



ONYXWorks[®] Lite

Installation and Operation Manual

Document LS10050-003NF-E
6/5/2015 Rev: **B**

P/N LS10050-003NF-E:B

ECN 15-0292

Fire Alarm & Emergency Communication System Limitations

While a life safety system may lower insurance rates, it is not a substitute for life and property insurance!

An automatic fire alarm system—typically made up of smoke detectors, heat detectors, manual pull stations, audible warning devices, and a fire alarm control panel (FACP) with remote notification capability—can provide early warning of a developing fire. Such a system, however, does not assure protection against property damage or loss of life resulting from a fire.

An emergency communication system—typically made up of an automatic fire alarm system (as described above) and a life safety communication system that may include an autonomous control unit (ACU), local operating console (LOC), voice communication, and other various interoperable communication methods—can broadcast a mass notification message. Such a system, however, does not assure protection against property damage or loss of life resulting from a fire or life safety event.

The Manufacturer recommends that smoke and/or heat detectors be located throughout a protected premises following the recommendations of the National Fire Protection Association Standard 72 (NFPA 72), manufacturer's recommendations, State and local codes, and the recommendations contained in the Guide for Proper Use of System Smoke Detectors, which is made available at no charge to all installing dealers. This document can be found at <http://www.systemsensor.com/appguides/>. A study by the Federal Emergency Management Agency (an agency of the United States government) indicated that smoke detectors may not go off in as many as 35% of all fires. While fire alarm systems are designed to provide early warning against fire, they do not guarantee warning or protection against fire. A fire alarm system may not provide timely or adequate warning, or simply may not function, for a variety of reasons:

Smoke detectors may not sense fire where smoke cannot reach the detectors such as in chimneys, in or behind walls, on roofs, or on the other side of closed doors. Smoke detectors also may not sense a fire on another level or floor of a building. A second-floor detector, for example, may not sense a first-floor or basement fire.

Particles of combustion or "smoke" from a developing fire may not reach the sensing chambers of smoke detectors because:

- Barriers such as closed or partially closed doors, walls, chimneys, even wet or humid areas may inhibit particle or smoke flow.
- Smoke particles may become "cold," stratify, and not reach the ceiling or upper walls where detectors are located.
- Smoke particles may be blown away from detectors by air outlets, such as air conditioning vents.
- Smoke particles may be drawn into air returns before reaching the detector.

The amount of "smoke" present may be insufficient to alarm smoke detectors. Smoke detectors are designed to alarm at various levels of smoke density. If such density levels are not created by a developing fire at the location of detectors, the detectors will not go into alarm.

Smoke detectors, even when working properly, have sensing limitations. Detectors that have photoelectronic sensing chambers tend to detect smoldering fires better than flaming fires, which have little visible smoke. Detectors that have ionizing-type sensing chambers tend to detect fast-flaming fires better than smoldering fires. Because fires develop in different ways and are often unpredictable in their growth, neither type of detector is necessarily best and a given type of detector may not provide adequate warning of a fire.

Smoke detectors cannot be expected to provide adequate warning of fires caused by arson, children playing with matches (especially in bedrooms), smoking in bed, and violent explosions

(caused by escaping gas, improper storage of flammable materials, etc.).

Heat detectors do not sense particles of combustion and alarm only when heat on their sensors increases at a predetermined rate or reaches a predetermined level. Rate-of-rise heat detectors may be subject to reduced sensitivity over time. For this reason, the rate-of-rise feature of each detector should be tested at least once per year by a qualified fire protection specialist. Heat detectors are designed to protect property, not life.

IMPORTANT! Smoke detectors must be installed in the same room as the control panel and in rooms used by the system for the connection of alarm transmission wiring, communications, signaling, and/or power. If detectors are not so located, a developing fire may damage the alarm system, compromising its ability to report a fire.

Audible warning devices such as bells, horns, strobes, speakers and displays may not alert people if these devices are located on the other side of closed or partly open doors or are located on another floor of a building. Any warning device may fail to alert people with a disability or those who have recently consumed drugs, alcohol, or medication. Please note that:

- An emergency communication system may take priority over a fire alarm system in the event of a life safety emergency.
- Voice messaging systems must be designed to meet intelligibility requirements as defined by NFPA, local codes, and Authorities Having Jurisdiction (AHJ).
- Language and instructional requirements must be clearly disseminated on any local displays.
- Strobes can, under certain circumstances, cause seizures in people with conditions such as epilepsy.
- Studies have shown that certain people, even when they hear a fire alarm signal, do not respond to or comprehend the meaning of the signal. Audible devices, such as horns and bells, can have different tonal patterns and frequencies. It is the property owner's responsibility to conduct fire drills and other training exercises to make people aware of fire alarm signals and instruct them on the proper reaction to alarm signals.
- In rare instances, the sounding of a warning device can cause temporary or permanent hearing loss.

A life safety system will not operate without any electrical power. If AC power fails, the system will operate from standby batteries only for a specified time and only if the batteries have been properly maintained and replaced regularly.

Equipment used in the system may not be technically compatible with the control panel. It is essential to use only equipment listed for service with your control panel.

Telephone lines needed to transmit alarm signals from a premises to a central monitoring station may be out of service or temporarily disabled. For added protection against telephone line failure, backup radio transmission systems are recommended.

The most common cause of life safety system malfunction is inadequate maintenance. To keep the entire life safety system in excellent working order, ongoing maintenance is required per the manufacturer's recommendations, and UL and NFPA standards. At a minimum, the requirements of NFPA 72 shall be followed. Environments with large amounts of dust, dirt, or high air velocity require more frequent maintenance. A maintenance agreement should be arranged through the local manufacturer's representative. Maintenance should be scheduled monthly or as required by National and/or local fire codes and should be performed by authorized professional life safety system installers only. Adequate written records of all inspections should be kept.

Limit-D-1-2013

Installation Precautions

Adherence to the following will aid in problem-free installation with long-term reliability:

WARNING - Several different sources of power can be connected to the fire alarm control panel. Disconnect all sources of power before servicing. The control unit and associated equipment may be damaged by removing and/or inserting cards, modules, or interconnecting cables while the unit is energized. Do not attempt to install, service, or operate this unit until this manual is read and understood.

CAUTION - System Reacceptance Test after Software Changes. To ensure proper system operation, this product must be tested in accordance with NFPA 72 after any programming operation or change in site-specific software. Reacceptance testing is required after any change, addition or deletion of system components, or after any modification, repair or adjustment to system hardware or wiring.

All components, circuits, system operations, or software functions known to be affected by a change must be 100% tested. In addition, to ensure that other operations are not inadvertently affected, at least 10% of initiating devices that are not directly affected by the change, up to a maximum of 50 devices, must also be tested and proper system operation verified.

This system meets NFPA requirements for operation at 0°C to 49°C (32°F to 120°F) and at a relative humidity 93% ± 2% RH (non-condensing) at 32°C ± 2°C (90°F ± 3°F). However, the useful life of the system's standby batteries and the electronic components may be adversely affected by extreme temperature ranges and humidity. Therefore, it is recommended that this system and all peripherals be installed in an environment with a nominal room temperature of 15-27° C/60-80° F.

Verify that wire sizes are adequate for all initiating and indicating device loops. Most devices cannot tolerate more than a 10% I.R. drop from the specified device voltage.

Like all solid state electronic devices, this system may operate erratically or can be damaged when subjected to lightning-induced transients. Although no system is completely immune from lightning transients and interferences, proper grounding will reduce susceptibility. Overhead or outside aerial wiring is not recommended, due to an increased susceptibility to nearby lightning strikes. Consult with the Technical Services if any problems are anticipated or encountered.

Disconnect AC power and batteries prior to removing or inserting circuit boards. Failure to do so can damage circuits.

Remove all electronic assemblies prior to any drilling, filing, reaming, or punching of the enclosure. When possible, make all cable entries from the sides or rear. Before making modifications, verify that they will not interfere with battery, transformer, and printed circuit board location.

Do not tighten screw terminals more than 9 in-lbs. Over-tightening may damage threads, resulting in reduced terminal contact pressure and difficulty with screw terminal removal.

Though designed to last many years, system components can fail at any time. This system contains static-sensitive components. Always ground yourself with a proper wrist strap before handling any circuits so that static charges are removed from the body. Use static-suppressive packaging to protect electronic assemblies removed from the unit.

Follow the instructions in the installation, operating, and programming manuals. These instructions must be followed to avoid damage to the control panel and associated equipment. FACP operation and reliability depend upon proper installation by authorized personnel.

FCC Warning

WARNING: This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause interference to radio communications. It has been tested and found to comply with the limits for class A computing devices pursuant to Subpart B of Part 15 of FCC Rules, which is designed to provide reasonable protection against such interference when devices are operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his or her own expense.

Canadian Requirements

This digital apparatus does not exceed the Class A limits for radiation noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radio-electriques depassant les limites applicables aux appareils numeriques de la classe A prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

HARSH™, NIS™, NOTI•FIRE•NET™, eVance™, and SWIFT™ are all trademarks; and Acclimate® Plus, FlashScan®, FAAST Fire Alarm Aspiration Sensing Technology®, Intelligent FAAST®, NOTIFIER®, ONYX®, ONYXWorks®, VeriFire®, and VIEW® are all registered trademarks of Honeywell International Inc.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation.

The Chrome™ and Google™ are trademarks of Google Inc.

© 2015 by Honeywell International Inc. All rights reserved. Unauthorized use of this document is strictly prohibited.

Software Downloads

In order to supply the latest features and functionality in fire alarm and life safety technology to our customers, we make frequent upgrades to the embedded software in our products. To ensure that you are installing and programming the latest features, we strongly recommend that you download the most current version of software for each product prior to commissioning any system. Contact Technical Support with any questions about software and the appropriate version for a specific application.

Documentation Feedback

Your feedback helps us keep our documentation up-to-date and accurate. If you have any comments or suggestions about our on-line help or manuals, please e-mail us at FireSystems.TechPubs@honeywell.com.

On-Line Help – Please include the following information:

- Product name and version number (if applicable)
- Topic title
- The content you think should be corrected/improved
- Detailed suggestions for correction/improvement

Documents – Please include the following information:

- Document part number and title
- Page number and paragraph
- The content you think should be corrected/improved
- Detailed suggestions for correction/improvement

Please Note: If you have any technical issues, please contact Technical Services.

Manual Usage

This manual is written with the understanding that the user has been trained in the proper operations and services for this product. The information provided in this manual is intended to assist the user by describing the configurations and how they affect operations.

Table of Contents

Section 1 Product Overview	9
1.1: Operation	9
1.2: Functionality	9
1.2.1: System Functions.....	9
1.2.2: System Limits.....	10
Table 1.1 System Limits.....	10
1.3: Additional Software.....	10
1.3.1: Anti-virus Software	10
1.3.2: Windows Automatic Updates.....	10
1.4: Printer Overview.....	10
1.5: IP Requirements.....	10
1.5.1: IP Port Settings	10
Table 1.2 IP Port Settings.....	10
1.5.2: IP Restrictions	11
1.6: System Security	11
1.6.1: Software Security	11
1.7: ONYXWorks Lite Product Components	11
1.8: Network Topology	11
1.9: Network Technology.....	11
Section 2 Hardware Configuration	13
2.1: Installation Overview.....	13
2.2: Workstation Computer Requirements.....	13
2.2.1: Windows Operating System	13
2.2.2: Browser.....	13
2.2.3: Other Specifications	13
2.3: Software Installation Procedure.....	13
2.4: Starting Lite for the First Time	14
2.5: UPS Installation	14
2.6: Testing and Maintenance	14
Section 3 PC NFN Gateway Board Installation	15
3.1: Installing the PC NFN Gateway Board	15
Figure 3.1 Installing the PC NFN Gateway Board.....	15
3.2: Connections	16
3.2.1: Connecting to the PC COMM Port	16
Figure 3.2 PC NFN Gateway-to-PC Connections.....	16
3.2.2: Connecting to the NFN Network.....	17
Figure 3.3 OW-LITE-NW Network Connections.....	17
Figure 3.4 OW-LITE-NF Network Connections.....	17
3.2.3: Connecting to UPS Supervision	18
Figure 3.5 UPS Supervision Connections	18
3.2.4: Connection Specifications	18
Table 3.1 Connection Specifications.....	18
3.3: Setting the Network Control Switches	19
3.3.1: Setting OW-LITE-NW Switches.....	19
Figure 3.6 OW-LITE-NW Switch Settings.....	19
3.3.2: Setting OW-LITE-NF Switches	20
Figure 3.7 OW-LITE-NF Switch Settings.....	20
3.4: System Power	20
3.5: Testing/Maintenance.....	20
Section 4 PC NFN Gateway Configuration	21
4.1: Configuration Application Activation and Login.....	21
4.2: Basic Configuration Tool Layout	21

Figure 4.1 Basic Configuration Tool Layout	21
4.3: Main Menus	22
Table 4.1 Main Menus.....	22
4.4: Product Information.....	22
Table 4.2 Product Information	22
4.5: Additional Properties	23
Table 4.3 Additional Properties.....	23
4.6: Node List	24
4.7: Web Portal Setup	24
Section 5 Configuration Tool Settings.....	25
5.1: Administrator Login	25
5.1.1: New Workstation.....	25
5.1.2: Software Upgrade on Existing Workstation.....	25
5.2: Factory Defined User Profiles and their Passwords	25
5.3: Configuration Tool.....	25
5.3.1: Overview	25
5.3.2: Starting and Exiting the Configuration Tool	25
5.3.3: Configuration Tool Layout.....	26
Figure 5.1 Configuration Tool Layout	26
5.3.4: Monitoring Profiles	27
5.3.5: Color and Sound Configuration.....	27
5.3.6: Event Color Coding	28
Table 5.1 Event Icon Color Coding.....	28
5.3.7: System Options	29
Table 5.2 System Options Configuration	29
5.4: Network Right Click Commands.....	29
5.5: Auto-Creation of Screens, Nodes, and Points	30
Figure 5.2 Example of Navigation Tree with Auto-Creation Process.....	30
5.5.1: Managing the Auto-creation Process.....	31
Table 5.3 Managing Auto-created Screens	31
5.6: Autocreating Gateway Point IDs	31
5.7: Workstation Database Backup and Restore	32
5.7.1: Backing Up the Database	32
5.7.2: Restoring a Backed-Up Database	32
5.8: Macro Commands.....	32
5.9: Custom Icon Recommendations	33
Table 5.4 Effect on Non-PNG Icon File on Background	33
Table 5.5 Effects of Icon Color on Alarm Reporting	33
Section 6 Workstation Settings	35
6.1: Windows Settings	35
Table 6.1 Windows Settings.....	35
6.2: Workstation Settings.....	35
6.2.1: Options Window Command Buttons.....	35
Table 6.2 Options Window Command Buttons	35
6.2.2: General Tab	36
Table 6.3 General Tab Settings	36
6.2.3: User Features Tab.....	38
Table 6.4 User Features Settings.....	38
6.2.4: Event Printer Tab.....	38
Table 6.5 Event Printer Tab Settings.....	38
6.2.5: Output Tab.....	39
Table 6.6 Output Tab Settings	39
Section 7 Operation	41
7.1: Login and Log Out.....	41
7.1.1: Login.....	41

