NOTIFIER®
by Honeywell

Workstation

ONYXWORKS-WS

Installation and Operation Manual

Document LS10050-000NF-E Rev: R
5/6/2022 ECN: 14593

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 current edition 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.

Alarm Signaling Communications:

- **IP connections** rely on available bandwidth, which could be limited if the network is shared by multiple users or if ISP policies impose restrictions on the amount of data transmitted. Service packages must be carefully chosen to ensure that alarm signals will always have available bandwidth. Outages by the ISP for maintenance and upgrades may also inhibit alarm signals. For added protection, a backup cellular connection is recommended.
- **Cellular connections** rely on a strong signal. Signal strength can be adversely affected by the network coverage of the cellular carrier, objects and structural barriers at the installation location. Utilize a cellular carrier that has reliable network coverage where the alarm system is installed. For added protection, utilize an external antenna to boost the signal.
- **Telephone lines** needed to transmit alarm signals from a premise to a central monitoring station may be out of service or temporarily disabled. For added protection against telephone line failure, backup alarm signaling connections 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 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-F-2020

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. 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 manuals are read and understood.

CAUTION - System Re-acceptance 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. Re-acceptance 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 0-49º C/ 32-120º 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 its peripherals be installed in an environment with a normal room temperature of 15-27º C/60-80º 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 interference, 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 Department 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, or 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.

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.

Units with a touchscreen display should be cleaned with a dry, clean, lint free/microfiber cloth. If additional cleaning is required, apply a small amount of Isopropyl alcohol to the cloth and wipe clean. Do not use detergents, solvents, or water for cleaning. Do not spray liquid directly onto the display.

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.

Precau-D2-11-2017

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 radioelectriques 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™**, and **NOTI•FIRE•NET™** are all trademarks; and **Acclimate® Plus™**, **FlashScan®**, **FAAST Fire Alarm Aspiration Sensing Technology®**, **Honeywell®**, **Intelligent FAAST®**, **NOTIFIER®**, **ONYX®**, **ONYXWorks®**, **SWIFT®**, **VeriFire®**, and **VIEW®** are all registered trademarks of Honeywell International Inc. **Microsoft®** and **Windows®** are registered trademarks of the Microsoft Corporation. **Chrome™** and **Google™** are trademarks of Google Inc.

© 2022 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 online Help or printed manuals, you can email us.

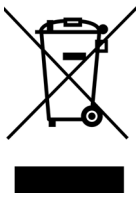
Please include the following information:

- Product name and version number (if applicable)
- Printed manual or online Help
- Topic Title (for online Help)
- Page number (for printed manual)
- Brief description of content you think should be improved or corrected
- Your suggestion for how to correct/improve documentation

Send email messages to:

FireSystems.TechPubs@honeywell.com

Please note this email address is for documentation feedback only. If you have any technical issues, please contact Technical Services.



This symbol (shown left) on the product(s) and / or accompanying documents means that used electrical and electronic products should not be mixed with general household waste. For proper treatment, recovery and recycling, contact your local authorities or dealer and ask for the correct method of disposal.

Electrical and electronic equipment contains materials, parts and substances, which can be dangerous to the environment and harmful to human health if the waste of electrical and electronic equipment (WEEE) is not disposed of correctly.

Table of Contents

Section 1 Product Overview 10
1.1: Operation 10
1.1.1: Smoke Control Feature 10
1.2: Functionality 10
1.2.1: Functions 10
1.2.2: Limitations 11
Table 1.1 Limitations 11
1.3: Recommended Cybersecurity Practices 11
1.4: Antivirus Software 11
1.5: Environmental Requirements 11
1.6: Printer Overview 11
1.6.1: Graphics Printer 11
1.6.2: Local Event Printer 11
1.6.2.1: Configuring an RS-232 Connection 12
1.6.2.2: Installing the Printer Driver 12
1.7: IP Requirements 12
1.7.1: IP Port Settings 12
Table 1.2 IP Port Settings 12
1.7.2: Bandwidth Usage 13
Table 1.3 Bandwidth Usage 13
1.7.3: IP Restrictions 13
1.8: Agency Listings 14
1.8.1: Standards 14
1.8.2: Agency Restrictions and Limitations 15
1.9: Software Security 15
1.9.1: Windows Control/Command Key Lockouts 15
1.9.2: User Security Options 15
Table 1.4 Basic PC Functionality 15
Table 1.5 Canada User Permissions and Settings 16
1.10: UL 2572 Security Levels 16
Table 1.6 Security Levels 16
1.11: Field Programmable Settings 16
Table 1.7 UL 864 Field-programmable Settings 16
Table 1.8 UL 2572 Field-programmable Settings 17
Table 1.9 CAN/ULC S527 Field-programmable Settings 17
1.12: Compatible Equipment 18
1.12.1: Current Compatible Equipment 18
Table 1.10 Compatible Equipment 18
1.12.2: Compatible 8th Edition Fire Panels 18
1.12.3: Legacy Compatible Equipment 19
Table 1.11 Legacy Compatible Equipment 19
1.13: System Configuration 19
Table 1.12 System Configuration 19

Section 2 Hardware Configuration 20
2.1: System Power 20
2.1.1: Primary and Secondary Power 20
2.1.2: System Power Requirements 20
Table 2.1 System Power Requirements 20
2.1.3: Safety 20
2.1.4: Motherboard Battery 20
2.2: Connections 20
2.2.1: Component Connections 20
Figure 2.1 Computer Component Connections 20
Table 2.2 Connection Specifications 21
2.2.2: Network (LAN) Connection 22
Figure 2.2 Single LAN Connection 22
Figure 2.3 Dual LAN Connection 22
Figure 2.4 Stand-alone ONYXWORKS-WS 22
2.2.3: AC Power Connection 23
2.2.4: Wiring Methods 23
2.3: UPS Installation 24

2.4: Testing and Maintenance 24
2.4.1: Testing 24
2.4.2: Maintenance 24
Section 3 Workstation License Activation 25
3.1: License Activation Procedure 25
Figure 3.1 License Manager Layout 25
Section 4 Configuration Tool Settings 27
4.1: Overview 27
4.2: Initial Administrator Login 27
4.2.1: New Workstation 27
4.2.2: Existing Workstation after Software Upgrade 27
4.3: User Profiles and Passwords 27
4.4: Configuration Tool 27
4.4.1: Overview 27
4.4.2: Launching and Exiting the Configuration Tool 28
Table 4.1 Configuration Tool Start Options in Windows 28
4.4.3: Configuration Tool Layout 29
Figure 4.1 Configuration Tool Floor Plan Editor Screen Features 29
4.4.4: Configuration Tool Menus 30
Table 4.2 Configuration Tool Menus and Floor Plan Toolbar Settings 30
4.4.5: Macros 31
4.4.6: Control Profiles 31
4.4.7: Networks 31
4.4.7.1: Importing Network Configuration Data 31
4.4.7.2: Adding a Network 32
4.4.7.3: Adding Nodes to a Network 32
4.4.7.4: Migrating Nodes 32
4.4.7.5: Deleting Networks and Nodes 32
4.4.8: Monitoring Profiles 32
4.4.9: System Options 33
Table 4.3 System Options Configuration 33
Section 5 Workstation Settings 35
5.1: Windows Settings 35
Table 5.1 Windows Settings 35
5.1.1: Disabling Automatic Updates - Windows 10 Professional 35
5.1.2: Manual Windows Updates 35
5.2: Workstation Mouse Click vs. Screen Touch Equivalents 35
Table 5.2 Click vs. Touch Equivalents 35
5.3: System Options Settings 36
5.3.1: General Tab 36
Table 5.3 General Tab Settings 36
5.3.2: User Features Tab 38
Table 5.4 User Features Settings 38
5.3.3: Event Printer Tab 38
Table 5.5 Event Printer Tab Settings 38
5.3.4: Email Tab 39
Table 5.6 Email Tab Settings 39
5.3.5: Output Tab 41
Table 5.7 Output Tab Settings 41
5.3.6: Smoke Control Tab and Multi-Station Smoke Control Tab 41
Section 6 Operation 42
6.1: Overview 42
6.2: Starting and Exiting the Workstation Application 42
6.3: User Login and Log Out 42
6.3.1: Login 42
6.3.2: Switching Users 42
6.3.3: Logout 42
6.4: Workstation Screen Layout 43
Figure 6.1 Example Workstation Screen 43
Table 6.1 Workstation Screen Descriptions 44
6.4.1: Workstation Menus 45

Table 6.2 Configuration Tool Settings....45
6.4.2: Graphic Elements....47
Table 6.3 Graphic Element Descriptions....47
6.4.2.1: Linked Media....47
6.4.2.2: Point Right-Click Command Options....48
Table 6.4 Default Node/Point Right-Click Options....48
6.4.3: Navigation Pane....49
Figure 6.2 Navigation Pane Overview....49
6.4.4: Events Panes....50
Figure 6.3 Event Pane Features....50
6.4.4.1: New Events Pane....50
6.4.4.2: New Events Buttons and Indicators....51
Table 6.5 New Events Buttons and Indicator Definition....51
6.4.5: Event Status Class Icons....53
Table 6.6 Event Status Class Icon Definition....53
6.5: Repositioning Windows....54
6.5.1: Overview....54
6.5.2: Using the Docking Guide....54
Figure 6.4 Window Docking Guide....54
6.6: When a New Event Occurs....55
Figure 6.5 Example - Fire Event in Progress (PPCU Mode)....55
6.7: Look-Ahead Enable Feature....56
Table 6.7 Look-Ahead Enable....56
Section 7 Data Management....57
7.1: Workstation Database Backup and Restore....57
7.1.1: Backing Up the Database....57
7.1.2: Restoring a Backed-Up Database....57
7.2: History Window....57
7.2.1: Overview....57
7.2.2: Back-up History Database....57
7.2.3: Viewing the History Window....57
7.2.4: Event Grid Screen....58
Figure 7.1 Event Grid Screen....58
Table 7.1 Event Grid Screen Features....58
Table 7.2 Event Grid Screen Menus....60
Table 7.3 Event Grid Column and Row Options....61
7.2.5: Creating, Renaming, and Deleting Queries....61
7.2.6: System View Screen....62
Figure 7.2 System View Screen....62
Table 7.4 System View Screen Features....63
7.3: System Explorer Searches....63
7.4: Walk Test Utility....64
7.4.1: Overview....64
7.4.2: Walk Test Procedure....64
Figure 7.3 Walk Test Screen....64
Table 7.5 Walk Test Options....65
Table 7.6 Walk Test in Progress - Button Definitions....65
7.4.3: Walk Test Points List....66
7.4.3.1: Overview....66
7.4.3.2: Features....66
Figure 7.4 Walk Test Points List Features....66
Table 7.7 Walk Test List Right-Click Data Filter Options....66
7.5: Test Monitoring....67
7.5.1: Test Monitoring Setup....68
Figure 7.5 Test Monitoring Configuration Window....68
7.5.2: Viewing Test Monitoring Event History....69
Figure 7.6 Test Monitoring Window....69
7.6: Security Log....70
Figure 7.7 Workstation Security Log....70
Section 8 System Architecture....71
8.1: Overview....71
Figure 8.1 Basic ONYXWorks System Example....71

Figure 8.2 Advanced ONYXWorks System Example 72
Figure 8.3 System with Redundant Gateway Example 73
8.2: Protected Premises Control Unit Overview 74
8.2.1: Architecture for Protected Premises Control Unit 74
Figure 8.4 Example Protected Premises Control Unit Life Safety System 74
8.2.2: Event Handling Overview for Protected Premises Control Unit 74
8.3: Proprietary Receiving Unit Overview 74
8.3.1: Architecture for Proprietary Receiving Unit 74
Figure 8.5 Proprietary Receiving Unit System - Example 1 75
Figure 8.6 Proprietary Receiving Unit System - Example 2 75
8.3.2: Overview of Event Handling for Proprietary Receiving Unit 76
8.4: Protected Premises Control Unit vs. Proprietary Receiving Unit Event Handling 76
Table 8.1 Protected Premises Control Unit vs. Proprietary Receiving Unit Comparison 76

Section 9 NetLogic 77

9.1: NetLogic Description 77
9.2: Changes in Fire System Database 77
9.3: Opening and Closing NetLogic 77
9.4: NetLogic Window 77
9.4.1: Conditions Tab 78
9.4.1.1: Conditions Tab Features 78
Figure 9.1 NetLogic Conditions Tab 78
Table 9.1 Conditions Tab Features 79
9.4.2: Conditions Grid 80
9.4.2.1: Overview 80
9.4.2.2: Conditions Grid Features 80
Figure 9.2 Conditions Grid Features 80
Table 9.2 Conditions Grid Definitions 80
9.4.2.3: Testing the Conditions 81
9.4.3: Actions Tab 82
Figure 9.3 NetLogic Actions Tab 82
Table 9.3 Actions Tab Features 82
Table 9.4 Action Elements 83
9.4.4: Logical Operators 84
Table 9.5 Boolean Logical Operators 84
9.4.5: Precedence Levels 84
9.5: NetLogic Entries in History Window 86
Table 9.6 NetLogic Entries in Workstation History 86
9.6: Troubleshooting Equations 86
Table 9.7 Troubleshooting Equations 86

Section 10 NOTIFY-IP 87

10.1: Operation 87
10.2: Functionality 87
10.2.1: System Functions 87
Table 10.1 System Parameters (General Paging) 87
Table 10.2 System Parameters (Mass Notification and Fire Paging) 88
10.3: Agency Listings 89
10.3.1: Standards 89
10.3.2: Agency Restrictions and Limitations 89
10.4: UL 2572 Security Levels 89
Table 10.3 Security Levels 89
10.5: Field Programmable Settings 89
Table 10.4 UL 2572 Field Programmable Settings - NOTIFY-IP 89
10.6: Compatible Equipment 90
10.6.1: Current Compatible Equipment 90
Table 10.5 Compatible Equipment 90
10.6.2: Legacy Compatible Equipment 90
Table 10.6 Legacy Compatible Equipment 90
10.7: System Configuration 91
Table 10.7 System Configuration 91
10.8: Power Requirements 91
10.9: Environmental Requirements 91
10.10: NOTIFY-IP System Architecture 91

10.10.1: Fire Network Only 91
10.10.2: Combination Fire and Mass Notification Network 91
10.11: Protected Premises Control Unit (PPCU) Mode Overview 92
10.11.1: Architecture for PPCU Mode 92
Figure 10.1 Example: NOTIFY-IP System Architecture (PPCU Mode) 92
10.11.2: PPCU Mode Agency Approval 92
10.12: Installation 92
10.12.1: Installing the Audio Supervision Card 92
10.12.2: Connecting the Cables 93
Figure 10.2 Sound Card and Audio Supervision Card Connections 93
10.12.3: Wiring Methods 93
10.13: Voice Paging License 93
10.14: Configuration 94
10.14.1: Microphone Sound Level Settings 94
10.14.2: Workstation Configuration Tool Settings 94
Table 10.8 Configuration Tool Settings for NOTIFY-IP 94
10.15: Audio Groups 95
10.15.1: Creating an Audio Group 95
10.15.2: Modifying an Audio Group 95
10.15.3: Creating Audio Buttons 95
10.15.4: Manipulating Audio Buttons 96
Table 10.9 Manipulating Audio Buttons 96
10.16: Voice Paging 96
10.16.1: Preparing to Page 96
10.16.2: Making a Live Page 97
10.16.3: Previewing the Live Page Before Broadcast 97
10.16.4: Making a Sequence Type Page 97
10.17: Paging Status Indicators 97
Table 10.10 Paging Status Indicators 97
10.18: Troubleshooting 98
10.18.1: Configuration Problems 98
10.18.1.1: Problems with Audio Point Selection 98
Table 10.11 Valid Audio Point Configurations 98
10.18.1.2: Missing Audio Points 98
10.18.2: Activation Problems 99
Table 10.12 Activation Problems 99
10.18.3: Problems Involving Group Types 99
10.18.4: Group Type Hierarchy 99

Appendix A Upgrades 100

A.1: Software Version 4 Upgrade Overview 100
A.2: Upgrade Decision Matrix 100
Table A.1 Software Upgrade Decision Matrix 100
A.3: Upgrading Systems with Echelon 101
A.4: Upgrading Systems with an Older PC and WS Software 3.X 101
A.5: Upgrading Systems with UL-listed PCs Purchased after January 2015 102
A.5.1: Overview 102
A.5.1.1: Prerequisites 102
A.5.1.2: Personnel - Information Transfer 102
A.5.2: Gathering Workstation Information 102
A.5.3: Recording Workstations in the CLSS Portal and Generating the License File 102
Figure A.1 Key Migrator Utility Window 103
A.5.4: Upgrading the License on the Workstation 104
A.5.4.1: Prerequisites 104
A.5.4.2: License Migration Procedure 104
Figure A.2 Key Migrator Window 104
A.5.5: Downloading the Workstation Software 104
A.5.6: Final Steps 105
Figure A.3 License Manager Layout 105
A.6: Upgrading Matrix v. 4.52 Workstation to v. 4.60 106

Section 1 Product Overview

1.1 Operation

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

When operating as a PRU, the ONYXWORKS-WS supports one or more gateways. The gateway(s) may run on the same PC as the ONYXWORKS-WS or they may run on other PCs and/or embedded hardware. The use of multiple gateways allows for redundancy and provides the ability to monitor multiple networks. One or more ONYXWORKS-WSs may be installed on a network. Multiple ONYXWORKS-WSs can be used to monitor a single network or a single ONYXWORKS-WS can monitor multiple networks. The ONYXWORKS-WS can be located at the protected premises or at a different location. The protected property may be contiguous or noncontiguous, but must be under one ownership.

When operating as a PPCU, support of gateways is limited to a single NFN Gateway that is installed and operating on the same PC as the ONYXWORKS-WS.

The ONYXWORKS-WS provides an optional graphic interface feature by which Administrator and Point Control privilege users can monitor and control the smoke control system for one or more buildings.

The ONYXWORKS-WS is hereinafter referred to as “the workstation”.

1.1.1 Smoke Control Feature

An optional smoke control feature is available for the workstation. This option allows users with Administrator and Point Control privileges to monitor and control smoke control systems in the monitored buildings. For detailed information about this option, refer to the *OW-SCS Configuration and Operation Manual* (LS10050-012NF-E).

1.2 Functionality

1.2.1 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 the following:
  - Life safety events
  - Security events
  - Smoke control system events (if licensed)
- Ability to silence, acknowledge, and reset all panels with off normal events when operating as a PPCU.
- Remote activate/deactivate of speakers and strobes when operating as a PPCU.
- Monitors the communications path between workstation and gateway.
- Annunciates a trouble event when communications with gateway is lost.
- Displays device location information.
- Annunciates CPU fan failure.
- Acts as a time server for gateways on the life safety network.
- Ability to send emails (see Table 1.1 for limitations).
- Displays an icon that when clicked, displays a list of the silenced fire panels.
- Monitors and controls building smoke control systems (if licensed).

NOTE: If the workstation is configured for use in a dedicated or non-dedicated smoke control system, refer to the *Smoke and HVAC Control Station SCS Series Operation and Installation Manual* (P/N 15712) for concepts and requirements for smoke control strategy and examples for implementing the system in various applications.

1.2.2 Limitations

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

Table 1.1 Limitations

Limit	Feature	Maximum Allowed
Physical Network Limit	Gateways	200 Total
	Workstations per System	50 Maximum
Logical Network & Screen	Screens	10,000
	Devices	250,000
	Devices Per Screen	1,000
	Macros	250
	Macro Buttons	2,000
	Navicons	1,000
	Monitoring Profiles	100
	Node Control Profiles	100
Workstation	Output Formats	25 per Workstation
	Email Recipients	10 per Workstation
	Email Recipients (MNS)	5 per Event
User Manager	Users	500

1.3 Recommended Cybersecurity Practices

Highly recommended cybersecurity practices for the workstation are specified in the *Cybersecurity Manual* (LS10217-000NF-E).

CAUTION: CYBERSECURITY RISK

FAILURE TO COMPLY WITH THE RECOMMENDED SECURITY PRACTICES MAY PLACE YOUR SYSTEM AT RISK.

1.4 Antivirus Software

Recommended and tested against McAfee™ Endpoint Security and Windows® Defender Antivirus.

1.5 Environmental Requirements

This product meets the following requirements for operation:

- Temperature - 0°C to 49°C (32°F - 120°F)
- Relative Humidity - 93 ±2% non-condensing at 32 ±2°C (90 ±3°F)

However, it is recommended that this product be installed in an environment with a normal room temperature of 15-27º C (60-80º F).

1.6 Printer Overview

The print option appears in the File menu only if the workstation detects a Windows-compatible printer has been installed. When a printer is initially added in Windows®, the workstation must be restarted so it can detect the printer.

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

1.6.1 Graphics Printer

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

1.6.2 Local Event Printer

The PRN-7 is an optional local event printer. It is a UL 864-listed, Windows-compatible, dot-matrix printer that prints workstation events.

A default output format and monitoring profile are preconfigured for a local event printer. It is necessary to enable the printer in Windows.

1.6.2.1 Configuring an RS-232 Connection

Configure the COM port used for an RS-232 connection as follows:

1. In Windows 10, click S**tart > Control Panel > Device Manager**. Alternatively, you can use the search feature to search for and then open Device Manager.
2. Double-click on **Ports (COM & LPT)** and double-click on the port to which the printer will be connected. A properties window displays.
3. On the Port Settings tab, verify the following settings:
   - Baud Rate: 9600
   - Data Bits: 8
   - Parity: None
   - Stop Bits: 1
   - Flow control: None
4. Click **OK**.
5. Close the Device Manager.

1.6.2.2 Installing the Printer Driver

Install the event printer driver as follows:

1. In the Control Panel, click **Start > Devices > Printers and Scanners**.
2. Click **Add a printer or scanner**. Windows performs a search and lists the available devices.
3. Click **The printer that I want isn't listed**.
4. Click **Add a local printer or network printer with manual settings**.
5. Select **Use an existing port** and select a COM port or, if listed, select **USB** (virtual Printer Port for USB) from the drop-down list.
6. Click **Next**.
7. Under Manufacturer, select **Generic**.
8. Under Printers, select **Generic/Text only** and click **Next**.
9. Enter **Local Event Printer** as the printer name and click **Next**.
10. Select **Do not share** and click **Next**.

Print a test page to verify the installation.

1.7 IP Requirements

1.7.1 IP Port Settings

The following IP ports must be available to the workstation:

Table 1.2 IP Port Settings

Port	Type	Direction	Purpose
25	TCP	Out	SMTP
123	UDP	In and Out	SNTP
2004	TCP	N/A	(Internal) Workstation Plug-in Access
2014	TCP	Out	Connection to DACR Gateway
2017	TCP	Out	Connection to NFN Gateway
2029	TCP	Out	Workstation Output Appliances (Signs)
4016	TCP	In	Database Import/Export

1.7.2 Bandwidth Usage

The worst-case sustained bandwidth values are described below:

Table 1.3 Bandwidth Usage

Worst Case Sustained Bandwidth	No. Gateways	Bandwidth
Typical	200	3,360 Bytes/Sec 26,800 bits/Sec 0.027 Mb/Sec (Approx.)
Maximum	200 + 50 Audio	617,580 Bytes/Sec 4,940,640 bits/sec 5 Mb/Sec (Approx.)

1.7.3 IP Restrictions

The following restrictions apply:

- Workstations cannot access gateways or other workstations through Network Address Translation or IP Masquerading.
- Must have a static IP address. DHCP is not supported.
- The use of a NAT is not supported.
- Multiple IP Addresses are not supported, either due to multiple enabled network adapters or due to a multi-homed adapter.

1.8 Agency Listings

1.8.1 Standards

■ **Compliance** - This product has been investigated to, and found to be in compliance with, the following standards:

National Fire Protection Association

- NFPA 92 Standard for Smoke Control Systems

Underwriters Laboratories

- UL 864 Control Units for Fire Alarm Systems, Tenth Edition
- UL 2017 General-Purpose Signaling Devices and Systems, Second Edition
- UL 2572 Mass Notification Systems, Second Edition
- UL 2610 Standard for Commercial Premises Security Alarm Units and Systems, Second Edition

Underwriters Laboratories Canada

- CAN/ULC S527-11 Standard for Control Units for Fire Alarm Systems, Third Edition
- CAN/ULC S559-13 Equipment for Fire Signal Receiving Centres and Systems, Second Edition

■ **Installation** - This product is intended to be installed in accordance with the following:

Local

- AHJ Authority Having Jurisdiction

National Fire Protection Association

- NFPA 70 National Electrical Code
- NFPA 72 National Fire Alarm and Signaling Code

Underwriters Laboratories

- UL 681 Standard for Installation and Classification of Burglar and Holdup Alarm Systems
- UL 2610 Standard for Commercial Premises Security Alarm Units and Systems, Second Edition

Underwriters Laboratories Canada

- CAN/ULC S524 Installation of Fire Alarm Systems
- CAN/ULC S561 Installation and Services for Fire Signal Receiving Centres and Systems

Canada

- CSA C22.1 Canadian Electrical Code, Part I, Safety Standard for Electrical Installations

1.8.2 Agency Restrictions and Limitations

- If the ONYXWORKS-WS or the transmitter is sharing on-premises communications equipment, the shared equipment shall be "listed for the purpose"; otherwise the transmitter must be installed ahead of the unlisted equipment. “Listed for the purpose” has been formally interpreted by NFPA (Formal Interpretation 72-99-1) for equipment on packet switched networks as being listed to the requirements applicable to general purpose communications network equipment.
- The ONYXWORKS-WS is UL listed only for monitoring when using an Ethernet connection for communications with a life safety network. The Ethernet connection can be part of, or connected to, a shared bandwidth network that operates over topologies such as an intranet, the Internet, or a frame relay.
- The ONYXWORKS-WS uses active communication for monitoring of devices. In Canada, infrastructure which involves LAN/WAN configurations may be used for monitoring of fire networks provided that a dedicated T-1 line is used and routers are battery backed with a power source capable of providing backup power for a period of 24 hours.
- The UL listing for the ONYXWORKS-WS includes the ability for the workstation to send emails. These emails are intended to be transmitted to a limited number of staff (refer to Table 1.1 for details) for maintenance purposes and system status reasons. This feature is approved by UL as supplementary.
- The ONYXWORKS-WS must be manned 24/7 by trained competent personnel.
- When operating as a Proprietary Receiving Unit, the ONYXWORKS-WS is UL listed only for monitoring of fire, smoke control, and mass notification devices.
- When operating as a Protected Premises Control Unit, the ONYXWORKS-WS is UL listed for monitoring and control of fire, smoke control, and mass notification devices.
- In Canada, when operating as a Proprietary Receiving Unit, the ONYXWORKS-WS is ULC listed only for monitoring of fire devices and must be configured in “Canada – Receiving Unit” mode.
- In Canada, when operating as a Protected Premises Control Unit, the ONYXWORKS-WS is ULC listed for monitoring and control of fire devices and must be configured in “Canada - Protected Premises Control Unit” mode or “Canada – Protected Premises Control Unit + DCC’’ (Display and Control Centre) mode.

1.9 Software Security

1.9.1 Windows Control/Command Key Lockouts

Workstation keyboard keys that are used to access Windows programs that are not part of the workstation software applications can be disabled. For example, keyboard key combinations used to shut-down or restart the workstation and for switching between software applications can be disabled. This is accomplished in the workstation application (**Menu > Help > Secure Windows**).

1.9.2 User Security Options

User accounts can be created with differing levels of access to the ONYXWorks® system. The user’s security option choice determines which functions are visible or selectable. Refer to the tables below for detailed information.

In Canada, user accounts with permissions must be granted in accordance with the following guidelines:

1. **Read Only:** The default setting with minimum permissions granted. This permission level is equivalent to no user logged in.
2. **Client Control:** Granted to persons having a general responsibility for safety supervision, who might be expected to investigate and initially respond to a fire alarm or trouble indication;
3. **Point Control:** Granted to persons who have a specific responsibility for safety and who are trained to operate the fire signal receiving center and systems;
4. **Administrator:** Granted to persons who are trained and authorized by the manufacturer to:
   a. Reconfigure the site specific data held within the fire signal receiving center and systems controlled by it; and
   b. Maintain the fire signal receiving center and systems in accordance with the manufacturer’s published instructions and data.

Table 1.4 Basic PC Functionality

Basic PC Functionality	Windows User Account Privileges	
	Limited User Account	Administrator Privileges Account
Run Workstation	YES	YES
Reset Operating System	NO	YES
Change PC Settings	NO	YES
Change/Install Software Programs	NO	YES
Change/Create Local PC User Accounts	NO	YES
Set Time and Date	NO	YES
Note: In Canada, the PC must be run with a Limited User Account.		

Table 1.5 Canada User Permissions and Settings

User Permissions	Accounts - Permissions Level			
	Read Only	Client Control	Point Control	Administrator
Print Events and Floor Plans	NO	YES	YES	YES
View History and Linked Media	YES	YES	YES	YES
Backup History Data	NO	YES	YES	YES
Acknowledge Events Locally	NO	YES	YES	YES
Acknowledge Field Events	NO	NO	YES	YES
Silence/Reset	NO	NO	YES	YES
Enable/Disable Points	NO	NO	YES	YES
Activate/Deactivate Points	NO	NO	YES	YES
Manual Evacuation	NO	NO	YES	YES
Change/Configure Site Specific Data	NO	NO	NO	YES
Change/Configure User Accounts	NO	NO	NO	YES
Change/Configure Software Options	NO	NO	NO	YES

1.10 UL 2572 Security Levels

The ONYXWORKS-WS meets the UL 2572 security levels stated below:

Table 1.6 Security Levels

Level Type	Level
Communication Security	1
Stored Data Security	0
Access Control Security	2
Physical Security	1
Audit Control Security	0

1.11 Field Programmable Settings

Table 1.7 UL 864 Field-programmable Settings

NOTICE TO USERS, INSTALLERS, AUTHORITIES HAVING JURISDICTION, AND OTHER INVOLVED PARTIES			
This product incorporates field-programmable software. In order for the product to comply with the requirements in the Standard for Control Units and Accessories for Fire Alarm Systems, UL 864, certain programming features or options must be limited to specific values or not used at all as indicated below.			
Program Feature or Option	**Permitted in UL 864 (Y/N)**	**Possible Settings**	**Settings Permitted in UL 864**
Remote resetting and silencing of a fire alarm control unit from other than the protected premises (ref: NFPA 72-2007 6.8.2.8)	No	Security Levels: • Administrator • User with Point Control • User with Client Control • Read Only	None
Block Acknowledge (PRU Mode Only)	No	• Yes • No	No
Use Node Control	No	• Yes • No	No
Enable NetLogic	No	• Yes • No	No
Alarm Reminders (Fire, CO, Supervisory, Trouble)	Yes	• Disable • 4 hours • 24 hours	• 4 hours • 24 hours

Table 1.8 UL 2572 Field-programmable Settings

NOTICE TO USERS, INSTALLERS, AUTHORITIES HAVING JURISDICTION, AND OTHER INVOLVED PARTIES			
This product incorporates field-programmable software. In order for the product to comply with the requirements in the Standard for Control Units and Accessories for Fire Alarm Systems, UL 2572 certain programming features or options must be limited to specific values or not used at all as indicated below.			
Program Feature or Option	**Permitted in UL 2572 (Y/N)**	**Possible Settings**	**Settings Permitted in UL 2572**
Inactivity Timeout	Yes	0 - 20 minutes (0 disables feature)	1 - 20 minutes
Alarm Reminders (Fire, CO, Supervisory, Trouble)	Yes	• Disable • 4 hours • 24 hours	• 4 hours • 24 hours

Table 1.9 CAN/ULC S527 Field-programmable Settings

NOTICE TO USERS, INSTALLERS, AUTHORITIES HAVING JURISDICTION, AND OTHER INVOLVED PARTIES			
This product incorporates field-programmable software. In order for the product to comply with the requirements in CAN/ULC S527, Standard for Control Units and Accessories for Fire Alarm Systems, certain programming features or options must be limited to specific values or not used at all as indicated below.			
Program Feature or Option	**Permitted in CAN/ULC S527 (Y/N)**	**Possible Settings**	**Settings Permitted in CAN/ULC S527**
Remote resetting and silencing of a fire alarm control unit from other than the protected premises (ref: NFPA 72-2007 6.8.2.8)	No	Security Levels: • Administrator • User with Point Control • User with Client Control • Read Only	None
Block Acknowledge (PRU Mode Only)	No	• Yes • No	No
Use Node Control	No	• Yes • No	No
Enable NetLogic	No	• Yes • No	No
Disable Trouble Reminder	No	• Disable • 4 hours • 24 hours	• 4 hours • 24 hours

1.12 Compatible Equipment

NOTE: The ONYXWORKS-WS operates with products that have been certified to comply with UL 864, 10th Edition requirements as well as certain products that have not received UL 864, 10th Edition certification. Operation of UL 864 10th Edition compliant equipment together with products not tested for UL 864 10th Edition has not been evaluated. Such operation requires the approval of the local Authority Having Jurisdiction (AHJ).

1.12.1 Current Compatible Equipment

The ONYXWORKS-WS is compatible with the following equipment.

Table 1.10 Compatible Equipment

Type	Equipment	Description
Fire Panels:	• N16 • NFS-320 • NFS2-640 • NFS2-3030	**Note:** N16 panel compatible with workstation in PPCU mode only.
Network Cards:	• NCM-W • NCM-F • HS-NCM-MF • HS-NCM-SF • HS-NCM-W-2 • HS-NCM-WSF-2 • HS-NCM-WMF-2 • HS-NCM-MFSF	
Monitors:	• MON-22LCDW	22” Wide Screen LCD Monitor
	• MON-22LCDW-TS	Touchscreen 22” Wide Screen LCD Monitor
	• MON-42LCDW	42” Wide Screen LCD Monitor
	• MON-42LCDW-TS	Touchscreen 42” Wide Screen LCD Monitor
	Notes: • To remain compliant with UL listing and to meet the “Condition of Acceptability”, the keyboard and mouse must be connected when using a touchscreen monitor. • In Canada, all wiring connections to the monitor must be encased in conduit.	
Network Gateways:	• NFN-GW-EM-3	Embedded NFN Gateway
	• NFN-GW-PC-HNW-2	NFN PC Gateway card (wire connections)
	• NFN-GW-PC-HNSF	NFN PC Gateway card (single mode fiber connections)
	• NFN-GW-PC-HNMF	NFN PC Gateway card (multi mode fiber connections)
	• NFN-GW-PC-W	NFN PC Gateway card (wire connections)
	• NFN-GW-PC-F	NFN PC Gateway card (fiber connections)
Other Products:	• DACR-GW	Digital Alarm Communicator Receiver Gateway
	• LEDSIGN-GW	LED Sign Gateway
	• NOTIFY-IP	Live Voice Paging Application
	• OW-SCS	Smoke Control Feature Application (Only with NFS2-3030 panels.)

1.12.2 Compatible 8th Edition Fire Panels

The ONYXWORKS-WS is compatible with the following UL 864, 8th Edition fire panels:

- NFS-640
- NFS-3030

1.12.3 Legacy Compatible Equipment

The following equipment is listed as compatible with the ONYXWORKS-WS, but is no longer available.

Table 1.11 Legacy Compatible Equipment

Type	Equipment	Description
Network Cards:	• HS-NCM-W • HS-NCM-WMF • HS-NCM-WSF	
Network Gateways:	• NFN-GW-PC-HNW	NFN PC Gateway card (wire connections)

1.13 System Configuration

Required and optional components are described in the following table:

Table 1.12 System Configuration

Accessory/Subassembly	Part No.	Description	Proprietary Receiving Unit	Protected Premises Control Unit
Fire Panels	**Refer to Tables 1.10 and 1.11.**	Current UL-listed Fire Panels	R	R
Network Cards		Current UL-listed Network Cards	R	R
Workstation		Current UL-listed PC with ONYXWorks Software	R	R
Monitors		Current UL-listed Monitors	R[1]	R[1]
Network Gateway		Current UL-listed Network Gateways	R[2]	R[3]
Receivers Gateway		Digital Alarm Communicator Receiver Gateway	O	O
Paging Application		Live Voice Paging Application	O[4]	O[5]
Smoke Control Application		Monitoring and Control of Building Smoke Control Systems	O[5]	O[5]
Sign Gateway		LED Sign Gateway	O	O
UPS		Uninterruptible Power Supply	R	R
Keyboard		USB Keyboard	R	R
Mouse		USB Mouse	R	R
Software License		Enables ONYXWORKS-WS features.	R	R

R - Required component for functionally minimal system.
O - Optional

Notes:
1 - At least one of the monitors listed in Table 1.10 is required. A second monitor from Table 1.10 may be used, but is not required.
2 - One or more network gateways listed in Table 1.10 and 1.11 is required.
3 - A PC version of the network gateways is required when operating as a Protected Premises Control Unit.
4 - Paging from a Proprietary Receiving Unit is limited to non-emergency paging.
5 - Smoke control application is only compatible with NFS2-3030 panels.
6 - Life safety, emergency and mass notification paging is permitted from a Protected Premises Control Unit.

Section 2 Hardware Configuration

2.1 System Power

2.1.1 Primary and Secondary Power

The ONYXWORKS-WS requires connection to a separate dedicated primary AC fire alarm circuit as the primary power source. The circuit must be labeled "FIRE ALARM" and must connect to the line side of the main power feed of the protected premises. No other equipment can be powered from the fire alarm circuit. This circuit must run continuously, without disconnect devices, from the power source to the workstation. Overcurrent protection for this circuit must comply with Article 760 of the National Electrical Code as well as local codes.

If available, backup power for the workstation must be supplied by the building emergency power source. A supervised Uninterruptible Power Supply (UPS) is required to provide power continuity during the transition period from the primary power source to the emergency power source. The UPS must be UL 1481 or UL 864 listed, regulated, and power limited.

In Canada, backup power for the workstation must be supplied by the building emergency power source. A supervised UPS is required to provide power continuity during the transition period from the primary power source to the emergency power source. The UPS must be CSA or ULC listed, regulated, and power limited.

2.1.2 System Power Requirements

Table 2.1 System Power Requirements

Device Type	Max Current (Amps)	Power
ONYXWORKS-WS	7.0	120 VAC, 60 Hz
MON-22-LCDW	1.97	
MON-22-LCDW-TS	1.97	
MON-42-LCDW	1.2	
MON-42-LCDW-TS	2.00	

2.1.3 Safety

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

2.1.4 Motherboard Battery

The motherboard battery employed is the Panasonic CR2032 lithium battery. This part is not user serviceable and is provided as information only.

2.2 Connections

2.2.1 Component Connections

The location of the connections to the workstation PC are shown in Figure 2.1. Each connection is described in Table 2.2.

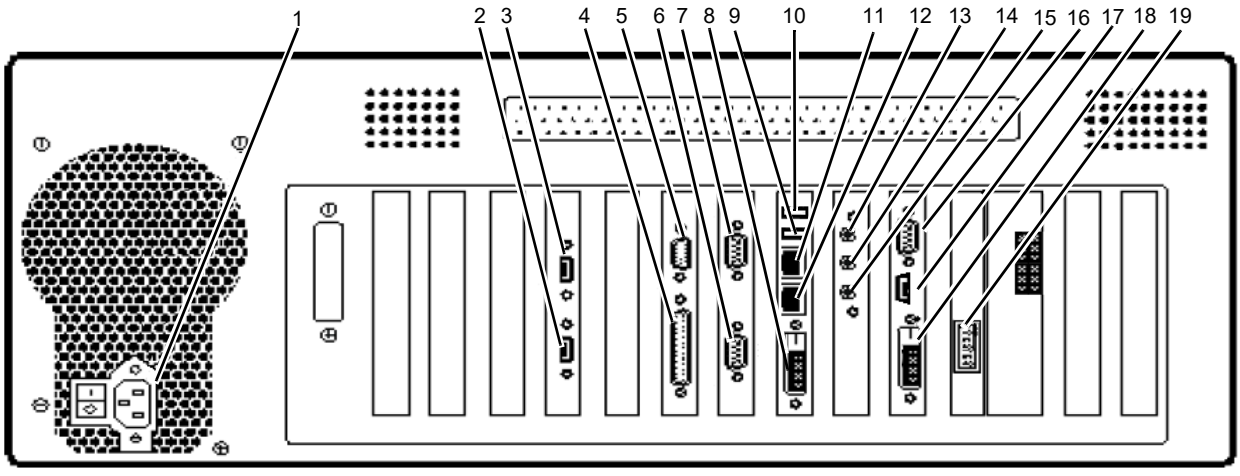


Figure 2.1 Computer Component Connections

Table 2.2 Connection Specifications

Item	Reference Designator	Description	Circuit Class	Specifications	Connection
1	Power	AC Power for Computer		• Voltage 120 VAC, 60 Hz • Current: 0.6 – 0.8 amps during normal operation	Refer to 2.2.3.
2	USB 2	USB 3.0 Type A Connector	2	• Line impedance 90±15% • Max distance 40 meters • Power limited • Supervised	
3	USB 3	USB 3.0 Type A Connector	2	• Line impedance 90±15% • Max distance 40 meters • Power limited • Supervised	
4	Parallel Port	Printer Port			Not Used
5	Com 3	RS-232	2	• Line impedance 5K ohm • Max distance 50 ft • Connection is power limited • Connection is supervised	
6	Com 2	RS-232	2	• Line impedance 5K ohm • Max distance 50 ft • Connection is power limited • Connection is supervised	
7	Com1	RS-232	2	• Line impedance 5K ohm • Max distance 50 ft • Connection is power limited • Connection is supervised	
8	DVI 0	DVI		Not Used	Not Used
9	USB 1	USB 2.0 Type A Connector	2	• Line impedance 90 ohm ±15% • Max distance 40 meters • Power limited • Supervised	Keyboard or Mouse
10	USB 0	USB 2.0 Type A Connector	2	• Line impedance 90 ohm ±15% • Max distance 40 meters • Power limited • Supervised	Keyboard or Mouse
11	LAN 1	RJ45	2	• Line impedance 100 ohm • Max distance 328 ft. (100 m) • Power limited • Supervised - Except for ground faults	Refer to 2.2.2
12	LAN 2	RJ45	2	• Line impedance 100 ohm • Max distance 328 ft. (100 m) • Power limited • Supervised - Except for ground faults	Refer to 2.2.2
13	Line In	3.5 mm		Audio Input	
14	Mic	3.5 mm		Microphone	
15	Speaker (Line Out)	3.5 mm		Audio Output	
16	VGA	VGA		Video	Display
17	HDMI	HDMI		Video	Display
18	DVI 1	DVI		Not Used	Not Used
19	J7	Digital I/O		Not Used	Not Used
Not Shown	USB	USB 2.0 Type A Connector on Front of PC	2	Maintenance Use Only	

2.2.2 Network (LAN) Connection

CAUTION: LAN TRANSIENT PROTECTION
IF LAN CONNECTIONS ARE REQUIRED TO LEAVE THE ROOM, TRANSIENT SUPPRESSION IS REQUIRED. USE SURGE SUPPRESSOR P/N PNET-1.

Make one of the following connections as applicable:

For a workstation that uses a single Ethernet connection for communications, attach the cable as shown in Figure 2.2.

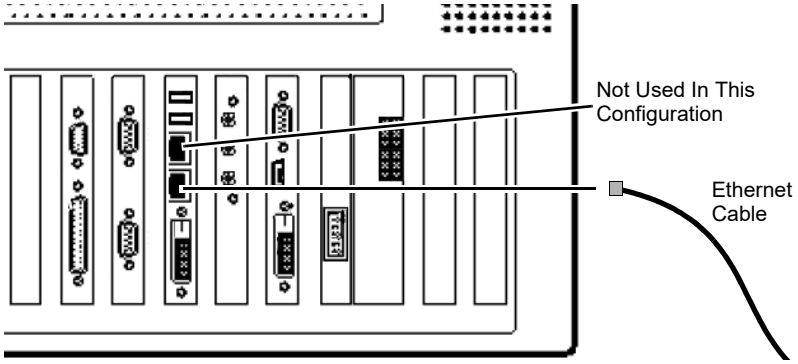


Figure 2.2 Single LAN Connection

For a workstation that uses dual connections for communications, attach the cable as shown in Figure 2.3.

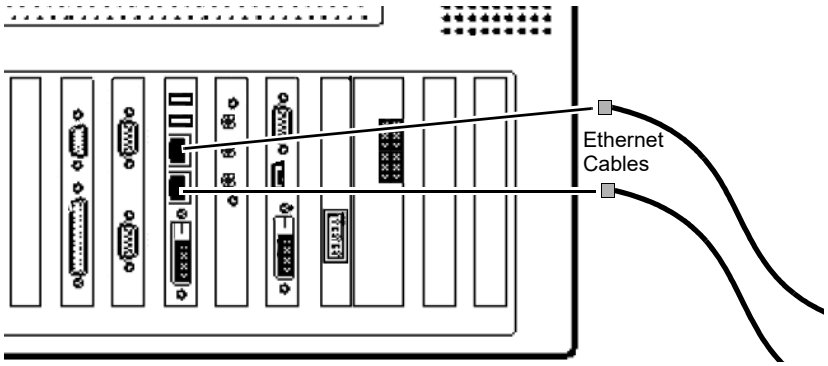


Figure 2.3 Dual LAN Connection

For an ONYXWORKS-WS that will not be using Ethernet for communications, a single Ethernet patch cable must be plugged in both RJ45 ports to create a loop-back between the Ethernet ports as shown in Figure 2.4.

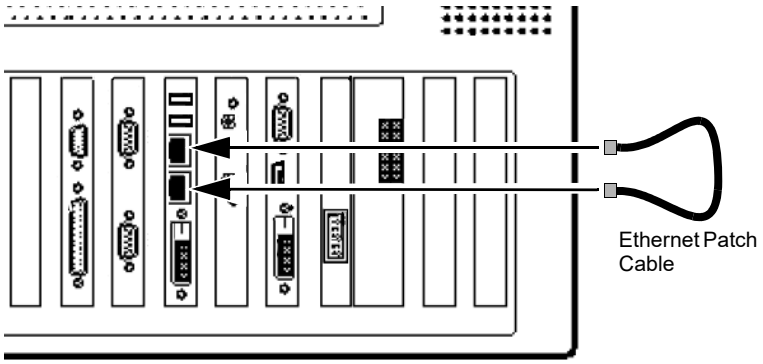
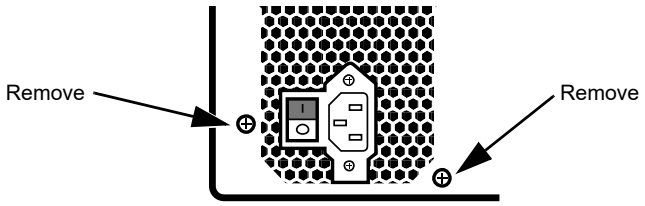


Figure 2.4 Stand-alone ONYXWORKS-WS

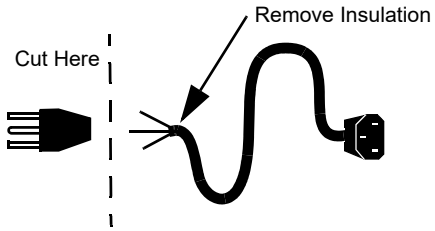
2.2.3 AC Power Connection

Connect AC power to the ONYXWORKS-WS computer as follows:

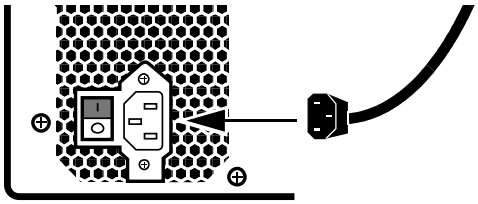
1. Verify that the voltage selection switch is in the correct position.
2. Verify that the rear-panel power switch is set to the **ON** (|) position.
3. Verify that the functional power switch, located behind the locking front door, is set to the **OFF** (O) position.
4. Remove the two screws shown below and retain for later use.



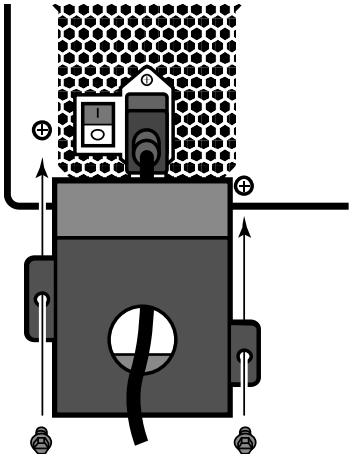
5. Cut the end off of the factory supplied AC power cord and remove outer insulation.



6. Plug the power cord into the ONYXWORKS-WS computer's AC power receptacle.



7. Feed the cut end of the power cord through the hole in the power cord locking bracket (PCLB) and reinstall the two screws removed earlier.



8. Strip the insulation from the ends of the three AC power cord wires and connect them to the UPS in accordance with manufacturer's instructions.

2.2.4 Wiring Methods

Wiring methods used shall be in accordance with UL 681.

2.3 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.

2.4 Testing and Maintenance

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

2.4.1 Testing

Testing shall be performed in accordance with NFPA-72 and CAN/ULC S536.

When acting as a smoke control subsystem, the workstation should also be tested in accordance with NFPA 92.

Before performing any testing on a fire alarm system or smoke control 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.

2.4.2 Maintenance

Maintenance shall be performed in accordance with NFPA-72.

If it is necessary to remove the cover of the PC during maintenance, perform the following steps:

1. Exit the workstation application.
2. Shut down the PC.
3. Ensure the computer's main power switch is in the OFF position.
4. Remove the power source from the PC.
5. Remove the PC cover.
6. Ensure that you are properly grounded.

Section 3 Workstation License Activation

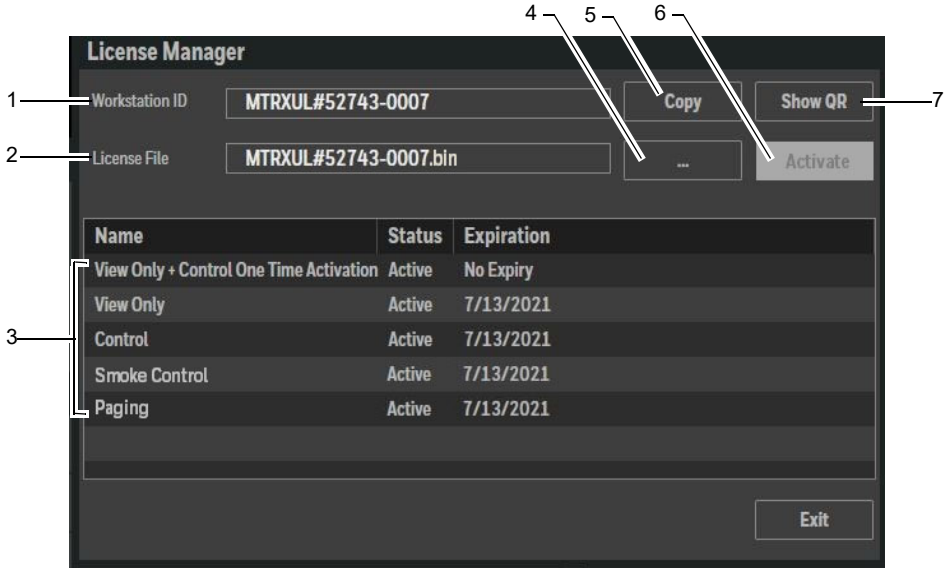
3.1 License Activation Procedure

NOTES:

- The configuration tool can be opened and used to configure a life safety system without an active software license. However, the configuration will not be able to be used unless the system's workstation has a software license.
- Once activated, the software license is valid for 5 years.

Perform the following steps to license a new workstation PC:

1. Type **License Manager** in the Windows search bar at the lower-left screen.
2. Double-click the License Manager app. The License Manager (see Figure 3.1) displays with an auto-generated workstation ID.



Item	Feature	Description
1	Workstation ID	Auto-generated ID number of the workstation to be licensed.
2	License File	Displays the license file name (.bin) after it has been activated in the workstation.
3	Features List	Displays the licensed features active on the workstation, status, and expiration date of the 5-year license.
4	Browse Button	Click to browse to the location of the license file.
5	Copy Button	Copies the Workstation ID to the clipboard.
6	Activate Button	Click to activate the selected license file.
7	Show QR	Displays the Workstation ID QR code to scan with a mobile device.

Figure 3.1 License Manager Layout

3. Click **Copy** to copy the Workstation ID number to the clipboard or click the Show QR button and scan the QR code if using a mobile device.
4. Using an Internet browser, go to fire.honeywell.com or use the CLSS Mobile App. The Honeywell CLSS portal displays.
5. Log in as follows:
   a. Click **Sign In**.
   b. Double-click the appropriate user account. The CLSS portal main window displays.
6. At the left side of the window, click the **Feature Activation** icon .
7. At the top-right side of the window, click the **All Customers** button and select the customer name from the list. Then click **Apply**. The feature activation window for the selected customer displays.
8. Click on **Workstations** and then on **+ADD WORKSTATION**. The *Workstation* window displays.
9. Select **Adding a New Workstation**, paste/enter the workstation ID number in the *Workstation ID #* field, and click **NEXT**. The *Add Workstation - Details* tab displays.
10. Click **Next**. A confirmation page displays with licensing details for the workstation.
11. Click **Confirm**. A license summary screen displays.

12. Click **Download License**. The license file is downloaded to the local PC *Downloads* folder. If using a mobile device, attach the license file to an email for transmission.
    - If license download process is being performed on the workstation PC, go to step 13.
    - If license download is being performed on a non-workstation PC, navigate to the Downloads folder, copy the license file (.bin) to a USB drive or paste as an attachment in an email for transmission to the worksite. Install the license file on the workstation PC and then go to step 13.
13. Close the workstation application (if running) on the workstation to be licensed and open License Manager (see step 1).
14. In License Manager (see Figure 3.1):
    a. Click the browse button (**…**).
    b. Navigate to the location of the license file.
    c. Double-click on the license filename (.bin extension). The filename displays in the *License File* field.
    d. Click **Activate**. A license activation success message displays. Click **OK**. The licensed features are displayed in the features list.
    e. When finished, click **Exit**.
15. Launch the workstation application from Windows 10 as follows:
    a. Click the Windows **Start** icon.
    b. Type "**workstation**" in the search field and **Enter**.
    c. Click the workstation application link in the search results window. The workstation application launches.
16. Log into the workstation and verify that the licensed features (if any) are activated in the workstation. If not, contact Technical Support.

NOTE: Once the license file has been successfully used, it can be deleted from the workstation, if desired.

Section 4 Configuration Tool Settings

4.1 Overview

This section describes the basic ONYXWorks Configuration Tool features and initial settings that an Administrator needs to make to set up the workstation. For more detailed information, refer to the *ONYX Configuration Tool Installation and Operation Manual* (P/N LS10050-007NF-E). For information about configuring the ONYXWorks Smoke Control Feature, refer to the *OW-SCS Configuration and Operation Manual* (P/N LS10050-012NF-E).

NOTE: The configuration tool can be opened and used to configure a life safety system without an active software license. However, the configuration will not be able to be used unless the system's workstation has a software license.

4.2 Initial Administrator Login

In order to configure the workstation, the Administrator must first log into the workstation. This is accomplished using one of the following methods.

4.2.1 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 Password dialog box displays with a random password in the field.
5. Enter a unique system password (20 characters maximum, case sensitive) in the field.
6. Click **OK**. The workstation starts.
7. Login to the workstation as specified in 6.3.1, "Login".

4.2.2 Existing Workstation after Software Upgrade

1. After upgrade, the *System Password* dialog box displays with a random password in the field.
2. Enter a unique system password (20 characters maximum, case sensitive) in the field.
3. Click **OK**. The workstation starts.
4. Login to the workstation as specified in 6.3.1, "Login".

4.3 User Profiles and Passwords

The workstation software application's factory-defined user profiles consist of the following:

- Administrator
- Read Only
- Point Control
- Client Control

The primary Administrator's password is configured upon initial installation of the ONYXWorks software. This factory-defined Administrator profile cannot be deleted.

Any Administrator-level user can configure profiles/passwords for other administrators and for the non-administrator users via the workstation configuration tool.

Any Administrator-level user can delete the profile for any users except their own profile or that of the primary Administrator.

4.4 Configuration Tool

4.4.1 Overview

The configuration tool is used to configure the system that is to be monitored by the workstation. Configuration primarily includes the following:

- Identifying the networks to be monitored
- Laying out the graphical floor plans representing the monitored facility
- Setting the parameters for system operation
- Configuring profiles for selective monitoring

Other system capabilities may be configured depending on the workstation software loaded. Refer to the configuration tool manual applicable to your workstation for additional information.

In the tool's floor plan screen, icons that represent fire system devices, display information, and navigate the system may be placed.

Once the system is configured, a first responder may use the configured system in the workstation to identify the location of, and respond to, an annunciated event.

After modifying a workstation graphics design in the configuration tool, verify it is correctly displayed on the workstation.

On the workstation, the configuration tool is installed along with the workstation software.

4.4.2 Launching and Exiting the Configuration Tool

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

- From within the workstation application, go to **Menu**> **Configure > Launch Configuration Tool**.
- From Windows 10:
  1. Click **Start**
  2. Type "**Configuration Tool**" in the search field and press **Enter**.
  3. Click the configuration tool application link in the search results window. The configuration tool opens.
  4. Select the applicable option in the table below and then click **OK**.

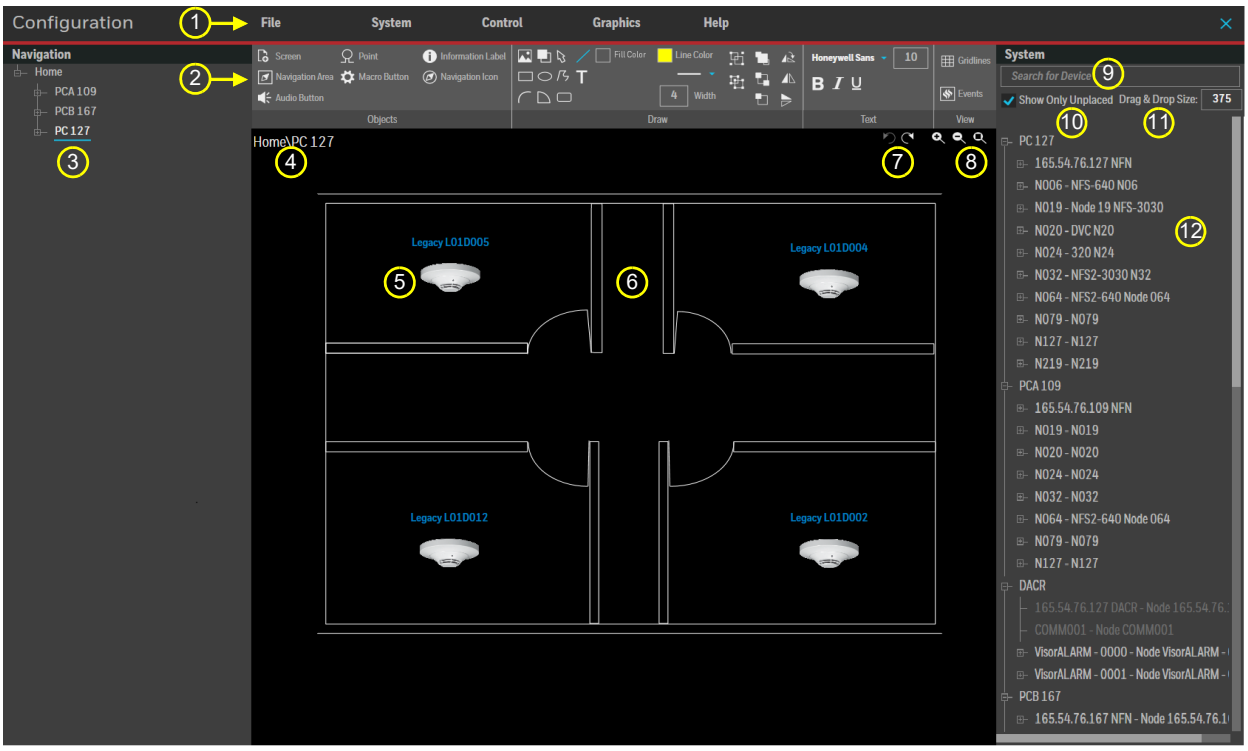
Table 4.1 Configuration Tool Start Options in Windows

Option	Description
Live System	Opens the configuration tool which uses the system database currently on the workstation PC. Displays only if the PC has the workstation software application installed.
New System	Creates a new, blank system database. After editing and saving the new system, it may be imported by a live workstation at a later time.
Browse	Allows selection and editing of an existing system's database. After saving, the edited system may be imported by a live workstation at a later time. Use one of the following methods: • Select for editing an existing remote system by entering the IP address of the remote PC. • Select for editing an existing system on the current PC by browsing for, and opening, the desired "Matrix.mdb" file. **Note:** If the selected system was created using an older version of the workstation software, it will be upgraded before allowing the user to perform editing.

To exit the configuration tool, go to **File > Exit** or click the "X" at the top right-hand corner of the floor plan screen and respond to the prompts that display.

4.4.3 Configuration Tool Layout

The configuration tool opens by default to the Configuration Tool Main Screen as shown in Figure 4.1. This screen allows the user to create and place informational objects on a floor plan. Other configuration screens can be accessed by clicking the menus at the top of the screen**.** The menu options are described in Table 4.2.



Item	Feature	Description
1	Main Menu Bar	Click to access configuration tool sub-menus. Refer to Table 4.2.
2	Floor Plan Tool Bar	Click items to access floor plan screen tools. Refer to Table 4.2.
3	Navigation Tree	Click labels to navigate to screens for system buildings, floors, etc.
4	Screen Title	Displays the label/address of the currently displayed screen.
5	Device Icon	Represents a fire system device. Click the icon for additional information.
6	Floor Plan Screen	Graphic area depicting the features of the selected area in the fire system.
7	Undo/Redo Buttons	Click to undo or redo the last action performed on the floor plan.
8	Zoom Tools	Click to zoom in, zoom out, or zoom to full size.
9	Device Search Tool	Search the system component list for a specific device.
10	Show Only Unplaced	Select to show only unplaced devices in the system tree.
11	Drag & Drop Size	Specify the size of device icons dragged onto floor plan from the system tree. The larger the number, the larger the icon will be on the floor plan.
12	System Tree	List of fire system devices, etc. Drag label to place icon on the floor plan.

Figure 4.1 Configuration Tool Floor Plan Editor Screen Features

4.4.4 Configuration Tool Menus

The following table describes the menus associated with the ONYXWorks Workstation configuration tool.

Table 4.2 Configuration Tool Menus and Floor Plan Toolbar

Location	Description
Main Menu Bar	Located along the top of the configuration tool main screen.
	File Menu: **Open** - Visible on stand-alone configuration PCs only. Allows the user to open and configure additional systems. **Merge Database** - Allows the user to import the data from an existing system database into the currently open system database. This creates a single database with the contents of both databases merged. **Save** - Saves the configuration tool settings without closing the configuration tool. **Exit** - Closes the configuration tool.
	System Menu: **Networks** - Allows the user to add, delete, modify networks and nodes. Refer to 4.4.7, "Networks" for additional information. **DVC Inputs** - Allows the user to map sequence inputs from their network Digital Voice Command modules (DVCs) to inputs that can be used by the workstation when configured for emergency audio. These inputs are then used by the Audio Group Manager, in which an audio group will be assigned one of the input numbers that were configured in the DVC Inputs window. **Note:** The input and priority settings must match those configured on the DVC(s). **Signs** - Allows the user to configure the LED Sign Gateways as part of the current system. This allows the user to send a message to the sign from the workstation. Using this feature violates the UL listing. **System Options** - Allows the user to select options as to how the workstation interface will operate. Refer to 4.4.9, "System Options" for additional information. **Monitoring Profiles** - Allows the user to configure the monitoring profiles which can be selected by the users in the workstation software. Refer to 4.4.8, "Monitoring Profiles" for additional information. **Users** - Allows the user to set workstation user passwords and privileges. **Chemicals** - FirstVision only. Opens the Chemicals screen where information about hazardous chemicals is stored. The user can add or remove chemicals from the list. Chemical information can be associated with a hazardous material icon on the floor plan. **Database Editor** - Allows the user to edit the workstation database in a spreadsheet format.
	Control Menu: **Macros** - Opens the Macro Editor Screen where the user can configure macros. Refer to 4.4.5, "Macros" for additional information. **Control Profiles** - Allows the user to configure the control profiles which can be selected by the users in the workstation software. Refer to 4.4.6, "Control Profiles" for additional information. **Audio Groups** - Allows the user to configure audio groups for use with NOTIFY-IP. Refer to 10.15, "Audio Groups" for additional information. **SCS Weekly Test** - Only visible with workstation optional smoke control feature. Allows the user to configure a weekly test of the smoke control system via specified fire panels. Refer to the *OW-SCS Configuration and Operation Manual* (LS10050-012NF-E) for additional information.
	Graphics Menu: **Default Icons** - Allows the user to view, search, and customize the icons in the currently selected icon set. **Status Classes** - Allows the user to configure custom colors and sounds for each event status class. **Floorplan Options** - Allows the user to configure the text displayed above the icons, the floor plan foreground and background colors, and the icon set to be used.
	Help Menu: About - Displays version and other information pertaining to the configuration tool.

Table 4.2 Configuration Tool Menus and Floor Plan Toolbar *(Continued)*

Location	Description
Floor Plan Tool Bar	Allows the user to configure and place/draw a variety of informational objects on the floor plan screen.
	Objects: **Screen** - Allows the user to add screen backgrounds, titles, and specify parent screens. **Navigation Area** - Allows the user to create and select the destination for a navigational area. **Navigation Icon** - Allows the user to create and select the destination for a navigation icon. **Point** - Allows the user to create and configure points. For each event status class, a point can be assigned an icon and linked media for text, image, audio, and video; each of which can be auto-activated. **Macro Button** - Allows the user to create and place buttons that activate configured macros. **Audio Button** - Allows the user to configure and place audio buttons. **Information Label** - Allows the user to configure and place information labels that provide important user information.
	Draw - Provides drawing tools for use on the floor plan screen. Hover to display the meaning of symbols.
	Text - Provides text settings for use on the floor plan screen. Active when text tool "**T**" is clicked.
	View: **Gridlines Button** - When clicked, grid lines are displayed on the floor plan to aid in placement of information. Does not appear on the workstation screen. **Events Button** - When this button is clicked, all device icons on the floor plan display in an alarm state. This includes tinting of each icon, placing a box around it, and displaying event text below each icon. The purpose of this option is to assist users when laying out floor plan icons. For instance, they can use it to ensure that the event text is easily readable and does not overlap lines on the floor plan background.

4.4.5 Macros

Macros allow users with point control-level privileges to execute a series of configured commands for system devices by clicking an on-screen button or link. Macros are created by the Administrator in the configuration tool (**Control > Macros**).

The Administrator creates a macro command by naming it and assigning it one or more macro options. Available macro options are contingent upon the gateway type, point, and node type that is selected.

Macros are executed through the workstation in one of the following ways:

- Clicking on a macro icon on the floor plan.
- Clicking on the label of the desired macro in the workstation Macros window (**Menu > View > Macros**).

4.4.6 Control Profiles

Control profiles are only available on workstations running in Proprietary Receiving Unit (PRU) mode. In addition, the Administrator must select **Yes** for Use Node Control via **Menu > Configure > Options > General Tab** on the workstation.

Control profiles are created by the Administrator in the configuration tool (**Control > Control Profiles)**.

Control profiles allow the user to select which nodes will be controlled by a workstation. When a control profile is activated in the workstation, it enables the right-click menu options (enable, disable, silence, reset, etc.) on point icons and on the events displayed in the workstation New Events pane.

A remote node can only accept a command or acknowledgment from a workstation which controls it. When a user acknowledges an event from a workstation that does not control the node where the off-normal device resides, the event is acknowledged at that workstation only.

Only one workstation at a time may control a given node. Taking control of a node from one workstation automatically cancels control of that node at any other workstation.

A fire network may be monitored by multiple workstations, each of which controls only a portion of the nodes on the network. This is often the most feasible solution for monitoring large networks.

Control profiles are activated through the workstation application by Administrators and users with permission as follows:

1. Select **Menu > Configure > Control Profiles**. The Control Profiles window displays.
2. Select a profile listed in the Control Profiles column of the window. The 'Default' profile may be the only one listed.
3. Click **Activate Profile**. The workstation will be able to send commands to the nodes specified in the selected control profile.

4.4.7 Networks

4.4.7.1 Importing Network Configuration Data

Copy the network (and screen, etc.) configuration from a peer workstation that has already been configured as follows:

1. In the workstation application, go to **Menu > File > Import System Data**. The *Select System To Import From* dialog box displays.
2. Select the IP address of the peer workstation from the *Available Systems* field or enter an IP address in the *IP Address to Import From* field.
3. Click **OK**.

4.4.7.2 Adding a Network

Network names and gateway connections are created using the configuration tool as follows:

1. In the configuration tool, go to **System > Networks**. The Networks window opens.
2. Click the **Add** button.
3. Type a unique network name into the *Alias* field (default is “New”).
4. Select the network type from the **Type** drop-down list.
5. Click the first *IP Address* field and enter the gateway IP address. Gateway and node labels are displayed in the navigation tree. Once the connection is made, clicking the arrow (❯) next to the IP address opens the configuration tool for the gateway. If it does not open, it could be for one of the following reasons:
   - The PC cannot connect to the gateway IP address.
   - The gateway is not running.
   - The gateway is a PC gateway running on another workstation PC.
6. If there is to be another gateway monitoring the system, enter its IP address in the second *IP Address* field. Gateway and node labels are displayed in the navigation tree.
7. Add nodes as described in the following paragraph or click **OK** to exit the screen.

4.4.7.3 Adding Nodes to a Network

Add nodes to a network as follows:

1. In the Networks window (**System > Networks)**, click the network label in the navigation tree under which the node is to be added.
2. Add nodes using either of the following methods:
   - Click the **Add Node** button. This option adds a single node to the network. Go to Step 3.
   - Click the **Import Panel Database**. This option adds all the nodes and points from a VeriFire® database. Any nodes and points that are in the database will be autocreated on the selected network. Go to Step 6.
3. Enter a unique node name into the *Alias* field (default is “New”).
4. Enter the IP address of the node in the *Address* field.
5. Select the node type from the *Node Type* drop-down list.
6. Click **OK**. The node or nodes are added to the network.

4.4.7.4 Migrating Nodes

Migrate a node from a network monitored by the workstation to a different network monitored by the same workstation as follows:

1. In the Networks window (**System > Networks)**, click a on the node label in the navigation tree.
2. Click the **Migrate Node** button. The Migrate Node dialog box displays.
3. Select the destination network from the drop-down list.
4. Enter a new, unused node number (1 to 240) in the field provided or use the up/down arrows to increment the number.
5. Click **OK**.

4.4.7.5 Deleting Networks and Nodes

Delete a network or node as follows:

1. In the Networks window (**System > Networks)**, click on the network or node label in the navigation tree.
2. Click **Delete**. Click **Yes** in response to the confirmation message.

4.4.8 Monitoring Profiles

NOTE: Monitoring Profiles must be configured before selecting settings on the Event Printer tab or Email tab and before configuring a custom-configured, logged-out monitoring profile.

Monitoring profiles are created by the Administrator in the configuration tool (**System > Monitoring Profiles**).

Monitoring profiles allow the user to select which nodes are monitored by a workstation. These profiles are event annunciation filters that are set up to monitor or not monitor an event location and its event status class 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.

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 status classes, the user must create a new monitoring profile.

Monitoring profiles are activated through the workstation application by Administrators and users with permission as follows:

1. Select **Menu > Configure > Monitoring Profiles**. The Monitoring Profiles window displays.
2. Select a profile listed in the Monitoring Profiles column on the left-hand side of the window. The 'Default' profile may be the only one listed.
3. Click the **Activate Profile** button.The workstation displays information only for the locations and event status classes specified in the selected monitoring profile.

4.4.9 System Options

In the configuration tool, go to **System > System Options**. Settings are described in the following table.

Table 4.3 System Options Configuration

Setting	Possible Settings	Comments
Operating Mode		The workstation must be set to the same operating mode as the NFN Gateway(s).
	Canada - Proprietary Receiving Unit	Canada - Proprietary Receiving Unit (PRU) mode meets ULC S527 requirements and otherwise runs exactly as the PRU Mode. NFN networks configured for Mass Notification operations are not supported in Canada - Proprietary Receiving Unit mode.
	Canada - Protected Premises Control Unit	Canada - Protected Premises Control Unit (PPCU) mode meets ULC S527 requirements and otherwise runs exactly as the PPCU mode. This mode is not available when more than one NFN is connected to the workstation.
	Canada - Protected Premises Control Unit + DCC	Canada - PPCU + DCC (Display and Command Center) mode meets ULC S527 requirements and otherwise runs exactly as the PPCU mode. This mode is not available when more than one NFN is connected to the workstation.
	China - CCCF	China - CCCF mode meets Certification Center for Fire Products (CCCF) standards.
	Proprietary Receiving Unit	PRU mode supports multiple gateways and workstations. NFN networks configured for mass notification operations are not supported in PRU mode.
	Protected Premises Control Unit	PPCU mode is not available when more than one NFN is connected to the workstation. In this mode, the workstation is a peer of a panel it monitors (i.e. actions taken at the panel register on the workstation). PPCU mode requires exactly one workstation and the NFN Gateway running on the same PC as the workstation.
Mass Notification Priority	• None • Lower than Fire • Higher than Fire	Active only in PPCU mode.Select from the drop-down list.
Logged-Out Monitoring Profile	• All Nodes, All Events (Default) • Custom Profiles	Select the desired monitoring profile from the drop-down list. If no one is logged in to the workstation, the selected monitoring profile is activated.
Extract Description from Panel	• Yes	Default. Use point descriptions as received from the FACP.
	• No	Use point descriptions as defined by the configuration tool and discard point descriptions received from the FACP.

Table 4.3 System Options Configuration *(Continued)*

Setting	Possible Settings	Comments
Time Server Settings	IP Address	This field is used to enter the IP address of the server that is used to synchronize the ONYXWorks system time. If the IP address for the time server is the same IP address as this workstation PC, then this workstation will function as the time server. Otherwise, the workstation PC will use the time server at the specified IP address.
Audio Multicast IP	IP Address	This setting is for use with the NOTIFY-IP option provided the IP network supports multicasting.
System Description	Enter a unique system description.	This description is an alias by which the system can be easily identified. This aids the user during off-line configuration where multiple systems may be configured.
System Password	Enter a unique password.	20 characters maximum, case sensitive. In order for the workstation to connect to a gateway, the system password must match the system password configured on the gateway. The system password must be manually entered individually on each workstation PC by entering this setting in the configuration tool residing on that PC. On workstation PCs, this setting is only available when editing the live system.
Require Confirmation	• Field Acknowledge • Silence • Reset • Manual Evacuation • Enable/Disable • Activate/Deactivate	Selecting 'Yes' causes a confirmation message to display before the action is performed. (Default is "No").

Section 5 Workstation Settings

5.1 Windows Settings

The following table contains Windows settings that are set in the factory and those the user must make to ensure the software operates properly on their system.

Table 5.1 Windows Settings

Setting Type	Setting	Required Value
Factory Default Settings:	Factory default settings must not be changed without the approval of a Technical Services representative.	
	Power Options	Screen: Turn off the display after: **Never** Sleep: PC goes to sleep after: **Never**
	Display Resolution: MON-22LCDW MON-22LCDW-TS MON-42LCDW MON-42LCDW-TS	1920 x 1080
	Display Scale	100%
User Configured Settings:	The user configures these settings as necessary to be compatible with their system.	
	Administrator Password	Change the default Admin password to a unique password (8 characters minimum, case sensitive).
	IP Address	Enter a valid IP Address if connecting to a LAN.
	Time Zone	Set the local time zone.
	Daylight Savings Time	Set as appropriate for the local area.

5.1.1 Disabling Automatic Updates - Windows 10 Professional

When using a non-Comark PC as a workstation, the user must disable automatic Windows updates as follows:

1. With Windows running, press **Windows key + R**. The Run dialog box displays.
2. Enter **gpedit.msc** and click **OK**. The Local Group Policy Editor dialog displays.
3. Navigate to **Computer Configuration > Administrative Templates > Windows Components > Windows Update**.
4. In the Windows Update folder, double-click **Configure Automatic Updates**. The Configure Automatic Updates dialog displays.
5. Select the **Enabled** radio button.
6. In the Options pane, under "Configure automatic updating", select **2 - Notify for download and notify for install** from the drop-down list.
7. Click **OK**.

5.1.2 Manual Windows Updates

While it is necessary to disable automatic Windows updates, it is recommended that Windows updates be manually downloaded at regular intervals to ensure proper workstation operation.

5.2 Workstation Mouse Click vs. Screen Touch Equivalents

The workstation user interface is operated using either a mouse or by touching the screen on a touchscreen monitor. The following table describes the equivalent user actions for these two methods.

Table 5.2 Click vs. Touch Equivalents

Click Type	Touchscreen Equivalent
Right-click	Tap
Double-click	Double-Tap
Left-click	Touch and Hold

5.3 System Options Settings

The workstation settings described in this section are available from **Menu > Configure > Options**. These settings apply only to the local workstation. Click **Apply** to save the settings.

5.3.1 General Tab

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

Table 5.3 General Tab Settings

Setting	Possible Settings	Description
Event Label: The event label is displayed in event lists throughout the workstation. The event label options are described below.		
Network Label	Description	Display the network description (alias).
	None	Default. No label is displayed.
Node Label	Description	Display the node description (alias).
	Address	Display the system-assigned node address.
	None	Default. No label is displayed.
Point Label	Description	Default. Display the point description (alias).
	Address	Display the system-assigned point address.
	None	No label is displayed.
History Backup: The external backup file is named with the date: YYYMMDD.HIS. History backup options are described below.		
Automatically Backup History	Scheduled	Activates the Backup Frequency field. Schedule history backup interval by number of days (1-62) or months (1-12).
	When Full	Default. History is backed up when the history database is full (2.5 million entries).
General: Options are described below.		
Show Only Off-normal Devices	Yes	Display only icons of points that are off normal. If there are no current events on the system, no points are visible in the graphics display.
	No	Default. Show all points regardless of state.
Auto-activate Next Event After Acknowledge	Yes	Once the first event in the New Events pane is acknowledged, the next event automatically activates. The workstation plays any media files linked to the event.
	No	Default. When the first event is acknowledged in the New Events pane, the next event does not auto-activate.
Automatically Navigate On Event	Yes	Default. Once an event reaches the top of the New Events list, the workstation navigates to the screen containing the device icon associated with the event.
	No	Do not automatically navigate to the screen with the off- normal event.
Show Navigation Icon Labels	Yes	Default. Display the user-defined text below the navigation icons.
	No	Hide the user-defined text located below the navigation icons.
Show Background Events on Navigation Icons	Yes	Navigation icons “illuminate” to indicate a status change of points that are in the floor plan or nested floor plans for mapped background events.
	No	Default. Navigation icons do not illuminate.
Save Toner When Printing	Yes	Causes the optional graphics printer to invert dark colors (i.e. black to white) when printing the floor plan. For optimum print quality, the floor plan background should be set to black or white.
	No	The graphics printer will print screen as it appears on the workstation.
Fire Alarm Reminder	Disabled	The fire alarm reminder feature is not enabled.
	4 hrs or 24 hrs	After the selected number of hours has passed, an on-screen reminder alerts the user that a system trouble has not been acknowledged. (Default is 24 hours.)

Table 5.3 General Tab Settings *(Continued)*

Setting	Possible Settings	Description
CO Alarm Reminder	Disabled	The CO alarm reminder feature is not enabled.
	4 hrs or 24 hrs	After the selected number of hours has passed, an on-screen reminder alerts the user that a system trouble has not been acknowledged. (Default is 24 hours.)
Supervisory Reminder	Disabled	The supervisory alarm reminder feature is not enabled.
	4 hrs or 24 hrs	After the selected number of hours has passed, an on-screen reminder alerts the user that a system trouble has not been acknowledged. (Default is 24 hours.)
Trouble Reminder	Disabled	The trouble reminder feature is not enabled.
	4 hrs or 24 hrs	After the selected number of hours has passed, an on-screen reminder alerts the user that a system trouble has not been acknowledged. (Default is 24 hours.)
Enable Emails (Optional Software Feature)	Yes	Default. The workstation sends emails as configured on the Email tab.
	No	Email function is disabled.
Use Node Control	Yes	Default. Proprietary Receiving Unit (PRU) modes only. Requires a user with control privileges to take manual control of nodes or networks via the Control Profiles window before sending commands to the node/network. Refer to 1.11, "Field Programmable Settings" for regulatory considerations.
	No	PRU modes only. Allows any user with control permissions to send commands to any nodes/networks on the system. Control Profiles window is inaccessible.
Block Acknowledge	Yes	Proprietary Receiving Unit (PRU) modes only. Allows acknowledgment of all events listed in the New Events pane by clicking the Block AK button.
	No	Default. PRU modes only. Block acknowledgment of new events is not available.
Enable NetLogic	Yes	Enables the NetLogic automatic event response application.
	No	Default. NetLogic is not Enabled
Monitor Fan	Yes	A fan trouble event appears in the New Events window on the workstation screen if a PC cooling fan malfunctions.
	No	Default. Fan monitoring is not enabled.
Omit Control Point On, Point Active, and Zone On From History	Yes	Control Point Activations, Point Activations, and Zone Activations are not written to history.
	No	Default. Store these events in history.

5.3.2 User Features Tab

The User Features tab allows the Administrator to configure various user interactions as described in the following table.

Table 5.4 User Features Settings

Setting	Possible Settings	Description
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	Yes	Automatic Unacked Alarm Operation enabled.
	No	Default. Automatic Unacked Alarm Operation disabled.
Unacked Event Timeout	3 - 60 minutes	Amount of time before the user-defined macro is executed. (Default is 3 minutes)
Macro Activated on Alarm	Macro Name	Select a macro from the drop-down list. Macros are configured in the workstation configuration tool.
	None	Default. Do not activate a macro.
Security:		
Inactivity Timeout	1-20 minutes	Amount of time with no activity after which a user is automatically logged out. **Note**: Must be enabled for UL 2572 compliance.
	0	Default. Do not automatically log out a user.
User Responses:	8 User-defined Responses	Enter text to be stored in history as responses to events. These are displayed when a user right-clicks on a floor plan icon.

5.3.3 Event Printer Tab

The Event Printer tab allows the user to enable or disable the optional printer. An event printer is not required for UL 864 operations. 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 is displayed using the selected output format. Settings are described in the following table.

Table 5.5 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	Yes	Enable the connected event printer.
	No	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 4.4.8, "Monitoring Profiles" for additional information.
Output Format	Default (Fire)	Use the system default output format.
	User-defined Output Format	Select an output format from the drop-down list. Refer to 5.3.5, "Output Tab" for additional information.
Sample Output: Displays a sample of the output that will be printed using the settings selected above.		

5.3.4 Email Tab

The Email tab allows the user to configure the optional email capabilities of the workstation.

Email notifications are only intended to be transmitted to a limited number of staff for maintenance and system status purposes. This feature is approved by UL as supplementary.

The Email tab provides the capability to send system information via the local email server to an email account. This configuration uses monitoring profiles and output formats to determine the information that is sent. The email server should be configured before an email account is added.

The following parameters govern the workstation email functions:

- The email server may be either on-site or provided by an Internet Service Provider (ISP).
- The email functions support SMTP format only.

Email settings are described in the following table.

Table 5.6 Email Tab Settings

Setting	Possible Settings	Description
Buttons:		
Add		Click to add and name an Email. Enter email configuration information in the fields listed below.
Delete		Click to delete the email selected in the event email list.
Event Email:		
Email List		Displays the names of configured emails. Select the email name to view/modify its settings.
Name	Text Field	Displays the email recipient's name. Click the field to rename.
Address	Text Field	Enter the email address of the recipient.
Enabled	Yes	Event email is sent to the selected recipient.
	No	Event email is not sent to the selected recipient.
All Day	Yes	Send the event email whenever it occurs.
	No	Send the event email at the configured start and stop times.
Start Time	12 AM to 11 PM in Hourly Increments	Activates only when "**All Day > No**" setting is selected. Select the times from the drop-down lists.
Stop Time		
Monitoring Profile	Default	Use the system default monitoring profile.
	User-defined Monitoring Profiles	Select a user-defined monitoring profile from the drop-down list. Refer to 4.4.8, "Monitoring Profiles".
Output Format	Default (Fire)	Use the system default output format.
	User-defined Output Format	Select a user-defined output format from the drop-down list. Refer to 5.3.5, "Output Tab".
Linked Media	Yes	Attaches the informational document associated with the point in alarm.
	No	Does not attach the point information document.
SMS	Yes	Send email as a text message to a cell phone.
	No	Does not send email as a text message.
Screen Shot	Yes	Attaches a screen shot of the floor plan area where the event has occurred. **Notes:** • Not available for text messages. • The floor plan need not be open on the workstation for this to function.
	No	Does not attach a screen shot to the email.
Sample Output:		Displays a sample of the email message that will be sent to the recipient using the output format configured above.
Email Configuration:		
Email Only Off-normal Events	Yes	Sends emails for off-normal events only.
	No	Sends emails for all events.
Subject	Text Field	The subject that is to appear in the email subject line.
Return Address	Text Field	Return email address of the email sender.

Table 5.6 Email Tab Settings *(Continued)*

Setting	Possible Settings	Description
SMTP Server:		
Server Address	Text Field	The IP address of the SMTP server.
Port	1 to 65535	The port the workstation uses to communicate with the SMTP server. It is dependent upon the SMTP server configuration. The most common ports are 25, 465, and 587. Use the up/down arrows or click the field and enter the port number.
Use Secure Sockets Layer (SSL)	Yes	Enables encrypted server communication. Enable only if the SMTP server supports SSL.
	No	SMTP server does not use SSL encryption.
Use Authentication	Yes	Allows the workstation to connect to an SMTP server that requires a user name and password. Activates user name and password fields.
	No	A user name and password is not required by the SMTP server.
User Name	Text Field	Limited to 255 characters.
Password	Text Field	Limited to 255 characters. Case sensitive.
Test Email		Click **Send** to send a test email.

5.3.5 Output Tab

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

Table 5.7 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 **OK**. The name is displayed in the Output Formats list.
Delete Format		Click to delete the output format selected in the Output Formats list. Click **Yes** in response to the output format delete confirmation prompt. • If the output format is NOT used in a printer, pager, modem, or email setup, the selected output format is deleted. • If the output format IS used in a printer, pager, modem, or email 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 List		Displays the names of configured outputs. Select the output name to view/modify its settings.
Available Fields	• 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: • Select one at a time - Double click on the field name or single-click on a field name and then click on the single down-arrow button. • Select several (consecutive) - Click the first field name desired, press and hold the **Shift** key, and click the last field name. Then click the single down-arrow button. • Select several (not consecutive) - Click the first field name, press and hold the **Ctrl** key, and select the other desired fields. Then click the single down-arrow button. • Select all - Click the double down-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 highlighted in the *Output Formats* field. To remove fields from the output, double-click the field name or select the field name and use the single-up arrow.
User Defined Messages:	• Fire • CO Alarm • Security • Supervisory • Trouble • Disabled • PreAlarm • Other • Advise • Background	Active only when the “User Defined” output format is in the *Available Fields* list. Click the field to the right of the event status class label to enter/modify the message associated with each type of event. The “Other” message is used for Mass Notification events and other events not included in the list.

5.3.6 Smoke Control Tab and Multi-Station Smoke Control Tab

The Smoke Control Tab and the Multi-Station Smoke Control Tabs are only visible when the workstation is licensed for the smoke control feature. For information about these tabs, refer to the *OW-SCS Configuration and Operation Manual* (P/N LS10050-012NF-E).

Section 6 Operation

6.1 Overview

This section describes the basic operation of the workstation as it is used to monitor a life safety system. For detailed information concerning the operation of the workstation using the optional smoke control feature, refer to the *OW-SCS Configuration and Operation Manual* (P/N LS10050-012NF-E).

6.2 Starting and Exiting the Workstation Application

Open the workstation application from Windows 10 as follows:

1. Click **Start**
2. Type "**workstation**" in the search field and press **Enter** or go to **Start > All apps > Facilities Monitoring > Workstation**.
3. Click the workstation application link in the search results window. The workstation application opens.

Only an Administrator can exit the workstation application by selecting **Menu > File > Exit**.

6.3 User Login and Log Out

The Administrator grants users workstation login and use privileges. When a user logs in, the user's information is recorded in the workstation history database and the user can perform workstation operations as allowed by the privileges. If another user logs in, the software automatically logs out the previous user.

6.3.1 Login

Log in as follows:

1. In the workstation software application, open the login window in one of the following ways:
   a. Go to **Menu > File >Login**.
   b. Click **Logged Out** in the top-right corner of the screen.
2. Select the desired user name in *Available Users* field.
3. Enter the password in the *Password* field.
4. Click **OK**. The name of the current user displays at the top-right corner of the screen.

6.3.2 Switching Users

Switch users as follows:

1. In the workstation software application, open the login window in one of the following ways:
   a. Go to **Menu > File >Login**.
   b. Click the current user's name in the top-right corner of the screen.
2. Select the new user's name in the *Available Users* field.
3. Type the password in the *Password* field.
4. Click **OK**. The name of the new user displays at the top-right corner of the screen.

6.3.3 Logout

Log out as follows:

1. In the workstation software application, open the login window in one of the following ways:
   a. Go to **Menu > File >Login**.
   b. Click the current user's name in the top-right corner of the screen.
2. Click **Logout**. The user is logged out, but the ONYXWorks system continues to be monitored according to the Logged-Out Monitoring Profile setting established in the configuration tool (refer to Table 4.3).

6.4 Workstation Screen Layout

The workstation main screen displays the ONYXWorks system as floor plans, point icons, informational labels, and real-time event information in tabular/list form. The Administrator designs the floor plan using the configuration tool. The user selects the particular area of the fire system to view.

The informational windowpanes displayed within the workstation screen can be customized by the Administrator. These panes can be positioned anywhere on the screen, allowing the user to customize the display. Workstations configured to use dual monitors provide additional space for display of these informational panes.

A default workstation display screen is shown in Figure 6.1. Each feature is described in Table 6.1.

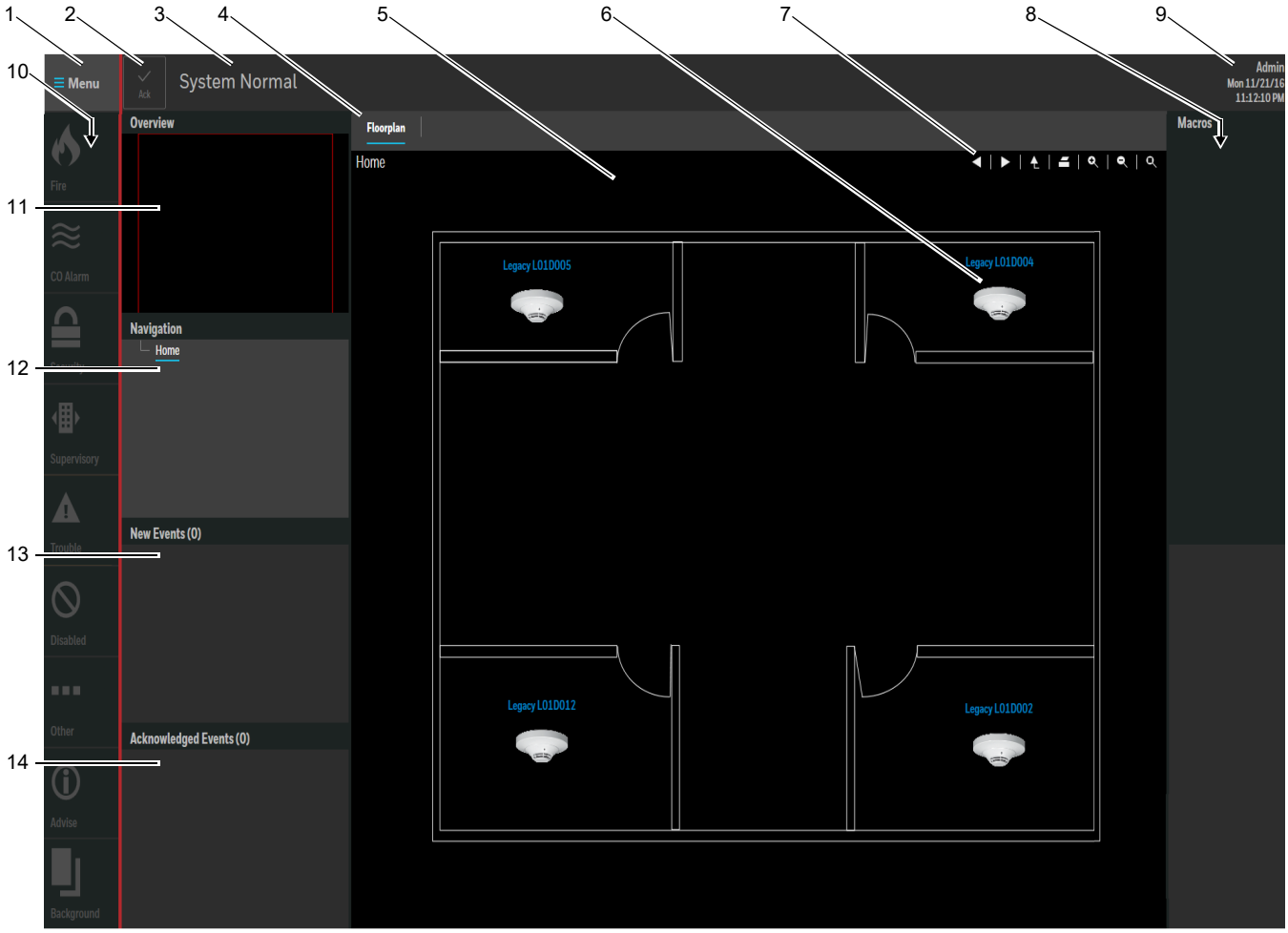


Figure 6.1 Example Workstation Screen

Table 6.1 Workstation Screen Descriptions

Item	Feature	Description
1	**Menu**	Click to display available workstation sub-menus. Refer to 6.4.1, "Workstation Menus" for additional information.
2	**Ack/Block Ack Button**	Click to acknowledge an individual new event (Ack) or group of new events (Block Ack). The button to be displayed is configured by the Administrator in the Options menu (Menu > Configure > Options).
3	**System Status Bar**	Displays the current status of the system. During events, the event status class indicator, event status class color, and event command buttons/indicators are displayed. Refer to 6.6, "When a New Event Occurs".
4	**Open Windows Bar**	Displays a tab for each open workstation application window. Click tabs to display the application windows. Hover over the tab and click the “X” to close the application.
5	**Floor Plan Window**	The floor plan window displays a building floor plan as background with graphic elements showing where devices and other features are located. It serves as the primary source for visual feedback for the location of an off-normal event in the system. The floor plan window’s title identifies which area of an system that is currently being displayed.
6	**Graphic Element**	Includes device icons (shown), navicons, and labels that provide the user with important system information. Refer to 6.4.2, "Graphic Elements" for additional information.
7	**Tool Bar**	**Previous Screen** – Displays, in order, the floor plan screens that were viewed before the currently displayed floor plan screen. **Example:** The user views screens 1, 3, 6, and 8. From floor plan 8, with each click of this button, the user goes back, in order, one previously viewed floor plan screen (e. g. screens 6 to 3 to 1). **Next Screen** – Displays, in order, the next floor plan in a sequence of viewed floor plans. **Example:** The user uses the previous screen button to go back from floor plan 8 to 6 to 3 to 1. From floor plan 1, with each click of this button, the user advances, in order, one previously viewed floor plan screen (e.g. screens 3 to 6 to 8). **Up One Level** – Displays the next floor plan above the current floor plan in the navigation tree hierarchy. **Print Current Screen** – Prints the floor plan display to the currently selected printer. **Zoom In One Level** – Increases the zoom of the floor plan display by 50% (ranges from 100% to 3700%). **Zoom Out One Level** – Decreases the zoom of the floor plan display by 50% (ranges from 100% to 3700%). **Zoom Full Image** – Display current displayed floor plan at 100%.
8	**Docked Panes**	Panes for various workstation functions can be docked along the side of the floor plan window (or on another monitor if configured for dual monitors) for easy access. These panes can be dragged to other screen locations. Hover over the pane label and click the “X” to close the pane.
9	**Current User**	Displays the name of the current user. Left-click the user name to log out or change users.
10	**Event Status Class Column**	Icons represent each event status class except those that have been configured to be hidden via the configuration tool. The icons are normally gray, but when there is an event, the icon displays in its configured event status class color along with the number of active events of that class. Click the icon to display a tabular list of all the points currently in that status. Click the **Print** button to print the displayed event list at the local printer (if installed). Refer to 6.4.5, "Event Status Class Icons".
11	**Overview Pane**	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 pane is helpful when a zoom-in scale is selected for the workstation floor plan. The overview pane does not display graphic elements.
12	**Navigation Tree Pane**	Displays the ONYXWorks system in a structured hierarchy form similar to Microsoft’s Windows Explorer. Refer to 6.4.3, "Navigation Pane".
13	**New Events Pane**	Displays a 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 “Acked” notation until acknowledged at the workstation. Refer to 6.4.4, "Events Panes".
14	**Acknowledged Events Pane**	Displays a list of events acknowledged by the current user. Events remain on this list until the event is cleared.

6.4.1 Workstation Menus

The following table describes the menus associated with the ONYXWorks Workstation application. To view the menus, click **Menu** located at the top-left of the screen (see Figure 6.1).

Table 6.2 Workstation Menus

Menu	Sub-Menu	Description
File	**Login**	Opens the login window for user login/logout.
	Add History Entry	Allows the user to manually add an entry into the system history database.
	Print Events	Appears only if the workstation detects an installed Windows printer. Allows the user to print a tabular list of local events.
	Launch Applications	Opens gateways configured to operate with the workstation (e.g. NFN Gateway and Receivers Gateway).
	Back Up System Data	When the destination of the backup is located on a drive that is accessed across the Ethernet network, the drive must be mapped to the workstation PC using the Windows drive mapping function. Upon initiating this procedure, the user must select or create a folder (C:\Facilities Monitoring\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 external media. **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 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.
	Compact and 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.
	Import System Data	This procedure updates the system data in the local workstation to match the system data from another workstation.
	Export System Data To All Workstations	This procedure updates the system data on all networked workstations to match the system data on the local workstation. **Note:** Export is achieved by selecting Export To All Workstations on the source workstation and then selecting Import System Data on the destination workstations and providing the source IP to import the exported data.
	Exit	Allows the Administrator to exit the workstation application.
View	**History**	Opens the History window where the user can view, back up, and clear system history. Automatic backup settings are made on the Options window's General tab.
	System Explorer	Opens the System Explorer window displaying a Windows-type navigation tree showing local system layout. Clicking on a navigation tree label displays additional details. Provides a system search function.
	Background Activations	This option is only displayed when the Background event icon is hidden via the Colors and Sounds window in the configuration tool. Click this option to display a list of background activations.
	Armed/Disarmed Points	Opens a window that displays all armed/disarmed points in the system. Displays a list of all points with their control profile, status, and description.
	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.
	Test Monitoring	Allows the user to view test monitoring events. Refer to 7.5, "Test Monitoring" for additional information.

Table 6.2 Workstation Menus *(Continued)*

Menu	Sub-Menu	Description
View *(Continued)*	**Security Log**	Displays only if an Administrator is logged in. Displays a chronological log of certain workstation events considered important for cybersecurity purposes. Refer to 7.6, "Security Log" for additional information.
	Overview	Displays the Overview pane on the workstation screen.
	Navigation Tree	Displays the Navigation Tree pane on the workstation screen.
	New Events	Displays the New Events pane on the workstation screen.
	Acknowledged Events	Displays the Acknowledged Events pane on the workstation screen.
	Floorplan	Displays system floor plan view on the workstation screen. The floor plan is configured using the configuration tool.
	Emergency Audio	Displays only when the workstation is licensed for the NOTIFY-IP audio feature. When selected, the emergency audio pane will be displayed for use by an authorized operator to activate emergency audio paging.
	General Audio	Displays only when the workstation is licensed for the non-UL audio feature. When selected, the general audio pane will be displayed for use by an authorized operator to activate non-emergency audio paging.
	Macros	Displays the Macros pane on the workstation screen from which authorized users can activate macros.
	Smoke Control	Displays only when the key is configured for the Smoke Control feature. Opens the smoke control building schematic window.
	Smoke Control Operations	Displays only when the key is configured for the Smoke Control feature. Displays the Smoke Control Operations pane on the right-hand side of the workstation window. Smoke control operations can be run and monitored from the operations widgets in the pane.
	Smoke Control Device Status	Displays only when the key is configured for the Smoke Control feature. Displays the Smoke Control Device Modules Status window on the right-hand side of the workstation window. Displays the status of the modules associated with fans, dampers, and operations.
	Restore Default Layout	Restores the workstation screen to its default layout. **Note:** An alternate method is to right-click the workstation icon in the Windows task bar and select “Restore Default Layout.”
Action	**Open Verifire Tools**	Allows the user to open a Verifire Tools database for editing, create a new database, or browse for a database located on another workstation on the network.
	Signs	Displays a list of connected LED signs and their status. Provides a means to override the message on the selected sign. **Note:** Overriding the message on a sign may violate UL standards.
Configure	**Launch Configuration Tool**	Launches the ONYXWorks Configuration Tool application.
	Control Profiles	Displays only if “Use Node Control” is set to “Yes” in the Options window. Opens the Control Profile window where authorized users can activate/deactivate control profiles configured in the configuration tool.
	Monitoring Profiles	Opens the Monitoring Profile window where authorized users can activate/deactivate monitoring profiles configured in the configuration tool.
	NetLogic	Displays only if “Enable NetLogic” is set to “Yes” in the Options window. Opens the NetLogic Window.
	Options	Opens the Options window that allows the user to configure local workstation settings. Refer to 5.3, "System Options Settings".
	Test Monitoring Configuration	Opens a window that allows the user to select nodes which they want to stop monitoring for test and maintenance purposes. Refer to 7.5, "Test Monitoring" for additional information.

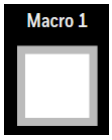
Table 6.2 Workstation Menus *(Continued)*

Menu	Sub-Menu	Description
Help	**About**	Opens a splash screen that displays information about the ONYXWorks Workstation application (version, language, legal information, etc.).
	Secure Windows	Opens a document describing how to disable and enable the ability of the user to access the windows taskbar and use keyboard shortcuts (e.g. Ctrl + Alt + Delete).
	Generate Local Machine Report	Generates a report about the computer and installed software. It includes PC hardware and operating system information, key information and software versions.
	Advanced Diagnostics	Used for informational/diagnostic purposes.

6.4.2 Graphic Elements

Graphic elements provide information to the user about different features displayed on the workstation screen and allows the user navigate between different areas of the fire system. They are added to the floor plan and configured using the workstation configuration tool (refer to 4.4.3, "Configuration Tool Layout"). If configured to do so, a descriptive point label displays above the icon. Typical graphic elements are described in the following table.

Table 6.3 Graphic Element Descriptions

Type	Example	Description
Point Icons		Point icons represent a physical, addressable device on the system. Examples of point icons are fire panels and fire detection devices. If the point's status becomes off-normal, its icon flashes in the color of the event status class. A paper clip symbol ( ) indicates that there is linked media associated with the device that can be accessed by right-clicking the icon. Left-clicking on a point icon displays additional point information. Right-clicking on a point icon displays command options. Refer to 6.4.2.2, "Point Right-Click Command Options".
Navigation Icons		Navigation icons (navicons) represent a method to navigate between workstation floor plan areas to find points or an event. Navicons change color to match the off-normal event that is reported to the workstation. Click on the colored navicon to navigate to the location of the event.
Macro Buttons		Authorized users can click on a macro button to activate a configured macro in the workstation system. Refer to 4.4.5, "Macros" for additional information.
Information Labels		Clicking an information label displays information about a feature on the workstation floor plan. A paper clip symbol ( ) indicates that there is linked media associated with the label that can be accessed by right-clicking the icon.
Audio Button		When NOTIFY-IP is enabled, an audio button can be added to the workstation floor plan. Clicking on an audio button activates an associated audio group page.

6.4.2.1 Linked Media

Linked media provides important information during monitoring such as a photograph, text document, video, or a sound clip. Linked media can be associated with point icons and information labels using the configuration tool. It is identified with a paper clip symbol ( ) next to a graphic element. An example would be to provide firefighters with a list of hazardous materials stored on-site.

Several types of media files may be linked to the node/point. One of each type media can be used. Linked media may include the following:

- A text file to give specific information or instructions to the user (.TXT, .RTF).
- A graphic image (.BMP, .GIF, .JPG, .PNG).
- A sound file providing audible information or instructions (.WAV).
- A video file (.AVI).

6.4.2.2 Point Right-Click Command Options

Factory-defined and Administrator-assigned control commands are available for all point icons. The commands are accessed by right-clicking on the icon or its navigation tree label.

Control commands are available only when the user has a node control and security profile that allows it. Node control is signified by the presence of a flag icon ( ) next to the icon. 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.

Addressable devices have right-click menus that provide the user with a list of available device-specific command options, The choices that display depend on the type of device, the situation, and the user's security permissions. If the option is grayed out with the text "Control Required" next to it, it indicates that the workstation does not have control of the device.

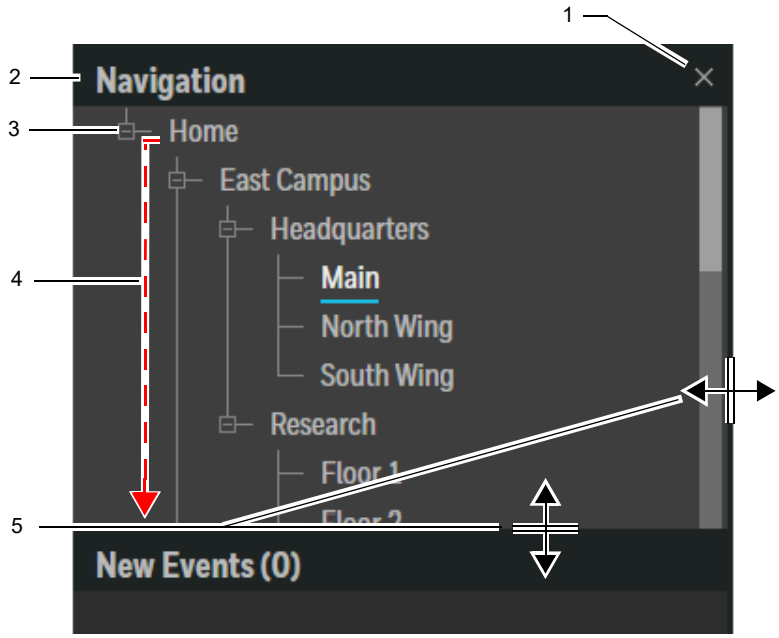
The following table describes default right-click features and command options:

Table 6.4 Default Node/Point Right-Click Options

Option/Feature	Description
Point Description	The top line of the menus displays the device description designated by the Administrator or read from a panel on the system.
Enter User Response	Allows the user to select from a drop-down 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: • Dispatched Personnel To Investigate • Response Personnel on Scene • Device Undergoing Test • Device Testing Completed • Contacted System Contractor • Faulty Device • Replaced Device • Preventative Maintenance • Custom - User can create a customized response.
History of Device	Opens the History window that displays the history information relating to the selected device.
Clear Event	Only active when the point is in an off-normal condition. Deletes the event from the workstation and the event is removed from the event list.
View... (Text, Picture) or Play... (Audio, Video)	If the device icon has a paper clip symbol ( ) displayed next to it, a choice to view or display the media displays in the list of choices.

6.4.3 Navigation Pane

The navigation pane displays the ONYXWorks system in a structured, hierarchical format. Figure 6.2 describes navigation pane features.



Item	Feature	Description
1	Pane Operator Buttons	= Close Pane (hover cursor over a title bar to view) = Maximize Pane (displays when pane is floating) = Restore Pane (displays when pane is maximized)
2	Title Bar	Name of the pane. Use as a handle for moving the pane.
3	Level Indicator Box	Click "+" to expand the level. Click "–" to collapse the level. Right-click the box to expand all or collapse all levels.
4	Navigation Tree	Hierarchical structure of the fire system (buildings, floors, etc.). The currently displayed location is underlined in blue.
5	Pane Boundaries	Click, hold, and drag (up-down, left-right) to change the pane size.

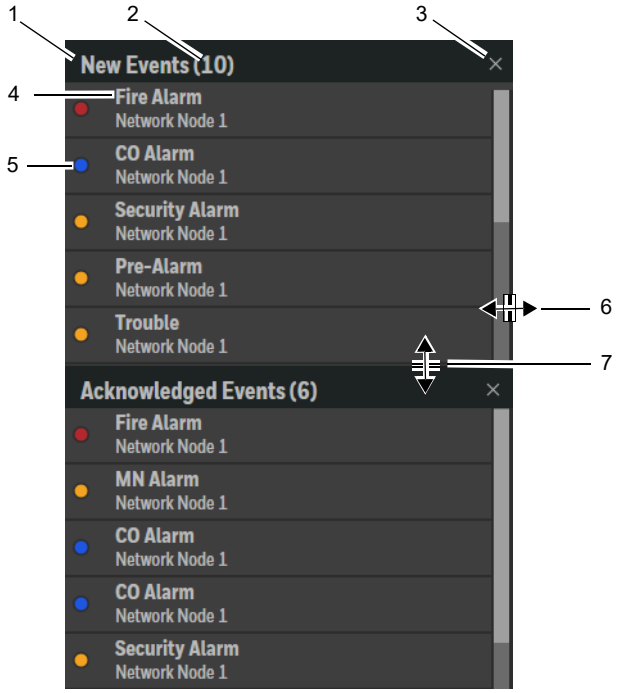
Figure 6.2 Navigation Pane Overview

6.4.4 Events Panes

The New Events and Acknowledged Events panes provide event information to the workstation user. They display by default when the workstation application is opened.

When an event is reported to the workstation, its label displays in the New Events pane with a corresponding event status class colored indicator. An audible alarm also sounds at the workstation.

Once an event is acknowledged, the event either moves to the Acknowledged Events pane or is removed from the workstation. The event is cleared from the Acknowledged Events pane when the alarm or trouble condition is no longer present.



Item	Feature	Description
1	Title Bar	Pane title. Use as a handle for moving the pane.
2	Event Count	Number of events that are currently active.
3	Pane Operator Buttons	= Close Pane (hover cursor over a pane title bar to view) = Maximize Pane (displays when pane is floating) = Restore Pane (displays when pane is maximized)
4	Event Label	Label with event status class and point information as configured in the configuration tool.
5	Event Status Class Indicator	Displays the configured event status class color if the workstation has node control of the point.
6	Column Boundary	Click, hold, and drag to the right to widen the entire column of docked panes. Drag all the way to the right to view tabular information about new and acknowledged events.
7	Pane Boundary	Click, hold, and drag up or down to change the vertical pane size.

Figure 6.3 Event Pane Features

6.4.4.1 New Events Pane

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 small flag icon will appear to the left of the event label.
- If the event is unreliable (meaning it was reported while a gateway or node was in fault), an asterisk (*) is displayed prefixing the event.
- If there is linked media configured for the point, a small paper clip symbol appears to the left of the event label.

6.4.4.2 New Events Buttons and Indicators

Buttons and indicators display in the system status bar the top of the workstation screen to allow the user to respond to, and obtain information about, new events reported to the workstation. These buttons and indicators are described in the following table.

Table 6.5 New Events Buttons and Indicator Definition

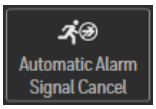
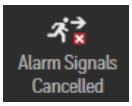
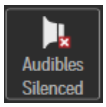
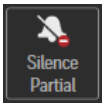
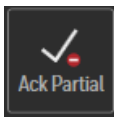
Button	Description
	Displays only in Canada Protected Premises Control Unit (PPCU) modes. Available to users with point control and evacuate permissions. Allows the user to initiate an alarm signal to every node on the network.
	Displays only in Canada PPCU modes. Available to users with point control and silence permissions. Displays only when a two-stage alarm is in the first stage. Prevents the device from going into second-stage alarm.
	Displays only in Canada PPCU modes. Displays only when the alarm signal has been canceled for a device in the first stage of a two-stage alarm.
	Available to all users with client control. Acknowledges the most recent event.
	Available to users with client control. Available in PPCU mode and in PRU mode when enabled (Menu > Configure > Options), acknowledges all new events at one time.
	Displays in PPCU mode. Also displays when mass notification activations are present. Silences all audible alarms. In PPCU mode, it causes the Audibles Silenced button (see below) to display that when clicked, opens a list of the silenced fire panels.
	**Audibles Silenced** - Displays when any panel on the network has been silenced. Available to all users. When clicked, it opens a list of all silenced fire panels.
	Displays in all Canadian modes when a panel has automatically silenced itself.
	Displays only in PPCU mode. Available to users with point control and reset permissions. Sends a reset command to the panels.
	Displays only in PPCU mode when Mass Notification mode is set to Higher Than Fire. If a mass notification alarm is active, this icon will display to notify the user that all fire monitoring has been suppressed due to the MN alarm.
	Displays only in Canada PPCU+DCC mode. Available to users with point control. It requests control of the fire network. Once the workstation is in control, it can send commands to the panels.
	Displays only in Canada PPCU+DCC mode when the Workstation has full control of the fire network.
	Displays only in Canada PPCU+DCC mode when the Workstation has control of some, but not all, panels on the fire network.

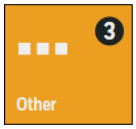
Table 6.5 New Events Buttons and Indicator Definition *(Continued)*

Button	Description
	Displays only in Canada PPCU+DCC mode when the workstation has no control of the fire network.
	Displays in PPCU mode with mass notification enabled. Available to users with point control and silence permissions. Displays when the workstation has partial control of the network. Sending the silence command only silences the panels for which the workstation has control.
	Displays in PPCU mode with mass notification enabled. Available to users with point control and reset permissions. Mass notification events and supervisories clear and any fire event silenced by the mass notification alarm becomes unsilenced. Displays when mass notification activations are present on the network. If a mass notification page is in progress when the MNS reset button is clicked, the mass notification alarm returns. If a device with an equal or higher priority is paging, the workstation is blocked from control. Priority for mass notification devices is as follows, highest to lowest: • ACU - Autonomous Control Unit • Local Operating Console (LOC) • Command and Control Station (CCS). The workstation is considered a CCS.
	Displays in PPCU mode with mass notification enabled when a mass notification event is present on the system. Available to users with point control and reset permissions. Displays when the workstation has partial control of the network. Sending the reset command only resets the panels for which the workstation has control. Mass Notification events and supervisories clear and any fire event silenced by the mass notification alarm becomes unsilenced.
	Displays in PPCU mode with mass notification enabled when there are no mass notification events on the system. Available to users with point control and reset permissions. Displays when the workstation has partial control of the network. Sending the reset command only resets the panels for which the workstation has control.
	Displays in PPCU mode with mass notification enabled. Displays when the workstation has partial control of the network. Sending the acknowledge command only acknowledges the event if the workstation has control of the panel.
	Displays in PPCU mode with mass notification enabled. Displays when workstation has partial control of the network. Sending the block acknowledge command only acknowledges the panels for which the workstation has control.

6.4.5 Event Status Class Icons

The event status class icons (grayed out when there are no events) display in the configured status class color when an event is reported to the workstation. Certain icons may be hidden if so configured by the administrator in the configuration tool (**Graphics > Colors and Sounds**). If an event status class is hidden, it comes in as Other. The numbers in the circles indicate how many events of that status have been reported. The affected icon remains highlighted until all off-normal conditions have been resolved.

Table 6.6 Event Status Class Icon Definition

Type	Example	Can Be Hidden?	Definition
Fire		Yes	Events issued by fire protection related devices such as pull-stations, smoke detectors, and sprinkler systems.
CO Alarm		Yes	Events issued by carbon monoxide detection devices on the system.
Security		Yes	Events issued by security related devices such as motion detectors, glass break detectors, and door contacts.
Supervisory		Yes	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		Yes	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.
Disabled		Yes	Events that indicate disabled points on the system.
Other		No	Other events such as mass notification alarms.
Advise		No	A condition that is an administrative event. This is not a life-safety or security event, but an internal warning of a condition that may need attention, such as the history database reaching the maximum number of entries.
Background		Yes	The backgrounds status class contains events which do not appear in the New or Acked event lists. These events are panel dependent, but may include output device activations.

6.5 Repositioning Windows

6.5.1 Overview

Administrators can customize the location of workstation windows by relocating them from their default positions as follows:

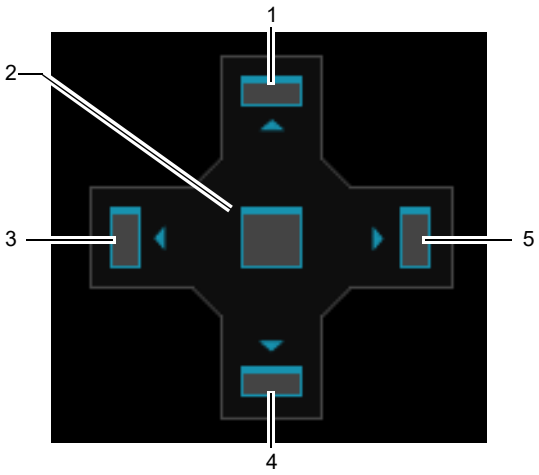
- Click and drag the window title bar to its new location and drop it into position. The window floats over the screen.
- Use the docking guide to dock the window in relation to another window on the screen.

To reset the workstation screen to show its default layout, go to **Menu > View > Restore Default Layout**.

6.5.2 Using the Docking Guide

The docking guide allows the Administrator to relocate a workstation window in relation to another window. Operate the docking guide as follows:

1. Click and drag the window's title bar out of position. The docking guide displays.
2. Continue dragging the window over the window to which it will be docked (destination window).
3. Hover the cursor over the docking guide in one of the positions described in Figure 6.4. A blue outline displays where the window will be docked in relation to the destination window.
4. Release the mouse button. The moved window is docked into its new position.

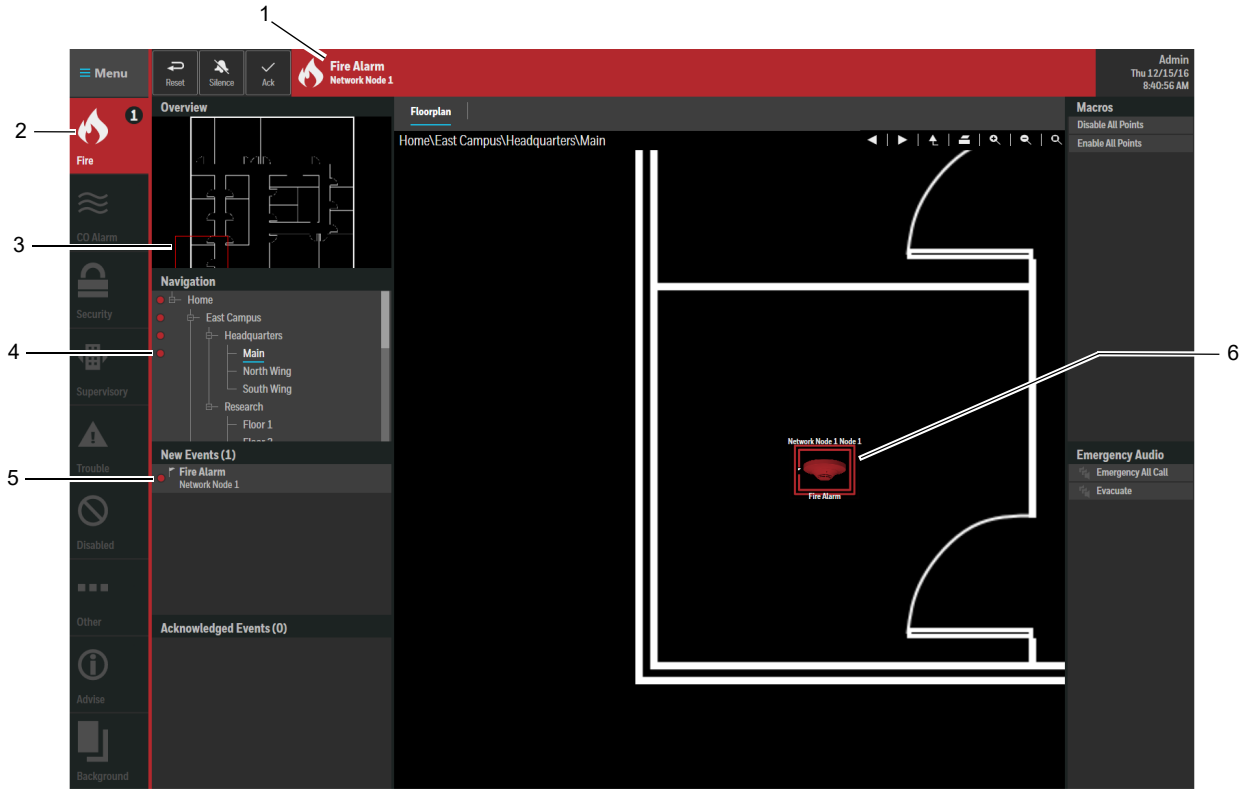


Item	Description
1	Docks the window above the destination window.
2	Docks the window on top of the destination window. Creates a tab group with the destination window.
3	Docks the window to the left of the destination window.
4	Docks the window below the destination window.
5	Docks the window to the right of the destination window.

Figure 6.4 Window Docking Guide

6.6 When a New Event Occurs

When an event is reported to the workstation, the actions described in Figure 6.5 simultaneously occur. In addition, a sound is emitted annunciating the event.



Item	Description
1	System Status Bar displays the event icon of the highest priority event. Event command buttons/indicators are displayed.
2	Event Status Class Column displays event icon(s) of new events. Number of devices in alarm for each event status class is shown. If the event icon has been configured to be hidden via the configuration tool, the Other event icon will activate. Refer to 6.4.5, "Event Status Class Icons"
3	Red box in Overview Pane indicates the location of event on the floor plan.
4	Navigation Pane displays the location of the event in a navigation tree with its event status class color indicator next to the label. Refer to 6.4.3, "Navigation Pane".
5	New Events Pane displays the device's event label with its event status class color indicator. Refer to 6.4.4, "Events Panes".
6	The icon for the device in alarm displays event status class color. Animation indicates the highest priority alarm.

Figure 6.5 Example - Fire Event in Progress (PPCU Mode)

6.7 Look-Ahead Enable Feature

The Look-ahead enable feature is available only on systems using NFS2-3030 panels. This feature alerts Administrators and users with point control privileges if a disabled point or disabled monitor module they are attempting to enable is in active alarm. Details of this feature are described in the following table.

Table 6.7 Look-Ahead Enable

Location	Action	Result
Floor Plan Detector and Monitor Module Icons	Right-click the icon and select “Enable Point If Not Active”.	• If point is not active - Point is enabled. • If point is active - Point is not enabled. An Advise event displays. Right-click the event status class icon to view the event details.
Floor Plan Macro Buttons	Click the button to execute the macro.	• If no points are affected by the macro are active, the macro is executed. • If a point affected by the macro is active, an Advise event displays for the point. The macro will still run on all non-active points. Right-click the Advise event status class icon to view the event details. **Note:** The macro must be configured for “Enable if not Active/Disable” in the *Multi-Function* field in the configuration tool (Monitor > Macros).
Workstation Macros Window	Click the macro label to execute the macro.	
Network Explorer	Right-click the point label and select “Enable Point If Not Active”.	• If point is not active - Point is enabled. • If point is active - A pop-up message displays saying the point is not enabled because it is active.

Section 7 Data Management

7.1 Workstation Database Backup and Restore

7.1.1 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. In the workstation application, go to **Menu > File > 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**.

7.1.2 Restoring a Backed-Up Database

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

1. Shut down all fire system applications including gateways.
2. In the workstation application, go to **Menu > File > Restore System Data**. The Restore System Data dialog box 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 7.1.1, "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.

7.2 History Window

7.2.1 Overview

The History window allows the user to view all of the events that are currently stored in the workstation history database. The user can view this information in either an Event Grid or a System View screen format. A set of filters can be applied to the list of events shown to allow the user to view specific event status classes, points, and events for specific dates.

The events list can be the current history database or a history database that was previously backed-up and stored in an archive on the workstation PC.

To access the History window in the ONYXWorks application, go to **Menu >View > History**. By default the Event Grid screen is displayed.

7.2.2 Back-up History Database

The history database is backed up at an interval set by the Administrator using the **Menu > Configure > Options** menu in the workstation application (refer to 5.3.1, "General Tab"). Open a back-up history database as follows:

1. Open the History window.
2. Go to **File > Open Database**. The Select Database dialog box displays.
3. Double-click on the desired history database (.HIS). The back-up history database opens.

To return to the current most recent database, close and then reopen the History window.

7.2.3 Viewing the History Window

The History window may open within the screen area allowed for the floor plan and be too small in size to clearly view the information. To maximize the view of the History window do the following:

- Reduce the size of, or close, windows on the screen, or
- Undock the window from its default position and click the full screen button () at the top-right corner of the window, or
- For dual monitor configured workstations, drag the window to another monitor and maximize.

Use the scroll bars to view any data columns not visible in the window.

7.2.4 Event Grid Screen

A typical Event Grid screen is shown in Figure 7.1 and is described in Table 7.1.



Figure 7.1 Event Grid Screen

Table 7.1 Event Grid Screen Features

Item	Feature	Description
1	**Menu Bar**	Refer to Table 7.2 for descriptions.
2	**Filters Pane**	Toggle this pane on/off via the View menu. **Queries** - Click the down arrow to view a list of available saved queries. Refer to 7.2.5, "Creating, Renaming, and Deleting Queries" for additional information. **Location:** • **Point Tab** - Navigation tree is displayed as nodes and points on the network. • **Screen Tab** - Navigation tree is displayed as screens on the network. **Applied Filters** - Displays the currently applied data filters or queries.
3	**Record Viewer**	Toggle this pane on/off via the View menu. Displays the icon for the device type with its unique device label and the color of its event status class. Includes these tabs: **Event Tab** - Displays event information for the device selected in the grid. **Point Tab** - Displays network, node, and point information for the device selected in the grid. **Screen Tab** - Displays a hierarchical map of the selected device's location on the network using workstation screen name. Includes the option to view child screens. **Statistics Tab:** • **SeqNo** - The numerical order of the event on the event grid. • **Event Count of Point** - Number of events logged for the selected point. • **Last Event on Point** - The date and time the last event occurred for the selected point.

Table 7.1 Event Grid Screen Features *(Continued)*

Item	Feature	Description
4	**Event Grid**	Displays an event list using filters applied by the user. Columns available to display may include the following. Information displayed varies on the event and point type. • Event Status Class Indicator (in configured color) • Status Label • ACK - A check mark indicates that the event was acknowledged. • Received Time Local - When event message was received (Local Time) • Actual Time Local - When event occurred (Local Time) • Actual Time UTC - When event occurred (Universal Coordinated Time) • Action Description - The action taken by the user. • Analog Information • Card Information • Seq No - Event sequence number in the workstation history database. • Event Description • Network Description • Node Type • Network Number • Node Address • Node Alias • Point Address • Point Alias • Point Type • Point Description • Status Class - (Normal, Advise, Trouble, Other, etc.) • Screen (device's workstation screen location) - Change the order of a column by dragging the heading to its desired location. - Resize a column by hovering between column headings until a horizontal arrow (⇔) displays and then dragging to the desired width. For additional column and row display options, refer to Table 7.3.
5	**Window Buttons**	- **Minimize** - Click to minimize the window. Only visible when the window is not docked with another window. - **Full Screen** - Click to maximize the size of the window. Only visible when the window is not docked with another window. - **Close -** Closes the window.
6	**Information Bar**	Displays the number of records currently displayed.
7	**Export Button**	Allows the user to export the historical data as a comma delimited (.csv) file.

Table 7.2 Event Grid Screen Menus

Menu	Description
File	• **Open Database** - Allows the user to open a previously saved event history database. • **Print Displayed Records** - Opens a print dialog box which provides options for printing of the event grid. • **Export to Delimited Text** - Allows the user to export the historical data as a comma delimited (.csv) file. • **Back Up And Clear History Database** - Backs up the current history file and clears the Event and System view grids.
View	• **Refresh** - Refreshes the event list to include the most recent events received. • **System** - Opens the System View screen (7.2.6, "System View Screen") that shows how the events displayed by the History window are distributed over the fire system. This view option is only available when the Event Grid view is displayed. • **Select Columns To Show** - Opens a dialog box from which the user can select which informational columns appear in the event grid. • **Show All Columns** - Displays all columns. (Clicking this option also automatically checks all the boxes in the Select Columns To Show dialog box.) • **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. With the Record Viewer 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 Filters pane on the left side of the event list. **Note:** Hiding the filter pane does not hide any events.

Filter	• **Time/Date** - Allows the user to filter the events by time or date as follows:
	  • **Time** - Select whether the times displayed are Actual Time Local, Actual Time UTC (Coordinated Universal Time), or Received Time Local. The events displayed fall within the specified time range as calculated by the selected time scheme.
	  • **Filter By**- Options include Today, Yesterday, This Month, Number of Previous Days, and Date Range.
	• **Event Status** - Allows the user to filter the events by event status class.
	• **Save Current Query** - Allows the user to name and save the current query for later use. The name of the saved query is added to the Queries drop-down list in the Filters pane.
	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** - Displays only if a query is displayed in the *Queries* field. Allows renaming of the query displayed in the *Queries* field.
	• **Delete Selected Quer**y - Displays only if a query is displayed in the *Queries* field. Deletes the query appearing in the *Queries* field.

Table 7.3 Event Grid Column and Row Options

Option Type	Description
Column	**Right-click** on a column heading 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 column heading and click the up/down arrows (⇳) to sort the column in ascending/descending order.
Row	**Right-click** on any row to display the following options: • **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 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 *after* 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 *before* the selected event are displayed. • **History of Device** - Displays the history for the device on the selected row.

7.2.5 Creating, Renaming, and Deleting Queries

Create a query in the Event Grid screen as follows:

1. Set the desired filters using the Filter menu. The applied filters display in a hierarchical format in the Filters pane.
2. Go to **Filter > Save Current Query**. The Save Query dialog box displays.
3. Enter a unique name for the query and click **OK**. The query name appears in the Queries drop-down list.

Rename a query as follows:

1. Select the query to be renamed from the Queries drop-down list in the Filters pane.
2. Go to **Filter > Rename Selected Query**. The Rename Query dialog box displays.
3. Change the name of the query in the field provided and click **OK**.

Delete a query as follows:

1. Select the query to be deleted from the Queries drop-down list in the Filters pane.
2. Go to **Filter > Delete Selected Query**. The query is removed from the list of available queries.

7.2.6 System View Screen

The System View screen (Figure 7.2) allows the user to view the system status and history at a glance in a tabular format. Features are described in Table 7.4. If not already displayed, go to **View > System** in the Event Grid screen menu bar.

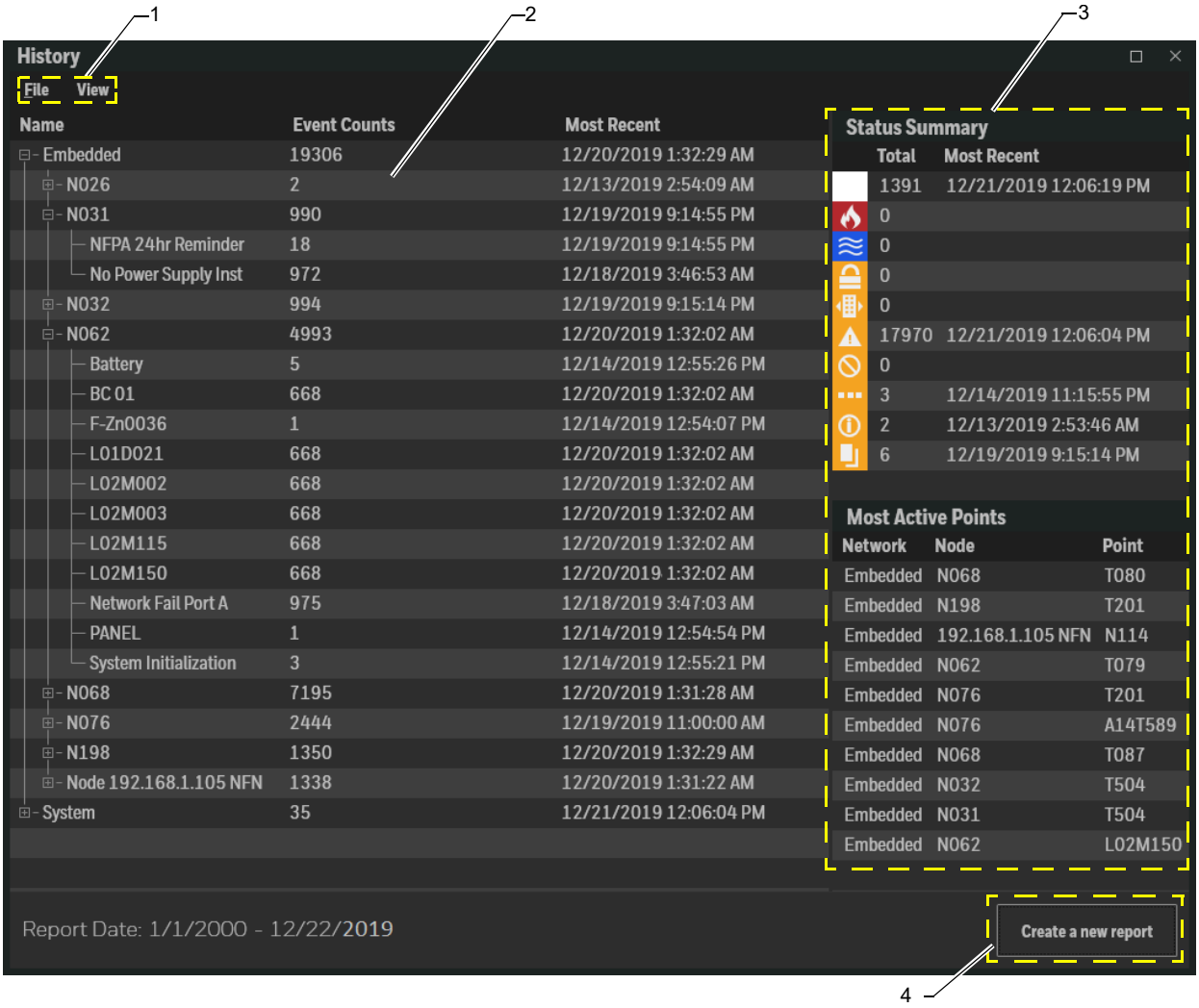


Figure 7.2 System View Screen

Table 7.4 System View Screen Features

Item	Feature	Component	Description
1	**Menu Bar**	File	• **Open Database** - Open a previously saved event history database. • **Back Up And Clear History Database** - Backs up the current history file and clears the System View and Event View grids.
		View	• **Refresh** - Refreshes the screen to include the most recent information. • **Event Grid** - Displays the Event Grid screen.
2	**Event List**		Displays system event history as filtered by the settings in the Device Report dialog box. Columns include a system navigation tree, event count, and the date and time of the most recent event. Double-clicking a row brings up the Event Grid view for that node or point.
3	**Statistics Pane**		The statistics pane provides summaries of events on the network as filtered by the setting in the Device Report dialog box.
		Status Summary	Displays the total number of events of each event status class (by icon) and the date and time of the most recent occurrence.
		Most Active Points	Displays the location (network, node, point) of the ten most active points in the current history database.
4	**Create a New Report Button**		Displays the Device Report dialog box where the user can set filters.
		Start Time	Click the calendar icon to select the start date of the report.
		End Time	Click the calendar icon to select the end date of the report.
		Tree View	Allows the user to select how the navigation tree is shown on the screen. • **Points** - Displays the event list in navigation tree format as points and nodes on the network. Nodes and points are alphanumerically listed. • **Screen** - Displays the event list in navigation tree format by location on workstation screens.
		Show points with no events	• **Yes** - Points with no events are displayed. • **No** - Points with no events are not displayed (default).
		Event Filter Settings	Check the checkboxes for the types of events to display in the event list.

7.3 System Explorer Searches

The System Explorer allows the user to search for and locate system devices as follows:

1. In the workstation application, go to **Menu > View > System Explorer**. The System Explorer window opens.
2. Click inside the **Search** field and type the search text. As the search term is entered, results matching the term are displayed in tabular format under Point, Point Type, and Description headings.
3. If the device is associated with an icon on the system floor plan, double-clicking the desired search result causes the workstation to auto-navigate to, and center, the icon in the floor plan window.
4. Click the '**X**' in the upper-right corner of the window to close the System Explorer.

7.4 Walk Test Utility

7.4.1 Overview

The walk test utility allows the user to capture and record information received during testing of points on the system monitored by the workstation. When a panel is put into walk test mode, all events generated at the panel are sent to the workstation as "test" events. The events created are logged in a Walk Test Point List and in the workstation history database, but are not reported as actual alarms. The walk test utility is available on the following FACPs:

- NFS-320
- NFS-640
- NFS2-640
- NFS-3030
- NFS2-3030

With the exception of system trouble events, a walk test cannot be conducted while a workstation has active alarms.

7.4.2 Walk Test Procedure

The walk test is performed with the workstation in floor plan view with no active alarms. Perform a walk test as follows:

1. If not already open, open Network Explorer as follows:
   a. Display a menu of options using one of the following methods:
      - Using the workstation navigation tree, select a floor plan level containing the device to be tested. Then, right-click on a device icon in the floor plan.
      - Right-click on any event in the New Events or Acknowledged Event windows.

   b. Select **Network Explorer**. The Network Explorer window displays.
2. In the Panels pane, right-click on the node to be tested and select **Walk Test**. The Walk Test window displays (see Figure 7.3).

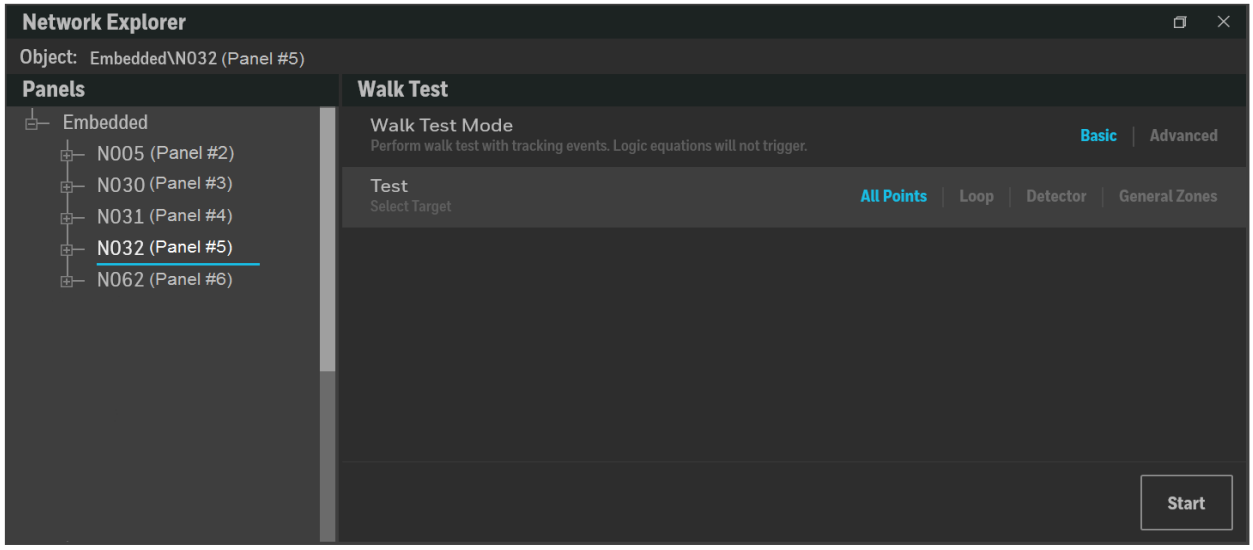


Figure 7.3 Walk Test Screen

3. Configure the walk test using the options described in the following table. For NFS-3030 and NFS2-3030 panels, select the desired test target from the options displayed.

Table 7.5 Walk Test Options

Feature	Option	Description
Walk Test Mode	Basic	Default. The walk test is performed with tracking events. Logic equations do not trigger. Select this option when testing devices individually.
	Advanced	An audible walk test is performed with latching events. Logic equations trigger. Select this option when testing devices and their associated logic equations.
Test		The available test target options depend on the type of panel under test.
	All Points	Default. Select to test all points on the node.
	Loop	Click the tab and select the checkboxes for the loop(s) on the node to test.
	Detector	Click the tab and use the up/down arrows to specify the loop and point address of the detector to test. ***Example:*** For a detector at L0**1**D0**10**, set the loop to '1' and set the point address to '10'.
	General Zones	Available only when Basic mode is selected. Click the tab and use the up/down arrows to specify the network zone to test.
Start Button		Click to start the walk test.

4. Click **Start**. A "walk test in progress..." message displays in the walk test screen. System troubles are displayed in the New Events pane for each node currently undergoing walk test. The following table describes the on-screen buttons.

Table 7.6 Walk Test in Progress - Button Definitions

Feature	Description
Stop Button	Stops the walk test in progress.
Start Button	Active after the walk test is stopped. Restarts the walk test in progress.
Previous Button	Active after the walk test is stopped. Returns to the previous walk test screen.

5. Create events for each device under test for the selected node.

   Walk test events are listed in the walk test points list (refer to 7.4.3, "Walk Test Points List") and recorded in the workstation history database (refer to 7.2, "History Window"). Filter the workstation history database for walk test events by selecting **Walk Test Events** from the Queries drop-down list.

6. To take the node out of walk test, perform the following:
   a. In **Network Explorer**, right-click the node under test in the Panels pane.
   b. Select **Walk Test**. The Walk Test window with the "walk test in progress..." message displays.
   c. Click the **Stop** button.
   d. Right-click the label for the node under test in the Panels pane and select **Reset**.
7. If testing is complete, close the Network Explorer window.

7.4.3 Walk Test Points List

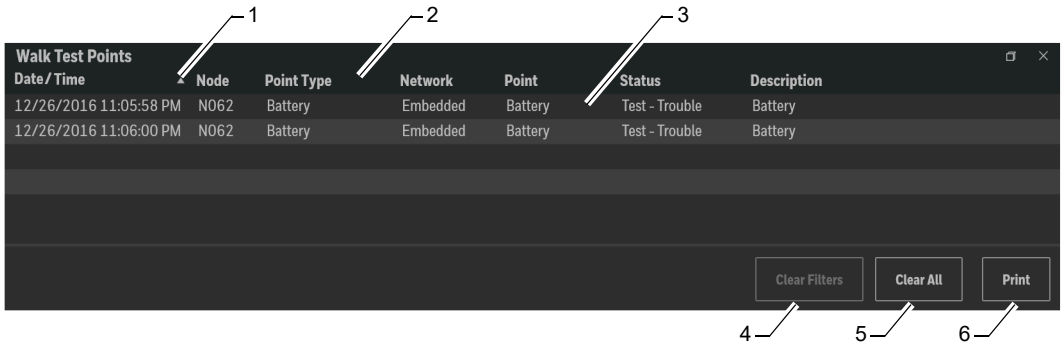
7.4.3.1 Overview

The walk test points list displays a maximum of 4000 test events before it overwrites the earliest record. It does not remove events if they return to normal, so it is possible to have multiples of the same event on the same device displayed in the list. The user must manually clear the list to remove the events.

Access the walk test points list by clicking **Menu > View > Walk Test Points** in the workstation main screen (refer to Table 6.1).

7.4.3.2 Features

Walk test points list features are described in Figure 7.4.



Item	Description
1	Left-click on a column heading and click the up/down arrows (⇳) to sort the column in ascending/descending order.
2	Resize a column by hovering between column headings until a horizontal arrow (⇔) displays and then dragging to the desired width.
3	Right-click within any column to view available filter options (see Table 7.7).
4	Removes all applied filters and causes all walk test events to be visible.
5	Removes all walk test points on the list.
6	Prints the current list at the local printer (if installed).

Figure 7.4 Walk Test Points List Features

Table 7.7 Walk Test List Right-Click Data Filter Options

Option	Description
Hide Column	Temporarily hides the selected column. The column itself is not deleted; only hidden.
Show All Columns	Removes all previously applied column data filters so that all columns and data display.
Filter By Selection	Filters the event according to the event and column that was right-clicked.
Filter Excluding Selection	Filters the data to exclude displaying all records according to the event and the column that was right-clicked.
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 (%).
Filter 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 Date/Time column. Only events occurring at the same time and *after* the selected event are displayed.
Filter 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 Time/Date column. Only events occurring at the same time and *before* the selected event are displayed.

7.5 Test Monitoring

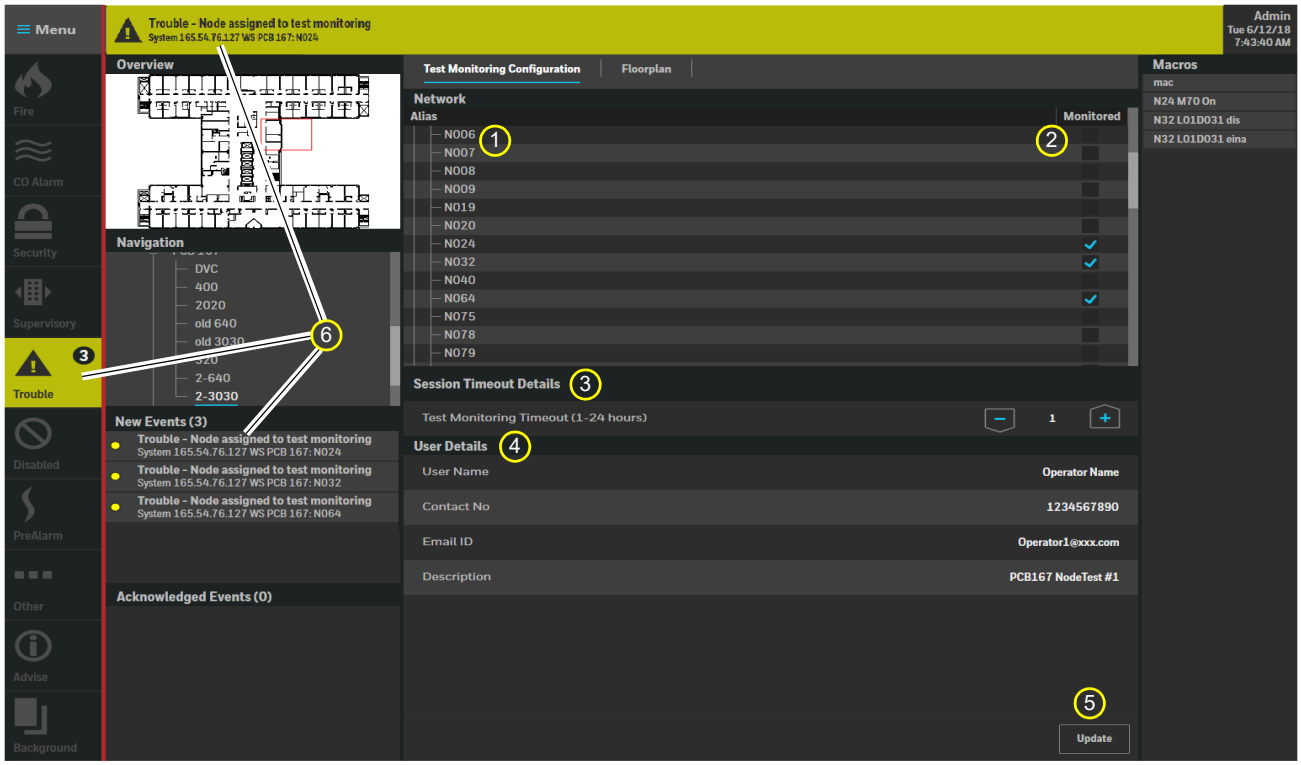
The test monitoring feature allows the Administrator or user with point control to disable monitoring of selected fire system nodes during maintenance and test. The following apply to this feature:

- When using the test monitoring feature, the events that are triggered on any nodes being tested will not be reported in the primary window of the workstation, but will only be displayed in the Test Monitoring window (see Figure 7.6). However, nodes being tested display a trouble event in the primary window to indicate they are off-line during testing.
- The test monitoring mode only affects the workstation on which the mode was activated. Therefore, nodes can be in active monitoring mode on one workstation and in test monitoring mode on another workstation.
- Test monitoring session trouble events and test monitoring configuration change information displays in the workstation history window.
- The user's active monitoring profile governs the nodes which can be placed into test monitoring mode.
- The user is not allowed to change their active monitoring profile once test monitoring is activated. This applies to both the workstation and the configuration tool. Display settings for events are the same as settings of the active monitoring profile.
- The workstation monitors event types as configured on the active monitoring profile.
- In Network Explorer, the user is still able to command the nodes/points in test monitoring mode.
- User logout, new user login, and exiting the workstation application is prohibited when the workstation in test monitoring mode.
- Points in test monitoring mode on the floor plan will not blink on the events, but will show the event status upon the click of icon.
- When in test monitoring mode, an Advise event displays:
  - Twenty (20) minutes before the scheduled test session time out. The user has the option to extend the session.
  - Upon expiration of the test session.
  - When the user has not performed any action during the test session for the configured duration (1-20 minutes). The Advise event indicates that the timeout will not occur because of an active test monitoring session.The inactivity timeout value is set in the workstation (**Menu > Configure > Options >User Features > Inactivity Timeout**).
  - When the user has not acknowledged workstation active events for the configured duration (3-60 minutes). The Advise event indicates that the timeout will not occur because of an active test monitoring session. The unacked event timeout value is set in the workstation (**Menu > Configure > Options >User Features > Unacked Event Timeout**).
- Nodes with active events cannot be put into or removed from being in test monitoring mode.

7.5.1 Test Monitoring Setup

Set up the test session as follows (see Figure 7.5):

1. In the workstation application, click **Menu > Configure > Test Monitoring Configuration**. The Test Monitoring configuration window displays.
2. Click the checkbox for each node to be put into test monitoring mode. A check mark in the "Monitored" column indicates that the node is selected for test monitoring mode.
3. Set the session timeout time and enter user details (optional).
4. Click **Update**. A confirmation pop-up message displays.
5. Click **OK**. A trouble event for each selected node displays in the New Events window indicating selected nodes are in test monitoring mode.

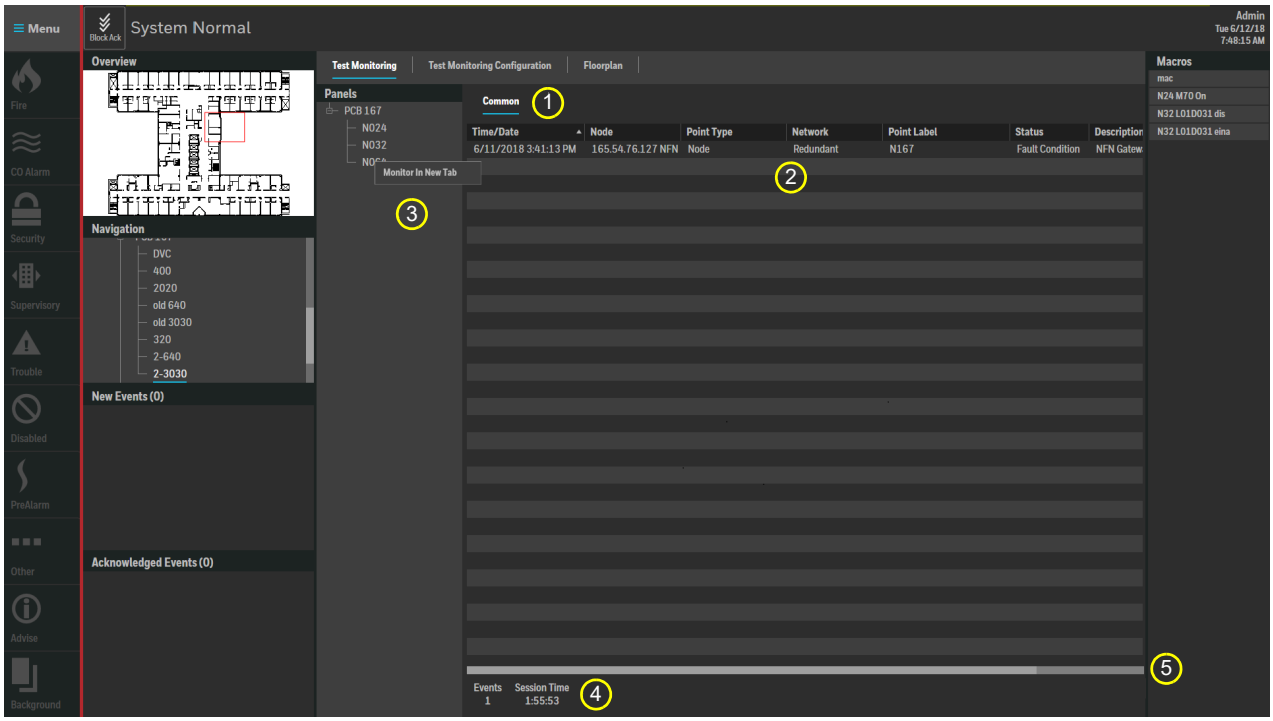


Item	Feature	Description
1	Node List	Hierarchical list of nodes on the system.
2	Monitored Checkboxes	Click the checkbox to select (3) node. Click the checked box to deselect.
3	Session Timeout Details	Test Monitoring Timeout - Use the up and down arrows to set the number of hours the test session will be in test monitoring mode before automatically being restored to active mode. (Default is 1 hour) **Notes:** • If the test monitoring session expires before testing is completed, reset/increment the timeout value in the Test Monitoring Configuration window. • An automatic reminder displays 20 minutes before expiration of the test session. • Once the session expires, the test monitoring configuration screen and monitoring screen is disabled (read only) except for the increment timer on configuration screen. The user will again be able to perform other operations once the session time is incremented.
4	User Details	• User Name - Enter the user's name (required). • Contact No. - Enter the user's phone number (required). • Email ID - Enter the user's email address (required). • Description - Enter any other information necessary (optional).
5	Update Button	Click to save/update settings. A confirmation message displays.
6	Trouble Event Indicators	Trouble event indicators display when nodes are put in test monitoring mode.

Figure 7.5 Test Monitoring Configuration Window

7.5.2 Viewing Test Monitoring Event History

To view a chronological list of events that have taken place while the selected nodes are in test monitoring mode, click **Menu > View > