. PROFIBUS devices connected to the PROFIBUS network give diagnostic information about the health of the devices and the measured values, along with the values themselves. This information is helpful for better maintenance and thus reducing downtime. PROFIBUS is used in process automation, factory automation, motion control, and so on.

FDM supports the configuration and collection of diagnostics of PROFIBUS PA and PROFIBUS DP devices using FDT-DTM and FDI Package technologies. FDM hosts the device, communication, gateway DTMs, and FDI Packages provided by the PROFIBUS device vendors. You can configure and perform maintenance activities on PROFIBUS devices in the field using these DTMs and FDI Packages. With FDM R500, Honeywell PGM is natively integrated with FDM eliminating the need for a third-party Comm DTM mechanism.

PROFIBUS International has over 1200 members worldwide which includes many field device vendors. For more details about PROFIBUS and PROFIBUS International, visit the website at:

www.profibus.com.

Multi master configuration

At a high level, PROFIBUS Masters are classified into two types:

- The Master which supports cyclic data communication (DPV0) is normally referred to as a Class 1 Master. The Class 1 master (DPM1) is the central control unit of a system, for example, a PLC that exchanges data with field devices within a specified message cycle. All measured values and set point values required to control the system as well as the device status data are transmitted. When compared with conventional techniques, the cyclic communication of the Class 1 master assumes tasks of the analog 4 to 20 mA standardized signals and additionally enables the bidirectional exchange of data.
- The Master which supports acyclic data communication (DPV1) is normally referred to as a Class 2 Master (DPM2). These are used for operation, monitoring purposes, and during start-up. The associated exchange of data takes place, if required. Therefore, Class 2 masters require acyclic communication services exclusively.

FDM supports PROFIBUS DP networks connected through the Experion Series C PROFIBUS Gateway Module (PGM) and through third-party PROFIBUS gateway devices. PA devices are supported through DP-to-PA network gateways.

In the Control System, essential parameters are available through cyclic data (DPV0). If you want additional data regarding the devices, use acyclic data communication. In this case, you can send commands to the devices and request for additional data from the Asset Management Tool through Class 2 masters, which support DPV1 Communication.

Typical examples are mentioned here.

- Softing FG100
- T&H xEPI
- PROFIBUS Gateway Module

2.15.4 ISA100 protocol

ISA100 is a wireless networking technology standard developed by the International Society of Automation (ISA). This ISA standard is intended to provide reliable and secure wireless operation for non-critical monitoring, alerting, supervisory control, open loop control, and closed loop control applications. This standard defines the protocol suite, system management, gateway, and security specifications for low-data-rate wireless connectivity with fixed, portable, and moving devices supporting very limited power consumption requirements. The ISA100 Wireless devices are industrial wireless devices, such as temperature or pressure transmitters. Compatible ISA100 Wireless devices function as wireless routers to provide connectivity between wireless field devices.

FDM supports ISA100 Wireless devices connected to the Honeywell Wireless Device Manager (WDM) through the OneWireless network. WDMs can be standalone or can be connected to Experion.

2.15.5 Honeywell Digitally Enhanced (DE) protocol

Honeywell Digitally Enhanced (DE) protocol is a smart device protocol for communication between DE smart field devices and DE host interfaces: TPS Process Manager Smart Transmitter Interface Module (STIM), and Honeywell MCToolKit handheld communicator. Introduced in 1989, it makes diagnostics and transmitter status information continuously available to the TPS system. FDM supports DE devices connected to TPN networks through HPMs with STIM and STIMV (multivariable STIM) IOPs (Input/Output Processors).

2.16 FDM software components and utilities

FDM consists of the following software components and utilities.

Components

FDM Server: The FDM Server forms the FDM application's core. It is used for managing FDM Clients and interacts with the HART, FF, PROFIBUS, ISA100 Wireless, and DE devices through the FDM Remote Communication Interfaces (RCIs). It stores all persistent information related to the HART, FF, PROFIBUS, ISA100 Wireless, and DE devices, networks, and FDM users. It also stores device configuration information, device history, offline configurations, audit trail information, and so on.

FDM Client: The FDM Client is a user interface used for interacting with the FDM Server to perform various device operations. It also interacts with the database and the field network through the FDM RCI to carry out necessary tasks. You can access all the FDM functions and communicate with the devices remotely using this component.

FDM RCI: The FDM RCI is a single PC node capable of handling multiple network interfaces to communicate with field devices. As its name implies, it can be located remotely from the FDM Server. However, the FDM RCI is also a component of the FDM Server.

MUX Monitoring Solution: It consists of an FDM Gateway, which combines FDM MUX Monitoring components and unlicensed ACE components to populate Experion with non-Experion connected HART device information. It enables Experion to access alarm information from HART devices associated with the following networks.

- RS-485 HART Multiplexer
- Experion-integrated Safety network
- Experion-integrated OneWireless network

For OneWireless networks, MUX Monitoring applies only to HART devices connected through OneWireless Adapters (OWAs).

FDM HART Multiplexer: This component enables third-party applications to access all HART devices on both Experion and non-Experion networks without using additional physical connections. Also, this component emulates P+F MUX and allows third-party applications to access device information from FDM.

Station Maintenance View: This component is installed with the FDM Client on an Experion Flex Station to view the device detail display pages and to view detailed information of devices.

Utilities

The following FDM utilities are also featured.

FDM Server Management Tool: Used to configure and view network communication interfaces, update product license, and control (start and stop) the FDM Server.

FDT Comm Console: Used to configure and build complete FDT networks using DTMs. It displays all networks configured on a given FDM Server, but configuration access is limited to the RCI node hosting the FDT Comm Console.

FDM Maintenance: Using the FDM installation software, you can modify the present installation by selecting or removing any product component, or reinstall program data if any existing file becomes corrupted or unusable. FDM can also be removed without using the installation software.

Dr. FDM: Used to collect diagnostic information related to FDM functioning. This diagnostic tool can be run on systems where FDM components are installed in case issues arise due to usage of FDM software, log files can be sent to Honeywell TAC for further analysis.

FDM Data Backup - Restore: Used to back up the FDM database and restore FDM data with the backed up database.

FDM Migration Tool: Used to migrate data from previous releases to the current release of FDM.

Plant Area View: Used to group available devices based on their geographical locations. It is also used to represent virtual grouping of devices mimicking the way they are grouped in the plant.

PVST Planner: This interface provides a "one-view interface" for all ESD valve status and PVST schedule performance. It allows automatic uploading of PVST data and clearly indicates potential valve problems that require immediate action.

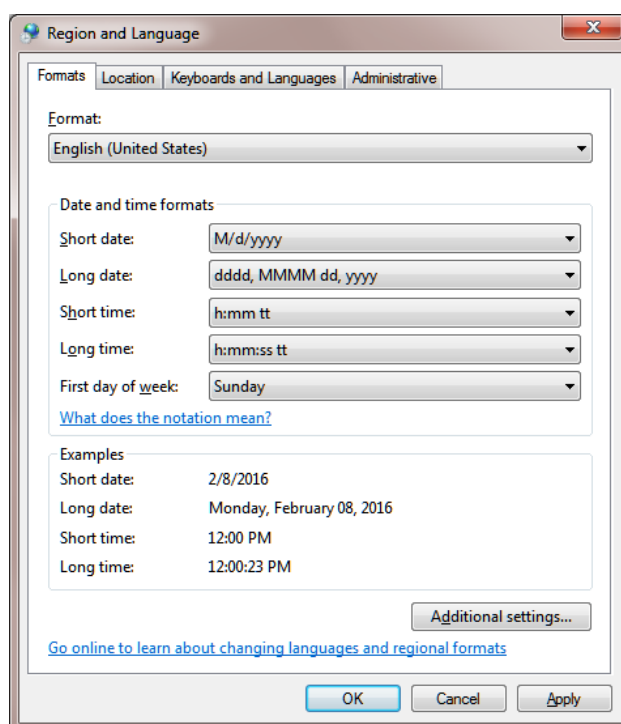
GETTING STARTED WITH FDM

3.1 Locale

FDM supports US-English locale

Ensure the local time zone format is set to English (United States).

1. Click Control Panel > Clock, Language, and Region.
2. Select English (United States) from the Format list.
3. Retain the default date and time formats of US English locale as shown here.



4. Click Apply and click OK.

Editing the date and time parameters may fail if the local time zone changes.

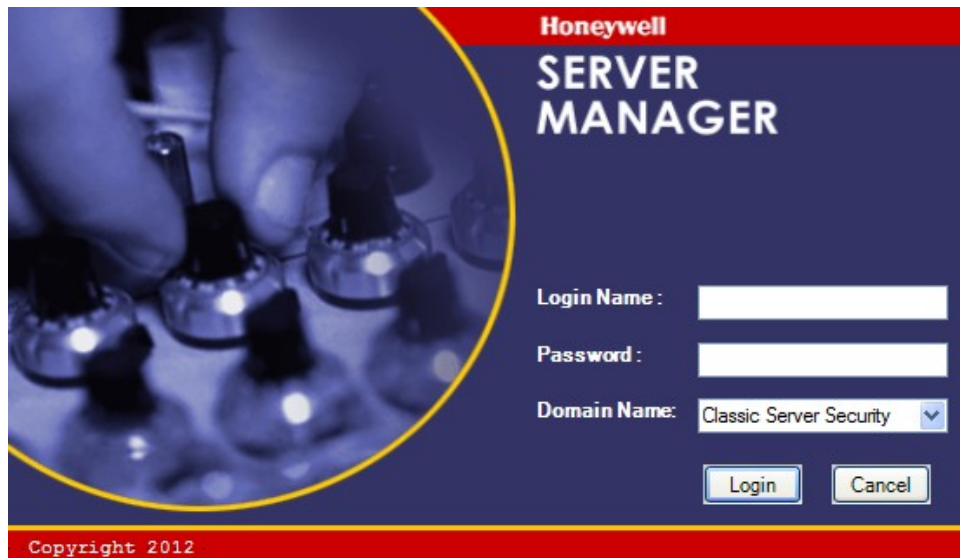
3.2 Logging on to the FDM Server Management Tool

The FDM Server Management Tool is used to update licenses and manage networks. It can be run only from the FDM Server and is not available on other nodes with FDM components.

If you log on to the server computer as any user other than Administrator and launch the FDM Server Management Tool, you are prompted to provide administrative privileges.

To logon to the FDM Server Management Tool:

1. Double-click FDM Server Management Tool desktop icon, or click Start > All Programs > Honeywell FDM > FDM Server Management Tool. The Server Manager login window appears.



ATTENTION

- If logging on for the first time, use Administrator credentials. Ensure that you change the Administrator password after the first login.
- It is recommended to use single sign on, as the user specified password login is insecure.

2. Type Login Name and Password.
3. By default, domain name is selected as Classic Server Security. To choose another domain name, select it from the Domain Name list.
4. Click Login. The FDM Server Management dialog box appears, displaying the Network Configurator option by default.

ATTENTION

Only a user with Administrator privileges can make changes to the configuration in the FDM Server Management Tool. By default, all other users have only read-only access to view information.

5. Perform necessary management tasks.

ATTENTION

If logging on to the Server Management Tool for the first time, update the license and configure the networks as described in the [“Updating the FDM license”](#) and [“Configuring networks”](#) sections, respectively.

If Single Sign-on is enabled, the login screen does not appear.

6. Click Exit to close the FDM Server Management screen.

3.3 Updating FDM Server status

ATTENTION

Ensure that the FDM Server is stopped to update the licensing information.

To update the FDM Server status:

1. If the server is running, the button under Server Control in the left pane appears in green, with the label **CLICK TO STOP** displayed on it. This indicates that the server is running currently.
2. Click **CLICK TO STOP** to stop the server.
3. Type the reason for service status change, and click **OK**.
4. The FDM Server Management dialog box appears prompting you to change the status of the service. It also prompts you to inactivate the configured and loaded FDM Gateway(s) in Control Builder.
5. Click **Yes** to confirm the operation. The server is stopped and the button under Server Control in the left pane displays **CLICK TO START** and appears in Yellow.
6. To restart the FDM Server, click the **CLICK TO START** icon under Server Control.
7. Type the reason for service status change, and then click **OK**.
8. Click **Yes** to proceed with the operation.

3.4 Updating the FDM license

You can view or update FDM license using the FDM Server Management Tool.

ATTENTION

After installing FDM, you must first update the license in the FDM Server Management Tool.

In the FDM Server Management dialog box, when you click the Licensing icon, the following license information is displayed.

- **Option:** Indicates the name of the licensed feature.
- **Status:** Refers to the present status of the license for a feature. It is either **Licensed** or **Not Licensed**.
- **Value(s):** Specifies the value of each licensed feature. For some features, the values can either be **License Enabled** or **Disabled**.

The following table describes the different licensing options. For more information about the FDM base license components, refer to the FDM Technical and Specifications.

Licensing option...	Indicates...
Offline Configuration	Offline configuration feature is enabled/disabled for HART devices. YES indicates that it is licensed.
Maximum FDM HART MUX (FHM) devices	Total number of devices that can be connected through the FDM HART Multiplexer. Note that FHM works with third party applications use Network Server Interfaces to establish connections with MUXs.
Maximum Remote Comm Interface (RCI) nodes	Total number of Remote Communication Interfaces that can be connected to the FDM Server and running simultaneously.
Maximum FDM Client connections	Total number of FDM Clients that can be connected to the FDM Server simultaneously to access all device functions and features.
Maximum Server Network Interfaces (MUX/OW/HART-IP)	Total number of RS-485 HART Multiplexers, OneWireless networks, and HART-IP network interfaces that can be configured in the FDM Server through the FDM Server Management Tool.
Maximum number Experion/TPS interfaces nodes	Total number of Experion/TPS interfaces that can be configured in the FDM Server through the FDM Server Management Tool. Note: Each Experion/TPS interface license includes a required RCI interface, which can be used for either Experion Server or TPN Server. To configure both Experion and TPS networks, you must have two Experion interface licenses that includes two RCI interface licenses.
Maximum connected devices	Total number of devices (of all types) that can be connected to the FDM Server through various configured network interfaces.
Maximum devices supported by Audit trail	Total number of devices that can be audit trailed.
Maximum MUX Monitoring Networks	Total number of RS-485 HART Multiplexer interfaces, OneWireless which are enabled for MUX Monitoring feature.
Maximum Level 2 Virtualized Servers	Total number of virtualized servers (FDM Server and FDM gateway) that can be connected on the level 2 node.

Licensing option...	Indicates...
Maximum number of Valves allowed for PVST	Total number of valves that are allowed for PVST schedule and execution.
Instrument Monitoring in UAS	Instrument Monitoring in UAS is enabled/disabled. YES indicates that it is licensed.

3.4.1 Prerequisites

- FDM license file
- FDM Server is in Stop mode

To update the FDM license

1. In the FDM Server Management dialog box, click the Licensing icon.
2. Under Upgrade license, click Select, browse to the folder where the license file is stored and choose the file.
3. Click Open in the Select a License File dialog box. A confirmation message appears.
4. Click OK. The path for the license file with the .xml extension appears and the license information is updated and appears under Licensing Information.
5. Verify that the Licensing Information is correct before closing the Server Management Tool.

3.5 Logging on to the FDM Client

If the FDM Client and FDM Server reside on the same computer, perform the following steps to log on to the FDM Client.

ATTENTION

If you are logging on for the first time, ensure that FDM is updated with the proper license file. To update the license, refer to section [“Updating the FDM license”](#).

If Single Sign-on is enabled, the logon screen does not appear.

Logging on to any FDM Client, automatically starts the FDM Server, if it is stopped. You need not log on to the FDM Server Management Tool to start the Server.

1. Double-click the FDM Client Desktop icon, or click Start > All Programs > Honeywell FDM > FDM Client. The Field Device Manager login window appears.
2. Type the name of the Server or select the server from the drop-down list.

TIP

If you are connecting to the server for the first time, enter the server name. If FDM connects to the specified FDM Server successfully, then the server name is cached and is available for selection from the drop-down list during subsequent logins.

If both server and client are running on the same computer, you can use LOCALHOST as server name in the Server box.

3. Click Login. The Field Device Manager login window appears.

ATTENTION

If you are logging on for the first time, use Administrator credentials.

Ensure that you change the Administrator password after your first log on.

FDM only supports passwords greater than or equal to 8 characters.

4. Type Username and Password.
5. By default, domain name is selected as Classic Server Security. To choose any other domain name, select the Domain Name from the list.

ATTENTION

If you are trying to logon as an FDM user, select Classic Server Security from the drop-down list.

To use Windows credentials, select the appropriate domain.

6. Click Login to validate your login credentials. The Field Device Manager window appears.

The Network View tree under the Online View group appears. The name of the server you are currently connected to appears in the title bar. The left pane of the FDM Client contains two groups.

- Online View
- Offline View

If the FDM Client is installed on a different computer (remote), the logged on user must be a member of the FDMAccessGroup in both systems (FDM Client and FDM Server).

ATTENTION

Any Windows user or Windows group user who wants to access the FDM Server from a FDM Client must be added to the FDMAccessGroup in both FDM Server and FDM Client computers.

User should log off and log on again for the permissions to take effect.

If the Windows user has logged on to the FDM Client computer as FDMMgr, the user need not be added to the FDMAccessGroup.

The user who is currently logged on to Windows must be a part of an FDM user group. For more information, refer to section [“Roles and privileges”](#).

To add a user to the FDMAccessGroup, perform the following steps.

1. On the client computer, right-click Computer and click Manage. The Server Manager dialog box appears.
2. In the Server Manager tree, expand Configuration > Local Users and Groups > Groups. The list of groups appears in the right pane.
3. Right-click FDMAccessGroup and click Add to Group.
4. Add the logged on user to this group and click OK.
5. Repeat steps 1 through 4 on the FDM Server computer and all computers where FDM Client is installed.

You can logon to the FDM Server from a remote FDM Client.

In case of any problem during remote access, refer to the FDM Troubleshooting Guide.

To add a domain group with FDMOPCAccessGroup access

1. Right-click on **Start** menu (Windows icon), and click **Computer Management** or type "compmgmt.msc" in **Run** command.

NOTE

For Windows 7, use the **Run** command option to launch **Computer Management**.

2. Expand **Local Users and Groups** in the **Computer Management** pane.
3. Right-click on **Users** and select **New User...**
4. Enter the **User name**, Password, and **Confirm password** for the user.

NOTE

The User name and the Password should match with the one provided in the Sentinel.

5. Uncheck **User must change password at next logon** check box.
6. Check **Password Never Expires** check box.
7. Click **Create** to create new user.
8. Click **Close** to close the New User window.
9. Click on **Users**, under **Local Users and Groups** in the **Computer Management** pane.
10. Right-click on the newly created user and select **Properties**.
11. Select **Member Of** tab and click **Add**.
12. Click **Advanced** in **Select Groups** window and click **Find Now**.
13. Select **FDMOPCAccessGroup** from the list and click **OK**.
14. Click **OK** in the **Select Groups** window.
15. Select **FDMOPCAccessGroup** in the **Properties** window.
16. Click **Apply** and then click **OK**.

NOTE

Log out and login to get the permission reflected.

3.6 Changing the password

It is recommended you change the default password after the first login to the FDM system.

ATTENTION

Only a user with the Administrator privileges can change other users' passwords.

Login credentials for the FDM Client and FDM Server Management Tool are identical.

FDM system password is not the same as the password for the FDMMgr user account is used for authentication purposes.

To change your password:

1. In the FDM Client main window, click Tools > User Management. The User Manager pane appears displaying the list of existing users and their roles in the right pane.
2. Select the appropriate user, based on your roles and privileges.
3. In the User Manager pane, click Edit User. The Edit User pane appears.
4. Type the existing password in the Old Password field.
5. Type the New Password.
6. To confirm your password, retype your new password in the Confirm New Password box.
7. Click Save. FDM validates the details that are entered and updates the new password in the database.

3.7 Logging on to FDT Comm Console

FDT Comm Console allows you to configure FDT networks and build the complete network using DTMs only on the RCI Server. The FDT Comm Console is installed in every node where the RCI component is installed.

To log on to the FDM Comm Console, which is installed along with the FDM RCI, perform the following steps.

ATTENTION

If you are logging on for the first time, ensure that FDM is updated with the proper license file. To update the license, refer to section [“Updating the FDM license”](#).

If Single Sign-on is enabled, the logon screen does not appear.

1. Click the FDT Comm Console icon on your desktop, or click Start > All Programs > Honeywell FDM > FDT Comm Console. The Field Device Manager login window appears.
2. Type the name of the Server or select the server from the drop-down list.

TIP

If you are connecting to the server for the first time, enter the server name. If FDM connects to the specified FDM Server successfully, then the server name is cached and is available for selection from the drop-down list during subsequent logins.

NOTE

If both server and client are running on the same computer, you can use LOCALHOST as server name in the Server box.

3. Click Login. The Field Device Manager login window appears.

ATTENTION

Use Administrator credentials if logging on for the first time.

Change the Administrator password after logging on for the first time.

4. Type User name and Password.
5. Select the name of the Domain.

ATTENTION

If you are trying to logon as an FDM user, select Classic Server Security from the drop-down list.

To use Windows credentials, select the appropriate domain and type the password.

FDM only supports passwords greater than or equal to 8 characters.

6. Click Login to validate your login credentials. The Field Device Manager – FDT Comm Console window appears. The Network View tree under the Online View group is displayed by default.

The left pane of the FDT Comm Console contains two groups.

- Online View
- Offline View

CONFIGURING NETWORKS

FDM communicates with HART, FOUNDATION Fieldbus (FF), PROFIBUS, ISA100 Wireless, and DE devices through various communication interfaces. If this is a new installation or you are adding interfaces to an existing system, you must configure the network after installing the software. Based on the field devices and interfaces used for communication with FDM, you must identify and configure the appropriate network.

You can configure the following network communication interfaces using the FDM Server Management tool.

- **RS-232 HART Modem:** Widely used when the requirement is to communicate with a single device at a time. An RS-232 HART Modem plugs into the COM port of a Personal Computer. USB HART Modems have become available now. Refer to the FDM Specifications for supported models.
- **Honeywell HART DE Modem:** Capable of handling both HART and Honeywell DE protocols. However, FDM supports only HART protocol. FDM supports HART DE Modem connection through USB to RS232 converter from CableMAX.
- **RS-485 HART Multiplexer:** Enables FDM to communicate with multiple HART Multiplexers, each connected to multiple HART field devices, over a single serial communication line. A maximum of six MUX networks per RCI are allowed, all of which must be associated with a single FDM Server.
- **Honeywell Experion PKS:** Enables FDM to communicate with HART, FF, and ISA100 Wireless devices. With Honeywell Experion PKS interface, you can also associate Safety network with Universal Safe Modules (to configure HART and SM-connected devices) and OneWireless network (to configure ISA100 Wireless and HART devices).
- **COMM DTM Interface:** Enables FDM to configure PROFIBUS Gateways (through Communication/ Gateway DTMs), PROFIBUS DP and PA devices (through DTMs), and connected HART devices where supported (through EDDLs or DTMs).
- **Safety Network with Universal Safe Modules:** Can be configured as Standalone Safety Network (without Experion integration) to configure HART devices connected to Universal Safe Modules.
- **OneWireless Network:** Can be configured as a standalone OneWireless network (without Experion integration) to configure ISA100 Wireless and HART devices through the OneWireless adapter connected to WDM.
- **HART-IP Network:** Enables FDM to configure HART devices connected to third-party HART IP gateways.
- **Honeywell RTU Network:** Enables FDM to connect HART and ISA devices using Honeywell ControlEdge RTU.
- **Honeywell PLC Network:** Enables FDM to connect to HART devices using Honeywell ControlEdge PLC/HC900.
- **Honeywell TPS:** Enables FDM to configure DE devices connected to the TPS system. It is configured as an Experion-integrated TPS network (indicates that TPS connected to Experion systems through Experion-T nodes such as ESV-T and ES-T).

Number of networks configured per RCI

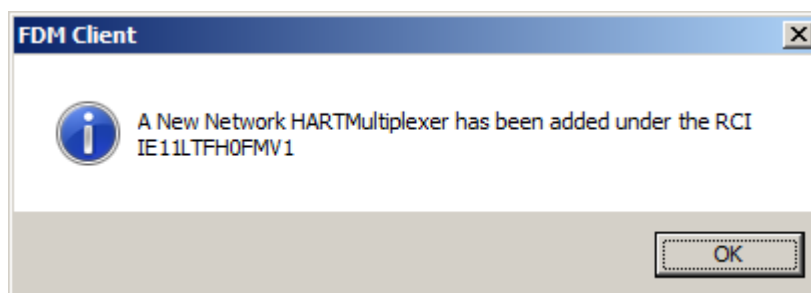
The network types and the permitted maximum number of networks configured per RCI are listed here.

Network type	Number of networks per RCI
Modems and MUX networks	6
Experion PKS networks ¹	1
FDT/DTM networks	1
Safety Manager Networks (with Universal Safety I/O)	5
HART-IP network/ Honeywell ControlEdge RTU/ Honeywell ControlEdge PLC/HC900 network	5
OneWireless networks	2
Honeywell TPS network ²	1
Note 1: If an RCI is configured for an Experion Server, it cannot be used for any other type of network connection. Note 2: If an RCI is configured for a TPS network, it cannot be used for any other type of network connection.	

ATTENTION

You can add, edit, or delete the network irrespective of the FDM Server status (running or stopped).

If you add, edit, or delete a network interface when the FDM Server is running, a confirmation message appears in the FDM Client. For example, when you try to add a network, the following message appears.



4.1 Configuring RS-232 HART Modem

FDM uses the RS-232 HART Modem to communicate with HART devices using the serial port. You must configure FDM to send and receive the data through the HART communication port. It is used for configuring a single device at a time.

ATTENTION

For an RS-232 HART Modem configuration, it is imperative that the Use FIFO buffers (requires 16650 compatible UART) check box is cleared in the Advanced Settings dialog box while configuring the COM Port settings.

Prerequisites

Ensure that COM port settings are configured before configuring the RS-232 HART Modem in the FDM Server Management Tool. To configure COM port settings, refer to the section [“Configuring COM port settings”](#).

To configure FDM for an RS-232 HART Modem:

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. Select the network type as RS-232 HART Modem from Network Type.
6. Type the interface name (a unique name) in Network Interface Name.
7. Type the name of the server in RCI Server Name.
8. The configured network is connected to the RCI Server.
9. Select the COM port from the COM Port drop-down list. FDM supports COM ports 1 through 255.
10. Specify the retry count ranging between 0 and 9 in Retry Count, as required.

ATTENTION

For the RS-232 HART Modem, the BAUD rate is 1200 bps, which is predefined. You are not allowed to modify the BAUD rate.

11. Click OK to save the configuration.

ATTENTION

By default, FDM populates the RCI Server Name with LOCALHOST. If you leave this unchanged, FDM considers the RCI Server to be the local host and displays an appropriate message to that effect.

4.2 Configuring FDM for a Honeywell HART DE Modem

The Honeywell HART DE Modem provides the network communication interface to HART devices. This modem supports both HART and Honeywell Proprietary DE (Digital Enhanced) protocols.

Prerequisites

Ensure that COM port settings are configured before configuring the Honeywell HART DE Modem in the FDM Server Management Tool. To configure COM port settings, refer to the section [“Configuring COM port settings”](#).

To configure FDM for a Honeywell HART DE Modem:

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. Select the network type as Honeywell HART DE Modem from the Network Type drop-down list.
6. Type the name of the interface, in the Network Interface Name box.
7. Type the name of the RCI server in the RCI Server Name box. The configured network is connected to the RCI Server.
8. Select the COM port from the COM Port drop-down list. FDM supports COM ports 1 through 255.

ATTENTION

Honeywell HART DE Modem supports a BAUD rate of 9600 bps, which is predefined. You cannot manually enter/edit this value.

9. Specify the retry count ranging between 0 and 9 in Retry Count box.
10. Enter the poll address of the modem ranging between 0 and 15 in the Start Poll Address box.
11. Enter the poll address (any value between 0 and 15) in the End Poll Address. The entered range reflects the poll addresses that are scanned for detecting the HART devices in the network.

ATTENTION

The value entered in End Poll Address must be greater than the value entered in Start Poll Address.

12. Click OK to save the configuration.

ATTENTION

By default, FDM populates RCI Server Name with LOCALHOST. If you leave this unchanged, FDM considers the RCI Server to be the local host and displays an appropriate message to that effect.

4.3 Configuring FDM for an RS-485 HART Multiplexer

Using the RS-485 HART Multiplexer network, FDM can communicate to multiple HART devices in the field. Multiplexers transmit signals over a single communication line. The RS-485 HART Multiplexers can also be used to enable remote configuration, monitoring, and troubleshooting of those devices. A single RS-485 HART Multiplexer network can have up to 31 multiplexers and is connected to up to 1000 devices.

Prerequisites

Ensure that COM port settings are configured before configuring the RS-485 HART Multiplexer in the FDM Server Management Tool. To configure COM port settings, refer to the section [“Configuring COM port settings”](#).

To configure FDM for an RS-485 HART Multiplexer:

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. Select the network type as RS-485 HART Multiplexer from the Network Type drop-down list.
6. Type the interface name (a unique name) in the Network Interface Name box.
7. Type the name of the server in the RCI Server Name. The configured network is connected to the RCI Server.
8. If you want the MUX Monitoring feature to be enabled for this particular network configuration, select the Enable MUX Monitoring check box.

ATTENTION

The Enable MUX Monitoring check box is enabled only if you have updated the Maximum Number of MUX Monitoring Network supported license.

9. Select the COM port where the multiplexer is connected, from COM Port. FDM supports COM ports 1 through 255.
10. Select the BAUD Rate. The BAUD rate for RS-485 HART Multiplexer is 9600 and 19200.
11. Enter the poll address of the multiplexer ranging between 0 and 127 in the Start Poll Address and End Poll Address box. The entered range reflects the poll addresses that are scanned for detecting the multiplexers in the network.

ATTENTION

Ensure that the value you enter in End Poll Address is greater than the value you enter in Start Poll Address.

The MTL network does not support poll address 0.

To achieve optimum performance, it is recommended that the poll address range closely matches the actual addresses to which multiplexers are configured on the network.

12. Click OK to save the configuration.

ATTENTION

By default, FDM populates the RCI Server Name with LOCALHOST. If you leave this unchanged, FDM considers the RCI Server to be the local host and displays an appropriate message to that effect.

4.4 Safety network configuration

Safety Manager integration supports configuration and maintenance of HART devices connected to Safety Manager/Safety Manager SC Universal Safe I/O (USIO) modules. Features and functions supported are similar to RS-485 HART Multiplexer networks. HART devices connected to Safety Manager (SM)/Safety Manager SC non-USIO analog I/O modules are supported in FDM only

through RS-485 HART Multiplexer network connections.

NOTE

The following will also be applicable for Safety Manager SC.

To use FDM with Safety Manager USIO-connected HART devices, the following general tasks should be performed, in the recommended order.

1. Commission all SM/Safety Manager SC -connected devices and strategies.
2. Export the configuration from Safety Builder and import it into FDM.
3. Configure the Safety network using the FDM Server Management tool.

ATTENTION

If any changes are made to the Safety Manager configuration that affect the connected devices, the configuration must be re-exported from Safety Builder and re-imported in FDM to provide a proper update. FDM does not dynamically update the Safety Builder configurations as in the other networks. FDM can import only one Safety Builder configuration file; multiple Safety Builder files are not supported.

FDM Safety network can be configured for either of the following scenarios.

Experion-integrated Safety network configuration (SM is associated with the Experion Server in Safety Builder). For more information about configuring the Experion-integrated Safety network, refer to the [section "Configuring FDM for the Experion-integrated Safety network"](#)

Standalone Safety network configuration (SM is not associated with the Experion Server in Safety Builder)

4.4.1 Importing Safety Builder Export file

Prerequisites

- Ensure all SM connected devices and strategies are commissioned before using FDM with Universal Safe Modules connected HART devices.
- Ensure Safety Builder configuration data is exported from Safety Builder in XML format. This file is referred to as the Safety Builder Export File.

For more information about the Safety Manager network configuration in Safety Builder and exporting the Safety Builder configuration data from Safety Builder, refer to the Safety Builder Users Guide.

ATTENTION

You can import only one SB Export file per FDM Server. Hence, you must plan the configuration accordingly in Safety Builder.

The SB Export file generated from Safety Builder can have a combination of Standalone and Experion integrated Safety networks. Hence, you can import this file and configure both Standalone and Experion integrated Safety networks without reimporting the file again.

Ensure that the SB Export file is imported before beginning the Safety network configuration. You can also merge 2 or more Export file before importing.

If changes are made to Safety Builder after you import the configuration file to FDM, re-import the SB Export file to reflect these changes.

To import Safety Builder Export file:

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. Click Import Resource.
4. Under Add Resource, click Safety Builder Export File from the drop-down list and then click Browse. The Open dialog box appears.

ATTENTION

You can add SB Export file from any system within the network. It is not necessary that you must add it from the FDM server.

Importing resource operation may modify the network(s) configuration. Hence, ensure that no networks operations are in progress and only then import the resource when the FDM Server is running.

5. Select the SB Export file and click Open. The Reason for Resource Update dialog box appears.
6. Type the reason for resource update and then click OK. A confirmation message appears. The added resource is listed under Available Resources.

ATTENTION

Safety Builder (SB) is case-sensitive for tag names (SM/IOTA/Channel). For example, consider two tag names, "Test" and "test". In this case, while SB considers both tag names as different, FDM considers them the same. Hence a tag conflict occurs. When such an SB Export file is imported to FDM, the second tag is renamed to "_Conflict" when it appears in the FDM Client. Perform the following to avoid tag conflicts.

Rename the tag names in SB.

Re-export the tags in SB using the SB Export file.

Re-import the updated SB Export file in the FDM Server database using the Online Update tool.

Follow the steps to merge multiple SB Export files

Each SM Controller is represented by SMController block in the SBExport.xml file. The SMControllers block contains details for all the SM Controllers. To add multiple controllers, you must replicate the SMController block for each controller. To merge multiple SBExport.xml files, you must copy all the SMController blocks into SMControllers block of XML file that must be imported.

Following is snippet of the XML file.

```

1  <?xml version="1.0" encoding="utf-8"?>
2  <SM Network="Physical Network" Version="1" ConfiguredDateTime="2012-01-09T11:41:22.136256+05:30">
3    <SMControllers>
4      <SMController Name="SM 1" Redundant="1" ControllerVersion="2" ConfigurationVersion="10">
5        <DCS Type="" Alias="" />
6        <CP1 IPAddress="127.0.0.1" />
7        <CP2 IPAddress="127.0.0.2" />
8        <Links>
9          <Link NetworkNumber="1">
10             <IOTAs>
11               <IOTA IOTANumber="1" IOTAName="IOTA_1">
12                 <Channels>
13                   <Channel ChannelNumber="1">
14                     <PointType>1</PointType>
15                     <TagNumber>Device_1</TagNumber>
16                   </Channel>
17                   <Channel ChannelNumber="2">
18                     <PointType>1</PointType>
19                     <TagNumber>Device_2</TagNumber>
20                   </Channel>
21                   <Channel ChannelNumber="3">
22                     <PointType>1</PointType>
23                     <TagNumber>Device_3</TagNumber>
24                   </Channel>
25                 </Channels>
26               </IOTA>
27               <IOTA IOTANumber="2" IOTAName="IOTA_1">
28                 <Channels>
29                   <Channel ChannelNumber="1">
30                     <PointType>1</PointType>
31                     <TagNumber>Device_1</TagNumber>
32                   </Channel>
33                   <Channel ChannelNumber="2">
34                     <PointType>1</PointType>
35                     <TagNumber>Device_2</TagNumber>
36                   </Channel>
37                   <Channel ChannelNumber="3">
38                     <PointType>1</PointType>
39                     <TagNumber>Device_3</TagNumber>
40                   </Channel>
41                 </Channels>
42               </IOTA>
43             </IOTAs>
44           </Link>
45         </Links>
46       </SMController>

```

Follow the steps to merge:

1. Open the SBExport.xml files that must be merged in a text editor such as Notepad++.
2. Decide which must be the master SBExport.xml file for import process.
3. Copy SMController code blocks from remaining files and paste after within SMControllers code block.

ATTENTION

Make sure not to delete the existing SMController code blocks in the file.

4. Save the file.
5. Import the master SBExport.xml file in FDM and configure different controllers in network as required.

4.4.2 Configuring FDM for standalone Safety network

By configuring the standalone Safety network (without Experion integration), FDM can discover HART channels when SM is integrated with a third-party DCS.

Prerequisites

Ensure that Safety Builder export file is imported to FDM.

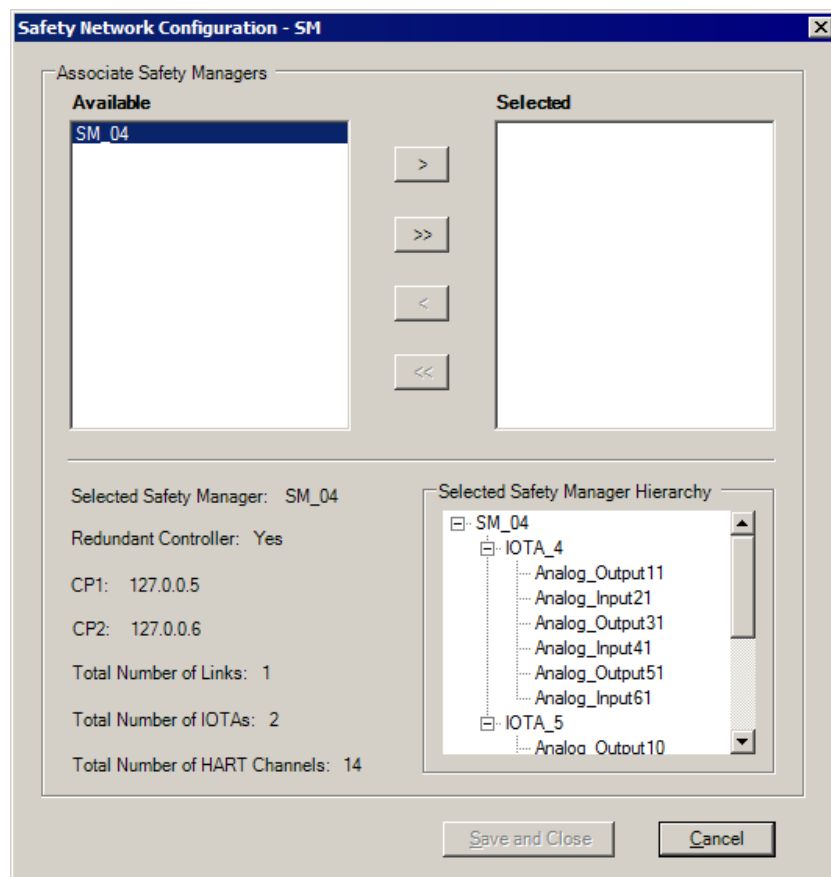
To configure FDM for standalone Safety network:

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 Safety Network with Universal Safe Modules.

ATTENTION

You can group the SMs under different standalone Safety networks in the same or different RCIs. This option helps you distribute SMs across standalone Safety networks.

6. Click Associate Safety Managers. The Safety Network Configuration dialog box appears.



7. To associate Safety Managers from export file:
 - Select an SM from the Available list.
 - Click > to move it to the Selected list. Then, selected SM is configured to the particular network.
 - To move all SMs to the Selected list, click the >> button. Then, selected SMs are configured to the particular network.

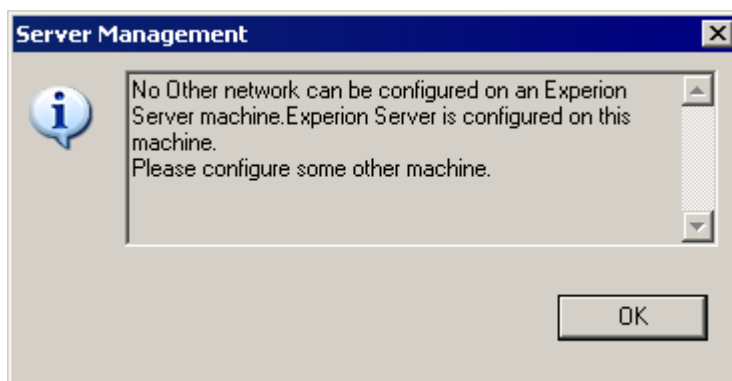
The selected SM, IOTA and HART channels are displayed under Selected Safety Manager Hierarchy.

8. Click Save and Close.
9. In the FDM Server Management dialog box, the configuration status is displayed as Complete, that indicates standalone Safety network configuration is completed.
10. Type the name of the RCI Server in RCI Server Name. The configured network is connected to the RCI Server.

ATTENTION

The COM Port, Start Poll Address, BAUD Rate, End Poll Address and Retry Count fields are not applicable when configuring Safety Network with Universal Safe Modules network type. Hence, FDM disables these fields.

11. Click OK to save the configuration. The following message appears if any other network is configured on an Experion Server computer.



12. Click OK to configure the network on non-Experion Server computer.

ATTENTION

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

4.4.3 Online update of network configuration

After an SB export file is imported to FDM and Safety network is configured (as integrated with Experion or as standalone), in order to update the network information like adding/removing SM/IOTA/HART channels to the already configured networks, online update of network configuration can be used. Most of the changes that can be accommodated through this online update of network configuration are supported without stopping the FDM Server.

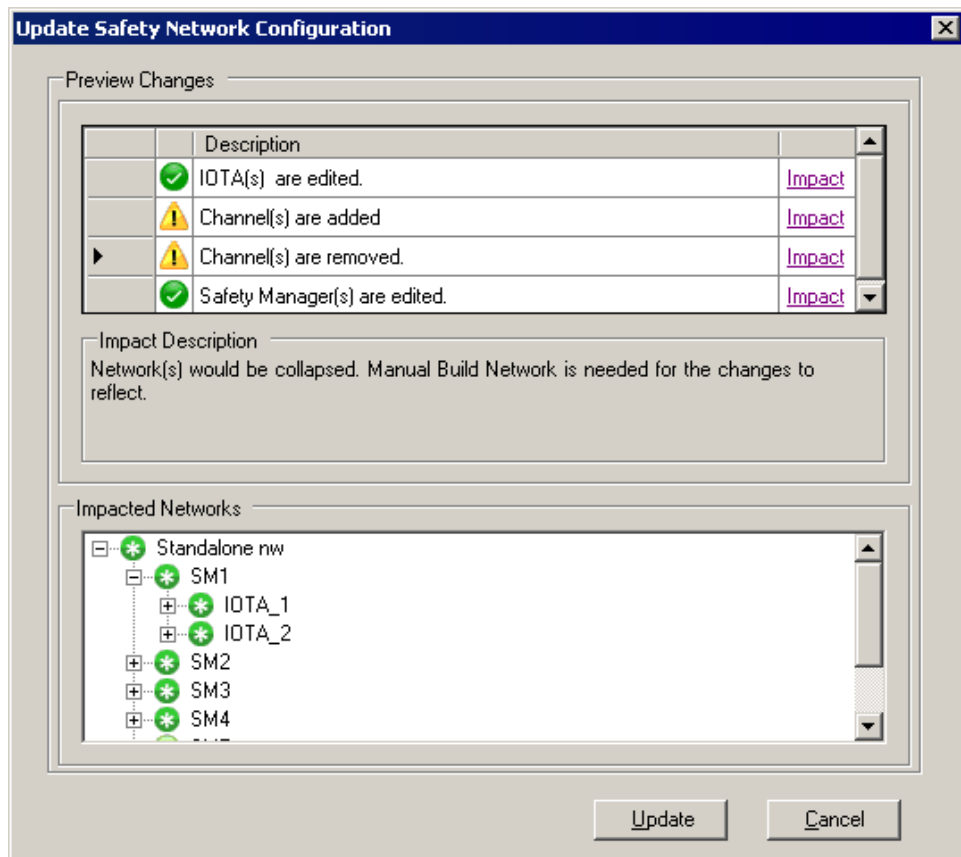
To update (import) network configuration data to FDM:

1. Log on to the FDM Server Management Tool.
2. In FDM Server Management dialog box, click Import Resource.
3. In the right pane, under Add Resource, click Safety Builder Export File from the drop-down list and then click Browse. The Open dialog box appears.

ATTENTION

Provide the audit trail reason to update (import) the network configuration data to FDM.

4. Select the updated SB export file and then click Open.
5. The Update Safety Network Configuration dialog box appears. The updated SB export file is compared with the previously imported SB export file and the differences are displayed under Preview Changes with their corresponding impact.



6. If you want to view the impact due to changes made in SB export file, click the Impact link. The description of the impact is displayed under Impact Description. All impacted networks are listed in the Impacted Networks list; the network hierarchy is also displayed with the changes in the form of icons and tooltips for updated SM/IOTA/HART channels.

Icons that can appear in the summary grid view and Impacted Networks list are listed here.

Icon	Description
	Network(s) would be updated automatically with the edited SM(s), IOTA(s), and HART channel(s). These changes are reflected in the FDM Client Network View after reconfiguration is successful.
	Network is not impacted with the changed SB export file. This is either because the new Safety Builder export file has insignificant changes or that changes are available in other SMs, which are not configured in the existing networks. You can still click the Update button to update the new Safety Builder export file into the FDM Database.
	Network(s) would be collapsed. Perform Build network operation to view the new network configuration after reconfiguration is successful.
	Stop the FDM Server to associate the newly added SM(s) to either standalone Safety network or Experion integrated Safety network as shown in the Impact Description.
	Displays if SM/IOTA/HART channel is not changed.
	Displays if SM/IOTA/HART channel is added.
	Displays if SM/IOTA/HART channel is removed.
	Displays if SM/IOTA/HART channel is edited.

7. Click Update to reconfigure the network.

- If the FDM Server is not running, the online update network configuration operation updates the updated SB export file into the FDM database and the impacted network configuration. When the FDM Server and the FDM Client are started after the build network operation, changes are reflected in the FDM Client Network View.
- If the FDM Server is running, the online update network configuration operation updates the new network configuration in the FDM database. The changes are also reflected in all FDM Clients. The following changes are visible in the FDM Client (without restarting the FDM Server) due to network resource update.
 - In case of both Experion integrated Safety network and Standalone Safety network:
 - If the impact on the network is only renaming of SM/IOTA/HART tags, the network in the Client is automatically updated with the new configuration.

ATTENTION

When the device tags which are alarm monitored are renamed, the changes are not reflected in FDM Client automatically. For these changes to be reflected, inactivate the devices in Control Builder and do a build network at the appropriate level (Network/SM/IOTA).

- If the impact on the network is addition/removal of SM/IOTA/HART, the impacted network tree is collapsed and the build network operation must be performed only on the impacted network to view the updated network changes.
- If new SM controllers are added in the updated SB Export file which has no Experion association, stop the FDM server and click the Edit option in the FDM Server Management Tool. The newly added SMs are associated either to the existing network or to the new Standalone Safety network.
- If new SMs are added under a Honeywell Experion PKS network that is already configured in the Server Management Tool, then the network tree collapses and the new SMs are reflected after the build network operation is performed on the corresponding Safety Network. If the SMs are added under a new Honeywell Experion PKS, import the resource file, stop the FDM server, and configure a new Honeywell Experion PKS with Safety Network.

ATTENTION

Before you click the Update button, verify the details under Preview Changes for the changes in an SB export file and corresponding impacts.

8. Click Yes. The Update Network Summary dialog box appears. It displays the summary of the network name and the reconfiguration status. Click the reconfiguration status link to view the status description.

If the reconfiguration status displays any error for the updates, refer to the FDM Troubleshooting Guide.

9. Click OK.

ATTENTION

Sometimes, when importing the updated SB export file, you may not be able to view the direct impact on the network tree. This might be due to some specific changes on the SM controller (For example, IP address changes).

4.5 OneWireless network configuration

OneWireless integration supports the configuration and maintenance of ISA100 Wireless devices connected to multiple Wireless Device Managers (WDMs) through a single FDM Server. It enables maintenance of ISA100 Wireless devices through any FDM Client as well as through FDM Station Maintenance View when WDMs are integrated with Experion. OneWireless integration also supports connecting a HART device through the OneWireless adapter through WDM. FDM supports all functions on the HART devices detected through the OneWireless network.

ATTENTION

WDM and all network components must be upgraded to OneWireless R220 or later.

Before using FDM with the OneWireless-connected devices, perform the following tasks in the recommended order.

1. Commission all the WDM and WDM-connected devices in OneWireless User Interface. FDM dynamically updates as the new devices are provisioned and activated in WDM after the first build network. This includes the HART devices connected to OneWireless Adapters (OWAs). For more information, see the OneWireless WDM User's Guide.
2. Configure the OneWireless network using the FDM Server Management tool. Specify the IP address of WDM while configuring the OneWireless network.

OneWireless network can be configured in one of the following scenarios.

- Experion-integrated OneWireless network configuration (WDM is associated with the Experion Server). For more information about configuring the Experion-integrated OneWireless network, refer to the section, [“Configuring FDM for Experion-integrated OneWireless network”](#)
- Standalone OneWireless network configuration (WDM is not associated with the Experion Server)

4.5.1 Configuring FDM for standalone OneWireless network

By configuring the standalone OneWireless network (without Experion integration), FDM can discover the WDM and the following connected devices.

- ISA100 Wireless devices
- HART device connected through OneWireless adapter

Prerequisites

- Enable the HART-IP server on WDM if any HART device is connected to WDM
- Commission all WDM and ISA100 Wireless devices
- Enable the GCI (Gateway General Client) interface on WDM

ATTENTION

The GCI interface is an external interface that is used with GCI-based client applications to communicate with ISA100 Wireless devices.

To configure FDM for standalone OneWireless 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. Type the Network Interface Name, and in the Network Type drop-down list click OneWireless Network.
6. Under IP Address Configuration, enter the IP addresses for a WDM, and then click Add IP. The specified IP address appears under OneWireless Configuration.

ATTENTION

If you want to delete the existing IP, click Delete IP.

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

7. Click OK.

4.6 Honeywell Experion network configuration

Honeywell Experion network in the FDM Server Management tool helps you configure, monitor, and perform device specific operations on the HART/FF/ISA100 Wireless devices/PROFIBUS/HoP connected to an Experion system.

Options to configure a network against Honeywell Experion are listed here.

- Honeywell Experion as a redundant or non-redundant server configuration
- Honeywell Experion-integrated Safety network with Universal Safe Modules configuration
- Honeywell Experion-integrated OneWireless network configuration

4.6.1 Configuring FDM for Honeywell Experion network

Prerequisites

When an Experion Server is configured as an FDM network, it cannot be used as an RCI node for any other FDM network interface.

To configure FDM for Honeywell Experion 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. Type the Network Interface Name, and from the Network Type drop-down list click Honeywell Experion PKS.
6. Under Redundancy:
 - Click Non Redundant and then type the Primary Server name if you are configuring FDM for a non-redundant server. By default, FDM populates Primary Server with LOCALHOST. If you leave this unchanged, FDM considers the local host as the Primary Server.
 - Click Redundant and type the names of the Primary and Secondary Servers if you are configuring FDM for a redundant server. By default, FDM populates Primary Server with LOCALHOST and Secondary Server with NOT SELECTED.

ATTENTION

The COM Port, Start Poll Address, BAUD Rate, End Poll Address and Retry Count fields are not applicable when configuring the Honeywell Experion network type. Hence, FDM disables these fields.

7. If you are configuring FDM for the Experion-integrated Safety network, select the Safety

Manager with Universal Safe Modules Present check box. For more details, refer to the section [“Configuring FDM for the Experion-integrated Safety network”](#).

8. If you are configuring FDM for the Experion-integrated OneWireless network, select the Wireless Device Manager Present check box. For more details, refer to the section [“Configuring FDM for Experion- integrated OneWireless network”](#).
9. Click OK to save the configuration.

ATTENTION

If the redundant system (secondary) stops responding, the primary server takes over the FDM operations automatically.

If you are adding a Honeywell Experion network, you cannot add other network communication interfaces on the same computer. A message appears prompting you to remove all existing networks when you try to add a Honeywell Experion PKS.

If the Experion server is not found on the system, a confirmation message appears.

Click Yes, if the network interface name matches with the Alias name of the Primary Server

Click No, if you want to modify the Experion Server Name/Network Interface Name (Alias Name).

4.6.2 Configuring FDM for the Experion-integrated Safety network

Prerequisites

Ensure that Safety Builder export file is imported to FDM. For more details, refer to the section [“Importing Safety Builder Export file”](#).

To configure FDM for the Experion integrated Safety 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 Honeywell Experion PKS and select the Safety Manager with Universal Safe Modules Present check box. The Enable Alarm Monitoring option is enabled.

ATTENTION

When the resource file is not imported, SMs are not available to configure the Experion-integrated Safety network and Safety Manager with Universal Modules Present check box is not available. In this case, if you try to add an Experion-

integrated Safety network,  appears. However, if you proceed with the Experion-integrated Safety network configuration, only Experion network is configured.

6. If you want to monitor the alarms for devices, select Enable Alarm Monitoring .

ATTENTION

The Enable Alarm Monitoring check box is enabled only if the MUX monitoring license is available.

7. Type the name of the Experion Server based on the redundancy.

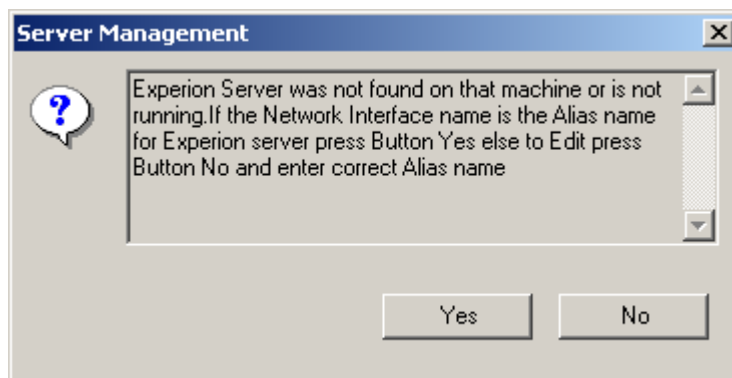
ATTENTION

The COM Port, Start Poll Address, BAUD Rate, End Poll Address and Retry Count fields are not applicable when configuring the Honeywell Experion network type. Hence, FDM disables these fields.

8. Click OK to save the configuration.

ATTENTION

By default, FDM populates Primary Server with LOCALHOST. If you leave this unchanged, FDM considers the local host as the Primary Server. If the Experion server is not found on the system, the following message appears.

**ATTENTION**

Click Yes, if the network interface name matches with the Alias name of the Primary Server.

Click No, if you want to modify the Experion Server Name/Network Interface Name (Alias Name).

If you try to add a Honeywell Experion PKS network on the computer where other network communication interfaces are configured, a message appears prompting you to remove all existing networks.

4.6.3 Configuring FDM for Experion-integrated OneWireless network

Prerequisites

- All WDM and ISA100 Wireless devices are commissioned
- If HART devices are connected to WDMs through OneWireless Adaptors, ensure that the HART-IP server is enabled on WDM
- Enable the GCI (Gateway General Client) interface on WDM.

To configure FDM for the Experion-integrated OneWireless 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. Type the Network Interface Name and in the Network Type drop-down list, click Honeywell Experion PKS.
6. Type the name of the Experion Server based on the redundancy.

ATTENTION

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

7. Under OneWireless, select the Wireless Device Manager Present check box.
8. Type the WDM's IP and click Add. The specified IP address appears under OneWireless Configured Server.
9. If you want to monitor the alarms for the devices, select Enable Alarm Monitoring.
10. Click OK.

4.7 Configuring Comm DTM network in FDM

PROFIBUS networks other than Honeywell PROFIBUS Gateway Module (PGM) can be accessed only by using FDT/DTM technology through specific gateways. Access to the gateways, PROFIBUS controllers, I/O modules, and any connected device is done using supported Comm and Gateway DTMs.

HART devices connected to I/O modules that support HoP, can be accessed either using device DTMs or EDDLs. PROFIBUS PA devices can be accessed either using device DTMs or the FDI Package option. Third-party HART interfaces that are supported by Comm DTMs may be similarly used. The FDT Comm Console allows you to configure FDT networks and build the complete networks using DTMs only on the connected RCI Server. For more details about building FDT networks, refer to the section [“Building FDT networks”](#).

To configure the Comm DTM 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 COMM DTM Interface.

6. Type the unique interface name in Network Interface Name box.
7. Type the name of the server in the RCI Server Name box.
8. Click OK to save the configuration.

TIP

Click View Details to view the details of the configuration in the FDM Server Management Tool.

ATTENTION

In case of Honeywell PGM, FDT network must be configured to access HART devices connected under remote IOs that do not support HoP (e.g. Phoenix Contact RIO).

4.8 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. After it is commissioned, the HART-IP network can be configured using the FDM Server Management tool. To configure a HART-IP network, specify the IP address range of all HART-IP devices in that network. Use the Build Network operation to discover all controllers and available HART devices.

Prerequisites

- All HART-IP connected devices are commissioned.
- 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 IPAddress Configuration:
 - To configure a HART-IP connected device (example, RTU2020), click Add IP and type the IP address.
 - To configure multiple HART-IP connected devices (example, RTU2020 nodes) simultaneously, 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 for RTU2020. If a different port number has been set in the RTU2020, enter that port number in this box.
8. Click Add IP. The specified IP address appears under HART-IP Configuration.

ATTENTION

To change the IP address or to delete the existing IP address, click Delete IP. The IP address will be 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.

4.9 Configuring FDM for Honeywell ControlEdge RTU Network

Honeywell ControlEdge RTU controllers and connected devices are supported by FDM via the creation of the Honeywell ControlEdge RTU Network. Before using FDM with any Honeywell RTU connected device, it is recommended (but not mandatory) that the devices are commissioned first. After commissioning, use the FDM Server Management tool to configure Honeywell ControlEdge RTU network. To configure a Honeywell RTU network, specify the IP address range of all connected RTUs in that network. Use the Build Network operation to discover all RTUs and available HART/ISA Wireless devices.

Prerequisites

- Ensure all RTU connected devices are commissioned.
- Enable the HART-IP interface and Wireless IO as applicable in Honeywell ControlEdge Builder.

To configure the RTU:

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 Honeywell ControlEdge RTU Network.
6. Under IPAddress Configuration:
 - To configure a Honeywell RTU, click Add IP and type the IP address.
 - To configure dual IP addresses, enter the second IP address in the second text box.
 - To configure multiple Honeywell RTU nodes simultaneously, click Add IP Range(s) and enter the range of IP addresses for those devices. (From address in the Add IP field and To address in the Add IP Range(s) field).

ATTENTION

In case of configuring multiple Honeywell ControlEdge RTU nodes with dual IP, then make sure to configure each node individually with the dual IP address. Add IP Range(s) option does not support addition of dual IP addresses.

7. In the Port No box, default port number is displayed as 5094 . If a different port number has been set in the RTU, enter that port number in this box.
8. Click Add IP. The specified IP address appears under Configured IP(s).

ATTENTION

To change the IP address or to delete the existing IP address, click Delete IP. The IP address will be deleted under Honeywell RTU 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.

4.10 Configuring FDM for Honeywell ControlEdge PLC/HC900 Network

ControlEdge PLC/HC900 controllers and connected devices are supported by FDM via the creation of the ControlEdge PLC/HC900 Network. Before using FDM with any ControlEdge PLC/HC900 connected device, it is recommended (but not mandatory) that the devices are commissioned first. After commissioning, use the FDM Server Management tool to configure ControlEdge PLC/HC900 network. To configure a ControlEdge PLC/HC900 network, specify the IP address of all connected PLCs in that network. Use the Build Network operation to discover all PLCs and available HART devices.

Prerequisites

- Ensure all PLC connected devices are commissioned.
- Enable the HART-IP interface as applicable in ControlEdge PLC/HC900.

To configure ControlEdge PLC/HC900:

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 Honeywell ControlEdge PLC/HC900 Network.
6. Under IPAddress Configuration:
 - To configure a single ControlEdge PLC/HC900, click Add IP and type the IP address.
 - To configure dual IP addresses, enter the second IP address in the second text box.
7. In the Port No box, default port number is displayed as 5094 . If a different port number has been set in the ControlEdge PLC/HC900, enter that port number in this box.
8. Click Add IP. The specified IP address appears under Configured IP(s).

ATTENTION

To change the IP address or to delete the existing IP address, select the IP under Configured IP(s) and then click Delete IP. The IP address will be deleted 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.

4.11 Configuring FDM for Honeywell TPS network

FDM-TPS integration supports configuration and maintenance of DE devices connected to a TPS system using the Honeywell TPS network. Before using FDM with any TPS connected device, it is recommended (but not necessary) that the devices are commissioned first. After commissioning the devices, configure the Honeywell TPS network using the FDM Server Management Tool by specifying the LCN identifier and the RCI node type. The Build Network operation is used to discover all DE devices connected to the TPS network through HPM and STIM IOPs (using the TPS DocTool).

ATTENTION

If Honeywell TPS network is configured, FDM supports Experion + Honeywell TPS network on one RCI node. However, FDM does not support all other networks (Safety Manager + Experion + OneWireless) along with Honeywell TPS network on the same RCI node.

Prerequisites

All TPS-connected DE devices are commissioned.

To configure the Honeywell TPS 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 Honeywell TPS.
6. Create and add LCN identifier.

ATTENTION

FDM requires a unique identifier to differentiate multiple LCNs connected to the same FDM Server.

To create LCN IDs:

- a. Under LCN Configuration, click Add/Remove LCN ID.
- b. In the FDM-Add LCN Identifier dialog box, type the LCN identifier and Description.
- c. Click Add. The LCN IDs are listed under Available LCN IDs.
- d. Click Close to close the FDM-Add LCN Identifier dialog box.
- e. From the LCN Identifier drop-down list box, select the LCN ID.

The LCN ID selection enables all other fields such as RCI configuration, redundancy of the nodes, and UCN configuration as shown in the following figure.

7. Under RCI Configuration:
 - From the RCI Node Type drop-down list box:
 - Select ESV-T.
 - Select ES-T, only if there is a need for load distribution across multiple RCIs for the same LCN, provided there is no ESV-T available.

TIP

If multiple ESV-Ts are connected to the LCN and if there is a need for load distribution, preference must be given to ESV-T instead of using ES-T as an additional RCI.

- If ESV-T is the selected as the RCI Node Type, redundancy is supported. Perform these additional Redundancy settings.
 - If you have a non-redundant ESV-T, click Non Redundant and then type the RCI Server name. By default, FDM populates RCI Server Name with LOCALHOST. If you leave this unchanged, FDM considers the local host as the RCI Server (Primary Server).
 - If you have a redundant ESV-T, click Redundant and then type both Primary and Secondary RCI server names. By default, FDM populates Primary Server with LOCALHOST and Secondary Server with NOT SELECTED.

To configure both Experion and TPS networks on the same RCI node, ensure that both Primary and Secondary Servers of the Experion machine match the Primary and Secondary Servers of TPS machine, respectively.

DITR410SVR_TPS	DITR410SVRA	Honeywell TPS	Redundant Server : DITR410SVRB
DITR410SVR	DITR410SVRA	Honeywell Experio...	Redundant Server : DITR410SVRB

ATTENTION

ES-T node does not support redundancy.

- In the DOCTool ES-T Address box, type the LCN address of the selected ES-T node (Engineering Station). It is recommended to use Engineering Station instead of using User Station for DocTool.

The DocTool application, which is on ES-T node, is used for discovering the network hierarchy for TPS-connected DE devices.

8. Under UCN Configuration, by default all available UCNs are listed under Configured UCNs box. FDM discovers devices which were under the Configured UCNs box only. For load balancing, you can configure multiple RCIs for one LCN, where each RCI is associated to a set of UCNs. If

you want to remove some of the configured UCNs for load distribution, you can click  or click  to remove all UCNs under Configured UCNs box.

ATTENTION

The FDM network configuration ensures that the same UCN is not assigned to two different RCIs per LCN network.

9. Click OK.

4.12 Editing a network configuration

To edit a network configuration:

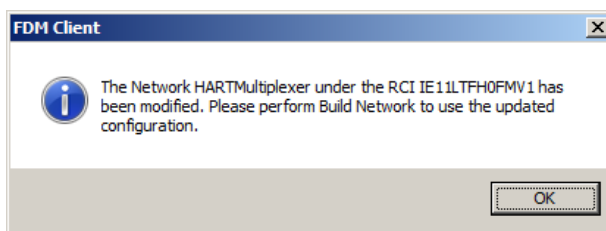
1. Log on to FDM Server Management Tool. The FDM Server Management dialog box appears.
2. Click Network Configurator in the left pane. In the right pane, the list of configured networks are displayed.
3. Select the network from the list and then click Edit. The Edit Network pane appears.
4. Make the necessary changes to the network configuration in the Edit Network pane. However, you cannot edit the Network Interface Name and Network Type. You cannot enable/disable the MUX Monitoring option for RS-485 HART Multiplexer and Alarm Monitoring option for Experion network. To enable/disable the MUX Monitoring option, refer to the section [“Configuring FDM for an RS-485 HART Multiplexer”](#) and [“Configuring FDM for Honeywell Experion network”](#).

ATTENTION

When editing the Safety Network with Universal Safe Modules network configuration, you can add/remove SM(s).

5. Click OK to save the modified the network configuration.

For example, after you edit a network, the following confirmation message appears in the FDM Client, only if the FDM Server is running.



In the Network view, the nodes under the network are deleted for the edited network. You must rebuild the network to discover all the nodes for the edited network.

ATTENTION

Even when the FDM Server is stopped, the FDM RCI keeps running to store the network information. When the FDM Server is stopped, any modification to the configured network will be effective only when the FDM Server starts again.

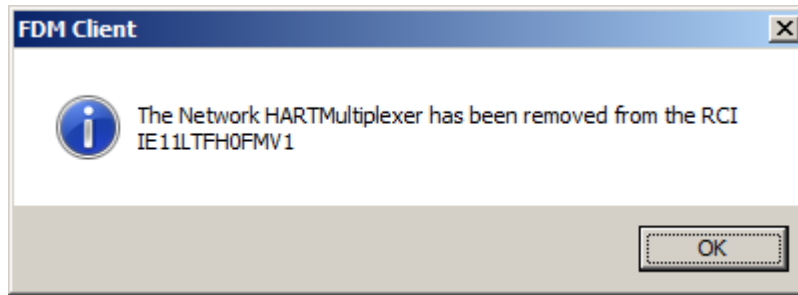
To edit the COMM DTM Interface, close the FDT Comm Console on that FDM RCI before editing the network. Restart the FDT Comm Console after editing that network.

4.13 Deleting a network configuration

To delete an existing network configuration:

1. Log on to FDM Server Management Tool. The FDM Server Management dialog box appears.
2. Click Network Configurator in the left pane. In the right pane, the list of configured networks are displayed.
3. Select the network from the list and click Delete. Click Yes to acknowledge the confirmation message.

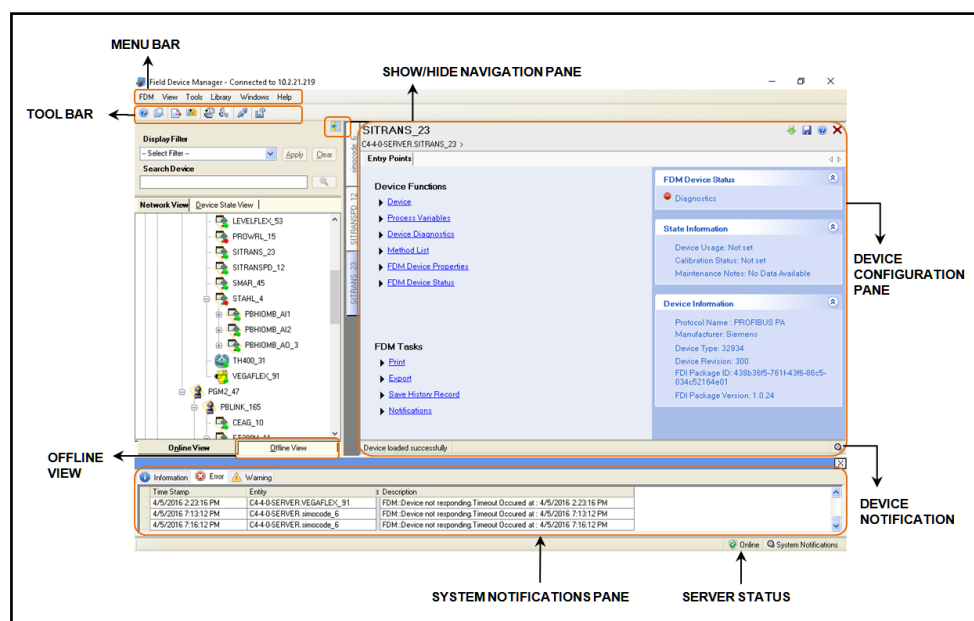
For example, after you delete a network, the following confirmation message appears in the FDM Client only if the FDM Server is running.



The devices are disconnected from the network and moved to the Disconnected Nodes list in Network view.

UNDERSTANDING THE FDM CLIENT USER INTERFACE

When you log on to the FDM Client after configuring the network, the main window appears, with groups arranged in a tree view in the left pane. By default, the Online View group appears. Also, by default, devices are not visible until a Build Network operation is performed on each network.



FDM Client user interface consists of:

- **Menu bar** –FDM specific menu items which provide access to functions to interact with an application.
- **Toolbar** – Icons or menus such as Help, Import and Export icons, Plant Area View, and so on.
- **Online View** – Network View, Device State View, Display Filter, and Search Device tabs. It is mainly used for configuring and viewing HART, FF, PROFIBUS, ISA100 Wireless, HoP, and DE devices that are connected to FDM.
- **Offline View** –Offline Configuration, Display Filter, and Device Library tabs. It is used for all offline activities like managing offline configuration, managing display filters for the Network Tree view, and to view the Device Library that lists all DDs and DTMs available in FDM.
- **Device Configuration** – Provides an option to view the current configuration settings of a device and to download configurations from FDM to devices in the field.
- **Device Notifications** –Information, Error, and Warning tabs. It provides the notification of any error, information, and warning after you perform few operations in device configuration page.
- **System Notifications** –Information, Error, and Warning tabs. It provides the status of the operation that is performed in FDM Client/FDT Comm Console.
- **Server status** – Indicates the server polling status on the FDM Client status bar.

5.1 Online view

Online View consists of two tabs:

- Network View
- Device State View

5.1.1 Network View

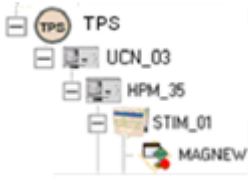
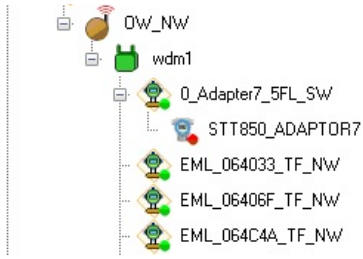
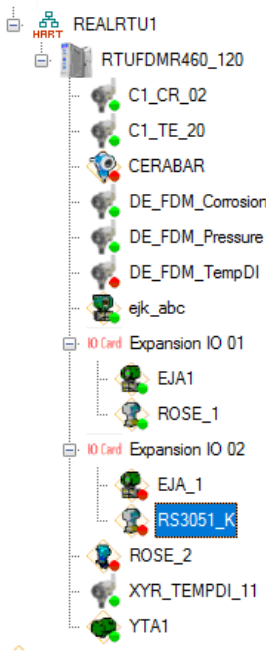
The Network View lists all devices that are currently connected and disconnected with the selected server through the network communication interface. It displays the complete hierarchy that includes the server, network communication interface, and all the field devices belonging to the connected server, and unhealthy devices.

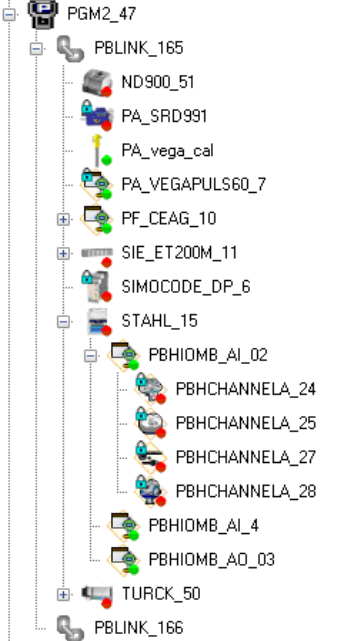
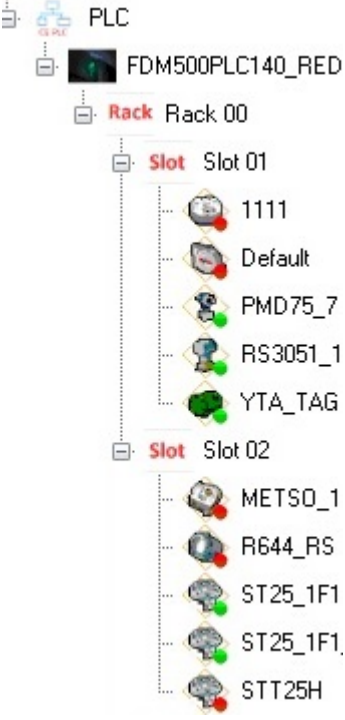
You can perform the following tasks in the Network View by right-clicking a device and selecting the appropriate option.

- Device configuration
- Comparing device configuration (currently supported only for DD based devices and DE devices)
- Viewing/deleting device history
- Viewing audit trail
- Locking and unlocking a device
- Downloading a DD/DTM based offline configuration to an online device
- Renaming FDM tags, when applicable
- Logging user-defined audit trail actions
- Device documentation at device level

The hierarchy of Network view is shown here.

	FDM SERVER RCI SERVER NETWORK COMMUNICATION INTERFACE
	NETWORK COMMUNICATION INTERFACE PROCESS GROUP SAFETY GROUP
	NETWORK COMMUNICATION INTERFACE
	NETWORK COMMUNICATION INTERFACE
	NETWORK COMMUNICATION INTERFACE

	FDM SERVER RCI SERVER NETWORK COMMUNICATION INTERFACE
	NETWORK COMMUNICATION INTERFACE
	NETWORK COMMUNICATION INTERFACE
	NETWORK COMMUNICATION INTERFACE

	FDM SERVER RCI SERVER NETWORK COMMUNICATION INTERFACE
	NETWORK COMMUNICATION INTERFACE
	NETWORK COMMUNICATION INTERFACE

- The Network View displays the complete hierarchy for all configured networks like Modem network, Multiplexer, Standalone Safety network, Standalone OneWireless network, HART-IP network, and TPS network. The complete hierarchy includes the FDM Server, RCI Interface name, FIM, links, Communication DTMs, Gateway DTMs, IO DTMs, SM controllers, IOTAs, HART channels connected to IOTAs, WDMs, OneWireless adapters, RTU, UCNs, HPMS, STIM, and all field devices belonging to the connected server.
- In case of the Honeywell Experion PKS network with Safety Manager and OneWireless, the Network View displays the complete hierarchy including FDM Server, RCI Interface name, and Process and Safety network groups. Under the Process network group, Experion Controllers, IOs, FIM, links, PGMs, WDMs, OneWireless adapters, ISA100 Wireless devices, HART devices connected to Experion server are displayed. Under the Safety network group, SM controllers, IOTAs, and HART channels connected to IOTAs are displayed.
- In case of Honeywell Experion PKS network with OneWireless (without Safety Manager), all Experion nodes, WDMs, OneWireless adapters, ISA100 Wireless, Wireless HART devices and HART devices connected to the OneWireless adapter directly under the Experion network are displayed.

TIP

When a redundant Experion network is configured, the RCI interface name appears corresponding to the RCI, which is currently disconnected in the Network View. If the primary server stops/fails, the RCI Interface name appears as secondary server's name, by default.

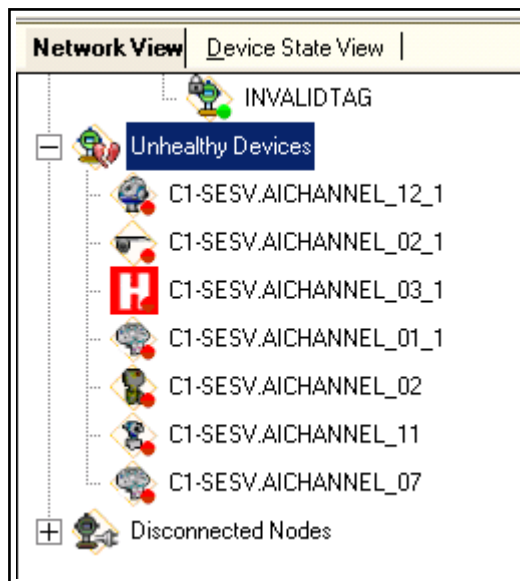
ATTENTION

When using FDM with a HART DE Modem connected to a device, do not connect another handheld to the device. However, if you connect the handheld to a device and change a few parameters, the device appears in FDM Client Network View even though the device is not available in the network.

Unhealthy devices

The device health is displayed when the device is discovered for the first time during the Build Network operation. A healthy device is indicated by green; an unhealthy one by red. The unhealthy devices are listed under Unhealthy Devices.

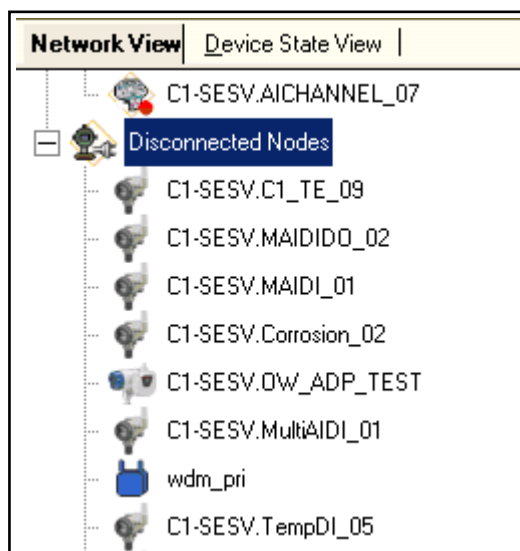
By default, the latest unhealthy device appears at the top of Unhealthy Devices hierarchy. All unhealthy nodes are sorted based on the time when the health status changed to unhealthy.

**ATTENTION**

The device health status can be monitored using Plant Area View. For more information, refer to the section [“PlantArea View”](#).

Disconnected nodes

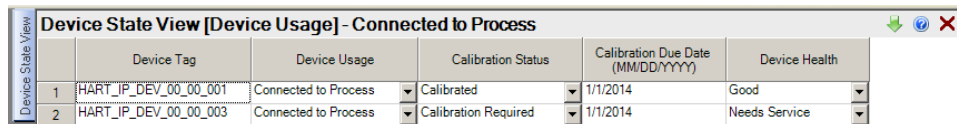
Any node that is disconnected from a network is moved to the Disconnected Nodes list. You can view the device history, rename the device tag, and delete the device tag from the Disconnected Nodes list.

**ATTENTION**

The device connection status can be monitored using Plant Area View. For more information, refer to the section [“Plant Area View”](#).

5.1.2 Device State View

The Device State View tab displays the state of both devices that are connected to the network or disconnected from the process. You must manually assign the devices to various device states from the FDM Device Properties tab in the Device Configuration page or from the Device State View tab.



	Device Tag	Device Usage	Calibration Status	Calibration Due Date (MM/DD/YYYY)	Device Health
1	HART_IP_DEV_00_00_001	Connected to Process	Calibrated	1/1/2014	Good
2	HART_IP_DEV_00_00_003	Connected to Process	Calibration Required	1/1/2014	Needs Service

These devices can be spares, connected to the process, disconnected for maintenance, or decommissioned. The different states of devices are listed here.

- Calibration Status – Status of devices are displayed as Calibrated, Calibration Required or Not set.
- Device Health – Device status is displayed as Good, Needs Service, Not Set, Sent to Repair, or Discarded.
- Device Usage – Device status is shown as Connected to Process, Decommissioned (device should not be used), Disconnected from Process, Not set, or Spare.

You can change the device state (Device Usage, Calibration Status, and Device Health) from the Device State View page and then download the modified device parameters.

ATTENTION

The device connection status and health status can be monitored using Plant Area View. For more information, refer to the section [“Plant Area View”](#).

For more details about changing device state from device configuration page, refer to the section [“Editing deviceproperties “](#).

5.1.3 Understand the icons

Icons appearing in the Network and Device State Views are listed here.

If the icon is...	Then it represents...	If the icons is...	Then it represents...
Network View			
	FDM Server Node		Remote Communication Interface
	RS-485 HART Multiplexer Network		Experion Network
	Honeywell HART DE Modem		HART Modem
	C200/C200E Controller Module/ FIM2		1756 HART I/O Module
	PM HART I/O Module		Series C I/O/Series 8 I/O Module
	IO Link Module		C300 Controller Module
	COMM DTM Interface		FIM4, FIM8
	FIM2, FIM4 Links		FDT Gateway DTM
	FDT Communication DTM		Device DTM
	SM controller		IOTA
	Process Network group		Safety Network group
	Standalone OneWireless network		Wireless Device Manager
	HART-IP network		RTU

If the icon is...	Then it represents...	If the icons is...	Then it represents...
	TPS network		TPS controller (UCN/HPM)
	TPS IO module (STIM)		Disconnected Nodes
	Unhealthy devices		
	Calibration Status		Calibration Status (Calibrated, Calibration Required, and Not Set)
	Device Health		Device Health – Different States (Discarded, Good, Needs Service, Not set, Sent to Repair)
	Device Usage		Device Usage – Different States (Connected to Process, Decommissioned, Disconnected from Process, Not set, Spare.)

5.2 Offline View

The Offline View group consists of three tabs:

- Offline Configuration: Used to configure a set of device parameters without the need for a device to be available physically. For more information, refer to the section [“About Offline Configuration”](#).
- Display Filter: Used to filter the nodes/devices displayed in the Online View > Network View tree. For more information, refer to the section [“Display filters”](#).
- Device Library: It has the DD Library and DTM Library hierarchy.

5.2.1 DD library

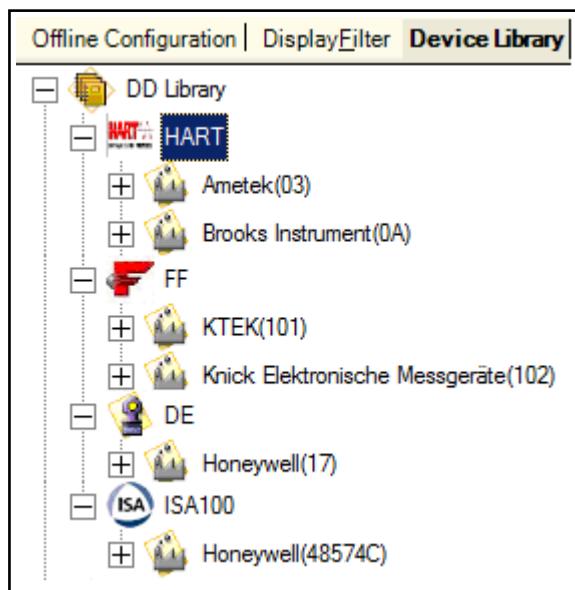
The DD Library has the following information about HART, FF, and ISA100 DDs available in FDM.

ATTENTION

The DD library has DE protocol to provide the specific information about templates only.

- Manufacturer name/ID
- Device type
- Device revision
- DD revision
- Manufacturer IDs are in Hexadecimal format for a given manufacturer are different for different protocols (HART, FF, and ISA100).

Device information is displayed in a hierarchical structure.



You can manage (attach/modify or upload/detach) the device documentation at the device type level using the Device Library tab. For more details on attaching/detaching/modifying or uploading device documentation, refer to the section [“Device documentation-related operations at system/device levels”](#).

You can transfer the DD files from FDM to any other system such as Experion or Asset Manager. For example, to receive alarms/events from the DD supported devices into Experion and Asset Manager (AM), all DD files must be loaded into Experion and AM.

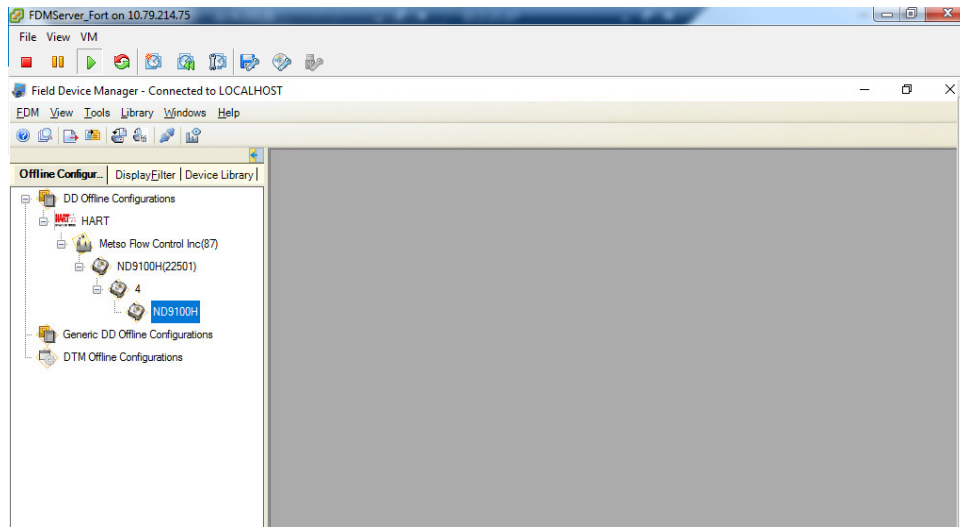
In such a scenario, to transfer the DD files from FDM:

1. From the device library, select the protocol, and then click Manufacturer ID > Device Type > Device Revision > DD Revision.
2. Copy the DD file from the FDM Server node available at: <Custom Installation Path>\ProgramData\Honeywell\FDM\Server\Database\Release\ to the other system to which you want to transfer the DD file. You can navigate to the corresponding DD using the information from step 1.
3. Import the DD file using the Import feature from the respective application. For example, in Experion, use the Device Description Manager utility to import the DD file. For more information about Device Description Manager utility, refer to the HART IO Implementation Guide.

5.2.2 Offline View Group

The Offline View group consists of three components:

- DD Offline Configuration
- Generic DD Offline Configuration
- DTM Offline Configuration



A device can be configured offline in two scenarios:

Scenario 1:

When a user is waiting for the device to be delivered. The device can be configured offline in the following way.

Prerequisites:

- DD of the device to be configured should be available in the Device Library.

Steps to configure device offline:

1. Right-click on the DD Offline Configuration.
2. Select Create to create the offline configuration of the selected device. DD Offline Configuration window appears.
3. Select the Communication protocol, Manufacturer, Device Type, Device Revision, and DD Revision and click Create to create the offline configuration of the selected device. A configuration data is created.

NOTE

If no content is displayed in configuration view area, it means that the device does not support offline enhancement view. In such case, inform the service vendor for the enhanced DD file of the device which support the offline functionalities.

4. An Entry Point page appears. It contains following options:
 - a. Device Function – It accepts the function/information from the DD file.
 - b. FDM Tasks – It refers to the task assigned by the FDM (Honeywell Host). It is also referred as Asset Management Tool.
5. Under Device Function, right-click on Offline view. The offline menu differs from vendor to vendor. Depending on the menu options, enter the required information for device parameters.

6. Click Save. A window will appear prompting you to enter Configuration Name, enter the desired name and click Ok.
7. Select the required device parameter from the list of all the offline parameters available which appears on the screen and click Save.
8. A message box appears, prompting that the offline configuration is saved successfully.
9. Once the Offline View of a device is created and the device is connected. Right-click on the device in Offline Configuration tab and click Download Offline Configuration. It allows you to download the offline configured parameters.

Scenario 2:

When device is connected but user wants to configure the device offline. It can be configured offline in the following way.

1. Right-click on the required device and select Configure with DD or DTM.
2. Under FDM Tasks, select Save As Offline Template.
3. Offline Tree will appear in the Offline Configuration tab, which will contain the offline template.
4. Right-click on the saved template and select Open to open the template. Depending on the menu options, enter the required information for device parameters.
5. Click Save. A window will appear prompting you to enter Configuration Name, enter the desired name and click Ok.
6. Select the required device parameter from the list of all the offline parameters available which appears on the screen and click Save.
7. A message box appears, prompting that the offline configuration is saved successfully.
8. Once the Offline View of a device is created and the device is connected. Right-click on the device in Offline Configuration tab and click Download Offline Configuration. It allows you to download the offline configured parameters.

5.2.3 DTM library

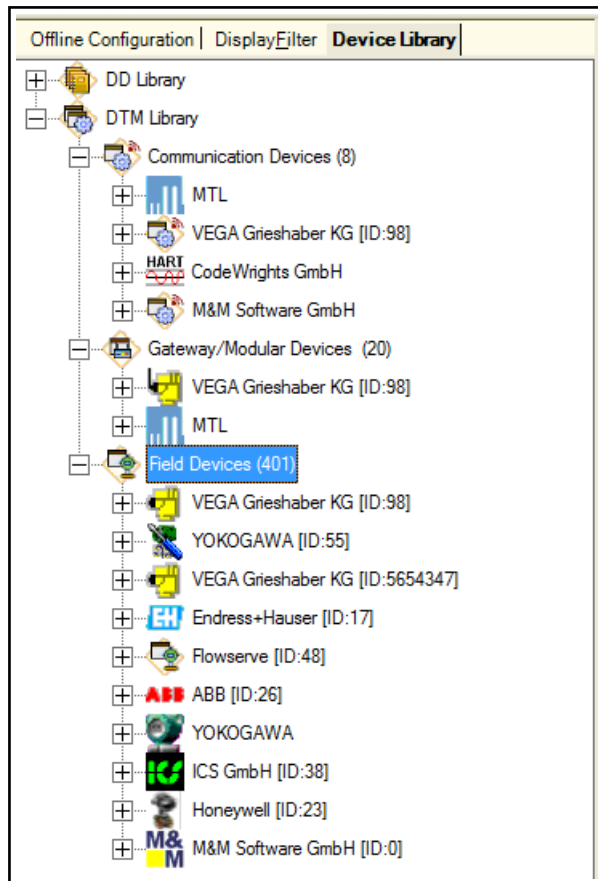
The DTM Library displays three types of DTMs along with the number of DTMs of each type.

- Communication devices
- Gateway/modular devices
- Field devices

It has the Manufacturer name/ID device information for each device type.

All DTMs that are installed and updated using the DTM Library Manager utility are reflected in the DTM library even if they are not used by FDM. If DTM is installed on the computer and not updated, it is not reflected in the DTM library.

Device information is displayed in a hierarchical structure.



5.2.4 FDI Package library

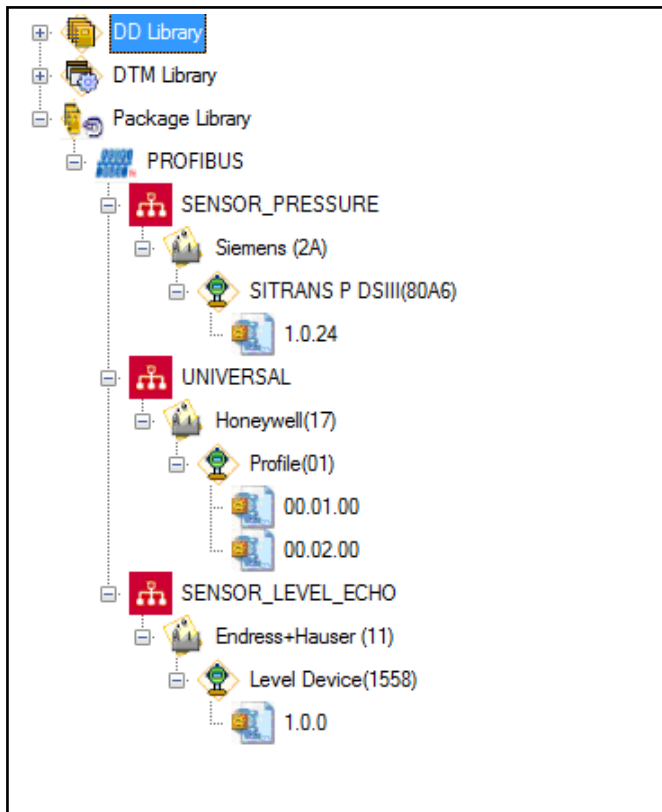
The Package Library has the following information about PA EDDs available in FDM.

ATTENTION

The DD library has DE protocol to provide the specific information about templates only.

- Manufacturer name/ID
- Device type
- Device revision
- DD revision
- Manufacturer IDs are in Hexadecimal format for a given manufacturer are different for different protocols (HART, FF, and ISA100).

Device information is displayed in a hierarchical structure.

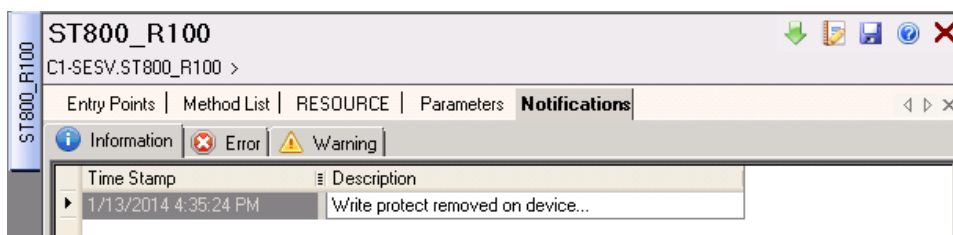


5.3 Device notifications

Notifications of errors, information, or warning that occur due to an operation performed in a device configuration page appear in the Notifications pane. All three tabs – Information, Error, and Warning display the Time Stamp and Description for all operations.

To view device notifications, click the Notifications link under FDM Tasks in the device configuration

page. Alternatively, click  from the lower-right of the device configuration page to view device notifications.



Only the changes made related to the write protection status of the device will be displayed on the Notifications tab and no other device changes will be reflected.

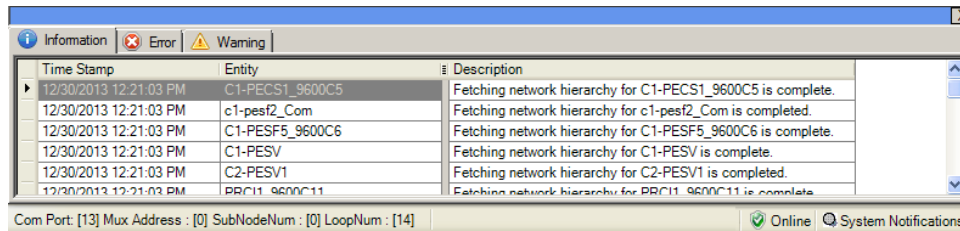
Each tab supports a maximum of 1000 rows. If this is exceeded, the first row is removed and at the end, the new row is added.

Right-click anywhere in the Notifications pane and click Clear Row(s) to clear the contents of the window.

5.4 System notifications

After you perform any operation in FDM Client/FDT Comm Console, its status appears in the System Notifications pane. The three tabs - Information, Error, and Warning, display Time Stamp, Entity, and Description for all operations.

To view the System Notifications pane, choose View > System Notifications. Click  to hide this pane.



Each tab supports a maximum of 1000 rows. If this is exceeded, the first row is removed and at the end, the new row is added.

Right-click anywhere in the Notifications pane and click Clear Row(s) to clear the contents of the window.

5.5 Server poll status indication

The FDM Server polls all open clients that are connected to it at regular intervals to know their status. The status indicator on the FDM Client status bar shows the status.

The polling states are described here.

- **Online:** Indicates that the server is actively polling the client at regular intervals.
- **Polling Delay:** Indicates that the server has not polled the client within the specified interval. This is an indication that the server is busy performing some other operation.
- **Polling Stopped:** If the server does not poll the client within a time interval greater than a predefined maximum time interval, the status changes to Polling Stopped. This usually indicates that the server is busy, has stopped or terminated, or that the server has stopped responding.
- **Polling Resumed:** If the Server is temporarily busy, the status can show Polling Delay or Polling Stopped depending on the time interval that FDM Server has not polled the client. The moment Server resumes polling the client, the status changes to Polling Resumed and subsequently back to Online.

ATTENTION

Polling Stopped status must not be construed as evidence that the FDM Server has stopped responding. In all possibility, the Server might be busy performing some operation. Refer to the FDM Troubleshooting Guide on how to determine whether the server has terminated or has stopped responding.

TIP

Placing the mouse pointer over the status area gives a short description of the current poll status.

FDM ROLE-BASED USER MANAGEMENT

FDM provides a robust role-based user management. There are two user verification mechanisms called FDM Classic Server Security and Windows Security. FDM supports adding an existing Windows user group to FDM and assigning specific roles to it.

FDM Classic Server Security

FDM user management allows creation of users with in-built authentication mechanism called FDM Classic Server Security. The user credentials such as user information, password, and so on are stored in the FDM Server database. At the time of login, the user credentials provided by the user are authenticated by the FDM Server.

Windows Security

If the Windows Security option is selected, FDM does not maintain the password information in its database. During login, FDM uses Windows security to authenticate the user. FDM also supports Windows groups as this simplifies the task of associating a large number of users to a specific role in FDM. The Single Sign On feature is supported for all users who choose Windows Security.

FDM supports Windows security in:

- A Windows work group
- A Windows domain

Support for Windows groups

FDM supports adding an existing Windows user group to FDM and assigning specific roles to it. The FDM Group Manager is used for managing FDM groups. Instead of associating one user to a specific FDM role, an administrator can create a Windows group and associate it with a specific role in FDM. This provides the administrator flexibility to associate any number of Windows users to that group. After a group is associated with a role, all users associated with that group inherit the group's privileges. FDM creates the following default groups during installation.

- FDM Administrators – User added to this group has all the privileges of the FDM administrator role.
- FDM Supervisors – User added to this group has all the privileges of the FDM supervisor role.
- FDM Engineers – User added to this group has all the privileges of the FDM engineer role.
- FDM Operators – User added to this group has all the privileges of the FDM operator role.
- FDM Access Group – This group is created on all the systems where FDM components are installed. FDM Access Group is not associated with any of the FDM roles. This group is associated with certain Windows privileges which are needed to start the FDM Client. Any FDM Windows user/ domain user who wants to start the FDM Client must be added to this group.

The user can add new Windows groups in FDM. To manage the groups in FDM, refer to the section [“Group management”](#).

6.1 Roles and privileges

FDM provides robust, role-based user management. FDM has a set of privileges that you can possess, and these privileges are grouped to form the roles. A role is a set of privileges with a common name. A user or a group can get the privileges by being associated with one of the roles. FDM has these predefined roles.

- **Administrator:** These users have full access and privileges to all functions of FDM. They are mainly responsible for managing users, processing user requests, and updating user data.
- **Engineer:** The user with this role enables the FDM user to change the values of certain parameters and other related settings, when necessary.
- **Supervisor:** These users are provided with the read and write permissions to FDM. They are allowed to make changes in the database and to change the operational settings, as required.
- **Operator:** These users are provided with very limited access to change any configuration. They are assigned the privileges to monitor the status of operations and respond to alarms.

In addition to these roles, other roles can be created based on the needs of your organization. Additional privileges to the predefined roles can also be assigned. However, the default privileges associated with the predefined roles cannot be removed.

ATTENTION

Privileges for administrators cannot be modified.

A summary of the default role-based access privileges enforced by FDM for performing different operations are listed here.

Function	User role				For more information, refer to...
	Administrator	Supervisor	Engineer	Operator	
Build Network	Yes	Yes	Yes	Yes	“Build networks”
Write Parameters	Yes	Yes	Yes	No	“Configuring a HART device using DD”
Compare Configuration	Yes	Yes	Yes	Yes	“Comparing configuration”
Change Device State	Yes	Yes	Yes	No	“Editing device properties”
Change Network	Yes	No	No	No	“Configuring networks”
Add/Delete DD/DTM	Yes	No	No	No	“Device Description file management” and “DTM management”
FDM Server start/stop	Yes	No	Yes	No	“Updating the FDM Server status”
FHM Create/Modify/Delete	Yes	Yes	Yes	Yes	User role privileges
Upgrade License	Yes	No	No	No	“Updating the FDM license”
Execute Method	Yes	Yes	Yes	No	“Executing methods”
Create/Modify/Delete User	Yes	No	No	No	“User management”

Function	User role				For more information, refer to...
	Administrator	Supervisor	Engineer	Operator	
					t
Create/Delete Role	Yes	No	No	No	“Roles management”
Rename Node	Yes	No	Yes	No	
Save/Delete History	Yes	No	Yes	No	“Saving history records”
Lock/Unlock Device	Yes	Yes	Yes	No	“Device access control”
Create/Edit/Rename/ Delete Offline Configuration	Yes	No	Yes	No	“About Offline Configuration” FDI Device Package Management
Download/ BulkDownload Offline Configuration	Yes	Yes	Yes	No	“Downloading bulk offline configurations”
Create/Edit/Rename/ Delete Display Filter	Yes	Yes	Yes	No	“Display filters”
Attach/Detach/Upload Documents	Yes	Yes	Yes	No	“Device documentation-related operations at system/device levels”
FDM Settings	Yes	No	No	No	“FDM settings”
Access FDMTagBuilder	Yes	No	Yes	No	FDM Tag Builder

Function	User role				For more information, refer to...
	Administrator	Supervisor	Engineer	Operator	
Tool					section in MUX Monitoring Solution User's Guide
Delete Device from disconnected nodes list	Yes	Yes	Yes	No	“Deleting device tags”
Import/Export	Yes	No	No	No	“Import and export operations” Import and Export Operations
Create/Modify/Delete Group	Yes	No	No	No	“Group management”
Modify Write Access for Process Active Devices	Yes	No	No	No	“Customizing the network settings”
Create/Edit/Delete Device Filters	Yes	No	No	No	“Display filters”
Bulk Operations	Yes	No	Yes	No	“Bulk operations”
Delete Records	Yes	No	No	No	“Delete records”
FDT Health Scan Settings	Yes	No	No	No	“Customizing the FDT health scan settings”
Edit PlantAreaView	Yes	No	No	No	“Editing projects in Plant Area View”

Function	User role				For more information, refer to...
	Administrator	Supervisor	Engineer	Operator	
Reset and Build Network	Yes	No	No	No	“Soft resetting a multiplexer”
Create/Edit/Rename/ Delete PVST Schedule	Yes	No	Yes	No	FDM PVST Planner User’s Guide
Execute/Cancel/ Acknowledge PVST	Yes	No	Yes	Yes	

6.2 User management

FDM has a robust user management feature to prevent unauthorized access and to ensure security of the system. It is classified into two categories based on the chosen authentication type.

- Classic Server Security
- Windows Security

ATTENTION

For an efficient authentication mechanism, it is recommended that you use Windows Security instead of FDM Classic Server Security. Using Windows Security, you can add/modify/delete users, manage passwords, manage overall password lockout policies, and so on.

If using FDM Classic Server Security, secure the password. FDM does not have password lockout policy unlike Windows based security.

For more information about Classic Server Security and Windows Security, refer to the section [“FDM role-based user management”](#).

Current User Info enables you to view the details of the current user who has logged on to FDM. To view current user details, choose View > Current User Info.

6.2.1 Adding a new user in Classic Server Security

ATTENTION

Only Administrators with Create/Modify/Delete user privilege can add a user.

To create a user with authentication type as FDM Classic Server Security and assign a role:

1. From the FDM Client, choose Tools > User Management. The User Manager pane appears, displaying the list of existing users and their roles in the right pane.
2. Click Add New User. The Add User pane appears.
3. Type the Login Name.
4. Select Classic Server Security from Domain Name.
5. Type the Password and retype the password in Confirm Password.
6. Click User Information tab to add user details.
7. Type the First Name, Middle Name and the Last Name of the user in the corresponding fields.
8. Type other details like Mailing address, Email ID, Telephone, and so on.

ATTENTION

Only the First Name field is mandatory on this tab. All other fields are optional.

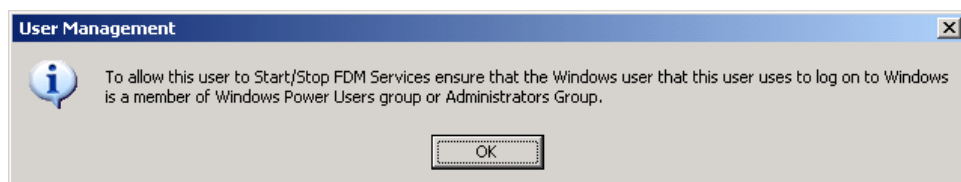
9. Click the Role Information tab. Select a role for the user from the drop-down list.
10. Depending on the role you select, the default associated privileges for the selected role are enabled.

ATTENTION

The check boxes against the privileges associated with a role are selected by default and appear in gray. To assign additional privileges to the user, select the check box against the privileges of your choice.

You cannot remove the default privileges assigned to a role.

While adding any new user to the role of Engineer or Administrator, the following message appears.



11. Click Save to save the user information.

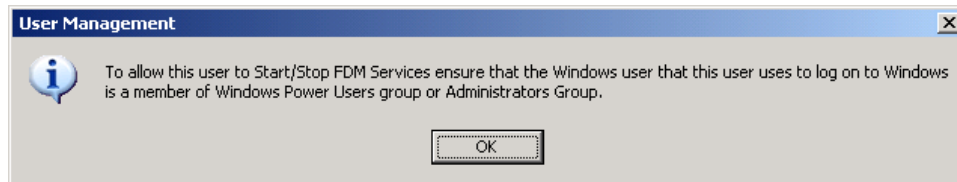
6.2.2 Adding a user in Windows Security

A Windows user can be assigned to an FDM role in these two ways.

- Associate a single Windows user to one of the roles in FDM.
- Associate a Windows group to a role in FDM, and then add any number of Windows users to the Windows group using Windows user management tools.

ATTENTION

While adding any new user to the role of Engineer or Administrator, the following message appears.



To add a user to Windows Work Group:

1. Create a Windows user on the FDM Server.
2. Add this user to the FDMAccessGroup on the FDM Server.
3. Create the same user on all the systems where FDM Client and FDM RCI are installed. Ensure that the password is same as that of the user in the FDM Server.
4. Add this user to the FDMAccessGroup on all the systems.

To add a user to Windows Domain:

1. Create a Windows user in the domain controller system.
2. Add the Windows domain user to the FDMAccessGroup on all the systems where FDM components (FDM Server, FDM Client, and FDM RCI) are installed.

ATTENTION

FDMMngr user must be created in the domain controller system with the same password as is used everywhere to enable users of domain controller to logon to FDM.

To associate a single Windows user to a role in FDM:

1. From the FDM Client, choose Tools > User Management. The User Manager pane appears, displaying the list of existing users and their roles in the right pane.
2. Click Add New User. The Add User pane appears.
3. Type the Windows Login Name.

ATTENTION

The Windows user password is considered automatically; you cannot edit the same.

4. Select the Domain from the drop-down list.
5. Repeat the steps 5 through 9 of [“Adding a new user in Classic Server Security”](#).

TIP

Click View Details button in the Server Management Tool to view the following details.

- Login Information
- User Information
- Role Information

Click Refresh to get the updated information from the system, if multiple users are performing user management tasks simultaneously.

ATTENTION

The installation of FDM creates a default Windows user by the name FDMMgr and adds it to FDM Administrators group and FDMAccessGroup on the Server system. FDMMgr is a local Windows user and is present on all nodes wherever FDM component is installed.

If the password policy has changed, ensure that the password is changed with respect to the new password policy in all FDM systems.

To reset the password on all nodes where FDM component is installed:

1. Right-click Computer on the desktop, and click Manage. Depending on the operating system installed one of the following windows appears.
 - Computer Management window appears if using Microsoft Windows 7 Professional
 - Server Manager window appears if using Microsoft Windows Server 2008 R2 Standard
2. In the left pane, expand System Tools > Local Users and Groups > Users.
3. In the right pane, right-click FDMMgr, and click Set Password.

To assign a Windows user to FDM by adding the user to one of the FDM groups:

1. On the FDM Server Start menu, right-click Computer and click Manage. The Server Manager dialog box appears.
2. In the Server Manager tree, expand Configuration > Local Users and Groups > Groups. The list of groups appears in the right pane.
3. Right-click FDM Group and click Add to Group.
4. Add the Windows user to this group and click OK.

For example, right-click the FDM Supervisors group and add the Windows user to this group. The user inherits all the privileges of the FDM Supervisors.

6.2.3 Modifying user details

ATTENTION

Only users with Create/Modify/Delete user privileges can modify details of all users and delete a user.

Users not having Create/Modify/Delete user privileges can modify their own details on the Login Information and Role Information tabs.

To modify the details of an existing user account:

1. From the FDM Client, click Tools > User Management. The User Manager pane appears, displaying the list of existing users and their roles in the right pane.
2. Select a user that you want to edit from the list of users.
3. Click Edit User to modify the information of the selected user. The Edit User pane appears.
4. Make the necessary changes to the user information under the Login Information tab.

ATTENTION

You can modify the password. However, do not modify the Login Name.

You cannot modify the password of a Windows user.

Any modification in user information does not take effect until you logon to the client again.

5. Click the User Information tab and make necessary changes to the user information, as required.
6. Click the Role Information tab and modify the user's role and privileges, if required.

ATTENTION

You cannot modify the default privileges assigned to a role. FDM disables the check boxes corresponding to the default privileges.

7. Click Save to save the modifications to the user account.

To delete a user:

- Select a user account, and click Delete User.

ATTENTION

You cannot delete the default Administrator user.

6.3 Group management

Managing groups involves these tasks:

- Adding a Windows Group and associating a Role
- Modifying a Group
- Editing roles and privileges of groups
- Deleting groups
- Viewing a group's details

6.3.1 Prerequisite to add a group in FDM

Only a valid Windows group can be added to the FDM. Any group that is associated to FDM must be assigned to the following policies.

- Access this computer from the network
- Act as part of the operating system
- Adjust memory quotas for a process
- Bypass traverse checking
- Log on as a batch job
- Log on as a service
- Log on locally
- Replace a process level token
- Take ownership of files or other objects

ATTENTION

These policies are set for all the default Windows groups created by FDM.

6.3.2 Assigning policies

To assign the policies

1. Click Start > Control Panel > System and Security > Administrative Tools > Local Security Policy. The Local Security Policy dialog box appears.
2. In the left pane, expand Local Policies and then click User Rights Assignments. The list of policies appears in the right pane.
3. Right-click the policy and then click Properties. The respective policy's properties dialog box appears. Click Add Users or Groups to assign the group.
4. The Select Users Computers, Service Accounts, or Groups dialog box appears.
5. Enter the object name and then click OK.
6. Click Apply and click OK in the Properties dialog box.

6.3.3 Mapping Sentinel runtime user to FDM Server OPC Group

1. Right-click on **Start** menu (Windows icon), and click **Computer Management** or type "compmgmt.msc" in **Run** command. The Computer Management window appears.

NOTE

For Windows 7, use the **Run** command option to launch **Computer Management**.

2. Expand **Local Users and Groups** in the **Computer Management** pane.
3. Click on **Groups**. The list of groups appear in the right pane.
4. Right-click on **FDMOPCAccessGroup** and Click **Add to Group**. **FDMOPCAccessGroup Properties window appears.**
5. Click **Add**. **Select Users, Computers, Services Accounts, or Groups window appears.**
6. Click **Advanced** to expand the window and click **Find Now**.

NOTE

The location of the domain server should be correct.

7. Select the User and click **OK**.
8. Click OK on the Select Users, Computers, Services Accounts, or Groups window.
9. Click **Apply** and click OK on the FDMOPCAccessGroup Properties window.

6.3.4 Adding a Windows group and associating a role

ATTENTION

Adding a group in FDM is assigning a valid Windows group to FDM, to make it a valid FDM group.

To add a Windows group to FDM

1. From the FDM Client, click Tools > User Management.
2. The User Manager pane appears, displaying the list of existing users and their roles in the right pane.
3. Click the Group Manager icon in the left pane.
4. The Group Manager pane appears in which the default groups available in FDM are listed.
5. Click Add New to add new user group. The New Group pane appears.
6. Type the Group Name and select the Domain name from drop-down list under New Windows Group tab. In case of Windows work group, the group must be created as local group in the FDM Server system and the FDM Server system name must be added as domain name.

ATTENTION

The group name entered must be that of an existing Windows group. If you enter the name of a non-existing group, an error message appears.

Local Groups are supported only if they are created on the FDM Server System and are part of FDM access group.

7. Click the Role Information tab and select the role from the drop-down list.

For the role you select, the corresponding privileges are automatically selected.

ATTENTION

If you want to give any additional privilege, select the corresponding check box in the Privileges list.

8. Click Save to associate the group.

ATTENTION

After associating Windows Group to a particular role, all users belonging to the Windows group can logon to FDM system and they inherit the group's role. You need not explicitly add the users to the database.

To add a domain group

1. Create a Windows group in the domain controller system.
2. Add the Windows domain group to the FDMAccessGroup on all the systems where FDM components (FDM Server, FDM Client, and FDM RCI) are installed.

ATTENTION

FDMMgr user must be created in the domain controller system with the same password as everywhere to enable groups of domain controller to work with FDM.

TIP

Click View Details to view a group, its default privileges, and all the users associated with the particular role.

6.3.5 Editing roles and privileges of groups

To edit roles and privileges of a group, perform the following steps.

1. [Follow steps 1 and 2 of “Adding a Windows group and associating a role”.](#)
2. In the Group Manager pane, select the group that you want to modify and click Edit. The Edit Group pane appears.
3. Click the Role Information tab and select a new role, if you want to change the role.
4. Select new privileges, if you want to change the privileges and then click Save.

To delete a group

- Select the group, and then click Delete.

6.4 Role management

Managing roles involves the following tasks.

- Adding a role
- Modifying a role
- Deleting a role
- Viewing details of a role

6.4.1 Adding a role

ATTENTION

Only users assigned with the Administrator privileges can add a new role.

To add a new user role:

1. From the FDM Client, click Tools > User Management. The User Manager pane appears, displaying the list of existing users and their roles in the right pane.
2. Click the Role Manager icon in the left pane. The Role Manager pane appears with list of available user roles.

3. Click Add New Role to add details for a new user role. The All Privileges list appears listing all the privileges that can be assigned to a user role.
4. Type the Role name.
5. Assign privileges to the new role, using the arrow buttons.
 - To assign all available privileges to the user role, select the privileges you want to add and click . All the privileges listed in All Privileges are moved to Selected Privileges.
 - To assign some of the privileges, select the required privilege from All Privileges and click . Repeat this step to continue adding other privileges.
 - To remove all the privileges from Selected Privileges and move them back to All Privileges, select the privileges you want to remove and then click .
 - To remove some of the privileges from the Selected Privileges, select the privilege that you want to move back to All Privileges, and then click . Follow this step to remove other privileges.
6. Click Save to save the new role. If you click Save, the new user role is listed in Role Manager.

TIP

Click View Details to view a role and its default privileges.

6.4.2 Modifying a role

ATTENTION

Only users assigned with Administrator privileges can modify and delete an existing role.

Modifying a role affects all users associated to that particular role. Hence, ensure that you change the role of the users you do not want to be affected by the role modification.

To modify the existing role:

1. From the FDM Client, click Tools > User Management. The User Manager pane appears, displaying the list of existing users and their roles in the right pane.
2. Click the Role Manager icon in the left pane. The Role Manager pane appears in which the list of roles available in FDM are listed.
3. From the list of roles, select a role that you want to edit and click Edit. The Edit Role pane appears.
 - The All Privileges list includes the privileges that are not assigned to the selected role.
 - The Selected Privileges list includes those privileges that are currently assigned to the selected role.
4. Use the arrow buttons to add or remove the privileges for the selected user role.
 - To assign all the available privileges to the user role, select the privileges you want to add and click . All the privileges listed in All Privileges are moved to Selected Privileges.
 - To assign some of the privileges, select the required privilege from All Privileges and click . Repeat this step to continue adding other privileges.

- To remove all the privileges from Selected Privileges and move them back to All Privileges, select the privileges you want to remove and then click .
- To remove some of the privileges from the Selected Privileges, select the privilege that you want to move back to All Privileges, and then click . Follow this step to remove other privileges.

ATTENTION

A user role must have at least one privilege. Hence, you cannot remove all the privileges from Selected Privileges.

5. Click Save to save the information.

ATTENTION

If you modify a role, all affected users must have the modified role's access privileges.

Any modification in Role information does not take effect until the corresponding user logs on to the client again.

To delete a role:

- Select the role, and click Delete Role.

ATTENTION

FDM does not allow you to delete a role if users are associated to the role.

FDM SETTINGS

The Settings dialog box is used for customizing FDM settings.

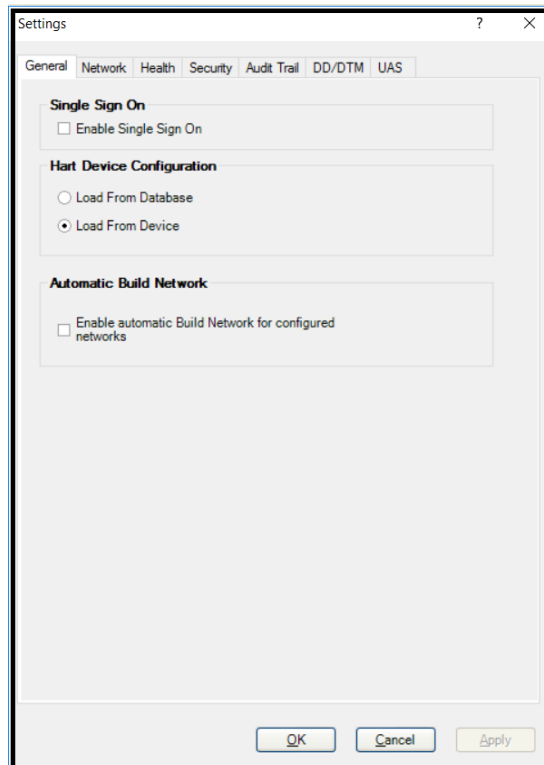
- **General:** The settings in this tab are used to enable/disable the Single Sign On feature, and to change the device configuration load option for HART devices.
- **Network:** The settings in this tab are used to enable/disable the network scan for the new devices connected to different types of networks.
- **Health:** The settings in this tab are used to enable/disable the health scan for the devices connected to different types of networks.
- **Security:** The settings in this tab are used to enhance security to the devices.
- **Audit trail:** The settings in this tab are used to select the audit trail time format and to view a log of actions that users perform on FDM.
- **DD/DTM settings:** The settings in this tab are used to enable the devices to determine if FDM loads the configuration using a DD or DTM
- **UAS:** The settings in this tab are used to connect to Sentinel and to select the type of connection.

For more information about the default role-based access privileges for each setting, refer to the section [“Roles and privileges”](#).

7.1 Customizing General settings

To view General settings:

1. Click **FDM > Settings**. The Settings dialog box appears. In the **General** tab, the following settings can be customized. All these settings affect relevant functionality at the FDM Server level.
 - Single Sign On
 - HART device configuration



2. Select the necessary settings, and then click OK. Refer to the following table for more details about the available settings.

Settings	Description
Single Sign On	Using the Single Sign On setting, any valid Windows user who is a part of the FDM user groups can log on to FDM without entering any credentials. To enable this setting, select the Enable Single Sign On check box. It is recommended to use single sign on, as the user specified password login is insecure.
HART Device Configuration	Using HART Device Configuration, configuration parameters can be loaded from the database or device. This applies only to DD/EDD devices and not to the devices loaded using DTMs. To load the configuration parameters from the database, click Load From Database. When you select this option, all the parameter values from the database are available. But, if there is any change in the configuration parameters' value, FDM automatically ignores the values from the database and loads from the device. To load the configuration parameters from the device, click Load From Device. All the recent changes in the configuration parameter values are available irrespective of the values stored in the database. When you are loading the device for the first time, irrespective of the settings' selection, the configuration parameters are loaded from the device. When the configuration parameters are modified by handheld or any other third-party application, the following message appears if you try to load a device from the database.  Click Ignore to load all parameters from the database. Click Suppress for the specified occurrences to load all the parameters from the device.
Automatic Build Network	Using the Automatic Build Network setting, the system will automatically recover the configured networks and will ensure that data is available in UAS Sentinel if the following services become unavailable: • FDM server

Settings	Description
	- FDM Remote Communication Interface - FDM network interfaces (Experion PKS, RTU, Safety Manger, oneWireless, and MUX). To enable this setting, select the Automatic Build Network setting check box. ATTENTION When the Automatic Build Network setting is enabled , there must be no networks configured at the RCI where the RCI machine is unavailable over the network, as the FDM server lags in setting up the RCI machine.

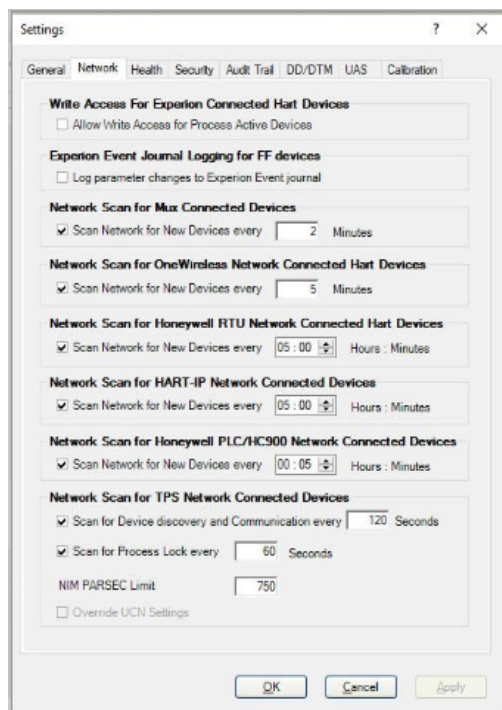
7.2 Customizing Network settings

To view Network settings:

1. Click **FDM > Settings**. The **Settings** dialog box appears.
2. In the **Network** tab, the following settings can be customized. All these settings affect relevant functionality at the FDM Server level.
 - Write access for Experion connected HART devices
 - Experion event journal logging for FF devices
 - Network scan for MUX connected devices
 - Network scan for Honeywell ControlEdge RTU network connected HART devices
 - Network scan for OneWireless network connected HART devices
 - Network scan for HART-IP network connected devices
 - Network scan for Honeywell ControlEdge PLC/HC900 network connected devices
 - Network scan for TPS network connected devices

The following table summarizes the network scan interval and default value for the different networks.

If the network scan for...	Range (minimum and maximum values)	And, the default value is...
MUX connected devices	2 minutes – 600 minutes	2 minutes
OneWireless network connected HART devices	5 minutes – 60 minutes	5 minutes
HART-IP network connected devices	5 minutes – 24 hours	5 hours
Honeywell ControlEdge RTU connected devices	5 minutes – 24 hours	5 hours
Honeywell ControlEdge PLC/HC900 connected devices	5 minutes – 24 hours	5 hours
TPS network connected devices		
Device discovery and communication		120 seconds
Process lock		60 seconds
NIM PARSEC Limit		750



Select the necessary settings, and click OK. More details about available settings are given here.

Settings	Description
Write Access For Experion Connected HART Devices	When FDM is connected to the HART devices through the Experion interface, the devices that are in active are locked by default. To edit any device parameter, you must inactivate the device or enable the Write Access For Experion Connected HART Devices setting. Select the Allow Write Access for Process Active Devices check box to allow the read/write access for the process active devices connected to Experion.
Experion Event Journal Logging for FF Devices	Every Fieldbus event such as point status change, operator parameter action, or Method execution is stored in the Experion event journal. In the Experion Station, to record all the parameter changes in the event summary for all FF devices that are connected to FIM, select the Log parameter changes to Experion Event Journal check box. The log parameter enables log for all FF devices in the Network tree. Experion Event journal logging for devices can also be changed from the Device Configuration page. For more details, refer to the section “Configuring a FF device using DD”.
Network Scan for Mux Connected Devices	The Scan Network for New Devices every Minutes setting defines the system behavior for the dynamic network update for the MUX network connected devices after the network is built in FDM. To discover new devices connected to the undiscovered loops/channels, select the Scan Network for New Devices every Minutes check box and set the time interval (in minutes). If this setting is enabled and the network build is complete, FDM continuously polls all the disconnected loops/channels of the multiplexers to find if new devices are connected to the network. If a new device is found at these loops/channels, it is displayed in the Network view. If the device is connected to the loop/channel which is already discovered, this option does not scan that device. To view the status for such devices, FDM uses the Scan for Device Health every Minutes option under Device Health for Mux Connected Devices in the Health tab. When you disable the Network Scan for Mux Connected devices setting, it disables the MUX Monitoring feature (if applicable) and alarms are not reported in Experion Station. It is recommended not to enable the Scan Network for New

Settings	Description
	Devices every Minutes setting during post commissioning phase or you provide a large interval to have better device load performance.
Network Scan for OneWireless Network Connected HART Devices	The Scan Network for New Devices every Minutes setting defines system behavior for the dynamic network update for OneWireless network connected HART devices after the network is built in FDM. To discover new HART devices connected to WDMs through the OneWireless Adapter, select the Scan Network for New Devices every Minutes check box and set the time interval (in minutes). If this setting is enabled, FDM continuously polls all WDMs to find if new HART devices are connected to the network or disconnected from the OneWireless network. If a new device is found, it is displayed in the Network view.
Network Scan for HART- IP Network Connected Devices	The Scan Network for New Devices every Hours: Minutes setting defines the system behavior for dynamic network update for HART-IP network connected devices. To discover a new HART device, select the Scan Network for New Devices every Hours: Minutes check box and set the time interval (in hours: minutes). If this setting is enabled, FDM continuously polls all the configured HART-IP gateways to find new HART devices that are connected to the HART-IP network. If a new device is found, it is displayed in the Network view.
Network Scan for Honeywell PLC Network Connected Devices	The Scan Network for New Devices every Hours: Minutes setting defines the system behavior for dynamic network update for PLC devices after the network is built in FDM. To discover a new HART device connected to the PLC, select the Scan Network for New Devices every Minutes check box and set the time interval (in minutes). If this setting is enabled, FDM continuously polls all PLC to find if new HART devices are connected to the network or disconnected from the PLC network. If a new device is found, it is displayed in the Network view.
Network Scan for Honeywell RTU connected HART	The Scan Network for New Devices every Hours: Minutes setting defines the system behavior for dynamic network update for RTU connected HART devices after the network is built in FDM. To discover a new HART device connected to the RTU controller, select the Scan Network for New Devices every Minutes check box and set the time interval (in minutes).

Settings	Description
Devices	If this setting is enabled, FDM continuously polls all RTU controllers to find if new HART devices are connected to the network or disconnected from the RTU network. If a new device is found, it is displayed in the Network view.
Network Scan for TPS Network Connected Devices	The Scan for Devices discovery and Communication every Seconds setting defines the system behavior for dynamic network update (device disconnect/reconnect status) for TPS network connected devices that are already discovered from the build network operation. To scan the devices that are disconnected and connected again in the network hierarchy, select the Scan for Devices discovery and Communication every Seconds check box and set the time interval (in seconds). If this option is enabled • FDM scans the network for every specified time in seconds. • FDM continuously monitors the communication status for all DE devices that are already discovered in the network view. For example, as in the Settings dialog box, FDM scans the network if there are any changes in the network tree for every 5 seconds. FDM does not support dynamic network scan for newly added TPS-connected DE devices. Hence, you have to rebuild the network to discover the newly configured devices.
	The Scan for Process Lock every Seconds setting defines system behavior for monitoring process lock/unlock status of all TPS network connected DE devices. FDM considers DE device as process locked if the device parameter, Point Execution State (PTEXECST) value is ACTIVE in TPS. If there is any change in the device parameter value from ACTIVE to INACTIVE or vice-versa, the devices in FDM are locked/unlocked based on the PTEXECST state. To monitor the process lock status for all TPS-connected DE devices, select the Scan for Process Lock every Seconds check box and set the time interval (in seconds). The process lock status or PTEXECST value cannot be changed in FDM. It can be changed only in TPS. When you clear the Scan for Process Lock every Seconds check box, the device is still in process lock condition.

Settings	Description
	NIM PARSEC Limit defines the threshold value for the maximum load that is allowed on the Network Interface Module (NIM). The parameter access rate (PARSEC = parameters per second requested on NIM) of a NIM is useful in determining its load. FDM checks the load on NIM with entered value (in Settings dialog box) before sending any requests to TPN system. FDM continuously monitors NIM PARSEC value. If the actual NIM PARSEC value is lesser than the entered NIM PARSEC value, which is entered in the Settings dialog box, FDM continues to communicate with the TPS system. However, if the actual NIM PARSEC value exceeds the entered value (in the Settings dialog box), FDM immediately stops new subscriptions/read parameters. If the system (TPN Server or NIM) is overloaded at a later time due to non-FDM clients, FDM does not remove its own load. It will ensure that additional load is not added to the system. Ensure that you have properly planned and entered the NIM PARSEC value based on the type of K2LCN/K4LCN (NIM boards) board pps (points per second) limits. For more information about K2LCN/K4LCN, refer to the TPN/TPS bookset. FDM has no direct control on NIM's parameter access. The TPN Server communicates with NIM to fetch the parameter values at a periodic update rate.

FDM subscribes with default scan rates of 120 seconds for Dynamic discovery and 60 seconds for Process lock for all TPS network connected DE devices. Changing these default values might affect the LCN load, and hence you have to plan the network settings accordingly.

TIP

Use this table can as a reference data from FDM-TPS integration tests.

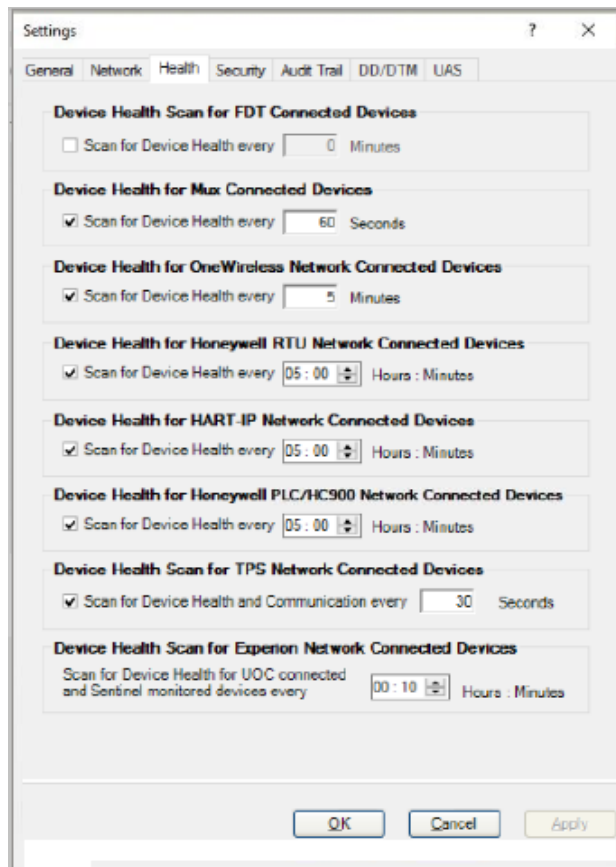
Number of DE devices per LCN	Scan rate		Device load (single variable transmitter)	Additional load on LCN due to FDM	Remarks
	Dynamic Discovery	Process Lock			
1282	30	5	4 devices	5.16%	
1282	120	60	4 devices	2.43%	Default FDM scan rates
1282	120	120	4 devices	2.20%	
2570	30	5	4 devices	11.45%	
2570	120	60	4 devices	2.80%	Default FDM scan rates
2570	120	120	4 devices	2.47	

7.3 Customizing Health settings

To view the health settings:

1. Click **FDM > Settings**. The **Settings** dialog box appears.
2. In the **Health** tab, the following settings can be customized. All these settings affect relevant functionality at the FDM Server level.
 - Device health scan for FDT connected devices
 - Device health for MUX connected devices
 - Device health for OneWireless network connected devices
 - Device health for HART-IP network connected devices
 - Device health for Honeywell ControlEdge PLC/HC900 network connected devices
 - Device health for Honeywell ControlEdge RTU network connected devices
 - Device health scan for TPS network connected devices
 - Device health scan for Experion connected devices

Device health scan	Range (minimum and maximum values)	Default value
FDT connected devices	1 minute – 60 minutes	5 minutes
MUX connected devices	60 seconds – 600 seconds	60 seconds
OneWireless network connected devices	5 minutes – 60 minutes	5 minutes
HART-IP network connected devices	5 minutes – 24 hours	5 hours
Honeywell ControlEdge RTU	5 minutes – 24 hours	5 hours
Honeywell ControlEdge PLC/HC900	5 minutes – 24 hours	5 hours
TPS network connected devices		30 seconds



Select the necessary settings, and then click OK. Refer to the following table for more details about the available settings.

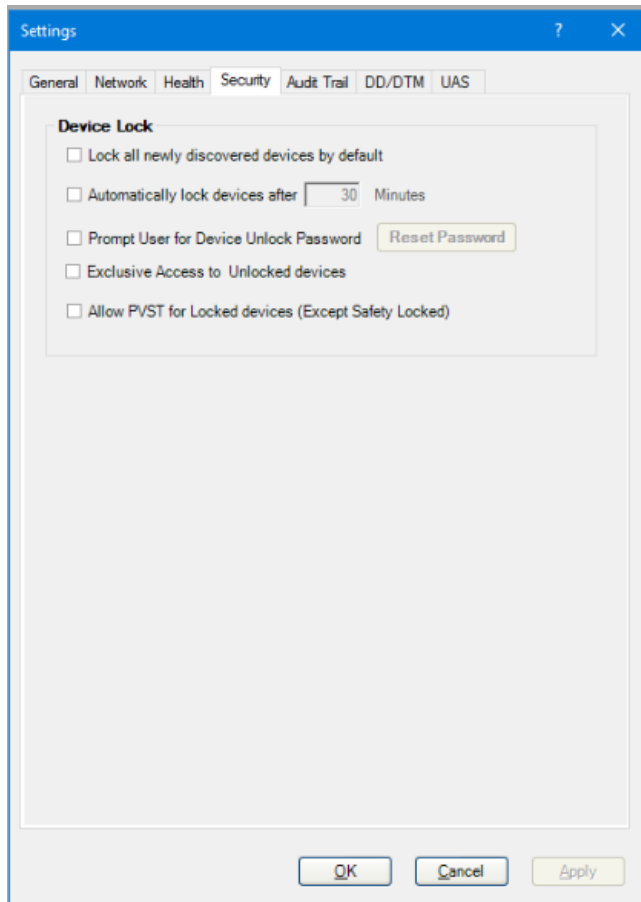
Settings	Description
Device Health Scan for FDT Connected Devices	The Scan for Device Health every Minutes setting defines system behavior with respect to scanning device health for FDT-connected devices. To scan device health, select Scan for Device Health every Minutes and set the frequency (time interval in minutes) at which the devices under FDT network must be scanned for health information. You can also configure device health for selected devices that are connected to the FDT network. For more details, refer to the section “Customizing the FDT health scan settings” .
	Frequent device health scans on the FDT network can cause the Comm/Gateway/IO DTMs state to become non-responsive and hinders basic FDT operations like network scan, DTM configuration, and so on. This behavior might worsen if a large number of devices are connected. It is therefore recommended to choose an appropriate health scan interval based on the size of the network. For a large FDT network, the health scan interval must be longer.
Device Health for Mux Connected Devices	The Scan for Device Health every Seconds setting defines system behavior with respect to scanning device health status. This setting is applicable to all the devices connected to the RS-485 HART multiplexer network. To scan health of the devices, select Scan for Device Health every Seconds and set the time interval (in seconds). Even if this setting is disabled, FDM displays the device health properly in the following cases. • When the network is built/rebuilt. • When a device is loaded in FDM Client/Experion Station. • When a device is accessed from a third party application through FHM. • When the device detail display page is opened in the Control Builder. • When the dynamic scan is enabled in the device configuration page. NOTE When you disable the Device Health for Mux Connected Devices setting, it disables the MUX Monitoring feature (if applicable) and alarms are not reported in Experion Station.

Settings	Description
Device Health for OneWireless Network Connected Devices	The Scan for Devices Health every Minutes setting defines system behavior with respect to scanning device health status for OneWireless network connected devices. To scan the health of devices, select Scan for Device Health every Minutes and set the time interval (in minutes). NOTE When you disable the Device Health for OneWireless Network Connected Devices setting, the Alarm Monitoring feature (if applicable) is disabled, and alarms are not reported in Experion Station.
Device Health for Honeywell RTU Network Connected Devices	The Scan for Devices Health every Hours: Minutes setting defines system behavior with respect to scanning device health status for ControlEdge RTU network connected devices. To scan the health of devices, select Scan for Device Health every Hours: Minutes and set the time interval (in hours).
Device Health for HART- IP Network Connected Devices	The Scan for Devices Health every Hours: Minutes setting defines system behavior with respect to scanning device health status for HART-IP network connected devices. To scan the health of devices, select Scan for Device Health every Hours: Minutes and set the time interval (in hours).
Device Health for Honeywell PLC Network Connected Devices	The Scan for Devices Health every Hours: Minutes setting defines system behavior with respect to scanning device health status for ControlEdge PLC/HC900 network connected devices. To scan the health of devices, select Scan for Device Health every Hours: Minutes and set the time interval (in hours).
Device Health Scan for TPS Network Connected Devices	The Scan for Device Health and Communication every Seconds setting defines system behavior with respect to scanning device health status for TPS network connected devices. To scan health of devices, select Scan for Device Health and Communication every Seconds and set the time interval (in seconds).

7.4 Customizing Security settings

To view the security settings for HART, PROFIBUS, FF, ISA100 Wireless, and DE devices:

1. Click FDM >Settings. The Settings dialog box appears.
2. In the Security tab, the device lock setting can be customized for enhancing security of devices. All device lock options are enabled only for the user with administrator privileges.



Settings	Description
Device Lock	Device Lock feature has the following settings that are used for enhancing security of devices. • Lock all newly discovered devices by default • Automatic lock devices after Minutes • Prompt User for Device Unlock Password • Exclusive Access to Unlocked devices • Allow PVST for locked devices (Except Safety Locked) Device lock options are recommended for FDM systems that are fully commissioned. Since, devices need to be modified extensively during commissioning, it is recommended to turn off the device lock settings during this phase.
	To lock newly discovered devices on the network automatically, select Lock all newly discovered devices by default. This affects the devices that are discovered using dynamic discovery or if you browse an existing network again. Even after enabling this setting, all the devices that were already discovered in the network retain their existing lock status.
	To automatically lock an explicitly unlocked device after a specified time period, select Automatically lock devices after Minutes. This feature does not affect devices that were explicitly unlocked before this option was enabled. If this option is enabled, a device might be automatically locked in the middle of device configuration or during method execution. Hence, FDM allows you to extend the automatic lock by displaying reminder message, “Device auto lock imminent. Click here to extend” in the Device configuration page 5 minutes before timeout. Click this message to extend the autolock timeout interval. Device autolock interval must be in the range of 30 to 120 minutes. When this setting is enabled, the devices under network are locked automatically for security in the following scenarios. • If the unlocked devices are disconnected. • If the RCI on which the device is connected, is stopped. • If the network on which the device is connected is re-browsed. • If the device configuration page is closed. • If FDM Station Maintenance View is refreshed or closed.
	To protect devices that are connected to a network using a password, select the Prompt User for Device Unlock Password check box and enter the password.

Settings	Description
	If the password is already set and if you want to reset the password, click Reset Password. The device unlock password must have a minimum of eight and maximum of 20 characters.
	To provide exclusive write access for a device in FDM Client where it is unlocked, select the Exclusive Access to Unlocked devices check box. In all other FDM Clients, the same device is read-only and locking/unlocking is not allowed unless the device is closed/locked in the first FDM Client. If this option is not enabled, it is possible to unlock a device in one FDM Client and load it in another FDM Client with write access. It is recommended to use this setting to implement better security by giving write access for device.
	To allow PVST (Automatic, Semi-Automatic, Manual) for locked devices, select the Allow PVST for Locked devices (Except Safety Locked) check box. When this setting is enabled, the following locks are overridden and PVST schedule/execution is allowed on locked devices. • Explicit Lock • Process Lock NOTE The Allow PVST for Locked devices (Except Safety Locked) setting does not override Safety lock, FHM lock, and Exclusive lock. Therefore, you cannot execute PVST on devices that are locked.

7.5 Customizing Audit Trail settings

The Audit Trail setting enables you to select audit trail time format, and to view and select which user actions are logged in the FDM audit trail. Some actions are implicitly logged. You can add user-defined audit trail actions using the **Log User Action** option from the Network view shortcut menu or from **Tools > Log User Action**.

Only an Administrator can change the audit trail settings.

To view/modify the audit trail settings:

1. Click **FDM > Settings > Audit Trail**. The following dialog box appears.

The screenshot shows the 'Settings' dialog box with the 'Audit Trail' tab selected. The 'Audit Trail Time Format' section has two radio buttons: 'Show UTC time' and 'Show Local time', with 'Show Local time' selected. The 'Audit Trail Action Settings' section has a checkbox for 'Check/Uncheck All' which is unchecked. Below this is a table with two columns: 'Action Type' and 'Reason Enabled'. The table lists 18 action types, each with an unchecked checkbox in the 'Reason Enabled' column.

Action Type	Reason Enabled
Param Change	☐
Rename Device	☐
Lock/Unlock Device	☐
Execute Method	☐
Build Network	☐
Add/Delete DD/DTM/FDI Package	☐
User Login	☐
Add/Delete/Modify User	☐
Add/Delete/Modify Role	☐
Change License	☐
Stop Server	☐
Delete Device	☐
Import/Export	☐
Add/Delete/Modify Group	☐
Device List Actions	☐
Change AuditTrail Settings	☐
User Explicit Action	☐

2. Select the necessary settings, and click **OK**. More details about available settings are listed here.

Feature	Description
Audit Trail Time Format	Audit Trail Time Format is used to display the time stamp in one of the following formats for Audit Trail records. • Show UTC time: To display the time stamp in the Coordinated Universal Time (UTC) for audit trail records, click Show UTC time. • Show Local time: To display the time stamp in the local time for audit trail records, click Show Local time. This is the default option.
Audit Trail Action Settings	Audit Trail Action Settings is used to select action types for which you want to enter a reason for performing the action. Action Type indicates the various system actions that can be audited. Reason Enabled indicates whether the entering the reason is mandatory for the action type or not. You can select or clear Check/Uncheck All to enable/disable entering the reason for all action types.

The following action types are audited in FDM.

Action Type	Description
Param Change	When a parameter is changed, FDM logs a record in the audit trail.
Rename Device	When a device is renamed, FDM logs a record in the audit trail.
Lock/ Unlock Device	When a device is explicitly locked/unlocked, FDM logs a record in the audit trail.
Execute Method	When a method is executed, FDM logs a record in the audit trail.
Build Network	When a network is built (using the Build Network option), FDM logs a record in the audit trail.
Add/Delete DD/DTM	When a DD or DTM is added/deleted, FDM logs a record in the audit trail.
User Login	When a user logs in, FDM logs a record in the audit trail.
Add/Delete/Modify User	When a new user is added, an existing user's details are modified, or when an existing user account is deleted, FDM logs a record in the audit trail.
Add/Delete/Modify Role	When a new user role is added, an existing user role's details are modified, or when an existing user role is deleted, FDM logs a record in the audit trail.
Change License	When a license is updated, FDM logs a record in the audit trail.
Stop Server	When the server is stopped, FDM logs a record in the audit trail.
Delete Device	When a device tag is deleted, FDM logs a record in the audit trail.
Import/Export	When a device tag/ history/audit trail/offline configuration is imported/exported, FDM logs a record in the audit trail.
Add/Delete/Modify Group	When a Group is added/ deleted/modified, FDM logs a record in the audit trail.
Device List Actions	When the device list is configured (created/modified/deleted), FDM logs a record in the audit trail.
Change Audit Trail Settings	When the audit trail settings are changed, FDM logs a record in the audit trail.
User Explicit Action	When any explicit user-defined action is performed, FDM logs a record in the audit trail.
Modify Write Access for Process Active Devices	When the write access is enabled or disabled for process active devices, FDM logs a record in the audit trail.
Device Status Change	When the device status is changed, FDM logs a record in the audit trail.
Device Lock Change	When the state of the device lock is changed (from locked to unlocked or unlocked to lock), FDM logs a record in the audit trail.
Hart Multiplexer Actions	When FDM Hart Multiplexer is started/stopped, FDM logs a record in the audit trail.
Add/Delete/Modify Network	When the network configuration is added /deleted /modified, FDM logs a record in the audit trail.
History Actions	When a user explicitly saves history or whenever the user deletes history, FDM logs a record in the audit trail.
Offline Configuration Actions	When a user creates /opens/modifies/deletes or renames an Offline Configuration, FDM logs a record in the audit trail.
Device Documentation Actions	When a user attaches/uploads/detaches a device document (at the device level, device type level or system level), FDM logs a record in the audit trail.

Action Type	Description
Display Filter Actions	When a user creates/modifies/opens/deletes or renames a Display Filter, FDM logs a record in the audit trail.
MUX Monitoring Actions	When a user performs an action related to MUX Monitoring, like accessing the FDM Tag Builder tool, FDM logs a record in the audit trail.
Device Application Launch	When a third-party application is started, FDM logs a record in the audit trail.
Bulk Operations	When a user performs bulk operation to create history record or offline templates for a certain set of devices, and bulk offline download, FDM logs a record in the audit trail.
Delete Records	When a user deletes the records of device tags, offline device configuration, and device history, FDM logs a record in the audit trail.
DTM Operations	When there is a DTM related audit trail events (if DTM supports audit trail) or user performs DTM library update, FDM logs a record in the audit trail.
Reset and Build Network	When a user performs the reset and build network operation to reset the multiplexer internally and to remove the invalid status on the multiplexer device status pages, FDM logs a record in the audit trail.
Add/Delete/Modify PVST Group	When a PVST group is added/deleted/modified, FDM logs a record in the audit trail.
PVST Execute/Cancel/Acknowledge	When a PVST group is executed/cancelled/acknowledged, FDM logs a record in the audit trail.

NOTE

For DTM Configuration, Audit Trail dialog box (Enter Reason for current action) appears only if it is supported by DTM.

7.5.1 View Audit Trail

There are two approaches to view audit trail data

1. View Audit Trail from Database
2. View Audit Trail from File

7.5.2 View Audit Trail from Database

To view the audit trail from database:

1. Click View > Audit Trail > Audit Trail from Database. The Audit Trail page appears.

TIP

You can also access the audit trail from database feature by clicking the  icon below the FDM Toolbar.

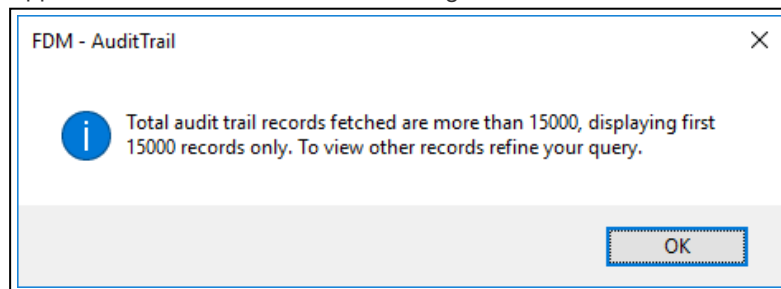
2. Action Type lists all the actions that are currently audited in FDM. For instance, Param Change indicates any change made to a parameter logged in the audit trail. Select the required action types from Action Type. To view the audit trail for all parameters, select All.
3. User lists all the users created in FDM. To view the audit trail for a particular user, select the user from the User list. To view the audit trail for all users, select All.
The actions 'Device Status Change' and 'Device Lock Change' are not specific to a user. Hence, these actions do not have a user assigned to them. While filtering these actions, select "All" in the User box.
4. Nodes lists all devices that are online and connected to FDM or devices from history (devices whose state is not online currently). Select the required device from the list of nodes. To view the audit trail for all devices, select All.
5. Select the From and To dates using the calendar.
To change Audit Trail settings, click the Settings button. The Settings dialog box appears. For details, refer to [section "Customizing the audit trail settings"](#).
6. Click View. The following audit trail details appear in the lower portion of the Audit Trail page.
 - **SNo:** Displays the serial number of audit trail records.
 - **Time Stamp:** Displays the date and time when the action was performed.
 - **Action:** Displays the action (Example: Param Change) that was performed.
 - **User:** Displays the user who performed the action.
 - **Tag:** Displays the device tag name for a device that appears in the Network Tree view. This field displays the device tag on which the action was performed.
 - **Description:** Displays the description that FDM automatically logs for each action implicitly.
 - **Reason:** If the Administrator has enabled reason logging for this particular Action Type, this column displays the Reason that the user has entered while performing the action.
7. To export the audit trail details, click Export.
8. To print the audit trail records in HTML format, click Print.

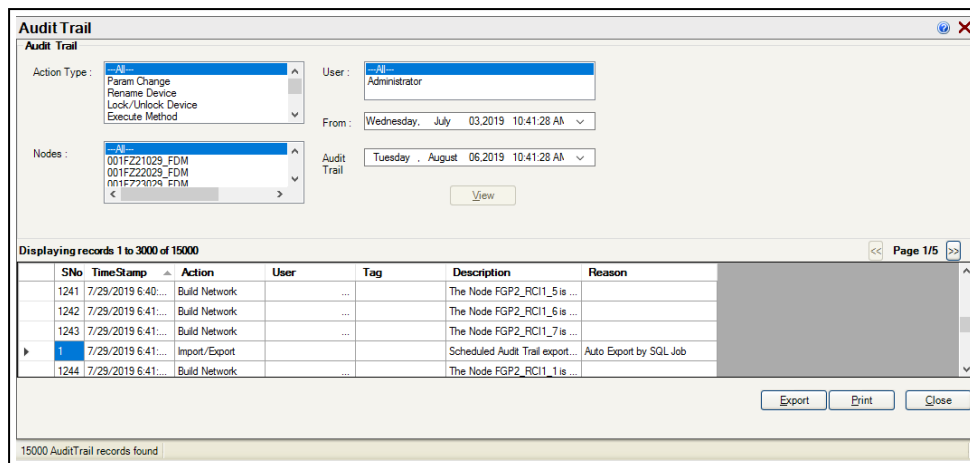
NOTE

While exporting the audit trail records in CSV and HTML formats, irrespective of audit trail time format settings, the time stamp is displayed in local time format. But, the exported audit trail records in XML format are always displayed in UTC time format.

When you want to view a large number of audit trail records, client takes time to collect all the records and the status is displays as fetching in the audit trail page.

The maximum number of audit trail records that you can view at any time is 15000. If the total audit trail records fetched are more than 15000, a confirmation message appears. Click OK to view the remaining audit trail records.





7.5.3 View Audit Trail from the File

To view the audit trail from the file:

1. Click View > Audit Trail > Audit Trail from File. The Audit Trail page appears.
2. Click **Browse**, and select the file (exported .csv file).

NOTE

The default automatic export location of .csv file is
C:\ProgramData\Honeywell\FDM\Client\AuditTrailAutoExport.

3. Action Type lists all the actions that are currently audited in FDM. For instance, Param Change indicates any change made to a parameter logged in the audit trail. Select the required action types from Action Type. To view the audit trail for all parameters, select All.
4. User lists all the users created in FDM. To view the audit trail for a particular user, select the user from the User list. To view the audit trail for all users, select All.

The actions 'Device Status Change' and 'Device Lock Change' are not specific to a user. Hence, these actions do not have a user assigned to them. While filtering these actions, select "All" in the User box.

5. Nodes lists all devices that are from history/file.

Click View. The following audit trail details appear in the lower portion of the Audit Trail page.

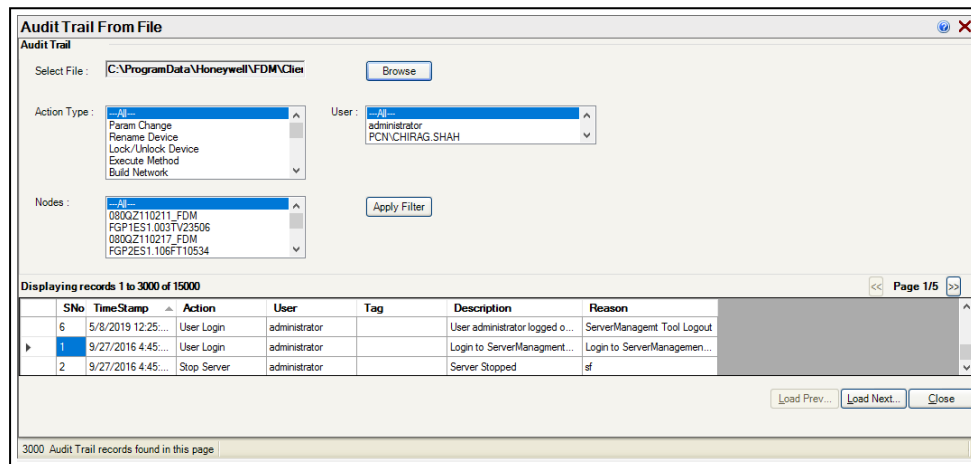
- **SNo:** Displays the serial number of audit trail records.
- **Time Stamp:** Displays the date and time when the action was performed.
- **Action:** Displays the action (Example: Param Change) that was performed.
- **User:** Displays the user who performed the action.
- **Tag:** Displays the device tag name for a device that appears in the Network Tree view. This field displays the device tag of the device on which the action was performed.
- **Description:** Displays the description that FDM automatically logs for each action implicitly.
- **Reason:** If the Administrator has enabled reason logging for this particular Action Type, this column displays the Reason that the user has entered while performing the action.

NOTE

When you want to view a large number of audit trail records, client takes time to collect all the records and the status is displays as fetching in the audit trail page.

The maximum number of audit trail records that you can view at any time is 15000. If the total audit trail records fetched are more than 15000, a confirmation message appears. Click OK to view the remaining audit trail records.

To view the next 15000 audit trail records, click **Load Next...** To view the previous 15000 audit trail records, click **Load Prev....**



7.5.4 Automatic export and purge of audit trail

FDM automatically exports the audit trail data to a .csv file and purge the audit trail data at the end of every month by keeping only the last 30 days data in the FDM database.

The csv file is exported to FDM server node in

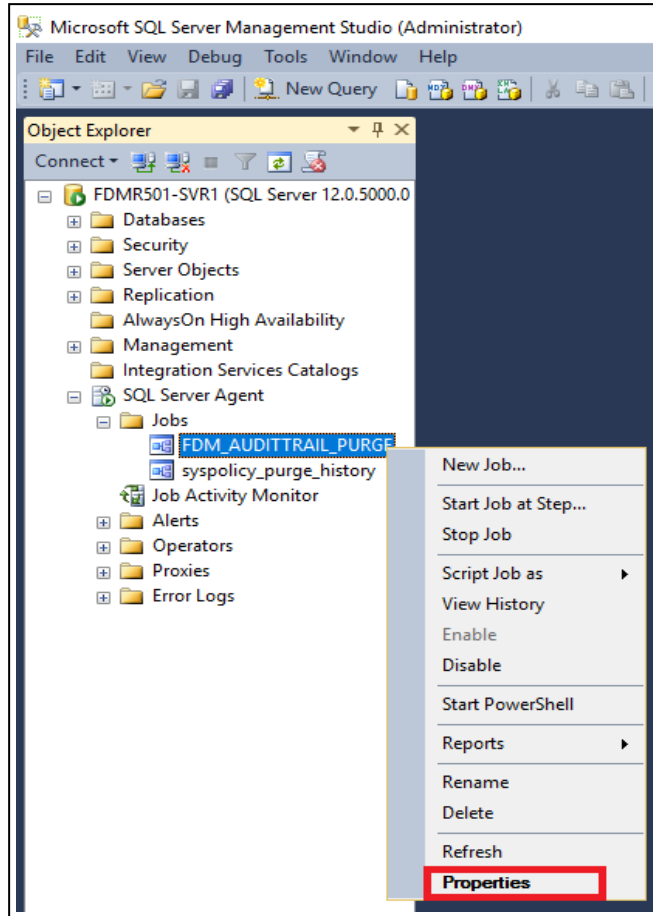
C:\ProgramData\Honeywell\FDM\Client\AuditTrailAutoExport.

To change the default automatic export schedule of audit trail records:

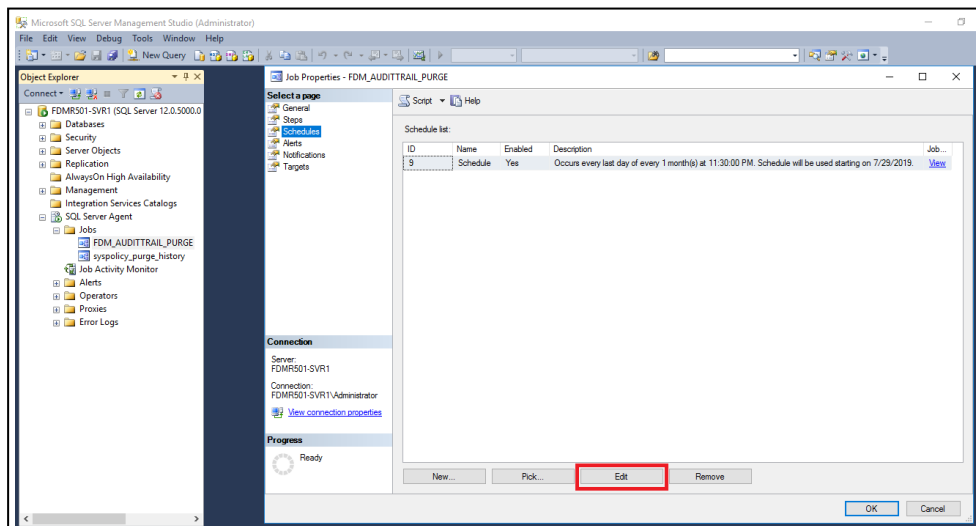
NOTE

If the number of audit trail records are more than recommended Tech & Spec, the user can perform manual export and purge the audit trail data. To perform the manual export of audit trail, refer to "Manual export and purge of audit trail" on page 131.

1. From the **Start** menu, select **SQL Server Management Studio (SSMS)**
2. Ensure **SQL Server Agent** is running.
3. Right click on **FDM_AUDITTRAIL_PURGE**, and select **Properties**.



4. Click **Schedules**, and select **Edit**.



5. The default frequency for data export is the last day of every month.

NOTE

If it is necessary, you can set a schedule with frequency in days, weeks or months. The default schedule should not be less than a month.

6. To access the audit trail .csv file, go to
C:\ProgramData\Honeywell\FDM\Client\AuditTrailAutoExport

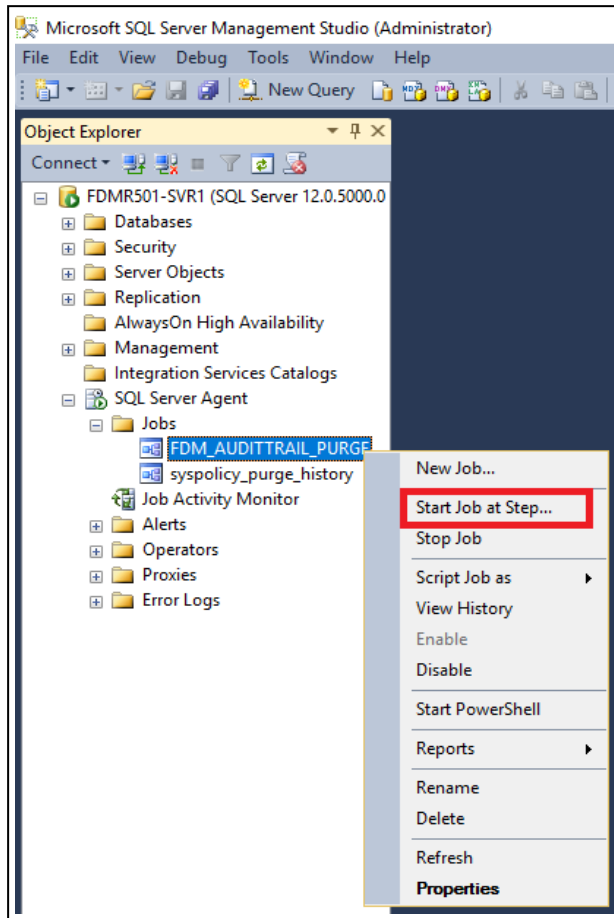
NOTE

If you want to schedule the job other than the default date, run it manually from SQL agent and check the file in the path
C:\ProgramData\Honeywell\FDM\Client\AuditTrailAutoExport.

7.5.5 Manual export and purge of audit trail

To configure the scheduler to manually export an audit trail

1. From the **Start** menu, select **SQL Server Management Studio (SSMS)**
2. Ensure **SQL Server Agent** is running.
3. Right click on **FDM_AUDITTRAIL_PURGE**, and select **Start Job at Step...**



4. Start jobs dialog box with Success message appears.
5. To access the audit trail .csv file which is on the FDM server node, go to **C:\ProgramData\Honeywell\FDM\Client\AuditTrailAutoExport**

7.6 Choosing DD/DTM load settings

This setting enables you to decide the specific default DTMs that will be used to load matching devices (device types) instead of using DDs/EDDLs. This applies to FDM Client and Station Maintenance View.

For FF Devices, if DD is not present, the device does not appear in Load using DD/EDD and cannot be set to Load using DTM by default in the Device Configuration Load Setting.

To set or change the DD/DTM setting:

1. Log on to the FDM Client.
2. Click FDM > Settings. The Settings dialog box appears.
3. Click the DD/DTM tab. All the HART, FF, and ISA100 Wireless device types, which have both DD and DTM are listed in Load Using DD/EDD by default. DTMs must be installed for the devices if you want to load a device with a DTM and DTM library must be updated.

4. To select a DTM as the default for a given device type, perform the following steps.
 - Select a device type from the Load Using DD/EDD list, and click > to move it to the Load Using DTM list.
 - To move all device types to the Load Using DTM list, click the >> button
5. To select DD/EDDL as the default for a given device type, perform the following:
 - Select a device type from the Load Using DTM list, and click < to move it to the Load Using DD/EDD list.
 - To move all device types to the Load Using DD/EDD list, click the << button
6. After you load a device to the required list, click Apply.
7. Click OK.

When you load a device, whether it loads with a DD or DTM depends on the setting you have made.

If the device is not listed in either of the two boxes, by default, it is loaded using DD.

When FDM Client is installed on RCI, and if you are updating DD/DTM settings in both FDM Client and FDT Comm Console, this setting is effective in both.

Settings for the device types currently loaded in one or more clients cannot be changed until you unload those devices. A warning message appears in case if you try to move these device types.



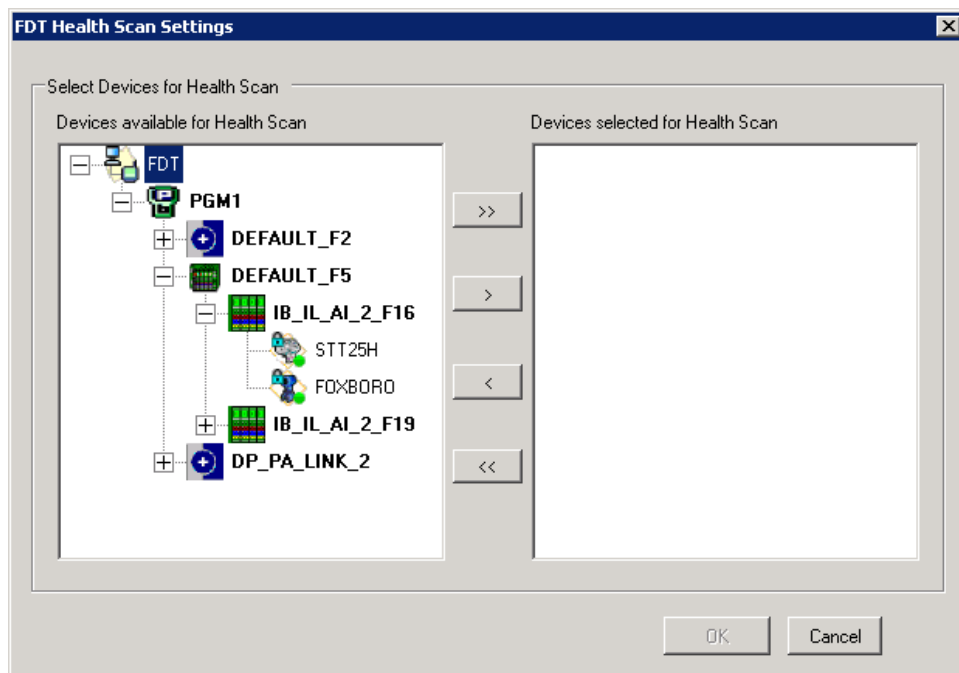
7.7 Customizing the FDT health scan settings

With this setting, you can scan the device health for the selected devices (HART and PROFIBUS) that are connected to the FDT network. A PROFIBUS device can support two types of health, Condensed and Classic. However, FDM supports only Classic type of device health.

- **Condensed type of device health status:** This status is created to make diagnostic events more obvious and to allow predictive and preventive maintenance.
- **Classic type of device health status:** This status is implemented to provide compatibility to systems which are not configured for Condensed Status.

The FDT Health Scan Settings is effective only if you select Device Health Scan for FDT Connected Devices option in the Settings dialog box.

1. From the FDT Comm Console, click FDM > FDT Health Scan Settings. The FDT Health Scan Settings dialog box appears.



2. By default, devices are not selected for health scan. From the Devices available for Health Scan list, select the device(s) and click any one of the following:
 -  to move the device to the Devices selected for Health Scan list. If you select Communication/ Gateway DTM and click , then all devices under that DTM will move to the Devices selected for Health Scan list.
 -  to move all the devices to Devices selected for Health Scan list.
3. Click OK.

Few communication DTMs consume more memory when the Device Health Scan for FDT Connected Devices option is enabled. The amount of memory consumed is proportional to the number of devices selected for the health scan. Since DTMs are third party components, FDM cannot control this memory consumption. Hence, it is recommended you to carefully monitor CPU usage and select only critical devices for the health monitoring.

For a device connected to the FDT Network, the device health does not update for a time period when that device is loaded with DTM in the FDT Comm Console. To resume the health update for that device, its DTM configuration page must be closed.

7.8 Switching between FDM Servers

You can connect the FDM Client to a different FDM Server without closing the FDM Client. To connect to a different FDM Server, perform the following steps.

1. From the FDM Client, click FDM > Switch Server. The Field Device Manager login screen appears.
2. Follow the procedure explained in [“Logging on to the FDM Client”](#) to connect to a different server.

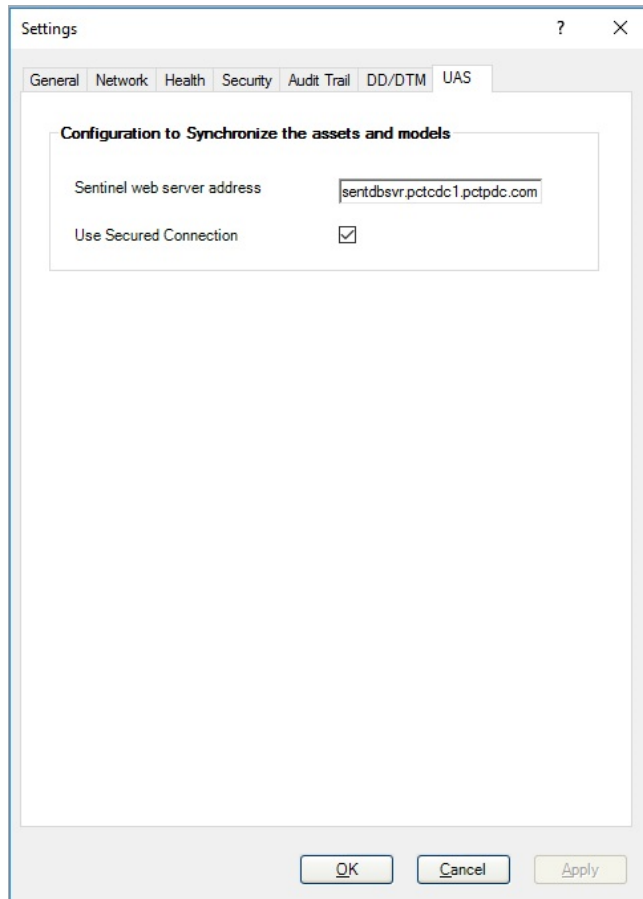
When you try to a logon to a different server, the connection to the current server is lost, irrespective of whether the logon succeeds or not.

7.9 Customizing UAS settings

The UAS setting enables you to configure to synchronize the assets and models. It also allows you to choose if the connection should be secured or not.

To view UAS settings:

1. Click FDM > Settings. The Settings dialog box appears.



2. Select the necessary settings, and then click OK. Refer to the following table for more details about the available settings.

Settings	Description
Sentinel web server address	Using the Sentinel web server address setting you can provide the web server address of the Sentinel server with which the assets and the models are to be synchronized. To synchronize, provide the fully qualified web server address in the text box.
Use Secured Connection	Using the Use Secured Connection setting, you can choose you whether you want connection to be secured or not. NOTE The user should check Secured Connection only if the Sentinel is installed with secured connection settings turned on. To enable this setting, select the check box.

DEVICE DESCRIPTION FILE MANAGEMENT

Every manufacturer of devices creates a Device Description (DD) file for each model or type of device that they make. The DD file contains device-specific information that is used for interpreting the responses received from the device. You can add and delete DD file from the client.

8.1 Adding a DD file

If the DD for a given device is not present in the FDM DD library, you can add DD to the DD library by using the Add DD File option. When you add a DD, the server automatically generates the corresponding template for the DD. This template is published to all the open clients.

NOTE

Before you attach the DD files, perform a scan using the recommended and up-to-date antivirus software to ensure that the DD files are free from malware. Honeywell is not responsible for any damages caused by corrupted DD files with malware present.

Only users assigned with the privileges associated with the administrator role can add/delete a template or synchronize the data.

Prerequisites

Ensure that the corresponding symbols files (.sym or .sy5) and .cff files are available before you add DD files for FF and ISA100 Wireless devices.

To add any new DD file from the client to the server

1. From the FDM Client, click Library > Manage DDs > Add DD File. The Select a DD file dialog box appears.

TIP

You can also click the Add DD File icon under the FDM Toolbar.

2. For HART devices, browse to the folder where the .fms or .fm6 or .fm8 file is located, select the file and then click Open or for FF and ISA100 Wireless devices, browse to the folder where the .ffo or .ff5 file is located, select the file, and then click Open.
3. Select a device profile from the drop-down list. You have options to select Field device or Gateway Device. Acknowledge the confirmation message.

NOTE

- To replace a DD file, you must first delete it from the library, then add the replacement DD file.
- If you add a DD that already exists in the DD library, then an error message appears displaying “The DD that you are trying to add already exists in the FDM database”.

4. Click OK.

8.2 Deleting a DD file

This feature enables you to delete a particular version of a DD file. When a DD for a particular device type and device revision is deleted, all subsequent loading of devices of that type uses the previous DD revision. If no previous DD revisions are present, it uses the Generic DD.

NOTE

- It is recommended not to use this option unless suggested by Honeywell TAC.
- After deleting a DD, the FDM Clients that are open must be synchronized as described in the section [“Synchronizing a DD-based template”](#).
- After a DD is deleted from the FDM database, offline configurations of that particular DD are deleted.
- You cannot delete generic DDs.
- You can delete DDs for either Gateway of Field devices.

To delete a DD file

1. Click Library > Manage DDs > Delete DD File from the FDM Client. The Delete DD File dialog box appears.
2. Select the protocol type (HART, FF, or ISA100) and then click Next.
3. Select the manufacturer of the device DD that needs to be deleted and then click Next. The list of device types appear supported by that manufacturer.
4. Select the device type of a DD that needs to be deleted and then click Next. The list of device revisions appear supported by that device type.
5. Select the device revision of a DD that needs to be deleted and then click Next. The list of DD revisions appear supported by that device revision.
6. Select the DD revision for the device revision of a device that needs to be deleted and then click Delete.
7. The Delete DD File dialog box appears displaying the details of the selected DD file that needs to be deleted and prompting you to confirm the deletion of the selected DD file.
8. Click Yes to delete the DD file. After deleting a DD, a message appears displaying DD Deleted successfully.

8.3 Synchronizing a DD based Template

FDM provides an option to synchronize the FDM Client data with the FDM Server data and update it with the latest templates.

When you add a DD file to the server, it generates the template for the corresponding DD that is added. To view this template on FDM Client, you need to either log off from the FDM and log on again, or use the Template Caching option to synchronize the data.

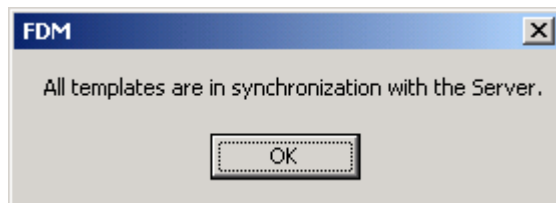
This functionality can be used for synchronizing DD information between the FDM Server and FDM Client. Closing and opening the FDM Client automatically performs the synchronization.

To synchronize and update the FDM Client with the FDM Server

1. Assume that the new template is generated in the FDM Server for the DD file added.
2. From the FDM Client, click Library > Template Caching. The Template or Icon Download dialog box appears.

NOTE

If all templates are already synchronized, the following message appears.



3. Click Start to start the synchronization.
4. The Template or Icon Download dialog box appears displaying the synchronization progress.
5. Click Close.

DTM MANAGEMENT

DTMs (Device Type Managers) are optional software components provided by device vendors for operating the devices, configuring device parameters, and accessing advanced diagnostic information. DTMs can range from a simple Graphical User Interface (GUI) for setting device parameters to a highly sophisticated application.

DTMs are capable of performing complex real-time calculations for diagnosis and maintenance purposes, or implement complex business logic for device calibration.

DTMs enables usage of devices in all asset management and device configuration software like FDM, with the help of FDT-DTM technology. The DTM Library Manager is a user interface, where you can view the details of all installed DTMs present in FDM, update the DTM library, add DTMs, and remove DTMs.

NOTE

The list of DTMs, which are qualified with every FDM release, is published at the <http://www.honeywellprocess.com> on the Honeywell Process Solutions support website. If you want to use any new DTM software, which is not listed in the qualified list, you are advised to:

- Contact the FDT group (<http://www.fdtgroup.com>) and verify if the DTM software is a registered software.
- Before installing, scan the new DTM software with the recommended antivirus software to ensure that the software is free from malware.
- Honeywell is not responsible for any damages caused by the third-party DTM software.
- For more information about DTM installation and removal, refer to the corresponding DTM installation guide from the vendor.

9.1 Installing DTMs

When a specific device or group of devices is to be used with a specific DTM software package, you must install the vendor provided setup package in each FDM Client where it is to be used. Note that most DTM packages install many DTMs and, in some cases, the entire vendor's catalog of devices. For more information about DTM installation, refer to the corresponding DTM installation guide from the vendor.

NOTE

- Before you install DTMs, check for the required operating system and some system components like Microsoft .NET. Also, you should check for installation requirements, like system memory, and so on.

- The list of DTMs, which are qualified with every FDM release, is published at the <http://www.honeywellprocess.com> on the Honeywell Process Solutions support website. If you want to use any new DTM software, which is not listed in the qualified list, you are advised to:
 - Contact the FDT group (<http://www.fdtgroup.com>) and verify if the DTM software is a registered software.
 - Before installing, scan the new DTM software with the recommended antivirus software to ensure that the software is free from malware.
- Honeywell is not responsible for any damages caused by the third-party DTM software.

9.2 Managing DTMs that support proprietary protocols

Some FDT 1.2.1 compliant Communication and Gateway DTMs implement their proprietary protocols. During a Topology Scan Operation, their scan response to FDM is based on proprietary protocol. In order for FDM to interpret this response, FDM requires xsl file to transform this protocol specific scan response to a FDT specified generic format. Typically DTMs install these files as part of their installation in their schema specific folder.

As Per FDT 1.2.1 specification, DTMs can provide their schema file path to FDM while updating DTM Library. But, most of the DTMs do not provide this Path. Hence, in order to support such DTMs in FDM, you need to manually provide the exact schema path for DTMs in FDMSchemaSource.xml available in FDM Schema path.

For these DTMs, you must follow the following SOP.

- For DTMs that support standard protocols compatible with FDT 1.2.1 specifications, you need not follow this SOP and this section can be skipped.
- For a list of FDT 1.2.1 supported protocols, refer to FDT Org website, <http://fdtgroup.org/technical-documents/>
- If DTM supports proprietary protocol, then SOP must be followed as this might affect Topology scan on the DTM.

Prerequisites

- The FDMSchemaSource.xml file must be updated after DTM installation and before updating DTM Library.
- You must update DTM Library every time this file is updating.
- Determine the third party Protocol GUIDs for all its supported protocols from DTM documentation.
- Determine the DTM Schema path for each of its supported protocols, which is usually in their installation folder. If unable to find the schema path, contact DTM Vendor.

SOP steps

1. Install the required DTMs.
2. Open
C:\ProgramData\Honeywell\FDM\CommonResources\FdtXmlFiles\FDMSchemaSource.xml
in a text editor.
3. Under Protocol element for GUID attribute, provide the GUID for that particular protocol.
4. Under SchemaPath element and for Path attribute, provide the absolute path of schema folder within double quotes.
5. If the Protocol already has schema path from one DTM and new path needs to be added for

another DTM for same protocol, you can repeat SchemaPath element and provide the new path.

6. If there are many such DTMs with proprietary protocols, you can repeat the Protocol element for each protocol.
7. Once the FDMSchemaSource.xml file is updated accordingly, you can proceed with Updating DTM Library.

9.3 Updating the DTM library

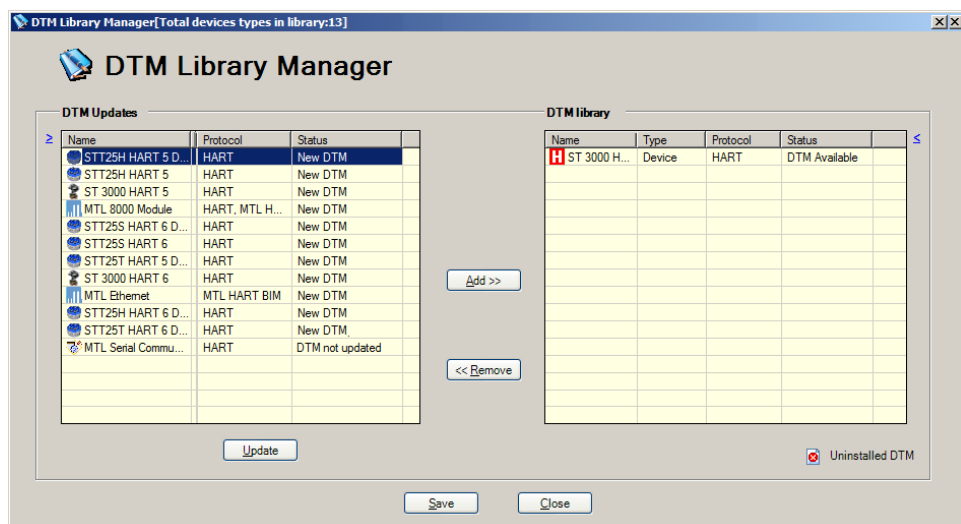
After you have installed DTMs from the FDM Client or FDT Comm Console, you need to perform an update to detect these changes.

NOTE

- DTM library is system dependent. If you have installed and updated the DTM library in one client, it does not reflect in other clients. This procedure has to be performed on all clients wherever DTM(s) are installed.
- When FDM Client is installed on RCI, and if you are updating the DD/DTM settings in both the FDM Client/FDT Comm Console, then this setting is effective in both.
- When FDM Client is installed on RCI, and if you have installed/removed DTMs on the RCI system, then you must update the DTM library on both the FDM Client and the FDT Comm Console.
- Ensure to close the FDM Client/FDT Comm Console after updating the DTM library and re-launch to proceed.

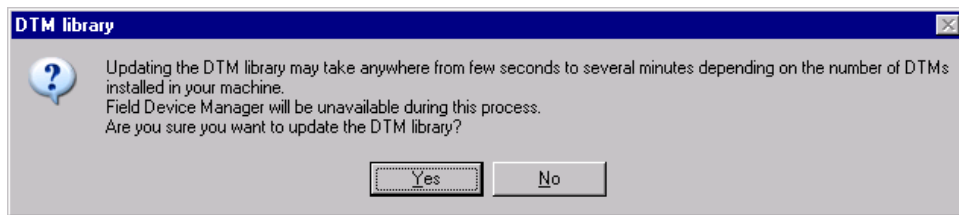
To update the DTM library

1. Log on to the FDM Client.
2. Click Library > Manage DTM Library. The DTM Library Manager dialog box appears.



- Click  to expand the DTM Updates pane.
- Click  to expand the DTM library pane.
3. Click Update. A confirmation message appears.

- Click Yes to discard the changes and continue with updating the library. The following DTM library message appears.



- Click Yes to update the DTM library. The DTM Updates lists all the newly installed and removed DTMs in the system.

For more information about adding newly detected DTMs to the DTM Library, refer to the section [“Adding DTMs to the DTM library”](#).

Following are the different DTM status and their indications as in the DTM Library Manager dialog box.

Status	Description
DTM not updated	Indicates that the DTM is not updated recently.
New DTM	Indicates that the DTM is updated recently.
DTM Available	Indicates that the DTM is available and selected to the DTM library.
DTM Unavailable	Indicates that the DTM is removed.
Modified DTM (Available)	Indicates that the DTM is modified.

The DTM Updates pane shows the previously scanned list of DTMs that were not selected in DTM library pane. To view the latest list of DTMs, ensure to click Update.

9.4 Adding DTMs to the DTM library

To add DTMs to the DTM Library

- Ensure that the required DTMs are installed in the computer. For more information, refer to the section [“Installing DTMs”](#).
- Perform the steps 1 through 5 of the [“Updating the DTM library”](#) section. The DTM Library Manager dialog box appears.
- Select the DTMs that you want to add to the DTM Library from the DTM Updates.

TIP

To select all the DTMs in any of the lists, select the first DTM and then press CTRL+SHIFT+END on the keyboard. To select multiple DTM(s), press CTRL and then select the required DTMs.

- Click Add >>. The new DTMs are added to the DTM Library.
- Click Save.

9.5 Removing DTMs from the DTM library

To remove DTMs from the DTM Library

1. Log on to the FDM Client.
2. Click Library > Manage DTM Library. The DTM Library Manager dialog box appears.
3. Select the DTM or DTM(s) that you want to remove from the DTM Library.
4. Click <<Remove. The selected DTM or DTM(s) are removed from the device types in the current DTM Library and moved to the device types that are not part of current DTM library. It is not necessary to uninstall the DTM after you remove the DTM from the library.
5. Click Save.

NOTE

Updating the DTM library operation may cause more resource consumption of the FDM Client/FDT Comm Console. This is dependent on the type and number of DTMs installed. Hence, it is recommended to close the FDM Client/FDT Comm Console application and relaunch before proceeding with any further operation after every DTM library update.

9.6 Upgrading DTM version

If you want to upgrade the version of an already existing DTM in DTM library, perform the following steps.

1. From the FDM Client, open the DTM Library Manager and remove the older version of the DTM which is not in use. If several DTMs are part of a package, all of those DTMs must be removed for the removal to be successful.
2. Save/close the DTM Library Manager.
3. Close FDM Client.
4. Uninstall the older version of the DTM setup from the computer through Programs and Features.
5. Verify whether all older versions of DTMs are removed from the DTM library. To verify, from the FDM Client, open the DTM Library Manager, and then click Update.
6. Close the FDM Client.
7. Install the newer version of the DTM software.
8. From the FDM Client, open the DTM Library Manager and then update the DTM library.
9. Add the newer version of DTMs in DTM library and then save/close the DTM Library Manager. For more details, refer to the section [“Updating the DTM library”](#) and [“Adding DTMs to the DTM library”](#).

NOTE

- For more information about DTM installation/upgrade and troubleshooting, refer to the DTM installation guide from the vendor.
- Failure to follow the DTM Version Upgrade procedure given here might result in DTM "ghosts".

9.7 Uninstalling DTMs

To uninstall a DTM, perform the following steps. If an installed DTM contains more than one device, all such devices must be removed. Otherwise, ghosts will remain.

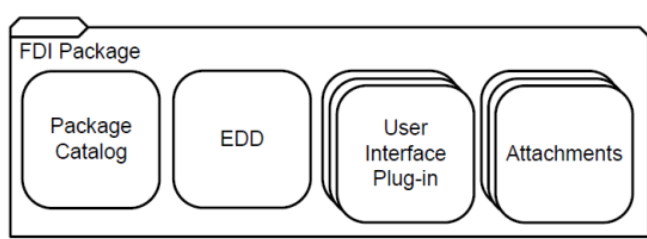
1. From the FDM Client, open the DTM Library Manager and remove the older version of the DTM which is not in use. If several DTMs are part of a package, all of those DTMs must be removed for the removal to be successful.
2. Save/close the DTM Library Manager.
3. Close FDM Client.
4. Uninstall the older version of the DTM setup from the computer through Programs and Features.
5. Verify whether all older versions of DTMs are removed from the DTM library. To verify, from the FDM Client, open the DTM Library Manager, and then click Update.

For more information about DTM uninstallation, refer to the corresponding DTM installation guide from the vendor.

FDI DEVICE PACKAGE MANAGEMENT

FDI device package is a new entity standardized by FDI Corp. for effective device management. Most device manufacturers create an FDI package for each model or type of device that they make. The EDD contained in the FDI package contains device-specific information that is used for interpreting the responses received from the device. You can add and delete FDI packages from the client. The FDI device package feature is supported for PROFIBUS PA profile v3.01 and later versions.

Contents of an FDI device package



In the FDM R500 release, FDM uses only EDD content in the package for PROFIBUS. Future releases may have full support for all FDI package specifications.

NOTE

FDI Packages are supported only for PROFIBUS PA V3.01 and later devices. However, it is NOT supported for PROFIBUS DP devices even though Package selection option is enabled.

Before you attach the Packages, perform a scan using the recommended and up-to-date antivirus software to ensure that the Packages are free from malware. Honeywell is not responsible for any damages caused by corrupted Packages with malware present.

10.1 Adding a Package

If the FDI package for a given device is not present in the FDM package library, you can add FDI package to the package library by using the Manage Package option. This option contains – Add and Delete package submenus. You can also update a package with a later version.

When you add a package, the server automatically generates the corresponding template for the EDD. This template is published to all the open clients.

NOTE

Only users assigned with the privileges associated with the administrator role can add/delete a package.

10.1.1 Package validation

A package is validated before it is added. The Package is considered valid if:

- It contains a valid signature
- The digital certificate (or any of its parent certificates) with which the package was signed is a trusted one
- The package contains attachments as per FDI specifications. The permitted attachments according to the specifications are:
 - Image
 - Documentation
 - Protocol support file
 - FDI registration certificate

Appropriate error messages appear if you are trying to add a package that is:

- Invalid
- Valid but does not contain a valid signature
- Valid but does not contain a valid certificate
- Contains invalid attachments

If you however proceed in spite of a validation failure, the package will be added to the system and will be audit trailed.

To add any new package from the client to the server

1. From the FDM Client, click the **Add Package** icon under the FDM Toolbar or click **Library > Manage Packages> Add Package**. The **Select a Package** dialog box appears.
2. Browse to the folder where the **.fdix** file is located, select the file and click **Open**.
3. Click **Add**. A confirmation message appears. Click **OK** to acknowledge.

10.2 Updating a Package

You can select a later version of the package and update. To revert back to a previous version, first delete the later version and then add the previous version.

To update to a later version of the package:

1. From the FDM Client, click the Add Package icon under the FDM Toolbar or click Library > Manage Packages> Add Package. The Select a Package dialog box appears.
2. Browse to the folder where the .fdix file is located, select the file and click Open.
3. Click Add. A confirmation message appears. Click OK to acknowledge.

10.3 Deleting a Package

This feature enables you to delete a particular version of a package. When a package for a particular device type and device revision is deleted, all devices of that type loaded subsequently use the previous package revision. If no previous package revision is available, the profile package shipped by Honeywell is used.

NOTE

It is recommended not to use this option unless suggested by Honeywell TAC.

After deleting a package, the FDM Clients that are open must be synchronized as described in the section [Synchronizing a Package-based template](#).

To delete a Package

1. Click Library > Manage Packages> Delete Package from the FDM Client. The Delete Package dialog box appears listing all devices by all manufacturers for all devices.

Delete Package

All Protocols All Manufacturers All DeviceTypes Show

List of available packages; Please Select a package and click on delete. Please note profile packages cannot be deleted.

PROTOCOL	MANUFACTURER	DEVICE TYPE	PACKAGE TYPE	PACKAGE VERSION	Delete
PROFIBUS PA	Siemens	SITRANS P DSIII	Device	1.0.24	Delete
PROFIBUS PA	Honeywell	Profile	Profile	00.01.00	Delete
PROFIBUS PA	Honeywell	Profile	Profile	00.02.00	Delete

2. Sort the list to identify the package you want to delete by selecting the protocol, manufacturer, and device from the respective drop-down lists. Click Show.
3. Packages meeting your selection criteria are listed displaying Package Type and Package Version information.
4. Click Delete corresponding to the package you want to delete. Note that Profile Packages cannot be deleted.
5. Acknowledge the confirmation message and click OK.

SYNCHRONIZING FDM TEMPLATES

FDM provides an option to synchronize the FDM Client data with the FDM Server data and update it with the latest templates.

When you add a DD file/FDI Package to the server, it generates the template for the corresponding DD/Package that is added. To view this template on FDM Client, you need to either log off from the FDM and log on again, or use the Template Caching option to synchronize the data.

This functionality can be used for synchronizing DD/Package information between the FDM Server and FDM Client.

NOTE

Closing and opening the FDM Client automatically performs the synchronization.

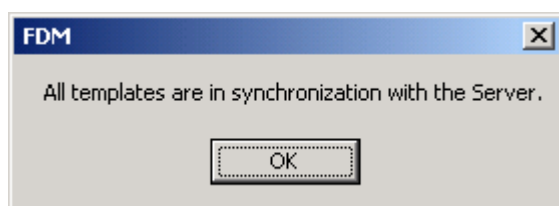
To synchronize and update the FDM Client with the FDM Server

1. Assume that the new template is generated in the FDM Server for the DD file/FDI Package added.
2. From the FDM Client, click Library > Template Caching. The Template or Icon Download dialog box appears.

NOTE

If all templates are already synchronized, the following message appears.

If all templates are already synchronized, the following message appears.



3. Click Start to start the synchronization.
4. The Template or Icon Download dialog box appears displaying the synchronization progress.
5. Click Close.

ABOUT OFFLINE CONFIGURATION

The Offline Configuration feature enables you to configure and save a set of device parameters without the need for a device to be available physically. In other words, it enables you to create a configuration for a device, without the device being available online and this can be downloaded to an online device (of the same type) later.

The Offline View > Offline Configuration tab enables you to create an offline configuration for a device. The offline configuration can be downloaded to the device by right-clicking a device in the Online View > Network View.

A user can create three types of Offline Configurations which are as follows:

- DD offline configurations
- Generic DD offline configurations
- DTM offline configurations

NOTE

This feature is ONLY supported for HART devices including HoP devices.

Though you can create a DD offline configuration for a device as described below, it is recommended to use an offline configuration of a device by using Save as Offline template feature. For more information, refer to the section [“Saving an online configuration as an offline configuration using DD”](#). An offline configuration thus saved is more accurate in terms of reflecting proper configuration of device and the representative values.

When creating an offline configuration for the first time, you have to explicitly select the manufacturer, device type and device revision for the configuration, from the respective list boxes in the Create Configuration form. However, if you are creating another offline configuration for the same manufacturer and/or device type and/or device revision, you can browse through the Offline Configurations tree, right-click and choose the Create Configuration option, either at the manufacturer level, the device type level or the device revision level. FDM automatically populates the appropriate vendor information in the respective list boxes in the Create Configuration page.

12.1 Creating a DD offline configuration for a specific device type

For a specific device type, you can create a DD offline configuration. You can use this offline configuration only for devices belonging to the specific device type.

To create a DD offline configuration for a specific device type

1. Log on to the FDM Client.
2. Click the Offline View group. The Offline Configuration, Display Filter and Device Library tabs appear.
3. Click the Offline Configuration tab. The DD Offline Configurations/Generic DD Offline Configurations/DTM Offline configurations tree appears in the left pane.
4. Right-click DD Offline Configurations and then click Create Configuration. The Offline – Create Configuration page appears in the right pane.
5. From the Protocol list, select the HART protocol.
6. From the Manufacturer list, select the manufacturer of the device. Based on the manufacturer that you select the device types are populated in the Device Type list.
7. Select the appropriate device type from Device Type. FDM populates the corresponding device revisions.
8. Select the appropriate Device Revision and DD Revision.
9. Click Create. The device parameters appear in the Configuration View panel with default parameters populated as per the DD file.

Offline - Create Configuration

Configuration Name: Offline - Untitled

Configuration Details

Protocol: HART
 Manufacturer: ABB_26
 Device Revision: 5
 Device Type: K5X
 DD Revision: 2
 Create

Configuration View

☐ View IDs ☐ Select All

Items	Value	Units	Select
Sta pres unit	psi		☐
Sensor trim units	inH2O @20DegC		☐
Max working pres unit	inH2O @20DegC		☐
Pressure unit	inH2O @20DegC		☐
Max working pres	0	inH2O @20C	☐
Upr snsr trim pt	0	inH2O @20C	☐
Lor snsr trim pt	0	inH2O @20C	☐
Static Pres	0	psi	☐
LRV	0	inH2O @20C	☐
URV	0	inH2O @20C	☐
Poll addr	0		☐
Tag	????????		☐
Message	????????????????????????????????????		☐
Descriptor	????????????????		☐
Date	1/1/1900		☐
Xfer fnctn	Linear		☐

Save Save As Close

The Items (Parameters), Value and the Units appear in a tabular format. To display the parameter IDs, select View IDs.

10. If necessary, you can edit the parameters. For more information about editing parameters, refer to the section [“Editing an offline configuration”](#). After making the required changes to the parameter values, select the check box (located in the Select column) corresponding to the parameters that you want to later download to the device(s). Select All to download all the parameters to the device.
11. Click Save to save the changes. The Save Offline Configuration As dialog box appears.
12. Type an appropriate name for the offline configuration in Name box. Click OK to save the configuration. The name of the configuration appears in Configuration Name box.

NOTE

If you want to save the copy of offline configuration as a new offline configuration with the specified file name, click Save As. The new offline configuration name appears in the DD Offline Configurations tree.

Ensure that file name does not contain special characters.

In addition, the name of the configuration appears under Manufacturer ID > Device Type > Device Revision in DD Offline Configurations tree.

TIP

If you want to rename a DD Offline Configuration, right-click offline configuration (name) and click Rename.

If you want to delete a DD Offline Configuration, right-click offline configuration (name) and click Delete.

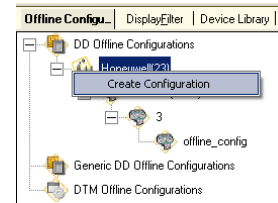
You cannot rename and delete a DD Based configuration if another user (FDM Client) has opened the configuration form.

For instance:

Creating an offline configuration at Manufacturer level:

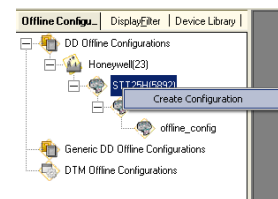
To create an offline configuration, as an existing configuration for the same manufacturer, but for a different device type and device revision, perform the following:

- In the Offline Configurations tree, right-click Manufacturer and then click Create Configuration.

**Creating an offline configuration at Device Type level:**

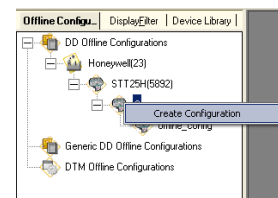
To create an offline configuration for the same manufacturer and device type, but for a different device revision, perform the following:

- In the Offline Configurations tree, right-click the Device Type and click Create Configuration

**Creating an offline configuration at Device Revision level:**

To create an offline configuration for the same Manufacturer, Device Type and Device Revision, perform the following:

- In the Offline Configurations tree, right-click the Device Revision, and click Create Configuration.



12.2 Creating a generic DD offline configuration

FDM enables you to create a DD offline configuration that contains a set of standard parameters that are applicable to all device types. Hence, you can use a generic DD offline configuration to configure devices of any device type.

To create a Generic DD offline configuration for all device types

1. Log on to the FDM Client.
2. Click the Offline View group. The Offline Configuration, Display Filter, and Device Library tabs appear.
3. Click the Offline Configuration tab. The DD Offline Configurations/Generic DD Offline Configurations/DTM Offline configurations tree appear in the left pane.

4. Right-click Generic DD Offline Configurations and click Create Generic Configuration. The Offline – Create Configuration page appears in the right pane. As the configuration is generic, the fields (Manufacturer, Protocol, Device Revision, Device Type, and DD Revision) in the Configuration Details panel are disabled and populated with predefined values.
5. Click Create. The generic device parameters appear in the Configuration View panel.

Offline - Create Configuration

Configuration Name: Offline - Untitled

Configuration Details

Protocol: HART
 Manufacturer: Generic
 Device Revision: 5
 Device Type: Generic
 DD Revision: 5
 Create

Configuration View

☐ View IDs ☐ Select All

Items	Value	Units	Select
PV range unit	inH2O		☐
PV LRV	0	inH2O	☐
PV URV	0	inH2O	☐
Poll addr	0		☐
Tag	????????		☐
Message	????????????????????????????????		☐
Descriptor	????????????????		☐
Date	1/1/1900		☐
PV Damp	0	s	☐

Save Save As Close

6. The Items (Parameters), Value, and the Units appears in a tabular format. To display the parameter IDs, select View IDs.
7. If necessary, you can edit the parameters. For more information about editing parameters, refer to section [“Editing an offline configuration”](#). After making the required changes to the parameter values, select the check box (located in the Select column) corresponding to the parameters that you want to download to the device(s). Select All to download all the parameters to the device.
8. Click Save to save the changes. The Save Offline Configuration As dialog box appears.
9. Type the name for the offline configuration in Name. Click OK to save the configuration. The name of the configuration appears in Configuration Name box.

NOTE

If you want to save the copy of offline configuration as a new offline configuration with the specified name, click Save As. The new offline configuration name appears in the Generic DD Offline Configurations tree.

Ensure that file name must not contain special characters.

In addition, the name of the configuration appears in Generic DD Offline Configuration tree view.

TIP

If you want to rename a Generic DD Offline Configuration, right-click the offline configuration (name) and click Rename.

If you want to delete a Generic DD Offline Configuration, right-click the offline configuration (name) and click Delete.

You cannot rename and delete a Generic DD Based configuration if another user (FDM Client) has opened the configuration form.

12.3 Creating a DTM offline configuration

FDM enables you to create an offline configuration for DTM. For DTMs that support offline configuration, you can use this only with devices for which the load setting is Load Using DTM.

NOTE

The DTM offline configurations can be created only in FDM Client in which the DTMs are installed and the FDM DTM Library is updated with the installed DTMs.

To create a DTM offline configuration

1. Log on to the FDM Client.
2. Click the Offline View group. The Offline Configuration, Display Filter, and Device Library tabs appear.
3. Click the Offline Configuration tab. The DD Offline Configurations/Generic DD Offline Configurations/DTM Offline configurations tree appear in the left pane.
4. Right-click DTM Offline Configuration and click Create Configuration. The Create Configuration page appears.

NOTE

The functionality and appearance of the offline configuration page is vendor specific.

5. Select the device manufacturer from Manufacturer drop-down list and device from Device Type drop-down list, and click View. The DTM Start Page appears in the right pane.
6. Edit the parameter required for offline configuration. Refer to section [“Configuring a device using DTM”](#) for the steps on how to edit device parameters.
7. Click  icon to save the DTM offline configuration. The Save Resource As dialog box appears.
8. Type the name for the offline configuration in Name.
9. Click OK to save the DTM offline configuration. The saved configuration appears in the DTM Offline Configurations tree.

TIP

If you want to rename a DTM offline configuration, right-click the offline configuration (name) and click Rename.

If you want to delete a DTM offline configuration, right-click the offline configuration (name) and click Delete.

You cannot rename or delete a DTM offline configuration if it is being used in another FDM Client.

DTM offline configuration is available only in the clients in which the respective DTMs are installed. For example, if you create a Honeywell DTM configuration in Client 1, it is available only in the clients in which Honeywell DTMs are present in the DTM library.

12.4 Editing an offline configuration

After creating an offline configuration, FDM lists the configurations in the DD Offline Configurations/ Generic DD Offline Configurations/DTM Offline Configurations tree under the Offline Configuration tab. You can browse through the DD/Generic DD/DTM offline configuration tree, open a specific/generic configuration, modify the configuration, and save the changes if required.

To modify a DD/Generic DD/DTM offline configuration

1. Log on to the FDM Client.
2. Click the Offline View group. The Offline Configuration, Display Filter and Device Library tabs appear.
3. Click the Offline Configuration tab. The DD Offline Configurations/Generic DD Offline Configurations/ DTM Offline configurations tree appears in the left pane.
4. Right-click the offline configuration and then click Open. If you select DD offline configuration name, its configuration page appears in the right pane.

The screenshot shows the 'Offline - ST800_Offline_config' window. It has a sidebar on the left with 'Offline' and '...' buttons. The main area is divided into two sections: 'Configuration Details' and 'Configuration View'.

Configuration Details:

- Configuration Name: ST800_Offline_config
- Protocol: HART
- Manufacturer: Honeywell_23
- Device Type: ST 800
- Device Revision: 1
- DD Revision: 10

Configuration View:

There are checkboxes for 'View IDs' and 'Select All'. Below is a table with columns: Items, Value, Units, and Select.

Items	Value	Units	Select
PV unit	ftH2O		☐
PV LRV	0	ftH2O	☐
PV URV	924.3	ftH2O	☐
Poll addr	0		☐
Tag	ST8		☐
Message	VGHVGH		☐
Descriptor	VHNVB GHVBH		☐
Date	1/23/2013		☐
Long tag	ST800		☐
PV AO	21.5	mA	☐
Loop mA	Disabled		☐
PV Damp	1	s	☐
Xfer Fn	Linear		☐
Low Flow Cutoff Mode	Dual Slope		☐
Low Flow Cutoff Brkpt(User Config Mod	7.071068	%	☐

At the bottom of the window are buttons for 'Save', 'Save As', and 'Close'.

The offline configuration allows you to edit all the parameters of the device that affect the configuration of the device. The solution provides an interactive interface that guides you to change the values and configuration of the device as you edit it.

NOTE

- Few writeable parameters are not directly exposed through the menu structure of a device, and can be edited only through a method. But they often are critical in configuring the device and hence are exposed in offline configuration. Sometimes, such parameters may not always succeed in a download. It is advised to ensure the value of such parameters to be same as that in the device.
- A device description file may contain variables whose values have an impact on other variable(s). In FDM, the former is referred to as dominant variable and the latter as dependent variable(s). An example is the dependency of sensor range value on the sensor type. Hence, sensor type can be referred to as a dominant variable.
- When you edit a dominant variable, FDM automatically updates the corresponding values for the dependent variables.
- Read-only parameters which are not editable in the device, but have other editable parameters that depend on its value.

When you are editing parameters, the pre/post edit actions and warnings appear if they are defined in the DD. You must respond to those actions. These actions and warning varies from one variable to another.

Following icons are used for indicating different states of the parameters during an offline configuration.

-  indicates Invalid parameters. – These parameters are not valid parameters as per the current configuration.
-  indicates Valid parameters – These parameters are valid as per the current configuration and the writable parameter can be downloaded to the device.
-  indicates Changed parameters – When a valid parameter is edited, any other parameter(s), which are dependent on it must have the icon changed to green. This indicates that the value of these parameters needs to be verified and probably downloaded.

5. If you make any modification, the Save button is enabled.

NOTE

You cannot modify the offline configuration if another user (FDM Client) has opened the configuration form before. You can modify the parameter values, only after all other users who have opened the configuration before you close the form.

6. Click Save and then click Close. If you select a DTM offline configuration, respective DTM Start page appears in the right pane.
7. To edit parameters, refer to the section [“Configuring a device using DTM”](#).

NOTE

- If you make modifications and close the screen without saving the changes, a confirmation message appears prompting you to save. Click Yes to save.
- The Reason dialog box appears only if the Administrator has enabled reason logging for the action type, in the Audit Trail settings.

8. Click  icon to save DTM Offline Configuration.
9. If you want to download the offline configuration, refer to the section [“Downloading a DD based offline configuration to an online device”](#)

DOWNLOADING BULK OFFLINE CONFIGURATIONS

The Bulk Offline Download feature enables you to use a DD offline configuration to configure multiple devices simultaneously. In other words, you can download multiple DD offline configurations to multiple devices of the different Manufacturer, Device Type, Device Revision, and DD Revision.

You can do bulk offline download with following options.

- Bulk offline download with Select devices.
- Bulk offline download with Import records from file.

NOTE

- This feature is only available for HART devices including HoP devices.
- To perform the bulk offline download, you must ensure to create a DD offline configuration.
- When the device autolock/exclusive access to unlock devices feature is enabled, you are not allowed to perform the bulk offline download.

To download bulk DD offline configurations using Select Devices option

1. Log on to the FDM Client.
2. Click Tools > Bulk Offline Download. The Bulk Offline Download page appears in the right pane.
3. Under Select Devices pane:
 - Select the HART protocol from the Protocol list.
 - Select the required Manufacturer from Manufacturer. FDM populates the Device Type list with the device types corresponding to the selected manufacturer.
 - Select the device type from Device Type. FDM populates the Device Revisions list corresponding to the selected device type.
 - Select the appropriate device revision from the Device Revision list.
4. If the devices matching the selected vendor information are found online, FDM lists the online devices under Device Tag.
5. From Device Tag, select the device(s) to which you want to download the offline configuration.
6. Based on the details (Manufacturer, Device Type, Device Revision, and DD Revision) you have selected, FDM populates the Offline Configuration list box with the matching offline configuration (s).

7. From Offline Configuration, select the appropriate offline configuration to download to the selected devices.

NOTE

If no offline configurations matching your selection are created, then Offline Configuration list box appears empty.

8. Click Add.

NOTE

You can only select the device(s), if an offline configuration corresponding to the selected vendor information (Manufacturer, Device Revision, Device Type, or DD Revision) is available. FDM disables the Add button, if no offline configuration is available.

You can only select the device(s), if an offline configuration corresponding to the selected vendor information (Manufacturer, Device Revision, Device Type, or DD Revision) is available. FDM disables the Add button, if no offline configuration is available.

The following page appears.

Bulk Offline Download

Select Devices

Protocol: HART [Import records from file](#)

Manufacturer: Honeywell_23 Device Revision: 1

Device Type: ST 800 DD Revision: 10

Device Tag: C1-SESVB.AICHANNEL_03_1 Offline Configuration: ST800_Offline_config **Add**

Device Name	Offline Configuration	Status	Report
C1-SESVB.AICHANNEL_03_1	ST800_Offline_config		

Device Timeout (Minutes): 10 **Download** **Abort** **Close**

The grid shows the device name, offline configuration, status, and report for the selected devices.

9. Enter Device Timeout (in minutes), before you start downloading the offline configuration.

NOTE

The device timeout range is 4 to 30 minutes.

10. Click Download. A confirmation message appears.

NOTE

When you click Download button, only if some other operations are in progress, then an error message appears displaying Operation is denied. Acknowledge the error and close the operations listed in the error message on the corresponding Clients to start bulk offline download.

11. Click Yes to continue the Bulk offline Download. The progress report indicates the progress in downloading the offline configurations and provides the following information.
 - Individual devices selected offline configuration, status and report. The device status can be Pending, Loading, Downloading, Success, Failed, Timed out or Aborted.
 - Total number of offline configurations downloaded.

Status	Description
Pending	Device is not yet loaded.
Loading	Device is loading.
Downloading	Downloading of offline configuration starts on the device.
Success	Downloading offline configuration is completed.
Failed	Downloading offline configuration is failed.
Timed out	Downloading offline configuration did not happen within the specified timeout.
Aborted	Downloading offline configuration is aborted.
Disconnected	The device is disconnected from the network.
Load Failed	The device failed to load due to some internal error.
Device Tag does not exists	Device tag entered in CSV file is not a valid device tag.
Offline configuration does not exists	Offline configuration entered in CSV file is not a valid offline configuration.
Device is locked	Bulk Offline Download is failed due to devices are locked.
Unknown Error	Bulk offline download is failed for some of the devices due to internal error.
No parameters selected for download	Bulk offline download is failed due to parameters are not selected for download in the offline configuration.
Communication Error	Bulk offline download is failed while writing parameters to device due to command sent to the device was timed out or command response was returned as communication error.

NOTE

When Downloading of offline configuration on device fails, you can view the report by clicking Download Failed link in Report column.

12. After the download is complete, a confirmation message appears and then click OK.
13. Click Export to export the summary of bulk offline download operation.

To download multiple DD offline configurations to multiple devices with Import records from file link, perform the following steps.

1. 363BLog on to the FDM Client.
2. Click Tools > Bulk Offline Download. The Bulk Offline Download page appears.

NOTE

You have to update the .csv file which is present at the default location
C:\ProgramData\Honeywell\Fdm\Client\Resources\ Resource Templates with device
tags and offline templates that is required for download.

3. Click Import records from file. The Select File dialog box appears. The selected .CSV file with device tags and offline configuration shows in the Device Name and Offline Configuration columns in the grid. It also displays the status and report of bulk offline download operation.
4. Click Download. A confirmation message appears.
5. Click Yes to continue the Bulk offline Download. In the next page, the progress report indicates the progress in downloading the offline configurations.
6. After the download is complete, a confirmation message appears and then click OK.
7. Click Export to export downloaded DD offline configuration for selected devices in the CSV format.

BUILD NETWORKS

After configuring the network, you must establish the connection with the network and detect the devices connected to the network.

This process of detecting devices and components connected to the configured networks is known as building a network.

All the devices must be commissioned and active to appear in FDM Network View. For example, FF devices are detected when you configure Experion network in the FDM Server Management Tool and Fieldbus Interface Module (FIM) in Control Builder to which FF devices are connected.

NOTE

- FDM builds the network automatically if the following services become unavailable:
 - FDM server
 - FDM Remote Communication Interface
 - FDM network interfaces (Experion PKS, RTU, Safety Manger, oneWireless, and MUX).
- Before trying to connect to the devices using FDM, ensure that you establish the physical connection between the device and the required network communication interfaces (RS-232 HART Modem, RS-485 HART Multiplexer, Honeywell HART DE Modem, Honeywell Experion PKS, Safety Network with Universal Safe Modules, COMM DTM Interface, HART-IP Network, OneWireless Network, or Honeywell TPS).
- During build network, if you try to perform multiple operations, FDM system becomes slow.
- You cannot perform the build network operation, if devices connected to the similar network are in use.
- If you perform build network from the cache, a message appears displaying Network build operation from cache for the configured RCI is complete in the Device notifications pane. This message appears only when you stop the FDM Server, open a new FDM Client (connecting to new instance of the FDM Server), and perform build network from the cache.
- If you perform build network for a device that is active under MUX monitoring in Control Builder, a message appears displaying Network build is aborted in the Device notifications pane.
- OneWireless network builds can take a long time if the devices are newly provisioned.

14.1 Detecting devices on the network

To detect a device connected to the network

1. From the Network View under Online view, expand FDM Server network tree. The list of network interfaces appears.
2. Right-click the required network interface and then click Build Network. When Build Network operation is performed, the status of the operation appears in the System Notifications pane.

FDM detects the devices connected to the network and displays them in the tree view.

NOTE

Depending upon the type of the communication hardware and interface, discovery of devices varies in FDM.

When a new device is detected, it automatically appears in the Network View tree. Similarly, when a device goes offline or is disconnected, it disappears from the Network View tree and is assigned to the Disconnected Nodes list.

NOTE

For the Safety networks, when the devices are disconnected, changes are reflected automatically in the online network view. But, when the devices are connected back, they are not reflected in the network view automatically till you turn the Fault Reset key on the SM controller.

14.2 Building FDT networks

The FDT Comm Console allows you to configure the FDT networks and build the complete network using DTMs only on the RCI Server. After configuring the communication and gateway DTMs and scanning the network, the network is available on the FDT Comm Console. It shows other networks configured on a particular FDM server. In the FDT Comm Console, you can view all network related updates, but device related operations are restricted to the local FDT network configured for that particular RCI.

The following table lists the features, which are supported in FDM Client and FDT Comm Console.

Features	FDM Client	FDT Comm Console
Advanced Search	Supported	Supported
Add/Edit/Delete User	Supported	Supported
Add/Edit/Delete Role	Supported	Supported
Add/Edit/Delete Group	Supported	Supported
Bulk Offline Download	Supported	Not supported
Bulk Operations	Supported	Not supported
Import and Export	Supported	Not supported
Delete Records	Supported	Supported
Attach/Detach/Upload Document	Supported	Supported
Attach/Detach Application	Supported	Supported
Add/Delete DD File	Supported	Supported
FDT Health Scan Settings	Not supported	Supported
Save and Restore network	Not supported	Supported
Go Online/Offline	Not supported	Supported
Upload/Download parameters	Not supported	Supported
Add/Delete device	Not supported	Supported
Rename device tag	Supported	Supported

To build the FDT networks

1. Add and configure a COMM DTM Interface in the FDM Server Management Tool. For more details, refer to the section [“Configuring Comm DTM network in FDM”](#).
2. Log on to the FDT Comm Console.

NOTE

The RCI machine name on which the FDT Comm Console is launched, appears in bold in Network View to clearly highlight the local RCI node.

3. In the Network View list, right-click the COMM DTM interface name and then click Add Device. The DTM Selection Dialog appears with the list of all the available DTMs.

4. Select the communication DTM and then click OK. The communication DTM is added to the Server and appears in the left pane.

NOTE

Ensure that DTM library is updated with the installed DTMs before you creating the network.

For more information about updating the DTM library, refer to section [“Updating the DTM library”](#).

5. Right-click the communication DTM and then click Open Configuration. The configuration page appears in the right pane.
6. The configuration page provides all the available functions of the communication DTM. Use these functions to configure the communication DTM. For more information, refer to the DTM specific help to ensure proper configuration. The following figure displays the configuration page of Softing Communication DTM.

You must enter appropriate values in all the fields, for the communication DTM to function as required.

7. After configuring the communication DTM, right-click the communication DTM and then click Go Online to make it online.

NOTE

It is not necessary to open the configuration page to make DTM online.

8. Right-click the communication DTM and then click Scan for Devices. The Channel Selection Dialog appears.

9. Select the required channels or All and then click OK. The ScanStatus message appears displaying the progress of the scan. After scanning, the Dtm Assignment dialog box appears. The devices are detected and listed in the Dtm Assignment dialog box.
10. For the selected channel number and address, assign DTMs to the devices. You can view the suggested DTMs for the devices.
11. Select the suggested DTM or if you want to assign different DTM, then click the Assign DTM button. The DTM Selection Dialog appears. Select the necessary DTM and then click OK.
12. Click OK in the DTM Assignment dialog box. The detected devices are visible in the FDT Comm Console (Network View > COMM DTM Interface).
13. If a gateway DTM is detected, perform steps 5 through 10 on the gateway DTM. The detected devices are visible in the FDT Comm Console (Network View > COMM DTM Interface).

NOTE

- Ensure to close all the configuration pages in FDT Comm Console before closing it.
- Ensure to make the modules offline (if they are online) before closing the opened configurations in the FDT Comm Console.
- Ensure to close all the configuration pages in FDT Comm Console before deleting the device. To delete the device, right-click the device and then click Delete device. The device is deleted from both FDT Comm Console and FDM Client Network View.
- Ensure to save the network before you close the FDT Comm Console. If you do not save the network, the entire FDT network configured in the FDT Comm Console is lost.
- You can rename the tags in the FDT Comm Console network view. To rename the tags, right-click the device and then click Rename. The tag name is changed and it is saved in the FDM database.
- FDM uniquely identifies devices based on device identification information received from the device. However, some PROFIBUS devices may not respond with the correct device identification information. As a result of this, the same device appears with a different tag name on every scan.

You can configure the device parameters, view history, and download offline configuration for DTM based devices from the FDT Comm Console.

14.2.1 Saving and restoring FDT networks

The Save and Restore feature in the FDT Comm Console allows you to save the FDT network that has been configured on a particular RCI computer. This network can be later restored and used.

To save and restore network, perform the following steps during building FDT network.

1. Initiate scanning a Comm DTM or Gateway DTM. For more information, refer to section [“Building FDT networks”](#).
2. After the scan completion, DTM Assignment dialog box appears.
3. After necessary changes, acknowledge the DTM Assignment dialog box.
4. Click  icon to save the FDT network. The Save Project dialog box appears where you can

specify file name and location. The network is saved in a xml file.

5. After saving the network, close the FDT Comm Console.
6. Launch the FDT Comm Console and then click  icon to restore the saved network file (XML), and make the Comm DTMs and Gateway DTMs online.

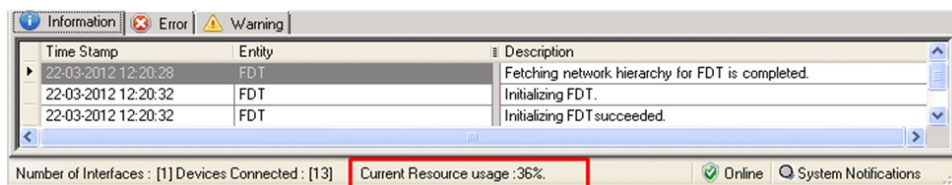
14.2.2 Resource consumption notifications in the FDT Comm Console

The current resource usage of the FDT Comm Console is indicated in the status bar in percentage format as shown below. This is important because FDT Comm Console deals with third party DTMs that might primarily contribute to overall resource consumption of this tool. The following are the three types of computer resource consumption information.

NOTE

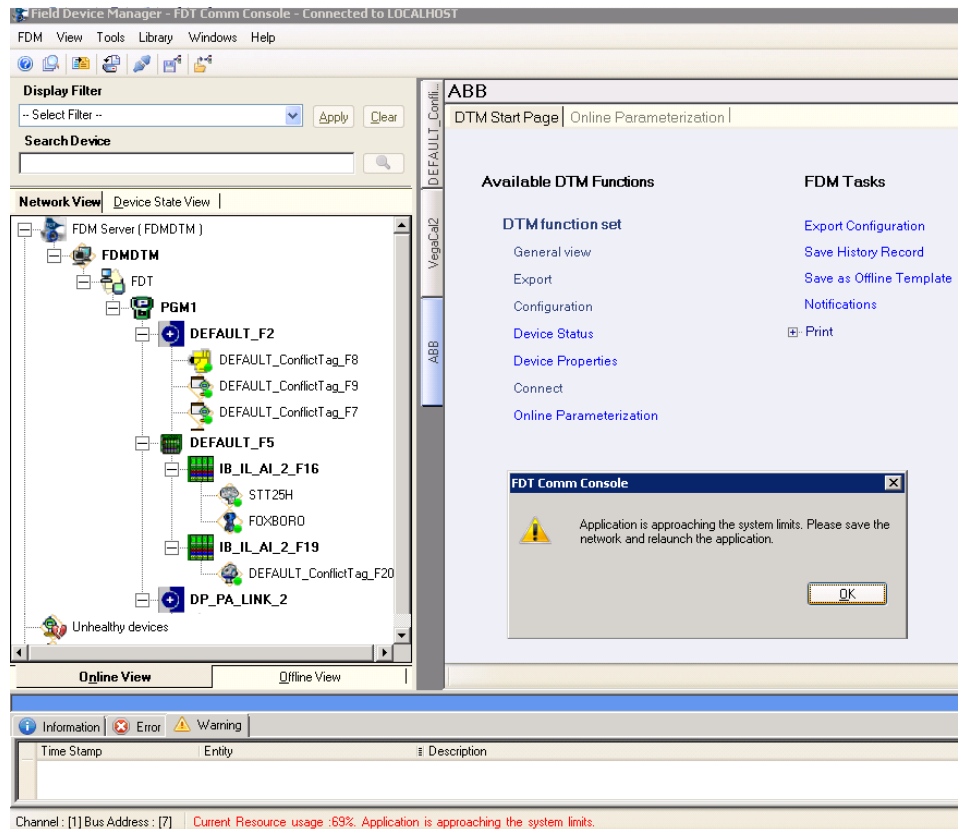
FDM records a log in the audit trail for resource consumption and you can view these logs using View > Audit Trail.

- Normal Resource Usage information: During Normal Resource Usage, you can continue to work on the FDT Comm Console.

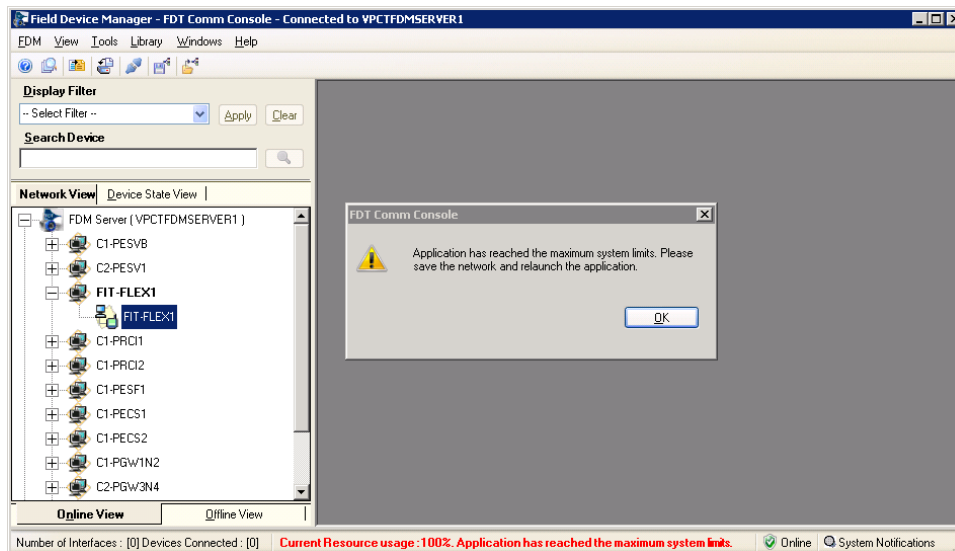


- Resource Warning Message: FDM monitors the resource consumption of FDT Comm Console and warns you appropriately when the resource consumption goes higher than the threshold limit. This allows you to take appropriate actions like saving the network, closing FDT Comm

Console and restoring the network.



- Maximum Resource Limit Warning Message: FDT Comm Console warns you appropriately when the resource consumption exceeds the maximum resource limit. This allows you to take appropriate actions like saving the network, closing FDT Comm Console and restoring the network.



NOTE

Creating a FDT network consumes the process memory of the FDT Comm Console program. The amount of memory consumed varies from one DTM to another. The resource monitor on the FDT Comm Console status bar allows you to keep track of the resource usage. If the resource usage exceeds the set threshold limits, the user is notified. Hence, it is recommended you to save the network, close and restart FDT Comm Console and then restore the network to reduce the resource consumption. This is to ensure that any further FDT operations are not affected by high resource consumption.

14.2.3 Configuring Gateway modules which do not support scan operation

Some Gateway DTMs do not support scan operation on them. You must manually add devices under DTM.

To configure the modules in FDT Comm Console

1. Perform steps 1 through 10 of the section [“Building FDT networks”](#) to configure DTMs in FDT Comm Console. The configuration varies from one Gateway to another. For more information about the configuration details, refer to the individual gateway manuals.
2. After the Gateway is made Online, select the Gateway module in FDT Comm Console.
3. Right-click the Gateway module and then click Add Device. The DTM Selection Dialog appears.
4. Select the appropriate Gateway module and click OK. The Channel Address Selection dialog box appears.
5. Select the channel number from the drop-down list and type an appropriate number in the Bus address box, which depends on the Gateway and click OK. For more information, refer to the gateway manuals. The appropriate module is listed under the Gateway of the FDT Comm Console hierarchy.
6. Perform steps 5 through 10 of the section [“Building FDT networks”](#) on the gateway DTM. Detected device DTMs along with the Communication and Gateway DTMs are listed in the FDM Client Network View under Comm DTM network. You can configure these devices from FDM Client and also from FDT comm console in the RCI machine where these devices are connected.

Example of configuring Phoenix Contact IO in the FDT Comm Console that does not support dynamic scan

1. Scan the Communication DTM to which the Phoenix Contact IO module is connected. The Phoenix Contact IO module must be detected.
2. After the Gateway is made Online, select the Gateway module in FDT Comm Console.

NOTE

It is not necessary to open the configuration page to make DTM online.

3. Right-click the Gateway DTM and click Add device. The DTM Selection Dialog appears.
4. Select Phoenix Contact Hart AI module DTM and click OK. A Channel Address Selection dialog box appears.
5. Select the channel number.

6. Type the appropriate module in the Bus Address and click OK. The DTM Dialog appears.

NOTE

Ensure that bus number should be unique for IO DTMs.

7. Select the slot number as necessary from the Slot drop-down list and click OK in the DTM Dialog.
8. After you made Hart module Online, right-click the HART module and click Scan for Devices. The ChannelSelectionDialog dialog box appears.
9. Select the required channels or All and click OK. After the scan operation on all selected channels completes, DTM Assignment dialog box appears, listing all the devices detected.
10. The DTM Assignment dialog box lists the recommended DTM against each device, if a matching DTM is found in the current DTM library.
11. You can select the suggested DTM or for a selected device at a particular channel/address, you may change the DTM. For this, click the Change DTM button. The DTM Selection Dialog appears. Select the necessary DTM and click OK.
12. Click OK in the Dtm Assignment dialog box. The detected devices are visible in the FDM Client (Network View > COMM DTM Interface).

NOTE

Ensure that the connected devices in Communication and Gateway DTMs are unloaded from FDM Client before making the Communication and Gateway modules Offline.

14.3 Configuration of PROFIBUS masters

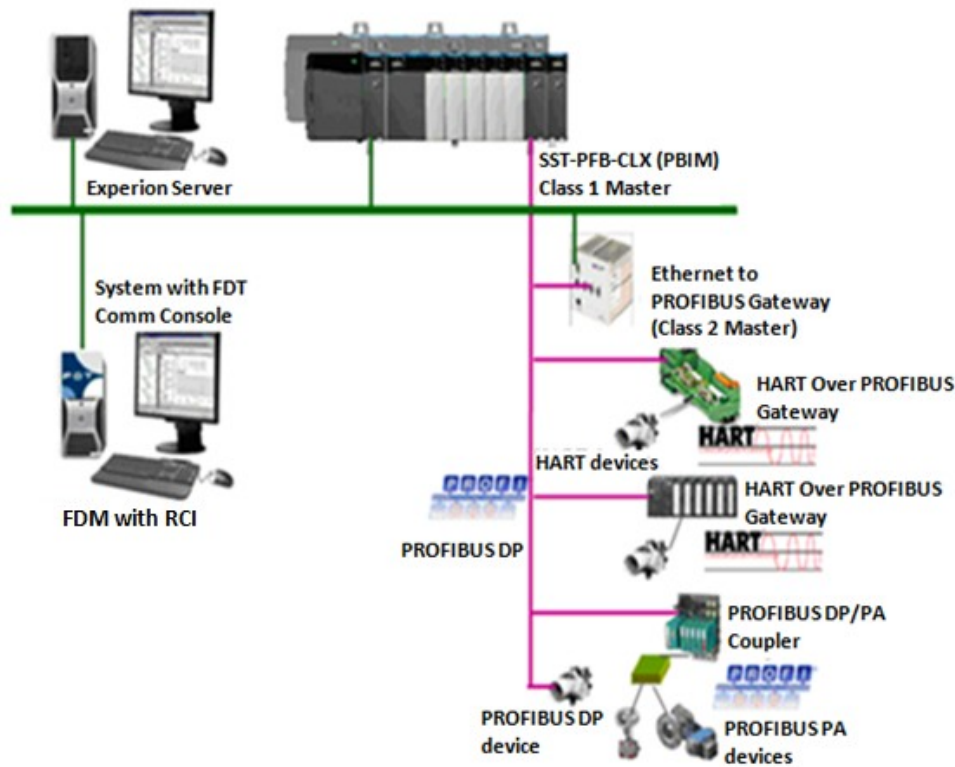
Class-II masters (DPM2) are used for operation and monitoring purposes and during the start-up. The associated exchange of data takes place if required. Therefore, class-II masters require acyclic communication services exclusively.

Following are the two scenarios in which a Class-II master is used.

- In first scenario, the Class-I master cannot provide the data into the Asset management system. In this case, the setup needs both Class-I and Class-II masters in order to obtain the data into DCS and also in Asset management system.
- In second scenario, the Class-I master itself acts as both Class-I and Class-II and provides data into DCS and also Asset management system.

14.3.1 Configuration with both Class-I and Class-II Master

Class-I masters which do not have communication DTMs cannot provide the data into Asset management tools like FDM. In this case, in order to obtain data into FDM, you must use both Class-I and Class-II masters.



When you are using both Class-I and Class-II masters, during configuration of Class-II master in FDM, the configuration parameters must be same as that of Class-I master.

This scenario can be better explained by taking the example of Woodhead SST-PFB-CLX module (PBIM) multi-dropped with Softing's FG100. Woodhead SST-PFB-CLX module (PBIM) is a Class-I Master which does not have a communication DTM and Softing's FG100 is a Class-II master which has communication DTM.

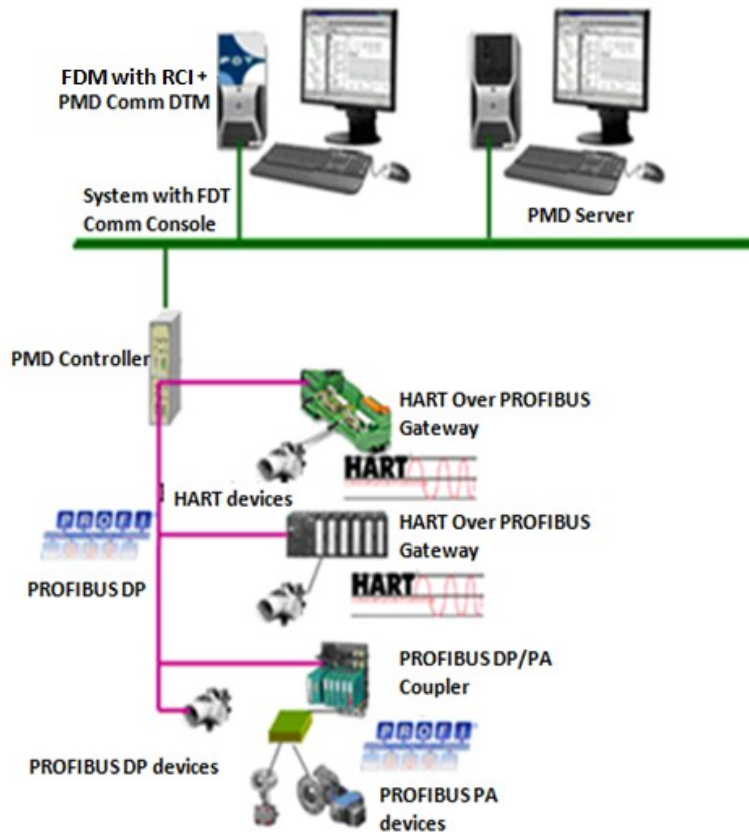
Multi master configuration of Woodhead SST-PFB-CLX module (PBIM) with Softing's FG100. In this scenario:

- The Woodhead SST-PFB-CLX module (PBIM), Softing's FG100, and other DP slaves are connected in Multi drop.
- Woodhead SST-PFB-CLX module (PBIM) acts as a Class-I master and fetches process data cyclically into a DCS system.
- Softing's FG100 acts as a Class-II master and fetches acyclic data as and when requested by the FDM.

14.3.2 Configuration with only Class-I master

Class-I masters which have communication DTMs can be used for providing the process data cyclically into DCS as well as for providing acyclic data into an Asset management system like FDM.

Honeywell's PMD Controller which has communication DTM can be taken as an example for this scenario. Following is a procedure for configuring and scanning PROFIBUS PA devices connected to PMD controller through Pepperl and Fuchs DP/PA link.



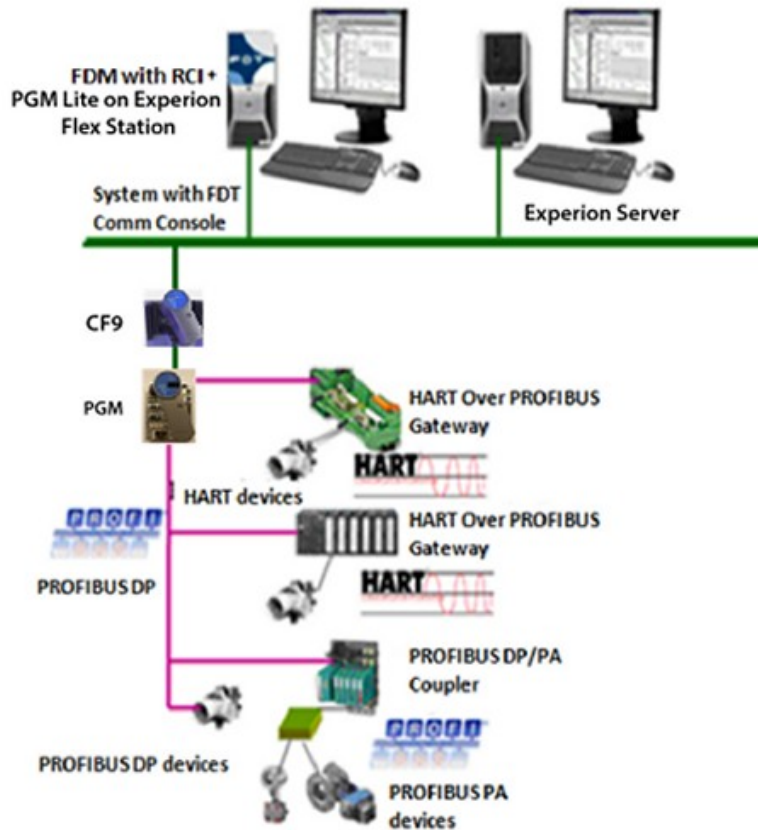
Configuring PMD in FDM

Perform the following steps.

1. Configure all the DP slaves connected to PMD controller in multi drop from the PMD builder and download into the PMD controller.
2. Install the PMD Comm DTM provided by the vendor in the RCI machine to perform the PMD configuration in FDM.
3. Add the PMD Comm DTM to FDM DTM library. For more information, refer to section [“Updating the DTM library”](#).
4. Open the FDT Comm Console in the RCI machine where PMD Comm DTM is installed.
5. Right-click COMM DTM Interface and then click Add device. The PMD Comm DTM is added in the FDT Comm Console hierarchy.
6. Right-click the PMD node and then click Open Configuration. The Configuration page appears.
7. Click the Configuration tab and select the check box for the required devices and click OK.
8. Make the PMD Comm DTM Online and scan for the devices.
9. The communication DTM detects devices present in the network. The Dtm Assignment dialog appears with the list of available DTMs for all the detected devices. Select the Suggested DTM or if you want to change DTM, click the Assign DTM button. The DTM Selection Dialog appears. Select the necessary DTM and then click OK.
10. Click OK in the Dtm Assignment dialog box. As the Pepperl and Fuchs DP/PA link acts as a transparent link, it is not detected when the network is scanned, instead the PA devices are detected directly under the Communication DTM in network hierarchy.

14.3.3 Configuring PROFIBUS Gateway Module in FDM

The PROFIBUS Gateway Module provides a common module platform to support the interface to the PROFIBUS DP and the C300 Controller. The PGM is developed in the Series C form factor for use with the C300 Controller. The PGM module is an FTE resident module. You can configure PGM connected devices in FDM using FDT-DTM technology. To support PGM with FDM, the PROFIBUS Gateway (Lite) Communication DTM must be installed and configured.



Prerequisites

Ensure that FDM RCI and PROFIBUS Gateway (Lite) communication DTM is installed on Experion Flex Station, where PGM software is installed.

To configure PROFIBUS Gateway (Lite) communication DTM

1. Install the PROFIBUS Gateway (Lite) communication DTM provided by the vendor in the RCI computer. For installing PGM (Lite) communication DTM, download the HonProfiGWDTM.zip from Honeywell Process Solution website and follow the on-screen instructions.
2. After installing PGM (Lite) communication DTM, browse for the XML file Honeywell.Script.xml at the following location, C:\ProgramData\Honeywell\SYCONnet\PROFIBUS\CommMaster_netX. The PGM (Lite) communication DTM uses this XML scripting for Master specific identifications definitions.
3. In the Honeywell.Script.xml file, change the timeout value to "15000" for the following elements.

```
<Component name=" " >"TimeoutSettings" version="1.0">
```

```
<Properties>
```

```
<StringProperty name="LifeListTimeout" value="45000"/>
```

```

<StringProperty name="ExtendedDiagTimeout" value="5000"/>

<StringProperty name="FirmwareDiagTimeout" value="1000"/>

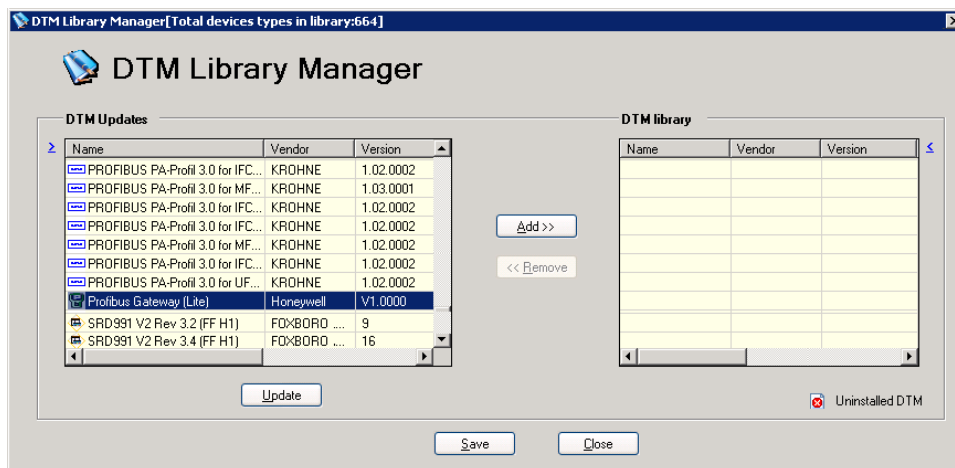
<StringProperty name="DPV1ReadWriteTimeout" value="5000"/>

</Properties>

</Component>

```

4. Configure the COMM DTM Interface in the FDM Server Management tool. For more information about configuring the COMM DTM Interface, refer to the section [“Configuring Comm DTM network in FDM” on page 66](#).
5. Open the FDT Comm Console in the RCI computer where PROFIBUS Gateway (Lite) communication DTM is installed and update the DTM library. For more information about updating the DTM library, refer to the section [“Updating the DTM library”](#).
6. The DTM Library Manager is scanned for all the DTMs in the RCI computer and you can view the PROFIBUS Gateway (Lite) communication DTM in the DTM Updates pane.



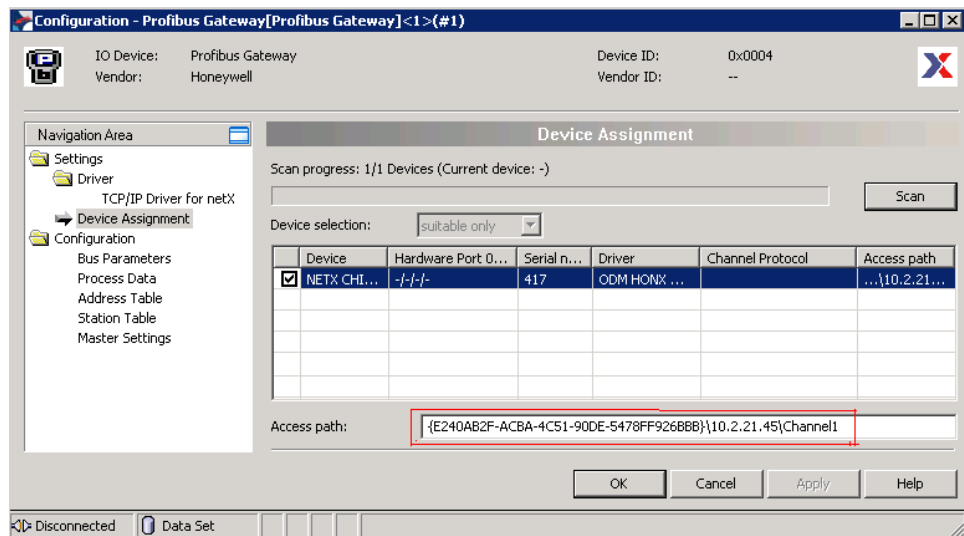
7. Select the PROFIBUS Gateway (Lite) communication DTM and then click Add >>. Now, this DTM is available in the DTM library.
8. Click Save in the DTM Library Manager dialog box. A confirmation message appears displaying DTM library is updated.

NOTE

After the DTM library update, you must restart the FDT Comm Console.

9. Open the FDT Comm Console, right-click COMM DTM Interface and then click Add device from the network view. The DTM Selection Dialog appears with the list of all the available DTMs.
10. Select the PROFIBUS Gateway (Lite) communication DTM and then click OK. The PROFIBUS Gateway (Lite) communication DTM is added in the FDT Comm Console hierarchy.
11. Right-click the PROFIBUS Gateway (Lite) communication DTM and then click Open Configuration. The Configuration page appears.

12. In DTM Start Page, under Settings> Device Assignment, you must copy the access path from the Control Builder and then paste it in the Access path box. To get the access path from the Control Builder, perform the following steps.
 - a. In Control Builder, click PBLINK from Project-Assignment tree. The PBLink configuration form appears.
 - b. Click the Field Network Configuration tab. The Network view is displayed.
 - c. Right-click the device in the Network view and then click Configuration. The configuration form of the specific device appears.
 - d. Click Settings > Device Assignment in the Navigation Area. The Device Assignment page appears in the right-pane.
 - e. Click Scan. This reads the information from the hardware through the network. After the scan is complete, the device information such as the chip type, the serial number, and the access path is displayed.



- f. Copy this access path and paste it in the Access path box in the Device Assignment page of the FDT Comm Console.
13. Click OK in the DTM Start Page. A confirmation message appears and click Yes to accept the access path.
14. Click Apply in the DTM Start Page.
15. Right-click the PROFIBUS Gateway (Lite) communication DTM and then click Go Online to make it online.
16. Right-click the PROFIBUS Gateway (Lite) communication DTM and then click Scan for Devices. The Channel Selection Dialog appears.
17. Select the required channels or select All and then click OK. The ScanStatus message appears displaying the progress of the scan. After scanning, the Dtm Assignment dialog box appears. The devices are detected and listed in the Dtm Assignment dialog box.
18. Select the Suggested DTM, or if you want to assign the different DTM, click Assign DTM. The DTM Selection Dialog appears. Select the necessary DTM and then click OK.

19. Click OK in the Dtm Assignment dialog box. The discovered devices/gateway are displayed in the Network View.

NOTE

After configuring PROFIBUS Gateway (Lite) communication DTM, you can load only one device (with DD/ DTM) per gateway in FDM Client/FDT Comm Console when HART Over PROFIBUS is configured for gateway.

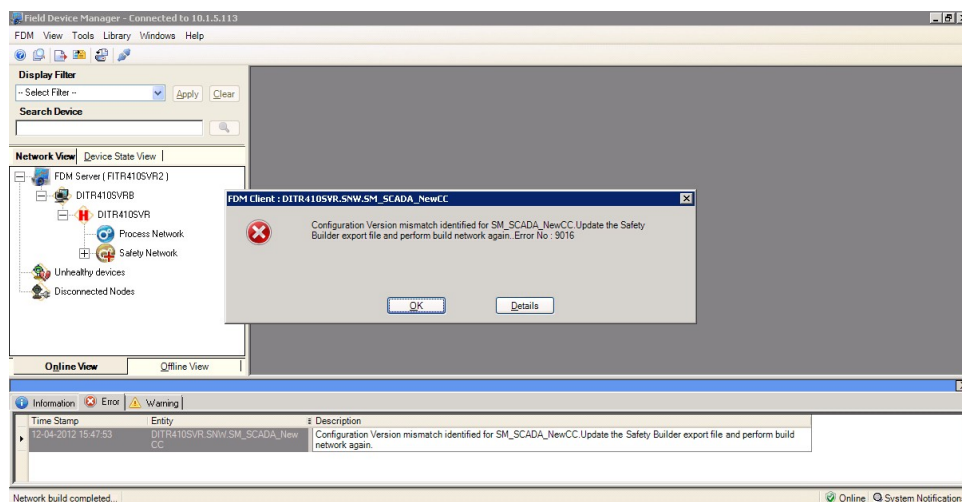
14.4 Building Safety networks

You can build the safety network in the following ways.

- If the standalone Safety network is configured, then you can perform build network at network level, SM controller level, and IOTA (Universal Safe Modules) level.
- If the Experion-integrated Safety Network is configured, then you can perform the build network at network level and at group level (Process and Safety network level). And also, you can perform build network at SM controller level, IOTA (Universal Safe Modules) level.
- For more information about building Experion-integrated Safety network, refer to the section [“Building Experion networks”](#).

Prerequisites

When you export configuration file from Safety Builder, there is an element called controller version in XML file. This controller version should exactly match with version in the actual firmware of the controller. If they do not match, FDM does not perform build network operation and displays the configuration mismatch error message in the Error tab as follows.



To resolve this issue, you need to generate the new SB Export file with proper configuration information and update in FDM. Then, perform the build network.

To build the standalone Safety network

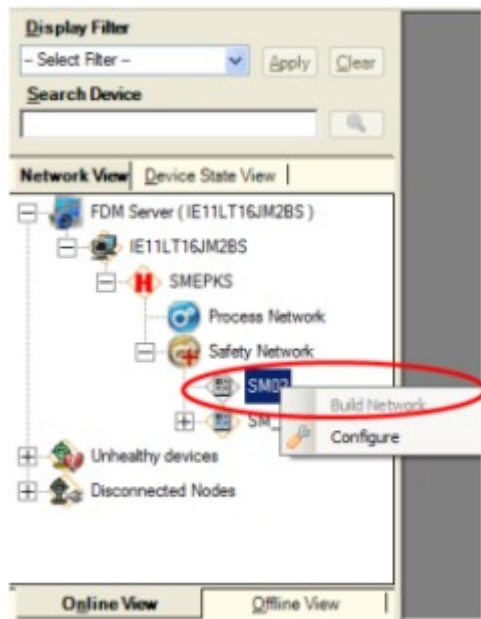
1. From the Network View under Online view, expand FDM Server network tree. The list of network interfaces appears.
2. Perform any one of the following to build Standalone Safety network.
 - Right-click the standalone network interface and then click Build Network. FDM detects the SM controllers, IOTAs and HART channels connected to the network and displays them in the tree view.

- Right-click the SM controller and then click Build Network. FDM detects the IOTAs and HART channels connected to the network and displays them in the tree view.
- Right-click the IOTA and then click Build Network. FDM detects the HART channels connected to the network and displays them in the tree view.

14.4.1 SM network redundancy handling in FDM

The redundant SM has two Control Processors, CP1 and CP2. Control Processor (CP) has different states that are Running, Idle, and Unknown.

When both the CPs are in Idle state, only SM is shown in network with “grayed out” icon and you cannot perform build network on it.

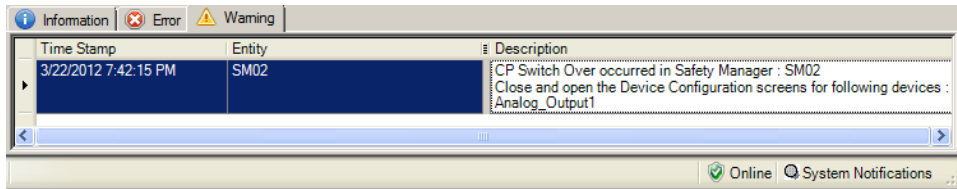


- The network communication is available when any one of the CPs or both the CPs are in running state.
- If one of the CPs state is changing from Running to Idle/Unknown and vice-versa, then Network View is not impacted due to the CP switchover.
- If both the CPs are in Idle state or if one of the CP is in Unknown and other CP is in Idle state, then, only SM is displayed in the network. But, there is no communication with IOTAs and devices from FDM.
- If both the CPs are in Unknown state, then it does not display SM(s) in Network View.

The following notifications appear in System Notification pane under Warning tab for the above scenarios during CP switchover.

Information Error Warning		
Time Stamp	Entity	Description
3/22/2012 7:27:37 PM	SMEPKS.SNw.SM02	Communication loss for SM02 CP(s) are in Idle state.
3/22/2012 7:27:44 PM	SMEPKS.SNw.SM02	Communication loss for SM02. At least one of the CPs is in unknown state and other in idle state.
3/22/2012 7:27:55 PM	SMEPKS.SNw.SM02	Communication loss for SM02 CP(s) are in unknown state.
3/22/2012 7:28:04 PM	SMEPKS.SNw.SM02	Communication loss for SM02. At least one of the CPs is in unknown state and other in idle state.
3/22/2012 7:28:10 PM	SMEPKS.SNw.SM02	Communication loss for SM02 CP(s) are in Idle state.
3/22/2012 7:28:17 PM	SMEPKS.SNw.SM02	Communication loss for SM02. At least one of the CPs is in unknown state and other in idle state.

If CP switchover occurs during device configuration, the warning message appears in System Notifications pane under Warning tab as follows:



To avoid communication error and timeout error, close the device configuration page and retry the operation. For more information about CP switchover behavior, refer to the FDM Troubleshooting Guide.

14.5 Building OneWireless networks

You can build the OneWireless network in the following ways.

- If the standalone OneWireless network is configured, then you can perform build network at network level and WDM level.
- If the Experion-integrated OneWireless network is configured, then you can perform the build network at network level and at process group level only if Safety Manager is available. Otherwise, you can perform the build network at network level and WDM level.

For more information about building Experion-integrated OneWireless network, refer to the section [“Building Experion networks”](#).

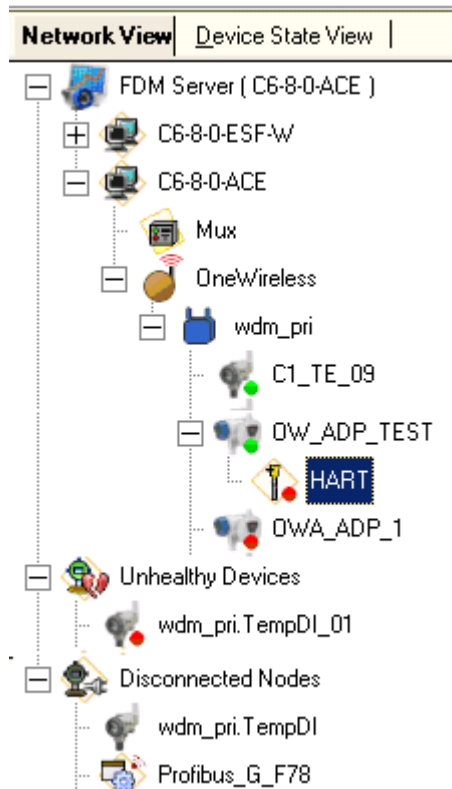
Prerequisites

- Ensure that WDM, ISA100 Wireless, and Wireless HART devices are commissioned in OneWireless User Interface.
- Ensure that GCI and HART-IP interface are enabled on WDM.
- Ensure that OneWireless network is configured in the FDM Server Management Tool.

To build the standalone OneWireless networks

1. From the Network View under Online view, expand FDM Server network tree. The list of network interfaces appears.
2. Perform any one of the following to build the OneWireless network.
 - Right-click the OneWireless network interface and then click Build Network. FDM detects the WDMs, ISA100 Wireless devices, and HART devices connected to the network and displays them in the tree view.

- Right-click the WDM and then click Build Network. FDM detects the ISA100 Wireless devices, Wireless HART, and HART devices connected to the network through OneWireless adapter and displays them in the tree view.



- FDM uses the GCI and HART interfaces of WDM to communicate to ISA100 Wireless, Wireless HART, and HART devices. If both the interfaces are not enabled on WDM, then:
 - The devices under WDM (HART and ISA100 Wireless) are not discovered in the FDM network view.
 - The devices are moved to Disconnected Nodes list, if they are already discovered.
- If HART device is disconnected and its OneWireless adapter is still connected, then the HART device is moved to Disconnected Nodes list. However, if OneWireless adapter is disconnected, then both OneWireless adapter and HART devices are moved to Disconnected Nodes list.
- Each OneWireless adapter is connected to only one HART device though a Wireless HART Adapter can have multiple HART devices connected to it.

14.6 Building Experion networks

You can build Experion networks in the following ways.

- If the Experion network is configured (without Safety Manager and OneWireless), then you can perform the build network at network level. Controllers like C300, C200, UOC will appear as a part of build network.
- If the Experion network is configured with Safety Manager, then you can perform the build network at network level and at group level (Process and Safety network level). And also, you can perform the build network at SM controller level, IOTA (Universal Safe Modules) level.

- If the Experion network is configured with OneWireless (with Safety Manager), then you can perform the build network at network level and at process group level. And also, you can perform the build network at WDM level.
- If the Experion network is configured with OneWireless (without Safety Manager), then you can perform the build network at network level and at WDM level.

Prerequisites

For Experion network (without Safety Manager and OneWireless)

- Ensure that the Experion network is configured in the FDM Server Management tool.

For Experion-integrated Safety network

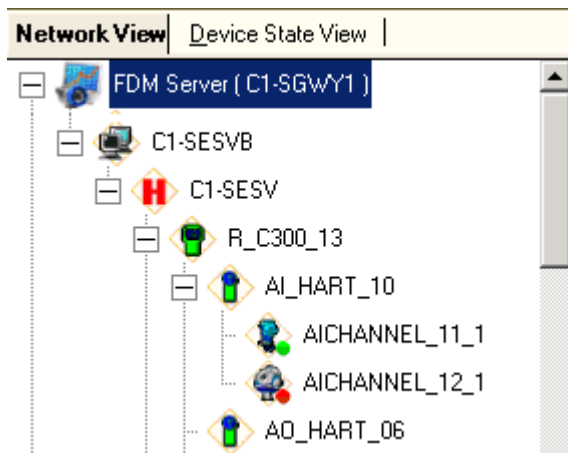
- Ensure that the controller version in the XML file and the version in the actual firmware of the controller are identical when you export the configuration file from Safety Builder.
- Ensure that the Experion-integrated Safety network is configured in the FDM Server Management tool.

For Experion-integrated OneWireless network

- Ensure that WDM, ISA100 Wireless devices, and Wireless HART are commissioned in OneWireless User Interface.
- Ensure that GCI and HART-IP interfaces are enabled on WDM.
- Ensure that the Experion-integrated OneWireless network is configured in the FDM Server Management tool.

To build the Experion networks without SM and OneWireless

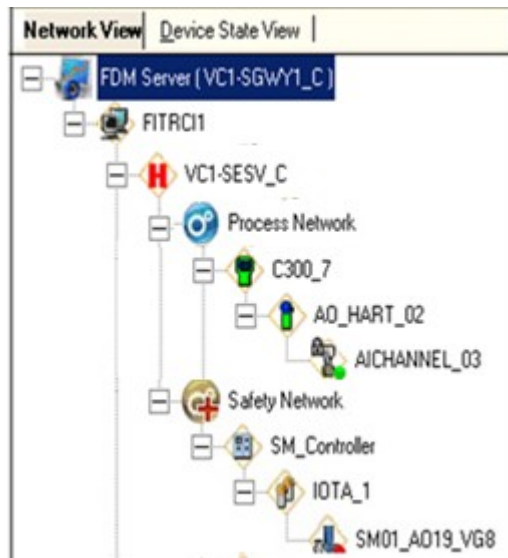
1. From the Network View under Online view, expand FDM Server network tree. The list of network interfaces appears.
2. Right-click the Experion network interface and then click Build Network. FDM detects the Experion controllers, IOs, FIM, links and devices connected to the Experion Server and displays them in the network view.



To build the Experion-integrated Safety network

1. From the Network View under Online view, expand FDM Server network tree.
2. The list of network interfaces displays with both Process and Safety network groups.
3. Perform any one of the following to build Experion integrated Safety network.
 - Right-click the Experion network interface and then click Build Network. FDM detects all devices connected to SM and Experion and displays them in the tree view.

- After SM controller is discovered, right-click the SM controller and then click Build Network. FDM detects the IOTAs and HART channels connected to the network and displays them in the tree view.
- Right-click the Process group and then click Build Network. FDM detects all devices connected to the Experion network and displays them in the tree view.
- Right-click the Safety group and then click Build Network. FDM detects all SM controllers, IOTAs, and HART channels connected to the Safety network and displays them in the tree view.
- After SM controller is discovered, right-click the IOTA and then click Build Network. FDM detects the HART channels connected to the network and displays them in the tree view.

**NOTE**

When the Build Network operation is initiated on the Safety Network from FDM, you might see few devices than actual devices or devices might not appear. This issue is observed when the HART devices and USIOs (configured in SB) are disconnected and connected back to Safety Manager. To detect these HART devices and USIOs dynamically in FDM, turn the Fault Reset key on Safety Manager and check for defined diagnostic messages on Safety Manager. For more details about diagnostic messages on Safety Manager, refer to Safety Builder User's Guide.

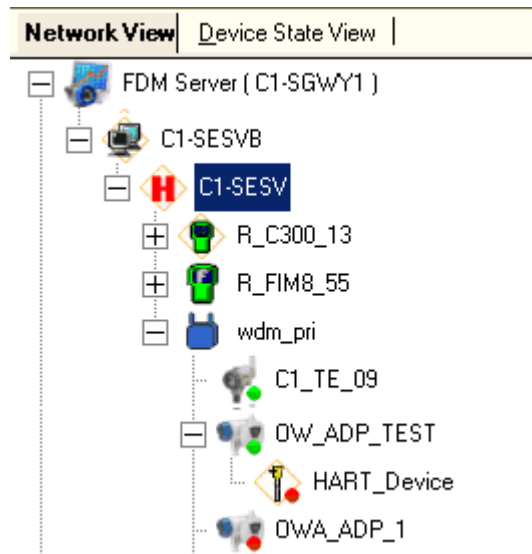
To build the Experion-integrated OneWireless network

1. From the Network View under Online view, expand FDM Server network tree. The list of network interfaces appears.
2. Perform any one of the following to build Experion-integrated OneWireless network.
 - Right-click the network interface and then click Build Network. FDM detects the WDMs, ISA100 Wireless devices, and Wireless HART, and HART devices connected to the OneWireless adapter and displays them in the tree view.

NOTE

If the Experion network is configured with SM and OneWireless, then perform the build network at process group level to detect the OneWireless network connected devices.

- Right-click the WDM and then click Build Network. FDM detects the ISA100 Wireless devices, Wireless HART, and HART devices connected to the network through OneWireless/Wireless HART adapter and displays them in the tree view.



- FDM uses the GCI and HART interfaces of WDM to communicate to ISA100 Wireless, Wireless HART, and HART devices. If both the interfaces are not enabled on WDM, then:
 - The devices under WDM (HART and ISA100 Wireless) are not discovered in the FDM network view.
 - The devices are moved to Disconnected Nodes list, if they are already discovered.
- If HART device is disconnected and its OneWireless adapter is still connected, then the HART device is moved to Disconnected Nodes list. However, if OneWireless adapter is disconnected, then both OneWireless adapter and HART devices are moved to Disconnected Nodes list.
- Each OneWireless adapter is connected to only one HART device though a Wireless HART Adapter can have multiple HART devices connected to it.

14.7 Building HART-IP networks

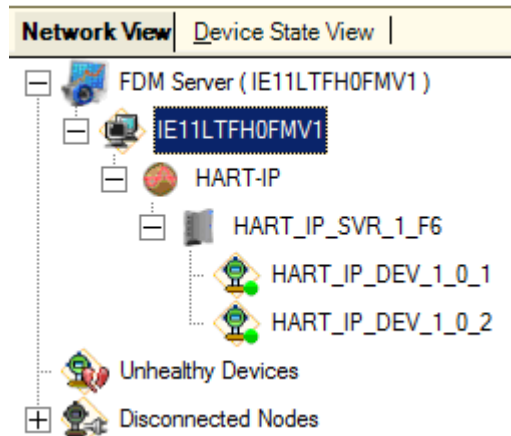
Prerequisites

Ensure that HART-IP network is configured in the FDM Server Management tool.

To build the HART-IP networks

1. From the Network View under Online view, expand FDM Server network tree. The list of network interfaces appears.
2. Perform any one of the following to build the HART-IP network.
 - Right-click the HART-IP network interface and then click Build Network. FDM detects the HART devices connected to the network and are displayed in the network view.

- You can also build a network by right-clicking the HART-IP gateway and then clicking Build Network. FDM detects the HART devices connected to the network and are displayed in the network view.



14.8 Building Honeywell ControlEdge RTU

Prerequisites

- Ensure that RTU and ISA100 Wireless devices are commissioned in ControlEdge RTU User Interface.
- Ensure that GCI and HART-IP interface are enabled on ControlEdge RTU.
- Ensure that ControlEdge RTU network is configured in the FDM Server Management Tool.

To build the ControlEdge RTU networks:

- From the Network View under Online view, expand FDM Server network tree. The list of network interfaces appears.
- Perform any one of the following to build the ControlEdge RTU network.
 - Right-click the RTU network interface and then click Build Network. FDM detects the RTUs, ISA100 Wireless devices, and HART devices connected to the network and displays them in the tree view.
 - Right-click the RTU and then click Build Network. FDM detects the ISA100 Wireless devices and HART devices connected to the network through on-board and expansion IOs and displays them in the tree view.

FDM uses the GCI and HART interfaces of ControlEdge RTU to communicate to ISA100 Wireless and HART devices. If both the interfaces are not enabled on ControlEdge RTU, then:

- The devices under RTU (HART and ISA100 Wireless) are not discovered in the FDM network view.
- The devices are moved to Disconnected Nodes list, if they are already discovered.

14.9 Building Honeywell ControlEdge PLC/HC900

Prerequisites

Ensure that ControlEdge PLC/HC900 network is configured in the FDM Server Management tool.

To build the ControlEdge PLC/HC900 networks:

1. From the Network View under Online view, expand FDM Server network tree. The list of network interfaces appears.
2. Right-click the PLC network interface and then click Build Network. FDM detects the ControlEdge PLC/HC900 and devices connected to it and are displayed in the network view.

14.10 Building TPS networks

FDM uses the TPS Documentation Tool (DocTool) application, which is on the ES-T node to discover the DE channels configured in TPS system. FDM initiates the DocTool query on a specified ES-T node (Engineering Station) and uses the output file results (which is stored on the History Module node) to build the network hierarchy of DE Devices. Using the build network operation, FDM discovers the “online” network hierarchy of DE devices and their parent modules like UCNs, HPMs, and STIM IOPs.

During the build network operation, when FDM executes the DocTool query, the total load on ES-T might be more than 70% for a time period of 1 to 2 minutes. Hence, it is recommended to use an Engineering Station (ES-T) address for DocTool query, instead of User Station (ES-T) address in FDM.

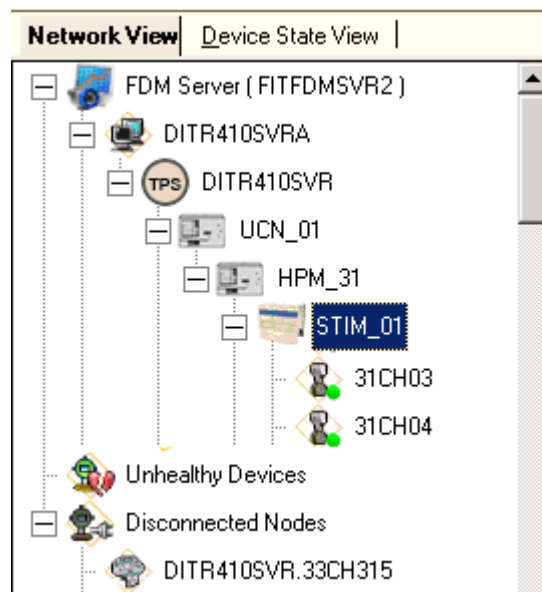
Prerequisites

- Ensure that you provide the address of ES-T node that runs the DocTool query is provided during network configuration in FDM.
- Ensure that the availability of the CPU Free percentage (percentage of CPU available for loading) is minimum 80% on ES-T before initiating the build network operation. Here, the CPU Free parameter is an environment parameter that reads the CPU Free percentage.

To build the TPS network

1. From the Network View under Online view, expand the FDM Server network tree. The list of network interfaces appear.
2. Perform the following to build the TPS network.
 - Right-click TPS network interface and then click Build Network. FDM detect UCNs, HPMs, STIMs, and DE devices connected to the network and displays them in the tree view.
 - Right-click UCN and then click Build Network. FDM detect HPMs, STIMs, and DE devices connected to UCN and displays them in the tree view.
 - Right-click HPM and then click Build Network. FDM detect STIMs and DE devices connected to HPM and displays them in the tree view.

- Right-click STIM and then click Build Network. FDM detect DE devices connected to STIM and displays them in the tree view.



After building the TPS network, the following DE network hierarchy is displayed in the Network View.

NOTE

TPS Network Name (RCI Name) > UCN <Number>>HPM <Number> >STIM <SlotNumber> >DE devices.

- During the Build Network operation, do not update any system configuration settings (example, NIM PARSEC Limit value).
- During the Build Network operation, due to the load on station (ES-T node) from the DocTool query execution, you might experience some delay while updating the parameter values on that station display/trends for one or two seconds.
- If any new DE channel/point is added in TPN, you must perform the manual build network operation at respective parent level, to discover the newly added DE channel/point in FDM.
- When an UCN/HPM/STIM IOP is disconnected from the network, all the devices connected to the UCN/HPM/STIM IOP are still available in the network.
- FDM does not detect the Controller, IO card (STIMv), and DE devices configured with Remote NIM configuration when you perform the Build Network operation.
- For SMV (multi variable device) device type, the tooltip does not show actual device type. Perform the Build Network operation at STIM level to display the actual device type.

14.11 Soft resetting a multiplexer

When you remove and replace the devices that are connected to a hardware multiplexer, invalid device status may appear on the multiplexer device status page. The soft reset feature, using the Reset & Build Network option, facilitates resetting the multiplexer internally and removes the invalid device status if any, on the multiplexer device status page. Soft resetting a multiplexer also results in the network being rebuilt.

This feature is supported on all hardware multiplexers, which are qualified with FDM. By default, administrators group has privileges to reset a multiplexer. An administrator can provide this privilege to other roles by assigning the Reset and Build network privilege to the required roles. For more information about assigning the privileges to roles, refer to the section [“User management”](#).

To reset a multiplexer

1. From the Network View under Online View, expand FDM Server network tree. A list of network interface appears.
2. Stop all other operations on the required multiplexer network in FDM before performing the reset and build network operation.
3. Right-click the required multiplexer network and then click Reset & Build Network on the shortcut menu. FDM resets the multiplexer and rebuilds the network automatically. You can also view status of the operation in the System Notifications pane.

NOTE

When multiplexers are connected in Multi Master/Daisy chain topology, and if reset operation is performed on one multiplexer, then diagnostic alarm is removed on all the multiplexers. These alarms are viewed on the Device Status page in FDM.

DEVICE ACCESS CONTROL

Device lock is a feature used for locking devices from being accessed by multiple users.

When a DE device or a device loaded with DD is locked, the device is in read-only mode. This means that the user can view the device configuration but cannot modify it. When a device loaded with DTM is locked, you cannot open the device configuration page.

The following table summarizes the appearance of icons for each lock state.

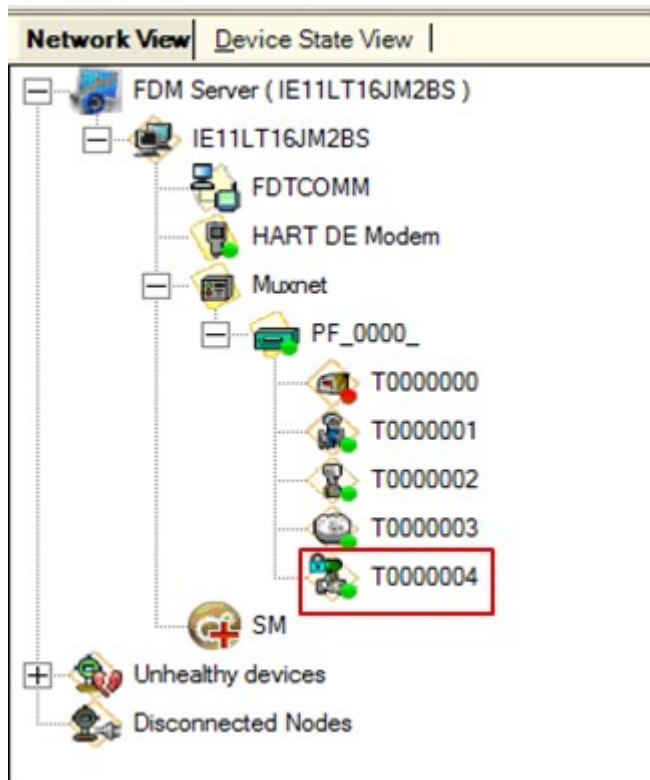
Lock state	Icon
Explicit lock	
Implicit lock/Safety lock	
Exclusive access lock	

15.1 Explicit locking

FDM allows you to lock or unlock a device manually, when required. When a device is explicitly locked, users cannot modify the device configuration, not even the user who locked it.

To lock the device explicitly

1. Select the device tag from the Online View > Network View tree.
2. Right-click the device and then click Lock. The lock icon appears for the device in the Network View as follows:



3. Subsequently, when you select Device Configuration, the lock  appears on the upper-right corner of the window. The lock status can also be viewed by selecting QuickView from the context menu of the device. If you want to lock all devices simultaneously, right-click the network and then click Lock All. If the Prompt User for Device Unlock Password feature is enabled, then you are prompted to enter the password.

15.2 Implicit locking

NOTE

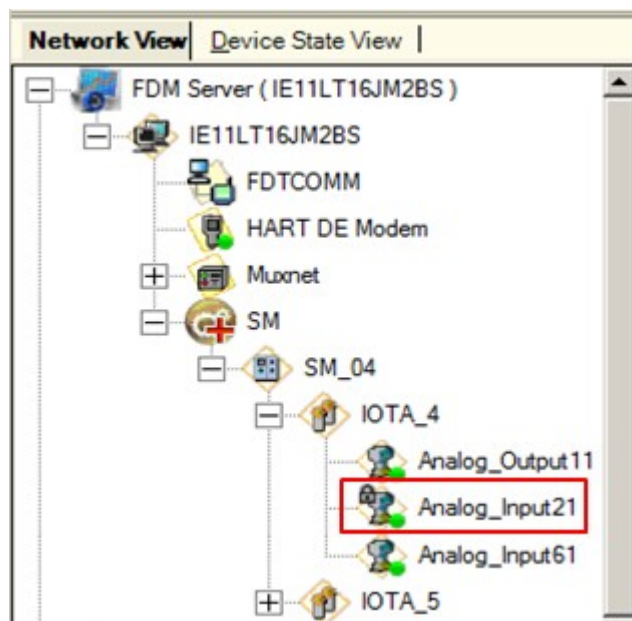
Implicit lock cannot be removed by performing an explicit unlock on the device and the system continues to display the Implicit lock icon on the upper-right corner of the window.

- FDM tool provides implicit access locking of device when more than one user accesses the same device concurrently. When the first user accesses the device, the device is locked for all subsequent users, and are provided read-only access. In addition, there is a lock icon displayed the upper-right corner of the device configuration page to indicate that another user has already opened the selected device.
- Process Lock: When devices are connected through Experion, devices that are in process are implicitly locked. And also, when DE devices are connected through the TPS network interface, it is considered as Process Locked, if the point execution state (PTEXECST) is ACTIVE. A process locked device provides read-only view of DE parameters and device parameters

cannot be changed from FDM. To edit any DE device parameter, you must change the PTEXECST value to INACTIVE in the Native Window application on ES-T. For more information on the Native Window application, refer to the Integrated Experion-TPS User's Guide in the TPN/TPS bookset.

NOTE

- When FDM is connected to the field devices through the Experion interface through the PM HART IO or the Series C I/O module, devices that are in process are locked by default. To edit any device parameter or run a method, you need to inactivate the device.
 - When FDM is connected to field devices through the Experion interface through the 1756 HART IO module, the channel mode needs to be changed to 'OFF CONTROL'.
 - Process locked devices can also be unlocked by enabling the setting "Allow Write Access for Process Active Devices" with administrator privileges.
- Safety Lock is a lock initiated by Safety System to prohibit any configuration of Safety Devices from FDM. Safety Lock/Unlock happens at Safety Builder and the device lock state is modified accordingly in FDM Network View for that device. And also, to see the lock status, right-click the device and then click QuickView from the shortcut menu.



Subsequently, when you open Device Configuration page, the lock  icon appears on the upper-right corner of the window.

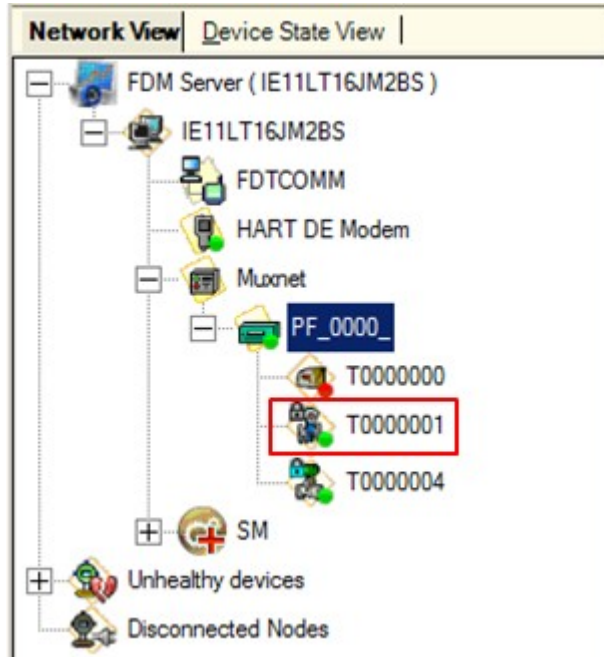
Devices connected to SM controllers have a safety lock by default. You can load those devices in read-only mode only with the DD. You cannot open the device configuration pages with DTM for safety locked devices.

- FHM Lock: when a device is in use by FDM HART Multiplexer, the device is locked and not available for use elsewhere in FDM. This is termed as an FHM lock in FDM. Ensure to consider the following while using FHM.
 - When the device is explicitly locked, it cannot be used with FHM.

- When a device is used by one instance of FHM it cannot be used by FHM on another client.
- When a device has an exclusive lock on it, only the FHM on the client that has received exclusive access can use it.

The following is the example scenario for Implicit Locking when multiple users access the same device.

1. User A accesses a device to perform a necessary task.
2. When the User B tries to access the same device, the lock icon appears for the device in Network View as follows:



Subsequently, when you select Device Configuration, the lock  icon appears on the upper-right corner of the window.

And also, to see the lock status, right-click the device and then click QuickView from the shortcut menu. When locked, you can only view the device data, but cannot edit them.

3. When User A closes the device, a notification message appears to User B of the device in Notifications pane under Information tab. This indicates that the User B can edit the device data.

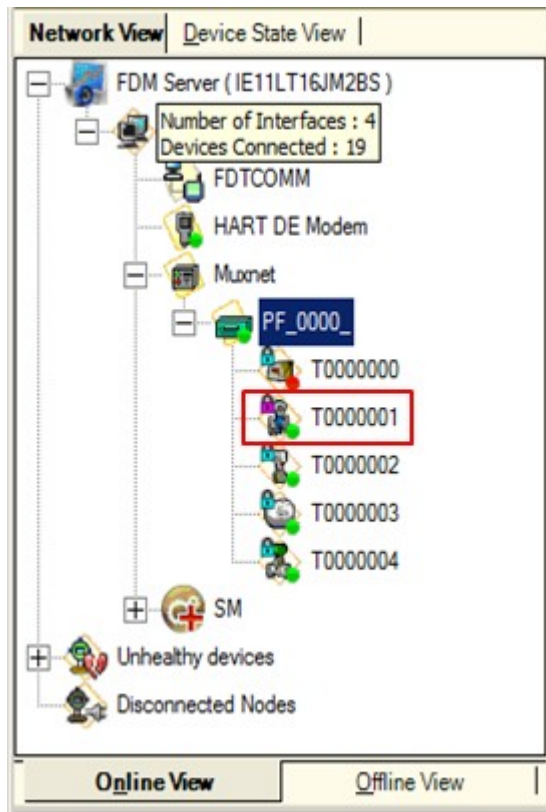
NOTE

If there are more than two users trying to access the device, the access to the device is granted in the order in which the users load the device. For instance, if three users A, B and C try to load the device one after another, the device is locked for B and C when A loads the device. When A unloads the device, the access is granted to B and when B unloads the device, the access is granted to C.

15.3 Exclusive locking

FDM provides the exclusive read/write access to the device which is unlocked in one FDM Client. However, in multi-client scenarios, the same device remains exclusive locked in other clients. The following is the example scenario for Exclusive Locking when two clients are connected to single FDM Server.

1. Open two clients which are connected to single FDM Server.
2. In Client-1, choose FDM > Settings. The Settings dialog box appears.
3. Under Device Lock, select Exclusive Access to Unlocked devices check box.
4. Click Apply and then click OK.
5. In Client-1, right-click the device and then click Unlock from the shortcut menu. If the Prompt User for Device Unlock Password feature is enabled, then you are prompted to enter the password to Unlock the device.
6. A similar device in Client-2 is in Exclusive lock state and lock icon appears for the same device in Network View as follows:



And also, to see the lock status, right-click the device and then click QuickView from the shortcut menu. Subsequently, when you open Device Configuration page, the lock icon appears on the upper-right corner of the window.

For the device which is in Exclusive lock state, you do not have Lock/Unlock option in the shortcut menu. You need to lock the device explicitly in Client-1 (where the device is unlocked exclusively) and then Lock/Unlock option appears in the shortcut menu for the device in Client-2. For more information about how to lock and unlock HART channels connected to Universal Safe Modules, refer to Safety Builder User's Guide

15.4 Unlock a device

You can unlock an explicitly locked device, process active device and FHM locked device.

15.4.1 Unlocking an explicitly locked device

To unlock the device, right-click the device under Network View and click Unlock. A message appears confirming that write-protection is removed on the device in Notifications pane. This process immediately unlocks a device and provides write access to the user even if the device configuration is open. And also, you can unlock an explicitly locked device by clicking Lock icon

from the device configuration page.

15.4.2 Unlocking a process active device

You can unlock process active device by following three ways.

- By enabling Pass Through setting: This is applicable when FDM is connected to the field devices through the Experion interface through the 1756 HART I/O, PM HART I/O module or the Series C I/O module. In such cases, when you access the devices that are in process, the device appears as locked. To edit any device parameter or run a method, you need to inactivate the device or enable the pass through setting in FDM.
- Unlocking device connected through 1756 HART IO: To modify the device configuration when connected through 1756 HART IO, you need to first change the state of the device to off-process. This can be done through the Control Builder in the following two ways.
 - Changing the state of the device block to OFFCONTROL – Refer to the procedure “To change the state of a device connected through 1756 HART IO to off-process”
 - Changing the state of the IO Module to INACTIVE – Refer to the procedure [“To change the state of a device connected through 1756 HART IO to INACTIVE”](#)

NOTE

- If you change the state of the device block to OFFCONTROL, only the specific device becomes inactive.
- If you inactivate the IO Module, all the devices connected to the IO module go off-process.

- Unlocking devices connected through PM HART I/O or Series C: To modify the device configuration when connected through PM HART IO/Series C I/O, you need to first change the state of the device to off-process. This can be done through the Control Builder, in the following two ways.
 - Changing the state of the device block to INACTIVE – Refer to the procedure [“To change the state of a device connected through PM HART IO/Series C I/O to off-process”](#)
 - Changing the state of the IO Module to INACTIVE – Refer to the procedure [“To change the state of a device connected through PM HART I/O/Series C I/O to off-process by changing the state of the IO Module to INACTIVE”](#)

NOTE

- If you inactivate the device block, only the specific device becomes inactive.
- If you change the state of the IO Module to INACTIVE, all the devices connected to the IO module goes off-process.

- Unlocking DE devices connected through TPS network: To modify device configuration when connected through TPS network interface, you need to first change the state of the device parameter, PTEXECST from ACTIVE to INACTIVE. This can be done through the Native Window application on ES-T as given in the [section “To change the state of a device parameter from ACTIVE to INACTIVE, connected through TPS network interface”](#).

To change the state of a device connected through 1756 HART IO to off-process

1. From the Experion Control Builder, select the required device.
2. Right-click the device and then click Configure Module Parameters.
3. On the Main tab, select the value for Normal/Off-Control as OFFCONTROL.

HARTIO:STT25H_0103 Block, STT25H_02 - Parameters [Monitoring]

☐ Show Parameter Names

Execution State: ACTIVE

IOM and Channel Configuration:

IOM Block Name: TC_HAI081_1
 IOM Channel Number: 2

DEVICE BLOCK Assoc. Status: AssocOK

☒ Alarming Enabled

Hart Configuration:

Associated Process Definition:
 Device Location:
 Associated IOM Location:
 Normal/Off-Control: NORMAL
 Passthrough Mode: NORMAL
☐ HART Comm Failure

Warning: When set to OFFCONTROL, the associated channel block will go off control.

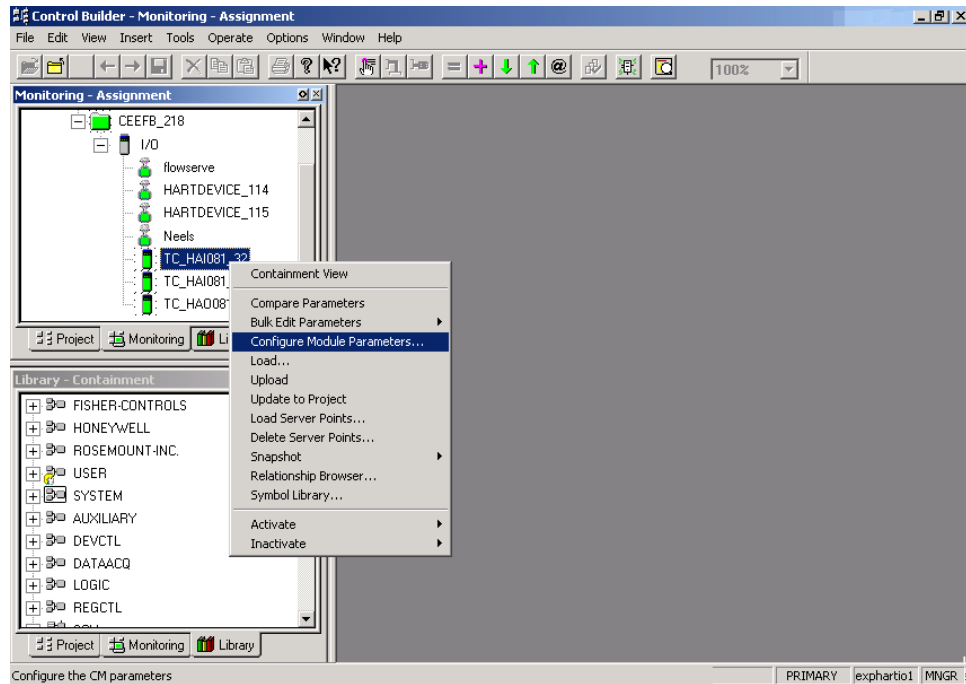
OK Cancel Help

A message appears informing you to change the mode.

4. Click Yes to change the mode. This action brings the device out of process and you can edit the configuration using FDM. A message appears confirming that write-protection is removed on the device.
5. After you finish editing the configuration using the FDM Client, repeat Steps 1 through 3 to restore the device state back to NORMAL.

To change the state of a device connected through 1756 HART IO to INACTIVE

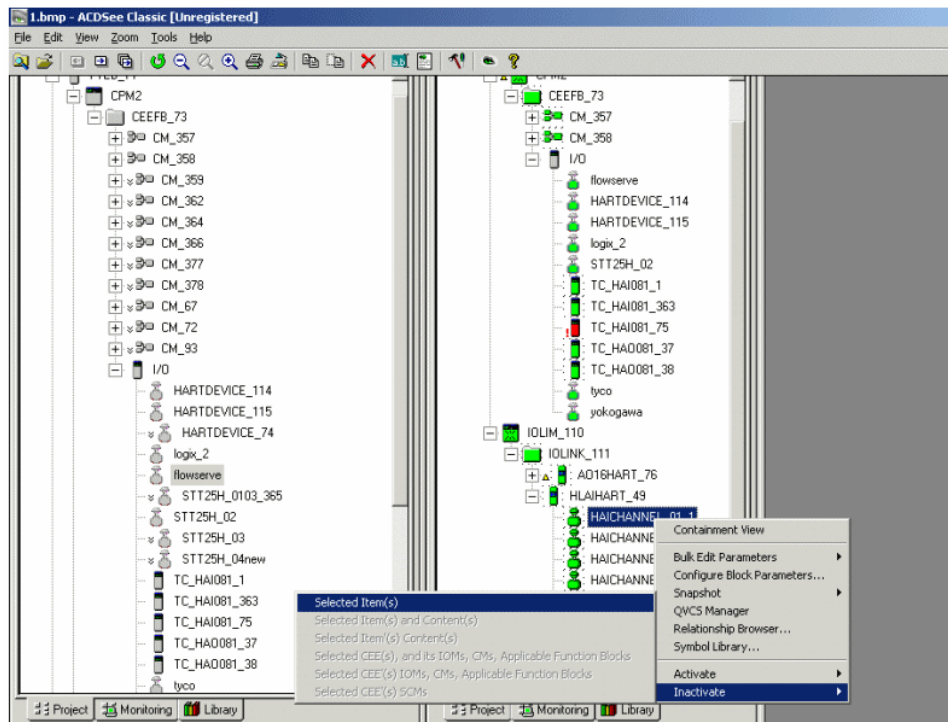
1. From the Experion Control Builder, select the required IO Module.
2. Right-click the IO module and click Configure Module Parameters.



3. Click the Module Configuration tab.
4. In the Execution State drop-down list, click INACTIVATE. A message appears informing you to change the mode.
5. Click Yes to change the state of the device block. This action brings the device off process and you can edit the configuration using FDM. A message appears confirming that write-protection is removed on the device.
6. After you finish editing your configuration using the FDM Client, repeat step 3 to set the value of the field Execution State back to ACTIVE.

To change the state of a device connected through PM HART IO/Series C I/O to off-process

1. From the Experion Control Builder, select the required device.
2. Right-click the device and choose Inactivate > Selected Item(s).

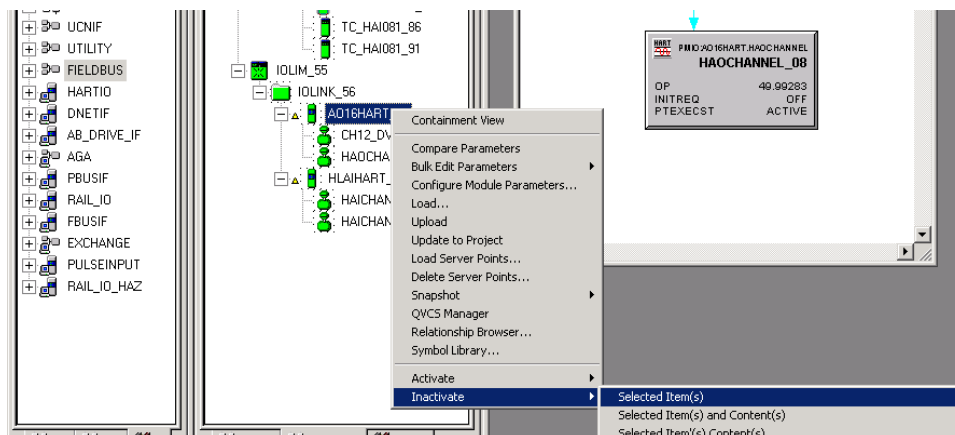


The Change State dialog box appears.

3. Click Yes to make the device block inactive. This action brings the device out of process and you can edit the configuration using FDM. A message appears confirming that write-protection has been removed on the device.
4. After you finish editing the configuration using FDM, in Control Builder, select the device, right-click and choose Activate > Selected Item(s). The Change State dialog box displays the message Set Selected object(s) Active? Click Yes to activate the device block.

To change the state of a device connected through PM HART I/O/Series C I/O to off-process by changing the state of the IO Module to INACTIVE

1. From the Experion Control Builder, select the required IO Module.
2. Right-click the IO module and choose Inactivate > Selected Item(s).

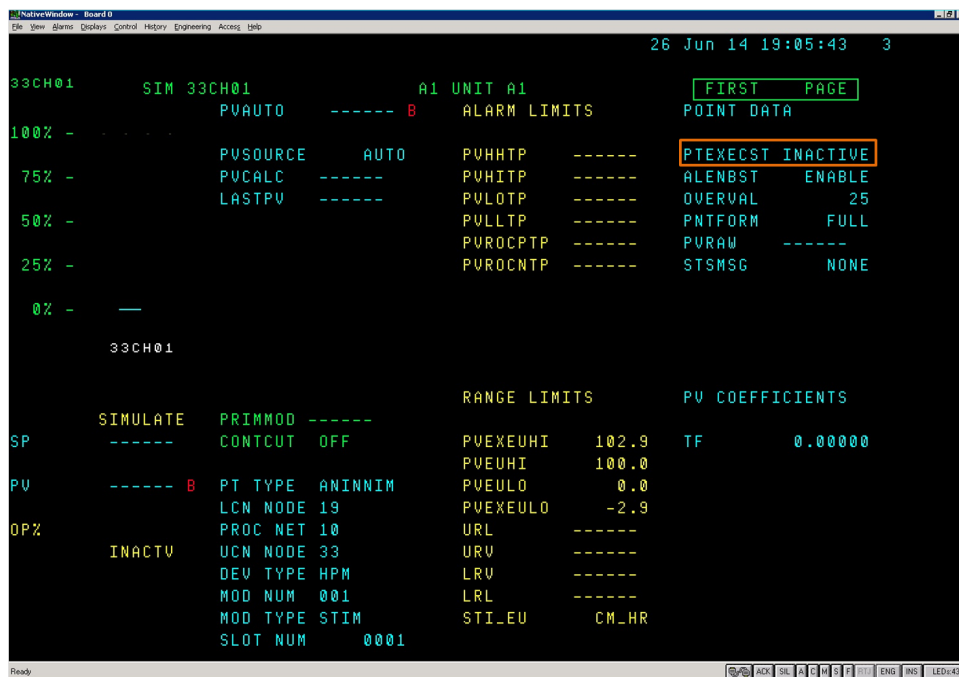


The Change State dialog box appears.

3. Click Yes to change the IO Module to inactive state. This action brings the device out of process and you can edit the configuration using FDM. A message appears confirming that write-protection is removed on the device.
4. After you finish editing the configuration using FDM, in Control Builder, select the device, right-click and choose Activate > Selected Item(s). The Change State dialog box displays the message Set Selected object(s) Active? Click Yes to activate the IO Module.

To change the state of a device parameter from ACTIVE to INACTIVE, connected through TPS network interface

1. In the Native Window application on ES-T node, click Displays > Operating > DETAIL.
2. Type the device tag name in ENTER PT ID box and press Enter to display the Detail display page. The PTEXECST parameter value is displayed as ACTIVE. You can also view the other values for this parameter in the left side of the Detail display page.
3. Select the parameter value as INACTIVE, and press ENTER. The PTEXECST value is changed to INACTIVE as in the following figure and also the device status is changed to INACTIVE in the FDM DE device configuration page.



15.4.3 Unlocking an exclusively locked device

You can unlock the device in the following scenarios.

- When you lock the device explicitly in client using Lock option in shortcut menu.
- When Automatically lock devices Minutes check box is selected in the Settings dialog box.
- When you close the client which is unlocked.
- When devices are disconnected or RCI is down.

15.4.4 Unlocking FHM locked device

To unlock FHM, click Stop button in the FDM HART Multiplexer form. All devices in the FHM list become available to FDM Clients. The third party application connected to FHM is closed and the selected devices will no longer be available for use in the third party application. For more details, refer to the section [“About FDM HART Multiplexer \(FHM\)”](#).

15.5 Lock All/Unlock All

Using this feature, you can lock or unlock all devices that are connected to a network.

- If you want to lock/unlock all devices simultaneously, right-click the network and then click Lock All/ Unlock All. If the Prompt User for Device Unlock Password feature is enabled, then you are prompted to enter the password.

NOTE

- The Lock All/Unlock All feature is a convenience option provided, so that you need not perform individually lock/unlock of devices in the network. There is no explicit lock/unlock state applied to the network when this feature is used. Due to this, it is possible to unlock any device under a network on which you have performed a lock all or lock a device under a network on which you have performed an unlock all.
- The autolock feature is applicable to the devices under a network that are unlocked using the Unlock all feature.
- When device is in Exclusive lock state, if you perform Lock All operation, then it overwrites the Exclusive lock state.
- Unlock All operation (overrides the Exclusive Lock, if there is any) unlock the devices under that Network and provides Read-Write access to all the Clients.

15.6 Dynamic Updates to Networks

After the network is built for the first time, FDM automatically discovers any newly connected or disconnected nodes in the network view. The dynamic network update happens for the devices connected to the following networks.

- MUX network
- Experion network
- Safety network
- OneWireless network
- HART-IP network
- Honeywell ControlEdge RTU network
- Honeywell ControlEdge PLC network
- Honeywell TPS network

Dynamic update of TPS network

NOTE

- The dynamic network update happens for TPS network connected DE devices only for the devices that are already discovered from the build network operation. And also, this happens only if the Scan for Devices discovery and Communication every Second setting is enabled under Network Scan for TPS Network Connected Devices in the Settings dialog box. For more information, refer to the section [“Customizing the network settings”](#).
- When the FDM system exceeds the allowed load limit (TPN Server or NIM), the dynamic discovery or dynamic removal of DE devices do not work.

In the following scenarios, devices are discovered automatically in the network view.

- When an existing device is disconnected from the TPS network
- When a device is disconnected and reconnected again

Dynamic update of MUX network

NOTE

The dynamic network update happens for MUX connected devices only if Network Scan for Mux Connected Devices setting is enabled in the Settings dialog box. For more information, refer to the section [“Customizing thenetwork settings”](#).

In the FDM network view, devices are discovered automatically when devices or MUXs are dynamically added or removed from the network. And also, when the devices are commissioned and decommissioned in Experion, automatically reflects in the FDM network view.

In the following scenarios, devices are discovered automatically in the network view.

- When a new device is connected to any MUX
- When the MUXs are disconnected and reconnected again
- When an existing device is disconnected from the MUX

Dynamic update of Experion network

In the FDM network view, devices are discovered automatically when devices, controllers, or FIMs are dynamically added or removed from the network. And also, when the devices are commissioned and decommissioned in Experion, automatically reflects in the FDM network view.

In the following scenarios, devices are discovered automatically in the network view.

- When a new device is connected to any FIM2/FIM4/FIM8 link and commissioned in Experion Control Builder
- When the controller, I/O modules, or FIM modules are disconnected and reconnected again
- When the FIM links are inactivated and activated
- When an existing device is disconnected from the controller/FIM link

Dynamic update of OneWireless network

NOTE

- The dynamic network update happens for OneWireless network connected devices only if Network Scan for OneWireless Network Connected HART Devices setting is enabled in the Settings dialog box. For more information, refer to the section [“Customizing the network settings”](#).
- The devices connected to WDM are dynamically discovered only after the first build network.

In the FDM network view, devices are discovered automatically when ISA 100.11a supported devices are dynamically added or removed from the network. And also, when the devices are commissioned and decommissioned in OneWireless User Interface, automatically reflects in the FDM network view.

In the following scenarios, devices are discovered dynamically in the network view.

- When a new device is connected to WDM, which is commissioned/decommissioned through OneWireless User Interface and device status should be Joined.
- When the WDM modules and WDM-connected devices are disconnected and reconnected again.
- When an existing device is disconnected from the WDM.

Dynamic update of Safety network

In the FDM network view, devices are discovered automatically when SM, IOTA, or devices are dynamically added or removed from the network. And also, when the devices are commissioned and decommissioned in Safety Builder, automatically reflects in the FDM network view.

In the following scenarios, devices are discovered automatically in the network view.

- When a new device is connected to any SM/IOTA
- When the SMs/IOTAs are disconnected and reconnected again
- When an existing device is disconnected from the SM/IOTA

Dynamic update of HART-IP network

The dynamic network update happens for HART-IP connected devices only if Network Scan for HART-IP Network Connected Devices setting is enabled in the Settings dialog box. For more information, refer to the section [“Customizing the network settings”](#).

In the FDM network view, devices are discovered automatically when devices are dynamically added or removed from the network.

In the following scenarios, devices are discovered automatically in the network view.

- When a new device is connected
- When the device is disconnected and reconnected again
- When an existing device is disconnected

Dynamic update of Honeywell ControlEdge RTU network

- The dynamic network update happens for RTU network connected HART devices only if Network Scan for RTU Network Connected HART Devices setting is enabled in the Settings dialog box. However, ISA 100.11a devices are automatically detected regardless of the Network Scan setting. For more information, refer to the section [“Customizing the network settings”](#).
- The devices connected to RTU are dynamically discovered only after the first build network.
- Behavior described for devices below, in context of HART device is applicable to devices connected to both, on-board IO and an expansion IO.
- Any of the Expansion IO(s) connected to RTU appear in FDM network hierarchy only, if at least one device is connected to it.

NOTE

- Disconnection of an expansion IO from the RTU will lead to the corresponding expansion IO and all connected devices to also get disconnected from the FDM network hierarchy.
- Changing address of an expansion IO(already existing in FDM network hierarchy), will lead to existing expansion IO tag to move to disconnected and a new expansion IO tag will appear in FDM network hierarchy, based on new address.

Dynamic update of Honeywell ControlEdge PLC network

- The dynamic network update happens for ControlEdge PLC network connected HART devices only if Network Scan for Honeywell PLC Network Connected Devices setting is enabled in the Settings dialog box. For more information, refer to the section [“Customizing the network settings”](#).
- The devices connected to ControlEdge PLC are dynamically discovered only after the first build network.
- Behavior described for devices below, in context of HART device is applicable to devices connected to both local racks and remote slots.
- Any of the racks and slots connected to ControlEdge PLC appear in FDM network hierarchy only, if at least one device is connected.
- Disconnection of all the devices connected to racks and slots from the ControlEdge PLC will lead to the corresponding rack, slot, and all connected devices to be moved to disconnected nodes.
- Changing address of rack and slot (already existing in FDM network hierarchy), will lead to existing rack and slot tag to move to disconnected and a new rack and slot tag will appear in FDM network hierarchy, based on new address.

In the FDM network view, devices are discovered automatically when devices are dynamically added or removed from the network.

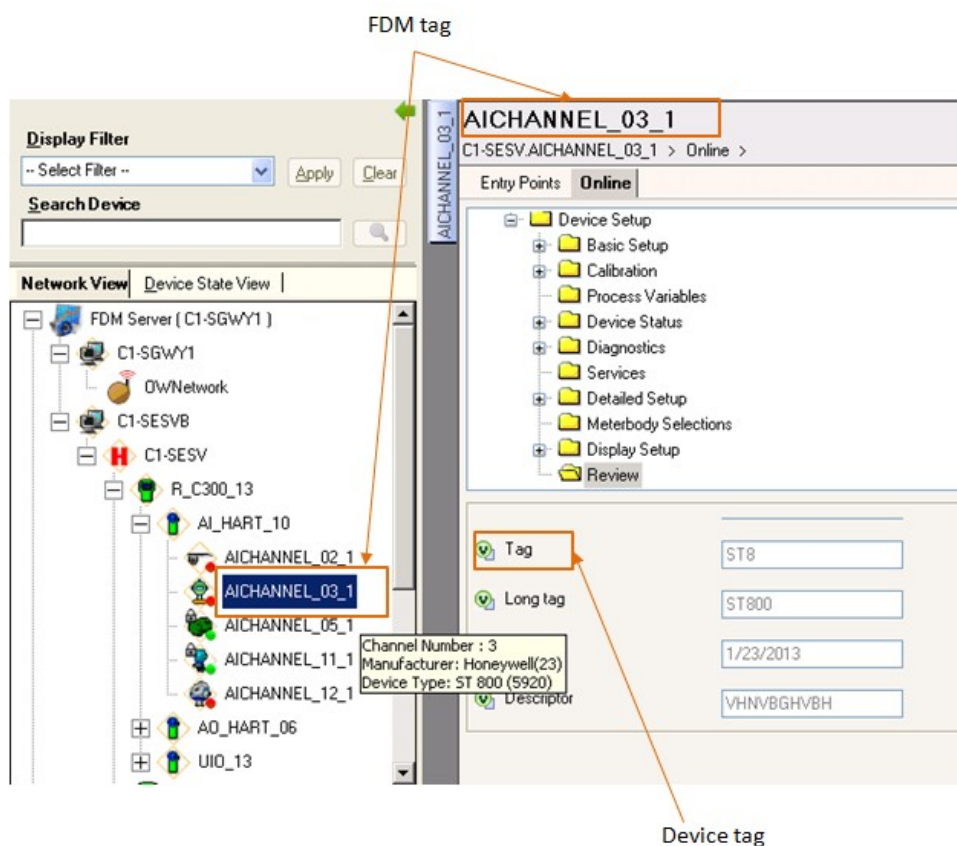
In the following scenarios, devices are discovered automatically in the network view.

- When a new device is connected
- When the device is disconnected and reconnected again.
- When an existing device is disconnected

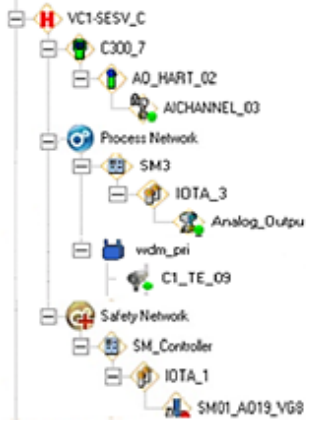
FDM TAGS

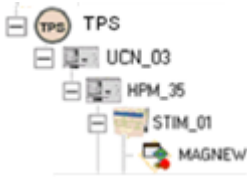
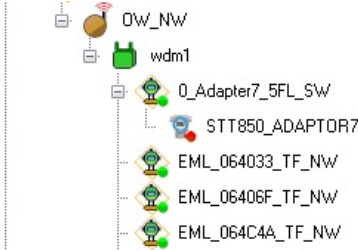
FDM provides each device a unique name to identify the device, which is called FDM tag, appears adjacent to the device icon in the Network View tree. When you browse a network for the first time, the devices are listed under network view with the FDM tags.

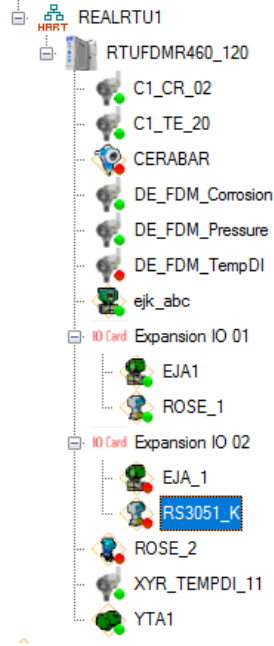
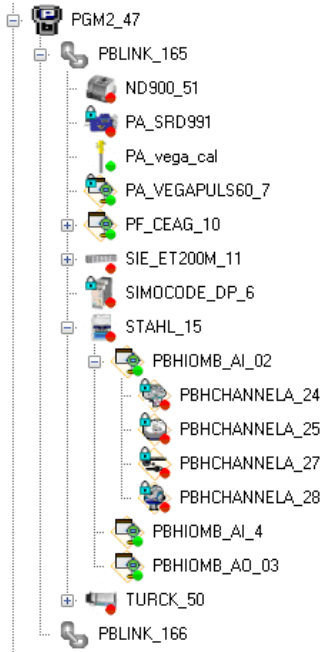
Device Tag indicates the tag as configured in the physical device. After you load a device, the device tag appears as one of the parameters in the device configuration page when you navigate through the entry points for Tag field, as indicated in the below figure.

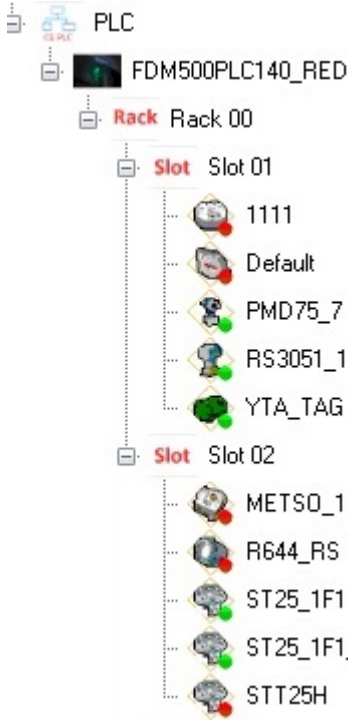


The following illustrates the appearance of tags for each network type.

	FDM Tag Appearance for RS-485 Multiplexer and Modem networks Tag for HART 5 appears as HART tag and for HART 6/7 appears as HART Long tag INVALID tag if no tag for device Tag appended by conflict tag and a number if more than one device with similar tag These tags can be renamed in the Network View through Rename operation. Rename the device tag in the device configuration page
	FDM Tag Appearance for Experion network Alias name appears instead of Network Interface Name. For example: VC1-SESV_C Tag is the same as the tag present in Experion These tags can be renamed using Control Builder
	FDM Tag Appearance for Safety network Tag is the same as the tag present in Safety Builder These tags can be renamed using Safety Builder and requires re-import to reflect the renamed tags in FDM
	FDM Tag Appearance in COMM DTM Interface Tags are automatically generated for devices connected to COMM DTM Interface

	These tags can be renamed in Network View through the Rename operation
	FDM Tag Appearance for HART-IP network Tag is the same as the tag present in the physical device Rename the tag in the FDM Configuration page
	FDM Tag Appearance for Honeywell TPS network Tag is the same as the name configured in the TPS system Rename the tag in the TPS system
	FDM Tag Appearance for OneWireless network Tag is the same as the tag present in OneWireless User interface These tags can be renamed in OneWireless User interface

	FDM Tag Appearance for Honeywell RTU network Tag is the same as the tag present in the device
	FDM Tag Appearance for PGM network Tag is the same as the tag present in Experion

	FDM Tag Appearance for Honeywell PLC network Tag is the same as the tag present in the device

The following table describes source of the tag for each network type.

Network type	Supported protocol type	Source of the tag	Can tags be renamed in FDM?	FDM Tag length
RS-485 Multiplexer and Modem network	HART	As in the physical device	Yes	HART 5 – 16 characters HART 6/7 – 32 characters
Experion network	HART connected to Series C/PMIO/Series 8/ Series C UIO/ Series C UIO -2	Experion	No	40 characters
	Attention The tag length is 16 characters for HART devices connected to 1756 HART I/O.			
	FF	Experion	No	16 characters
	ISA100 Wireless	OneWireless User Interface	No	16 characters
	PROFIBUS DP/PA	PGM	No	40 characters
COMM DTM Interface	HART	As in the physical device	Yes	16 characters
	PROFIBUS	Auto generated by FDM	Yes	16 characters
Safety network	HART	Safety Builder	No	16 characters
OneWireless network	WDM and ISA100 Wireless	OneWireless User Interface	No	ISA100 Wireless – 16 characters

Network type	Supported protocol type	Source of the tag	Can tags be renamed in FDM?	FDM Tag length
	HART devices connected to OneWireless adapter	As in the physical device	Yes	HART 5 – 16 characters HART 6/7 – 32 characters
HART-IP/ Honeywell ControlEdge RTU/ Honeywell ControlEdge PLC network	HART	As in the physical device	Yes	HART 5 – 16 characters HART 6/7 – 32 characters
Honeywell TPS network	DE	TPS system	No	8 characters

16.1 Considerations for FDM tags

For RS-485 Multiplexer and Modem networks

- FDM does not allow you to rename the FDM tag in the following scenarios.
 - When a device is being MUX monitored.
 - When the device configuration page is open for the device.
- When a device is MUX monitored, the tag name remains same across all applications, such as FDM, Control Builder, Experion Station, and Alert Manager.

For Experion networks

- For Experion connected devices, the tags are derived from ERDB (Engineering Repository Database) and these tags can be renamed only using Control Builder.
- You cannot rename an Experion device until it is in disconnected state. If you rename a HART device tag in Experion and reload, FDM will take the renamed tag name.
- From a Multiplexer network, if a device is moved to Experion network, the tag of the device in the Network View appears same as Experion tag. From an Experion network, if a device is moved to any other network (Example: Multiplexer network), the device would use the device tag.
- When a device is monitored for alarms, the tag name remains same across all applications, such as FDM, Control Builder, Experion Station, and Alert Manager.

For Safety network

- When devices connected to Safety network are moved to other network, based on the network type, the tag might be retained in the new network. Example, From Safety network, if a device is moved to Multiplexer network, the device would appear with the same tag as in Safety network. And also, if a device is moved from Safety network to Experion network, the device would appear with the tag as configured in Experion.
- During build network of Safety network, any device tag of Safety network has conflict with the device tag of existing networks (For example, Multiplexer network), Safety network tag is appended with tag conflict. Then, warning message appears in the Warning tab in FDM Client System Notifications pane.

To resolve the tag conflict, rename the device connected to Multiplexer network and then rebuild the network at IOTA level corresponding to the device where conflict is observed.

For OneWireless network

- When the HART devices connected to the OneWireless network are moved to other network, based on the network type, the tag might be retained in the new network. Example, From OneWireless network, if a HART device is moved to Multiplexer network, the device would appear with the same tag as in OneWireless network. And also, if a device is moved from OneWireless network to any Experion HART I/O module connected Experion network, the device would appear with the tag as configured in Experion. For Experion-integrated OneWireless network, if a HART device is moved to WDM-connected to an Experion network, device would appear with the same tag. But, ISA100 Wireless devices connected to the OneWireless network cannot be moved to any other network.

For HART-IP/ Honeywell ControlEdge RTU/ Honeywell ControlEdge PLC networks

FDM does not allow you to rename the FDM tag, when the device configuration page is open for the device.

For Honeywell TPS network

- For TPS connected devices, tags (point names) are configured in the TPS system and you cannot rename those tags in FDM. However, if you rename the tag in TPS system, you must rebuild the network to view the renamed tag in the FDM Network View.

PLANT AREA VIEW

The Plant Area View feature enables you to group the available devices based on their geographical locations. It can be used to represent the virtual grouping of devices as they are grouped in the plant. In addition, this feature allows users to easily identify a device location and to view and monitor the device directly by its location. The device grouping strategy followed in Plant Area View is with reference to ANSI/ISA–88.01–1995 standards.

This feature is also used to:

- View the list of devices mapped to a particular group.
- View the summary of health and connection status using pie charts at various levels (device, group, or plant) in the hierarchy.
- Filter the devices by their health or connection status.
- Locate a device in the FDM Client Network View from the plant area view.

NOTE

Ensure that you do not open Plant Area View during Build Network operation.

17.1 Structure of the Plant Area View

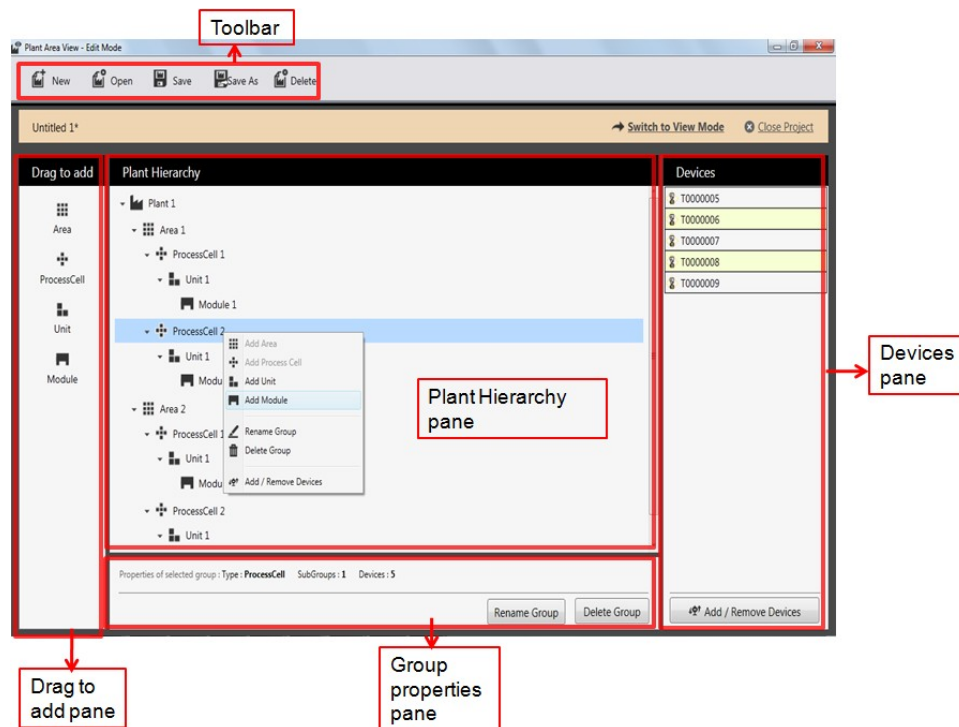
The Plant Area View feature has the following two modes through which Plant Area View projects can be created and viewed.

Edit Mode: Users with Edit Plant Area View privileges are allowed to create/edit Plant Area View projects. By default, administrators group has privileges to create/edit Plant Area View projects. An administrator can provide this privilege to other roles by assigning Edit PlantAreaView privilege to the required roles. For more information about assigning the privileges to roles, refer to the section [“Roles and privileges”](#). You can map the available devices to any group, plant, area, process cell, unit, or module.

View Mode: Users are allowed to view any Plant Area View project from the pre-created set of projects. It is a read-only mode and you can view the entire hierarchy, health, connection status, percentage of healthy/ unhealthy, and disconnected devices in a group.

17.1.1 Plant Area View – Edit Mode

The following figure illustrates the edit mode of the Plant Area View.



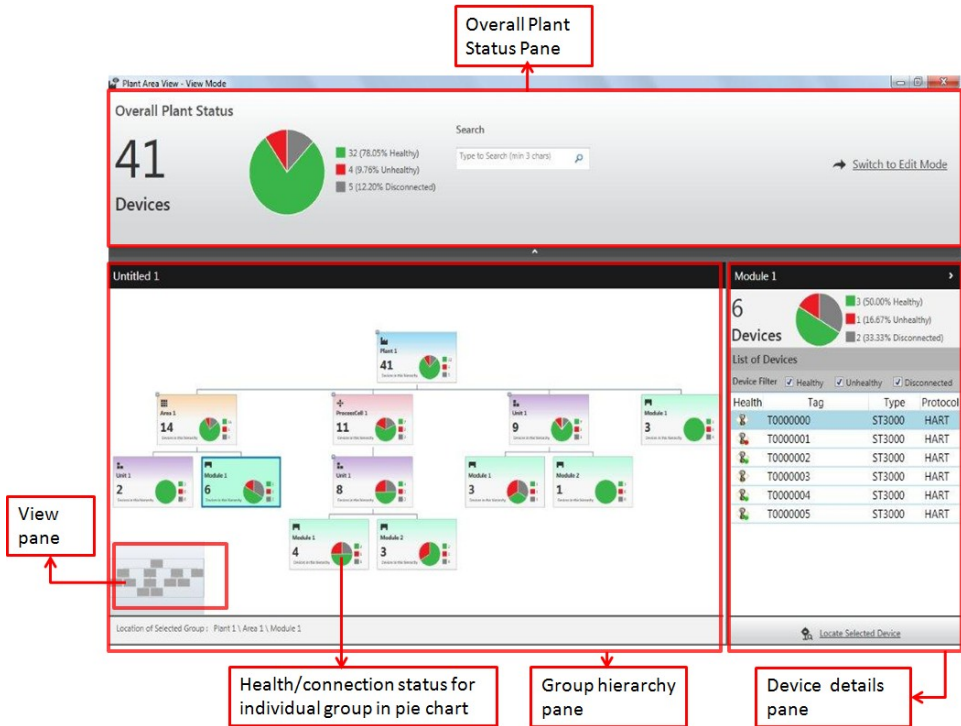
The following table describes the different elements/icons available in the Plant Area View – Edit Mode window.

Element/Icon	Description
Toolbar	
	New: Click to create a new Plant Area View project.
	Open: Click to open an existing Plant Area View project.
	Save: Click to save the Plant Area View project.
	Save As: Click to save a project as another copy of that project.
	Delete: Click to delete the project.
Drag to add pane	
 Area	Drag this group under Plant in the plant hierarchy. An Area is a group in the plant hierarchy that is identified by physical, geographical, or logical segmentation within the plant. NOTE It may contain process cells, unit, and modules.
 ProcessCell	Drag this group under Plant/Area in the plant hierarchy. A Process Cell is a logical grouping of unit and modules that are required to make plant hierarchy.
 Unit	Drag this group under Plant/Area/Process Cell in the plant hierarchy. A Unit is a collection of associated modules.
 Module	Drag this group under Plant/Area/Process Cell/Unit in the Plant hierarchy. A Module is a lower level group in the plant hierarchy. NOTE You cannot drag any group under Module.

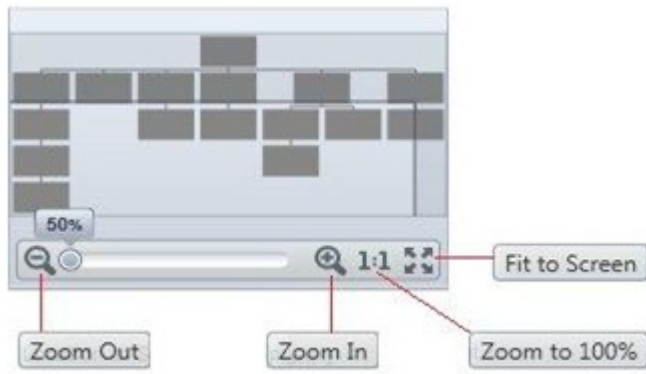
Element/Icon	Description
Plant Hierarchy pane	Displays the plant hierarchy where you can add/delete groups and add/remove devices. The root group of the hierarchy is named as Plant 1 by default. A Plant is a higher level group in the plant hierarchy. NOTE A project can have a maximum of 100 groups.
Devices pane	Displays the devices that are assigned to the selected group.
Group properties pane	Displays the type of the selected group, number of subgroups under the selected group, and number of devices assigned to the selected group.

17.1.2 Plant Area View - View Mode

The following figure illustrates the view mode of the Plant Area View.



Move the mouse pointer over the View pane for an enlarged version, as shown:



User Interface elements		Description	
Group hierarchy pane		Displays the group hierarchy where each group is identified using different background shades. It displays the name, icon, number of healthy/unhealthy/disconnected devices, and the total number of devices in its hierarchy along with the pie chart. The following background shades are used to identify the groups.	
		Group	Background color
		Plant	Blue
		Area	Yellow
		Process Cell	Pink
		Unit	Purple
		Module	Green
	Health/connection status for individual group in pie chart	Displays the health/connection status at the group level by selecting a group. The pie chart in each group describes the group hierarchy health, which is a consolidated health of a group and all the groups which are under its hierarchy.	
	Location of Selected group	The path of the currently selected group is available at the lower-left corner of the view mode which indicates where exactly the group is located in the hierarchy. This helps in identifying a group/device in the entire hierarchy instantly.	
	View pane	You can use the View pane available at the lower-left corner of the Group hierarchy pane, to change the magnification of the groups. This helps you to auto fit, zoom in, and zoom out the group hierarchy.	
Device details pane		Displays the details of the devices that are mapped to the selected group. It has group name, number of healthy/unhealthy/disconnected devices, and total devices in that group along with pie chart, and a list of devices mapped only to that group. You can filter the devices based on their health and connection status.	

User Interface elements		Description
		NOTE Click  to expand and  to collapse Device details pane.
	Locate Selected Device	You can also locate a device in the FDM Client Network View from the Device details pane of the Plant Area View. Select a device from the device list, and then click Locate Selected Device link. The selected device is highlighted in FDM Client Network View.
Overall Plant Status pane		Displays the health/connection status of entire plant in a pie chart in expanded mode, by means of indicators. The size of the indicators (healthy, unhealthy, and disconnected) varies according to the change in health/connection status. NOTE Click  to expand and  to collapse Overall Plant Status pane.
	Search	You can search a device or a group. When you search a group, all the groups in View Mode are highlighted, which has the searched string. When you search a device, all the groups are highlighted, which have at least one device whose tag/name contains the searched string.
	Switch to Edit Mode	Click this to edit the Plant Area View projects.

NOTE

The pie charts at group level/group hierarchy level/entire plant level in the Plant Area View – View Mode does not update in the following scenarios.

- When a filter is applied in the device dashboard for a group.
- When build network is in progress.

You need to close the project and open it again.

17.2 Creating projects in Plant Area View

Based on the geographical locations, you can create the groups and it creates the plant hierarchy. The process of assigning a group to the plant hierarchy and adding available devices to each group is called as project.

To create a project in Plant Area View, perform the following steps.

1. In the FDM Client main window, click View > Plant Area View or click  icon from the toolbar. The Plant Area View – Projects Wizard appears with the list of all existing projects. It allows you to open one project at a time.
2. Click Create New Project. The Plant Area View – Edit Mode window appears. This allows you to create and edit the Plant Area View projects. The root group of the hierarchy is named as Plant 1 by default.

TIP

You can also click New in the Plant Area View – Edit Mode window to create a new project. This creates a new project after closing any other opened projects.

3. Click Save. The Save dialog box appears.
4. Type the project name, and then click OK.

NOTE

- You can create a maximum of 25 projects in Plant Area View.
- A group or project name can contain up to of 20 alphanumeric characters and must not contain special characters except for white space.

17.2.1 Adding a group

To add a group to the plant hierarchy, perform the following steps.

1. In the Plant Area View – Edit Mode window,
 - From the Drag to add pane, drag a group under another group of higher level in Plant Hierarchy pane. You can drag a group only under a group which is of higher level. For example, you cannot drag a Unit under Module. But you can drag a Module under Unit as the Unit is in higher level compared to Module.

Or

 - Right-click any group, and then click Add Area/Process Cell/Unit/Module on the shortcut menu. The dragged group is added as a child group.

NOTE

You cannot add any group under Module. Hence, when you right-click any Module, the option Add Area/ Process Cell/Unit/Module is unavailable.

2. Click Save.

TIP

When you drag a group from the Drag to add pane, the groups are highlighted in Plant Hierarchy pane to which you can add a group.

17.2.2 Deleting a group

To delete a group from the plant hierarchy, perform the following steps.

1. In the Plant Area View – Edit Mode window,
 - From the Plant Hierarchy pane, right-click the group, and then click Delete Group on the shortcut menu.
 - Or
 - From the Plant Hierarchy pane, select the group, and then click Delete Group, which is available at the lower right of the Group properties pane. The selected group is deleted from the Plant Hierarchy pane.

NOTE

The root group (Plant) cannot be deleted from the Plant Hierarchy pane. Hence, the Delete Group option is unavailable if the selected group in the hierarchy is root group.

2. Click Save.

17.2.3 Renaming a group

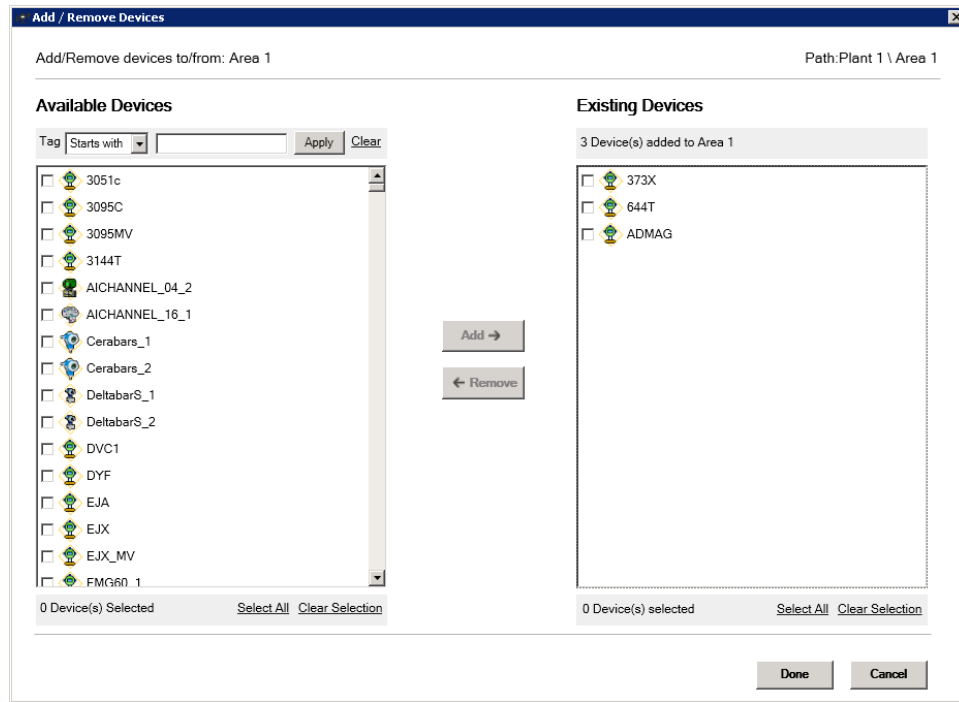
To rename a group in the plant hierarchy, perform the following steps.

1. In the Plant Area View – Edit Mode window,
 - From the Plant Hierarchy pane, right-click the group, and then click Rename Group on the shortcut menu.
 - Or
 - From the Plant Hierarchy pane, select the group, and then click Rename Group, which is available at the lower right of the Plant Hierarchy pane.
2. Click Save.

17.2.4 Adding/removing devices

To add/remove devices to/from a group

1. In the Plant Area View – Edit Mode window, right-click the group and then click Add/Remove Devices on the shortcut menu. Or Click Add/Remove Devices button which is located at the lower right of the Devices pane. The Add/Remove Devices dialog box appears with a list of devices, which are available in the FDM Network View. These devices are mapped to the selected group.



2. Perform the following:

- If you want to add devices to a group, from the Available Devices box, select the device tag, and then click Add. The added devices appear under Devices pane in Plant Area View – Edit Mode window. Or
- If you want to remove devices from a group, from Existing Devices box, select the device tag, and then click Remove.
- If you want to add or remove all devices, click Select All.

NOTE

If you want to add an already added device from a group to another group, you must first remove the device from the group to which it is mapped and then add to the desired group.

3. Click Save.

17.3 Editing projects in Plant Area View

FDM allows you to edit the projects in Plant Area View. You can edit the projects, where you can add/delete a group, rename a group, or add/remove a device.

In multi-client scenario, if you edit similar projects at the same time in multiple clients, only the last change made with respect to that project (in any client) is saved.

For example, if you edit project 1 in Client 1 and Client 2 at the same time, and if changes made to the Client 2 are saved at the last, then, only those changes are available.

To edit the projects in Plant Area View, perform the following steps.

1. In the FDM Client main window, click View > Plant Area View or you can also click  icon from the toolbar. The Plant Area View – Projects Wizard appears with the list of all existing projects. It allows you to open one project at a time.
2. Under Existing Projects, click the project name to open an existing project. The Plant Area View – View Mode window appears.
3. Click Switch to Edit Mode.

The Plant Area View – Edit Mode window appears where you can edit the projects for the following as necessary.

- Adding groups: For more information, refer to the section [“Adding a group”](#).
 - Renaming groups: For more information, refer to the section [“Renaming a group”](#).
 - Deleting groups: For more information, refer to the section [“Deleting a group”](#).
 - Adding/removing devices: For more information, refer to the section [“Adding/removing devices” on page 197](#).
4. Click Save.

DEVICE CONFIGURATION USING DD

Device configuration constitutes performing the following:

- Loading a device
- Configuring a device
- Editing parameters
- Editing device properties
- Saving and downloading the device information

Supported devices for device configuration using DD

- HART (wired/wireless)
- FF
- ISA100 Wireless

NOTE

If a HART device has both DD and DTM and if you want to load a device using DD, ensure that the device is loaded using Load using DD/EDD setting.

FDM allows viewing/configuring of parameters as defined in the DD of a device, using the entry point in the right pane of the FDM Client. It depends on the style of the entry point and it varies from device to device. The related variables are grouped under various menus of different levels as defined in the DD file.

Each device includes a set of parameters to define the attributes and operating characteristics of the field device. These device parameters are the key elements of the information managed by the FDM. Device manufacturers define the HART field device parameters and their behavior in the Device Description file.

Device parameters are classified into the following three categories.

- Parameters that describe the device, such as its model and revision number. These parameters do not directly affect the device's operation, but they are useful while ordering a replacement.
- Parameters that define how the device operates and measures values, such as configuration values, calibration settings, and unit settings. These are called static parameters.
- Parameters that display the actual values obtained directly from the field device. The values of certain variables are updated by the field device without any stimulus from the communication network or the user. These parameters are called dynamic parameters. For example, PV, SV, TV, and so on.

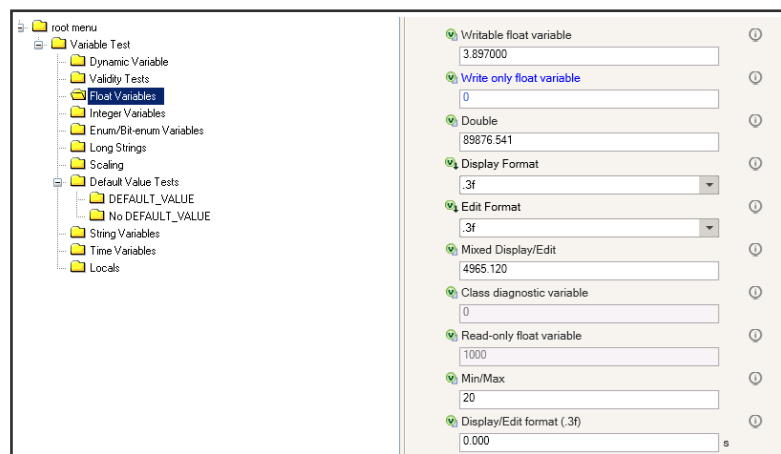
The following icons are displayed in the Device Configuration page in the right pane of the FDM Client.

Icon	Description
	Indicates a menu or submenu in the navigation tree.
	Indicates a currently selected menu or submenu in the navigation tree.
	Indicates a Variable item.
	Indicates a Method item.
	Indicates an Edit Display item.
	Indicates a Local Variable item.

NOTE

Local variable are used by host applications to access other items or variables in the field device. They are not written to or stored in the field device.

Uncertain or unread parameter labels appear in blue text. An indicative screen is shown here.

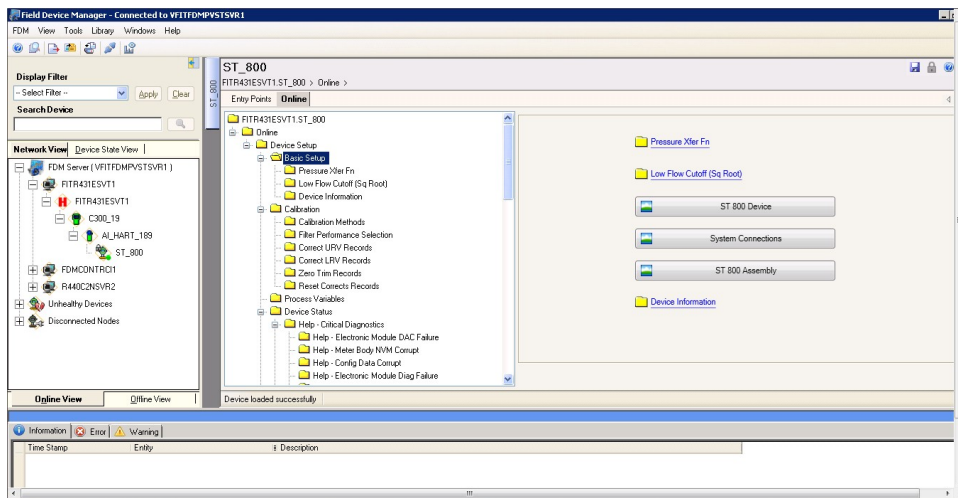


18.1 Configuring a HART device using DD

When a HART device is loaded there are 2 versions of the DD file which determines the view of the online device. The 2 views available are table and window view.

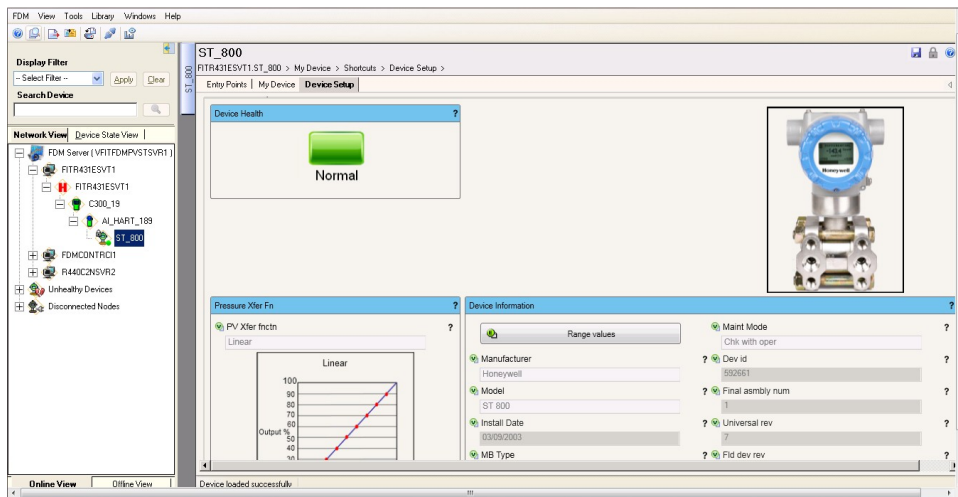
Table view

In the Table view, the Device Configuration page is split vertically into two panes. The left pane displays a group of menus as a tree view and the right pane displays the group of corresponding parameters with their values and units, method, and edit display of the selected menu.



Window view

In the Window view, the Device Configuration page opens in modeless window and the sub menus are displayed as a tabbed page. Clicking each tab allows you to navigate to the child menus.



To configure a HART device

1. Ensure that the device is displayed in Network View list under Online View.
2. In the Network View list, right-click the required device tag and click Configure. The device is loaded using Load using DD/EDD setting.

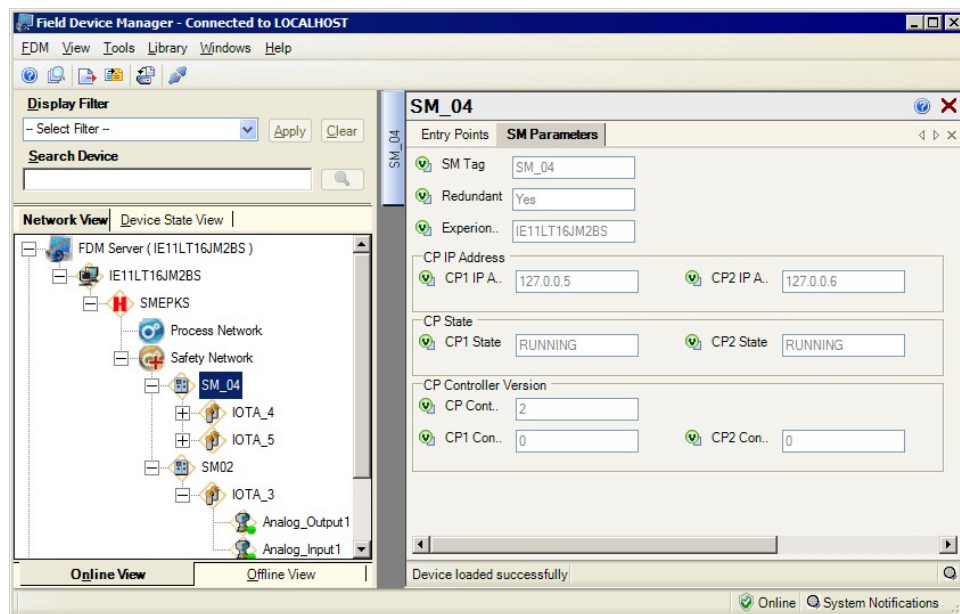
TIP

You can also open the device configuration page by double-clicking the device in the Network View list under Online View. It loads a device with the default setting. If you want to load a HART device using DD irrespective of DD/DTM settings, right-click the required device tag and choose Configure with > DD.

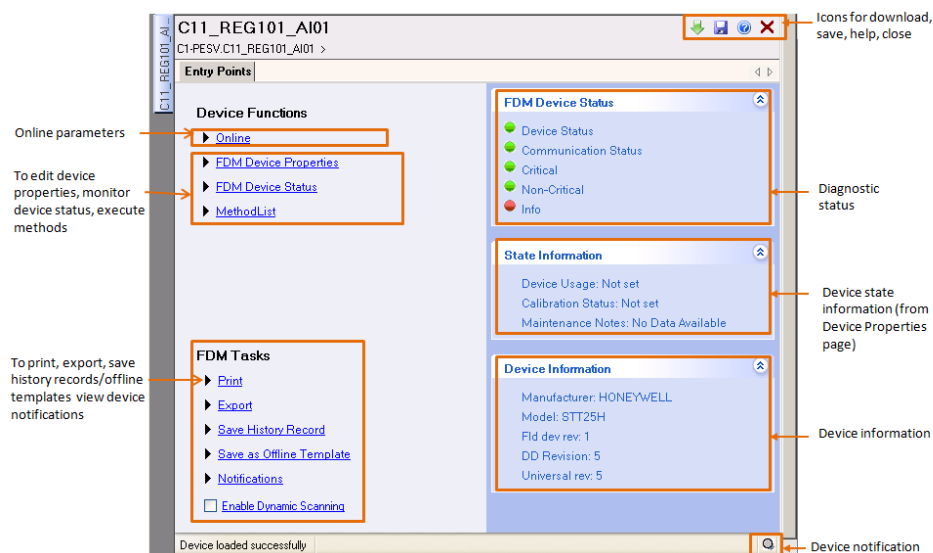
For Station Maintenance View, the device is always loaded with the default Load Setting.

When you right-click SM/IOTA and then click Configure, the device configuration page appears. To view the SM/IOTA parameters, click the corresponding parameters link in the Entry Points page.

For example, to view the SM parameters, click SM Parameters link. The following page appears with read-only parameters and you cannot configure those parameters.



The details appear on the Device Configuration page depending on the DD/DTM.



After the parameters are read, the device is loaded successfully.

If Device autolock feature is enabled and a device configuration page is open when the device's autolock timer is about to expire (5 minutes before the end of the autolock timeout interval), a message appears in the lower right side of the page. The autolock timeout interval can be extended from a range of 10 to 60 minutes. Clicking this message allows you to extend the autolock timer.

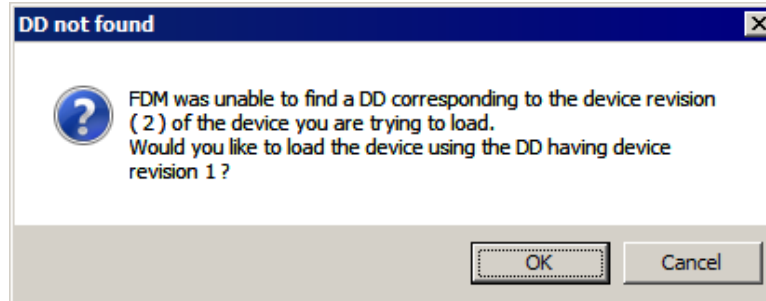
If you don't want to extend the timer, ignore the message and the device is locked automatically when the timer expires. The reminder message is displayed only to the users with Write Parameter privilege.

If you are viewing a device configuration page and an autolock reminder appears for a different device, that device's tab name turns red which indicates that a reminder message is being displayed for that device.

NOTE

When a device is in the process of loading, the options under Entry Points do not appear for some devices. The options appear only when the device is loaded completely. Depending on DD file complexity, some devices can take several minutes to load.

If a DD corresponding to the device revision that you are trying to load is not available for the device, then the following message appears.



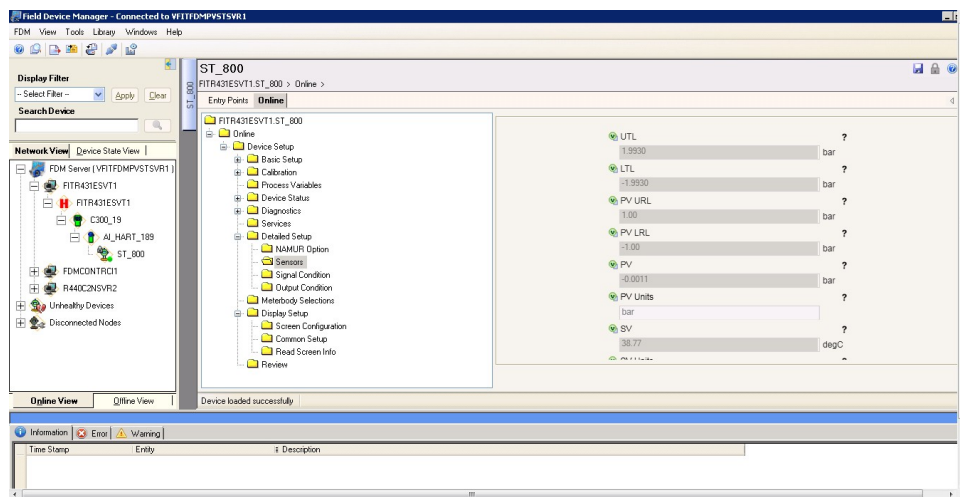
Click OK to load the device with the latest DD of previous device revision.

If a DD corresponding to the device type and device revision is not found, the device is loaded with a generic DD after user confirmation.

For Gateway and Field devices, you must already have selected the correct profile while adding the DD failing which this message will be received.

The following procedure is just an example. The options under entry points are device-specific and vary from device to device.

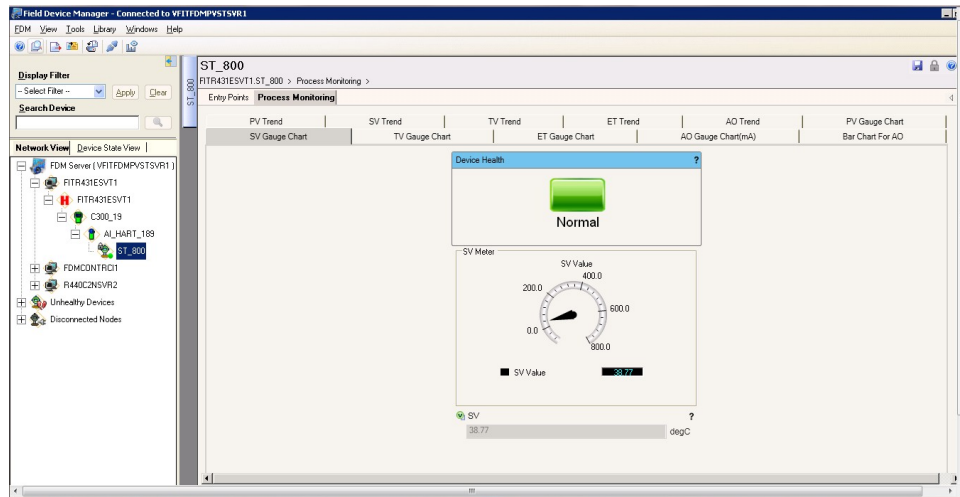
3. On the device configuration page, click Online. The device configuration page displays the menu options to configure the online parameters.



The following illustration shows the EDDL trend and charts for ST800 device.

On the device configuration page entry points, click Process Monitoring. You can view the different tabs for different types of chart.

The following page appears displaying the device health, variables, and so on.



NOTE

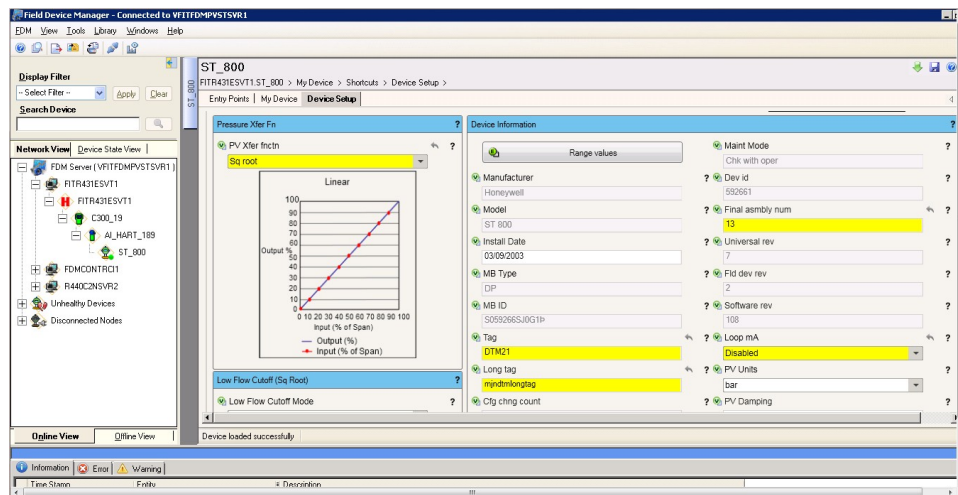
- You can change configuration of the device only if it is unlocked.
- When FDM is connected to the field devices through the Experion interface through the PM HART IO or the Series C I/O module, devices that are in process are locked by default. To edit any device parameter or run a method, you need to inactivate the device.
- When FDM is connected to field devices through the Experion interface through the 1756 HART IO module, the channel mode needs to be changed to 'OFF CONTROL' in order to configure the devices.

If the same device is open in two or more clients, then only the first client has read write access to the device, assuming that the user has required privileges. The second and subsequent client shows this device as locked. The bottom pane displays the parameter names, values, and their corresponding units, methods, and edit display. The parameter values are updated dynamically as per the actual values of the device in the field. If required, modify the values for the configurable parameters.

NOTE

You cannot modify the parameter values that appear in grey.

4. Select the parameter to modify the value. The parameter value field turns yellow when you modify the value.



Click the  icon to view information about the parameter such as Label, Value, Unit, Help, and so on. This information is available from the DD. When you are editing parameters, the pre/post edit actions and warnings appear if they are defined in the DD. Respond to those actions before editing the parameters. These actions and warning vary from one variable to another.

5. Click OK to edit the parameter. The post edit action message appears when you click parameter in a device.
6. Click  icon to update the modified parameters values to the field device. The Parameters To Download dialog box appears.
7. Click Download.

The modified parameter values are downloaded to the field devices.

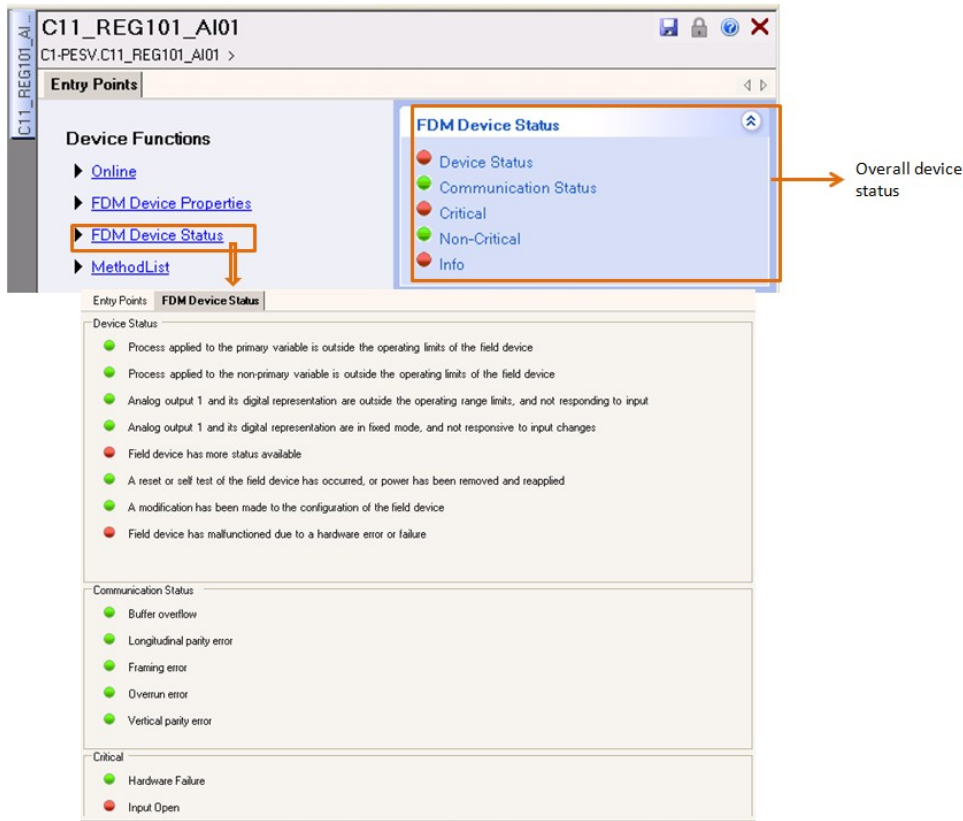
- For better performance of FDM, it is recommended to close the device configuration page after the configuration activities for a device are completed.
- For some devices to edit device parameters, device's write protect (if present in device) should be disabled.
- For a device connected to an RS-485, DD over Comm DTM networks or an Experion network communication interface, FDM does not allow changing of poll address.
- Ensure the local time zone format is set to "English (United States)" using Control Panel > Clock, Language, and Region > Change the time zone. Editing the date and time parameters may fail if the local time zone changes.

18.1.1 Monitor the HART device status

FDM assists in monitoring the diagnostics of HART devices.

To view the device status, on the HART device configuration page, click FDM device status under Device Functions. The FDM Device status page appears.

You can view the device status with respect to network communication, devices, and command-48 strings as illustrated in the following image.



The diagnostic details are common to all HART devices. However, command-48 strings vary from one device to another depends on DD.

NOTE

The communication status bit is set (indicated in red) in the device configuration page even though communication status bit is not set (indicated in green) in the FDM device status page. This might happen when the actual communication problem type is defined neither by the device nor in the DD.

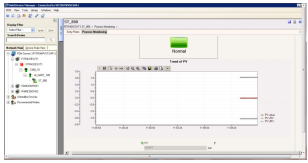
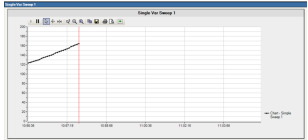
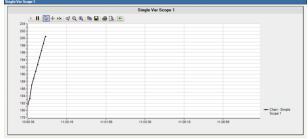
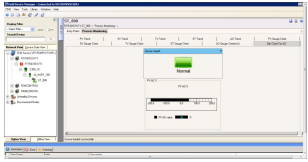
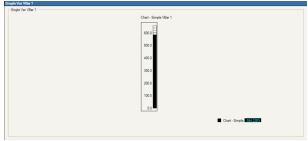
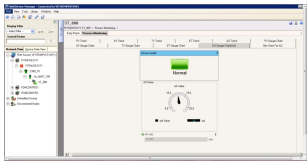
18.1.2 Graphical data representation

FDM supports two graphical data representation types - charts and graphs.

Charts

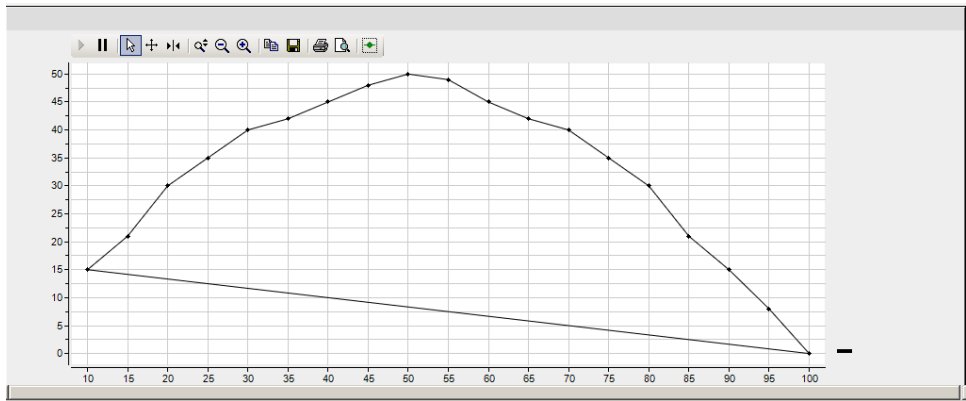
FDM supports charts with multiple dynamic variables sampled periodically as a continuous trend against a time-axis on an on-going basis. This is useful for detecting drift, intermittent problems, and other dynamics.

There are different types of charts available in various sizes to view data from field devices. The following table describes each type of chart.

Chart	Description	Graphical Representation
Strip	Data scrolls from right to left. New data is added at the right of the chart with the historical data shifted to the left.	
Sweep	Data is updated from left to right. Old historical data is overwritten. When the displayed plot reaches the right of the chart the data begins plotting again from the left of the display.	
Scope	Data is updated from left to right. When the displayed plot reaches the right of the chart, the display is erased and the data plotting begins again from the left of the display.	
Horizontal bar	A single line or bar proportional to the current value of the source is displayed. The bar is displayed horizontally with its origin (minimum value) on the left of the chart.	
Vertical bar	A single line or bar proportional to the current value of the source is displayed. The bar is displayed vertically with its origin (minimum value) at the bottom of the chart.	
Gauge	A circular, dial-type analog meter. The indicator is an arrow or pointer that rotates as the current source value varies. The minimum and maximum values are generally near the bottom of the dial and the indicator rotates clockwise as the source value increases.	

Graphs

FDM supports graphs that are available in various sizes to view data from field devices.



Graphical Toolbar

You can use the buttons on the graphs and charts display to modify it. The following table describes each button.

Button	Function
	Resumes live update. Restores the trend so that it is updated with live data.
	Pauses the trend so that data is not updated.
	Default cursor Allows scrolling of the axis to change the period and sample interval.
	Data cursor that highlights the values referenced by the data point.
	Enlarges a selected area within the chart or graph.
	Zooms out of the visible range. If a reference line is visible, the zooming is centered on the reference line.
	Zooms in to the visible range. If a reference line is visible, the zooming is centered on the reference line.
	Copies the displayed chart or graph to the clipboard.
	Saves the displayed chart or graph as a graphic file.
	Prints the displayed chart or graph.
	Previews the displayed chart or graph for printing.
	Shows or hides data points.

NOTE

At a minimum, charts and graphs are refreshed every 5 seconds. This refresh cycle time is linked to EDDL attribute of graphs and charts.

18.2 Configuring a FF device using DD

NOTE

- If a FF device has both DD and DTM and if you want to load a device using only DD, ensure that the device is loaded using Load using DD/EDD setting.

- Device level menu is not supported for FF devices.

To configure an FF device:

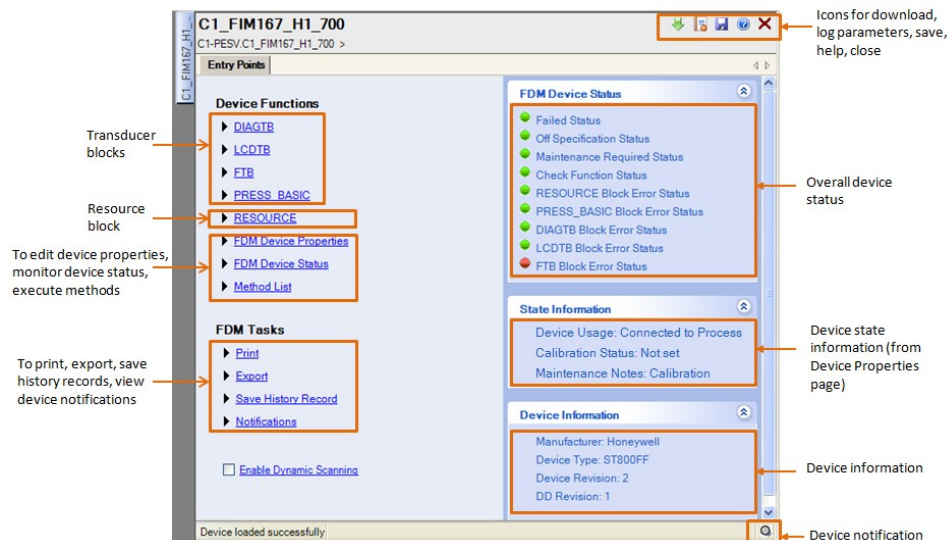
1. Ensure that the device is displayed in Network View list under Online View.
2. In the Network View list, right-click the required device tag and then click Configure or double-click the device in the Network View list under Online View. It loads a device with the default setting. The device is loaded using Load using DD/EDD setting.

TIP

If you want to load a FF device using DD irrespective of DD/DTM settings, right-click the required device tag and then click Configure with > DD.

For FDM Station Maintenance View, the device is always loaded with the default load setting.

The details appear on the Device Configuration page depending on the DD/DTM.



After the parameters are read, the device is loaded successfully.

If Device autolock feature is enabled and a device configuration page is open when the device's autolock timer is about to expire (5 minutes before the end of the autolock timeout interval), a message appears in the lower right side of the page. The autolock timeout interval can be extended from a range of 10 to 60 minutes. Clicking this message allows you to extend the autolock timer.

If you don't want to extend the timer, ignore the message and the device is locked automatically when the timer expires. The reminder message is displayed only to the users with Write Parameter privilege.

If you are viewing a device configuration page and an autolock reminder appears for a different device, that device's tab name turns red which indicates that a reminder message is being displayed for that device.

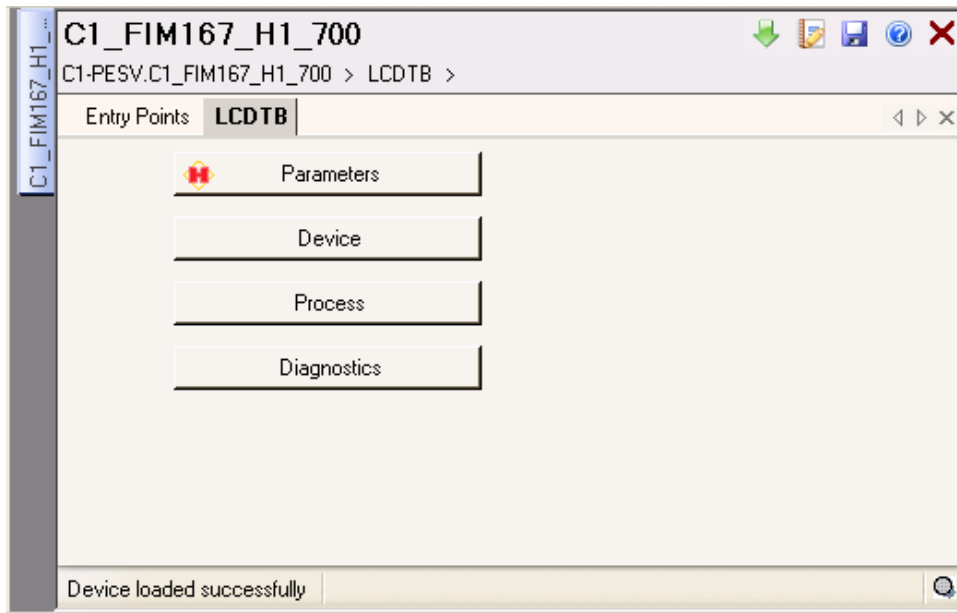
NOTE

- When a device is in the process of loading, the options under Entry Points do

not appear for some devices. The options appear only when the device is loaded completely.

- For better performance of FDM, it is recommended to close the device configuration page after the configuration activities for a device are completed.
- FDM supports one resource block and multiple transducer blocks. FDM does not support the function blocks.

3. Under Device Functions, click any block to view all the menus and to edit the parameter values as shown in the following sample illustration.



Each block has parameters menu. Along with this menu, block can also have other sub-menus and their parameters, if they are defined in the DD. These sub-menus are block-specific and vary from device to device.

4. Click Parameters menu within the block. Here, Honeywell logo indicates that these are Honeywell custom parameters and not defined in the DD. You can view the parameter layout with the different tabs as shown in the following figure. This menu is in synchronization with parameters menu from Experion.

5. If any parameter information (parameter layout and access levels) is updated in the device template from Experion, then a message appears informing that device information is changed in Experion and need to reload the device in FDM Client.
6. Click OK, close the device configuration page, and then reload the device in FDM Client. The modified parameter layout appears in FDM device configuration page.

NOTE

- If a device is not loaded in FDM and any parameter information is changed in Experion, then the parameter information will automatically update when you load the device in FDM.
- Changing a parameter in Experion does not necessarily update it in FDM in a timely manner, especially if Enable Dynamic Scanning is not selected.

7. Browse through the different sub-menus of block and edit their parameters, which have write access. The parameter value field turns yellow when you edit the value.
8. After editing the parameter values, click  icon to download the edited parameters values to the field device. The Parameters To Download dialog box appears.
9. Click Download. The modified parameter values are downloaded to the field devices.

NOTE

- The block names in both Control Builder and FDM are identical.
- You can change the configuration of the device only if it is unlocked.

10. In the Experion Station, if you want to record all the parameter changes in the event summary for all FF devices that are connected to FIM, click  icon on the right-corner of the device configuration page. The log parameter enables log for all FF devices in the network view.

TIP

Experion Event journal logging for devices can also be changed from the Settings dialog box. For more details, refer to the section [“Customizing the network settings”](#).

18.2.1 Monitor the FF device status

FDM assists in monitoring the detailed diagnostics of FF devices with guidance of required service actions, and system supported planning and execution of service tasks. As per the NE107 guidelines, the FF device status is organized into the following four categories based on the impact of the condition to the health of the FF device.

- Maintenance Required Status: The FF device is able to provide a valid output signal, but it is about to lose functionality or capability due to some external operational condition.
- Failure Status: The FF device provides a non-valid output signal due to device malfunction.
- Check Function Status: The FF device is temporarily non-valid due to some type of maintenance activity.
- Off Specification Status: The FF device operates out of the specified measurement range.

In the following scenarios, you can monitor the FDM device status for FF devices.

- FF device with Field Diagnostics support
- FF device with Advanced alarm configuration in Experion
- Neither FF device supports Field Diagnostics nor advanced alarms are configured

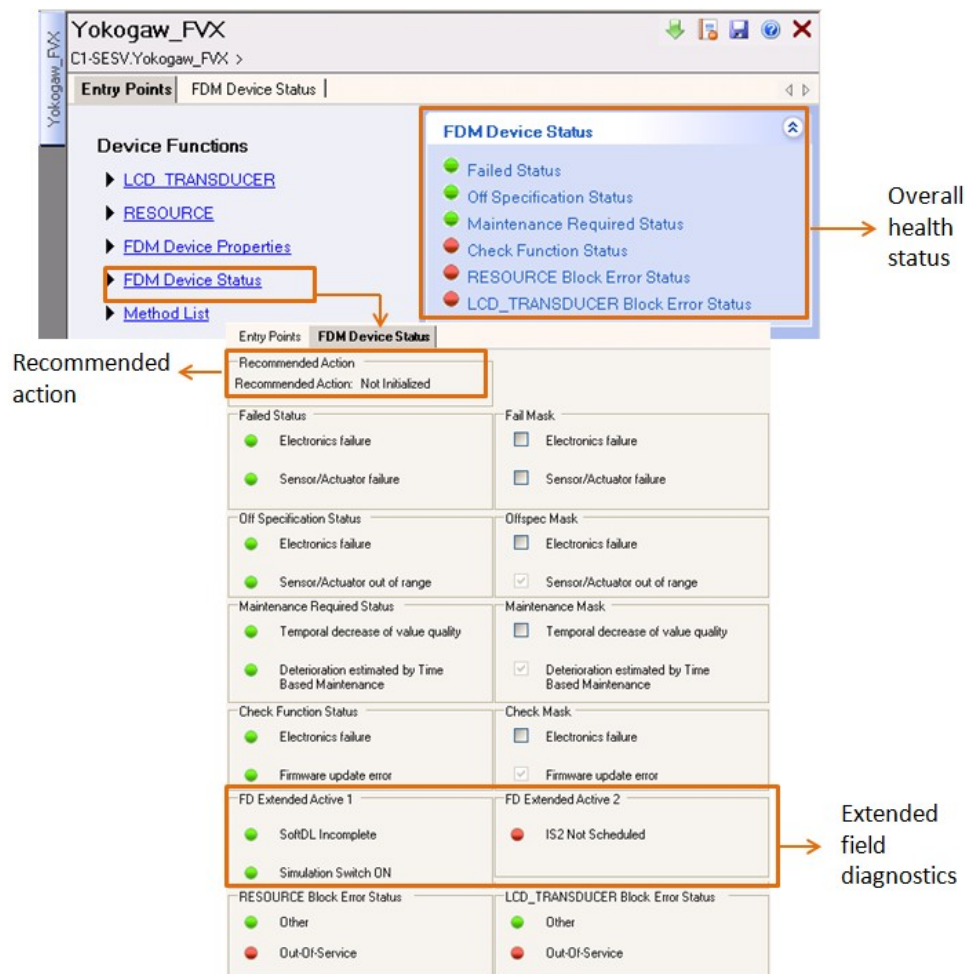
NOTE

If a FF device supports Field Diagnostics and also advanced alarm configuration is available in Experion, then FDM Device Status will be displayed as per the Advanced alarm configuration.

FDM device status when the FF device supports the Field Diagnostics

Foundation Fieldbus specification FF-912 allows devices to display alarm information organized by category. When a device and its DD supports FF-912 alerts, FDM displays these as well as the traditional Block Error Status information. The Field Diagnostic also provides the recommended corrective actions and detailed help, as well as an indication of the overall health of the device.

On the FF device configuration page, click FDM device status under Device Functions. The FDM Device status page appears.



The overall category can have maximum 32-bit conditions. If there are more than 31 device diagnostic events, you must group them by definition into these bits. The FF extended parameters are available in the device and displays the more detailed information to you to determine the root cause of the problem as displayed in this figure.

FDM displays only the mapped conditions for each category. In the FDM device status page, if the condition for category is in red, the device icon is indicated in red in the network view and the corresponding alarms are displayed in the Experion Station. And also, in the FDM device status page, the block error status for each block is displayed.

The condition for the category is in red and if it is masked (mask is enabled) in the device, then the alarms for the condition will not generate and the device will be healthy in the network view.

The recommended action, which is defined in the device based on the active condition and displayed at the top of the FDM device status page. Follow the recommended action to make the device healthy.

NOTE

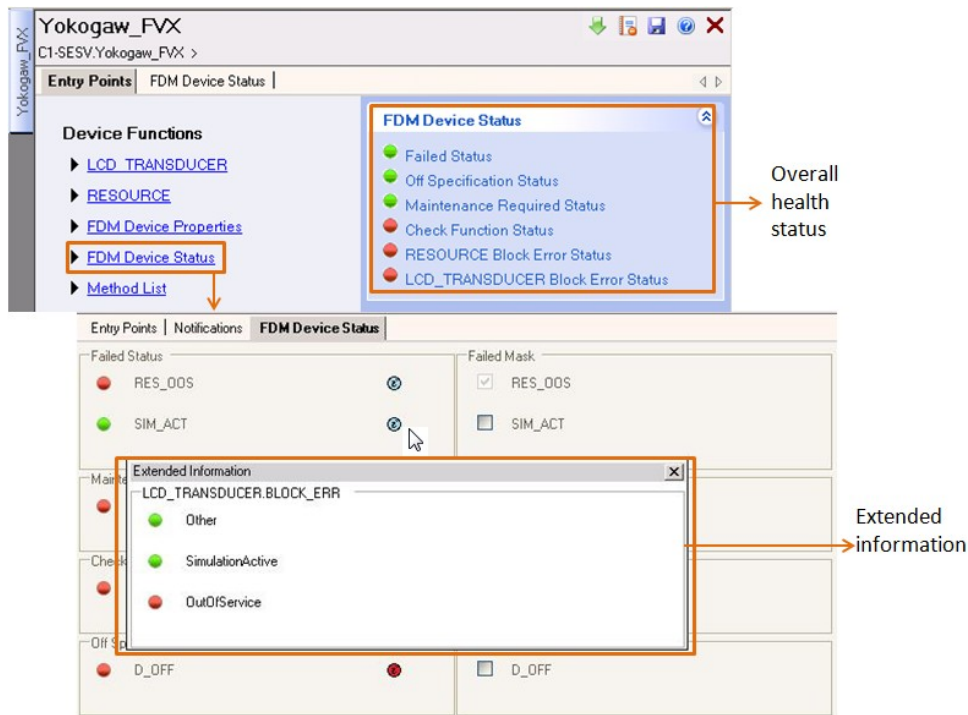
If the conditions for each category are in green, it indicates that device is healthy and “No Action” is displayed for the recommended action.

The overall device status shows the block error status and status of each category in the device configuration page as in the figure. If any of the condition bit for the category is in red in the FDM device status page, then overall device status for that category is displayed in red in the device configuration page, provided that condition is not masked.

FDM device status with advanced alarm configuration in Experion

Advanced alarms are configured in Experion and this data can be viewed in FDM. The FDM device status page shows the advanced alarm conditions for each category and the respective bits. If there are advanced alarms configured on a given FF device, and those alarms are set or reset, FDM would reflect these changes in the FDM device status page. However, if any changes to the condition, then a message appears informing you to reload the device in FDM.

On the FF device configuration page, click FDM device status under Device Functions. The FDM Device status page appears.



FDM displays only the mapped conditions for each category and the conditions are categorized as per the criticality. In the FDM device status page, if the condition for category is in red, then device icon is indicated in red in the network view. And also, the corresponding alarms are displayed in Experion Station.

If the condition is active, then the corresponding condition is in red as in the LED. When the condition is masked (condition is enabled in Experion), the alarms for the condition will not

generate and the device will be healthy in the network view. If you click , a dialog box appears displaying the comprising parameters and bits for the corresponding condition. If any of the bit is set (condition is in red) in this dialog box, then condition is also set.

The overall device status shows the block error status and status of each category in the device configuration page as in the figure. If any of the condition bit for the category is in red in the FDM device status page, the overall device status for that category is displayed in red in the device configuration page, provided that condition is not masked.

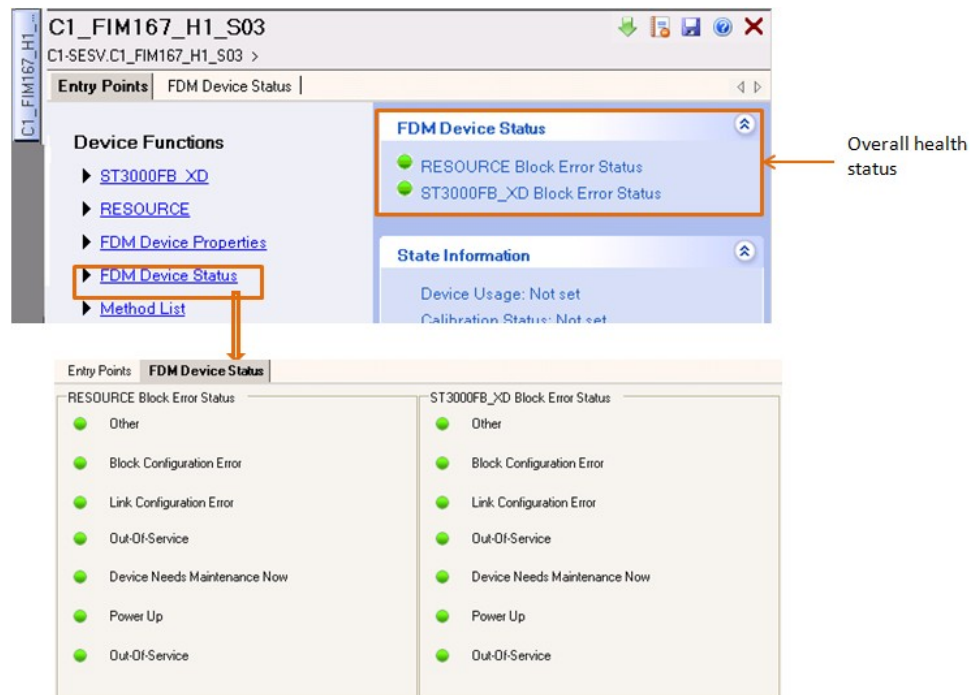
NOTE

When the FDM device status page is opened and if any alarm condition is changed, then you can view the device status update for every 60 seconds.

Field device status with block error

If the device does not support Field Diagnostics and advanced alarms are not configured in Experion, the FDM device status is comprised of Block Error information.

On the FF device configuration page, click FDM device status under Device Functions. The FDM Device Status page appears.



The FDM device status page shows the block error status for each block. The overall device status for each block is displayed in the device configuration page as in the figure. If any of the block error bit is in red in the FDM device status page, the overall device status for the block is displayed in red.

18.3 Configuring an ISA100 Wireless device using DD

Prerequisites

- Ensure that all WDM and ISA100 Wireless devices are commissioned in OneWireless User Interface.
- Ensure that OneWireless network is configured in the FDM Server Management Tool.

To configure a ISA100 Wireless device

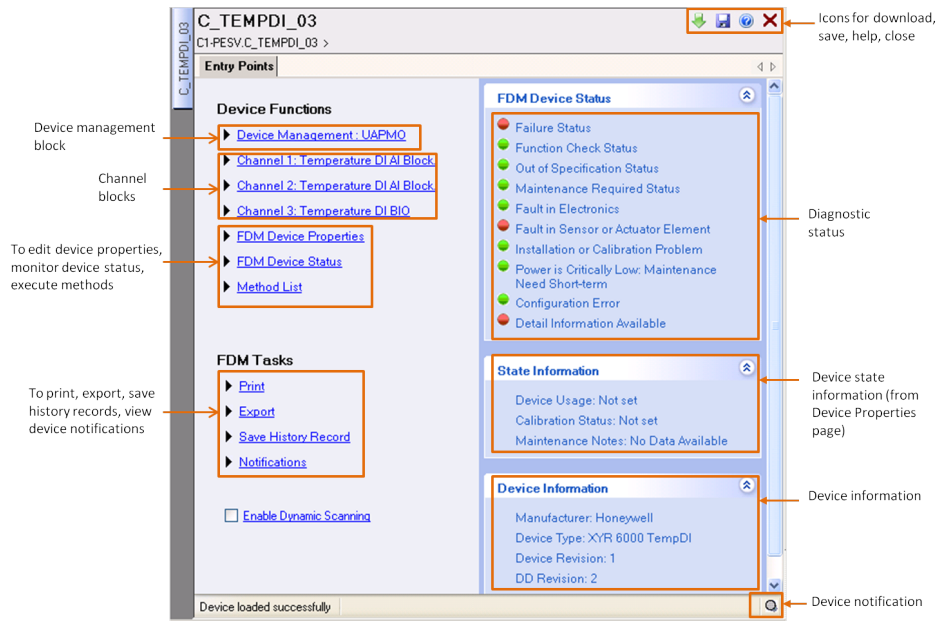
1. Ensure that the device is displayed in Network View list under Online View.
2. In the Network View list, right-click the required device tag and click Configure or double-click the device in the Network View list under Online View. It loads a device with the default setting.

The device is loaded using Load using DD/EDD setting.

TIP

FDM does not support configuration of ISA100 Wireless devices through DTM. For Station Maintenance View, the device is always loaded with the default load setting.

The details appear on the Device Configuration page.



After the parameters are read, the device is loaded successfully.

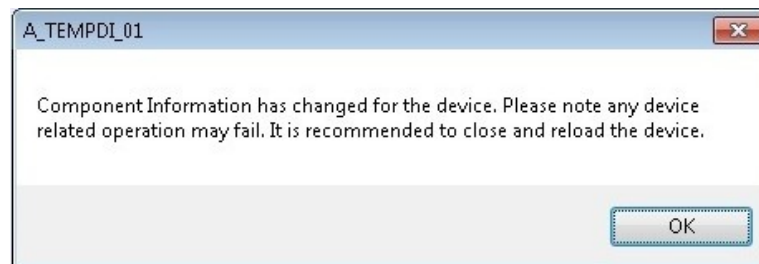
If Device autolock feature is enabled and a device configuration page is open when the device's autolock timer is about to expire (5 minutes before the end of the autolock timeout interval), a message appears in the lower right side of the page. The autolock timeout interval can be extended from a range of 10 to 60 minutes. Clicking this message allows you to extend the autolock timer.

If you don't want to extend the timer, ignore the message and the device is locked automatically when the timer expires. The reminder message is displayed only to the users with Write Parameter privilege.

If you are viewing a device configuration page and an autolock reminder appears for a different device, that device's tab name turns red which indicates that a reminder message is being displayed for that device.

NOTE

- When a device is in the process of loading, the options under Entry Points do not appear for some devices. These options appear only when the device is loaded completely.
- For better performance of FDM, it is recommended to close the device configuration page after the configuration activities for a device are completed.
- You can change configuration of the device only if it is unlocked.
- If you make any changes to the channel block in OneWireless User Interface, the following message appears.



Click OK and then close the device, and reload the device again.

- On the device configuration page, under Device Functions, click Channel 1: Temperature DI AI Block as shown in the following sample illustration. The corresponding channel block tab displays the options to configure the online parameters.

Entry Points **Channel 1: Temperature DI AI Block**

Temperature DI AI Object

Process Variable

- Process Value.Value: NaN
- Process Value.Status: Bad::OutOfService:Not Limited
- Transducer Scale.EU at 100%: 871.000000
- Transducer Scale.EU at 0%: -18.000000
- Transducer Scale.Units Index: °C

Mode

- Mode.Target: 00S
- Mode.Actual: 00S

Mode.Permitted

- ☒ 00S
- ☒ Auto

Scale

- Transducer Scale.EU at 100%: 871.000000

- Select the parameter to modify the value. The parameter value field turns yellow when you modify the value.
- Click  icon to update the modified parameters values to the field device. The Parameters To Download dialog box appears.
- Click Download.

If you modify any parameter value to the device in FDM, the modified parameter value is reflected automatically in the OneWireless User Interface. And also, the modified parameter values are downloaded to the field devices.

NOTE

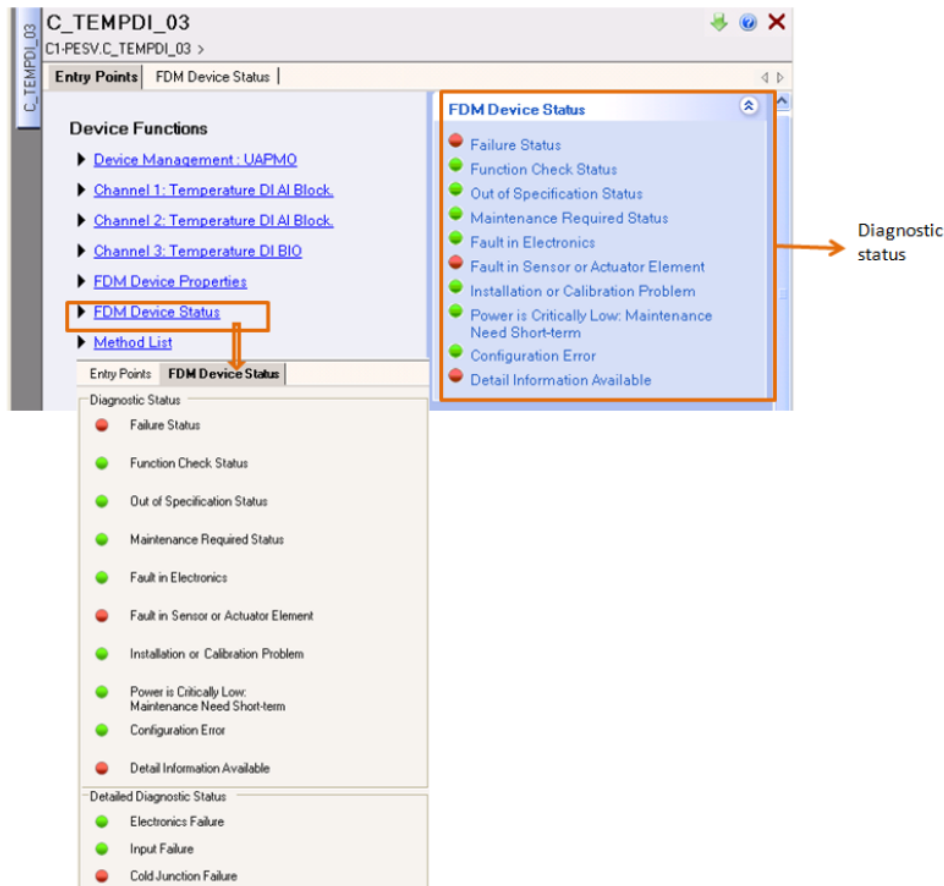
If any dynamic parameters like PV, SV, TV and so on are modified in OneWireless User Interface, the modified parameter values are reflected automatically in the FDM device configuration page. If any static parameter is modified in the OneWireless User Interface, then the modified parameter value is not reflected in FDM. To view the modified static parameters, you must close the device configuration page and reload the device in the FDM Client.

18.3.1 Monitor ISA100 Wireless device status

FDM assists in monitoring the diagnostics of ISA100 Wireless devices.

To view the device status, on the ISA100 Wireless device configuration page, click FDM device status under Device Functions. The FDM Device status page appears. You can view the following details on this page.

- Diagnostic Status: The diagnostic details are displayed for the device and common for all ISA100 Wireless devices.
- Detailed Diagnostic Status: The additional diagnostic details are displayed and these are specific to device. And also, these details vary from one device to another depends on DD.



18.4 Executing methods

Methods are a predefined sequence of actions that can be performed on HART, FF, and ISA100 Wireless devices. Methods are specified by the device vendor to perform the actions like loop test, calibration, write protection, and so on. The information regarding methods is available in the DD file of a device. Methods are available in the following two places.

- FDM lists all the methods in the Device Configuration page as Method List entry point.
- The method is defined in the DD for a device which can be browse through the menus.

NOTE

- When a device is in the process of loading, the methods under Method List

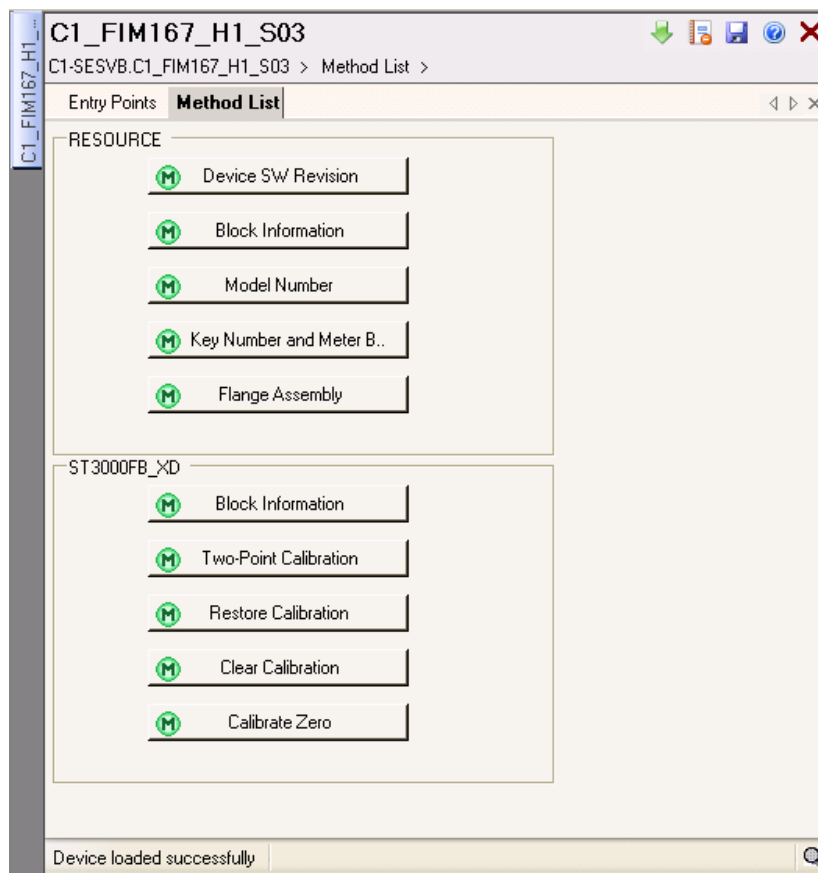
does not appear.

- When executing a method, you cannot perform any other operation on the device.
- If a method is running and the device autolock feature is enabled, then it may lead to method failure if the device is allowed to lock itself. Hence, it is recommended to extend the timeout interval or disable the device autolock feature before running methods.

The following procedure is just an example. The steps in each method type are device-specific and vary from device to device. Follow the instructions mentioned in the method's wizard to execute a method.

To execute a method for a device

1. On the Device Configuration page, click Method List. The following page appears with list of methods for FF transducer and resource blocks.



2. Click Device SW Revision. The method execution wizard appears.

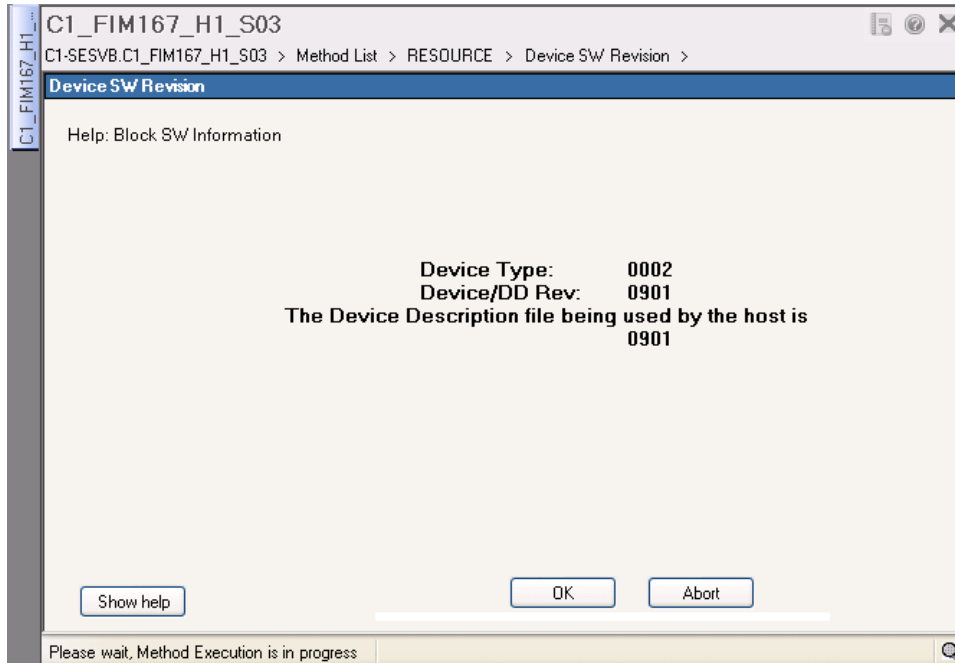
NOTE

The Help information is displayed in the wizard, if the help is defined for the device in the DD.

TIP

Place the mouse pointer over the method name. The tool tip appears displaying the label name and other information about the method. The tool tip information displays only when the help is defined in the DD.

To view the help information during the method execution process, click  in the wizard.



3. Click OK to continue with the method execution process for all subsequent steps. Or
4. Click Abort to cancel the method execution.

Similarly, select any other method and follow the on-screen instructions on the wizard to execute the method for HART and ISA100 Wireless device.

18.5 Editing device properties

On FDM Device Properties tab, you can view and edit the device properties such as device information, maintenance notes, and so on for HART, FF, ISA100 Wireless, and DE devices.

The following procedure is just an example of editing HART device properties. Similarly, you can view and edit device properties for FF, ISA100 Wireless, and DE devices.

To view/edit the device properties

1. On the Device Configuration page, click FDM Device Properties.

The screenshot shows the 'FDM Device Properties' window for device 'STT25H'. The window has a sidebar with 'STT25H' and a main area with various configuration fields. The fields are as follows:

Field	Value
Manufacturer	Honeywell
Model	STT25H
Fld dev rev	1
DD Revision	5
Universal rev	5
Maintenance Notes	No Data Available
Special Instruction	No Data Available
Device Usage	Not set
Calibration Status	Not set
Calibration Due Date (MM/DD/YYYY)	1/1/1900
Device Health	Not set

At the bottom of the window, a status bar indicates 'Device loaded successfully'.

It contains details such as Manufacturer, Model, Device Revision, DD Revision, Maintenance Notes, Special Instruction, Device Usage, Calibration Status, Calibration Due Date (MM/DD/YYYY), and Device Health.

NOTE

DD file is not supported for DE devices. Hence, on the FDM Device Properties page, the STISWVER [Software Version] is displayed for DE devices, along with other details.

2. If necessary, you can modify the values for Maintenance Notes, Special Instruction, Device Usage, Calibration Status, Calibration Due Date, and Device Health by re-entering/re-selecting the values from the list.
3. To change the device usage state, select any of the appropriate values (Not set, Connected to Process, Spare, Disconnected from Process, and Decommissioned) from the Device Usage list box.
4. To change the calibration status, select any of the appropriate values (Not set, Calibrated or Calibration Required) from the Calibration Status list box.

5. Change the calibration due date by re-entering the value in the MM/DD/YYYY format in the Calibration Due Date text box.

NOTE

Enter a value greater than the current date for Calibration Due Date. An appropriate message appears, if you enter a value in the past.

6. To change the device health, select any of the appropriate values (Not set, Good, Needs Service, Sent to Repair, and Discarded) from the Device Health list box.

 Device Usage	Spare
 Calibration Status	Calibrated
 Calibration Due Date (MM/DD/YYYY)	1/1/1900
 Device Health	Good

7. Click  icon. The Parameters To Download dialog box appears.
8. Click Download to download the values onto the field devices or click Reset to discard the changes and restore the original values.

NOTE

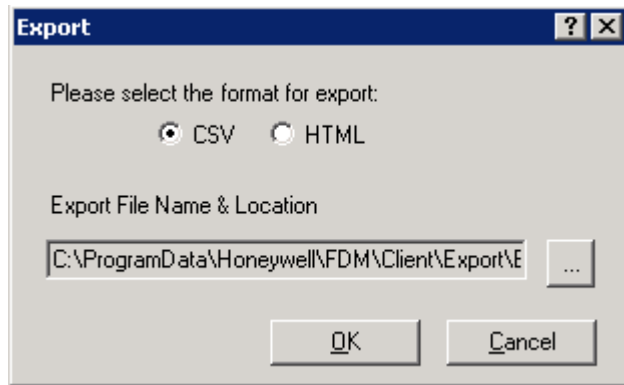
If you change the Device Usage, Calibration State or Maintenance Notes, these values are reflected in the State Information of the Entry Points page.

18.6 Exporting online configuration

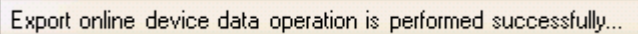
An online configuration of HART, FF, ISA100 Wireless, and DE device can be exported to a file in the CSV (Comma Separated Variable) or HTML format. Using Export option, you can export the summary of device configuration operation.

To export an online configuration, perform the following steps.

1. On the Device Configuration page, click Export under FDM Tasks. The Export dialog box appears.



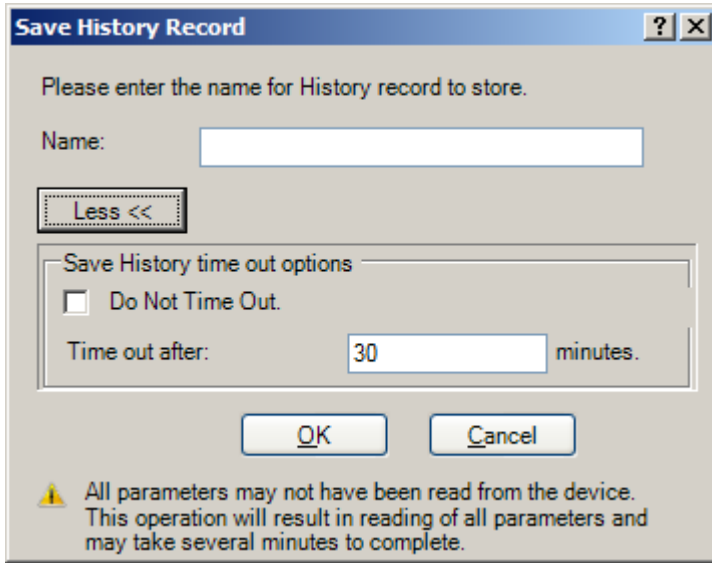
2. Click the required format for export. The Export File Name & Location box displays the name of the exported file and location. To change the name and/or location, click the  button. The Save As dialog box appears.
3. Choose the drive/directory/sub-directory on the FDM Client, where you want to save the file.
4. Type a file name and click Save. The Export dialog box with the updated file name and location appears.
5. Click OK. The following message appears on the status bar of the Device Configuration page.



18.7 Saving history records

To explicitly save the history records of HART, FF, ISA100 Wireless, and DE devices

1. On the device configuration page, click Save History Record or, on the upper-right corner of the device configuration page, click . The Save History Record dialog box appears.



Save History Record

Please enter the name for History record to store.

Name:

Save History time out options

☐ Do Not Time Out.

Time out after: minutes.

 All parameters may not have been read from the device. This operation will result in reading of all parameters and may take several minutes to complete.

NOTE

You must provide the audit trail reason for saving history records.

When Save History Record operation is performed, the parameters which are not already read are read from the device. Therefore, this operation may take some time.

2. Enter an appropriate file name to save history record.
3. If you want to set time out for saving history records, enter the time out in minutes in the Time out after: box. By default, the time out value is 30 minutes.

NOTE

If you do not want to set time out value, select Do Not Time Out check box.

4. Click OK. FDM reads all the parameters from the device and status is as shown in the following message.

Save History is in progress. Please wait... Read 52 of 134 parameters

When the operation is completed, the following message is displayed on the status bar

Save Device History operation performed successfully...

NOTE

- FDM does not accept duplicate names for history records. Ensure that you specify a unique name for each record.
- Depending upon the HART command traffic, load of FIM and WDM on the network, the reading of parameters from the device may be slow. If FDM cannot read all the required parameters from the device in time out value, which is set in minutes, the

operation is aborted and a message is displayed to the user stating Operation Timed Out. It is recommended to re perform the operation again without closing the device configuration page.

- Even if you change any dynamic parameter through Handheld Communicator at device level for HART and ISA100 Wireless devices, it is not saved by Save History Record operation.
- When you are closing the device configuration page, a confirmation message is displayed to remind you to save the changes made to the device using save history operation before closing the device record.

18.8 Saving an online configuration as an offline configuration using DD

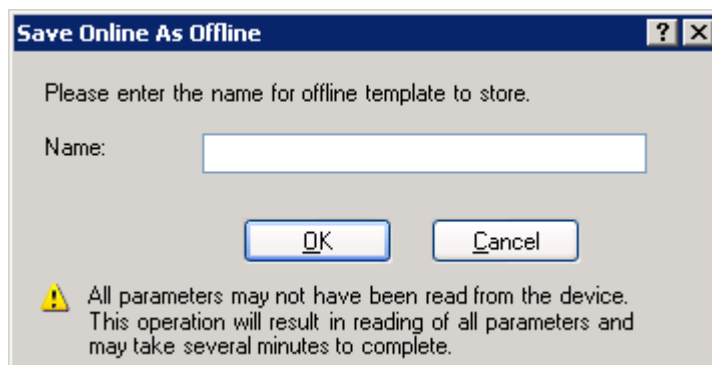
A device's online configuration can be saved as an offline configuration to use this configuration to configure other devices of the same Manufacturer, Device Type and Device Revision.

NOTE

FF and ISA100 Wireless devices do not support Save as Offline Template operation.

To save an online device's configuration as an offline configuration

1. On the device configuration page, click Save as Offline Template. The Save Online As Offline dialog box appears.



NOTE

- You must provide the audit trail reason for saving online configuration as offline configuration.
- When Save As Offline Template operation is performed, the parameters which are not already read are read from the device.
- When you are performing Save as Offline Template, the Enable Dynamic Scanning option under FDM Tasks must not be selected.

- Save As Offline is in progress. Please wait... Read 45 of 63 parameters

Save 'Online as Offline' operation is performed successfully...

- Depending upon the HART command traffic on the network, the reading of parameters from the device may be slow. If FDM cannot read all the required parameters from the device in 10 minutes, the operation is aborted and a message is displayed to the user stating Operation Timed Out. It is recommended to perform the operation again without closing the device configuration page.

NOTE

The download offline configuration feature is currently supported only for HART devices using DD files.

- LAICHANNEL 12.1

AICHANNEL_12_1

Configuration Details

Protocol

HART

Manufacturer

Rosemount_38

Device Type

5300

Device Revision

3

DD Revision

2

Select Configuration

Configuration Name

offline_config_HART

View

Configuration View

View IDs

Select All

	Items	Value	Units	Select

Time Out

Device Timeout (Minutes)

10

Download

Save

Save As

Close

4. Select the DD offline/generic DD offline configuration, from Configuration Name drop-down list.
5. Click View. The details of the DD/generic DD offline configuration appears.
6. If required, you can modify the parameter values. When you change the value of any parameter, the changed parameters turns yellow and Save button is enabled. To display the parameter IDs, select View IDs.
7. Click Save to save the changes.
8. If you had selected the parameters for downloading, at the time of creating the offline/generic offline configuration, the check boxes appears as selected against those parameters. If you want to download other parameters that you had not selected, while creating the offline/generic offline configuration, select the check box corresponding to those parameters. FDM allows you to download the whole set of parameters or a partial set of parameters. Check the Select All check box to select all parameters for downloading.
9. Enter Device Timeout (in minutes) under Timeout panel, before you start downloading the offline configuration.

If the download offline configuration fails in the specified timeout period, the following error message appears.

Device timed out. Please try again.

TIP

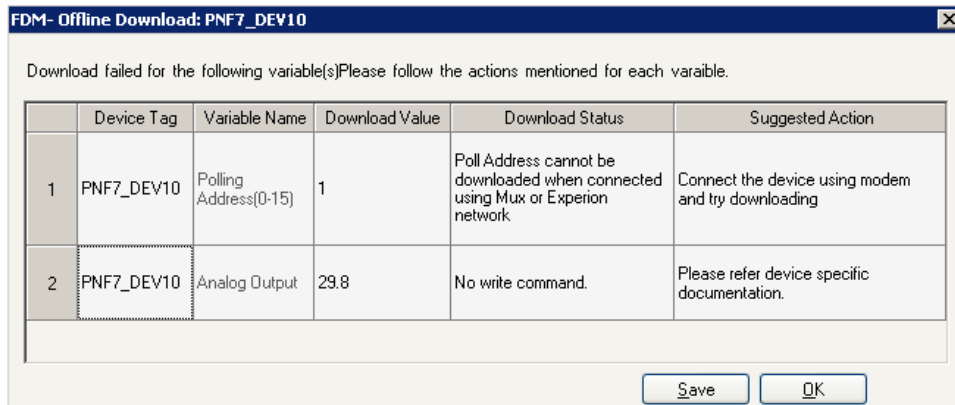
Device time out includes the time to load the device and download the parameters to the device. The time to complete the operation depends on the complexity of the device and the HART network. The user needs to carefully choose the time out period taking these into account.

NOTE

- Ensure that Device Timeout is in the range of 4 to 30 minutes.
- When all parameters are selected and downloaded, only the writable parameters are downloaded. The read only and method editable parameters are not downloaded. They are considered only to validate the correct values of the editable parameters.
- FDM does not allow you to download invalid parameters. These parameters appear in Red color. An appropriate message appears when you try selecting the checkbox corresponding to an invalid parameter.
- If you select a dependent variable for downloading, the corresponding dominant variables are also automatically selected for downloading. An appropriate message appears to this effect.

10. Click Download.

FDM does a validation of the parameters that are selected for downloading. If the validation fails, FDM does not download the offline configuration and the following download status window displays.



The download status window indicates the reason for the failure in validation and the action you need to do. FDM downloads the offline configuration only if the values that are selected for downloading are valid.

The actual downloading of parameters to the device proceeds after the validation succeeds. If the write for one or more parameter fails, then the download status box appears detailing the reasons and suggested actions for the failures. Follow the suggested actions to proceed further.

NOTE

The chances of having a valid offline template are more if the offline template is created from an online configuration using the Save Online as offline feature. This ensures that most parameters have valid values. You can modify this template and download the configuration.

The status bar in the right pane displays the status of the download operation. After the download is complete, the status bar displays Download completed.

NOTE

FDM does not allow downloading some invalid parameters while downloading a HART DD/EDD based offline configuration. For example, changing of poll address.

18.10 Scanning dynamic parameters

Values of certain variables are updated by the field device without any stimulus from the communication network or the user. Such variables are called as dynamic parameters. For example,

- The dynamic parameters for HART devices are PV, SV, TV, and so on.
- The dynamic parameter for ISA100 Wireless devices is PV.
- The dynamic parameters for FF devices (for example, ST800) are state PV, Meter body temperature, and pressure.

After reading the parameter values, FDM does not automatically refresh these values. Using Enable Dynamic Scanning option, parameter values can be refreshed periodically from the device. If Enable Dynamic Scanning is enabled, FDM refreshes any dynamic parameter value being viewed on the current menu every 40 seconds. By default, this option is disabled.

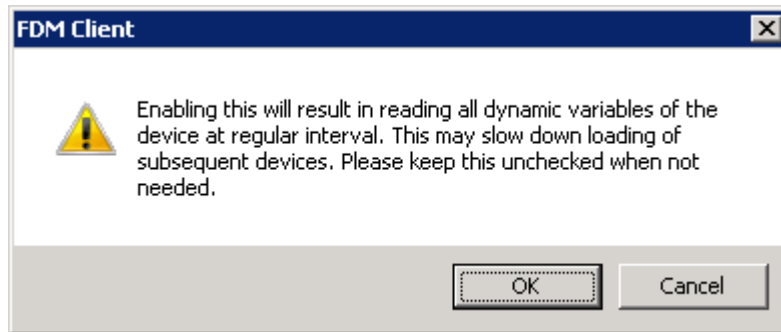
NOTE

The Enable Dynamic Scanning option is available only for DD/EDD configurations.

Enabling this option leads to sending more commands to the device on a periodic basis. Consequently, this increases the HART command traffic on the network. Hence, it is recommended to reset this option when not required, otherwise it affects other device related operations on the same network.

To enable periodic refreshing of dynamic parameters, perform the following steps.

1. On the device configuration page, select Enable Dynamic Scanning under FDM Tasks. The following message appears.



2. Click OK to scan all dynamic parameters of the selected device.

NOTE

The Enable Dynamic Scanning setting does not affect the graphical items update like charts.

DEVICE CONFIGURATION USING FDI PACKAGE

NOTE

FDI Packages are supported only for PROFIBUS PA V3.01 and later devices.

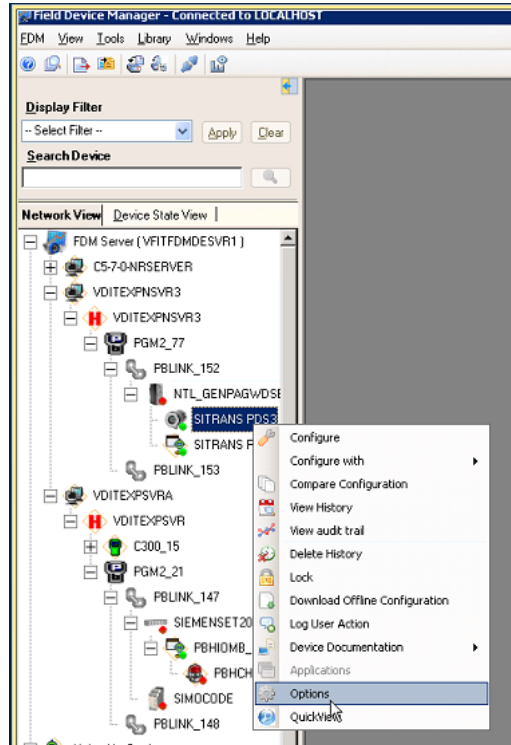
For FDM R500 only device description present in FDI Package is used for device parameterization. All other parts such as User Interface Plug in (UIP), etc., are not used though the entire Package is added to the system.

19.1 Associating Package

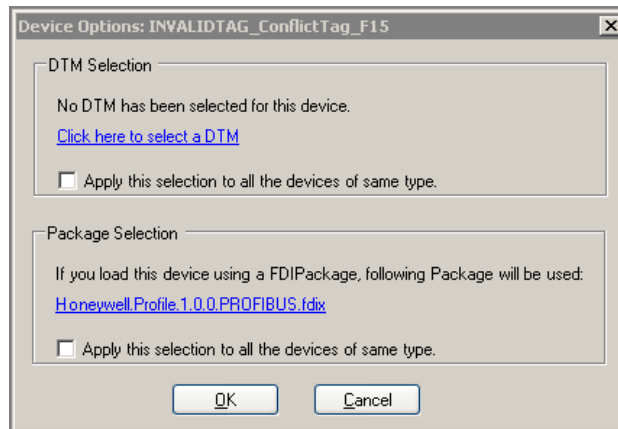
Per FDI protocol, device identity information is compared against FDI package to find a suitable package for a device. If found, the package will be used for configuration. In case of a conflict, a generic package is automatically associated. This generic package has only limited features, and you can only configure standard parameters. However, you can associate a package manually if a suitable package is already added.

To associate a package to a device:

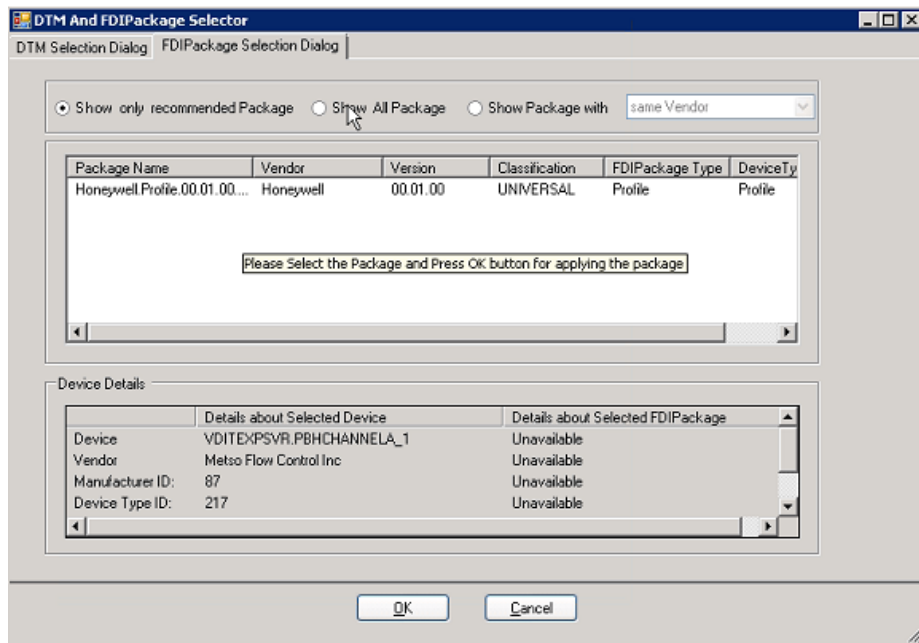
1. In the Network View, right-click the device and click Options.



2. In the ensuing Device Options dialog box, under Package Selection, click the package link displayed with *.fdx extension.



3. In the ensuing FDI Package Selection Dialog, click one of three options to display available packages. The options are:
 - Show only recommended package: Only recommended packages will be displayed. This is the default selection.
 - Show All Package: Displays all packages available for selection.
 - Show Package with: This option enables you to further sort available packages by vendor, device type, or Manufacturer ID.

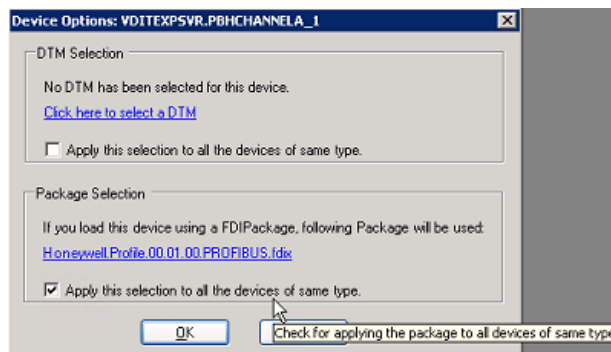


4. Based on your selection, the available packages are displayed with details such as Package Name, Vendor, Version, and so on. Click to select the required package.
5. Click OK.

NOTE

In case of a mismatch between the information read from the device and the one contained in the package, an error message is provided. Acknowledge the message and select the correct package.

6. The Device Options dialog box appears. Select the Apply this selection to all devices of same type option, if it is your requirement.



7. Click OK.

19.2 Configure PROFIBUS PA devices using FDI package

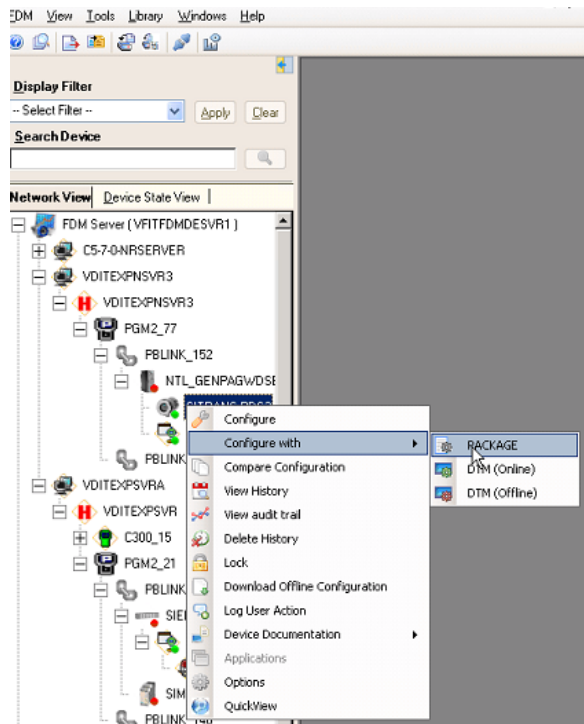
NOTE

Package configuration is supported for PROFIBUS PA devices only.

Honeywell does not ship FDI packages along with FDM. Ensure that FDI package is imported to the system before you begin configuration. In the event that the appropriate FDI package is unavailable, the device is loaded with a Generic Device Package.

To configure a PROFIBUS PA device using FDI package

1. Ensure that the device is displayed in Network View list under Online View.
2. In the Network View list, right-click the required device tag and click Configure with > Package.



NOTE

If you want to load a PROFIBUS PA device using FDI package irrespective of DD/DTM settings, right-click the required device tag and then click Configure with Package.

For FDM Station Maintenance View, the device is always loaded with the default load setting.

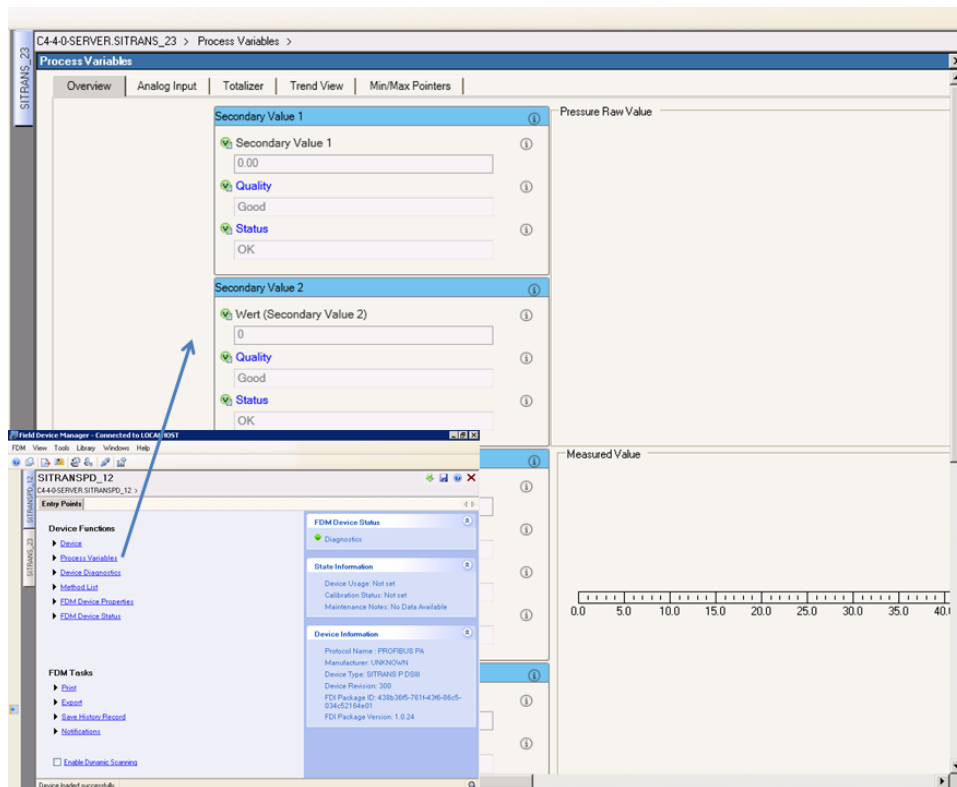
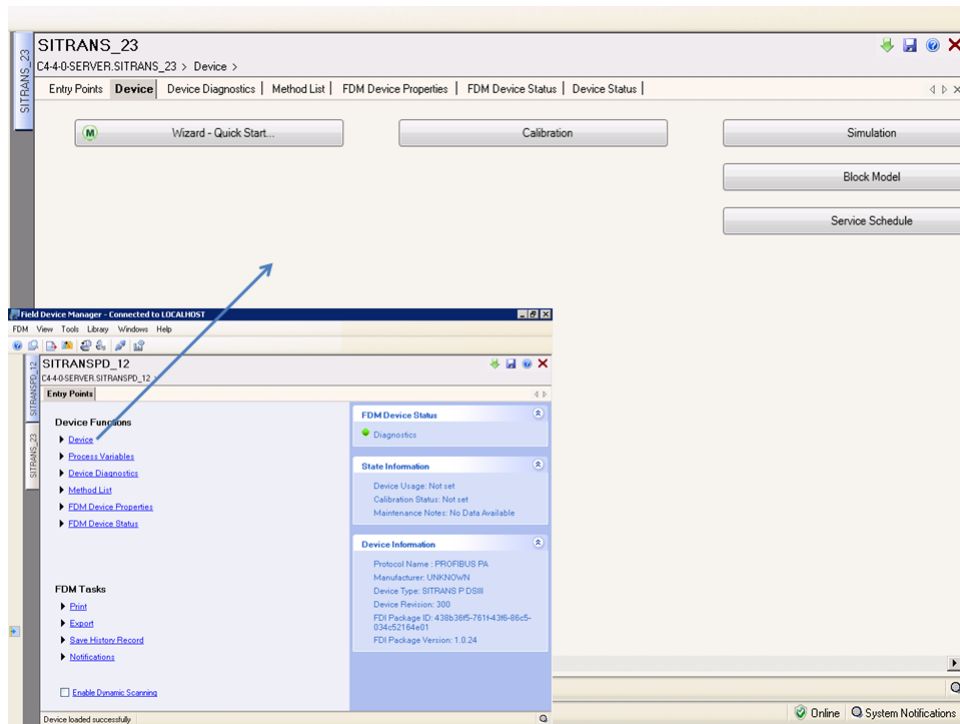
1. The details appear on the Device Configuration page depending on the EDD present in FDI package/DTM. After the parameters are read, the device is loaded successfully.

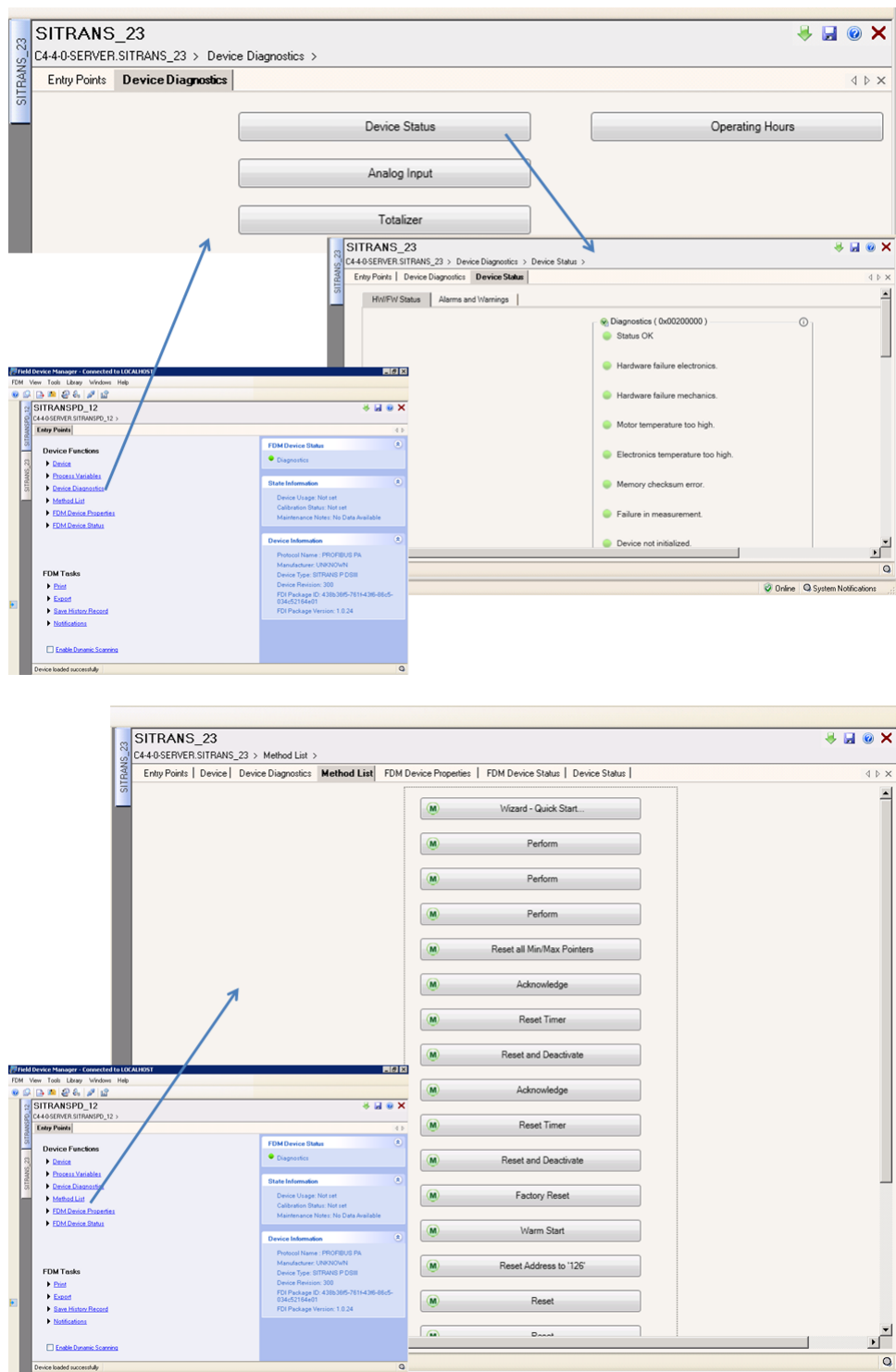
NOTE

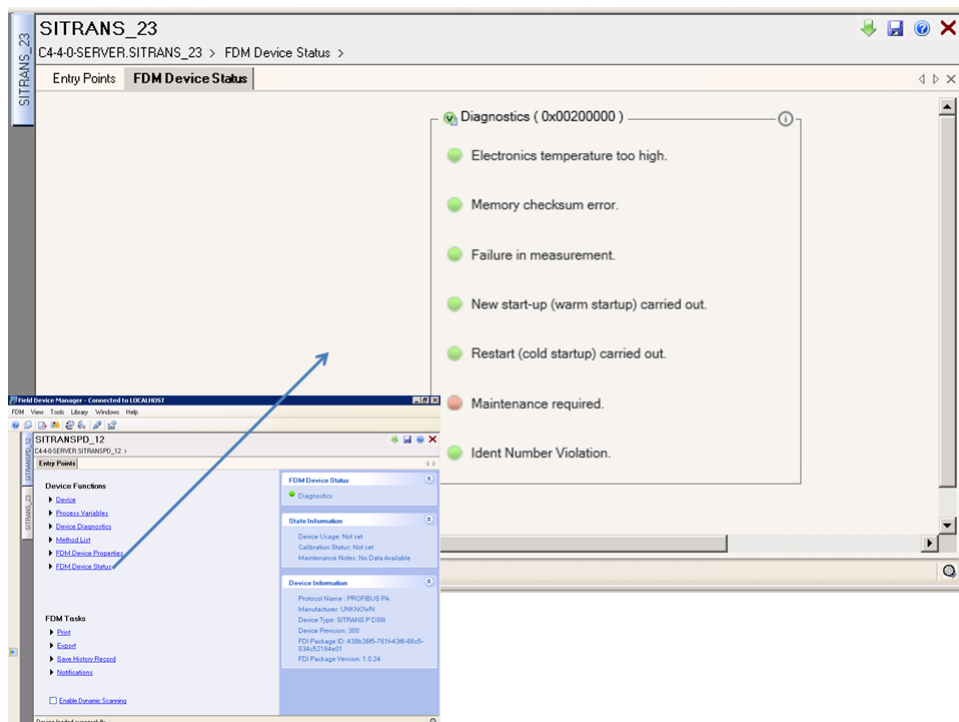
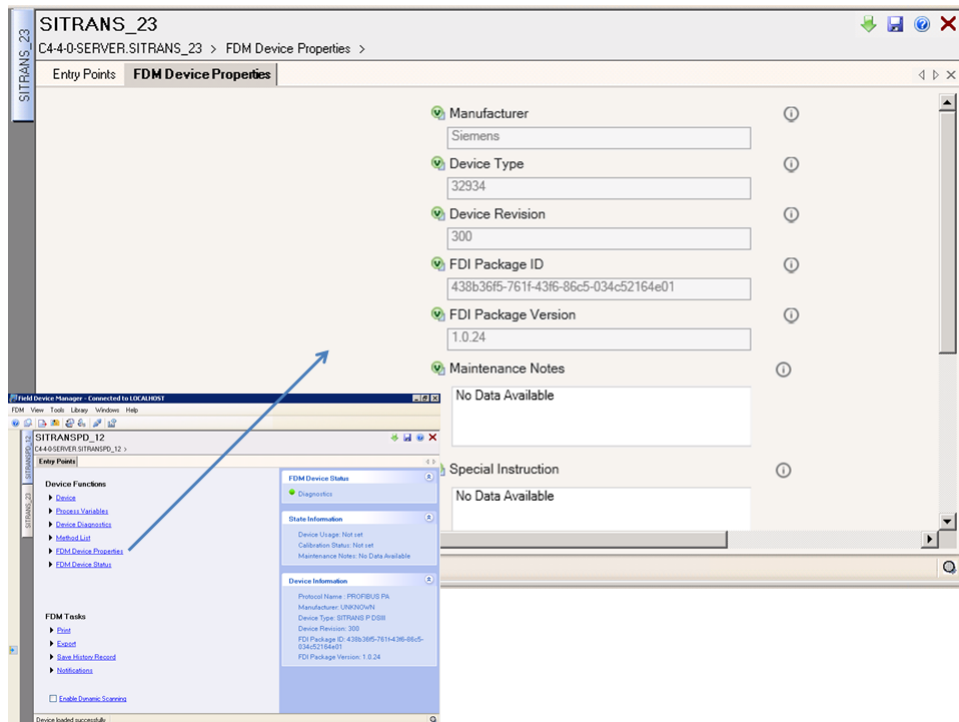
When a device is in the process of loading, the options under Entry Points do not appear for some devices. The options appear only when the device is loaded completely.

For better performance of FDM, it is recommended to close the device configuration page after the configuration activities for a device are completed.

- Under Device Functions, click any link to view all the menus and to edit the parameter values as shown in the following sample illustration.







3. Browse through the different sub-menus and edit required parameters that have write access. The parameter value field turns yellow when you edit the value.
4. After editing the parameter values, click  icon to download the edited parameters values to the field device. The Parameters To Download dialog box appears. Select the parameters you want to download and click Download.
5. Click Close.

The modified parameter values are downloaded to the field devices.

19.3 Monitor PA device status

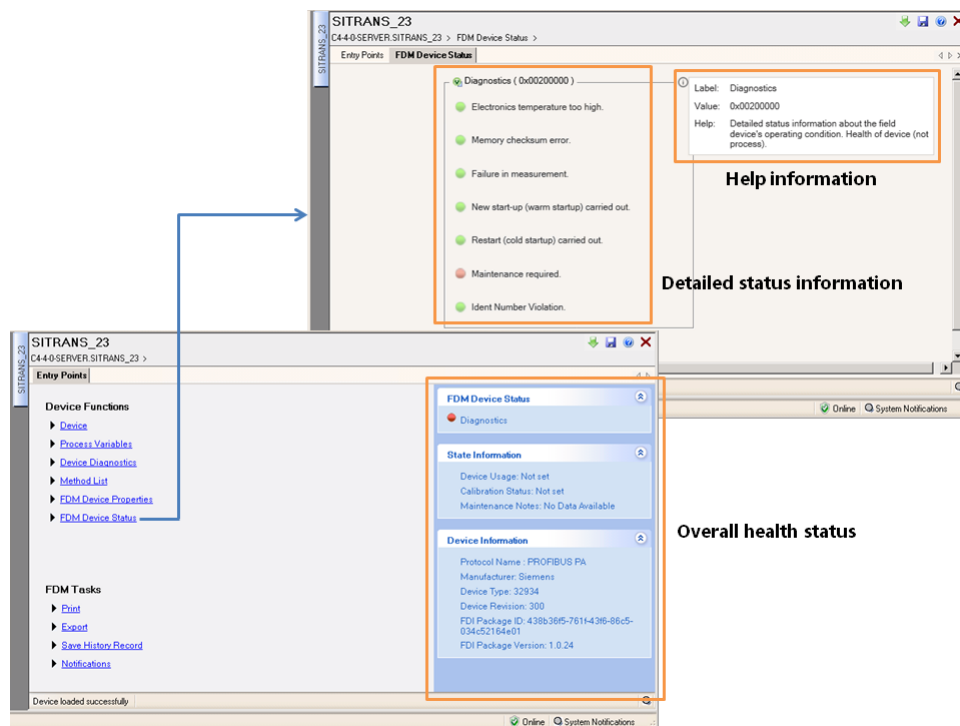
PROFIBUS PA Profile allows hosts to display diagnostic information through parameters like Diagnosis and Diagnosis Extension. FDM Device status provides an indication of the overall diagnostics of the device with guidance of required service actions.

NOTE

FDM Device status supports only classic diagnosis. If device has condensed status enabled, configure it to provide classic diagnosis.

FDM device status menu is different from standard diagnosis root menu available in packages.

On the PA device configuration page, click FDM device status under Device Functions. The FDM Device status page appears.



Diagnosis parameters will have bits as defined in package or will be according to PA profile. Bits will be masked to display only those supported by the device.

If diagnosis extension parameter is defined in the package, more detailed diagnostic information is provided.

DE DEVICE CONFIGURATION

DE device configuration is supported in FDM using a template-based approach. FDM subscribes to TPN Server as an OPC client. FDM shows only instrument-specific parameters of DE devices.

The following table lists the tasks that can be performed for DE devices.

If you want to...	Refer to the section...
Configure a DE device	“Configuring a DE device”
Editing DE specific system settings	“Editing DE specific system settings”
Monitor the process variables	“Monitor process variables”
Monitor the DE device status	“Monitor DE device status”
Monitor the device information	“Monitor device information”
Edit device properties	“Editing device properties ”
Save history records	“Saving history records ”
Export device history records	“Exporting online configuration ”
Compare configuration	“Comparing configuration”

20.1 Configuring a DE device

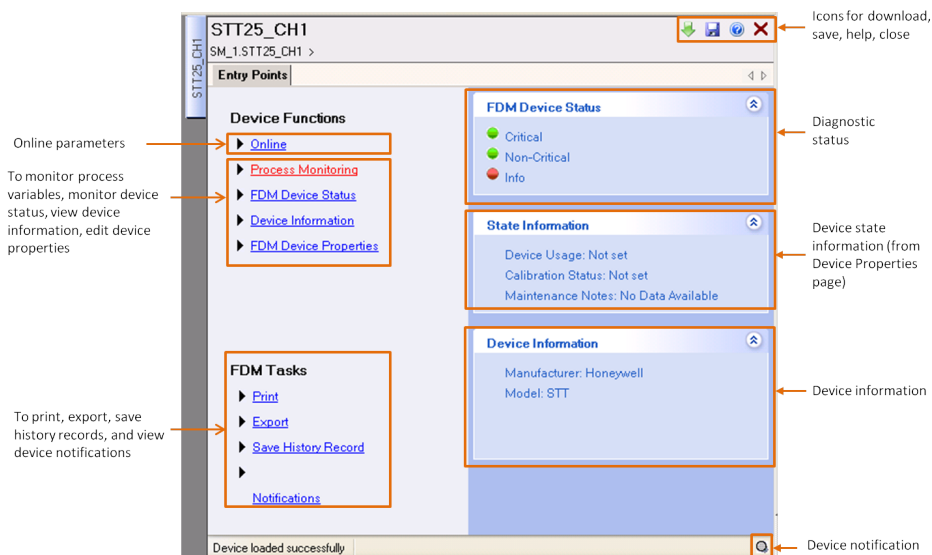
To configure a DE device

1. Ensure that the device is displayed in the Network View list under Online View.
2. In the Network View list, right-click the required device tag, and then click Configure.

TIP

You can also open the device configuration page by double-clicking the device in the Network View list under Online View.

The details appear on the Device Configuration page.



The following table provides the brief description about device configuration page entry points.

Entry point	Description
Online	This view provides a consolidated view of smart instrument configuration parameters, process operational parameters, dynamic parameters, and so on.
Process Monitoring	This view provides the graphical view (trend and gauge chart) for Process Variables (for example PVRAW)
FDM Device Status	This view provides the detailed diagnostics of DE devices
Device Information	This view provides the device information (for example Serial number, transmitter status, LCN node, UCN node, slot number and so on.), and also images of the device family
FDM Device Properties	This view allows you to edit the device properties such as device information, maintenance notes, and so on.
FDM Tasks	To perform different tasks like print, export configuration, save history records, and view device notifications

After the parameters are read, the device is loaded successfully.

If Device autolock feature is enabled and a device configuration page is open when the device's autolock timer is about to expire (5 minutes before the end of the autolock timeout interval), a message appears in the lower right side of the page. The autolock timeout interval can be extended from a range of 10 to 60 minutes. Click this message, if you want to extend the autolock timer.

If you don't want to extend the timer, ignore the message and the device is locked automatically when the timer expires. The reminder message is displayed only to the users with Write Parameter privilege.

If you are viewing a device configuration page and an autolock reminder appears for a different device, that device's tab name turns red which indicates that a reminder message is being displayed for that device.

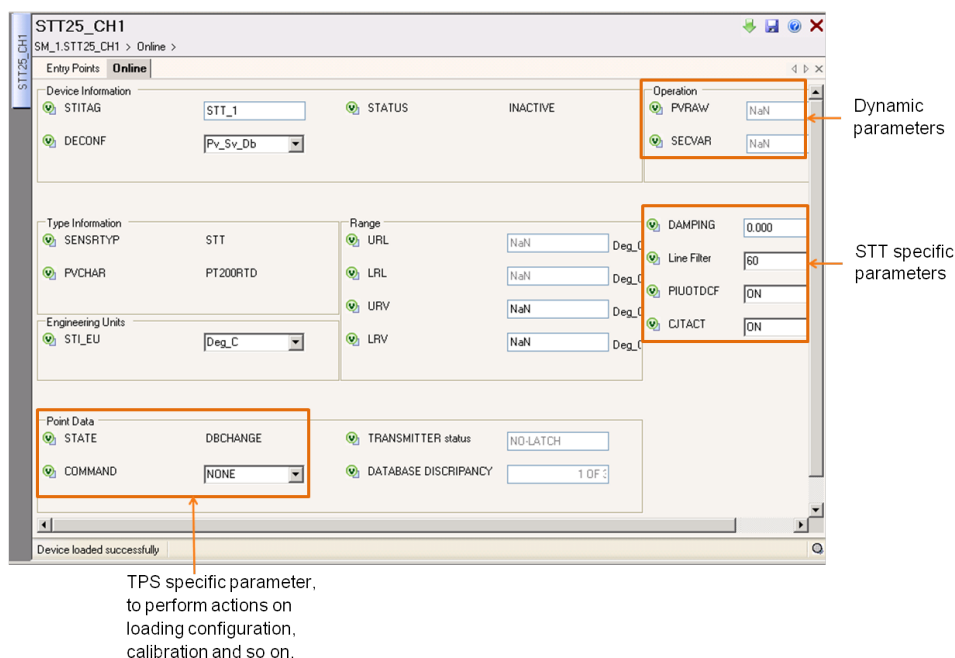
NOTE

When a device is in the process of loading, the options under Entry Points do not appear for some devices. The options appear only when the device is loaded completely.

The following procedure is just an example.

3. On the device configuration page, click Online.

This Online page is displayed based on device types, which are available and supported in the TPS system. This view also provides a consolidated view of smart instrument configuration parameters, process operational parameters, dynamic parameters and so on.



FDM supports Multi Variable Transmitter, which has separate PV slots configured in TPS as in the following image.

In the TPS system, a multi variable transmitter is physically connected to one PV slot (called as base slot) and configuration requires additional contiguous slots depending upon the number of PVs. FDM shows multi variable transmitter as a single device through TPS configuration, since all these slots belong to a single physical device.

The Online view has different tabs for each PV and these tab pages are dynamically displayed based on the number of PVs configured.

NOTE

- When an online page is opened for a multi variable transmitter and if a PV slot is deleted in the TPS system, you must reopen the configuration page to reflect these changes.
- You can change the configuration of a device only if it is unlocked.
- Ensure that a unique STITAG is entered in the system for all DE devices.
- If the DAMPING parameter is configured for the transmitter, the STI IOP adjusts the entered value to one of the acceptable damping values for the appropriate transmitter type. For more information about acceptable damping values for different transmitter types, refer to the Smartline Transmitter Integration Manual in the TPN/TPS bookset.
- By default, the Engineering Units (STI_EU) are displayed based on the configuration of device (single/multi variable device) in TPS. If you want to change the units for slots with SENSRTYP of SPT_DP, SPT_AP, SPT_GP, or STT from the Native Window, select the preferred and appropriate STI_EU.
- You cannot modify the state (STATE parameter) of the smart transmitter in FDM.
- The SECVAR parameter value is visible only if DE device is configured as Pv_Sv_Db mode in DECONF parameter. For more information about different modes, refer to the Smartline Transmitter Integration Manual in the TPN/TPS bookset.

4. Select the parameter to modify the value. The parameter value field turns yellow when you modify the value. The parameter values are updated dynamically as per the actual values of the device in the field. If required, modify the values for the configurable parameters.

5. Click  icon to update the modified parameters values to the TPS system. The Parameters To Download dialog box appears.
6. Click Download. The modified parameters values are downloaded to the TPS system and they are ready for download from the system to field device.
7. To download the modified values to field devices, select the Download DB from the COMMAND drop- down list and then click . The modified parameter values are downloaded to the field devices.

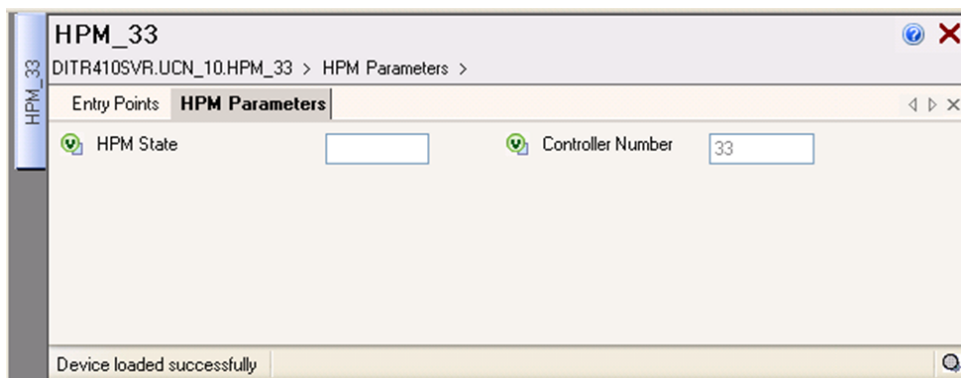
NOTE

- For better performance of FDM, you must close the device configuration page after the configuration activities for a device are completed.
- For some devices to edit device parameters, the hardware device lock (if present in device) should be disabled.
- If you select any command from the COMMAND list, the same command status is retained after downloading the edited parameter to the device. But, the command status should be displayed as None after the download is complete.

TIP

When you right-click STIM/HPM and then click Configure, the corresponding configuration page appears. To view the STIM/HPM parameters, click the corresponding parameters link in the Entry Points page.

For example, to view HPM parameters, click the HPM Parameters link. The following page appears with read- only parameters and you cannot configure those parameters.



20.2 Editing DE specific system settings

You can edit DE specific system settings such as, device health polling rate, process lock polling rate, dynamic discovery polling rate, NIM PARSEC Limit, and so on in the following ways.

- Settings dialog box: It is applicable for all UCNs at system level. For more information about editing DE specific system settings, refer to the sections [“Customizing the network settings” on page 102](#) and [“Customizing the health settings”](#).
- UCN configuration page: It is applicable only to the specific UCN.

To edit DE specific system settings using UCN configuration page

- If you want to change the polling rate (in seconds) of device health, device discovery, process lock, NIM PARSEC, and device configuration at UCN level as per requirement, right-click UCN, and then click Configure. The corresponding UCN configuration page appears. Click the UCN parameters link on the Entry Points page.

The screenshot shows the 'UCN_10' configuration window with the 'UCN Parameters' tab selected. The parameters are as follows:

Parameter	Value	Unit
Device Health polling Rate	30	Sec
Process Lock polling Rate	30	Sec
Dynamic Discovery polling Rate	14	Sec
Device configuration polling Rate	5	
NIM PARSEC LIMIT	400	
UCN State	FAILED	
UCN Number	10	

A status bar at the bottom indicates 'Device loaded successfully'.

These parameters are only applicable to the UCN whose parameters are modified and do not affect the polling rate of other UCN's in the network hierarchy. By changing the polling rate for these parameters, improves system performance and response time. These parameters are writable parameters, which can be downloaded to the system. After downloading these parameters, the system polls the device health/device discovery/process lock and so on with the new polling rates.

NOTE

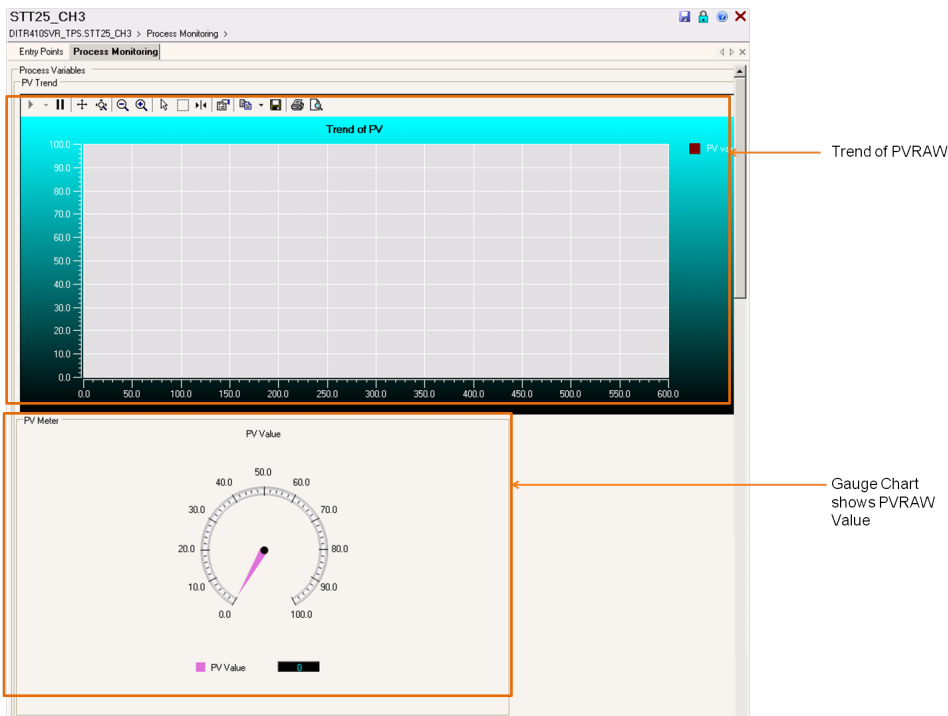
- When a DE device configuration page opened, it is not recommended to update the device configuration parameters at UCN level.
- The UCN configuration settings are not removed from the UCN configuration page even if you delete the network (Example, TPS_1) from Server Management Tool. And also, if you re-configure the TPS network with the same name (TPS_1), the UCN configuration page settings are not changed.
- TPS system will be loaded, if you modify the UCN parameters to lower value from the available range.

20.3 Monitor process variables

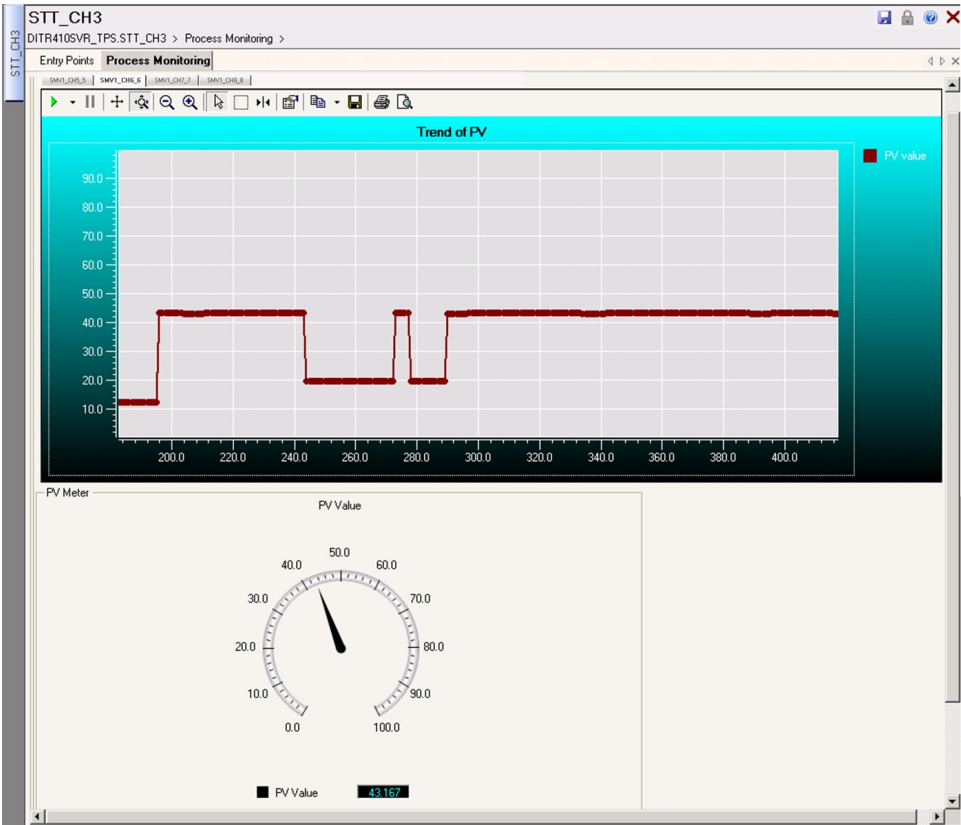
FDM assists in monitoring the graphical view for process variables (for example, PVRAW). You can view different types of chart like trend and gauge chart.

To view the graphical representation for process variables, on the device configuration page, click Process Monitoring under Device Functions. The Process Variables page appears.

The following illustration shows the PV trend and gauge chart.



For multi variable transmitter, these charts are displayed for each PVRAW (configured PV slot).



NOTE

- You can view the process variables only if device in ACTIVE state without any error.

- PV value, which is displayed in the PV meter is in the percentage (%) of Db.
- If the PV value is NaN, the PV meter does not display the needle and the trend of PV is not plotted.

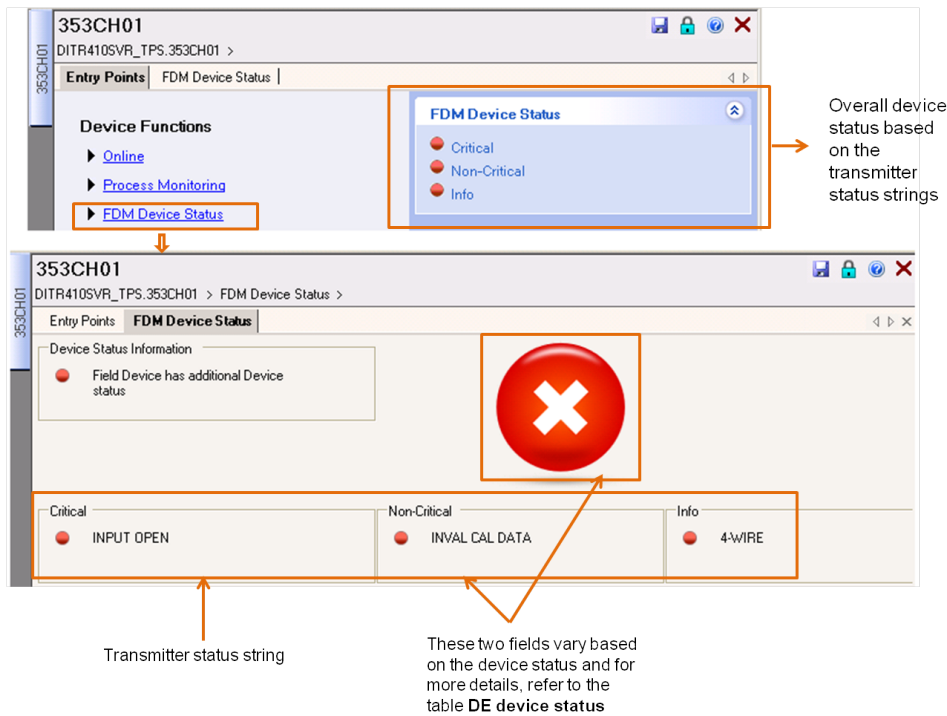
20.4 Monitor DE device status

FDM assists in monitoring the detailed diagnostics of DE devices. In the FDM Network View, a DE device health status is indicated in green or red based on the health condition.

However, to view the detailed diagnostics of the DE device, on the DE device configuration page, click FDM Device status under Device Functions. The FDM Device status page appears. The DE device status is categorized into the following groups.

- Critical
- Non-Critical
- Info

The overall device status shows only transmitter status strings (with red LED icons) that are set in the DE device instead of showing all the status strings supported by the device type. The following image has only one transmitter status string Info with red LED icon, and it does not have Critical and Non-Critical status strings. Hence, the overall device status shows Info is in red LED icon and Critical and Non-Critical are in green LED icons.



The device status shown for Multi Variable Transmitter is cumulative status for all the slots.

Table 1: DE device status

Icon	Device status	Additional device status information
	Unhealthy	Critical, Non-Critical, Info
	Healthy	Non-Critical, Info
	Healthy	Info
	Healthy	No additional status

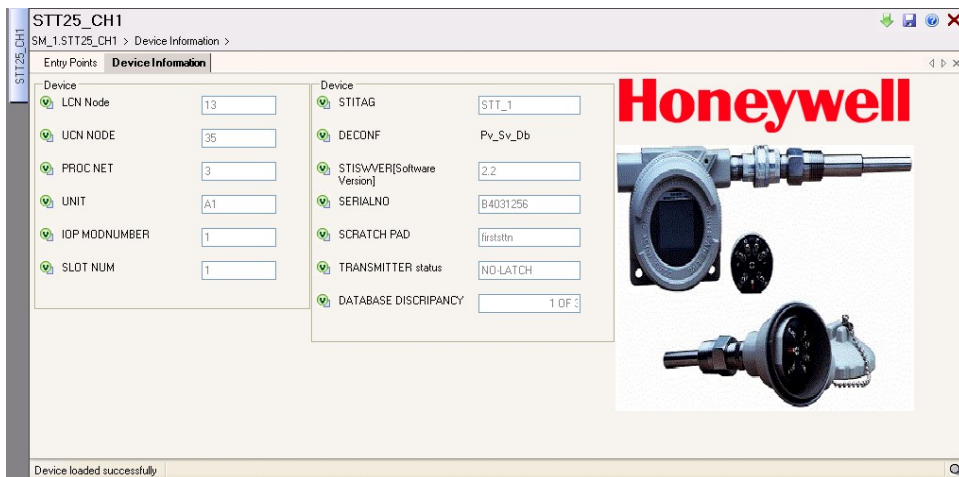
NOTE

The device health icon in the network view turns to red only if the device status is Critical. If the device status is Non-Critical or Info, then the device icon in the network view turns to green.

20.5 Monitor device information

FDM assists in monitoring the device information such as serial number, transmitter status, LCN node, UCN node, slot number and so on., and also images of the device family.

To view the device information, on the device configuration page, click Device Information under Device Functions. The Device Information page appears.



STT25_CH1
SM_1.STT25_CH1 > Device Information >

Entry Points: **Device Information**

Device

- LCN Node: 13
- UCN NODE: 35
- PROC NET: 3
- UNIT: A1
- IOP MODNUMBER: 1
- SLOT NUM: 1

Device

- STITAG: STT_1
- DECONF: Pv_Sv_Db
- STISWAVER[Software Version]: 2.2
- SERIALNO: B4031256
- SCRATCH PAD: firstattn
- TRANSMITTER status: NO-LATCH
- DATABASE DISCREPANCY: 1 OF 3

Honeywell

Device loaded successfully

NOTE

FDM shows only 8 characters of SERIALNO, which is in line with TPS system.

COMPARING CONFIGURATION

Using the compare configuration feature, you can compare either device data of two different devices belonging to the same device type or device data of the same device history. The compare configuration is supported for the DD/EDD based devices (HART, FF, and ISA100 Wireless) and DE devices. In case of DE device, this feature is supported for both single variable and multi variable DE devices. Additionally, for Fieldbus and ISA 100.11a Wireless devices with multiple blocks of the same type, different combinations of identical blocks can be compared.

NOTE

- FDM does not support import and comparison of MCToolKit device history records for multi variable device and Manew3000 device.
- For multi variable DE devices, the compare configuration feature allows you to compare all device types and their parameters.
- If the device is locked, the compare configuration page is read-only and you cannot modify it.
- For disconnected nodes, only device history can be compared using this feature.

The compare configuration is allowed for the following combinations.

Supported combinations	Devices	
	HART/FF/ISA100/PROFIBUS Wireless	DE
For online devices Current - Current (same device type) Current - History History - History	Supported	Supported (for both single variable device and multi variable device) Attention For a multi variable device, you can compare configuration with another multi variable device only.
Current-History/MCToolKit History (Here, MCToolKit History indicates that the device history is imported from MCToolKit to FDM) For more details about importing MCToolKit history to FDM, refer to the section “Importing DE device configuration history from MCToolKit into FDM” History-MCToolKit History MCToolKit History-MCToolKit History	Not supported	Supported (only for single variable device)
For disconnected nodes History - History	Supported	Supported

To compare the device configuration

1. Select the device from the Network View list.
2. Right-click the device and then click Compare Configuration. The Compare Configuration page appears. The selected device name is displayed in the Device Tag box.

NOTE

- To describe the functionality, device 1 is referred to as the base device.
- Device autolock in Compare Configuration: If the device autolock feature is enabled for a device loaded in the compare configuration page and the device's autolock timer is about to expire (5 minutes before the end of the autolock timeout interval), a message appears in the lower right side of the page. The autolock timeout interval can be extended from a range of 10 to 60 minutes. Clicking this message allows you to extend the autolock timer. If you don't want to extend the timer, ignore the message and the device is locked automatically when the timer expires. The reminder message is displayed only to the users with Write Parameter privilege.

3. Under Selected Device, select the history record's name as Current or select the date and time of a previously saved configuration of the base device.

NOTE

Only if the base device configuration is Current, then it can be edited.

The connection status for the selected device is displayed in Connection Status.

For DE devices, the Record Source is displayed as TPS or MCToolKit based on the Record Name selection.

- The record status as TPS indicates that the history record is imported from FDM older history files.
 - The record status as MCToolKit indicates that the history record is imported from MCToolKit.
4. Under Compare with, select the device from the Devices list, for which the base device configuration needs to be compared.
 5. Select the required saved history record name for the device that you want to compare with. If Current is selected, then the present configuration of the device is loaded. For DE devices, it also displays the Record Source as TPS or MCToolKit based on the Record Name selection.

6. Click Compare to compare the selected device configuration.

If you are comparing...	Then...
HART device	The device details appears as in the following image.

Items	ST3000:Current		ST3000H:Current	
	Value	Unit	Value	Unit
Meter bdy s/n	1		1	
Universal rev	5		5	
SV Unit	degC		degC	
AO	0	mA	0	mA
Software rev	1		1	
Fld dev rev	1		1	
AO Alm typ	Hi		Hi	
PV Xfer frctn	Linear		Linear	
Model	ST3000		ST3000	
Num req preams	1		1	
Dev id	0		1	

FF/ISA100 Wireless device	The Select Blocks to compare dialog box appears. You can compare different block instances from the same block.

Items	TempDI_01:Current		C1_TE_03/01/07/2014 14:26:01 HSA	
	Value	Unit	Value	Unit
Temperature DI BID	Channel 2: Temperature DI BID		Channel 3: Temperature DI BID	
Mode Permitted				
DDS	☒		☒	
Auto	☒		☒	
Mode Target	Auto		DDS	

Select the check box for the block type and select the block instances that you want to compare, and then click OK. The device details appear as in the following image.

Items	TempDI_01:Current		C1_TE_03/01/07/2014 14:26:01 HSA	
	Value	Unit	Value	Unit
Temperature DI BID	Channel 2: Temperature DI BID		Channel 3: Temperature DI BID	
Mode Permitted				
DDS	☒		☒	
Auto	☒		☒	
Mode Target	Auto		DDS	

If you are comparing...

Single variable DE device

Then...

The device details appear as in the following image.

Compare Configuration

Selected device:

Device Tag: ST3000_CH4

Connection Status: Online

Record Name: Current

Record Source: Tps

Compare with:

Devices:

DITR4105VR_31CH86
DITR4105VR_31CH87
DITR4105VR_31CH98
DITR4105VR_31CH99
DITR4105VR-ST3000_CH4

Connection Status: Online

Record Name: 3.32:52-MCT_ST3_Ch4_11012007180252

Record Source: MCToolKit

Compare

Items	ST3000_CH4:Current			<<	ST3000_CH4:11/01/2007 23:32:52-MCT_ST3_Ch4_11012007180252		
	Value	Unit			Value	Unit	
DECONF [Bus Type]	Pv_Srv_Db				Pv		
DAMPING	0				0		
COMMAND	NONE						
STATUS	INACTIVE						
UNIT	A1						
STTAG [Tag ID]	ST3_Ch4				ST3_Ch4		
STISWVER[Software Version] [Model N 4.2					4.2		
STI_EU [PV Units]	PSI				InH20		
STATE	LOADCOMP						
SLOT NUM	4						
SERIALNO [Serial Number]	46428447				4642844700		
SENSRTYP [Sensor Type]							

Reset

Download

Close

Multi variable DE device

In case of comparison of MCToolKit device history, you can compare all different slots of MVT device.

The Select Blocks to compare dialog box appears.

Select the check box for device type that you want to compare, and then click OK.

Compare Configuration

Selected device:

Device Tag: SMV1_CH5

Connection Status: Online

Record Name: Current

Record Source: Tps

Compare with:

Devices:

DITR4105VR_TPS_33CH03
DITR4105VR_TPS_33CH08
DITR4105VR_TPS-SMV1_CH5

Connection Status: Online

Record Name: 09/22/2014 16:18:21-MV1_HIST1

Record Source: Tps

Compare

Select Blocks to compare

Block Type	DITR4105VR_TPS-SMV1_CH5:Current	DITR4105VR_TPS-SMV1_CH5:09/22/2014 16:18:21-MV1_HIST1
☒ SPT-OP	SMV1_CH5_5	SMV1_CH5_5
☒ SPT-AP	SMV1_CH6_6	SMV1_CH6_6
☒ STT	SMV1_CH7_7	SMV1_CH7_7
☒ SPM	SMV1_CH8_8	SMV1_CH8_8

Reset

OK

You can expand or collapse the device types to view the parameter details.

The column on the left side (Device 1) displays the configuration for the base device. The column on the right side (Device 2) displays the configuration of the device that is being compared with the base device configuration.

The following table describes the different color indication.

Honeywell

- 276 -

Color indication	Description
Blue	If the parameter value is different between device 1 and device 2, the respective cells are indicated in blue in both the Value columns and << (copy) is enabled.
Yellow	If values are copied from device 2 to device 1 by clicking << button, the respective cell is indicated in yellow for the modified values.
Pink (Only for DE device)	If parameters of device 1 (imported from TPS) are not applicable to the parameters of device 2 (imported from MCToolKit) or vice-versa, the respective cell for that parameter is indicated in pink.

NOTE

- While comparing two configurations, only if the base device (left side) configuration is Current, then it can be edited. Consequently, only the << (copy) button is enabled for parameters where the values are different.
- When the base device configuration is Current, then you can change the values manually as well.
- While comparing parameter values of two devices, both with historical date and time, you can only view the parameters.
- While editing values of certain parameters either manually or through the << (copy) button, you may be prompted with some warning or pre/post edit actions. Follow the steps as directed.
- For Multi variable DE device, the Compare Configuration page and Print page does not display the Device Information parameters (such as LCN Node, UCN NODE, STITAG, and so on) and device status (critical, info, and non-critical) information.

If you have copied some parameters from device 2 configuration to the base device or modified any parameter values in the base device, the Reset and Download buttons are enabled.

7. To download the modified parameters to the device (HART/FF/ISA100/PROFIBUS Wireless),
 - a. Click the Download button. The Parameters To Download dialog box appears.
 - b. Click Download. The modified parameters values are downloaded to the device.
8. To download the modified parameters to DE device,
 - a. Click the Download button. The Parameters To Download dialog box appears
 - b. Click Download. The modified parameters values are downloaded to the TPS system and they are ready for download from the system to field device.
 - c. To download the modified values to field devices, select the DNLOADDB from the COMMAND drop- down list and then click Download in the Compare Configuration page.

The modified parameter values are downloaded to the DE devices

NOTE

To reset the values without downloading the copied parameters, click the Reset button.

DEVICE CONFIGURATION USING DTM

Calibration is a feature of a device, which is also available through the device specific DTM. You must first open the device configuration through DTM and then use Calibration methods which are available on the DTM. If no calibration methods are available, then you cannot do any calibration on that particular device.

NOTE

- FDM does not support configuration of ISA100 Wireless devices using DTM.
- For few device loaded with DTM, if it is locked and moved to disconnected nodes, the entry points are not disabled in the device configuration page. In this scenario, ensure to close device configuration page and reload it again.

22.1 Selecting DTM to device

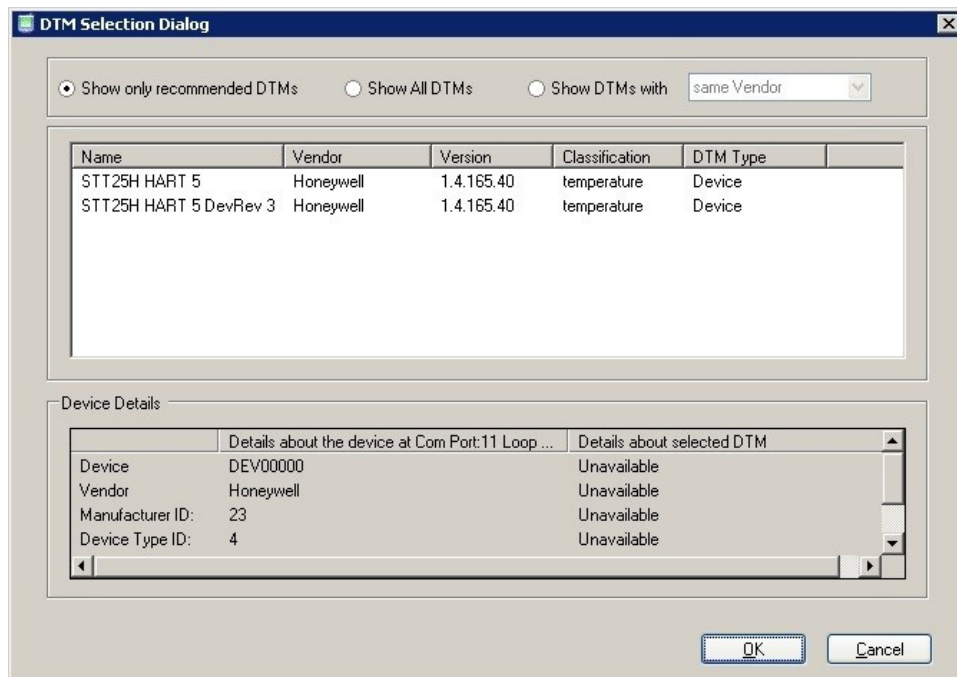
Using the Options shortcut menu, you can select a DTM any time and use it later. You can also change the selected DTM if required.

To select a DTM for a device

1. Right-click the device for that you want to select the DTM and then click Options. The Device Options dialog box appears.



2. Click Click here to select a DTM link under DTM Selection. The DTM Selection Dialog appears.



This dialog has the following options.

- Show only recommended DTMs: When you click this option, the recommended DTMs are listed based on the Manufacturer, device types, and protocols for the current device.
- Show All DTMs: When you click this option, all the DTMs are listed, which are available in the DTM library irrespective of Manufacturer or protocol.
- Show DTMs with: When you click this option, the DTMs are listed based on the selected value from the drop-down list for the current device. You can filter based on the Same Vendor, Same Device Type, and Same Protocol.

NOTE

FDT/DTM specifications do not support comparing the revision level of the device against the supported revision level of the DTM. Therefore, ensure to take care of this to avoid mismatches.

3. Select the necessary DTM and then click OK. The selected DTM appears in the Device Options dialog box.



4. If you want to use the selected DTM only to the selected device, then click OK or if you want to use the selected DTM to all devices of same device type, select Apply this selection to all the devices of same type check box and then click OK.
5. If you want to change the previously selected DTM, click the selected DTM link under DTM Selection. The DTM Selection Dialog appears.
6. Select the necessary DTM and then click OK. The changed DTM appears in the Device Options dialog box.
7. Click OK to assign the DTM.

22.2 Loading a device using DTM (online mode)

You can configure a device with DTM using online DTM configuration. In this mode, the DTM communicates with the field device that has to be configured.

NOTE

If a device has both DD and DTM and if you want to load a device using DTM, ensure that the device is loaded using Load Using DTM setting.

To load a device using DTM (online mode)

1. Ensure that the device is displayed in Network View list under Online View.
2. In the Network View list, right-click the required device tag and click Configure. The device is loaded using Configure with DTM setting.

TIP

You can also open the Device Configuration page by double-clicking the device in the Network View list under Online View. It loads a device with the default setting.

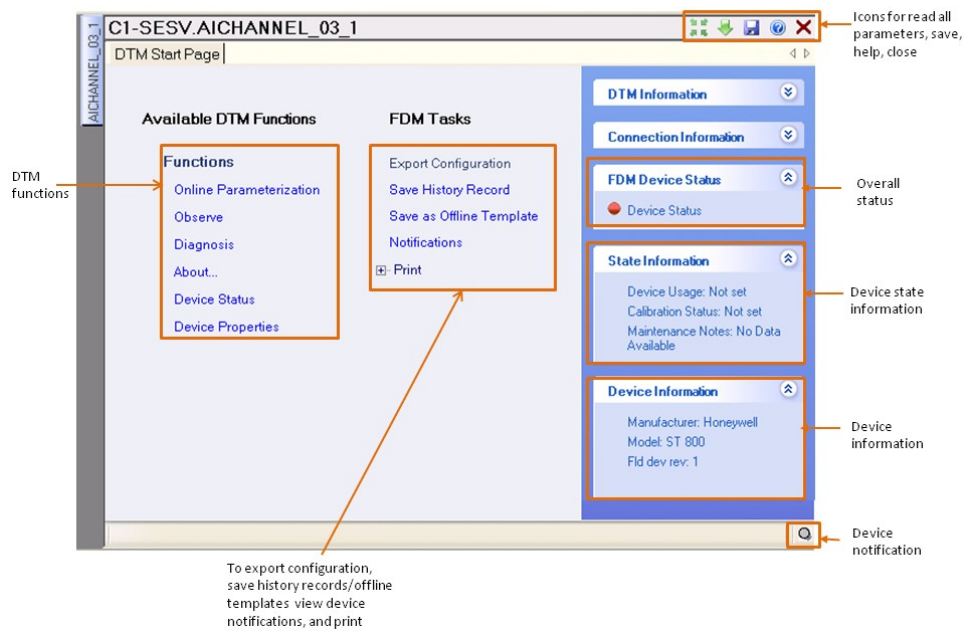
If you want to load a device using DTM irrespective of DD/DTM settings, right-click the required device tag and click Configure with > DTM online.

For Station Maintenance View, the device is always loaded with the default Load Setting.

If you have selected to load a device using DTM for the first time and if DTMs are available in the DTM library for the selected device, then the DTM Selection Dialog appears.

If the selected device has multiple DTM versions, then these versions are listed in the DTM Selection Dialog.

3. Select the appropriate DTM and click OK. The DTM configuration page appears.



NOTE

- If you are loading a device using DTM for which the DTMs are not installed, then the following message appears.



- Click OK
- Install the required DTM for the selected device or change the settings to load the selected device using DD/EDD.
- If you want to change the DTM, refer to section [“Selecting DTM to device”](#).
- You cannot load a device using DTM under the following conditions.
 - When the device is process active in Experion.
 - When the device is already loaded using DTM in other clients.
- The diagnostic information of the loaded device is displayed under FDM Device Status. It is applicable for HART and PROFIBUS devices connected to any network if it is loaded with DTM.
- You can view Device Properties under Available DTM Functions only when you open configuration page using DTM online mode.
- Some DTMs may take considerable time to load and become usable as per the nature of FDT/DTM technology.
- Make sure that the RIO's DTM is launched before configuring IOMs under RIOs using DTM.

22.3 Loading a device using DTM (offline mode)

You can configure a DTM offline to create offline DTM configurations. Here, the DTM works in offline mode and does not communicate with any device. The physical connection between the device and DTM is not established on the device configuration page, till you make it online.

NOTE

If a device has both DD and DTM and if you want to load a device only using DTM, ensure that the device is loaded using Load Using DTM setting.

To load a device using DTM (offline mode)

1. Ensure that the device is displayed in Network View list under Online View.
2. In the Network View list, right-click the required device tag and click Configure. The device is loaded using Load using DTM setting.

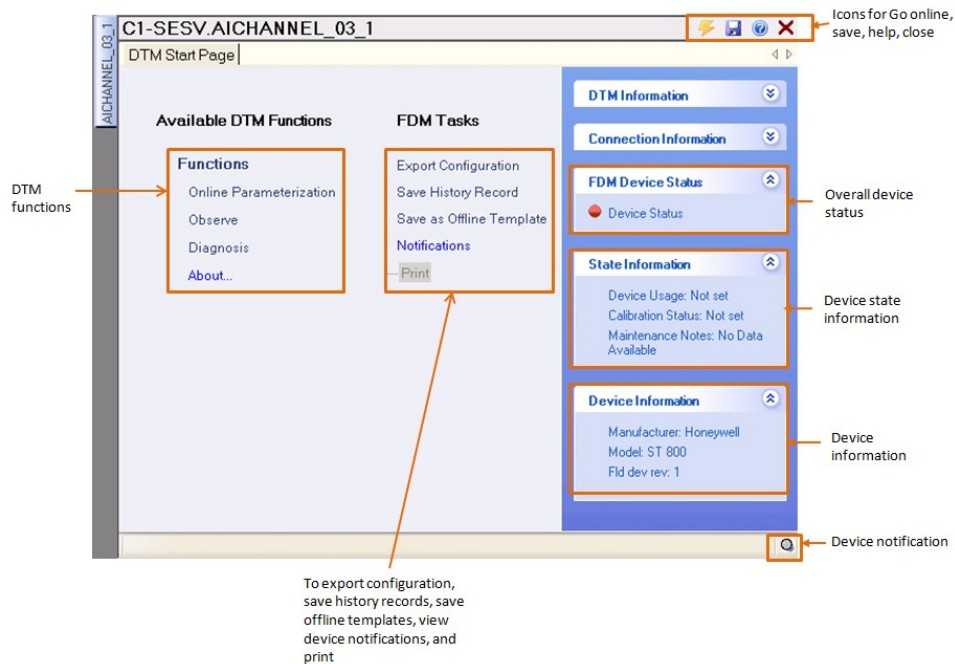
NOTE

- You can also open the Device Configuration page by double-clicking the device in the Network View list under Online View. It loads a device with the default setting.
- If you want to load a device only using DTM irrespective of DD/DTM settings, right-click the required device tag and choose Configure with > DTM offline.

If you have selected to load a device using DTM and if DTMs are available in the DTM library for the selected device, then the DTM Selection Dialog appears.

If the selected device has multiple DTM versions, then these versions are listed in the DTM Selection Dialog.

3. Select the appropriate DTM version and click OK. The DTM configuration page appears.



NOTE

- If you are loading a device using DTM for which the DTMs are not installed, then the following message appears.



- Click OK
 - Install the required DTM for the selected device or change the settings to load the selected device using DD/EDD.
- If you want to change the DTM, refer to section [“Selecting DTM to device”](#).
- You cannot load a device using DTM under the following conditions.
 - When the device is process active in Experion.
 - When the device is already loaded using DTM in other clients.
- Make sure that the RIO’s DTM is launched before configuring IOMs under RIOs using DTM.

4. Click  to make DTM online.

22.4 Configuring a device using DTM

- Ensure that DTM is in online mode before you configure a device using DTM.
- The DTM function links that are displayed on the DTM start page are specific to each DTM and the state of the DTM. “Online Parameterization” is an example of one such function link. You must use appropriate DTM functions to configure the device. Refer to the DTM documentation for details on DTM functions.

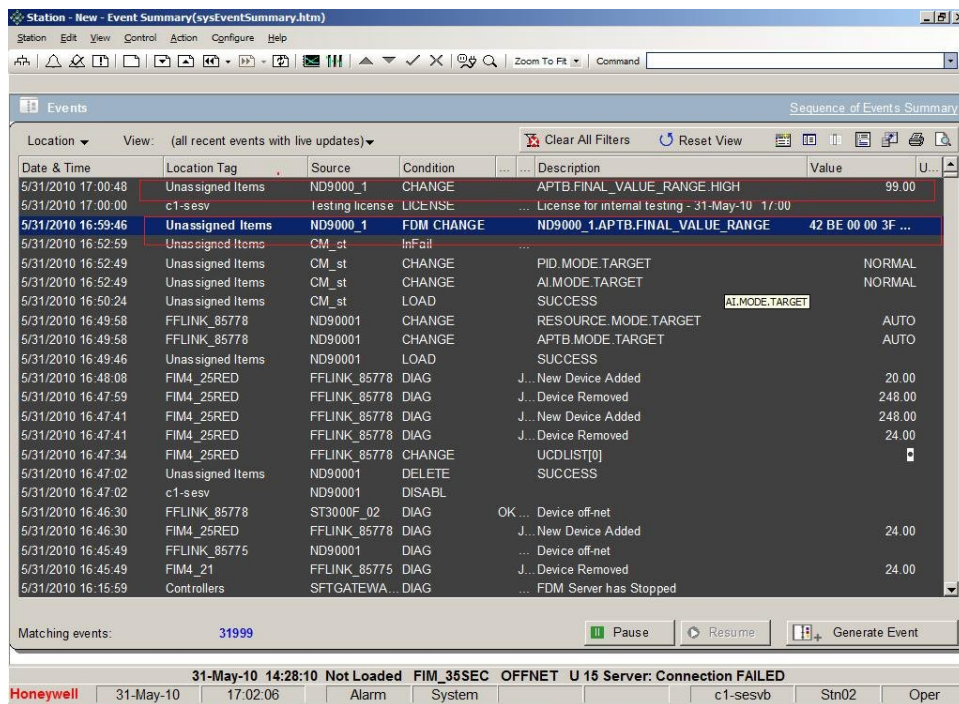
To configure a device using DTM

1. Perform the steps 1 through 3 in the section [“Loading a device using DTM \(online mode\)”](#).
2. To configure the online parameters of the selected device, click Online Parameterization. The configuration page appears with list of various parameters available in the device. These parameters are grouped into the sections which are displayed in the left pane of the Online Parameterize page.
3. To edit a parameter, select the required field and enter the value. To download this value to the device, follow the DTM specific instructions.

NOTE

- When a device reads all parameters from DTM, it may also try to write some parameters. Hence, only for FF devices, some events are logged in Experion Station as FDM changed events.
- In FDM Maintenance View, click  icon on the right-corner of the device configuration page to record all the parameter changes into Event summary for all FF devices connected to FIM.
- You cannot understand the format of the FDM changed parameter value

displayed in Experion station. Verify the values in FDM or Control Builder instead of verifying in Experion Station events.



22.5 Exporting online configuration using DTM

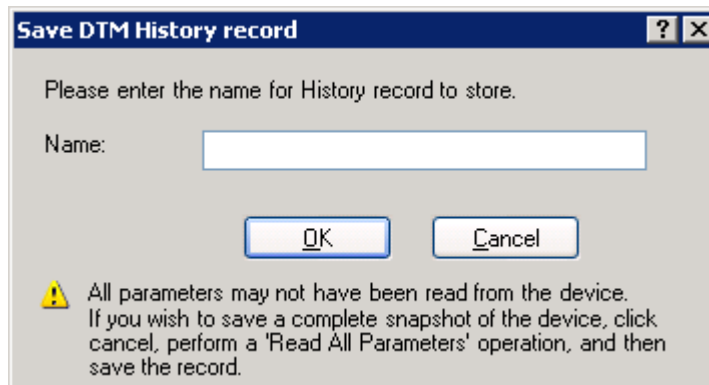
To export an online configuration using DTM

1. On the Device Configuration page, click Export Configuration. The Save As dialog box appears.
2. Select the location where you want to save the file.
3. Enter the file name and click Save. The Configuration Exported message appears.

22.6 Saving history records using DTM

To explicitly save history records using DTM

1. On the Device Configuration page, click Save History Record under FDM Tasks. The Save DTM History record dialog box appears.



2. Type the file name and click OK. The DTM history record is saved.

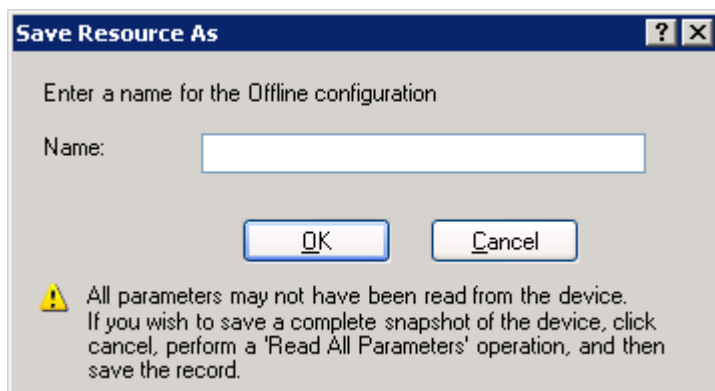
NOTE

- When you load a device, all parameters are not automatically read from the device. If you save history for the device, the history template contains only those parameter values that are read till that point. The unread parameters must have default values.
- If you want to capture a complete snapshot of the device, on the device configuration page, click  button to read all parameters from the device and then save the history record.
- Ensure that you do not close the device configuration page during save history operation.

22.7 Saving an online configuration as an offline configuration using DTM

To save an online device's configuration as an offline configuration using DTM

1. On the Device Configuration page, click Save as Offline Template under FDM Tasks. The Save Resource As dialog box appears.



2. Type the file name and click OK. The online configuration is saved as offline configuration.

NOTE

- When you load a device, all parameters are not automatically read from the device. If you save online configuration as offline template for the device, the offline template contains only those parameter values that have been read till that point. The unread parameters must have default values.
- If you want to capture a complete snapshot of the device, on the device configuration page, click  button to read all parameters from the device and then save the offline template.

22.8 Downloading a DTM based offline configuration to an online device

The download offline configuration feature is not supported for FF devices loaded with DTM.

To download DTM based offline configuration to an online device

1. Select the Offline Record and click View. The DTM start page is vendor specific. This is an indicative page.
2. If you want, you can edit the parameters before downloading those parameters. To edit parameters, refer to [section “Configuring a device using DTM”](#).
3. Click  to download the parameters to the device.

22.9 Integrating ValveLink DTM for FF devices

When you load FF Fisher Valve device with ValveLink DTM, it provides an option to launch the ValveLink application. FDM provides connectivity between ValveLink and FF Fisher Valves in Experion. Once ValveLink application is launched, you can start performing operations on the Fisher Valves.

ValveLink Software is a Windows software package that communicates with FF FIELDVUE digital valve controllers. ValveLink Software supports access to the information available from DVC2000, DVC6000, and DVC6000f Series digital valve controllers, and the obsolete DVC5000 and DVC5000f Series digital valve controllers.

NOTE

Few parameters such as RESERVED_A and RESERVED_AI are configured as Non-Cache for ValveLink DTM in Experion Control Builder. If these parameters are not configured as Non-Cache, then performing Valve signatures, Valve friction may not provide correct results.

To integrate ValveLink DTM for FF devices

1. Install ValveLink DTM and update the DTM library. For more information about how to update the DTM library, refer to section [“DTM management” on page 123](#).
2. On the FDM Client, ensure that the FF Fisher Valve device is displayed in Network View list under Online View.
3. Right-click the device and choose Configure with > DTM online. The Device Configuration page displays. For more information about how to load a device using DTM, refer to section [“Selecting DTM to device” on page 254](#).
4. On the Device Configuration page, click ValveLink DTM under Available DTM Functions. The ValveLink Software starts and you can see devices in the ValveLink tree.

**NOTE**

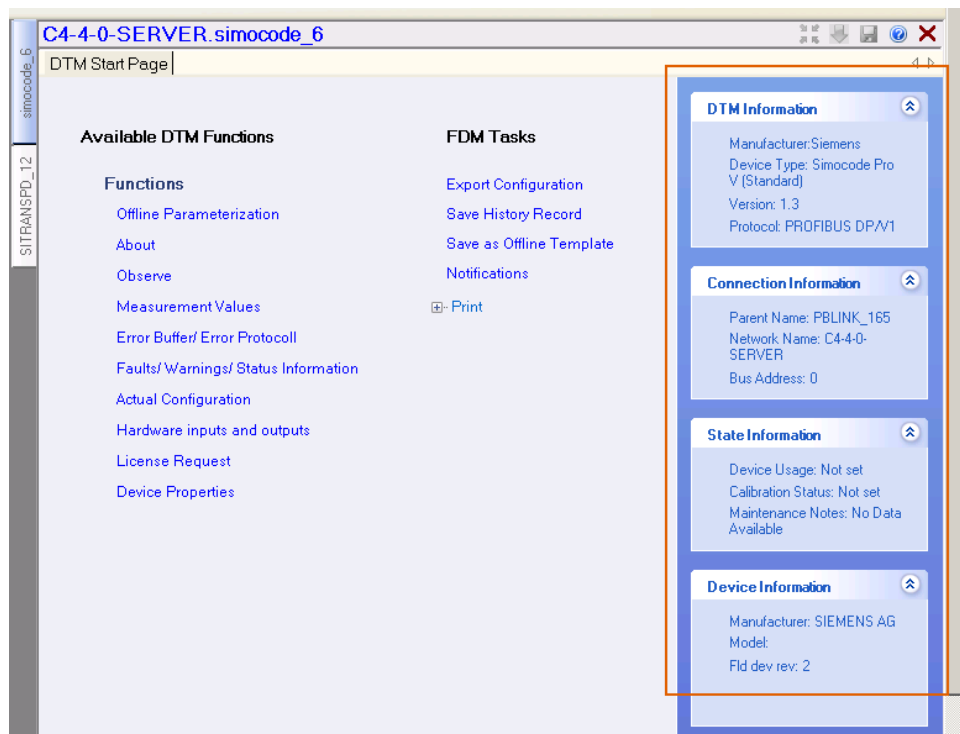
Choose Network > Refresh Device List to refresh the device tree in the ValveLink software for all devices which are appearing in FDM Client Network view list.

Choose Network > Refresh Device List to refresh the device tree in the ValveLink software for all devices which are appearing in FDM Client Network view list.

For more information about ValveLink operations, refer to the AMS ValveLink Software Guide.

22.10 PROFIBUS DP diagnostics

For PROFIBUS DP devices, diagnostics information is available solely via DTM. Double-click the DP device to view the DTM Start Page of the selected device. Overall health status is provided on the right as indicated in the following figure.



Click the Device Properties link to view additional information about the device.

IMPORT AND EXPORT OPERATIONS

The database maintains information such as device tags, audit trail, offline configuration, and history records for each device and this information can be imported or exported using Import and Export feature. Using the Import and Export wizard the following four operations can be performed.

- Import – Export of device tags
- Import – Export of audit trail
- Import – Export of offline device configuration
- Import – Export of device history

23.1 Import and export device tags

You can import device tags from Microsoft Excel (.CSV), XML, or FDM format. You can export device tags in HTML, Microsoft Excel (.CSV), FDM, or XML format.

23.1.1 Exporting device tags

To export the device tags

1. Log on to the FDM Client.
2. Click Tools > Import and Export or click  on the FDM tool bar. The Import and Export Wizard appears.
3. Click Export Data.
4. Click Device Tags in the list and then click Next. A dialog box appears prompting you to enter reason for the export action.

NOTE

The reason dialog box appears only if the Administrator has enabled reason logging, for this action type, in the Audit Trail settings. For more information, refer to section [“Customizing the audit trail settings”](#).

5. Type the reason for exporting the device tag and then click OK. The Export Device Tags page appears.

6. The Query View enables you to filter the device tags based on the combination of Network Type, Configured Network, Protocol, Manufacturer, and Device Types.

- To filter the device tags based on the Network type, select any Network type and Configured network corresponding to that network.
- To filter the device tags based on the protocol type, select any protocol from the Protocol list.
- When you select a protocol from the list, the manufacturer list appears as follows:
 - If you select the HART/FF/ISA100/PROFIBUS protocol then the manufacturer list appears using available respective DD library information. For the device that do not have a DD, the Unrecognized Manufacturers entry is available for the corresponding protocol. If the manufacturer is present in the DTM library then the device's manufacturer appears as a separate manufacturer entry.
 - If you select the DE protocol, then the corresponding manufacturer list appears.

NOTE

When you filter any protocol such as HART, FF, ISA100, or DE, the Manufacturer name is displayed as Honeywell_23 instead of Honeywell.

- If you select a protocol, which do not have an entry in the DD library, then the manufacturer list appears using list of manufacturers from the DTM library. For a device that do not have an entry in the DTM library, the Unrecognized Manufacturers entry is available in the list.
- If you select multiple protocols then the corresponding manufacturers are listed under Manufacturers list.
- You can select device types from device types list. The device types list appears as follows:
 - If you select HART/FF/ISA100/PROFIBUS manufacturers, then the device type appears using the respective DD library.
 - If you select DE manufacturers, then the device type appears for the respective manufacturers.
 - If you select non-DD manufacturers, then the device type appears using the DTM library information available.
 - If you select 'Unrecognized manufacturers' from the manufacturer list then the options available are the default 'All' option and 'Unrecognized device types'.
- To filter the device tags of selected configured network(s) based on Protocols, Manufacturers, and device types, select one or more Manufacturer(s) and Device Type(s).
- To export all the devices tags, select All for all options in the Query View and click Next.

NOTE

If the FDT network discovers few devices that uses protocols which are not qualified in FDM, then you must select Unqualified Protocols in the Protocols list.

Based on filter selection, select the device types to be displayed in the list.

In the next page, you can export connected devices, disconnected devices, healthy devices, unhealthy devices, or all devices from the list. Corresponding device tags populates in the following box.

7. Select the device tag and click  to move it to the Selected Device Tag List box. Or
8. Click  to move all the device tags to the Selected Device Tag List box.

NOTE

The number of device tags selected is listed in the right pane under Selected Device Tag List.

9. Click Next. In the next page, select the file format to export the device tags and click Browse.

NOTE

By default, the file location is:
C:\ProgramData\Honeywell\FDM\Client\Export\Device Tags\

10. Select the location to save the exported file. FDM populates the file location in the Save Exported File As box.
11. Click Export. In the next page, the progress report displays the progress in exporting the device tags and provides the following information.
 - Total number of devices succeeded, failed, and aborted.
 - The Operation state of the device tags exported.

NOTE

During exporting device tags, status column does not display the status of individual device export.

12. Click Next. In the next page, the Summary Report displays the path of the record and status of the exported device tag.

13. Click Finish to close the wizard. You can open the exported device tag file from the path, which is displayed in the Summary Report. The following figure displays the device tag information, which is exported in HTML format.

FDM Device Tags

Tag	NodeType	ManufacturerId	DeviceType	DeviceRev	DevTypeName	ManufacturerName	DeviceId	NodeId	DeviceTag	ProtocolId	ProtocolName	Release
device_1	7	38	9734	3	3051C	Rosemount	167970342	167970342_HART	3051C	036D1498-387B-11D4-86E1-00E0987270B9	HART	430.1
SM_A111_EJA	7	38	9734	3	3051C	Rosemount	151193126	151193126_HART	3051C	036D1498-387B-11D4-86E1-00E0987270B9	HART	430.1
SM_A111_RINT1	7	38	9734	3	3051C	Rosemount	100861478	100861478_HART	3051C	036D1498-387B-11D4-86E1-00E0987270B9	HART	430.1
SM_A111_RINT4	7	38	9734	3	3051C	Rosemount	16975398	16975398_HART	3051C	036D1498-387B-11D4-86E1-00E0987270B9	HART	430.1
SM_A124_YTA2	7	38	9734	3	3051C	Rosemount	134415910	134415910_HART	3051C	036D1498-387B-11D4-86E1-00E0987270B9	HART	430.1
SM_A126_Meto	7	38	9734	3	3051C	Rosemount	33752614	33752614_HART	3051C	036D1498-387B-11D4-86E1-00E0987270B9	HART	430.1
SM_A12_BEKA	7	38	9734	3	3051C	Rosemount	54054262	54054262_HART	3051C	036D1498-387B-11D4-86E1-00E0987270B9	HART	430.1
SM_A120_RINT3	7	38	9734	3	3051C	Rosemount	117635694	117635694_HART	3051C	036D1498-387B-11D4-86E1-00E0987270B9	HART	430.1
SM_A17_EJX	7	38	9734	3	3051C	Rosemount	67307046	67307046_HART	3051C	036D1498-387B-11D4-86E1-00E0987270B9	HART	430.1
SM_A008_DVC	7	38	9734	3	3051C	Rosemount	59529830	59529830_HART	3051C	036D1498-387B-11D4-86E1-00E0987270B9	HART	430.1
T0010000	7	23	5889	1	ST3000	Honeywell	68815	68815_HART	????????	036D1498-387B-11D4-86E1-00E0987270B9	HART	430.1
T0010001	7	23	5889	1	ST3000	Honeywell	1099511693591	1099511693591_HART	????????	036D1498-387B-11D4-86E1-00E0987270B9	HART	430.1
T0010001_Conflict_Tag_779	7	38	9734	3	3051C	Rosemount	198182	198182_HART	3051C	036D1498-387B-11D4-86E1-00E0987270B9	HART	430.1

The exported HTML file displays the Tag, NodeType, ManufacturerID, DeviceType, DeviceRev, DevTypeName, ManufacturerName, DeviceID, NodeId, and DeviceTag, ProtocolId, ProtocolName, and Release information.

The Tag column corresponds to the tag in the Network View. The Device Tag column corresponds to the tag in the device.

23.1.2 Importing device tags

To import device tags, perform the following steps.

1. Log on to the FDM Client.
2. Choose Tools > Import and Export. Or Click  icon on the FDM tool bar. The Import and Export Wizard appears.

NOTE

You cannot import Experion Tags.

3. Click Import Data.
4. Click Device Tags in the list and click Next. A dialog box appears prompting you to enter reason for the import action.

NOTE

The reason dialog box appears only if the Administrator has enabled reason logging, for this action type, in the Audit Trail settings. For more information, refer to section [“Customizing the audit trail settings”](#).

5. Type the reason for importing the device tag and click OK.
6. In the next page, click Browse to select the file that you want to import. The Open dialog box appears.
7. Select the file to import and select the file format from the Files of type list.
8. Click Open. The location of the file appears in the Select Files box.

9. Click Import. In the next page, the progress report indicates the progress of importing the device tags and provides the following information.
 - a. The grid displays the selected file path and status of import operation.
 - b. Total number of devices succeeded, failed, and aborted.
 - c. The Operation state of the device tags imported.
10. Click Next.
11. In the next page, the Summary Report displays the record name and status of the records.
12. Click Finish to close the wizard.

NOTE

- In case you want to rename the tags in the exported CSV, ensure that you rename only in the Tag column and not in the Device Tag column.
- It is recommended not to edit any other column in the exported file.
- After import operation, tag for the devices which are not connected to a network configured on a particular FDM Server, appears under the Disconnected Nodes list.

23.2 Import and export audit trail records

Audit trail records can be exported in XML, Microsoft Excel (.CSV), or HTML format using Import – Export wizard or Audit Trail option from the View menu. And also, audit trail records can be imported in XML format.

23.2.1 Exporting audit trail records

To export the audit trail records through Audit Trail option

1. Click View > Audit Trail. The Audit Trail page appears. For more information about how to view the audit trail records, refer to section [“Viewing audit trail”](#).
2. Click Export in the Audit Trail page after you receive the Audit Trail records. A dialog box appears prompting you to select the format (CSV, XML, HTML) in which you want to export. Click the required format.
3. The Export File Name & Location displays the name of the exported file and location where FDM saves the exported file. To change the name and/or location, click the  button.
4. In Save in box, choose the drive/directory /sub-directory on your system, where you want to save the file.
5. Type the File name and then click Save. The Export dialog box appears with the updated file name and location.
6. Click OK. The file is exported to the selected location and a confirmation message appears.

To export the audit trail records through Import and Export option

1. Log on to the FDM Client.
2. Click Tools > Import and Export or click  icon on the FDM tool bar. The Import and Export Wizard appears.
3. Click Export Data.

4. Click Audit Trail in the list and then click Next. A dialog box appears prompting you to enter reason for the export action.

NOTE

The reason dialog box appears only if the Administrator has enabled reason logging, for this action type, in the Audit Trail settings. For more information, refer to section [“Customizing the audit trail settings”](#).

5. Type the reason for exporting audit trail records and then click OK. The Export Audit Trail page appears.
6. The Query View enables you to filter the audit trails based on the combination of Network Type, Configured Network, Protocol, Manufacturer and Device Type.
 - To filter the audit trail records based on the Network type, select any Network type and Configured network corresponding to that network.
 - To filter the audit trail records based on the protocol type, select any protocol from the Protocol list.
 - When you select a protocol from the list, the manufacturer list appears as follows:
 - If you select the HART/FF/ISA100/PROFIBUS protocol then the manufacturer list appears using available respective DD library information. For devices that do not have a DD, the Unrecognized Manufacturers entry is available for the corresponding protocol. If the manufacturer is present in the DTM library then the device's manufacturer appears as a separate manufacturer entry.
 - If you select the DE protocol, then the corresponding manufacturer list appears.

NOTE

When you filter any protocol such as HART, FF, ISA100, or DE, the Manufacturer name is displayed as Honeywell_23 instead of Honeywell.

- If you select a protocol, which do not have an entry in the DD library, then the manufacturer list appears using list of manufacturers from the DTM library. For devices that do not have an entry in the DTM library, the Unrecognized Manufacturers entry is available in the list.
- If you select multiple protocols then the corresponding manufacturers are listed under Manufacturers list.
- You can select device types from device types list. The device types list appears as follows:
 - If you select HART/FF/ISA100/PROFIBUS manufacturers, then the device type appears using the respective DD library.
 - If you select DE manufacturers, then the device type appears for the respective manufacturers.
 - If you select non-DD manufacturers, then the device type appears using the DTM library information available.
 - If you select 'Unrecognized manufacturers' from the manufacturer list then the options available are the default 'All' option and 'Unrecognized device types'.

- To export all the audit trail records, select All for all options in the Query View and then click Next.

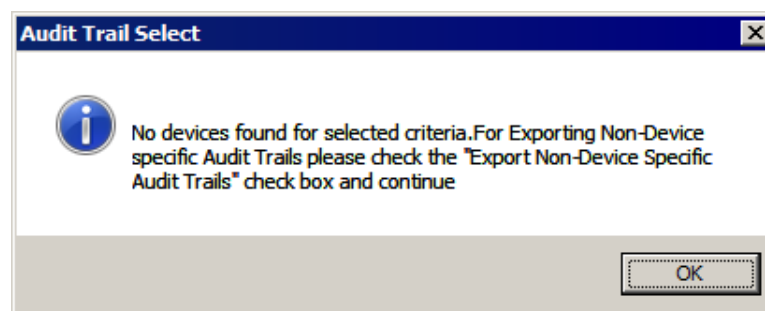
NOTE

If the FDT network discovers few devices that uses protocols which are not qualified in FDM, then you must select Unqualified Protocols in the Protocols list.

7. In the next page, based on filter criteria, Device list lists all the devices that are online and disconnected. Select the required device from Device list. To export the Audit Trail for all devices, select All. Selection of audit trail data based on the Device list is as follows:
 - If devices are found, select All in the Device list and then select Export Non-Device Specific Audit Trails check box. All audit trails of devices listed in the Device list and all non-device specific audit trails are exported.
 - If device list is empty, then select Export Non-Device Specific Audit Trails check box. All non-device specific audit trails are exported.
8. To view the audit trail for a particular user, select the user from User field. If you want to view the audit trail for all users, select All.
9. Select the required action types from Action Type. The Action Type drop-down list lists all the actions that are currently audited in FDM. For instance, Param Change indicates any change that you make to a parameter, logged in the Audit Trail. To view the Audit Trail for all parameters, select All.
10. If you select From and To dates using the calendar, the audit trail records of that particular period are exported.
11. Click Next.

NOTE

If device list is empty and Export Non-Device Specific Audit Trails check box is not selected, and if you click Next, then the following message appears.



Click OK and select the Export Non-Device Specific Audit Trails check box to export all non-device specific audit trails.

12. In the next page, select the file format to export the audit trail records and click Browse.

NOTE

By default, the file location is:
C:\ProgramData\Honeywell\Fdm\Client\Export\Audit Trail\.

13. Click Export. In the next page, the progress report indicates the progress of exporting and provides the following information.
- Total number of devices succeeded, failed, and aborted.
 - The Operation state of the audit trail records exported.
14. Click Next. In the next page, the Summary report displays the record and status of the exported audit trail records.

NOTE

During exporting of audit trail records, status column does not display the status of individual device export.

15. Click Finish to close the window.

23.2.2 Importing audit trail records

To import audit trail records, perform the following steps.

Log on to the FDM Client.

1. Click Tools > Import and Export or click  icon on the FDM tool bar. The Import and Export Wizard appears.
2. Click Import Data.
3. Click Audit Trail in the list and then click Next. A dialog box appears prompting you to enter reason for the import action.

NOTE

The reason dialog box appears only if the Administrator has enabled reason logging, for this action type, in the Audit Trail settings. For more information, refer to section [“Customizing the audit trail settings”](#).

4. Type the reason for importing the audit trail records and then click OK.
5. In the next page, click Browse and select .xml files to import.
6. Click Open. The location of the file appears in the Select Files field.
7. Click Import. In the next page, the progress report indicates the progress in importing and provides the following information.
 - The grid displays the selected file path and status of import operation.
 - Total number of devices succeeded, failed, and aborted.
 - The operation state of the audit trail data imported.
8. Click Next.

9. In the next page, the Summary report displays the record and status of all audit trail files, which are selected for import.
10. Click Finish to close the wizard.

NOTE

- Import of audit trail records automatically imports the tag of the particular audit trail record.
- After import operation, tags for the devices which are not connected to a network configured on a particular FDM Server, appears under the Disconnected Nodes list.
- If the audit trail is device specific, then the exported audit trail file contains corresponding tag information along with audit trail data.

23.3 Import and export offline device configuration

FDM enables you to import DD/Generic DD offline configuration from CSV and FDM (.fdm) format. You can export in HTML, CSV, and FDM (.fdm) format. But, you can export DTM offline configuration only in FDM format.

NOTE

- FF, ISA100 Wireless, and DE devices does not support the import/export of offline device configuration.
- The FDM (.fdm) format is not editable. Therefore, you cannot edit DTM offline configuration after exporting.

23.3.1 Exporting offline device configuration

To export DD/Generic DD offline configuration using Export option

1. Log on to the FDM Client.
2. Click the Offline View. The Offline Configuration, Display Filter and Device Library tabs appear.
3. Click the Offline Configuration tab. The DD Offline Configurations/Generic DD Offline Configurations/ DTM Offline configurations tree appear in the left pane.
4. Browse through the tree DD Offline Configurations > Manufacturer > Device Type > Device Revision > Offline Configuration (name), right-click and then click Export or browse through the tree Generic DD Offline Configurations > Generic Offline Configuration (name), right-click and then click Export. A dialog box appears prompting you to enter reason for the export action.

NOTE

A reason dialog box appears only if the Administrator has enabled reason logging, for this action type, in the Audit Trail settings. For more information, refer to section [“Customizing the audit trail settings”](#).

5. Type the reason for exporting offline configuration and then click OK. The Export dialog box appears. Select the required format and then click OK.

NOTE

If you try to export an old offline configuration that is migrated from previous releases, an appropriate message appears stating that you must upgrade the configuration before exporting.

Click Yes.

FDM upgrades configuration and a confirmation message appears displaying that configuration is migrated successfully.

6. Click  to select the location where you want to save the file. The Save As dialog box appears.
7. Select the location where you want to save the file and enter the name of the file in File name field.
8. Click Save. The Export dialog box appears with the name and location details populated in Export File Name & Location.
9. Click OK to export the file. A confirmation message appears and then click OK. FDM exports the file to the selected location.

To export DD/Generic DD/DTM offline configuration through Import and Export option

Log on to the FDM Client.

1. Click Tools > Import and Export. Or Click  icon on the FDM tool bar. The Import and Export Wizard appears.
2. Click Export Data.
3. Click Offline Device Configuration in the list and then click Next. A dialog box appears prompting you to enter reason for the export action.
4. Type the reason for exporting offline configuration and then click OK. The Export Offline Device Configuration page appears.
5. Select the offline configuration, which you want to export under Offline Library.
 - Click  to move it to the Selected Offline Templates box.
 - Click  to move all the offline configurations.
 - Click  to clear the offline configuration from the Selected Offline Templates box.
 - Click  to clear all the offline configurations.

TIP

The number of offline configuration selected are displayed under Selected Offline Templates : <number>.

6. Click Next. In the next page, select the file type for exporting and then click Browse. By default, the file location is: C:\ProgramData\Honeywell\Fdm\Client\Export\Offline Templates\.
7. Select the folder where you want to save the offline configuration file and click OK. The file location appears in the File Location field.

8. If output file exists, perform any one of the following as necessary.
 - a. Click Overwrite to replace the existing offline template with a new file, but with the same file name. Or
 - b. Click Auto Rename to automatically rename the existing file and to create a new file. The new file name appears in the format of <OfflineTemplateName>currentDateTimeStamp. Or Click Skip to skip the exporting the existing offline templates.
9. Click Export. In the next page, the progress report indicates the progress in exporting offline configuration and provides the following information.
 - The grid displays the individual offline template selected and their status.
 - Total number of devices succeeded, failed, and aborted.
 - The Operation state of the offline device configuration exported.
10. Click Next. In the next page, the Summary report displays the record and status of the offline configuration export operation.

NOTE

If you click Skip in the Select File Location page, then exporting of the existing offline templates are skipped and status in the Summary report displays as Export skipped as per user setting.

11. Click Finish to close the wizard. The following figure displays the offline device configuration information which is exported in CSV format.

	A	B	C	D	E
1	Id	Label	Value	WriteAccess	Selected
2	162	Poll addr		0 WRITE_WITH_WARNING	0
3	163	Tag	????????	WRITE_WITH_WARNING	0
4	164	Message	????????????????????????????????	WRITE_WITH_WARNING	0
5	165	Descriptor	????????????????	WRITE_WITH_WARNING	0
6	166	Date	1/1/1980	WRITE_WITH_WARNING	0
7	16391	PV Snsr unit		1 WRITE_WITH_WARNING	0
8	16398	PV Damp		0 WRITE_WITH_WARNING	0
9	16401	PV rng unit		1 READ_WRITE	0
10	234	PV URV		0 WRITE_WITH_WARNING	0
11	235	PV LRV		0 WRITE_WITH_WARNING	0
12	153	Manufacturer		38 READ_ONLY	
13	154	Model		128 READ_ONLY	
14	157	Fld dev rev		5 READ_ONLY	
15	104	DD Revision		5 READ_ONLY	
16					

The CSV file displays the Id, Parameter Label, Parameter Value, WriteAccess, and Selected columns. The Selected column displays 0 and 1.

If you want to edit CSV file before importing, change the value in Value column and variable 0 to 1 in the Selected column.

The WriteAccess column displays the variables like READ_WRITE, READ_ONLY, WRITE_WITH_WARNING, and so on.

23.3.2 Importing offline device configuration

FDM enables you to import DD/Generic DD offline configuration in the CSV or FDM (.fdm) format.

To import DD/Generic DD offline configuration

1. Log on to the FDM Client.
2. Click Tools > Import and Export or click  icon on the FDM tool bar. The Import and Export Wizard appears.
3. Click Import Data.
4. Click Offline Device Configuration in the list and then click Next. A dialog box appears prompting you to type the reason for the import action.

NOTE

The reason dialog box appears only if the Administrator has enabled reason logging, for this action type, in the Audit Trail settings. For more information, refer to section [“Customizing the audit trail settings”](#).

5. Type the reason for importing the offline configuration and click OK. In the next page, click Browse. The Open dialog box appears.
6. Select the file or files to import and select the file format for import from the Files of type list and click 446BOpen. The location of the file appears in the Select Files box.
7. Click Import. In the next page, the progress report indicates the progress of importing and provides the following information.
 - The grid displays the selected file path and status of import operation.
 - Total number of devices succeeded, failed, and aborted.
 - The Operation state of the offline device configuration imported.
8. Click Next. In the next page, the Summary report displays the record and status of the imported offline configuration.
9. Click Finish to close the window. The imported offline configuration appears in the Offline View.

23.4 Import and export device history

After viewing a history record, you can import the history records from FDM (.fdm) format and export the history in CSV, HTML, or FDM (.fdm) format. FDM also enables you to import MCToolKit configuration of DE device history in MCTK XML format and export the history records (which were imported to FDM only from MCToolKit) in .HTML, Microsoft Excel (.CSV), and MC Tool Kit (.xml) format.

NOTE

- For FDT/DTM based devices, history records are imported in .FDM format.
- FDM does not support import/export of DE devices such as Magnew 3000 device data and multi variable device (SMV 3000) data.
- FDM does not support import of MCToolKit device history files for DE devices, which are in analog mode.

You can export a history record in the following two ways.

- Using Device Configuration page
- Using the Import and Export option

23.4.1 Exporting device history

To export a history record using device configuration page

1. Perform the steps 1 through 4 of the section “Viewing the device history” and then click Export under FDM Tasks. The Export dialog box appears.
2. Click the required format. The Export File Name & Location displays the name of the exported file and location where FDM saves the exported file.
3. To change the name and/or location, click the  button. The Save As dialog box appears.
4. Choose the drive/ directory/sub-directory on your computer, where you want to save the file.
5. The default file name appears in the File name box. To save the file with a different name, enter a new name in File name.
6. Click Save to save the file. The Export dialog box with the updated file name and location appears.

Click OK in the dialog box. The file is exported to the selected location and the following message appears on the status bar.

Export device history operation is performed successfully...

To export the history records using the Import and Export option

1. Log on to the FDM Client.
2. Click Tools > Import and Export or click  icon on the FDM tool bar. The Import and Export Wizard appears.

NOTE

The history records for DTM devices are exported in FDM (.fdm) format.

3. Click Export Data.
4. Perform any one of the following as necessary and then click Next.
 - Click Device History in the list
 - Click Device History in the list, and then select MCToolKit DE Device under Options, if you want to export MCToolKit device configuration of DE devices.

The history records for DTM devices are exported in FDM (.fdm) format.

5. The Query View enables you to filter the history records based on the combination of Network Type, Configured Network, Protocol, Manufacturer and Device Type.
 - To filter the history records based on the Network type, select any Network type, and Configured network corresponding to that network.
 - To filter the history records based on the protocol type, select any protocol from the Protocol list.
 - When you select a protocol from the list, the manufacturer list appears as follows:
 - If you select the HART/FF/ISA100/PROFIBUS protocol then the manufacturer list appears using available respective DD library information. For the device that do not have a DD, the Unrecognized Manufacturers entry is available for the corresponding protocol. If the manufacturer is present in the DTM library then the device's manufacturer appears as a separate manufacturer entry.
 - If you select the DE protocol, then the corresponding manufacturer list appears.

NOTE

When you filter any protocol such as HART, FF, ISA100, or DE, the Manufacturer name is displayed as Honeywell_23 instead of Honeywell.

- If you select a protocol, which do not have an entry in the DD library, then the manufacturer list appears using list of manufacturers from the DTM library. For a device that do not have an entry in the DTM library, the Unrecognized Manufacturers entry is available in the list.
 - If you select multiple protocols then the corresponding manufacturers are listed under Manufacturers list.
- You can select device types from device types list. The device types list appears as follows:
 - If you select HART/FF/ISA100/PROFIBUS manufacturers, then the device type appears using the respective DD library.
 - If you select DE manufacturers, then the device type appears for the respective manufacturers.
 - If you select non-DD manufacturers, then the device type appears using the DTM library information available.
 - If you select 'Unrecognized manufacturers' from the manufacturer list then the options available are the default 'All' option and 'Unrecognized device types'.
- To export all the history records, select All for all options in the Query View and click Next.

NOTE

If the FDT network discovers few devices that uses protocols which are not qualified in FDM, then you must select Unqualified Protocols in the Protocols list.

6. Based on filter selection, select the types of devices to be displayed from the list. In the next page, you can export connected devices, disconnected devices, healthy devices, unhealthy devices, or All devices form the list. Corresponding device tags are populated in the Available Device Tags List box.
7. Select the device tag and click  to move it to the Selected Device Tag List box or click  to move all the device tags.
8. Click Next.
9. In the next page, click All records or Select Time Duration (From and To) and then click Next.
 - If you click All records, all the history records are exported.
 - If you click Select Time Duration (From and To), the history records of that particular period are exported.
10. In the next page, select the file format in which you want to export the history record.
11. Click Browse and select the folder to save the exported file.

NOTE

By default, the file location is:
C:\ProgramData\Honeywell\Fdm\Client\Export\History Records\

12. If output file exists, perform any one of the following as necessary.
 - Click Overwrite to replace the existing file.
 - Click Skip to skip the exporting the existing files.
13. Click Export. In the next page, the progress report indicates the progress in exporting and provides the following information.
 - Total number of devices succeeded, failed, and aborted.
 - The Operation state of the device history data exported.

NOTE

During exporting device history, the status column does not display the status of individual device history export.

14. Click Next. In the next page, the summary report displays the record and status of history records.
15. Click Finish to close the window.

23.4.2 Importing device history

FDM enables you to import history records in FDM (.fdm) format and the MCToolKit configuration of DE device history records in MCTK XML format.

To import history records, perform the following steps.

1. Log on to the FDM Client.
2. Click Tools > Import and Export or click  icon on the FDM tool bar. The Import and Export Wizard appears.
3. Click Import Data.
4. Perform any one of the following as necessary, and then click Next.
 - Click Device History in the list
 - Click Device History in the list, and then select MCToolKit DE Device under Options, if you want to import MCToolKit device configuration of DE devices.

A dialog box appears prompting you to enter reason for the import action.

NOTE

The reason dialog box appears only if the Administrator has enabled reason logging, for this action type, in the Audit Trail settings. For more information, refer to section [“Customizing the audit trail settings”](#).

5. Type the reason for importing history records and then click OK.
6. In the next page, click Browse to select files that you want to import. The Open dialog box appears.
7. Perform any one of the following as necessary.
 - Select the .fdm files to import, and then click Open.
 - Select the MCTK XML files to import the MCToolKit device configuration of DE devices, and then click Open. The location of the file appears in the Select Files field.

8. Click Import. In the next page, the progress report indicates the progress of importing and provides the following information.
 - The grid displays the selected file path and status of import operation.
 - Total number of devices succeeded, failed, and aborted.
 - The Operation state of the device history imported.
9. Click Next. In the next page, the Summary report displays the overall status of the imported history records.
10. Click Finish to close the window.

NOTE

- If the history record already exists in the database, the message History record already exists, is displayed in the summary report.
- Import of device history automatically imports the tag of the particular device.
- After import operation, tag for the devices, which are not connected to a network configured on a particular FDM Server, appears under the Disconnected Nodes list.

23.5 Importing device configuration history from FDC into FDM

The history snapshot saved in FDC can be imported into FDM for record and audit purposes. FDM allows you to synchronize the device configuration data through the MC Toolkit handheld. With FDC, you can save the device configuration snapshot as device history. This is saved as .fdm format. Consequently, the same device configuration history can be imported into FDM through the standard history import feature using the Import/ Export wizard.

NOTE

You must not make any changes to the history files exported from handheld application, before importing them into FDM. This is to ensure that the imported history files are free from errors. FDM does not validate if the imported files are tampered after they are exported from handheld application.

Perform the following steps to import the device configuration history from FDC into FDM.

1. Connect your MC Toolkit handheld to the computer where FDM Client is installed.
2. Browse to the folder for SD Card > FDC > Resources > History. The FDC history records are named as per the following convention for the primary name: 449BDeviceTag_ManufacturerIDDeviceTypeDeviceRevisionDDRRevision_DeviceID.
3. Copy the desired history record files (with .fdm extension) from the above mentioned location to a temporary location on FDM Client computer.
4. Use FDM Import/Export wizard to import the history records into FDM. For more details on how to use FDM Import/Export feature, refer to section [“Import and export device history”](#).

After you import successfully,

- The snapshot of device history is imported into FDM database and appear as a history record for the corresponding device in FDM.
- The Audit Trail entry for such a record identifies if it is imported through the MC Toolkit handheld.
- If the device is not part of any of the FDM configured networks, it appears under Disconnected Nodes in FDM network view.
- All operations allowed on Device History Record in FDM are allowed for the record imported through the MC Toolkit handheld.

23.6 Importing DE device configuration history from MCToolKit into FDM

The history snapshot saved in MCToolKit can be imported into FDM for record and audit purposes. With MCToolKit, you can save the DE device configuration snapshot as device history. This is saved as MCTK XML format. Consequently, the same device configuration history can be imported into FDM through the standard history import feature using the Import/Export wizard.

NOTE

You must not make any changes to the history files exported from the handheld application, before importing them into FDM. This is to ensure that the imported history files are free from errors. FDM does not validate if the imported files are tampered after they are exported from the handheld application.

Perform the following steps to import the device configuration history from MCToolKit into FDM.

1. Connect your MCToolKit handheld to the computer where FDM Client is installed.
2. Browse to the folder, where device configuration history is saved in the MCToolKit.
3. Copy the history record files (with MCTK XML extension) to a temporary location in FDM Client computer.
4. Use FDM Import/Export wizard to import the history records into FDM. For more details on how to use FDM Import/Export feature, refer to the section [“Import and export device history”](#).

After DE device configuration is imported successfully,

- The snapshot of device history is imported into FDM database and appear as a history record for the corresponding device in FDM.
- The naming convention of the imported MCToolKit device history file is as follows:
<date and time when the history file generated from device to MCToolKit-MCT_device tag name_ unique number to differentiate the history records>
- The Audit Trail entry for such a record identifies if it is imported through the MCToolkit handheld.
- If the device is not part of any FDM configured networks, it appears under Disconnected Nodes in Online view with the name of the STITAG.
- All operations allowed on device history record in FDM are allowed for the record imported through the MCToolKit handheld.

NOTE

After importing history records, the respective device history file is attached to the device in the network tree.

You can import the history records from MCToolKit to FDM in single file or multiple records in single file.

VIEWING DEVICE HISTORY

FDM supports historization and maintains of a device history with timestamps for connected and disconnected devices. History record saves all the details of a device that are displayed in the device configuration and device status.

NOTE

In FDM, you can view the history records for the DE devices and devices based on the DD/DTM load settings.

You can select a device and view the device history for the following:

- For the device, which is part of the configured network (from the Network view)
- For the device, which is under Disconnected Nodes tree

Prerequisites

Ensure that DE device history snapshot is imported to FDM from MCToolKit using Import and Export option to view the MCToolKit DE device history. For more details about importing device history, refer to the section [“Importing device history”](#).

To view the device history

1. To view the device history in the Network View list, right-click the required device tag and then click View History. The Device History page appears. For DD/EDD or DTM supported devices, the Device History page appears irrespective of DD/DTM load settings.
 - FDM saves each saved versions of the device history with the time stamp (date and time).
 - Explicitly saved history versions have user-defined names.
2. Select a history version from the list and click View. The Entry Points page appears.
3. Following is an example to view the page, which is opened through history form.
 - For DD/EDD and DTM supported devices, click Online under Device Functions. The Online window is split horizontally into the upper and lower panes.
 - The upper pane holds the set of menus based on timestamp selected.
 - The parameters associated with the selected menu appear in the lower pane
 - For MCToolKit DE device history, click the MCToolKit Device SnapShot link under Device Functions. The MCToolKit Device SnapShot page displays the following:
 - TPS Convention: The parameters layout (labels and values) are displayed based on the TPS convention.
 - MCToolkit Convention: The parameter layout (labels and values) are displayed based on the MCToolKit convention.

4. To view the device history for disconnected device under Disconnected Nodes tree, right-click the required device tag and then click View History and then continue with the steps 1 through 3.

NOTE

- When you are viewing the MCToolKit DE device history, all the applicable parameters are displayed in the Device History page and other few parameters (which are not displayed in the Device History page) are stored in the FDM database.
- If you want to delete the device history, right-click the selected device and then click Delete History.

BULK OPERATIONS

The Bulk Operations feature enables you to create the history records and offline templates for several devices at the same time. This feature ensures that you do not have to manually open each device and save history/ offline. This feature enables you to get the history snapshot of a set of devices in the maintenance database through a single operation. In addition, it is very helpful to create offline templates of a set of devices through a single operation.

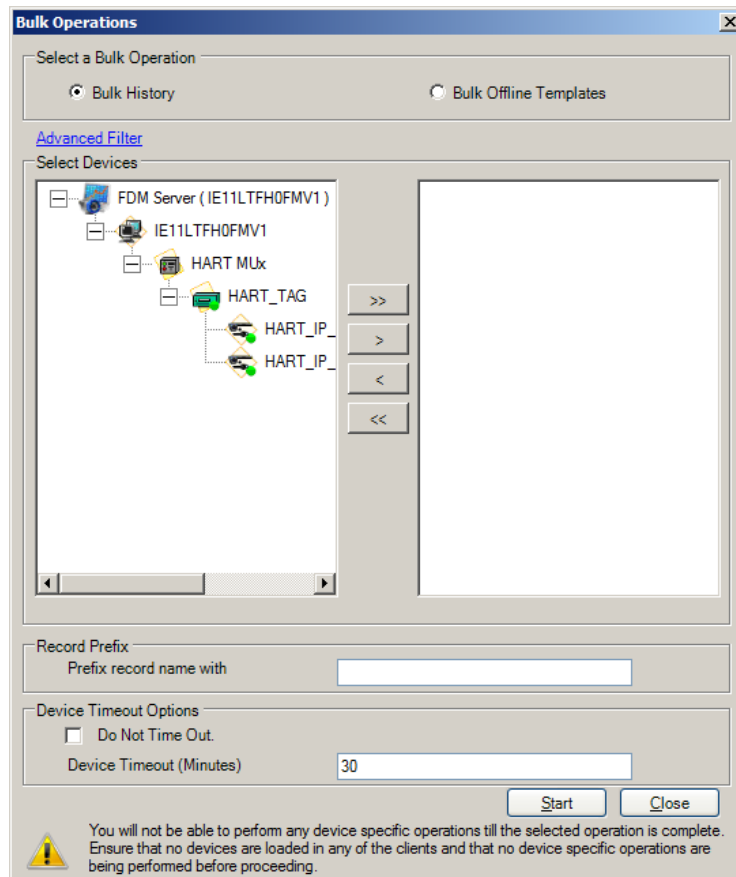
NOTE

- Bulk operations feature does not support creation of history and offline records using DTMs. It supports only DD/EDD based device history and offline records. Hence it is not applicable to the devices that can be loaded only with DTMs like PROFIBUS devices.
- FDM does not support the save bulk offline templates for FF, ISA100 Wireless, and DE devices.
- If the user does not have privilege to perform the bulk operations, then this option is disabled on the Tools menu.

25.1 Saving bulk history

To save the history records in bulk for the devices

1. Log on to the FDM Client.
2. Click Tools > Bulk Operations. The Bulk Operations dialog box appears.



3. Click Bulk History. The Advanced Filter enables you to filter the nodes/devices displayed under the Select Devices left tree. For more information about Advanced Filter, refer to section [“Using advanced filter”](#).

NOTE

You cannot select only the OneWireless adapter or only the devices under OneWireless adapter. You should select both OneWireless adapter and device under it.

4. The left tree view shows the available devices and right tree view shows the selected devices.
 - Click  to move all selected nodes/devices in the Network (under Select Devices) to the right pane.
 - Click  to move a single node/device in the Network (under Select Devices) to the Selected box.
 - Click  to remove a single node/device from the Selected box to Select Devices.

- Click  to remove all the nodes/devices from the Selected box to Select devices.

NOTE

- You must select at least one device for creating history of the data for the devices in Select Devices.
- If the devices are not selected from the list, then a dialog box appears prompting you to select a device before starting bulk operation.
- When performing the bulk operation, client must not perform any other device specific or server intensive operation.
- If the display filter is applied to the network tree, the filtered tree appears in the bulk operations.

5. Under Record Prefix,

- Type the prefix name for the history record in Prefix record name with box. You can maintain the unique name for history record with prefix. History record name contains the given prefix string followed by an internally generated number which is unique. The number is unique for each device.
- Under Device Timeout Options, type the time in Device Timeout (Minutes) box. This is the time in which FDM must save history of an individual device. If the device does not respond for all read requests during this time interval, the operation is timed out and is reported accordingly. This is a mandatory field. By default, the time out value is 30 minutes.

NOTE

- Ensure that the prefix name does not exceed 14 characters. If the prefix has any special characters, an error message appears.
- If you do not want to set the timeout value, select the Do Not Time Out check box.

6. From the Bulk Operations dialog box, click Start. A dialog box appears asking if you want to start this operation.

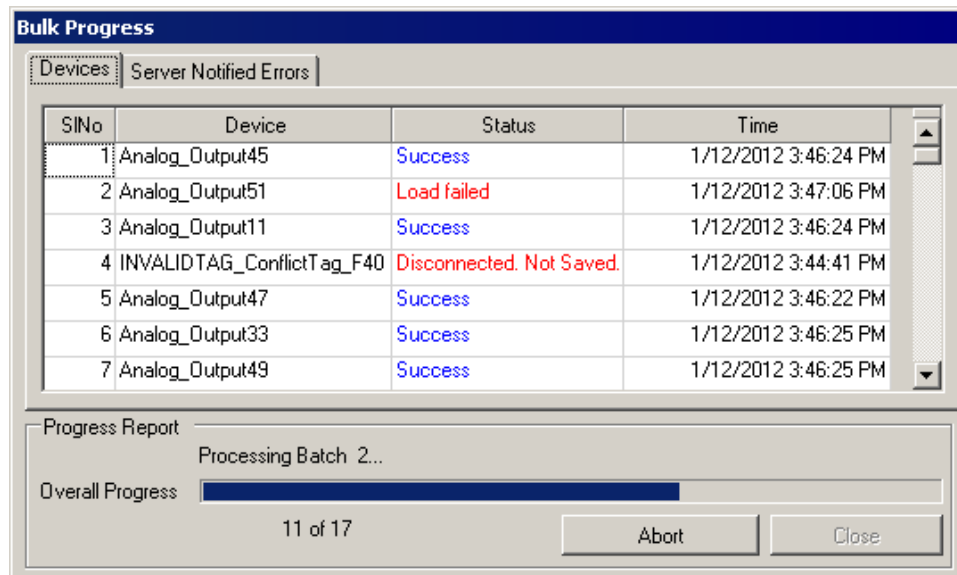
NOTE

- When the bulk operation starts, FDM internally changes the Device Configuration Load Option to Load From Device and disables Write Access option in FDM Settings temporarily. However, these options are restored to original settings after bulk operation completes.
- When you click Start button, an error message appears displaying Operation is denied due to some other operations on other Clients are in progress. Acknowledge the error and close the operations listed in the error message on the corresponding clients to start bulk operations.

7. Click Yes to continue. The selected devices are grouped into batches and operation is performed on one batch at a time.

8. The Bulk Progress dialog box appears. The following are the two tabs in Bulk Progress dialog box.

- Devices
- Server Notified Errors



The Devices tab displays the following information.

- Individual device selected in the bulk operation, status of the bulk operation. And also, the timestamp is recorded when history record is saved or when operation is failed in the Time column.
- The progress report indicates the overall progress of the bulk operation.
- Total number of devices for which bulk operation is completed.

All the error notifications received from the server are displayed under Server Notified Errors tab.

You can abort the bulk operation of the selected nodes/devices by clicking Abort. When you click Abort:

NOTE

- For Pending and Loading devices, the bulk operation is aborted.
- For Saving History devices, the bulk operation is aborted after historization is completed.

Following are the different device status and their indications.

Device status	Description
Pending	The device is not yet loaded.
Loading	The device is loading.
Saving History Note: For Bulk Offline Templates operation, device status displays as Saving Template	The device is loaded and Save History for the device is in progress.
Success	The device history is successfully saved.
Timed Out	The device is not loaded completely within the specified time out period.
Disconnected. Not Saved.	The device is disconnected from the Network. Although a device is disconnected, this status may not be shown for the device if it had succeeded or timed out before getting disconnected.
Load Failed	FDM Server failed to load the device.
Abort	Bulk operation is aborted.
Corrupt Template	The offline template generated for the device is corrupt.
Unknown Error	Bulk operation is failed for some of the devices due to internal error.
Device is in process active	Bulk operation is failed for the devices connected in Experion network due to devices are process active.

9. Click Save Report to save the summary of bulk operation. The Save As dialog box appears.
10. Type the File name and click Save. The history records are saved in CSV format that contains device name, status, and timestamp. The server notified errors also exported in CSV file if errors are received during the bulk operation.

25.2 Saving bulk offline templates

NOTE

FDM does not support the save bulk offline templates for FF, ISA100 Wireless, and DE devices.

To save the offline templates in bulk for the devices

1. Log on to the FDM Client.
2. Click Tools > Bulk Operations. The Bulk Operations dialog box appears.
3. Click Bulk Offline Templates. Refer to step 4 through 9 of [“Saving bulk history”](#) to continue with saving offline templates in bulk.

25.3 Using advanced filter

Advanced filter feature enables you to filter the nodes/devices displayed in the left tree view. Filters can be created based on the Network Type, Manufacturer Type, Device Type, and Device Tags. When a filter is applied, the Network View tree displays only those nodes/devices included in the filter.

NOTE

By default no Advance Filter is applied, when you select the bulk operation. The Advanced Filter must be applied explicitly.

To apply the advanced filter

1. Click Advanced Filter in the Bulk Operations dialog box.
2. From the Protocol list, select the required protocol (HART, FF, ISA100, or DE).
3. From the Network list, select the configured network.

NOTE

To select all the network types, select All.

4. From the Manufacturer drop-down list, select the manufacturer.

NOTE

To include all the manufacturers, select All.

When you filter any protocol such as HART, FF, ISA100, or DE, the Manufacturer name is displayed as Honeywell_23 instead of Honeywell.

5. From the Device Type drop-down list, select the device type for the selected manufacturer.

NOTE

To include all the device types, select All.

Device Tag is the tag name of the device that is displayed in the Network View tree. You can use the tag name to further filter the Advanced filter criteria. Type the tag name either fully or partially. (You can use wild card characters for searching such as '*' and '?') Example: To include devices with tag name containing STT25H, type *STT*.

Example:

To display devices starting with 'S' and 'A', you can enter *S*; *A*. This lists all devices matching the selected query criteria (Network Type, Network Configured, Manufacturer, and Device Type) that begin with S and/or A.

For example, to display devices of type STT25H, type STT25H in the tag name.

NOTE

Use semicolons to separate multiple tag names.

6. To view the devices included in the Advanced filter, click Select. The devices matching the selected filter criteria appear in the left tree view.

The screenshot shows a dialog box titled "Advanced Filter". It contains four dropdown menus: "Protocol" (set to "HART"), "Network" (set to "All"), "Device Type" (set to "All"), and "Manufacturer" (set to "All"). There is also a text input field for "Device Tag" which is currently empty. At the bottom of the dialog, there are two buttons: "Select" and "Reset".

7. Click Select. Under Select Devices, the left network tree view is filtered according to the selected filter criteria. Right network tree view remains unaffected.
8. Click Reset to undo filtering. The filter on the tree view is removed. The selected device remains in right network view even after Reset.

FDM DASHBOARD AND QUICKVIEW

26.1 Dashboard

The FDM Server maintains various types of information related to the FDM Client, devices, RCIs, gateways, networks and operations. The FDM Client does not display all types of information that FDM Server maintains. Using Dashboard feature, you can view all these types of information at a single place and provides quick and easy access to it.

You can view the following information.

- Tags Information
- Devices Information
- Clients Information
- Loaded Devices Information
- Network Information
- Gateways Information
- Operations Information
- License Usage Information
- You can refresh the information displayed in the dashboard by fetching the latest data from the FDM Server and save the dashboard report in HTML format.

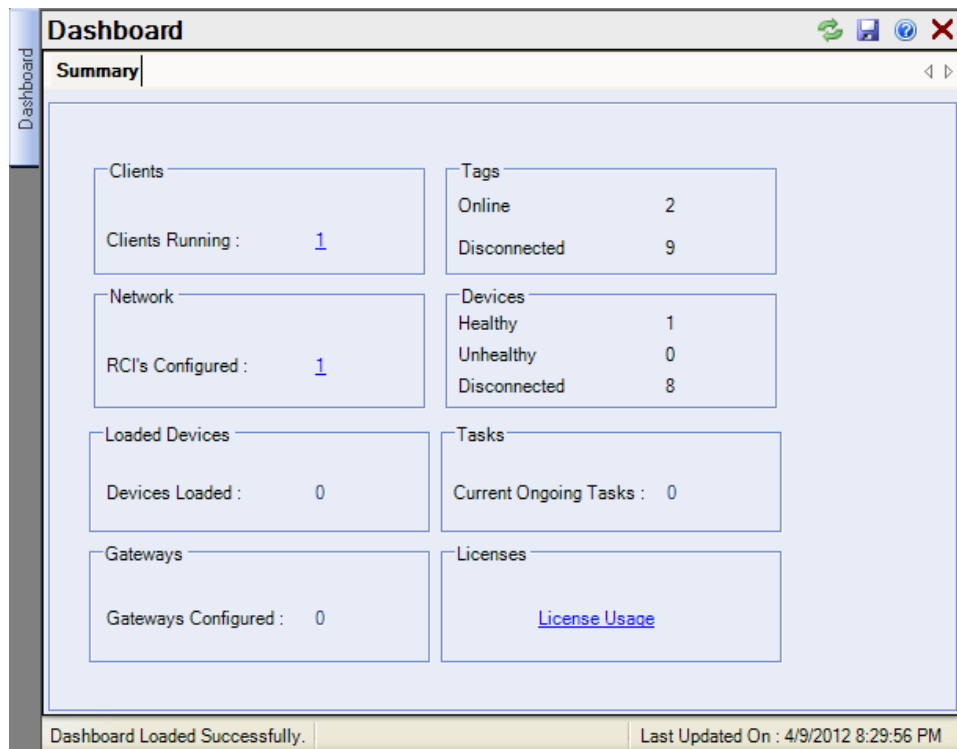
26.2 QuickView

Using this feature, you can view the information related to device status, device information, network information, device state information, lock state, and attached documents for all connected and disconnected devices. The information is available at a single place to access easily.

26.3 Viewing information through dashboard

To review the information

1. Log on to FDM Client.
2. Click View > Dashboard. Or In the Network View list under Online View, right-click the required RCI or Network node and click Dashboard. Once the data is fetched from the FDM Server, the details appear on the Dashboard page depending on the location from where it is launched. The following Dashboard page appears when launched through the View menu.

**NOTE**

- If Dashboard is launched through the View menu, then the Summary tab is displayed.
- If Dashboard is launched through the context menu of RCI or network node, then the Summary tab and the Network Information tab are displayed.

After data is fetched from the server, the message appears Dashboard Loaded Successfully on the status bar of the Dashboard page.

The Summary page displays the following details.

- Tags: It shows the total number of online and disconnected tags.
- Devices: It shows the total number of healthy, unhealthy and disconnected devices.
- Clients Running: It shows the total number of clients running at various locations including Sentinel clients and Station Maintenance View.
 - RCI's Configured: It shows the total number of RCI servers configured.
- Devices Loaded: It shows the total number of devices loaded across all the clients.
 - Gateways Configured: It shows the total number of gateways configured.
 - Current Ongoing Tasks: It shows the total number of tasks going-on across all the clients.
- License Usage: It shows the total number of licenses available for a particular entity and the number of licenses that are currently in use.

3. Under Tags, you can view the total number of online and disconnected tags.

Tags	
Online	10
Disconnected	0

4. Under Devices, you can view the total number of healthy, unhealthy and disconnected devices.

Devices	
Healthy	8
Unhealthy	0
Disconnected	0

5. Under Clients, click the link for Clients Running. The Clients Information page appears. It displays the following information for each client.
- The machine name on which the client is running.
 - The user who has launched the client.
 - Client Type and Client ID.
6. Under Network, click the link for RCI's Configured. The Network Information page appears. It displays the machine name on which RCI is configured, total number of online tags, disconnected tags, healthy devices, unhealthy devices, MUX monitored devices, and currently loaded devices. Click  to view the details of the network interface configured on the RCI.

NOTE

If any information related to configured network is not applicable, then value displays as -NA-.

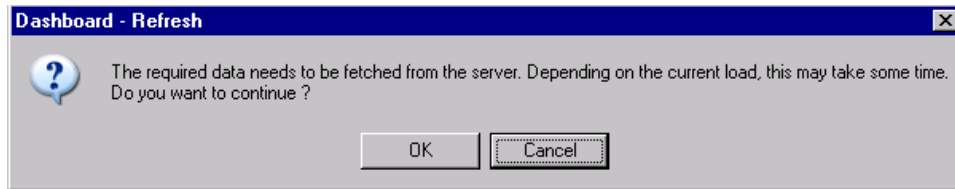
7. Under Loaded Devices, click the link for Device Loaded. The Loaded Devices Information page appears. This page displays the device name, manufacturer name, device type, device revision, DD revision, loaded With DD or DTM (Offline/Online), RCI name, network name, and name of the machine which has locked the device.

Click  to view the following information.

- Machine name on which the device is loaded.
- User who has launched the client.
- Client type

NOTE

If you want to refresh the dashboard data, click  which is present in the upper-right corner of the Dashboard page. The following message appears.

**NOTE**

Click OK to refresh the data.

8. Under Gateways, click the link for Gateways Configured. The Gateways Information page appears. The Gateways Information page displays the Experion Server name, gateway host name, gateway name, total number of monitored devices, active devices, and inactive devices.
9. Under Tasks, click the link for Current Ongoing Tasks. The Operations Information page appears. This page displays the details of each operation that is currently running in any of the clients.

Click  to view the following information.

- Machine name on which the operation is going on.
 - User who has launched the client.
 - Client type and Client ID.
10. Under Licenses, click the link for License Usage. The License Information page appears. It displays the following information.
 - The licensed entity name.
 - The number of licenses for the corresponding entity.
 - The number of licenses currently in use for the corresponding entity.
 11. To save the dashboard report, click  that is present in the upper-right corner of the Dashboard page.

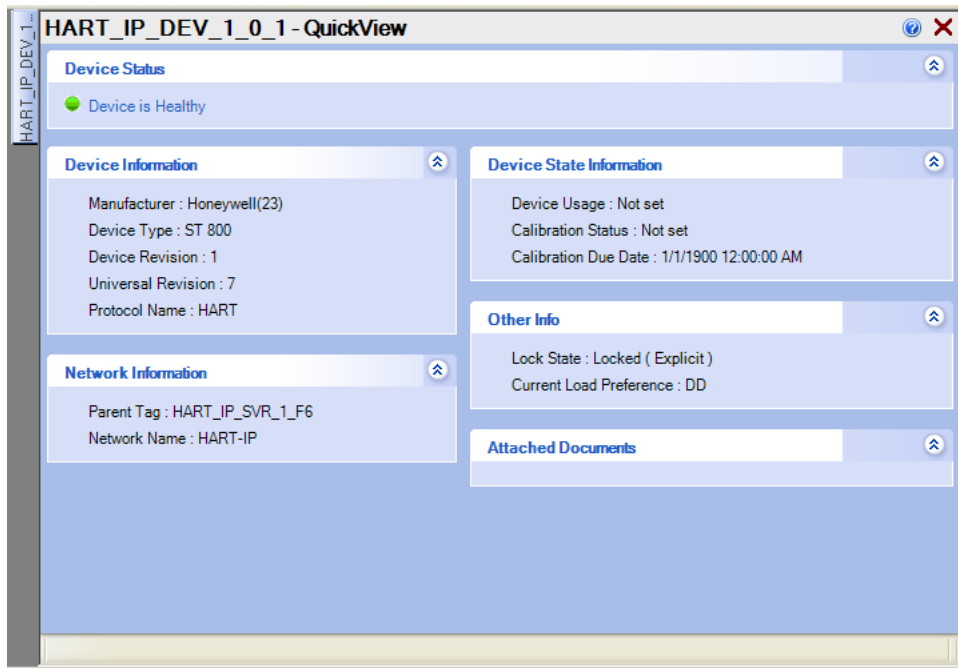
NOTE

The Save Report icon appears shaded if a dashboard Refresh operation is in progress.

26.4 Viewing information through QuickView

To view the information through QuickView option

From the FDM Client network view, right-click the device and then click QuickView. The QuickView page appears.



You can view the following details.

- Device Status: Displays health of the device based on device connection state.
- Device Information: Displays device details and may not match the DD revision.
- Network Information: Displays the configured network name to which device belongs to and parent tag of the respective device.
- Device State Information: Displays the device state details such as device usage, calibration status, and calibration due date.
- Other Info: Displays the device lock state and device load settings (DD/DTM)
- Attached Documents: Displays the attached document if any.

DISPLAY FILTERS

The display filter feature enables you to filter the devices displayed in the Online View > Network View tree. Filters can be created based on network type, manufacturer type, device type, configured networks, protocol, and device tags. When a filter is applied, the Network View tree displays only those nodes/devices included in the filter.

You can create a display filter in the following two ways.

- Query View - Enables you to create a display filter when you select appropriate values for network type, network configured, protocol, manufacturer, device type and tag name.
- Device View - Enables you to create a display filter by selecting the required nodes/ devices from the list of available devices, and moving them to Selected Devices.

NOTE

To create a display filter from Query View, the selected devices need not be connected and online, they may be disconnected devices as well. However, to create a display filter from Device View, only online devices can be included.

27.1 Creating a display filter from the Query View

To create a display filter from the Query View

1. Click the Offline View group. The Offline Configuration, Display Filter and Device Library tabs appear.
2. Click the DisplayFilter tab.
3. Right-click the Display Filter and then click New. The following page appears.

4. Select the network type from Network Type list. To select all the network types, select All. When you select the network type, the networks configured for the selected network type appears in Network Configured drop-down list.
5. Select the desired network configuration from Network Configured drop-down list.
6. Select the desired protocol from Protocol list.

NOTE

- When you filter any protocol such as HART, FF, ISA100, or DE, the Manufacturer name is displayed as Honeywell_23 instead of Honeywell.
- For PROFIBUS protocol devices, Manufacturer name is displayed only if updated DTM is installed on that machine.

7. Select the manufacturer from Manufacturer drop-down list. To include all the manufacturers, select All.
8. Select the device type from Device Type drop-down list. To include all the device types, select All.
9. Tag Name is the name of the device that is displayed in the Network View tree in the left pane of FDM. You can use the tag name to further filter your display filter criteria. Type the tag name either fully or partially. To type partially, use '*'. Example: To include devices with tag name containing STT25H, type *STT*.

Example:

To display devices starting with 'S' and 'A', you can type *S*; *A*. This lists all devices matching the selected query criteria (Network Type, Network Configured, Protocol, Manufacturer, and Device Type) that begin with S and/or A.

For instance, to display devices of type STT25H, type STT25H in the tag name.

NOTE

Use semicolons to separate multiple tag names.

Use Device View filter to filter devices that do not have DD(s).

10. To view the devices included in the display filter, click View. The devices corresponding to the selected filter criteria appear.
11. Click Save to save the display filter. To close the window without saving the changes, click Close.

NOTE

You can Save a display filter, without viewing (performing step 10) the details of the display filter.

12. If you click Save, a dialog box appears prompting you to type the reason for saving display filter. Type the reason for creating the new filter and click OK.

NOTE

The Reason dialog box appears only if the Administrator has enabled reason logging, for this action type, in the Audit Trail settings.

13. The Filter Name dialog box appears. Type the name for the display filter in Name and click OK. FDM saves the display filter with the specified name and displays the filter in the Display Filter tree in the left pane.

TIP

To open the display filter browse through the Display Filter tree, right-click the display filter you want to open and click Open.

To modify you can re-select the Display Filter criteria in the Query View or re-select the nodes/devices in the Device View.

To rename the display filter browse through the Display Filter tree, right-click the display filter you want to rename and click Rename.

To delete the display filter browse through the Display Filter tree, and right-click the display filter you want to delete and click Delete.

NOTE

FDM does not allow you to rename and delete a display filter, if the display filter has been applied to the Network View tree in the Online View group or if the display filter is open in any FDM Client.

14. To apply this display filter, select the display filter from the Display Filter drop-down list and then click 463BApply. FDM applies the display filter and displays only those nodes/devices included in the selected Display Filter.

NOTE

If none of the network nodes/devices that are included in the display filter is online and connected to FDM, then the Network View appears blank and does not display any device.

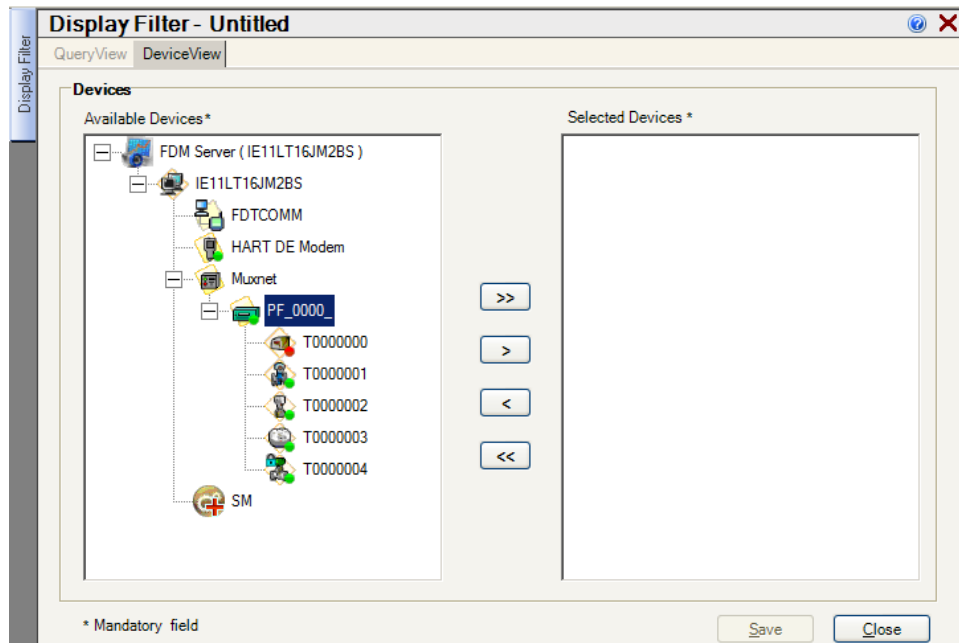
15. To remove an applied filter, choose the No Filter option from Display Filter and click Apply.

27.2 Creating a display filter from the Device View

Creating a display filter from the Device View involves selecting one or more nodes/devices that you want to be displayed in the Network View list.

To create a display filter using the Device View

1. Click the Offline View group. The Offline Configuration, Display Filter, and Device Library tabs appear.
2. Click the Display Filter tab.
3. Right-click the Display Filter and click New. The Display Filter page appears.
4. Click the Device View tab.



5. The online devices connected to FDM in Available Devices appear. Select the desired network node(s)/ device(s) using the following buttons.
 - To select all nodes/devices in the network (under Available Devices) and move them to Selected Devices, click .
 - To select a single node/device (under Available Devices) and move it to Selected Devices, click .
 - To remove a single node from Selected Devices, click .
 - To remove all the nodes from Selected Devices, click .

NOTE

You cannot select only the OneWireless adapter or only the devices under OneWireless adapter. You should select both OneWireless adapter and device under it.

You must select at least one device for creating a display filter from the Device View.

6. Click Save. The Reason dialog box appears. Type the reason for creating the new filter. The Filter Name dialog box appears.

NOTE

The Reason dialog box appears only if the Administrator has enabled reason logging, for this action type, in the audit trail settings.

7. Type the name for the display filter and click OK. FDM saves the display filter with the specified name and displays it in the Display Filter tree.
8. To apply this display filter, select the display filter from the Display Filter drop-down list and then click **Apply**. FDM applies the display filter and displays only those nodes/devices included in the selected Display Filter.

NOTE

If none of the network nodes/devices that are included in the display filter is online and connected to FDM, then the Network View appears blank and does not display any device.

9. To remove an applied filter, choose the No Filter option from Display Filter and click Apply.

27.3 Searching for devices using advanced search

FDM provides an advanced search feature to find the required devices listed under the FDM Server. To search for a device, you can use any of the following independently, or as a combination.

- Protocol indicates the type of devices which can be HART, FF, ISA100, PROFIBUS, or DE.
- Manufacturer ID indicates the unique ID for each device manufacturer.
- Device Type indicates the type of device – for instance, the device can be a pressure transmitter, temperature transmitter or flow transmitter.
- Device Tag indicates the tag as configured for the device. It can be alphanumeric string of length 8 characters.
- FDM Tag is the tag displayed for a device in the Network View tree.

Example:

If you want to search for an STT25H temperature transmitter manufactured by Honeywell, perform the following:

- a. Select HART protocol from the Protocol list.
- b. Select the Honeywell_23 from the Manufacturer ID list
- c. Select the device type for the STT25H from Device Type list.
- d. Click Search. FDM lists all the STT25H devices configured in the network.

TIP

To broaden your search results, restrict your search criteria to a few fields.

To show all devices from a given vendor, ensure to include the vendor name as listed by all protocols. Hence, for all Honeywell devices, use HART, Fieldbus, and DE list manufacturer names.

Based on the search result, the device names are listed. When you double-click the device, it is displayed in the Network View tree, if the device is online.

To search the required devices listed under the FDM Server, perform the following steps.

1. Click Tools > Advanced Search. The Advanced Search page appears.

TIP

You can also click the Advanced Search icon under the FDM tool bar.

2. To search
 - by protocol, select an appropriate value in Protocol. AND/OR
 - by manufacturer ID, select an appropriate value in Manufacturer ID. AND/OR
 - by device type, select an appropriate value in Device Type. AND/OR
 - by device tag, type an appropriate value in Device Tag. AND/OR
 - by FDM tag, type an appropriate value in FDM Tag.
3. Click Search. If a device matching the search criteria you have entered is found, it displays the search results in the Search Result pane.
4. Double-click the required device. FDM locates the device in the Network View tree, provided the device is online.

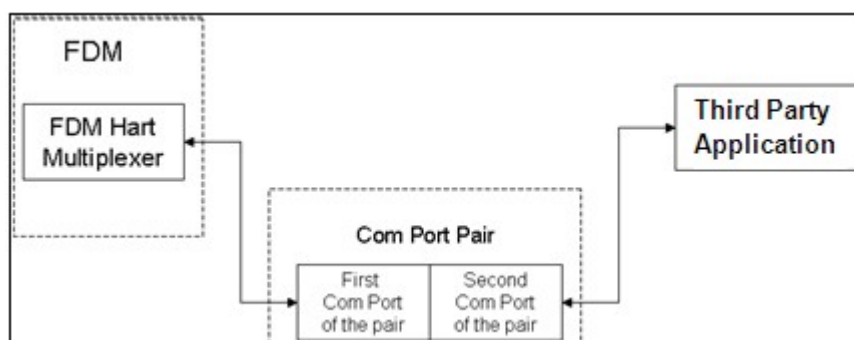
ABOUT FDM HART MULTIPLEXER (FHM)

The optional FDM HART Multiplexer (FHM) can be used by a third party application, such as valve diagnostic application to communicate with the HART devices connected to the FDM through one of the following networks.

- Experion PKS network
- Experion-integrated Safety network
- Experion-integrated OneWireless network
- RS-485 HART Multiplexer
- HART Modem
- HART DE Modem
- HART-IP network
- OneWireless network

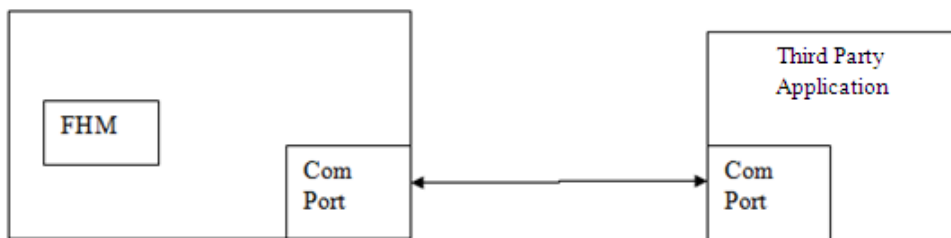
Though FHM emulates P+F multiplexer behavior to allow third party applications to connect through FDM, all P+F multiplexer functions may not be supported.

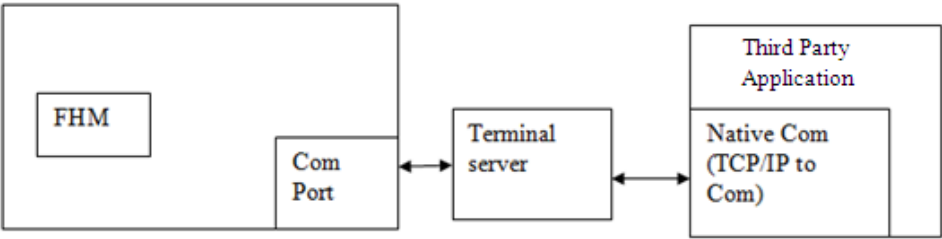
The following figure depicts the FHM installed on FDM Client.



FHM can also be installed on any other FDM node other than the node where the third party application is installed.

The following topologies are supported.





FHM can be used through an actual (real) pair of COM Ports or through a virtual COM port pair provided by the user. You must configure the pair of COM ports in a loopback connection and wire a loopback cable to connect the two ports. In FDM, you have to manually select the COM port that must be used by the FHM from the COM Port field. The third party application uses the other COM port.

The third party application communicates with the FHM through the COM ports that are selected. The third party application through FHM communicates with the devices connected to FDM through various networks.

28.1 User role privileges

The following table lists the privileges of all the groups with respect to FHM.

User Role	Privileges
Administrator	Create Device list Modify device list Delete device list Enable/Disable Write Access Note: Users with Administrator's role have the highest level of privileges and have full access to all the FHM functions.
Engineer	Create Device list Modify device list Delete device list
Supervisor	Create Device list Modify device list Delete device list
Operator	Create Device list Modify device list Delete device list

28.2 Enabling third party application for write access

The process active devices are read-only in FDM. The write operations cannot be performed on process active devices.

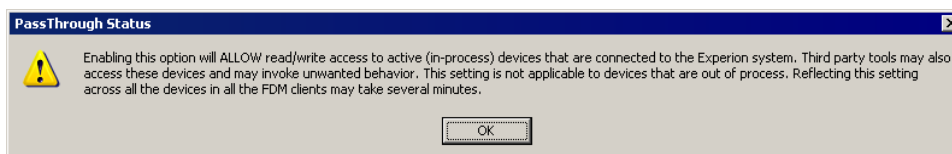
FDM has an option to enable the third party application to write to the HART devices even when the devices are in process active state. If the Allow Write Access for Process Active Devices option is enabled in FDM settings, the third party application can write to devices in the active state that are connected to the Experion network.

NOTE

- Allow Write Access for Process Active Devices option must not be selected in the following instances: If the network build is in progress Or If the device is getting loaded in FDM
- Only users with Administrator privileges can enable/disable the write access for the Experion connected devices.
- Users must have Windows Administrator/ power user privileges to Start/ Stop FHM service.

To allow write access for the Experion connected devices

1. In FDM Client, choose FDM > Settings. The Settings dialog box appears.
2. Under Write Access For Experion Connected HART Devices, select Allow write access for Process Active Devices check box. By enabling this check box, third party application can write to the Experion-connected process-active devices. The following confirmation message appears.



3. Click OK. The write access is enabled for the Experion connected process active devices.

28.3 Configure a device list

A device list must be created for the third party application to communicate with the selected devices. FHM enables you to configure a device list based on selection of multiple manufacturer and the device types. The device list can be created, modified or deleted. The created device list can be used for viewing the devices in the third party application such as ValveLink application.

28.3.1 Creating a device list

To create a device list, perform the following steps.

Prerequisites

Ensure that at least one device revision DD is available for a given device type to create device list.

To create a device list

1. In FDM Client, choose Tools > FDM HART Multiplexer > Configure DeviceList. The HART Mux Device list configuration wizard appears.
2. Click Create and then click Next.
3. In the next page, select one or more device manufacturer from the Manufacturer list box.

NOTE

Based on the third party application, select the appropriate device manufacturer.
For example: If the third party application is ValveLink, select Fisher Control as the device manufacturer.

The list of devices corresponding to the manufacturer appears in the Device Type list box.

4. Select one or more devices from the Device Type list box.

NOTE

Select All to select all devices in the Device Type list box.

5. Click View. The list of devices in the network that match with the device type of the selected manufacturer appears.

NOTE

Enter the starting characters of the device tag name followed by “*” in Tag Name and click View. For example, enter “INV*” to view a list of devices with tag name starting with “INV”.

Asterisk – “*” is a wildcard character used for selecting the devices.

6. Click Next. The Save DeviceList dialog box appears.
7. In the DeviceList box, enter a name for the device list. Ensure that the device list name matches the following criteria:
 - Unique name and maximum length – 16 characters
 - Special characters are not allowed.
8. Click Save.

NOTE

The saved device lists can be viewed in the FHM UI. If you want to attach an application, go to step 11.

9. Click Next. A confirmation message appears.
10. Click No to save the device list without attaching an application. Go to step 12.
11. Click the browse icon  associated with the Application Name to attach an application. For more information about launching an application, refer to the section [“Launching an attached application”](#).
12. Enter the Display Name, and Application Arguments if any.

13. Click Next.
14. Click Finish.

28.3.2 Modifying a device list

To modify a device list

1. In FDM Client, click Tools > FDM HART Multiplexer > Configure Device List. The HART Mux Device list configuration wizard appears.
2. Click Modify and then click Next. In the next page, select a device list name from the Existing device list(s) list. The selected manufacturer and the device type are highlighted in the respective Manufacturer and DeviceType list.
3. Click View to view the list of devices.

NOTE

You can select multiple manufacturer or device type to modify the device list.

4. Click Next. The message appears to confirm the selected device list modification.
5. Click Yes to modify the device list. The page appears with the options for attaching an application. If you want to attach an application, go to step 9.
6. Click Next. A confirmation message appears.
7. Click No to save the device list without attaching an application. Go to step 13.
8. Click the browse icon  associated with the Application Name to attach an application.
9. Enter the Display Name and then enter Application Arguments, if any.
10. Click Next.
11. Click Finish.

28.3.3 Deleting a device list

To delete a device list, perform the following steps.

1. In FDM Client, click Tools > FDM HART Multiplexer > Configure Device List. The HART MUX Device list configuration wizard appears.
2. Click Delete and then click Next. In the next page, select a device list name from the Existing DeviceList(s) list. The selected manufacturer and the device type are highlighted in the respective Manufacturer and Device Type lists.
3. Click View to view the list of devices and then click Next. A message appears to confirm the selected device list deletion.
4. Click Yes to delete the device list.
5. Click Finish.

NOTE

The device list cannot be deleted when a third party application is using the devices in the specified list.

28.4 Communicating third party application with HART devices

This section describes the usage of FHM and how the devices are made available to the third party application.

NOTE

The device list must be created before initiating the third party application to communicate with the FDM-connected devices through FHM.

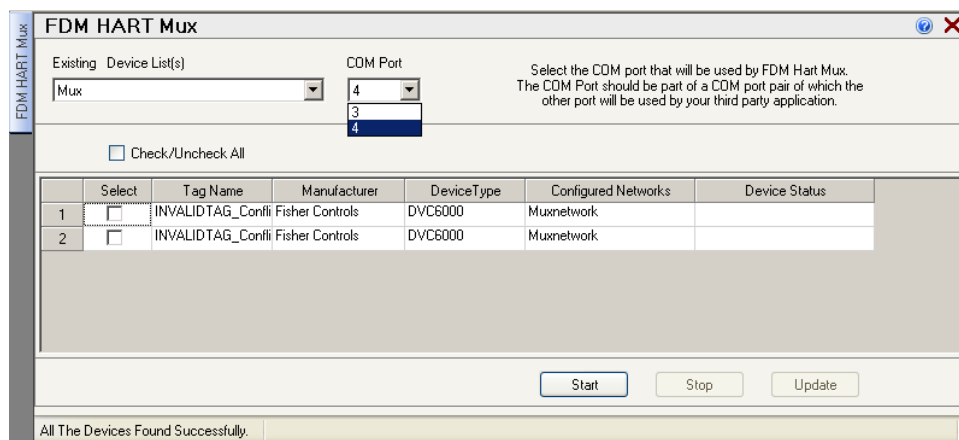
To create a device list, see [“Creating a device list”](#) 1.

To use FHM, perform the following steps.

1. Click Tools > FDM HART Multiplexer > HART Multiplexer. The FDM HART Mux window appears.
2. Select an already existing device list from the Existing DeviceList(s) list. The list of devices appears in the lower pane.
3. Select the communication port that must be used by the FDM HART MUX from the COM Port.

NOTE

The communication port selected must be a part of a COM Port pair of which the other communication port must be used by the third party application.



The following device details appear.

- Tag Name
- Manufacturer
- DeviceType
- Configured Networks
- Device Status

- Select the devices that you want to make available to the third party application.

NOTE

- The third party application communicates only with the selected devices.
- Individual device can be selected by selecting respective check box.
- Select the Check/Uncheck All check box to select all the devices.
- Clear the Check/Uncheck All check box to clear the selection.

- Click Start.

NOTE

If there are no devices selected in the device list, a message appears you to select the device(s). Click OK and perform step 4.

If the third party application is not connected to the other COM port in the loopback configuration, a message appears to connect the third party application.

- Click OK. When the FHM starts, the third party application starts communicating with the selected devices.

28.4.1 Updating the device list

The device list can be enhanced by selecting more number of devices that can be used by the third party application.

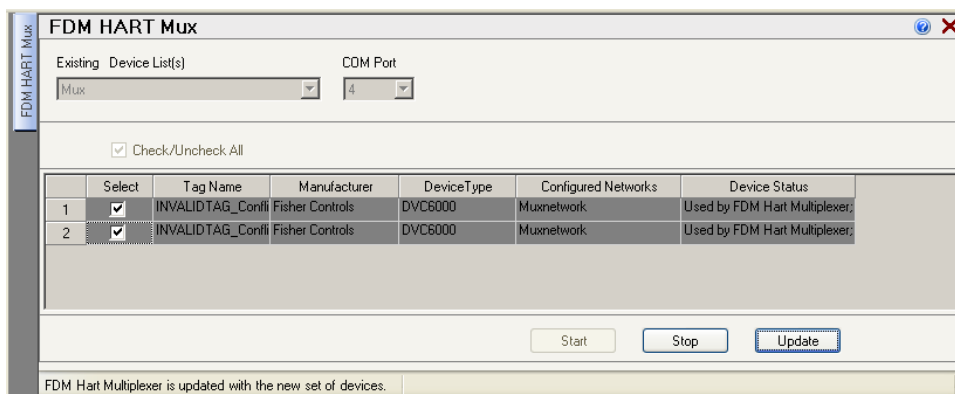
To update the device list

- Select the additional devices that you want to make available to the third party application.

NOTE

- The third party application communicates only with the selected devices.
- Individual device can be selected by selecting respective check box.
- Select the Check/Uncheck All check box to select all the devices.
- Clear the Check/Uncheck All check box to clear the selection.

- Click Update. The following window appears.

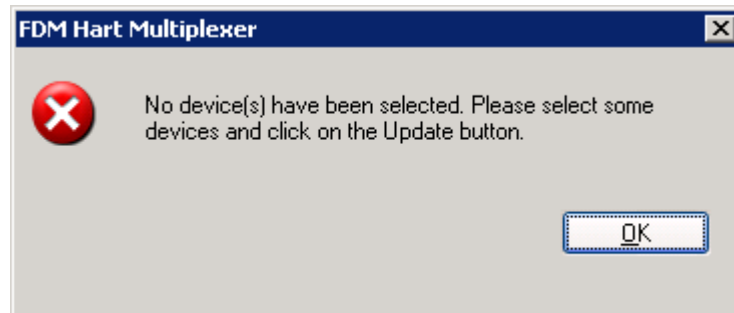


Now the additional devices selected from the device list is available to the third party application for communication.

NOTE

The devices, which are used by the third party application, cannot be modified or deleted.

If you update the device list without selecting the devices, the following error message appears.



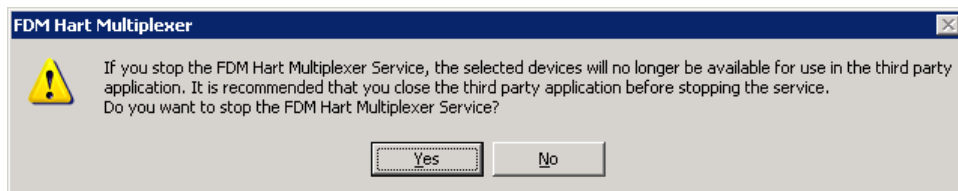
Click OK to continue.

28.4.2 Stopping the FHM

You can stop FHM for the devices selected to communicate with the third party application. The selected devices will no longer be available for use in the third party application.

To stop the FHM:

1. Close the third party application, which is connected to the FDM HART Multiplexer service.
2. Click Stop. The following message appears.



3. Click Yes to stop the FDM HART Multiplexer service.

NOTE

If you close the FDM HART MUX window without stopping the FHM service, the following error message appears.



Click Yes to continue.

You cannot stop the FHM when the third party application is running. Hence, it is always recommended to stop the third party application before you stop the FDM HART Multiplexer service.

28.5 Device locks in FHM

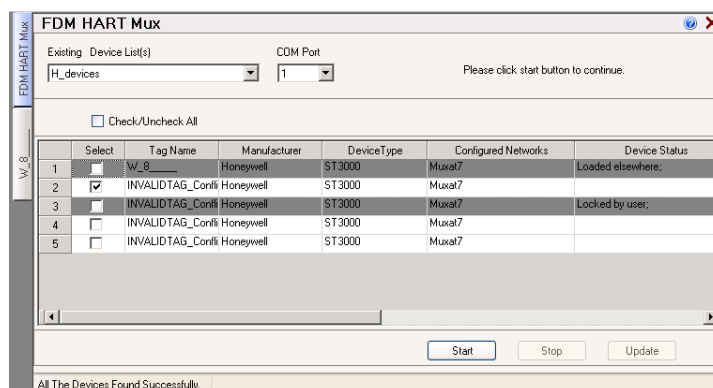
The following device locks are preventing devices from being used in FHM.

- Explicit lock
- Implicit lock
- Process lock (when the device is connected to the Experion network)

Also, if a device is being used by FHM, then they are not available for use in FDM Client.

NOTE

- When the device is loaded and explicitly locked by the FDM Client in other instance of FHM or process active, FHM user interface restricts the Client to select the device. You cannot view the device configuration in FHM.
- The devices that are locked in FHM are not available for use in other instance of FHM.



- When the device is exclusively locked by any of the FDM Client other than currently running FDM Client, FDM HART Multiplexer UI prevents the FDM Client to select the device.

DEVICE DOCUMENTATION-RELATED OPERATIONS AT SYSTEM/DEVICE LEVELS

FDM enables Administrators, Engineers, and Supervisors to attach device documents for a device instance, device type or at the system level (applicable to all devices across FDM) in any chosen document format. These documents can have information related to the specific device instance, device type or system level information.

NOTE

- Before you attach the documents, perform a scan using the recommended and up-to-date antivirus software to ensure that the documents are free from malware. Honeywell is not responsible for any damages caused by corrupted documents with malware present.
- Attaching documents at Device type level is applicable only to the DD library. You cannot attach documents to the DTM library.

Device documentation can be maintained at following three levels.

- **Device Instance Level** - Device documentation for a specific device instance can be attached/detached/ opened/modified/uploaded from the Online View > Network View tab. The document is associated only with device instance.
- **Device Type level** - Device documentation for a Device Type can be attached/detached/opened/modified/ uploaded from the Offline View > Device Library tab. The document is associated with all the devices of that type.

NOTE

FDM does not support attach/detach/upload of device documentation for DE devices at device type level from the Offline View > Device Library.

- **System level** – Device documentation can be attached/detached/opened/modified from the Tools > Systems Documents menu. The document is associated with the FDM application.

Task	To achieve, perform the following
Attaching document	Choose Offline View > Device Library > DD Library. Right-click Device Revision No and choose Device Documentation > Attach Document.
Uploading document	Choose Offline View > Device Library > DD Library. Right-click Device Revision No and choose Device Documentation > Upload Document.
Detaching document	Choose Offline View > Device Library > DD Library. Right-click Device Revision No and choose Device Documentation > Detach Document.

29.1 Attaching device documentation at device-type level

NOTE

FDM does not support attach/detach/upload of device documentation for DE devices at device type level from the Offline View > Device Library.

To attach device documentation at the Device-type level, perform the following steps.

1. Log on to the FDM Client.
2. Under Offline View, click the Device Library tab.
3. Browse through the DD Library tree and expand the network tree corresponding to the Device Type.
4. Select a Device Revision No.
5. Right-click and choose Device Documentation > Attach Document.

NOTE

The Reason dialog box appears, only if the Administrator has enabled reason logging for this action type in the Audit Trail settings.

6. Type the reason and click OK. The Open dialog box appears.
7. Browse through your computer and locate the folder where you have saved the document.
8. Select the document and click Open.
FDM attaches the document to the specific device type and a confirmation message appears.
9. To crosscheck if the document is attached, browse through the Device Library. Expand Manufacturer > Device Type > Device Revision No. Right-click the device revision no to which you have attached the document and click Device Documentation. The name of the attached document appears as a submenu under Device Documentation.

NOTE

- Device Documentation attached at the Device Type level can also be opened, modified, and uploaded at the Device Instance level.
- Two documents of the same type (.xls or .csv) attached to the device-type level cannot be opened at the same time. Close the first document and then open the second document of the same type.
- Any modification that you make after opening an attached document is only saved in the local version of the device document on the FDM Client. It is not updated onto the FDM Server, until you upload the document with the changes.
- Ensure that the document you want to detach is closed. FDM does not allow you to detach an open document.

29.2 Attaching device documentation at device instance level

To attach device documentation at the device instance level

1. Log on to the FDM Client.
2. From the Online View, click the Network View tab.
3. Browse through the network.
4. Right-click a device and then click Device Documentation > Attach Document. The Open dialog box appears.
5. Browse through your computer and locate the folder where you have saved the document.
6. Select the document and click Open. FDM attaches the document to the specific device and a confirmation message appears.
7. To crosscheck whether the document has been attached, browse through the Network View, select the device, right-click and click Device Documentation. The name of the attached document appears as a submenu under Device Documentation.

NOTE

- The two documents of the same type (.xls or .csv) attached to the device instance level cannot be opened at the same time. Close the first document and then open the second document of the same type.
- Any modification that you make after opening an attached document is only saved in the local version of the device document on the FDM Client. It is not updated on the FDM Server, until you upload the document with the changes.
- Documents attached at the device instance level can also be opened, modified, and uploaded from the device type level.

29.3 Attaching device documentation at system level

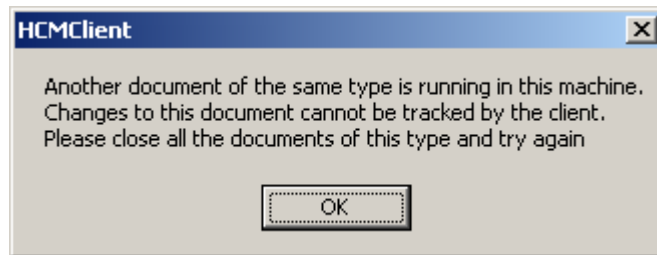
To attach device documentation at the system level

1. Log on to the FDM Client.
2. Click Tools > System Documents > Attach Document. The Open dialog box appears.
3. Select the document that you want to attach and click Open. FDM attaches the document at the system level and a confirmation message appears.

4. Click OK.

NOTE

- The two documents of the same type (.xls or .csv) attached to the system level cannot be opened at the same time. Close the first document and then open the second document of the same type.
- If another document of the same type as the attached document is open in your system, FDM does not allow you to open the attached document. An appropriate message appears.



- Close the document of the same type as the attached document and then retry opening the attached document.

NOTE

Ensure that you upload the document(s) that you modify. If you do not upload, the changes to the document(s) are lost when you close the FDM Client.

Documents attached at the System Level, can only be detached from the System Level and not from the device level.

29.4 Uploading an updated document

If you open a device document attached at the device type level and modify it, you must ensure that it is uploaded onto the FDM Server, so that the changes are updated in FDM and the modified document(s) are available to all users. You can upload a modified document at the device type, device instance, and system level.

NOTE

FDM does not support attach/detach/upload of device documentation for DE devices at device type level from the Offline View > Device Library.

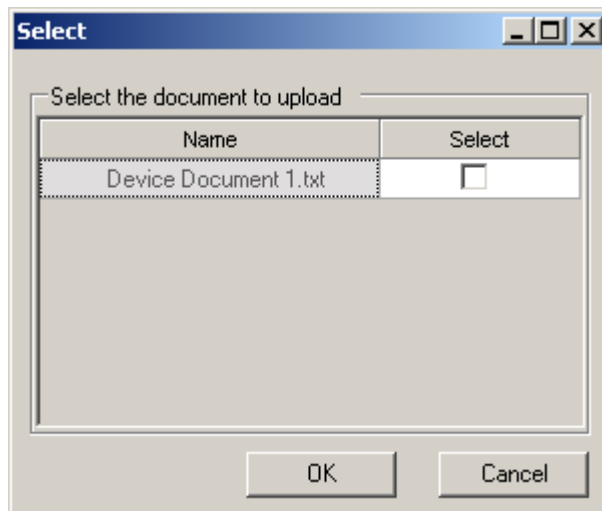
For example, to upload a modified document at device type level to the FDM Server, perform the following steps.

1. Log on to the FDM Client.
2. Under Offline View, click the Device Library tab.
3. Browse through the Device Library tree.
4. Expand the Manufacturer > Device Type > Device Revision No. Right-click the device revision no to which you have attached the document and click Device Documentation > Upload Document.

NOTE

- The Upload Document option is enabled only if you have attached at least one document to a device type.
- The Upload Document option lists only those (attached) documents that are opened and modified from the FDM Client using the Device Documentation > 'Document Name' menu option. Hence, ensure that you open and modify the attached document from FDM Client only.
- A document attached at the device type level can also be uploaded by launching from a device instance.

5. The following dialog box appears.



This dialog box lists all the documents are opened and modified, from the FDM Client, but not uploaded onto the FDM Server.

6. Select the check box corresponding to the document(s) you want to upload. Click OK. FDM uploads the revised document to the FDM Server.

NOTE

Some type of documents such as Microsoft Paint documents (.bmp) cannot be tracked by FDM. So if you attach a BMP file, launch it from FDM, modify it and save it, this document is not detected as being modified by FDM and hence, it is not available for upload. (An error message appears, stating that there is no document to upload). To upload such documents, detach the document and attach it again after modification.

29.5 Detaching device documents

You can detach documents attached to a device, device type or system level.

To detach documentation attached to a device

1. Log on to the FDM Client.
2. From the Online View, click the Network View tab.
3. Browse through the network.
4. Right-click a device and click Device Documentation > Detach Document. The Select dialog box appears.

NOTE

- If a document is attached at the Device Type level, it can only be detached from the Device Type (from Offline View > Device Library tab). It cannot be detached from a Device (Online View > Network View tab) belonging to that Device Type.
- However, you can open, modify, and upload documents attached at a Device Level, from a device (Online View > Network View tree).

5. Select the check box corresponding to the document(s) you want to detach and then click OK.

NOTE

Ensure that the document you want to detach is closed.

A confirmation message appears.

6. To proceed with the operation, click Yes in the message box. The Reason dialog box appears.
7. Type the reason in the dialog box and click OK. FDM detaches the device.

NOTE

The Reason dialog box appears only if the Administrator has enabled reason logging, for this action type, in the Audit Trail settings.

FDM APPLICATION-RELATED OPERATIONS AT SYSTEM/ DEVICE LEVELS

FDM enables Administrators, Engineers, and Supervisors to attach applications for a device type or at the system level (applicable to all devices across FDM). These applications can be any third party applications that you can use to perform additional tasks on the devices or can be any other tool, which is relevant to device management.

NOTE

Before you attach the applications, perform a scan using the recommended and up-to-date antivirus software to ensure that the applications are free from malware. Honeywell is not responsible for any damages caused by corrupted applications with malware present.

Application can be maintained at the following two levels.

- Device-Type level - Application for a Device-Type can be attached/launched/detached from the Offline View > Device Library tab.

NOTE

FDM does not support attach/launch/detach of any application for DE devices at device type level from the Offline View > Device Library tab.

- System level – Application can be attached/launched/detached from the Tools > Other Applications menu.

Task	To achieve, perform the following
Attaching application	Choose Offline View > Device Library > DD Library. Right-click Device Revision No and then click Applications > Attach Application.
Launching application	From the applications listed under Applications, click the application that you want to launch.
Detaching application	Choose Offline View > Device Library > DD Library. Right-click Device Revision No and then click Applications > Detach Application.

NOTE

Attaching applications at device type level is applicable only to the DD library. You cannot attach applications to the DTM library.

Attached applications are client specific. This means that if you attach an application in one client, it is valid only on that computer. You cannot launch or detach that application from another client.

30.1 Attaching an application at device-type level

NOTE

FDM does not support attach/launch/detach of any application for DE devices at device type level from the Offline View > Device Library tab.

To attach an application at the device-type level

1. Log on to the FDM Client.
2. Under Offline View, click the Device Library tab.
3. Browse through the DD Library tree and expand the network tree corresponding to the Device Type.
4. Select a Device Revision No.
5. Right-click and click Applications > Attach Application. The Select Application dialog box appears.
6. Click  to browse for an application. The Open dialog box appears.
7. Browse through your computer and locate the folder where you have saved the document.
8. Select the application and click Open. The Select Application dialog box appears displaying the application name along with its path in the Display Name.
9. Enter a suitable display name to the application in the Display Name.
10. If any arguments are to be passed to the attached application, enter them in the Application Arguments.
11. Click OK. FDM attaches the application to the specific device type and a confirmation message appears.
12. Click OK.
13. To crosscheck whether the application has been attached, browse through the Device Library, expand the Manufacturer > Device Type > Device Revision No to which you have attached the application. Right- click and click Applications. The name(s) of application(s) appears as a submenu under Applications.

30.2 Attaching an application at system level

To attach an application at the system level

1. Log on to the FDM Client.
2. Click Tools > Other Applications > Attach Application. The Select Application dialog box appears.
3. Click  to browse for the application. The Open dialog box appears.
4. Browse to the location where you have saved the application on your computer.
5. Select the application that you want to attach and click Open. In the Select Application dialog box, the application name appears along with its path in the Display Name.
6. Type a suitable display name to the application in Display Name.
7. Type the arguments in Application Arguments and click OK. FDM attaches the application at the system level and a confirmation message appears.
8. Click OK.
9. To crosscheck whether the application has been attached, click Tools > Other Applications. The name(s) of the attached application(s) appears as a submenu under Other Applications.

NOTE

If the application is already launched on your computer, FDM does not allow you to launch the attached application. An appropriate error message appears.

Close the application and then retry launching the attached application.

30.3 Launching an attached application

You can launch the attached application from device type and also from the system level.

To launch an application attached at the system level

1. Log on to the FDM Client.
2. Click Tools > Other Applications > <Name of attached application>. FDM launches the selected application.

NOTE

If the application is already launched in your system, FDM does not allow you to launch the attached application. An appropriate error message appears.

Close the application and then retry launching the attached application.

30.4 Detaching an attached application

You can detach an application at device type and system level.

NOTE

FDM does not support attach/launch/detach of any application for DE devices at device type level from the Offline View > Device Library tab.

To detach an application attached at the device-type level

1. In the FDM Client, under Offline View, click the Device Library tab.
2. Browse through the Device Library tree.
3. Expand the Manufacturer > Device Type > Device Revision No to which you have attached the application.
4. Right-click and click Applications > Detach Application. The Select dialog box appears.
5. Select the check box corresponding to the application(s) you want to detach.
6. Click OK. An appropriate confirmation message appears.
7. Click Yes to detach the application or click No to cancel the operation.

NOTE

Ensure that the application you want to detach is closed. FDM does not allow you to detach an application that is running. An appropriate message appears.

If you click Yes, FDM detaches the application from the specific device type and a confirmation message appears.

8. Click OK.

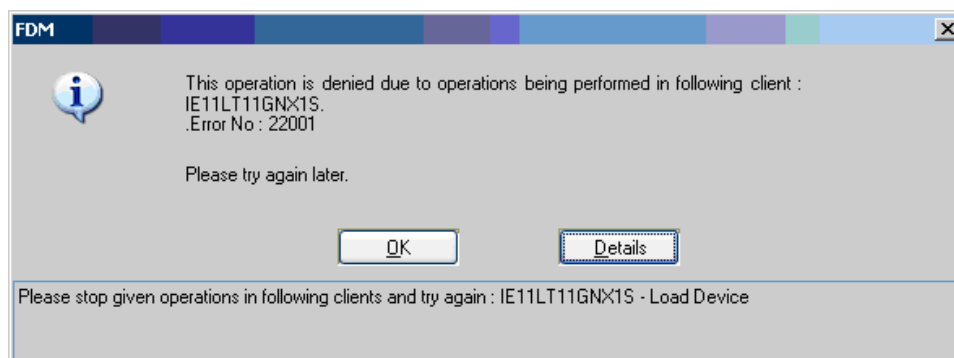
NOTE

Applications attached at the device-type level cannot be detached at the device level.

FDM OPERATIONAL RESTRICTIONS

In a multiple client scenario, it is important to ensure integrity of the operations. Therefore, FDM restricts concurrent execution of certain operations to ensure success of a given operation.

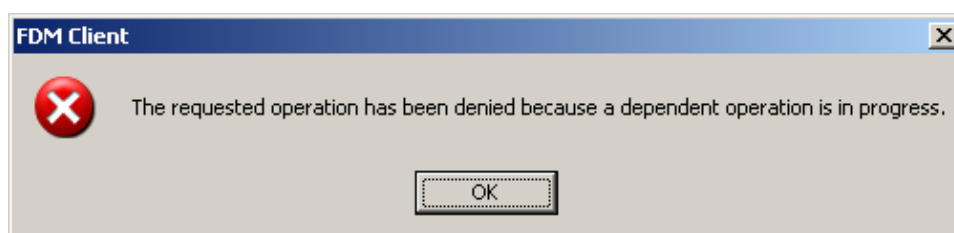
When you try to execute an operation and if this operation is rejected by FDM Server, as certain operation(s) are currently in progress on other clients, following error message is displayed.



The error message gives the list of clients performing other operations, due to which, the current operation is denied.

- Click Details button to view the list of operations in each of the clients that are restricting the current operation.
- Click OK button to acknowledge the message.

If the attempted operation is restricted due to operations being performed by the same client, then the following error is displayed.



You may have to wait for these operations to complete or stop them to perform the necessary operation. The following table lists various operations and the operations that are restricted when they are in progress.

Current Operation	Restricted operation
Open Device Configuration	Bulk History, Bulk Template, Bulk Offline Download, and Import Export
Bulk History	Open Device Configuration, Explicit Build Network, Bulk History, Bulk Template, Bulk Offline Download, Import Export, Open Offline Configuration, Save Offline Configuration, Delete Offline Configuration, Rename Offline Configuration, Rename Tag, View Audit Trail, Add DD file, Delete DD file, Delete History, FDM Settings (Device Configuration Load Option and Write Access option), Tag Builder, and Delete Records
Bulk Template	Open Device Configuration, Explicit Build Network, Bulk History, Bulk Template, Bulk Offline Download, Import Export, Open Offline Configuration, Save Offline Configuration, Delete Offline Configuration, Rename Offline Configuration, Rename Tag, View Audit Trail, Add DD file, Delete DD file, Delete History, FDM Settings (Device Configuration Load Option and Write Access option), Tag Builder, and Delete Records
Bulk Offline Download	Open Device Configuration, Explicit Build Network, Bulk History, Bulk Template, Bulk Offline Download, Import Export, Open Offline Configuration, Save Offline Configuration, Delete Offline Configuration, Rename Offline Configuration, Rename Tag, View Audit Trail, Add DD file, Delete DD file, Delete History, FDM Settings (Device Configuration Load Option and Write Access option), Explicit Lock Node, Tag Builder, and Delete Records
Import Export	Open Device Configuration, Explicit Build Network, Bulk History, Bulk Template, Bulk Offline Download, Import Export, Open Offline Configuration, Save Offline Configuration, Delete Offline Configuration, Rename Offline Configuration, Rename Tag, View Audit Trail, Add DD file, Delete DD file, Delete History, FDM Settings (Device Configuration Load Option and Write Access option), Tag Builder, and Delete Records
Open Offline Configuration	Bulk History, Bulk Template, Bulk Offline Download, and Import Export
Save Offline Configuration	Bulk History, Bulk Template, Bulk Offline Download, and Import Export
Delete Offline Configuration	Bulk History, Bulk Template, Bulk Offline Download, and Import Export
Rename Offline	Bulk History, Bulk Template, Bulk Offline Download, and Import Export

Current Operation	Restricted operation
Configuration	
Rename Device Tag	Bulk History, Bulk Template, Bulk Offline Download, and Import Export
Add DD File	Bulk History, Bulk Template, Bulk Offline Download, Import Export, Add DD File, Delete DD File, and Tag Builder
Delete DD File	Bulk History, Bulk Template, Bulk Offline Download, Import Export, Add DD file, and Delete DD File
View Device History	Bulk History, Bulk Template, Bulk Offline Download, and Import Export
FDM Settings (Device Configuration Load Option and Write Access option)	Bulk History, Bulk Template, Bulk Offline Download, and Import Export
Tag Builder	Bulk History, Bulk Template, Bulk Offline Download, Import Export, and Add DD file
Delete Records	Bulk History, Bulk Template, Bulk Offline Download, Import Export, and Delete Records
Online Update Operation	Build network for any network at any level (Network level, Safety group, Process group, SM, IOTA and so on.), Bulk Operations, Device Load Note: It is recommended not to perform any network related operations in Client when online update is being performed.

DELETE RECORDS

Using this feature, you can delete the records such as device tags, offline device configuration, history records, and PVST reports for multiple devices at a time.

32.1 Deleting device tags

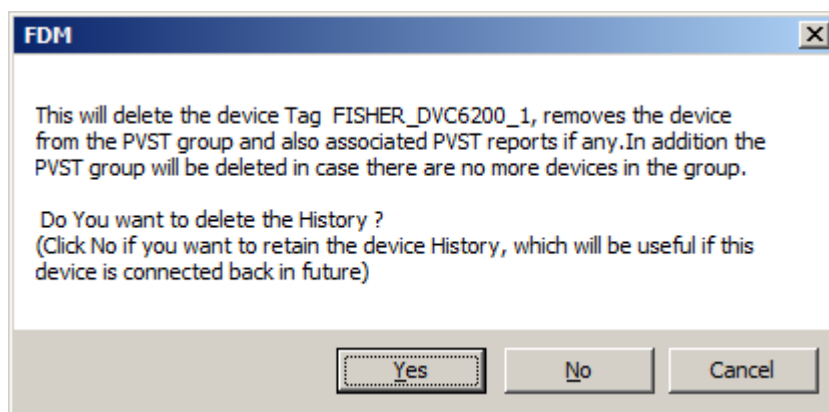
You can delete the disconnected device tags in the following two ways.

- Using Delete Tag/Delete All option under Disconnected Nodes list
- Using Delete Records feature

Deleting a device tag creates a free tag slot in the license.

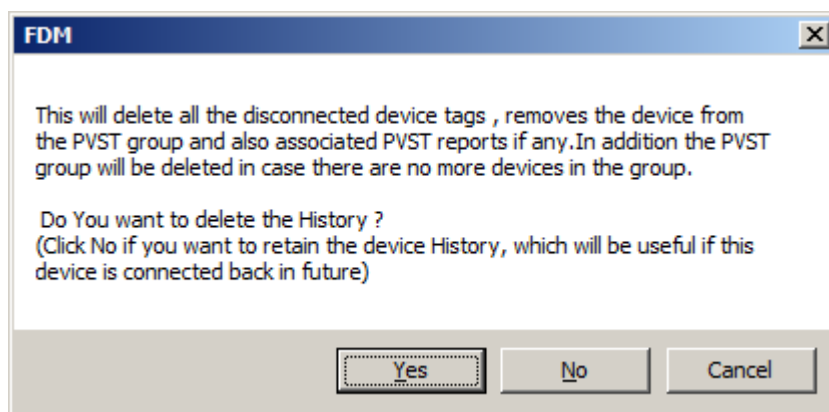
To delete the device tags using Delete Tag/Delete All option under Disconnected Nodes

1. In the FDM Client, under Disconnected Nodes list, right-click the device tag and then click Delete Tag. The following message appears.



Or

2. Right-click the Disconnected Nodes list and then click Delete All. The following message appears.



3. Click Yes, if you want to delete the disconnected device tags , associated PVST reports, and device history records from FDM . Also, the device will be removed from the group, if it is part of PVST group.

TIP

In addition, the PVST group will be deleted in case there are no other devices in the group.

Or

Click No, if you want to delete the device tags and associated PVST reports from FDM. But, the device history records are retained.

To delete the disconnected device tags using Delete Records feature

1. In the FDM Client, click Tools > Delete Records. The Delete Records Wizard appears.
2. Click Device Tags in the list and then click Next. The Delete Device Tags page appears.
3. The Query View enables you to filter the device tags based on the combination of Protocol, Manufacturer, and Device Types.
 - To filter the device tags based on the protocol type, select any protocol from the Protocol list.
 - When you select a protocol from the list, the manufacturer list appears as follows:
 - If you select the HART/FF/ISA100/PROFIBUS protocol then the manufacturer list appears using available respective DD library information. For the device that do not have a DD, the Unrecognized Manufacturers entry is available for the corresponding protocol. If the manufacturer is present in the DTM library then the device's manufacturer appears as a separate manufacturer entry.
 - If you select the DE protocol, then the corresponding manufacturer list appears.

NOTE

When you filter any protocol such as HART, FF, ISA100, or DE, the Manufacturer name is displayed as Honeywell_23 instead of Honeywell.

- If you select a protocol, which do not have an entry in the DD library, then the manufacturer list appears using list of manufacturers from the DTM library. For a device that do not have an entry in the DTM library, the Unrecognized Manufacturers entry is available in the list.
- If you select multiple protocols then the corresponding manufacturers are listed under Manufacturers list.
- You can select device types from device types list. The device types list appears as follows:
 - If you select HART/FF/ISA100/PROFIBUS manufacturers, then the device type appears using the respective DD library.
 - If you select DE manufacturers, then the device type appears for the respective manufacturers.
 - If you select non-DD manufacturers, then the device type appears using the DTM library information available.
 - If you select 'Unrecognized manufacturers' from the manufacturer list then the options available are the default 'All' option and 'Unrecognized device types'.

- To filter the device tags based on Protocols, Manufacturers, and device types, select one or more Manufacturer(s) and Device Type(s).
- To delete all the devices tags, select All for all options in the Query view and then click Next.

NOTE

If the FDT network discovers few devices that uses protocols which are not qualified in FDM, then you must select Unqualified Protocols in the Protocols list.

4. Select the device tag and then click  to move it to the Selected Device Tags List box. Or Click  to move all the device tags to the Selected Device Tag List box.

TIP

The number of device tags selected is listed in the right pane under Selected Device Tag List.

5. Click Next. If the history data is not associated with the device tag, then a message appears to confirm the deletion of the selected device and then perform step 7.

Or

If any of the tag(s) selected for deletion have history data associated with them, the Select Device Tags page appears.

- Under Select column, select the check box for which you want to delete the history data along with the device tag.
- Click Next. A message appears to confirm the deletion of the selected device tag along with history data and then perform step 7.

NOTE

While deleting device tags, it also deletes associated PVST reports if any and removes the device from PVST group. In addition, the PVST group will be deleted in case there are no other devices in the group.

6. Click Delete. In the next page, the progress report displays the progress in deleting the device tags and provides the following information.
- The grid displays the selected device tag and status of device tag deletion operation.
 - Total number of device tags deletion operation succeeded, failed, and aborted.
 - The operation state of the device tags deleted.
7. Click Save Report. The Save As dialog box appears.
8. Enter the file name and then click Save.
9. Click Finish.

32.2 Deleting offline device configuration

You can delete the DD/Generic DD/DTM offline configuration in following two ways.

- Using Delete option under Offline Configuration in Offline View tab.
- Using Delete Records feature

To delete the Offline Device Configuration using Delete option under Offline Configuration

1. In the FDM Client, click the Offline View. The Offline Configuration, Display Filter and Device Library tabs appear.
2. Click the Offline Configuration tab. The DD Offline Configurations/Generic DD Offline Configurations/ DTM Offline configurations tree appear in the left pane.
3. Browse through the tree DD Offline Configurations > Manufacturer > Device Type > Device Revision > Offline Configuration (name), right-click and then click Delete or browse through the tree Generic DD Offline Configurations > Generic Offline Configuration (name), right-click and then click Delete. A confirmation message appears.
4. Click Yes.

To delete DD/Generic DD/DTM offline configuration through Delete Records feature

1. In FDM Client, click Tools > Delete Records. The Delete Records Wizard appears.
2. Click Offline Device Configuration in the list and then click Next. The Delete Offline Device Configuration page appears.
3. Under Offline Library, select the offline configuration which you want to delete.
 - Click  to move it to the Selected Offline Templates box.
 - Click  to move all the offline configurations.
 - Click  to clear the offline configuration from the Selected Offline Templates box.
 - Click  to clear all the offline configurations.

TIP

The number of offline configuration selected are displayed under Selected Offline Templates : <number>.

4. Click Next. In the next page, a message appears to confirm the deletion of the selected offline device configuration.
5. Click Delete. In the next page, the progress report indicates the progress in deleting offline configuration and provides the following information.
 - The grid displays the individual offline template selected and status.
 - Total number of operations succeeded, failed, and aborted.
 - The operation state of the offline device configuration deleted.
6. Click Save Report. The Save As dialog box appears.
7. Enter the file name and then click Save.
8. Click Finish.

32.3 Deleting device history

You can delete the device history records in the following two ways.

- Using Delete History option from the shortcut menu
- Using the Delete Records feature

To delete a history record using Delete History option

1. In the FDM Client, click the Online View. The Network View and Device State View tabs appear.
2. Click the Network View tab. The devices belonging to the connected server are displayed.
3. Right-click the device and then click Delete History. The History Records dialog box appears.
4. Select the check box to delete the device history record. If you want to delete all history records at a time, select the Select All check box.
5. Click OK. The confirmation message appears before you delete the history records.
6. Click Yes. The historized data for the selected device is deleted.

To delete the history records using the Delete Records feature

1. In the FDM Client, click Tools > Delete Records. The Delete Records Wizard appears.
2. Click Device History in the list and then click Next. The Delete Device History page appears.
3. The Query View enables you to filter the history records based on the combination of Network Type, Configured Network, Protocol, Manufacturer and Device Type.
 - To filter the history records based on the Network type, select any Network type, and Configured network corresponding to that network.
 - To filter the history records based on the protocol type, select any protocol from the Protocol list.
 - When you select a protocol from the list, the manufacturer list appears as follows:
 - If you select the HART/FF/ISA100/PROFIBUS protocol then the manufacturer list appears using available respective DD library information. For the device that do not have a DD, the Unrecognized Manufacturers entry is available for the corresponding protocol. If the manufacturer is present in the DTM library then the device's manufacturer appears as a separate manufacturer entry.
 - If you select the DE protocol, then the corresponding manufacturer list appears.

NOTE

When you filter any protocol such as HART, FF, ISA100, or DE, the Manufacturer name is displayed as Honeywell_23 instead of Honeywell.

- If you select a protocol, which do not have an entry in the DD library, then the manufacturer list appears using list of manufacturers from the DTM library. For a device that do not have an entry in the DTM library, the Unrecognized Manufacturers entry is available in the list.
- If you select multiple protocols then the corresponding manufacturers are listed under Manufacturers list.
- You can select device types from device types list. The device types list appears as follows:
 - If you select HART/FF/ISA100/PROFIBUS manufacturers, then the device type appears using the respective DD library.
 - If you select DE manufacturers, then the device type appears for the respective manufacturers.
 - If you select non-DD manufacturers, then the device type appears using the

DTM library information available

- If you select 'Unrecognized manufacturers' from the manufacturer list then the options available are the default 'All' option and 'Unrecognized device types'.
- To delete all the history records, select All for all options in the Query View and click Next.

NOTE

- If the FDT network discovers few devices that uses protocols which are not qualified in FDM, then you must select Unqualified Protocols in the Protocols list.
- If you delete device tags and retain history records of these devices in the database, then these records are termed as Orphan records. To delete these orphan records, select Show Orphan Records check box.

In the next page, you can select device tags for connected devices, disconnected devices, healthy devices, unhealthy devices or for all devices form the list. Corresponding device tags are populated in the Available Device Tags List box.

4. Select the device tag and click  to move it to the Selected Device Tag List box or click  to move all the device tags to the Selected Device Tag List box.

TIP

The number of device tags selected is listed in the right pane under Selected Device Tag List.

5. Click Next.
6. In the next page, click All records or Select Time Duration (From and To) and then click Next.
- If you click All records, all the history records are deleted.
 - If you click Select Time Duration (From and To), the history records of that particular period are deleted.
7. In the next page, select the check box to delete history record and then click Next. In the next page, a message appears to confirm the deletion of the device history records.
8. Click Delete. In the next page, the progress report displays the progress in deleting the history records and provides the following information.
- The grid displays the selected device history record name and status of device history record deletion operation.
 - Total number of device history records deletion operation succeeded, failed, and aborted.
 - The operation state of the device history data deleted.
9. Click Save Report. The Save As dialog box appears.
10. Enter the file name and then click Save.
11. Click Finish.

32.4 Deleting PVST reports

If you want to delete the PVST reports that are generated using PVST Planner, perform any one of the following:

- Using Delete Tag/Delete All option under Disconnected Nodes list
- Using Delete Records > Device Tags option. For more information about deleting PVST reports using Delete Tag/Delete All option and Delete Records > Device Tags option, refer to the section [“Deleting device tags”](#).
- Using Delete Records > PVST Reports option. For more information on how to generate PVST reports, refer to the FDM PVST Planner User’s Guide.

To delete the PVST reports using Delete Records option:

1. In the FDM Client, click Tools > Delete Records. The Delete Records Wizard appears.
2. Click PVST Reports in the list and then click Next. The Delete PVST Reports page appears.
3. The Query View enables you to filter the PVST reports that are associated to device tags based on the combination of Protocol, Manufacturer, and Device Types.
 - To filter the PVST reports based on the protocol type, select HART protocol from the Protocol list. The corresponding manufacturer list appears.
 - Select one or more Manufacturer(s) and Device Type(s).
 - To delete PVST reports associated to all device tags, select All from the Manufacturer and Device Type list and then click Next.

In the next page, you can select device tags for connected devices, disconnected devices, healthy devices, unhealthy devices or for all devices form the list. Corresponding device tags are populated in the Available Device Tags List box.

4. Select the device tag and click  to move it to the Selected Device Tag List box. Or Click  to move all the device tags to the Selected Device Tag List box.

TIP

The number of device tags selected is listed in the right pane under Selected Device Tag List.

5. Click Next.
6. In the next page, click the All reports or Select Time Duration (From and To) options and then click Next.
 - If you click All reports, all PVST reports associated to selected device tags are deleted.
 - If you click Select Time Duration (From and To), the generated PVST reports of that particular period are deleted.

In the next page, a message appears to confirm the deletion of the PVST reports.

7. Click Delete. After PVST reports are deleted successfully, a message appears in the next page.
8. Click Finish.

FDM STATION MAINTENANCE VIEW

FDM Device Configuration pages are integrated into Experion Flex Station. This enables the use of the Experion Flex Station for maintenance and Console Station.

NOTE

Console Station is supported for Experion R511.4 or higher.

The supported protocols include:

- HART
- FF
- ISA100 Wireless device
- PROFIBUS – DP &PA
- HoP

When Station Maintenance View is installed with FDM Client in an Experion Flex Station, the FDM window is embedded with the devices of supported protocols' detail display pages and can be used for viewing detailed information of the devices. This provides very convenient access to device diagnostic, troubleshooting and configuration information directly from the operator console. This view shows the DD/DTM based device window, which is similar to the device configuration window displayed in the FDM Client.

The FDM embedded detail display page, within the Experion Flex Station is to be used only for Flex Station maintenance. Do not use it on Experion Flex Station used for plant operations. These detailed displays are also supported on Experion Console Stations.

In the Maintenance View of Station, you can view the devices of supported protocols connected to one of the following interfaces.

- 1756 HART I/O
- PMIO
- Series C I/O
- Series 8 I/O
- Hardware Multiplexer (P+F, MTL, STAHL, ELCON)
- FIM2, FIM4 and FIM8
- Universal Safe Modules (RUSIO, PUIO)
- Series C UIO -16
- Series C UOC
- Series C UIO -2 (16 and 32)
- WDM
- PGM

Guidelines to view a device in the Station Maintenance View

To view a device in the Maintenance View of Station, perform the following tasks in the recommended order.

1. The network interface to which the device is connected is configured in the FDM Server using the FDM Server Management Tool.
2. Network is browsed and the devices are detected by FDM.
3. The FDM Client and the FDM specific display files are installed on the Flex Station system.
4. A relationship between the FDM Server and Experion server is established using the configuration file.

33.1 Configuring relationship between Experion Server and FDM Server

To enable Station Maintenance View to open a specified device, you must know the name of the FDM Server on which the Experion server is configured. To view a device connected to a particular Experion server, it must be configured in the Server management tool of an FDM Server.

FDM Server and Experion server relationship must be configured in a file so that Maintenance view can be automatically connected to the device when it is opened in Experion Station.

To configure the relationship perform the following steps.

1. On Experion Station node, click Start > Run.
2. In the Open box, type notepad and then click the OK button.
3. Browse to the location C:\ProgramData\Honeywell\FDM\MaintenanceView and open the file FdmExperionCache.xml.

The default file contents are as follows.

```
<fdmExperionServerCache>

<map>

<experionServer>DUMMYEPKSSERVER</experionServer>

<fdmServer>DUMMYFDMSERVER</fdmServer>

</map>

</fdmExperionServerCache>
```

4. To configure relationship between FDM Server fdmsvr1 to Experion server expsvrA, modify the contents in the default file as follows:

```
<fdmExperionServerCache>

<map>

<experionServer>EXPSVRA</experionServer>

<fdmServer>FDMSVR1</fdmServer>

</map>

</fdmExperionServerCache>
```

Replace DUMMYEPKSSERVER by the name of the actual Experion server, expsvrA and DUMMYFDMSERVER by the name of the FDM Server, fdmsvr1.

NOTE

- Ensure that you enter the names in capital letters. For example, expsvrA and fdmsvr1 have to be entered as EXPSVRA and FDMSVR1 respectively.
- The text between <map> and </map> constitutes one FDM Server – Experion server relationship.
- Redundant Experion servers should have two entries in the configuration file, one for the primary and one for the secondary. The fdmServer name remains the same for both entries though.

For example:

```
< fdmExperionServerCache >

<map>

<experionServer>EPKSSERVERA</experionServer>

<fdmServer>FDMSERVER</fdmServer>

</map>

<map>

<experionServer>EPKSSERVERB</experionServer>

<fdmServer>FDMSERVER</fdmServer>

</map>

</fdmExperionServerCache>
```

5. To configure another relationship, perform the following:
 - Copy the text starting from <map> till </map>, and paste it after </map>.
 - Type the Experion server name between <experionServer> and </experionServer>.
 - Type the FDM Server between <fdmServer> and </fdmServer>.
6. If you want to add another relationship for redundant server, for example, between FDM Server fdmsvr2 and Experion Server expsvrB, the contents must look similar to the following one, after performing the previous step.

```
<fdmExperionServerCache>

<map>

<experionServer>EXPSVRA</experionServer>

<fdmServer>FDMSVR1</fdmServer>

</map>
```

```
<map>

<experionServer>EXPSVRB</experionServer>

<fdmServer>FDMSVR2</fdmServer>

</map>

</fdmExperionServerCache>
```

7. To configure a relationship between two redundant Experion clusters (EXPServer01a/b and EXPServer02a/b) with their own FDM servers (FDMServer01 and FDMServer02).

```
<fdmExperionServerCache>

<map>

<experionServer>EXPServer01a</experionServer>

<fdmServer>FDMServer01</fdmServer>

</map>

<map>

<experionServer>EXPServer01b</experionServer>

<fdmServer>FDMServer01</fdmServer>

</map>

</fdmExperionServerCache>

<fdmExperionServerCache>

<map>

<experionServer>EXPServer02a</experionServer>

<fdmServer>FDMServer02</fdmServer>

</map>

<map>

<experionServer>EXPServer02b</experionServer>

<fdmServer>FDMServer02</fdmServer>

</map>

</fdmExperionServerCache>
```

8. Repeat step 4 to add as many relationships as required.

33.2 Access rights for Station Maintenance View

The Experion Station user who wants to perform actions on this view has the privilege of the same access level in FDM. For example if you log on with your access level of Supervisor in Experion, then you have the privilege of the FDM Supervisor.

NOTE

To view the Maintenance View on a detailed display page, the user authentication is done by Experion and the authorization is done by FDM. FDM assigns the privileges depending upon the authorization.

When you log on in Experion Station, you are mapped to the FDM access privileges as follows:

Experion User Level	FDM User Level	Privileges (when accessed from FDM Client)	Privileges (when accessed from Experion Station)
Manager	Administrator	“Administrator access privileges”	Execute Method Read and Write Parameters
Supervisor	Supervisor	“Supervisor access privileges”	Execute Method Read and Write Parameters
Engineer	Engineer	“Engineer access privileges”	Execute Method Read and Write Parameters
Operator	Operator	“Operator access privileges”	Read Only view of device configuration
Ack only	Operator	“Operator access privileges”	Read Only view of device configuration
View only	Operator	“Operator access privileges”	Read Only view of device configuration

33.3 Starting Maintenance View in Station

To start the Maintenance View of a HART/ISA100 Wireless/FF device, the detail display page for that device must be accessed. On the Experion Station, you can access the detail display of HART/ISA100 Wireless/FF devices from the following pages.

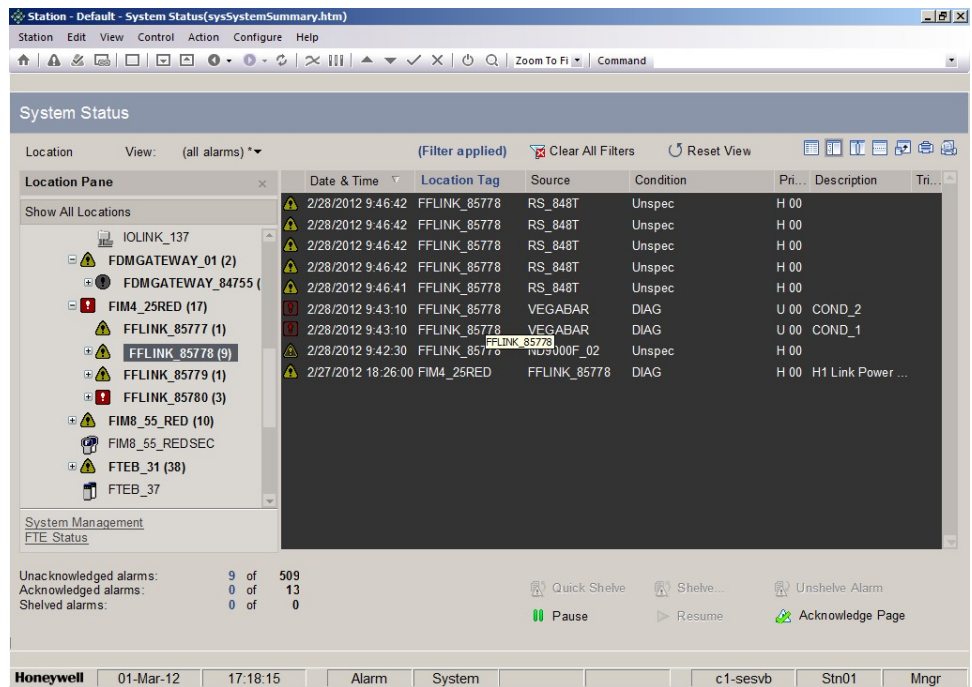
- Search Page
- System Status page
- Events page
- Alerts page

NOTE

Ensure that if you are opening DTMs in the Maintenance view the required executable is added to the DEP exception list. For more information about DEP exception list, refer to section Executables required in DEP Exception list in FDM Software Installation User's Guide.

For example, to get the FDM device detail display from the system status page, perform the following steps.

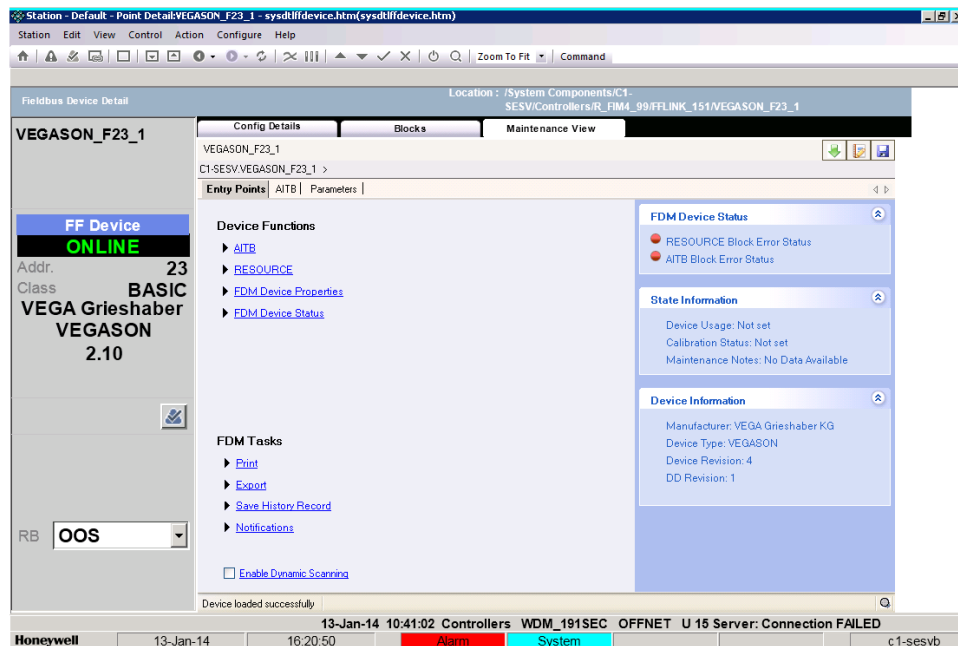
1. On the Experion Station computer, choose Start > All Programs > Honeywell Experion PKS > Client > Station and log on to the station.
2. Click  (System Menu) on the toolbar. The following page appears with the System tab.



Type the device name you want to search, in the command zone and press F12. If you type the name partially in the command zone, lists of matching device names appear.

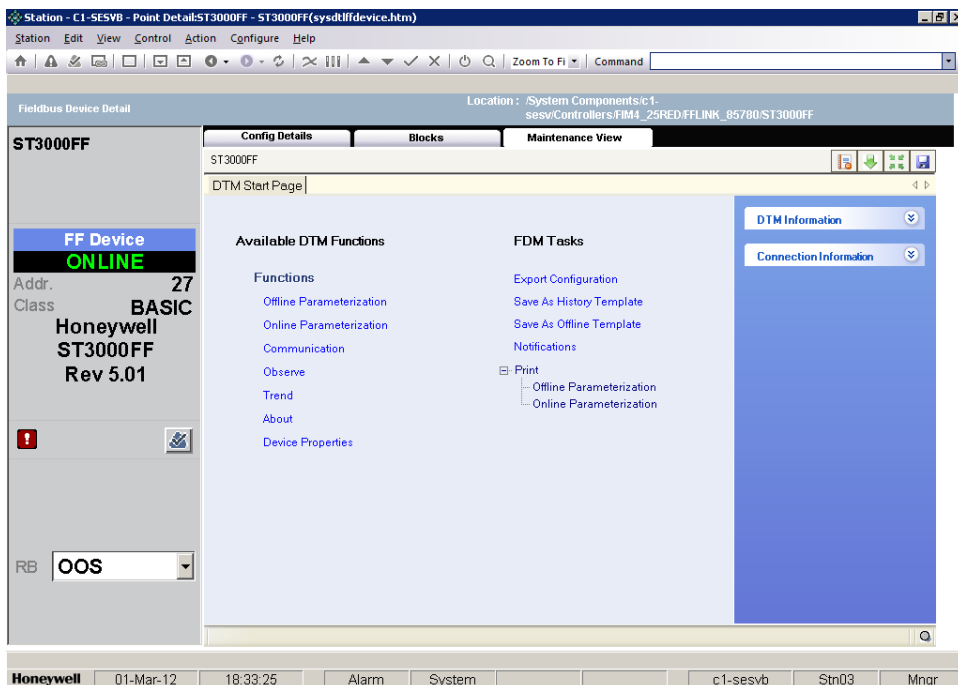
3. Select the component or node from the Location pane.

- Double-click or right-click the required device and click Detail Display. The Detail Display of the device appears, or If you type full name of the device in the command zone, the detail display of that device appears.

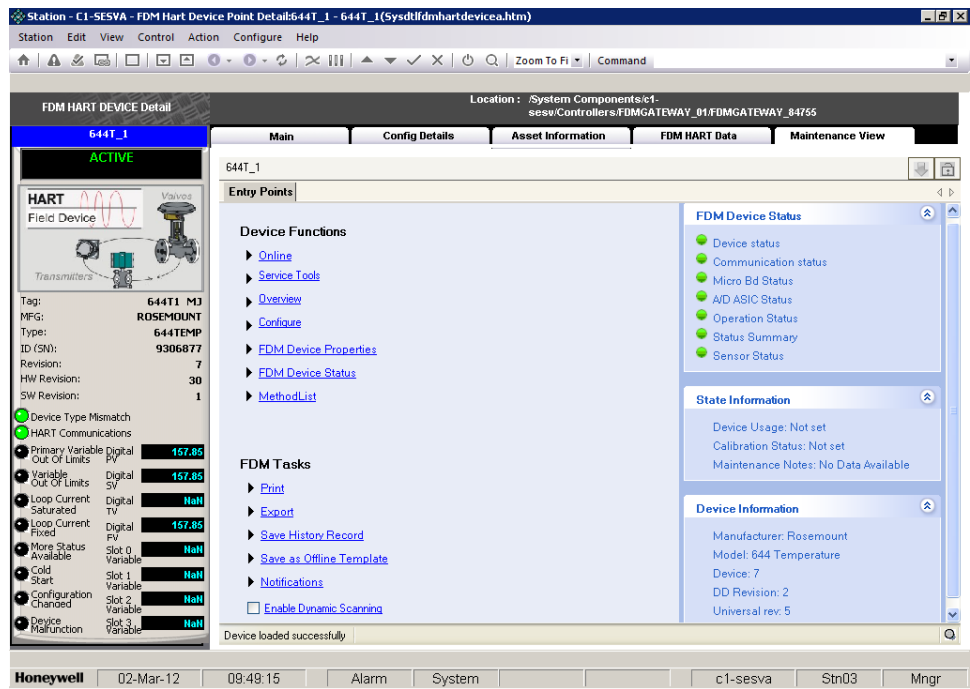


For more information about detail displays from other pages on the Experion Station, refer to the Experion Operator's Guide.

- To view the FDM device configuration details from Experion Station, click Maintenance View tab on the Device Configuration Detail Display. This page is identical to the Device Configuration page in FDM Client. In the following example, you can view DTM Start Page for FF devices.



In the following example, you can view entry points for HART devices.



You can read/write the device parameters, execute methods, and view the HART device status and properties.

UAS DEVICE VIEW

Honeywell's Uniformance Asset Sentinel solution continuously monitors equipment and process health, enabling industrial facilities to predict and prevent asset failures and poor operational performance.

A key feature of this solution is to fully realize the benefits of digital device diagnostic information. In conjunction with Field Device Manager (FDM), Asset Sentinel delivers an integrated instrument asset management solution to help achieve meaningful organization and prioritization for diagnostic device alerts. Automatic synchronization with Honeywell's Experion® Process Knowledge System (PKS) makes this task effortless. Asset Sentinel maintains fault history, bad actor and other records so reliability analytics can be employed over time to improve the overall reliability of instrumentation.

This feature is available to Sentinel users who have access to view FDM HART device configuration. See the Intuition Security Users Guide for information about how to provide this access. This user must also be an FDM user.

Asset Sentinel integration with FDM provides Sentinel users with the required privilege with the Device View to view parameters and diagnostic information for HART devices. This solution provides a read-only view of field instruments connected to the Experion network only.

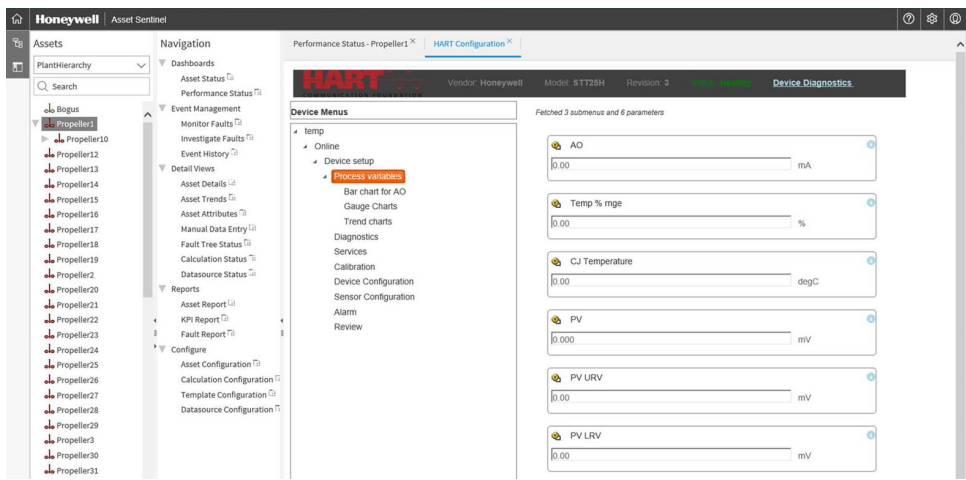
You can only view diagnostics and health data for HART devices. The data presented is dynamic and reflects current values in the devices. For configuration tasks, FDM Client is still required. The view provided by Asset Sentinel includes parameters and diagnostics data. It however, does not display images or EDD constructs as can be viewed via the FDM Client.

This feature is available only when FDM is configured to run in Windows Security Mode. It is not available in Classic Server Security mode.

NOTE

"FDM Web Service Provider" service must be started manually on the FDM Server machine for this feature to work. This is supported only for HTTP and not HTTPS.

Shown here is a screenshot of the parameters for a temperature transmitter device as seen on Asset Sentinel.



FDM DATA BACKUP-RESTORE UTILITY

The FDM database stores all information related to the network and device configurations. It also stores information related to the users and all actions performed by the users using FDM. The FDM Data Backup- Restore utility enables you to take a backup of the FDM database and use the backed up database at a later point in time for restoring FDM.

35.1 Taking a backup of the FDM database

To take a backup of the FDM database

1. Click Start > All Programs > Honeywell FDM > FDM Data Backup - Restore. The login screen appears for the FDM data backup-restore utility.
2. Type Login Name and Password.
3. Click Login. The FDM Data Backup/Restore dialog box appears.

NOTE

- Only a user with privileges assigned to an Administrator role can log on to this utility. Other users with Engineer, Supervisor, and Operator privileges cannot use this utility.
- Ensure that you stop the server before performing a backup operation. For more details, refer to section "Updating the FDM Server status".
- Ensure that the SQL Server management studio and FDM related applications are closed.

4. To take a backup of the FDM database, click Backup.
5. Click the  button to select the path where you want to store the backup files. The Browse for Folder dialog box appears.
6. Select the folder where you want to store the backup files. The selected folder's path appears in the dialog box.
7. Click Backup. A progress bar appears, which indicates the status of the backup operation. This operation stores the FDM database files in the selected folder. After the operation is complete, Backup operation completed message appears in the dialog box.

35.2 Restoring the database

To restore the FDM database

1. Log on to the FDM Data Backup-Restore utility. The FDM Data Backup/Restore dialog box appears.

NOTE

- Only a user with privileges assigned to an administrator role can log on to this utility. Other users with Engineer, Supervisor, and Operator privileges cannot use this utility.
- Ensure that you stop the server before performing a restore operation. For more details, refer to section “Updating the FDM Server status”.
- Ensure that the SQL Server management studio and FDM related applications are closed.

2. To restore the FDM database from a backup, click Restore.
3. Click the  button to select the folder where the backed up database is stored. The Browse for Folder dialog box appears.
4. Select the folder where you have saved the FDM database backup files.
5. Click OK. The selected folder's path

NOTE

It is recommended to take a backup of your current database before performing a restore operation from a previous backup, as restoring from a previous backup overwrites the current database information.

6. Click Restore. A progress bar appears which indicates the status of the restore operation. After the operation is complete, Restore operation completed appears in the dialog box.
7. Click Close.

FDM DIAGNOSIS USING DR. FDM

Dr. FDM is a diagnosis tool used for collecting diagnostic information related to the FDM system. In the event of issues faced with the usage of FDM software, this diagnostic tool can be run on the systems where FDM components are installed. The tool collects diagnostic information in the form of various log files. These files can be sent to Honeywell TAC for further analysis.

36.1 Capturing diagnostics

To capture the FDM diagnostic information

1. Click Start > All Programs > Honeywell FDM > Dr. FDM. The Dr. FDM dialog box appears.
2. Click Start Diagnostics to proceed.

NOTE

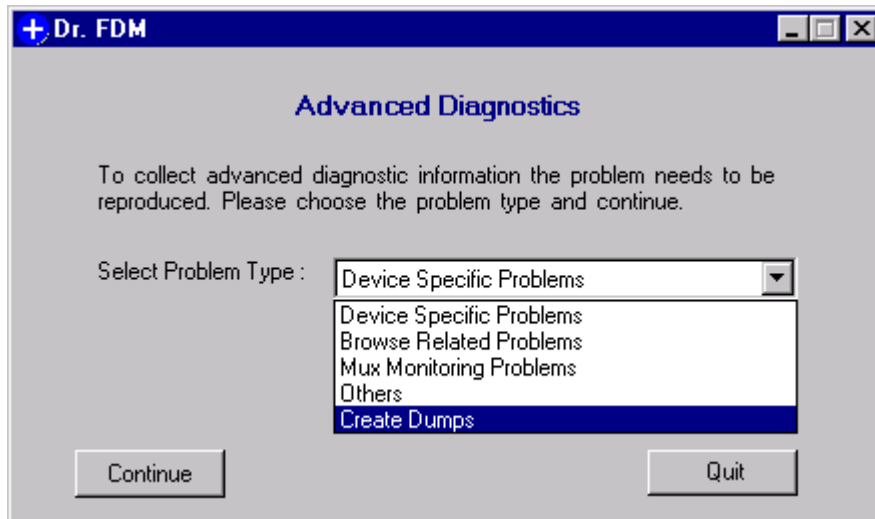
Click Quit, if you want to stop Dr. FDM during the diagnosis. A confirmation message appears. Click Yes to close Dr. FDM. The Choose Diagnostics page appears. By default, the Get Advanced Diagnostics option is selected.

3. Click Continue to proceed with collecting diagnostic information by reproducing the problem.

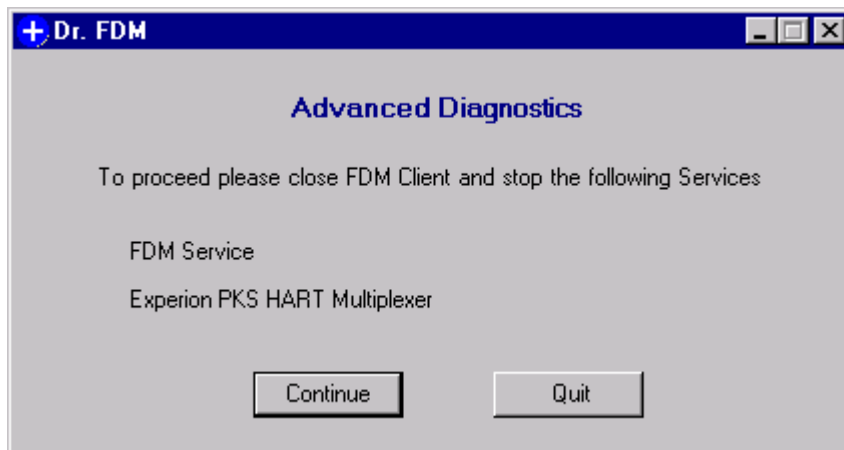
NOTE

- Honeywell recommends choosing the Get Advanced Diagnostics option always.
- To quit Dr. FDM after collecting the initial diagnostic information, select the Quit with Current Diagnostics option and then click Continue.

4. If you click Get Advanced Diagnostics, the following dialog box appears.



5. Choose the relevant option depending on the type of problem from Select Problem Type list.
- Click Device Specific Problems, if there is a problem related to device loading.
 - Click Browse Related Problems, if the problem is related to the number of nodes or hierarchy of nodes.
 - Click MUX Monitoring Related Problem, if the problem is related to the MUX Monitoring solution.
 - Click Others for any other scenario.
 - Click Create Dumps, to take dumps any time specifically during the time if you encounter any problem.
6. Click Continue. The following message appears.



7. All the services listed in the dialog box have to be stopped in order to proceed further.

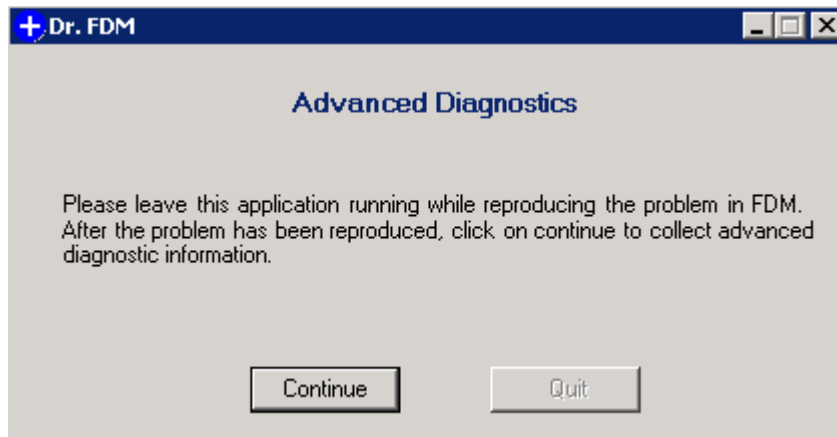
NOTE

- The Experion HART Multiplexer service is present only on the Experion system.
- Ensure that the services listed in the message are stopped. If any of the services is not stopped, the message appears until the service is stopped. For example, if the FDM Server service is not stopped, a message appears

informing you to stop the FDM Server.

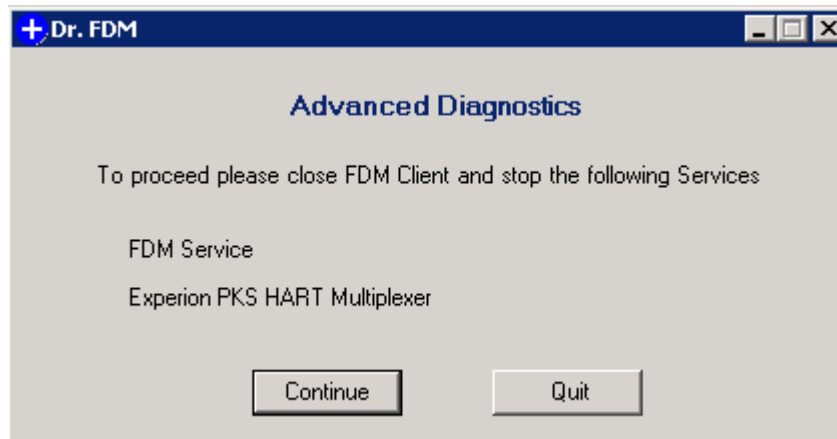
- Stop the service and click OK.
- Ensure that the FDM Remote Communication Interface service is stopped. If the FDM RCI service is not stopped, a message appears informing you to stop the FDM RCI.
- Stop the service and click OK.

8. Click Continue. The following message appears.



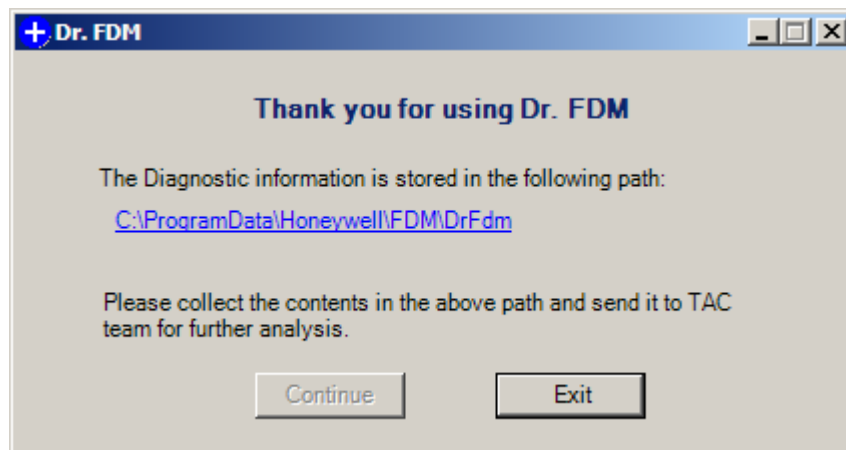
This screen remains in the background while you reproduce the problem.

9. Reproduce the problem scenario and then click Continue to proceed to the next step. A confirmation message appears.
10. Click Yes, if you have finished reproducing the problem and the following dialog box appears.



This step ensures that all changed values during the usage of Dr. FDM are reset to default values. For more details, refer instructions as in step 5.

11. Stop the services listed in the message dialog box and click Continue. The following message appears.



All the required diagnostic information is stored under the path depends on where the FDM is installed. In this example, it is in C:\ProgramData\Honeywell\FDM\DrFDM.

NOTE

For further analysis of the problem, move all the files from the path C:\ProgramData\Honeywell\FDM\DrFDM to Honeywell TAC.

36.2 Stopping/refreshing the device related services

Service control tool helps in stopping the device related services.

To stop or refresh the device related services

1. Click Start > All Programs > Honeywell FDM > Dr. FDM. The Dr. FDM dialog box appears.
2. Click Service Control to proceed. The Service Control Panel appears.

NOTE

When the Dr FDM is launched without clicking Run as administrator, then Service Control does not work.

3. Click Refresh to view the current status of the Device Related Services. If you click Refresh when the Device Related Services is running, then the following dialog box appears.



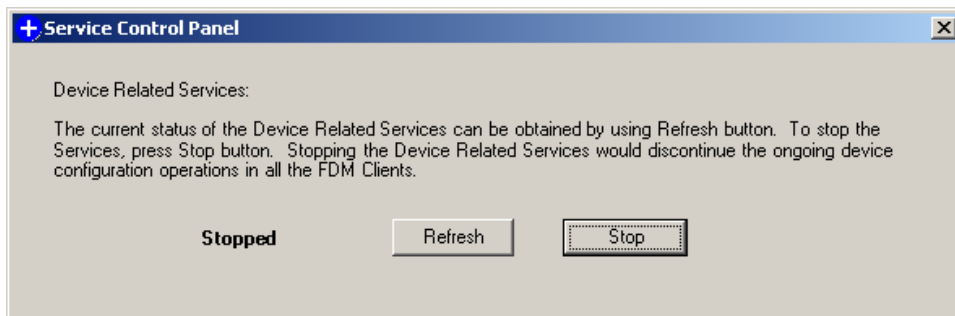
The status appears as Running.

If you click Refresh when the Device Related Service is not running, then the following dialog box appears.



The status appears as Not Running.

4. Click Stop to stop the Device Related Services. The following dialog box appears.



The status appears as Stopped.

NOTE

Ensure to save running device configuration operations in all the FDM clients before you stop the Device Related Services.

Notices

Trademarks

Experion®, PlantScape®, SafeBrowse®, TotalPlant®, ControlEdge™, and TDC 3000® are registered trademarks of Honeywell International, Inc.

OneWireless™ is a trademark of Honeywell International Sàrl

Other trademarks

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

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

Third-party licenses

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

Documentation feedback

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

- <http://www.honeywellprocess.com/support>

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

- hpsdocs@honeywell.com

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

Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, <https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx>.

Training classes

Honeywell holds technical training classes about Experion PKS. These classes are taught by experts in the field of process control systems. For more information about these classes, contact your Honeywell representative, or see <http://www.automationcollege.com>.