7.1.2: Log Out.....	41
7.2: Display Modes	42
7.2.1: Graphics Mode	42
Figure 7.1 Example Graphics Mode Screen	42
7.2.2: Text Mode.....	43
Figure 7.2 Example Text Mode Screen	43
7.3: Graphics Display Screen.....	44
Figure 7.3 Graphics Display Screen Features	44
Table 7.1 Graphics Display Screen Descriptions	45
7.3.1: Graphic Elements	47
7.3.1.1 Point Icons	47
7.3.1.2 Navicons	47
7.3.1.3 Linked Media.....	47
7.3.1.4 Control Commands.....	47
7.3.1.5 Point Right-Click Choices to Respond to Events.....	47
Table 7.2 Default Node/Point Control Commands	48
7.3.2: Navigation Tree	49
Figure 7.4 Navigation Tree Overview.....	49
7.3.3: New Events Pane	50
7.3.3.1 New Events Buttons	50
Figure 7.5 Normal Acknowledge, Silence, and Reset.....	50
7.3.4: Event Summary Icons.....	51
7.4: Auto-creation of Screens, Nodes, and Points	52
7.4.1: Overview	52
Figure 7.6 Example of Autogenerated Navigation Tree	52
7.5: Interpreting Events on the Workstation's User Interface	53
7.5.1: When a New Event Occurs.....	53
Figure 7.7 Example - New Event in Progress	53
Section 8 Data Management	55
8.1: Database Management.....	55
Table 8.1 Database Management Options.....	55
8.2: History Manager	56
Figure 8.1 History Manager Screen.....	56
8.2.1: Menu Bar	57
Table 8.2 History Manager Menus.....	57
8.2.2: Header and Row Display Options	58
8.2.2.1 Header Options.....	58
Table 8.3 History Manager Header Options.....	58
8.2.2.2 Row Filter Options	58
Table 8.4 History Manager Row Options.....	58
8.3: System Explorer Searches	58
8.4: Key Upgrade Utility	59
8.4.1: Overview	59
8.4.2: Upgrade Procedure	59
8.4.3: Key Upgrade Utility Field Descriptions.....	59
Table 8.5 Upgrade Utility Fields	59
Section 9 System Architecture	61
9.1: Overview.....	61
Figure 9.1 ONYXWorks Lite Network.....	61

Section 1 Product Overview

1.1 Operation

ONYXWorks Lite monitors building and life-safety systems and annunciates events (status change signals) that are received from the attached network(s). It functions as a Protected Premises Control Unit. Multiple user accounts are supported with monitoring and control permissions configured individually for each of the user accounts.

ONYXWorks Lite supports one gateway with up to four nodes.

ONYXWorks Lite is hereinafter referred to as “the workstation”.

1.2 Functionality

1.2.1 System Functions

The workstation provides the following major functions:

- Displays events by priority. New events are displayed in the list based upon their event type priority.
- Displays acknowledged and new events in separate lists.
- Visual and audible annunciation of events.
- Maintains a history of life safety events.
- Monitors the communications path between workstation and gateway.
- Annunciates a trouble event when communications with gateway is lost.
- Displays device location information.
- Acts as a time server for gateways on the life safety network.

1.2.2 System Limits

The workstation is designed to operate within the limits listed below:

Table 1.1 System Limits

Limit	Feature	Maximum Allowed
Logical Network & Screen	Screens	1000
	Devices	100,000
	Macros	100
	Macro Button	100
	NavIcons	1000
	Monitoring Profiles	100
	Node Control Profiles	100
Workstation	Output Formats	25 per Workstation
	Max Number of Monitored Panels	4 (not user-selectable)
User Manager	Users	500

1.3 Additional Software

1.3.1 Anti-virus Software

Recommended and tested against McAfee VirusScan[®] Enterprise.

1.3.2 Windows Automatic Updates

Must be set to “Check for updates but let me choose whether to download and install them”.

1.4 Printer Overview

The workstation software application supports graphics printing. Windows-compatible printers are required in order to print screens, floor plans, history reports, etc. and annunciated workstation events.

A graphics printer is a Windows-compatible printer that prints what is currently displayed on the workstation’s monitor.

1.5 IP Requirements

1.5.1 IP Port Settings

The following IP ports must be available to the workstation:

Table 1.2 IP Port Settings

Port	Type	Direction	Purpose
123	UDP	Both	SNTP
2004	TCP	N/A	(Internal) Workstation Plug-in Access

1.5.2 IP Restrictions

The following restrictions apply:

- Must have a static IP address. DHCP is not supported.
- Multiple IP Addresses are not supported, either due to multiple enabled network adapters or due to a multi-homed adapter.

1.6 System Security

1.6.1 Software Security

Workstation software security is as follows:

- **Secure Windows (Control/Command Key Lockouts)** - This type of lockout disables the workstation's keyboard keys that are used to access Windows programs that are not part of the workstation software applications. For example, keyboard key combinations can be used to shut-down or restart the workstation and for switching between software applications. The PC Monitor's Secure Windows selection disables those types of operations.
- **User Security Options** - User accounts can be created with differing levels of access to the NFN system. The user's security option choice determines which functions are visible or selectable. For example, some user accounts may not have permission to exit the workstation software application. Refer to the *ONYXWorks Lite Configuration Tool Installation & Operation Manual* (P/N 53508) for additional information.

1.7 ONYXWorks Lite Product Components

The following components are included with the ONYXWorks Lite product:

- ONYXWorks Lite Software CD ROM
- NFN Gateway PC Network Connection Card
- Configured USB Software Key
- User Manuals (On CD ROM)

1.8 Network Topology

ONYXWorks Lite communicates with attached node strictly over the NFN network. While the computer running the workstation may be attached to your IP network, ONYXWorks Lite does not communicate over IP.

1.9 Network Technology

ONYXWorks Lite supports one NFN network only. Other technologies which are supported by the full ONYXWorks suite, such as BACnet, and DACR, are not supported by ONYXWorks Lite.

Section 2 Hardware Configuration

2.1 Installation Overview

The workstation computer must be installed in accordance with local fire protection codes. Installation should be performed by a factory-trained fire alarm technician. The ONYXWorks Lite software application is shipped on a CD-ROM. Included in the shipment is a USB key that allows features of the network monitoring system to function on the workstation.

2.2 Workstation Computer Requirements



CAUTION: Possible Loss of Network Communication

Power management options must be disabled in the CPU BIOS and on the monitor, or loss of network communication or alarm reporting may result.

2.2.1 Windows Operating System

The workstation computer operating system must be Windows 7, 64-bit Professional.

2.2.2 Browser

Google[®] Chrome[™] must be installed and set as default browser.

2.2.3 Other Specifications

The workstation computer must meet the following minimum specifications:

- Intel i5 Processor or better
- 16 GB RAM
- 240 GB Hard Drive
- Monitor, Minimum resolution of 1280x1024 Landscape Mode
- Microsoft[®] compatible mouse
- 104-key keyboard
- USB Connector
- TCP/IP Ethernet Network Adapter Card
- Speakers

2.3 Software Installation Procedure

Install workstation software as follows:

1. Load the software CD-ROM into the computer drive.
2. Using Windows Explorer, browse to, and double-click **Setup.exe**. An allow changes to computer message displays.
3. Click **Yes**.
4. Follow the on-screen prompts to allow the software installation to proceed. Accept all software licensing agreements.

There are three installation wizards that appear during the installation:

- HASP Run-time Installation Wizard - Click **Finish** to proceed.
- Microsoft Access Database Engine Installation Wizard - Click **OK** to proceed.

- Facilities Monitoring - InstallShield Wizard - Click **Finish** to proceed. A computer restart message displays.
5. Click **Yes**. The computer restarts.
 6. Connect the ONYXWorks Lite USB key to the computer.

To start the workstation application, go **Start>All Programs>Facilities Monitoring>Workstation**.

2.4 Starting Lite for the First Time

The first time ONYXWorks Lite is started, you will be required to create an Administrator password. Enter a password at least 8 characters in length. Enter the password again to confirm. A randomly-generated system name displays next which can be changed, if desired. Both the password and system name are case-sensitive.

2.5 UPS Installation

Install the uninterruptible power supply (UPS) and connect the power cord and monitor module in accordance with manufacturer's instructions.

For UPS supervision, connect a monitor module from an FACP to the low current connectors of the UPS battery charger. The monitor module must be rated for 2A @ +30 VDC.

Relay output is used to enable annunciation by any external device:

- That uses power limited dry contacts.
- The common relay output is a contact that is not supervised and is rated for 2A @ +30VDC.

2.6 Testing and Maintenance

Remove all power sources to equipment before connecting electrical components. The ONYXWorks Lite computer's main power switch must be in the OFF position until installation of the entire ONYXWorks Lite system is complete and ready for testing.

Before performing any work on a fire alarm system:

1. Notify the fire department and the central alarm receiving station if transmitting alarm conditions.
2. Notify the people occupying the facility about the impending test, the expected time period of the test, and to disregard any alarm during the test period.
3. When appropriate, disable activation of alarm notification appliances and speakers to prevent their sounding.
4. Always physically disable releasing devices before system tests to prevent accidental discharge.

Improper installation, maintenance, and lack of routine testing could result in system malfunction.

Testing and maintenance shall be performed in accordance with the *Testing and Maintenance* section of NFPA-72.

Section 3 PC NFN Gateway Board Installation

3.1 Installing the PC NFN Gateway Board

If installation of the PC NFN Gateway board is required, perform the following steps:

1. Remove insulation strip from between the battery and the terminal as shown in [Figure 3.1](#).
2. Exit all applications and shut down the computer.
3. Remove the power cord.
4. Open the computer's cover and locate a vacant PCI slot.
5. Remove the PCI slot cover and save the screw from the vacant slot.
6. Insert the board's edge connector into the vacant PCI slot and then secure it with the screw.
7. Set NCM switches in accordance with [3.3, "Setting the Network Control Switches"](#).
8. Reinstall the computer cover and power cord, and then start the computer.

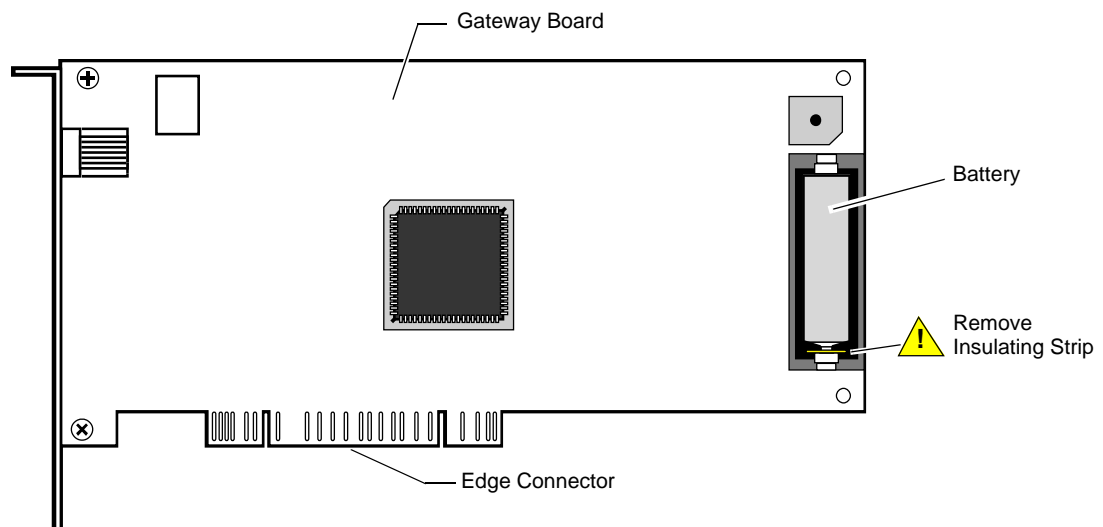


Figure 3.1 Installing the PC NFN Gateway Board

3.2 Connections

3.2.1 Connecting to the PC COMM Port

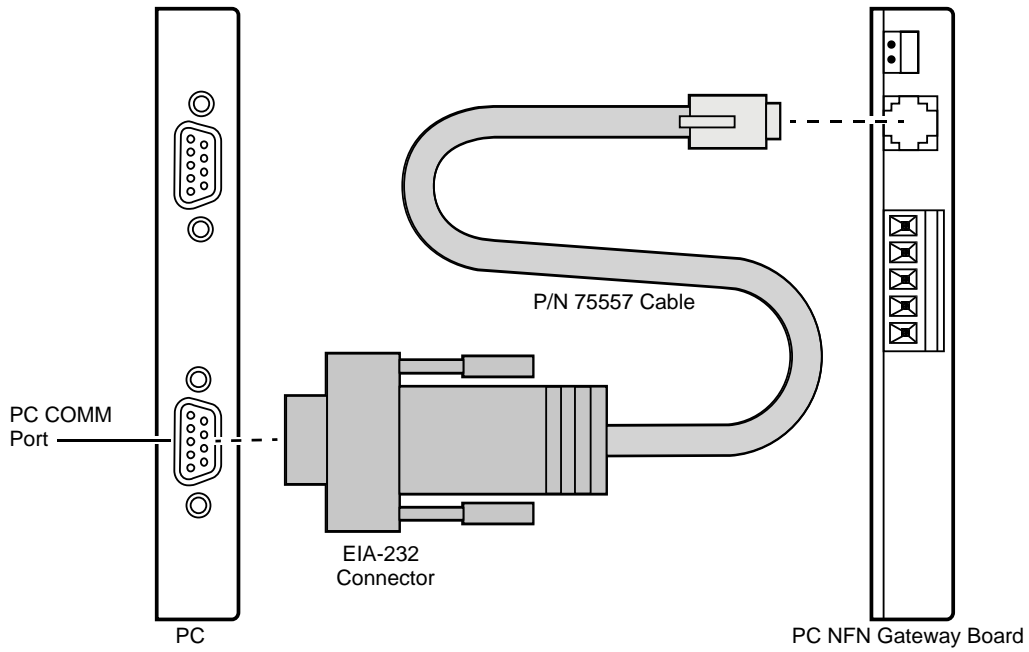


Figure 3.2 PC NFN Gateway-to-PC Connections

3.2.2 Connecting to the NFN Network

Connection to an NFN network is made through the network port using one of the following methods:

- For the OW-LITE-NW, connect the wire pairs to the terminal connector as shown in [Figure 3.3](#).
- Connect the fiber-optic connectors to the OW-LITE-NF as shown in [Figure 3.4](#).

For additional network connection instructions, refer to the *Network Communications Module NCM-W/F Product Installation Document* (P/N 51533).

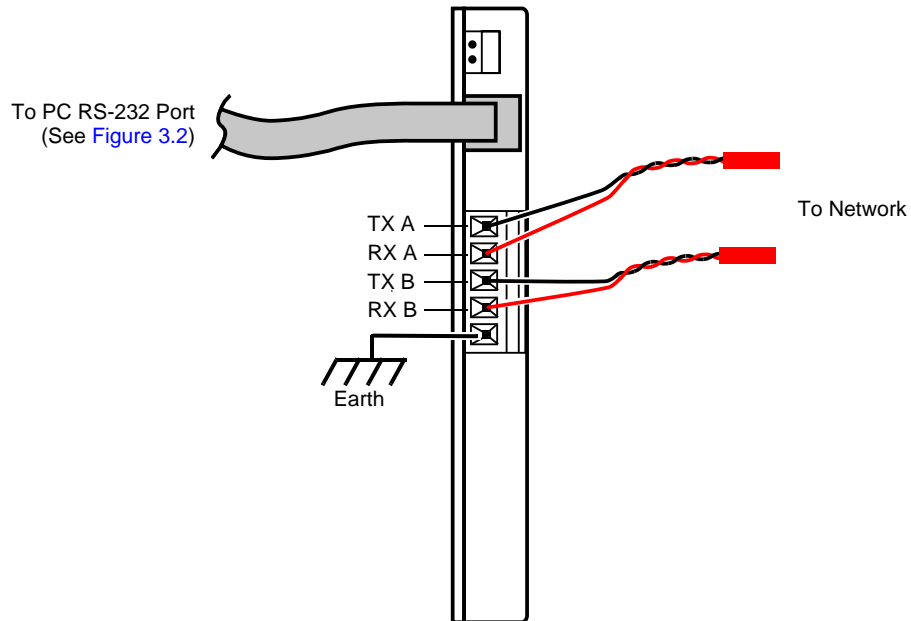


Figure 3.3 OW-LITE-NW Network Connections

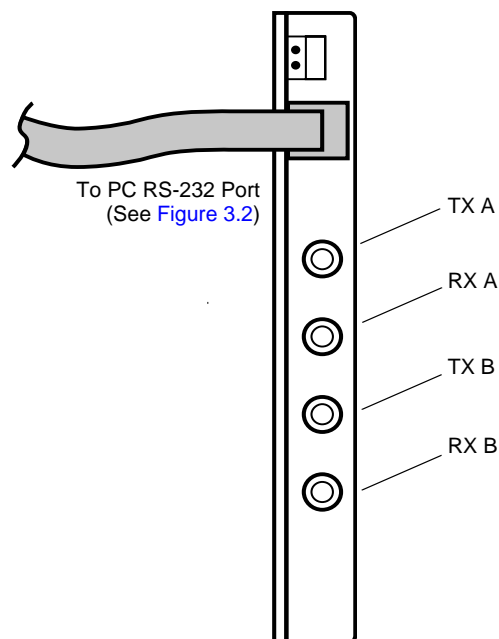


Figure 3.4 OW-LITE-NF Network Connections

3.2.3 Connecting to UPS Supervision

Note: The PC NFN Gateway board is supplied with a shunt plug over the UPS SUPV pins. Remove the shunt to make the connection for UPS supervision.

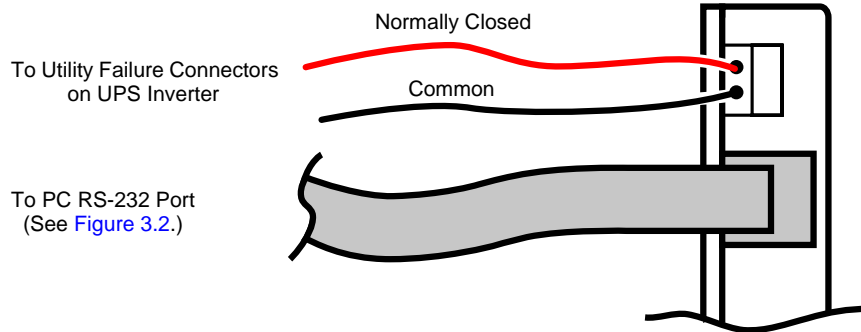


Figure 3.5 UPS Supervision Connections

3.2.4 Connection Specifications

Table 3.1 Connection Specifications

Type	Circuit Class	Specifications
UPS SUPV	2	Connect to the Utility Failure connector on the UPS Inverter.
RS-232	2	Must use P/N 75557 cable shipped with the workstation.
Wire	2	Refer to the <i>NOTI•FIRE•NET Manual</i> (P/N 51584).
Fiber	2	
Notes: <ul style="list-style-type: none"> • Wire length resistance cannot exceed 15 ohms. • Zero ohms to ground causes a ground fault. 		

3.3 Setting the Network Control Switches

In order for PC NFN Gateways to operate on the network, the network control switches must be configured depending on whether the network uses wire or fiber-optic connections.

3.3.1 Setting OW-LITE-NW Switches

Set switches on the OW-LITE-NW as follows (see [Figure 3.6](#)):

- Set ground fault detection EF switch to **ON**. The OW-LITE-NW does not indicate ground faults; it enables its +24V power supply to detect and indicate ground faults.
- If the OW-LITE-NW is at the end of line, activate on-board, end-of-line resistors by setting TERM A switch SW100 and/or TERM B switch SW102 to **ON** as necessary.

Correct configuration depends on your network design. For an explanation of design concepts, refer to the *Network Communications Module NCM-W/F Product Installation Document* (P/N 51533).

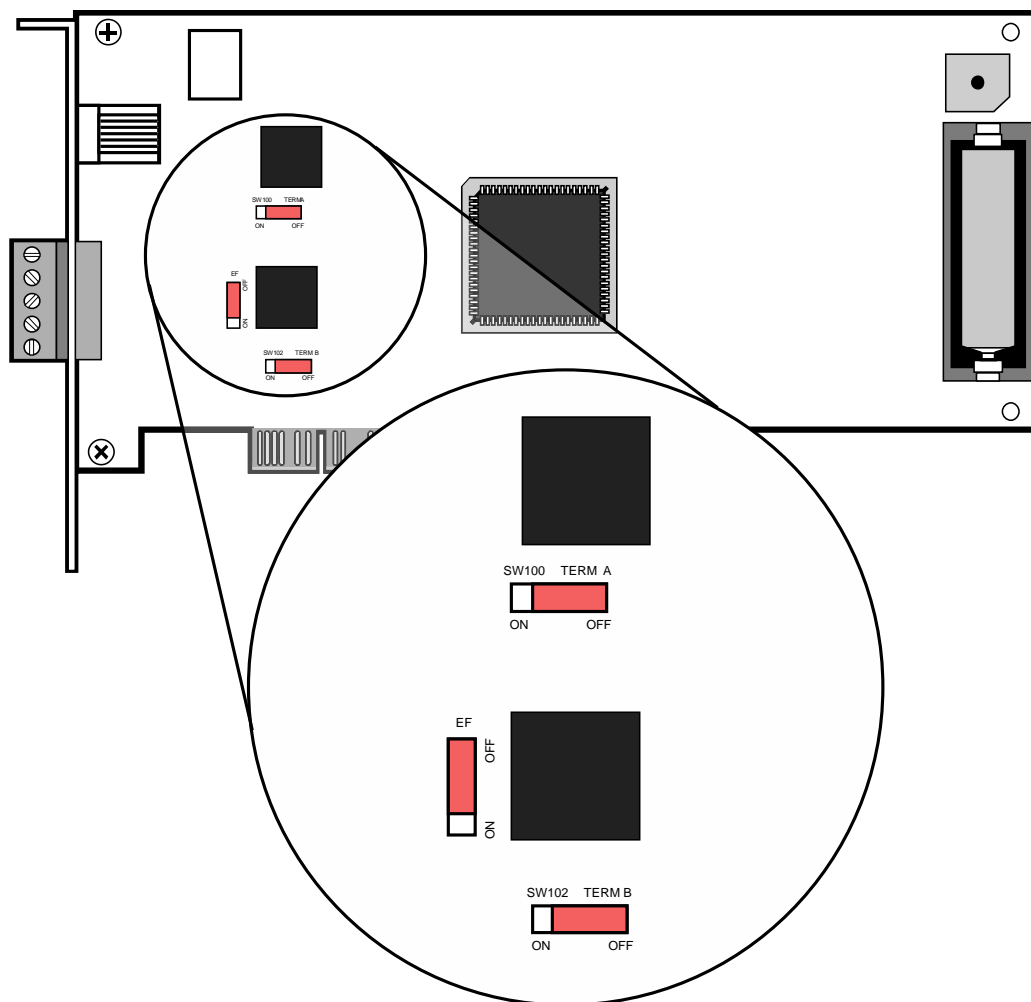


Figure 3.6 OW-LITE-NW Switch Settings

3.3.2 Setting OW-LITE-NF Switches

The OW-LITE-NF provides a set of switches (SW200 and SW202) to attempt to resolve any issues that might arise with back reflections or signal overdriving. Set switches on the OW-LITE-NF as follows (see [Figure 3.7](#)):

- For default configuration, leave the switches set to **FULL** for normal signal power.
- If an issue arises with a short distance of fiber or low dB loss, set the switch to **LOW**.

For additional information concerning switch settings and network connections, refer to the *Network Communications Module NCM-W/F Product Installation Document* (P/N 51533).

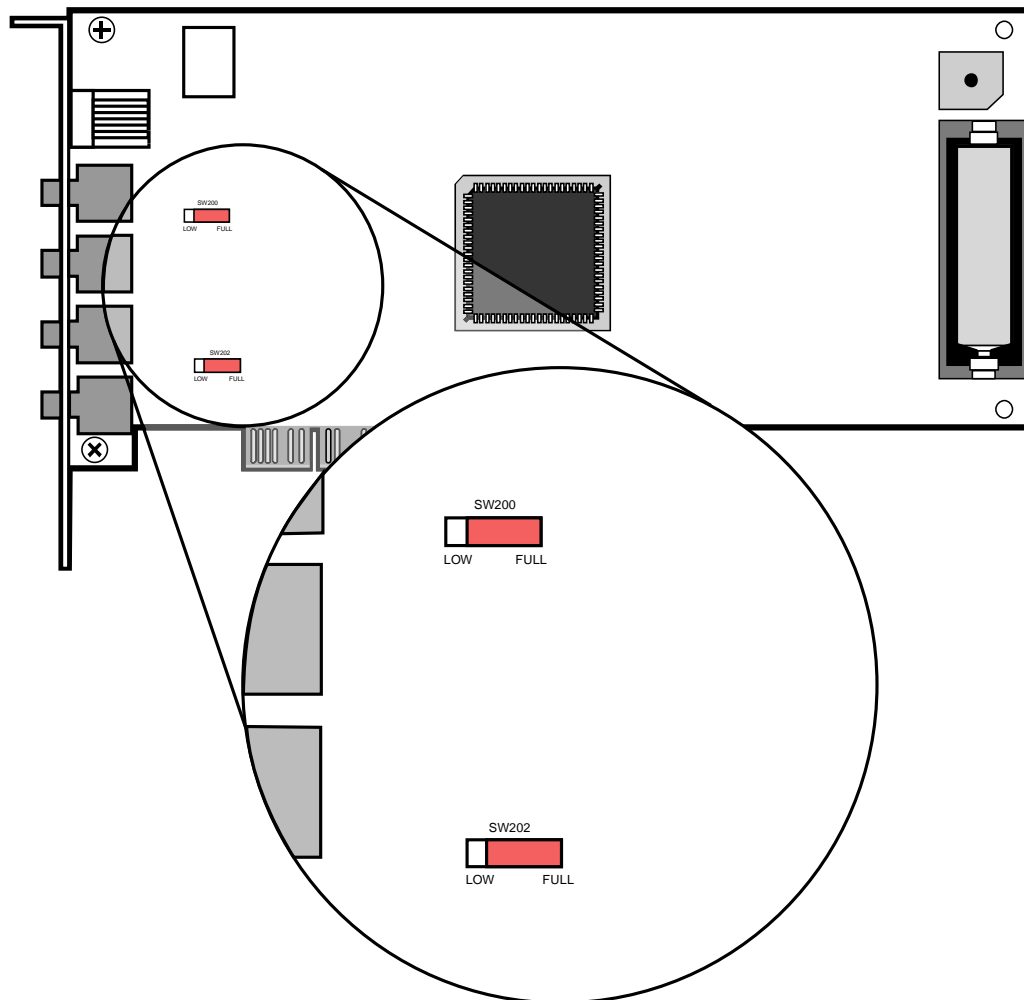


Figure 3.7 OW-LITE-NF Switch Settings

3.4 System Power


The OW-LITE-NW and OW-LITE-NF are powered via the PCI slot. No external power is required.

3.5 Testing/Maintenance

Testing and maintenance should be performed according to the *Testing and Maintenance* section of NFPA-72.

Section 4 PC NFN Gateway Configuration

4.1 Configuration Application Activation and Login

1. Double-click the  icon in the Windows Notification Area.
2. When the login dialog box displays, enter the password and click **Login**. If a password has not been set, then you will be prompted to create the password. For details regarding the password, refer to **Tools > Set Device Password** in 4.3, "Main Menu".

4.2 Basic Configuration Tool Layout

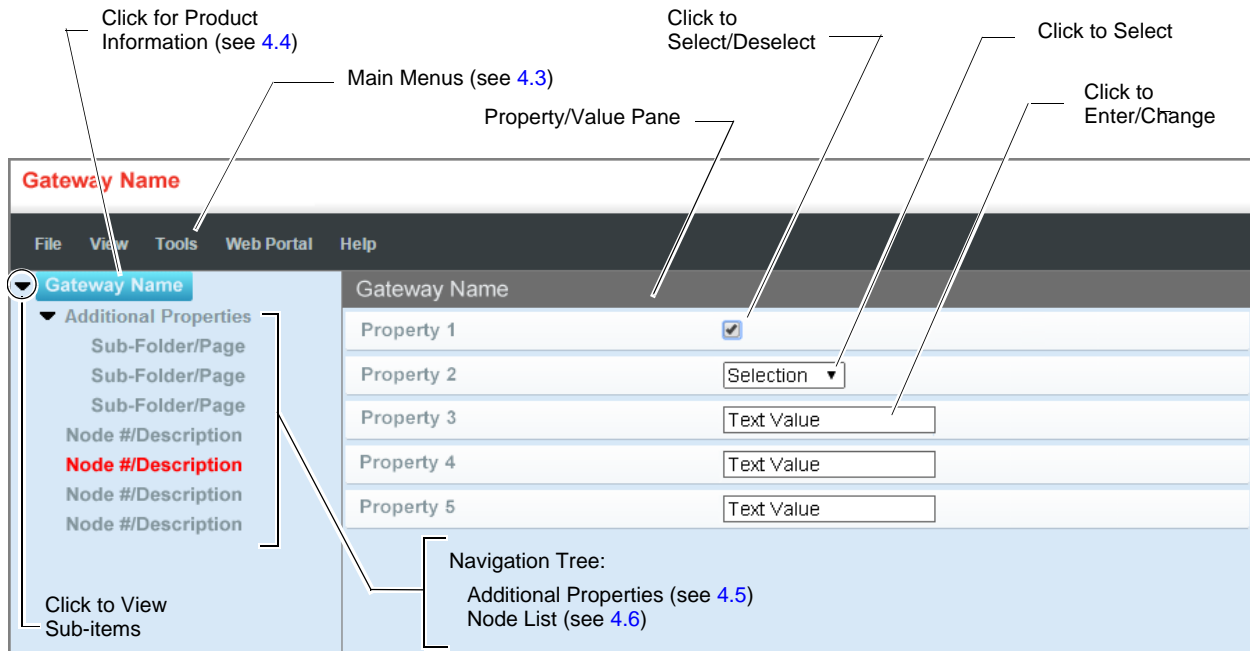


Figure 4.1 Basic Configuration Tool Layout

4.3 Main Menus

The configuration main menus are located at the upper left-hand area of the screen (see [Figure 4.1](#)).

Table 4.1 Main Menus

Menu	Sub-Menu	Description
File	Shutdown	Deactivates the PC NFN Gateway.
View	History	Displays a window containing a list of error messages.
	Node Table	Displays a window containing software version information for all monitored nodes.
	Connected Clients	Displays a window containing IP address and description information for clients connected to the PC NFN Gateway.
Tools	Set Device Password	Displays a dialog box allowing the user to change the current password. <ul style="list-style-type: none"> • Passwords are case sensitive. • Alpha and numeric characters are supported. • One character minimum and 8 characters maximum.
	Auto Detect Nodes	Select to have the gateway automatically detect all connected nodes.
Web Portal	Commission Web Portal	Selecting this option causes the web portal to request the point information from the FACP(s) to update the information on the eVance server. Refer to 4.7 , " Web Portal Setup ".
	Unregister Web Portal	Used prior to removing the PC NFN Gateway from the FACP connection.
Help	Legal	Displays legal information pertaining to the OW-LITE-NW and OW-LITE-NF.

4.4 Product Information

The following information displays when initially opening the configuration tool. It may also be accessed by clicking the first entry in the navigation tree (see [Figure 4.1](#)).

Table 4.2 Product Information

Property	Value
Type	Displays the gateway type by name.
Brand	Displays brand information.
Version	Displays the gateway version number.
Current Time/Date	Displays the current date and time information after the gateway synchronizes the clock with the SNTP server.

4.5 Additional Properties

The Additional Properties folder is located in the navigation tree area of the configuration tool (see [Figure 4.1](#)). After configuring the settings, click **Apply** in the lower right corner of the window.

Table 4.3 Additional Properties

Navigation Tree Label	Sub-Item	Property	Value
NFN Settings	Gateway Settings	Mode	Select the mode in which the PC NFN Gateway is running. (Default is Proprietary Receiving Unit)
		System Name	Unique identifier for a specific network.
	General Information	Connection Port	Displays the type of connection port used (USB).
		Connection Type	Describes how the gateway is connected to the NFN.
		NCM Version	Displays the NCM version number. Note: NCM Version does not appear when there is no NFN connection.
		NCM Status Bits	Displays the NCM status, which can be: Piezo, UPS Failure, Network Fail Port A, Network Fail Port B, High Speed Audio, NCM Sniffer Mode Active, Local Connection Limit Exceeded, or None. Note: NCM Status Bits does not appear if when there is no NFN connection.
		Fire Network Time Policy	Displays one of the following depending on the type of time synchronization used: <ul style="list-style-type: none"> • Send time: The PC NFN Gateway sets the time on the NFN network. • Unsynced: The PC NFN Gateway and NFN network are not synchronized with each other.
	Node Settings	Node	Assign the NFN node number of the OW-LITE-NW and OW-LITE-NF. (Default is 240)
		Panel Label	Enter panel label.
		Mass Notification Priority	<ul style="list-style-type: none"> • Select None for no Mass Notification. • Select Higher than Fire for Mass Notification events to take priority over Fire events. • Select Lower than Fire for Fire events to take priority over Mass Notification events.
		Send Time to Panels	Check the box to make the PC NFN Gateway send messages to each panel on the NFN network to synchronize the panel time to that of the PC NFN Gateway.
	Network Settings	Channel A Threshold	<ul style="list-style-type: none"> • Select High for a high-noise NFN network. • Set to Low for a low-noise NFN network.
		Channel B Threshold	<ul style="list-style-type: none"> • Select High for a high-noise NFN network. • Set to Low for a low-noise NFN network.
		Style 7	<ul style="list-style-type: none"> • Select the checkbox for a Style 7 SLC (Signaling Line Circuit) configured NFN network. • Uncheck the checkbox for Style 4 SLC configured NFN network.
	Web Portal Setup	Configures the Web Portal feature for use with eVance. Requires the eVance user ID, password, unique web portal name, and web portal description. Utilizes predefined customers and buildings from eVance. Refer to 4.7, "Web Portal Setup" .	

4.6 Node List

The node list is located in the navigation tree area of the configuration tool screen (see [Figure 4.1](#)). Click the desired node label to view information about that node. The information displayed is dependent on the node type. Labels for off-line nodes display in red text.

4.7 Web Portal Setup

To receive events and configuration information for use in tools such as the Inspection Manager, the ONYXWorks Lite must be associated with a specific site, as follows:

1. In the navigation tree section of the ONYXWorks Lite configuration tool, select **Additional Properties > Web Portal Setup**.
2. Enter the information in the text boxes in the right-hand column. The user name and password are the same as those used to access the eVance web site. The web portal name must be unique for the eVance account to register this web portal. The web portal description is used in eVance to identify this specific ONYXWorks Lite.
3. Click **Apply**. When successfully completed, a dialog box displays.
4. Click **OK**. The “Assign the Web Portal...” dialog box displays.
5. From the customer drop-down list, select the appropriate customer for this site. The web portal displays the node number(s) for the connected FACP(s).
6. Select the appropriate building for each node using its drop-down list.
There are additional selections for “<Unassigned – Delete Equipment>” and “Unassigned” options. In both of these cases, the panel’s points will not be configured on eVance and, with the Delete Equipment option, the existing equipment for that node will be deleted from eVance.
7. Click **Apply**. A commissioning prompt displays.
8. Click **Yes**.

The ONYXWorks Lite communicates with each connected panel and sends a list of all the configured points to eVance. Because these points are defined in eVance, they are displayed when a new test session is created.

Section 5 Configuration Tool Settings

5.1 Administrator Login

5.1.1 New Workstation

1. Start the workstation if it is not already running. The Administrator Password dialog box displays.
2. Enter the Administrator password (8 characters minimum, case sensitive).
3. Re-enter the password to confirm.
4. Click **OK**. The System Name dialog box displays with a random system name in the field.
5. Enter a unique system name in the field.
6. Click **OK**. The workstation starts.
7. Login to the workstation as specified in 7.1.1, "Login".

5.1.2 Software Upgrade on Existing Workstation

1. Start the workstation if it is not already running. The Administrator Password dialog box displays.
2. Enter the Administrator password. Use the same password used for the previous software version.
3. Click **OK**. The System Name dialog box displays with a random system name in the field.
4. Enter a unique system name in the field.
5. Click **OK**. The workstation starts.
6. Login to the workstation as specified in 7.1.1, "Login".

5.2 Factory Defined User Profiles and their Passwords

The user must log into the workstation before any of its settings can be configured. An Administrator needs to log in to change an existing user's password or to add a user and their password. The factory defined user "Admin" has such a security option.

5.3 Configuration Tool

5.3.1 Overview

The configuration tool is used to customize the workstation's graphical user interface (GUI) to display the building's facilities monitoring system. An authorized event responder uses the customized GUI to identify the location of, and respond to, an annunciated event. After modifying a workstation GUI design with the configuration tool, it must be verified to be correctly displayed.

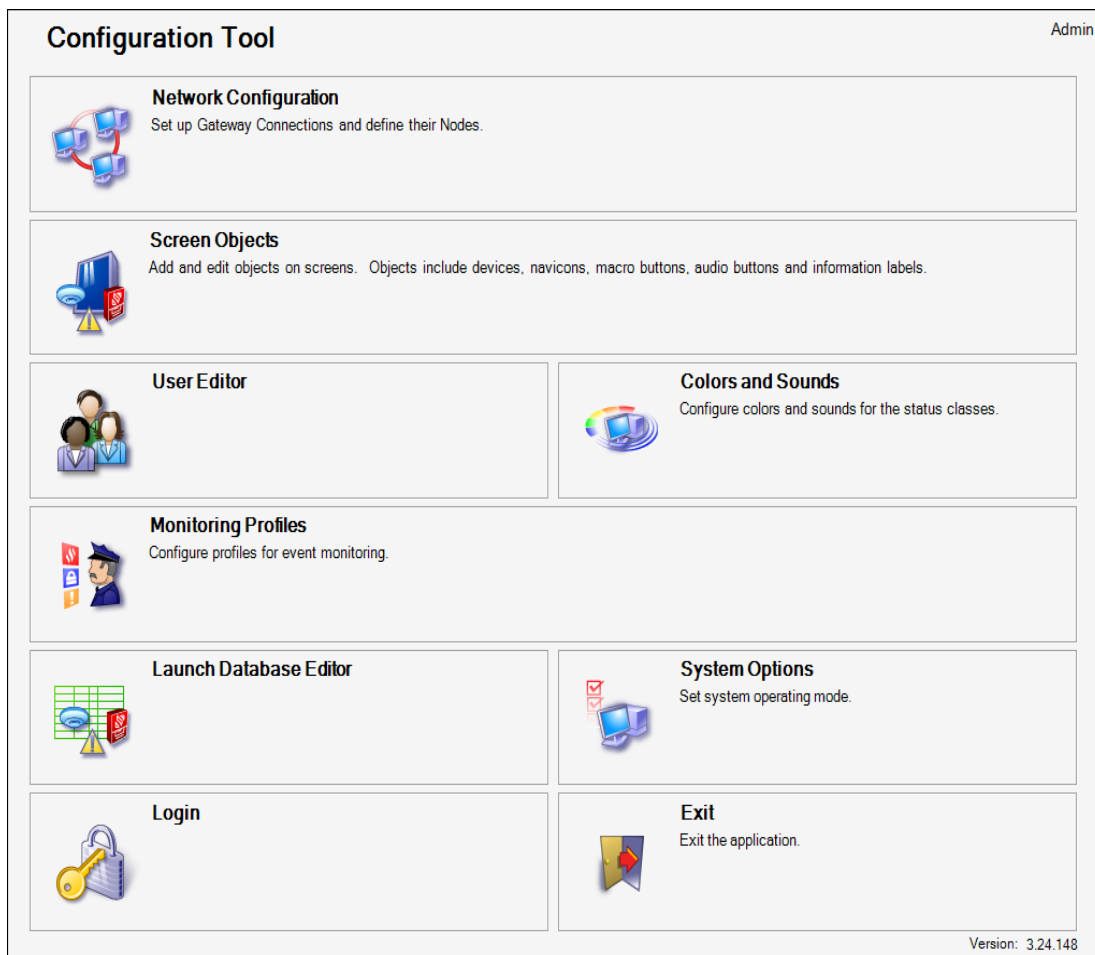
5.3.2 Starting and Exiting the Configuration Tool

Start the configuration tool on the workstation using one of the following methods:

- In the workstation application, go to **Configure > Launch Configuration Tool**.
- From Windows, go to **Start > Programs > Facilities Monitoring > Configuration Tool** and click the **Use System Database** icon.

Exit the configuration tool by clicking the **Exit** icon.

5.3.3 Configuration Tool Layout



Screen Feature	Description
Network Configuration	Allows an Administrator to add or delete monitored networks to the system configuration.
Screen Objects	Allows an Administrator to create and place informational objects on a graphics screen.
User Editor	Allows an Administrator to set workstation user passwords and privileges.
Monitoring Profiles	Allows an Administrator to select which nodes are monitored by a workstation. Refer to 5.3.4, "Monitoring Profiles" for additional information.
Launch Database Editor	Allows an Administrator to edit the workstation database in a spreadsheet format.
Login	Allows a user to log in to the NFN system. The user can also log out of the system and log in as another user.
Colors and Sounds	This section of the configuration tool allows a user to configure custom colors and sounds for each event type. Refer to 5.3.5, "Color and Sound Configuration" for additional information.
System Options	Allows an Administrator to select options as to how the workstation interface will operate. Refer to 5.3.7, "System Options" for additional information.
Exit	Click the icon to exit the configuration tool.

Figure 5.1 Configuration Tool Layout

5.3.4 Monitoring Profiles

Monitoring profiles allow the Administrator to select which nodes are monitored by a workstation.

Monitoring profiles are event annunciation filters that are set up to monitor or not monitor an event location and its event type at the workstation.

By using monitoring profiles along with control profiles, supervision of portions of the network is possible.

Each profile is defined for a specific network and/or node on a network and determines which events are displayed by the workstation.

Monitoring profiles are configured using the configuration tool. Refer to the *ONYXWorks Lite Configuration Tool Installation & Operation Manual* (P/N 53508) for additional information.

The factory defined monitoring profile 'Default' is set to monitor all networks and nodes. Therefore, to hide any desired networks or nodes and the respective event types, the Administrator must create a new monitoring profile using the configuration tool.

Monitoring profiles are activated through the workstation as follows:

1. Select **Configure > Monitoring Profiles**. The Monitoring Profiles window displays.
2. Select a profile listed in the Monitoring Profile column of the window. The 'Default' profile may be the only one listed.
3. Click **Activate Profile**. The workstation displays information only for the locations and event types specified in the selected monitoring profile.

5.3.5 Color and Sound Configuration

Custom colors and custom sounds for different event types are created in the configuration tool (**Tools >Color and Sound Configuration**) that is launched from the workstation's main menu (**Configure >Launch Configuration Tool**). Color and sound settings are saved when exiting the configuration tool and clicking **Yes** to the Save Changes prompt. Refer to the *ONYXWorks Lite Configuration Tool Installation & Operation Manual* (P/N 53508) for additional information.

5.3.6 Event Color Coding

Each event within the NFN system has a corresponding color. This color coding is used when displaying the event on-screen, when viewing events in history manager, and various other applications throughout the software.

Each off-normal event has a corresponding normal event. Every normal discrete event within the workstation is displayed with the color gray when in Graphics mode.

Off-normal events and their corresponding default colors are listed in the following table.

Table 5.1 Event Icon Color Coding

Default Event Color	Off-Normal Event	Default Event Color	Off-Normal Event
Yellow	<ul style="list-style-type: none"> • Pre-Alarm • Verifying for Fire Alarm • Alert Condition • Soft Anti-Passback Warning • Point Inactive • Fault Condition • Temperature Alarm • Zone Trouble • Ground Fault • AC Power Failure • Trouble • Loop Trouble • Very Low Value • Very High Value • High Value • Low Value • Cover Open • Out of Paper • Transmission Trouble • Fuse Failure • Short Circuit • Open Circuit • Position Alarm • Video Signal Loss • Unlock • Program Entry • Program Exit 	Red	<ul style="list-style-type: none"> • Fire Alarm (Non Latching) • Alarm • Agent Release • Tamper Switch Activated • Agent Release Abort • Door Ajar • Forced Entry • Recent Alarm • Panic Alarm • Supervisory Alarm • Extremely Low Value • Extremely High Value • Addressable Input On • Restart
	Gray		<ul style="list-style-type: none"> • Offline

5.3.7 System Options

System options settings are described in the following table.

Table 5.2 System Options Configuration

Setting	Possible Settings	Comments
Icon Set	Select the desired icon set for the workstation to use for screen objects.	After selecting an icon set, the selection will not be displayed in the Icon Set drop-down list when the System Options dialog box is reopened.
Operating Mode	Protected Premises Control Unit	
System Name	Enter unique name.	20 characters maximum.
Time Server Settings	IP Address	If the IP address for the time server is the same IP address as this PC, then the time server will run, else this PC will connect to the time server to synchronize the clock on this PC.
Audio Multicast IP	Does not apply.	
Mass Notification Priority	Does not apply.	

5.4 Network Right Click Commands

In the configuration tool, navigation tree, right clicking on a network name displays the following options:

- **Add Node** - Adds a node to the network. Select the node type from a list of choices and type in the IP address of that node.
- **Import Panel Database** - Imports a Verifire Tools database. Any nodes and points that are in the database will be autocreated on the network.
- **Rename** - Allows the user to rename the network. This is the equivalent of replacing the network alias in the Properties window.
- **Delete** - Allows the user to delete the network. A confirmation prompt displays.
- **Properties** - Allows the user to change the network alias name and IP address of a gateway.

5.5 Auto-Creation of Screens, Nodes, and Points



NOTE: Every addressable device must be represented on a workstation screen as a point icon. If the workstation software application auto-create function has been disabled, meaning the check box that controls the operation has been unchecked, or if a addressable device has been deleted, then the first time the addressable device reports an event an addressable device will be assigned to the default workstation screen. Device icons generated in that manner should be edited to ensure all information is complete and relocated to an appropriate workstation screen.



NOTE: The navigation tree may be a maximum of six levels deep including the Home screen.

The auto-creation process takes place each time a new point on the gateway reports an off-normal event to the workstation. Point information is placed on a “holding screen” with a generic name (i.e., Screen 1) from which an Administrator can relocate the point to its proper screen location using the Screen Objects window in the configuration tool. Refer to the *ONYXWorks Lite Configuration Tool Installation & Operation Manual* (P/N 53508) for additional information.

The auto-creation process creates a parent screen for the gateway reporting the event, a child screen for the node, and a child screen under that for the points for that node (see [Figure 5.2](#)). Up to 64 point icons may be auto-created on a workstation screen before another screen is created.

An asterisk (*) next to an entry indicates the entry and its name were auto-created and its position in the tree must be redefined by an Administrator.

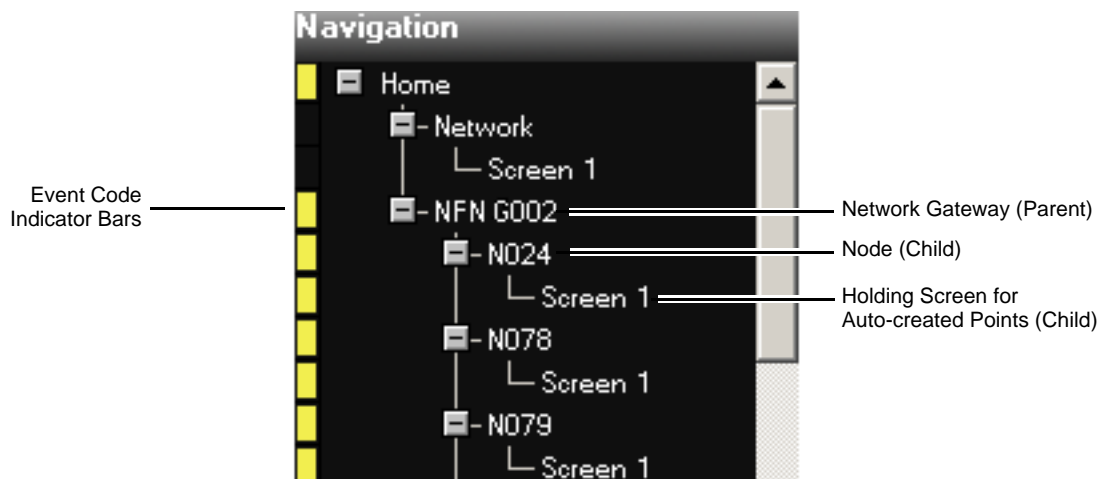


Figure 5.2 Example of Navigation Tree with Auto-Creation Process

The Administrator organizes the navigation tree in such a manner that it will aid the user with locating a specific event in a campus (site) or building. The navigation tree can be arranged in a parent-child hierarchical relationship so a user can, in a logical progression, “drill-down” from a site view to the floor plan of a building on that site. The tree also shows at what level of the hierarchy an event is occurring. When events occur, boxes appear at the left side of the tree in the color corresponding to the highest priority event (see [Figure 5.2](#)).

5.5.1 Managing the Auto-creation Process

The Administrator can rename, reorder, cut and paste, copy, and delete auto-created screens in the configuration tool's Screen Objects window. Refer to the *ONYXWorks Lite Configuration Tool Installation & Operation Manual* (P/N 53508) for additional information.

Table 5.3 Managing Auto-created Screens

Action	Description
Reorder Screens	Left-click on the screen label in the navigation tree and drag and drop it to the desired hierarchical level. Dropping between screen levels places the screen between those levels. After screens are moved, navicons maintain their link to the screen.
Delete Screen	Right-click the screen label and select Delete . Note: A workstation screen cannot be deleted if it contain point icons. Icons must first be deleted or relocated.
Cut and Paste Points	Right-click the point and select Cut . Navigate to the desired screen location, right-click, and select Paste .
Copy and Paste Points	Right-click the point and select Copy . Navigate to the desired screen location, right-click, and select Paste .
Delete Points	Right-click the point and select Delete . Click Yes to the confirmation prompt.

5.6 Autocreating Gateway Point IDs

A gateway's nodes and the node's points can be manually added and defined with the configuration tool, however it is highly recommended that the auto-creating method be used instead. The auto-creating method captures the node's exact point ID. It is highly recommended that when initially configuring a facility's monitoring network that it be modified off line; not while the workstation is monitoring the gateway. Autocreate gateway point icons as follows:

1. Make sure the connection between the respective networks and the monitoring workstation is made.
2. Start the monitoring workstation software application.
3. If you have not already done so perform the steps in [5.8, "Macro Commands"](#).
4. Work with others to initiate troubles in the gateway devices (points) that will be reported as off-normal events to the monitoring workstation.
 - The troubles in those points will automatically create an icon on the monitoring workstation screen (64 icons per screen before another screen is automatically added).
 - Those icons will have the exact point ID.
 - When points are auto-created, a system backup should be performed using the monitoring workstation's PC Monitor application.
5. If applicable to your situation, you are now ready to proceed with [5.7, "Workstation Database Backup and Restore"](#).

5.7 Workstation Database Backup and Restore

5.7.1 Backing Up the Database

Backing up the workstation database is recommended before making any modifications to prevent inadvertent data loss. Back up the database as follows:

1. From the Windows taskbar, right click the **PC Monitor** icon and then click **Backup System Data**.
2. Browse to the location where the backup files are to be stored (such as a USB flash drive).
3. Create a new folder to hold the backup files and folders.
4. Enter a file name for the backup database in the 'File name' field and then click **Save**.

5.7.2 Restoring a Backed-Up Database

Restore backed-up database files on the workstation as follows:

1. Shut down all fire system applications, including gateways, except for PC Monitor.
2. From the Windows taskbar, right click the **PC Monitor** icon, and then click **Restore System Data**. The PC Monitor dialogue opens.
3. Click **Yes** to verify all other applications have been closed. The Open dialog box opens.
4. Browse to the backed-up database folder (created in 5.7.1, "[Backing Up the Database](#)") and click the data file (*.dat) to select it.
5. Click **Open**. The backed up fire system database is restored.
6. Verify the database was correctly restored.

5.8 Macro Commands

Macro commands are created in the configuration tool which is launched from the workstation's main menu (**Configure >Launch Configuration Tool**).

Macro commands are created and edited on the configuration tool Screen Objects window. Administrators access the Macro Editor function in the Tools menu (**Tools > Macro Editor**). The Administrator creates a macro command by naming it and assigning it a macro command. The macro command's Menu list of choices will be contingent on the gateway type, point, and node type that is selected. Macro settings are saved when exiting the configuration tool and clicking **Yes** to the Save Changes prompt. Refer to the *ONYXWorks Lite Configuration Tool Installation & Operation Manual* (P/N 53508) for additional information.

On the workstation, a macro command is activated in one of two ways:

- Clicking on a macro icon in the graphics display.
- Clicking on the **Macros** menu item on the workstation menu bar and selecting the desired macro from the list. The Macros menu item displays only if the user has administrator-level privileges.

5.9 Custom Icon Recommendations

When creating custom icons, the following recommendations should be followed for optimal appearance:

- 32 bit PNG File – Works best for the color tinting used in alarm reporting. Refer to [Table 5.4](#).
- 256 x 256 pixels, square – Image files larger than the recommended size require more memory and may degrade system operation.
- Gray scale – Light colored, gray scale images work best, since colored images interfere with the color tinting used in alarm reporting. Refer to [Table 5.5](#).

Table 5.4 Effect on Non-PNG Icon File on Background















PNG File	Non-PNG File
 <p data-bbox="527 821 709 842">Visible Background</p>	 <p data-bbox="852 821 1151 842">Background Blocked by Square</p>

Table 5.5 Effects of Icon Color on Alarm Reporting

Icon Type	If Normal Icon Has This Color...	Alarm and Trouble Icons Appear As These Colors	
Recommended Icon	Normal Status 	Alarm 	Trouble 
Normal Icon Too Dark	Normal Status 	Alarm 	Trouble 
Normal Icon with Color	Normal Status 	Alarm 	Trouble 
Normal Icon Same Color as Alarm Icon	Normal Status 	Alarm 	Trouble 

Section 6 Workstation Settings

6.1 Windows Settings

Table 6.1 Windows Settings

Setting	Required Value
Windows Update	Check for updates but let me choose whether to download and install them
IP Address	Valid IP Address required if connecting to LAN
Power Options	Display: Turn off the display: Never Computer: Put the computer to sleep: Never
Time Zone	Local time zone
Daylight Savings Time	Set appropriate for local area

6.2 Workstation Settings

The workstation settings described in this section are available from the Configure > Options menu. These settings apply only to the local workstation.

6.2.1 Options Window Command Buttons

On-screen command buttons common to the Options window tabs are described in the following table.

Table 6.2 Options Window Command Buttons

Button	Description
Apply	Saves the settings, but keeps the Options window open.
OK	Saves the settings and closes the Options window.
Cancel	Closes the Options window without saving settings.

6.2.2 General Tab

The General tab allows the Administrator to configure overall settings for workstation operations as described in the following table.

Table 6.3 General Tab Settings

Setting	Possible Settings	Description	Comments
Event Label:			
The event label is displayed in the event list when the point is in an off normal condition. The event label consists of a combination of network, node, and point labels as described below.			
Network Label	Network Alias	Display the user-defined description of the network.	
	None	Do not display the assigned network alias.	
Node Label	Node Alias	Display the user-defined description of the node.	
	Node Number	Display the system assigned node number.	
	None	Do not display the assigned node alias or number.	
Point Label	Point Alias	Display the user-defined description of the point.	
	Point Number	Display the system assigned point number.	
	None	Do not display the assigned point alias or number.	
Icon Label:			
The icon label is displayed below the icon on the graphics screen. Icon label options are described below.			
	Event Label	Display the event label as described above.	
	Description	Display the point description programmed into the FACP.	
	None	Display nothing.	
History Backup:			
The external backup file is named with the date: YYYYMMDD.HIS. History backup options are described below.			
Number of days before performing history backup	Disabled	Do not back up history.	
	1 - 62	Interval in days that history backup is performed.	
Number of days to keep in history following backup	0 - 30	Length of time in days to retain a history backup.	
Check Boxes:			
Options selectable via check boxes are described below.			
Show only off normal devices	True	Display only icons of points that are off normal. If there are no current events on the system, there will be no points visible in the graphics display.	
	False	Show all points regardless of state.	
Auto-activate next event after acknowledge	True	Once the first event in the New Events box is acknowledged, the next event automatically activates. The workstation plays any media files linked to the event.	
	False	When the first event is acknowledged in the event box does not auto-activate when an event is acknowledged.	
Automatically Navigate On Event	True	Once an event reaches the top of the New Events box, the workstation navigates to the screen containing the device icon associated with the event.	Recommended setting.
	False	Do not automatically navigate to the screen with the off-normal event.	

Table 6.3 General Tab Settings (Continued)

Setting	Possible Settings	Description	Comments
Extract Descriptions from Panel	True	Use point descriptions as received from the FACP.	
	False	Use point descriptions as defined by the configuration tool and discard point descriptions received from the FACP.	
Shut Down PC on Workstation Shutdown	True	Automatically shut down the computer hosting the workstation when the application is closed normally (through File > Exit).	
	False	Do not automatically shut down the workstation's computer when normally closed.	
Suppress Automatic Device Icon Creation	True	Use this selection to hide automatically-created device icons from all navigation window displays. This selection also prevents the workstation from automatically navigating to display off-normal events on devices with automatically created icons.	When this setting is enabled, the workstation will continue to autcreate icons and screens, but they will be hidden in the workstation graphics display as well as the navigation tree.
	False	Do not hide automatically created device icons.	
Show Navigation Icon Labels	True	Display the user-defined text below the navigation icons.	
	False	Hide the user-defined text located below the navigation icons.	
Omit Control Point On, Point Active, and Zone on From History	True	Control Point Activations, Point Activations, and Zone Activations will not be written to history.	
	False	Store these events in history.	

6.2.3 User Features Tab

Table 6.4 User Features Settings

Setting	Possible Settings	Description	Comments
Unacked Event Alarm Configuration:			
This feature is used to automatically activate a user-defined macro if an alarm is present in the new event list for more than the configured amount of time.			
Use Unacked Event Supervision	True	Automatic Unacked Alarm Operation enabled.	
	False	Automatic Unacked Alarm Operation disabled.	
Unacked Event Timeout (3-60 Minutes)	3 - 60	Time in minutes before the user-defined macro is executed.	
Macro Activated on Alarm	Macro name	Select a macro from the list.	
	None	Do not activate a macro.	
Security:			
Inactivity Timeout (0-20) minutes	1-20	Length in minutes of no activity after which a user will be automatically logged out.	
	0	Do not automatically log out a user.	
User Responses:	8 user-defined responses.	Enter text that will be stored in history as responses to events. These are displayed when a user right-clicks on an icon in the graphics screen.	

6.2.4 Event Printer Tab

The Event Printer tab allows the user to enable or disable the optional printer. A default output format and monitoring profile are preconfigured for a local event printer. It is only necessary to enable the printer in Windows. The local event printer must be named "Local Event Printer" through Windows. Consult Windows information for details about naming the printer. To modify the printer configuration, a user-definable monitoring profile must be selected along with a user-definable output format. A sample event will be displayed using the selected output format. Settings are described in the following table.

Table 6.5 Event Printer Tab Settings

Setting	Possible Settings	Description
Event Printer:		
The event printer settings are available only if a Windows printer is connected to the workstation. Click the fields below the headings to display the options.		
Enabled/Disabled	Enabled	Enable the connected event printer.
	Disabled	Do not enable the connected event printer.
Monitoring Profile	Default	Use the system default monitoring profile.
	User-defined Monitoring Profiles	Select a user-defined profile from the drop-down list. Refer to 5.3.4, "Monitoring Profiles" .
Output Format	Default	Use the system default output format.
	User-defined Output Format	Select an output format from the drop-down list. Refer to 6.2.5, "Output Tab" .
Sample Output:		
Displays a sample of the output that will be printed using the settings selected above.		

6.2.5 Output Tab

An output is the format of data that is sent to a local event printer. Once output formats are created and named, they appear on a list of choices on the Event Printer tab. Output tab settings are described in the following table.

Table 6.6 Output Tab Settings

Setting	Possible Settings	Description
Buttons:		
Add Format		Click to display an output format name dialog box. Enter a unique output format name and click Yes . The name is displayed in the Output Formats field.
Delete Format		Click to delete the output format name displayed in the Output Formats list. Click Yes in response to the output format delete confirmation prompt. <ul style="list-style-type: none"> If the output format is NOT used in a printer setup, the selected output format is deleted. If the output format IS used in a printer setup, a message displays indicating that the output format cannot be deleted. In order to delete the format, the setups using the format must be configured to use another output format or be deleted.
Output Formats:		
Output Formats Field	Listed Outputs	Click the down-arrow to display the available output formats (added formats display automatically). The selected output is configured/modified using the Available Fields/Format Fields lists.
Available Fields	<ul style="list-style-type: none"> Action Actual Time Card Facility Code Card Number Card Time Description Network Alias Node Alias Point Alias Point Type Status User Defined 	Lists the types of information that can be included in the selected output. Add fields using any of the following methods: <ul style="list-style-type: none"> Select one at a time - Double click on the entry or click on an entry and then click on the right arrow button. Select several - Press and hold the Ctrl key while selecting all desired fields. Then click the right arrow button. Select all - Click the double right-arrow button. Selecting "User Defined" activates the User Defined Messages field (see below).
Format Fields	Selected Fields	Displays the format fields configured for the output format displayed in the Output Formats field. To remove fields from the output, select the field name(s) from the list (see above) and use the left arrows to remove from the output.
<p>User Defined Messages: Active only when the "User Defined" output format is selected in the Format Fields list. Click the field to the right of the event types to enter/modify the message associated with each type of event. The "Other" message is used for other event types not included in the list.</p>		

Section 7 Operation

7.1 Login and Log Out

7.1.1 Login

The Administrator grants users workstation login privileges. When a new user logs in, the workstation software automatically logs out the previous user. Log in as follows:

1. On the workstation software application's Main Menu, select **File >Login**. The User Login window displays.
2. Click the desired user name in Available Users field.
3. Type the password in the Password field.
4. Click **OK**. The name of the current user appears at the top right of the workstation floor plan area.

7.1.2 Log Out

1. On the workstation software application's Main Menu, select **File >Login**. The User Login window displays.
2. Click the current user's name in the Available Users field.
3. Click **Logout**. The user is logged out, but the system continues to be monitored.

7.2 Display Modes

The Administrator configures how the workstation graphical user interface is normally displayed. If the Administrator allows it, the user can toggle between graphics and text display modes from the workstation View menu. These display modes are described below.

7.2.1 Graphics Mode

In graphics mode, the workstation displays the system as floor plans, point icons, and real-time event information in tabular/list form (see [Figure 7.1](#)). The Administrator designs and implements the floor plan that is used when the workstation is in graphics mode.

A floor plan is a drawing or imported file that is the background layer of the workstation screen. It serves as the primary source for visual feedback for the location of an off-normal event in the system. It serves as a visual representation of a point's location in a building. The point types can include fire panels, fire protection points, security points, and other equipment.

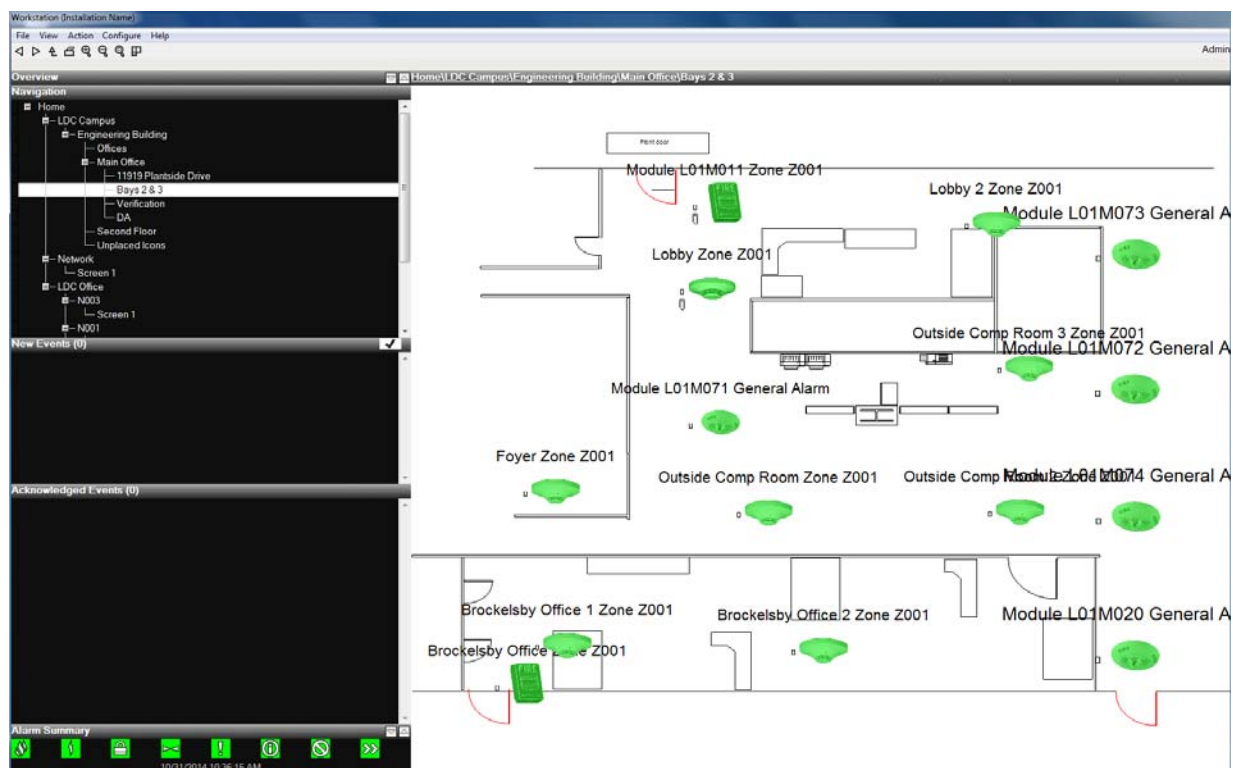


Figure 7.1 Example Graphics Mode Screen

7.2.2 Text Mode

In text mode, the New Events and Acknowledged Events panes are expanded (in tabular form) across the entire workstation display (see [Figure 7.2](#)). As in graphics mode, events are updated in real time. A Panel Ack column is displayed with check-boxes to indicate that the event is known to be acknowledged at the fire alarm control panel (FACP).

Workstation (LDC)
File View Action Configure Help Admin

New Events (273)

Point	Reported Time	Network	Point Type	Status	Descript...	Node	Event Description
NET 218 N003 L01M010	5/16/2012 11:21:33 AM	NET 218	Monitor Module	ACKed Fire A...	This is N...	N003	
NET 218 N069 BRAND	1/2/2003 7:39:51 AM	NET 218	Control Panel	ACKed Trou...	Incompa...	N069	Network Incompatible
NET 218 N069 T251	1/2/2003 7:44:36 AM	NET 218	Network Device	ACKed Trou...	NETWO...	N069	NETWORK INCOMPATIBLE
NET 218 N033 L04M130	5/16/2012 9:55:05 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M131	5/16/2012 9:55:05 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M132	5/16/2012 9:55:05 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M133	5/16/2012 9:55:05 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M134	5/16/2012 9:55:05 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M135	5/16/2012 9:55:05 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M136	5/16/2012 9:55:05 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M137	5/16/2012 9:55:05 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M138	5/16/2012 9:55:05 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M139	5/16/2012 9:55:06 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M140	5/16/2012 9:55:06 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M141	5/16/2012 9:55:06 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M142	5/16/2012 9:55:06 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M143	5/16/2012 9:55:06 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M144	5/16/2012 9:55:06 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M145	5/16/2012 9:55:06 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M146	5/16/2012 9:55:06 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M147	5/16/2012 9:55:06 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M148	5/16/2012 9:55:06 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response
NET 218 N033 L04M149	5/16/2012 9:55:06 AM	NET 218	Monitor Module	ACKed Trou...	Module ...	N033	No Response

Acknowledged Events (92)

Point	Reported Time	Network	Point Type	Status	Descript...	Node	Event Description
NET 218 Node 192.168...	5/15/2012 2:07:10 PM	NET 218	Node	*Fault Condit...	DVC	Node 192.168.1.2...	
NET 218 Node 192.168...	5/15/2012 2:07:11 PM	NET 218	Node	*Fault Condit...	VESDA	Node 192.168.1.2...	
NET 218 Node 192.168...	5/15/2012 2:07:11 PM	NET 218	Node	*Fault Condit...	NFS-640	Node 192.168.1.2...	
NET 218 Node 192.168...	5/15/2012 2:07:11 PM	NET 218	Node	*Fault Condit...	NFN Gat.	Node 192.168.1.2...	
NET 218 Node 192.168...	5/15/2012 2:07:12 PM	NET 218	Node	*Fault Condit...	DVC	Node 192.168.1.2...	
NET 218 Node 192.168...	5/15/2012 2:07:12 PM	NET 218	Node	*Fault Condit...	NFN Gat.	Node 192.168.1.2...	
NET 218 Node 192.168...	5/15/2012 2:07:12 PM	NET 218	Node	*Fault Condit...	NFN Gat.	Node 192.168.1.2...	
NET 218 Node 192.168...	5/15/2012 2:07:12 PM	NET 218	Node	*Fault Condit...	NFN Gat.	Node 192.168.1.2...	
NET 218 Node 192.168...	5/15/2012 2:07:12 PM	NET 218	Node	*Fault Condit...	NFN Gat.	Node 192.168.1.2...	
NET 218 Node 192.168...	5/15/2012 2:07:12 PM	NET 218	Node	*Fault Condit...	NFN Gat.	Node 192.168.1.2...	

Alarm Summary

5/16/2012 11:39:45 AM

Figure 7.2 Example Text Mode Screen

7.3 Graphics Display Screen

The workstation graphics display screen is shown in [Figure 7.3](#). Each feature is described in [Table 7.1](#).

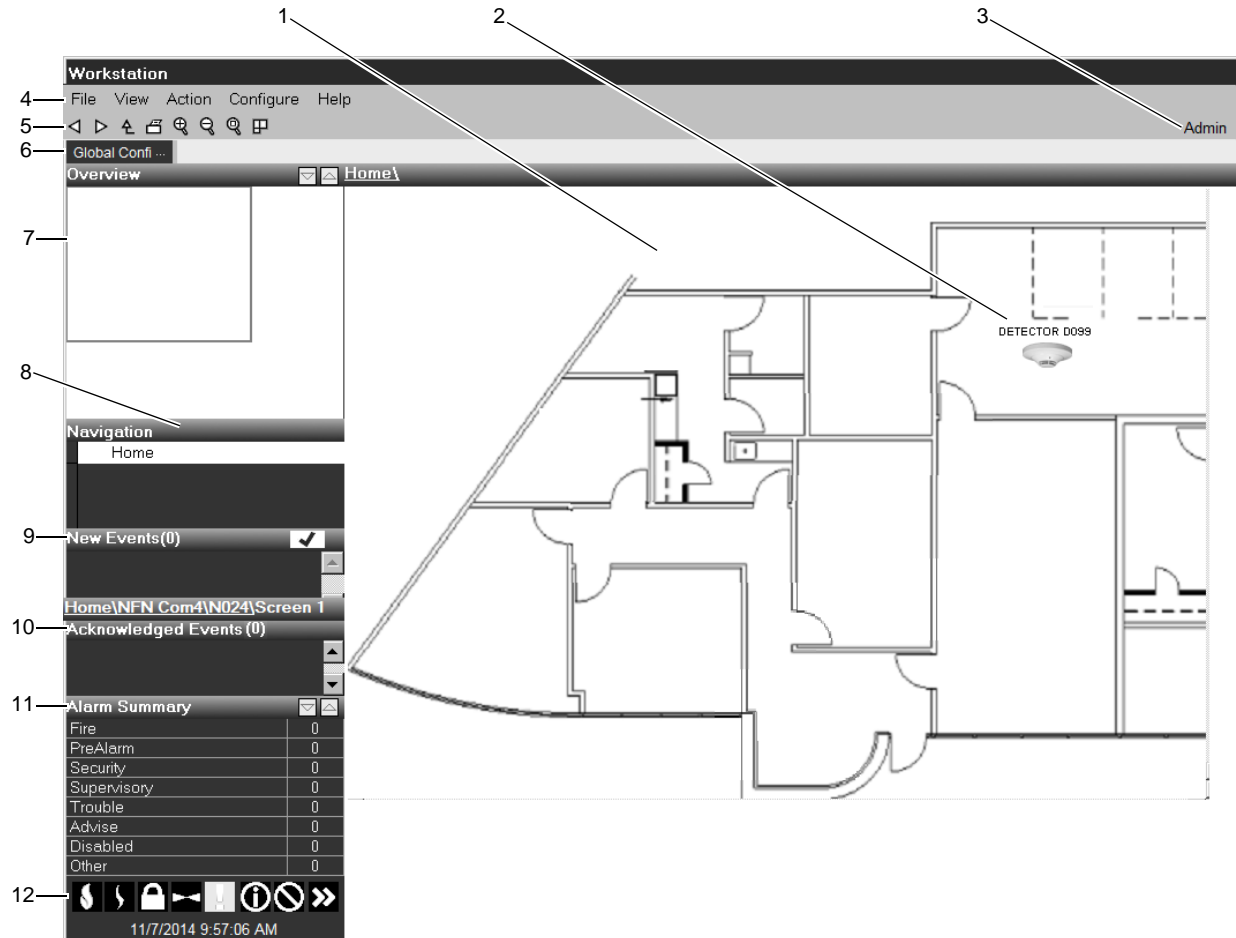











Figure 7.3 Graphics Display Screen Features

Table 7.1 Graphics Display Screen Descriptions

Item	Feature	Description
1	Floor Plan Window	The floor plan window usually displays a building floor plan as background and serves as the primary source for visual feedback. The floor plan window's title identifies which area of an system that is currently being displayed. The location of an off-normal event in an system which corresponds to the point's (device) location in a building.
2	Graphic Elements	Includes point icons (shown), navicons, and information labels that provide the user with important system information. Refer to 7.4, "Auto-creation of Screens, Nodes, and Points" for details.
3	Current User	Displays the name of the current user. Left-click the label to change users.
4	Menu Bar	<p>File:</p> <ul style="list-style-type: none"> • Login - Opens User Login dialog box where the user can log in/out, change users, etc. • Add History Entry - Opens Add History Entry dialog box where the user can manually add an entry into the system history file. • Print - Appears only if the workstation detects an installed Windows printer. Allows the user to print the workstation's Floor Plan Area display or local events list. • Exit - Click to exit the system application. <p>View:</p> <ul style="list-style-type: none"> • Text Mode/Graphics Mode - If not grayed-out, click to toggle between text and graphic display modes. Refer to 7.3.1, "Graphic Elements" for details. • History - Opens the History Manager window. • System - Opens the System Explorer window displaying a Windows-type navigation tree showing local system layout. • Search for Device - Opens the System Explorer window where the user can search for a particular device on the system. Click on the device label displays detailed information about the device. • Armed/Disarmed Points - Displays a list of all points with their control profile, status, and description. • Background Activations - Displays a list of non-event point activations occurring in the background. Used for informational/diagnostic purposes. • Walk Test Points - Displays a list of points currently being tested in walk test mode showing time/date, node label, type, network, status, and description. <p>Configure:</p> <ul style="list-style-type: none"> • Launch Configuration Tool - Opens the workstation configuration tool. • Control Profiles - Opens the Control Profile Configuration Window. • Monitoring Profiles - Opens the Monitoring Profile Configuration Window. • Options - Opens a window that allows the user to configure local workstation settings. • Backup and Clear History Database - Backs up and clears system history per the history settings made on the General Tab. <p>Help:</p> <ul style="list-style-type: none"> • About - Click to display system software application information.

Table 7.1 Graphics Display Screen Descriptions (Continued)

Item	Feature	Description
5	Tool Bar	<p> Previous Screen – Displays the floor plan that was viewed before the currently displayed floor plan.</p> <p> Next Screen – Displays the next floor plan below the current floor plan in the navigation tree hierarchy.</p> <p> Up One Level – Displays the next floor plan above the current floor plan in the navigation tree hierarchy.</p> <p> Print Current Screen – Prints the floor plan display to the currently selected printer.</p> <p> Zoom In One Level – Increases the zoom of the floor plan display by 50% (ranges from 100% to 3700%).</p> <p> Zoom Out One Level – Decreases the zoom of the floor plan display by 50% (ranges from 100% to 3700%).</p> <p> Zoom Full Image – Display current displayed floor plan at 100%.</p> <p> Show Floor Plan – Brings the floor plan display to the foreground, replacing any other open dialogs.</p>
6	Task Bar	Displays a link to each open system application.
7	Overview Window	Displays the user's location on the currently displayed workstation floor plan. A red rectangle indicates the area currently being viewed. The red rectangle can be clicked and dragged for repositioning the viewing area. This window is helpful when a zoom-in scale is selected for the workstation floor plan. The overview window does not display the graphic elements within it.
8	Navigation Tree	Displays the NFN system in a structured hierarchy form similar to Microsoft's Windows Explorer. Refer to 7.3.2, "Navigation Tree" .
9	New Events Pane	Displays list of newly reported events on the network. Events remain on the list until they have been acknowledged at the workstation. Events acknowledged at the fire panel remain on this list followed by an "Aked" notation until acknowledged at the workstation. Refer to 7.3.3, "New Events Pane" .
10	Acknowledged Events Pane	Displays a list of events acknowledged by the current user. Events remain on this list until the event is cleared.
11	Alarm Summary Pane	Displays a running total of new and acknowledged events by type and order of priority. This pane (hidden by default) is revealed by clicking on the up-arrow (△) adjacent to the Alarm Summary title.
12	Event Summary Icons	Click an icon to display a list of all the points currently in that state. Hover over the icon to displays its label. Click the Print button () to print alarm summaries. Refer to 7.3.4, "Event Summary Icons" .

7.3.1 Graphic Elements

7.3.1.1 Point Icons

Point icons represent a physical, addressable device on the system. Examples of point icons are fire panels and fire protection devices. The name of the point displays above the icon and if the point's status becomes off-normal, its icon flashes and information about its status is displayed below it.

Clicking on a point icon displays a box across the bottom of the workstation screen with detailed information and the current state of the associated point.

7.3.1.2 Navicons

Navicons represent a method to navigate between workstation floor plan areas to find points or an event. Each workstation floor plan area (parent) has one navicon that hyperlinks to each of its respective subordinate (child screen) workstation floor plan areas (refer to the Navigation Tree hierarchy). Navicons change color to match the off-normal event that is reported to the workstation. They are used to locate an event on parent or child screen; follow the same colored navicon to find an event.

7.3.1.3 Linked Media

Linked media provides important information during monitoring such as a photograph, text document, video, or a sound clip. Linked media is identified with an asterisk (*). One suggested use is to provide firefighters with an image of hazardous materials stored on-site.

7.3.1.4 Control Commands

Factory defined and Administrator assigned control commands are available for all point icons. They are accessed with right-clicks on its icon or navigation tree label.

Control commands are available only when you have a node control and security profile that allows it. Only one workstation can control any single system device at a given time. Taking control of a device removes control from the previous supervisor of that device. Default control commands are described in [Table 7.2](#).

7.3.1.5 Point Right-Click Choices to Respond to Events

Addressable devices have right-click menus that provide you with a list of device-specific choices used to control a device. The choices that appear in the menu depend on the type of device, the situation, and the user's security option permissions. An asterisk next to a choice indicates that another workstation has control of the device. A workstation must have control of the device in order to perform a command on it.

The following descriptions are provided for an overview of some right-click menu options:

- **<Point Description>** – Selecting the top line Device Description displays window which shows the devices provided description. This description may have been entered by the Admin User or the description was read from a panel on the system.
- **Enter User Response** – This choice displays a window with predefined User responses for reporting various conditions and operations related to the device. There is also a custom field for text-entry if a unique situation occurs. The selected response is logged to the history file.
- **History of Device** – Opens the History Manager window that displays the history information relating to the selected device.
- **View or Play: Text, Bitmap, Video, Audio** – Only if the device has an asterisk displayed adjacent to a choice, it has linked media and a choice will also display in the list of choices.
- **Zoom** – This choice allow the selection of various zoom levels and a return to the previous zoom level choice. When a zoom is selected, the zoom will center on the current mouse pointer location.

Table 7.2 Default Node/Point Control Commands

Command	Description
Enter User Response	<p>Allows the user to select from a list of default or user-created responses. These options provide the user the means to report various conditions and operations related to a node/point. Default responses are as follows:</p> <ul style="list-style-type: none"> • Dispatched Personnel To Investigate • Response Personnel on Scene • Device Undergoing Test • Device Testing Completed • Contacted System Contractor • Faulty Device • Replaced Device • Preventative Maintenance
History Of Device	<p>Only displays the history information in the History Manager window for the selected node/point.</p>
Linked Media	<p>Accesses any media that has been created and then assigned to the node/point. Several types of media files may be linked to the node/point. One of each type can be used.</p> <ul style="list-style-type: none"> • A text file to give specific information or instructions to the User (.TXT). • A raster image type graphic can be linked (.BMP). • A sound file may be linked giving audible information or instructions (.WAV). • A video file may be linked (.AVI).

7.3.2 Navigation Tree

The navigation tree displays the NFN system in a structured hierarchy form. Figure 7.4 describes navigation tree features.



Item	Feature	Description
1	Window Title	Describes the hierarchy levels displayed in the floor plan window.
2	Expand/Contract Buttons	Click to expand ▾ and collapse ▴ the pane.
3	Level Indicator Box	Click “-” to collapse the level and its child screens.
4	Node Label	Double-click to display the nodes devices location on the floor plan.
5	Level Indicator Box	Click “+” to expand the level and view its child screens.
6	Pane Boundary	Click, hold, and drag to change the pane size.

Figure 7.4 Navigation Tree Overview

7.3.3 New Events Pane

When an event is reported to the workstation, it displays the event information in the New Events pane and sounds an audible alarm at the workstation. The workstation auto-navigates to the floor plan window that has the highest priority event.

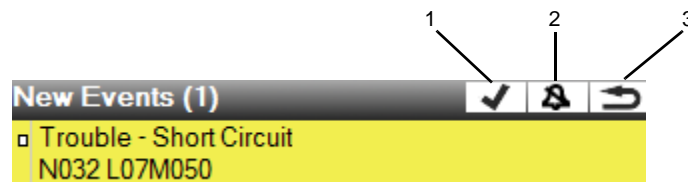
New events are events that have been reported to, and received by the workstation but not yet acknowledged by the user. Once an event is acknowledged, the event either moves to the Acknowledged Events window or is removed from the workstation.

The following may occur when new events are received:

- If the event is acknowledged at the panel, “Acked” will be displayed prefixing the event in the New Events list.
- If the workstation has node control of the point, a colored box will display to the left of the event in the Navigation Tree.
- If the event is unreliable (meaning it was reported while a gateway or node was in fault), an asterisk (*) will be displayed prefixing the event in the New Events list.

7.3.3.1 New Events Buttons

The alarm acknowledge button (✓) is available to all users and is displayed next to the New Events pane title. If the workstation is configured for protected premises operating mode, then the silence and reset buttons are also available. [Figure 7.5](#) describes the buttons available.



Item	Feature	Description
1	Alarm Acknowledge Button	Acknowledges the event.
2	Alarm Silence Button	Silences all audible alarms.
3	Reset Button	Sends reset command to the panels.

Figure 7.5 Normal Acknowledge, Silence, and Reset

7.3.4 Event Summary Icons

The event summary icons (while always visible) display in a highlighted, priority related color when an event is reported to the workstation. The affected icon remains highlighted until all off-normal conditions have been resolved. Hovering the cursor over the icon displays its label. Clicking on the icon displays the following information:

- **Fire** - Events issued by fire protection related devices such as pull-stations, smoke detectors, and sprinkler systems.
- **PreAlarm** - Events that indicate that a point is close to declaring an alarm, giving the facility manager opportunity to address the problem before an emergency develops.
- **Security** - Events issued by security related devices such as motion detectors, glass break detectors, and door contacts.
- **Supervisory** - Alarms that are special alarms to indicate action that has functionally disabled a key device (for either fire protection or security). An example of this is the event generated if the water valve is shut off for a sprinkler system.
- **Trouble** - Events that indicate a functional problem with a device on the network. Examples of trouble events include a device or workstation going off-line, a battery low or no power event, a dirty head on a smoke detector, etc.
- **Advise** - A condition that is an administrative event, internal to the NFN system. This is not a life-safety or security event, but an internal warning of a condition that may need attention, such as the history file reaching 100,000 entries.
- **Other** - Other event types such as disabled points on the system.

7.4 Auto-creation of Screens, Nodes, and Points

7.4.1 Overview

The auto-creation process of the workstation software application accomplishes the following:

- Creates a parent screen for the gateway (1), a child screen for the node (2), and a child screen under that (3) for the points for that node in a navigation tree format (see [Figure 7.6](#)).
- Places up to 64 point icons on a workstation screen before it creates the next screen.

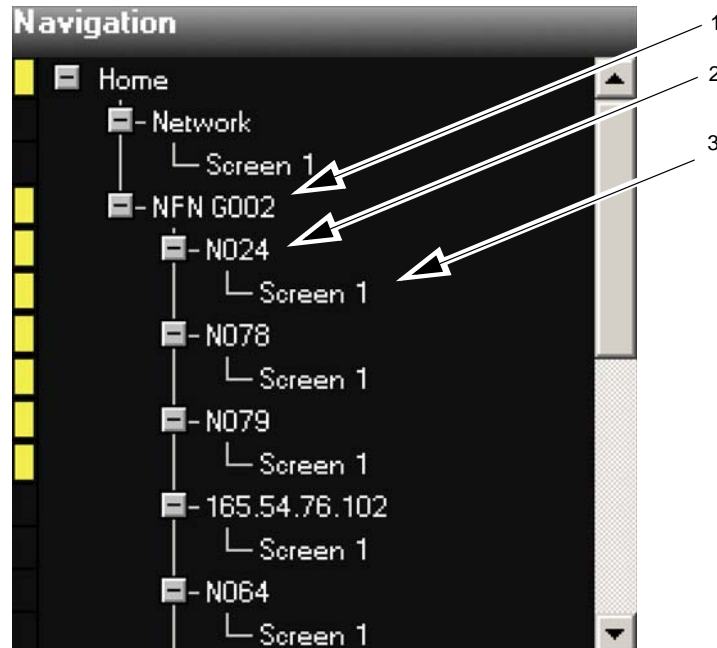


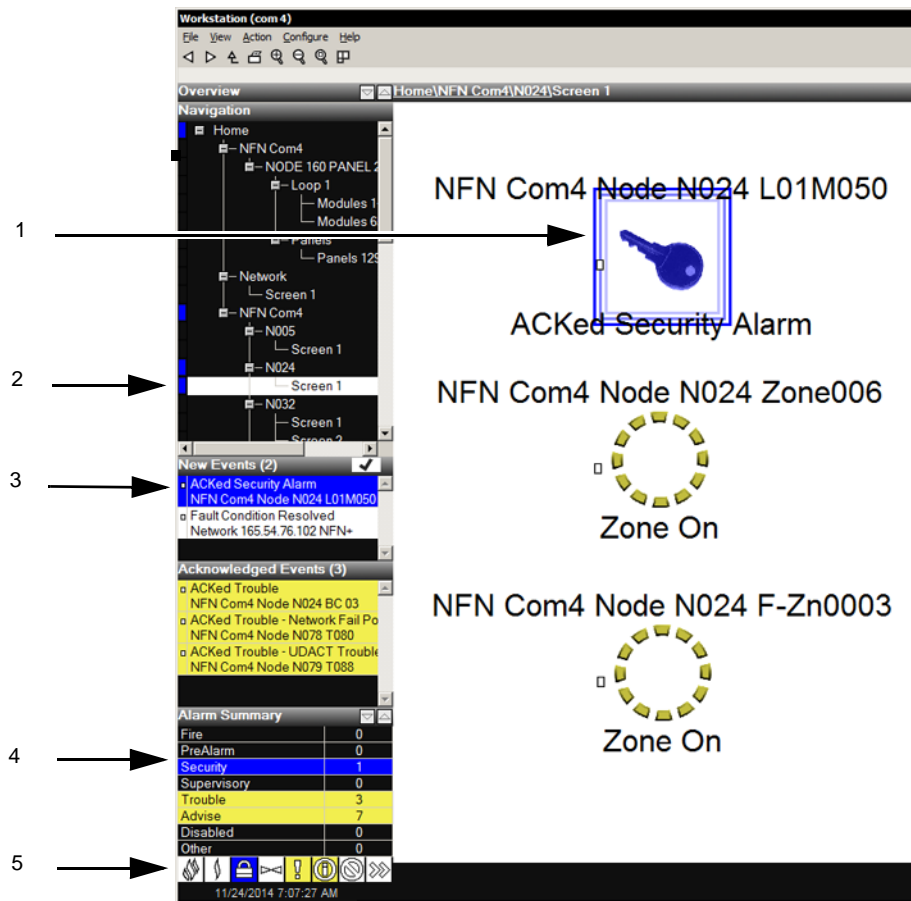
Figure 7.6 Example of Autocreated Navigation Tree

7.5 Interpreting Events on the Workstation's User Interface

7.5.1 When a New Event Occurs

When an event is reported to the workstation, the following actions simultaneously occur (see Figure 7.7):

- The workstation displays the floor plan area with the icon of the device in alarm displayed in its priority color. The software attempts to center the point icon in the window. An animated box around an icon indicates this is the highest priority event. Clicking the icon displays a window across the bottom of the screen with details about the point. The window's title bar is color coded based on the current state of the associated icon.
- In the Navigation Tree, a colored box displays adjacent to the level(s) with the event(s). Priority of the event(s) is displayed by color (red for fire, blue for security, yellow for trouble, etc.).
- In the New Events window, the event is added to a list.
- In the Alarm Summary window, the alarm is added to its list.
- The corresponding alarm summary icon displays its priority color.
- A sound is emitted indicating the event.



Item	Description
1	Device Icon in Alarm - Animation Indicates Highest Priority.
2	Event Priority Color Box
3	Event Added to New Events List
4	Alarm added to Alarm Summary List
5	Alarm Summary Icon Displays Priority Color

Figure 7.7 Example - New Event in Progress

Section 8 Data Management

8.1 Database Management


Several database management procedures are available for working with fire system data. Administrators can access these procedures by right clicking the PC Monitor icon () in the Windows system tray, and then selecting one of the options listed in the following table.

Table 8.1 Database Management Options

Option	Description
Compact & Repair System Data	This operation recovers dead space in the database, and reconstructs the index file. CAUTION: To avoid data loss, do not perform this operation unless instructed to do so by Technical Services.
Backup System Data	Upon initiating this procedure, the user must select or create a folder (C:\Facilities Monitoring 3.0\Backup is the default) and a “.dat” file that is used to identify the backup. In most situations, it is most practical to back up the fire system database to the default folder, using the same “.dat” file, after each editing session and then archive to a CD. The workstation has a CD-RW drive. CAUTION: If a second backup file is saved to an existing backup folder, both “.dat” files remain, but the newer backup overwrites the data for the existing one. Do not save backup system data to a folder which contains existing backup data that needs to be saved.
Restore System Data	This procedure is only available when all fire system applications, except PC Monitor, are shut down. This workstation command provides the Administrator with the option to restore a database created with the Backup System Data command. The operation prompts the user to select the location and folder in which the system data is to be stored.
Import System Data	Does not apply.
Export System Data To All Workstations	Does not apply.

8.2 History Manager

History Manager is an application program interface for viewing all of the events that are currently stored in the history database of a network client application. It serves as a viewer that can organize all events that pass through the workstation software application. It allows a set of filters to be applied to the events in order to view specific event types, points, and events for specific dates.

History Manager is accessed by clicking **View > History** within a network client (such as the workstation), or it can be started from outside the application environment from **Start > Programs > Facilities Monitoring > History Manager**.

At the top of the window are File, View and Filter menus (see [Figure 8.1](#)). Below that are the record viewer tabs (Event, Point, Screen, and Statistics) if they are enabled. The information bar at the bottom of the window displays the number of entries in the database, which events are being shown, the date and current time.

The lists of events:

- Are displayed according to any applied filters.
- Can be the current history file or an archived history file.
- Displayed depends on what specific application provided the database.

The screenshot shows the History Manager window for device F-Zn0001. The main display area shows a table of events with the following columns: ACK, Received Time Local, Status, and Action Description. The events listed are:

ACK	Received Time Local	Status	Action Description
<input checked="" type="checkbox"/>	10/31/2014 11:10:22 PM	Zone Off	
<input type="checkbox"/>	10/31/2014 11:08:55 PM	Trouble Restored	
<input type="checkbox"/>	10/31/2014 11:08:55 PM	Trouble	
<input type="checkbox"/>	10/31/2014 11:08:55 PM	Trouble	
<input type="checkbox"/>	10/31/2014 11:08:37 PM	Trouble Restored	
<input type="checkbox"/>	10/31/2014 11:08:39 PM	Zone On	
<input type="checkbox"/>	10/31/2014 11:08:37 PM	Trouble	
<input type="checkbox"/>	10/31/2014 11:08:37 PM	Trouble	
<input type="checkbox"/>	10/30/2014 2:08:57 PM		User Admin logged in.
<input type="checkbox"/>	10/30/2014 2:07:27 PM		User Logged Out logged in.
<input type="checkbox"/>	10/29/2014 12:08:27 PM	Fault Condition Resolved	
<input type="checkbox"/>	10/29/2014 12:08:27 PM	Fault Condition	
<input type="checkbox"/>	10/29/2014 12:08:21 PM	Advise	
<input type="checkbox"/>	10/29/2014 12:08:21 PM	Advise	
<input type="checkbox"/>	10/29/2014 12:08:27 PM		User Admin logged in.
<input type="checkbox"/>	10/29/2014 12:08:26 PM		Loading new system configuration. F
<input type="checkbox"/>	10/29/2014 12:06:30 PM		User Admin logged in.
<input type="checkbox"/>	10/29/2014 12:05:13 PM	Fault Condition Resolved	
<input type="checkbox"/>	10/29/2014 12:05:13 PM	Fault Condition	
<input type="checkbox"/>	10/29/2014 12:05:14 PM	Advise	

Figure 8.1 History Manager Screen

8.2.1 Menu Bar

Menus located on the History Manager menu bar are defined in [Table 8.2](#).

Table 8.2 History Manager Menus

Menu	Description
File	<ul style="list-style-type: none"> • Open Database - Open a previously saved event history database. • Export to Delimited Text -Name and create a comma delimited (.csv) file listing the events in the history list. • Print Displayed Records - Opens a print dialogue which allows printing of the records displayed by the history manager. Note: To cancel a print job, right-click the printer icon that appears in the Windows taskbar and select Cancel Print Job or cancel the job at the local printer.
View	<ul style="list-style-type: none"> • Refresh - Refreshes the event list to include the most recent events received. • System - Opens a System view window that shows how the events displayed by the history manager are distributed over the fire system. This view option is only available when the Event Grid view is displayed. • Event Grid - From within the System view window's View menu, click to display the Event Grid view. • Select Columns To Show - Opens a dialog from which the user can select which informational columns appear in the event list. • Show All Columns - Displays all columns. (Clicking the option also automatically checks all the boxes in the Select Columns To Show dialog.) • Resize All Columns - Automatically resizes all displayed columns to the width of either the column heading or the longest entry of any cell in the column, whichever is wider. • Record Viewer - Toggles display of the record viewer tabs. With the record viewer tabs displayed, click an item from the event list to select it, and then click a record viewer tab (Event, Point, Screen, or Statistics) to view that type of information about the selected event. • Filters - Toggles display of the filter pane on the left side of the event list providing more horizontal space for the event list. Note: Hiding the filter pane does not hide any events. • Display Labels - Select whether nodes displayed in the System view are labeled with their alias or with their network address. • Time - Select whether the times displayed are Received Time Local, Actual Time Local, or Actual Time UTC (Coordinated Universal Time). Selecting Time/Date constraints on the events displayed (in the System view) shows only events that fall within the specified time range as calculated by the selected time scheme.
Filter	<p>The Filter menu is not available in System view. However, the options in the Event Type, Time/Date, and View panes on the left side of the System view, used with the Update button below them, allow filtering of the events shown.</p> <ul style="list-style-type: none"> • Save Current Query - Saves the current query for later use. The current query is shown under the Applied Filters heading in the pane to the left of the event grid. The information shown there is a summary of the settings chosen under the General and Location headings in the pane to the left of the event grid. Note: To use an already-saved query, select the query name from the drop down list under the Queries heading in the pane to the left of the event grid. • Clear All Filters - Removes all filters and shows all recorded events in the event grid. • Rename Selected Query - Renames the selected query. • Delete Selected Query - Deletes the selected query.

8.2.2 Header and Row Display Options

8.2.2.1 Header Options

The options listed in [Table 8.3](#) can be accessed by right-clicking the column headings in the main body of the History Manager window. These options organize the information in the database columns for easier viewing.

Table 8.3 History Manager Header Options

Option	Description
Right-click on a header to display the following options:	
Hide Column	Temporarily hides the selected data column. The column itself is not deleted, only hidden.
Select Columns to Show	Opens a dialog box that allows the user to select the columns that are displayed.
Show All Columns	Removes all previously applied column data filters so that all columns display.
Resize Column	Resizes the width of the selected column such that any hidden text is displayed.
Resize All Columns	Resizes the width of all displayed columns such that any hidden text is displayed.
Left-click on a header to do the following:	
Sort Ascending/Descending	Toggles between sorting the column data in ascending or descending order (numeric or alphabetical).

8.2.2.2 Row Filter Options

The filter options listed in [Table 8.4](#) can be accessed by right-clicking any row in the main body of the History Manager window.

Table 8.4 History Manager Row Options

Option	Description
Filter By Selection	Allows the Administrator to display all records according to the event and column that was right-clicked on.
Filter Excluding Selection	Allows the Administrator to exclude displaying all records according to the event and the column that was right-clicked on.
Filter For	Displays a dialog box which allows the Administrator to filter for a specific word or phrase using keywords and/or the wild card character (%).
Clear All Filters	Allows the Administrator to return the History Manager window to the factory default filters. Once this option has been chosen, all filters are lost unless they were saved using the "Save Current Query" command.
Show If Greater Than Or Equal To	Only displays when time-related data in a row is selected. Allows event filtering by the data in the Received Time Local column. Only events occurring at the same time and <i>after</i> the selected event are displayed.
Show If Less Than Or Equal To	Only displays when time-related data in a row is selected. Allows event filtering by the data in the Received Time Local column. Only events occurring at the same time and <i>before</i> the selected event are displayed.

8.3 System Explorer Searches

The System Explorer can conduct a generic text search for system devices as follows:

1. Click **View > System**. The System Explorer window opens.
2. Enter the search text.
3. Click **Search**. The results appear in the pane on the right.
4. Click **OK** to close the System Explorer window.

8.4 Key Upgrade Utility

8.4.1 Overview

Every workstation is shipped with an internal USB key. This key is programmed to allow features of the network monitoring system to function on that workstation. A USB key upgrade is required when a new feature is desired. You must acquire an upgrade code from Technical Services to update the key.

8.4.2 Upgrade Procedure

Upgrade the USB key as follows:

1. Shut down the workstation software application.
2. Select **Start >Facilities Monitoring >Key Upgrade Utility**. The Key Upgrade Utility window displays.
3. Type the code into the Upgrade Code field.
4. Click on the Perform Upgrade button. Fields on the window update to reflect the upgrade code.
5. Click **Done** to complete the upgrade and close the window.

8.4.3 Key Upgrade Utility Field Descriptions

Refer to the following table for descriptions of the fields in the Key Upgrade Utility:

Table 8.5 Upgrade Utility Fields

Field	Description
Installation Name	This is typically a default site name. It is not recommended, but the name can be changed by typing a new name into the field.
Registered	This is typically a default site name. It is not recommended, but the name can be changed by typing a new entry into the field.
Node License	Shows how many node licenses are included with the current key configuration.
Serial #	Displays the serial number of the USB key (different from the authorization code).

Section 9 System Architecture

9.1 Overview

An example system architecture is described in the figure below.

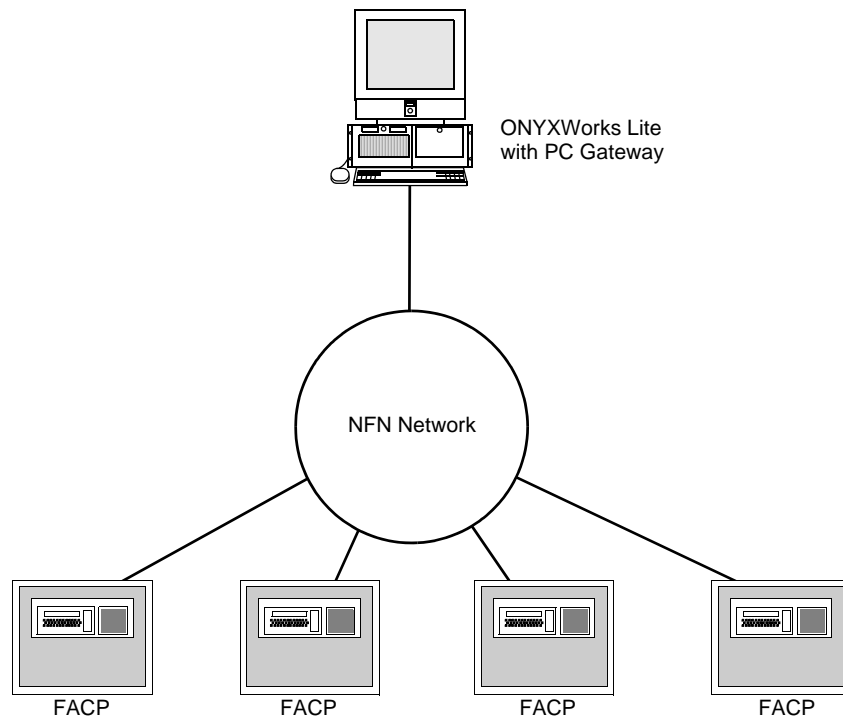


Figure 9.1 ONYXWorks Lite Network

Manufacturer Warranties and Limitation of Liability

Manufacturer Warranties. Subject to the limitations set forth herein, Manufacturer warrants that the Products manufactured by it in its Northford, Connecticut facility and sold by it to its authorized Distributors shall be free, under normal use and service, from defects in material and workmanship for a period of thirty six months (36) months from the date of manufacture (effective Jan. 1, 2009). The Products manufactured and sold by Manufacturer are date stamped at the time of production. Manufacturer does not warrant Products that are not manufactured by it in its Northford, Connecticut facility but assigns to its Distributor, to the extent possible, any warranty offered by the manufacturer of such product. This warranty shall be void if a Product is altered, serviced or repaired by anyone other than Manufacturer or its authorized Distributors. This warranty shall also be void if there is a failure to maintain the Products and the systems in which they operate in proper working conditions.

MANUFACTURER MAKES NO FURTHER WARRANTIES, AND DISCLAIMS ANY AND ALL OTHER WARRANTIES, EITHER EXPRESSED OR IMPLIED, WITH RESPECT TO THE PRODUCTS, TRADEMARKS, PROGRAMS AND SERVICES RENDERED BY MANUFACTURER INCLUDING WITHOUT LIMITATION, INFRINGEMENT, TITLE, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. MANUFACTURER SHALL NOT BE LIABLE FOR ANY PERSONAL INJURY OR DEATH WHICH MAY ARISE IN THE COURSE OF, OR AS A RESULT OF, PERSONAL, COMMERCIAL OR INDUSTRIAL USES OF ITS PRODUCTS.

This document constitutes the only warranty made by Manufacturer with respect to its products and replaces all previous warranties and is the only warranty made by Manufacturer. No increase or alteration, written or verbal, of the obligation of this warranty is authorized. Manufacturer does not represent that its products will prevent any loss by fire or otherwise.

Warranty Claims. Manufacturer shall replace or repair, at Manufacturer's discretion, each part returned by its authorized Distributor and acknowledged by Manufacturer to be defective, provided that such part shall have been returned to Manufacturer with all charges prepaid and the authorized Distributor has completed Manufacturer's Return Material Authorization form. The replacement part shall come from Manufacturer's stock and may be new or refurbished. THE FOREGOING IS DISTRIBUTOR'S SOLE AND EXCLUSIVE REMEDY IN THE EVENT OF A WARRANTY CLAIM.

Warn-HL-08-2009.fm



World Headquarters
12 Clintonville Road
Northford, CT 06472-1610 USA
203-484-7161
fax 203-484-7118

www.notifier.com

ISO 9001
CERTIFIED
ENGINEERING & MANUFACTURING
QUALITY SYSTEMS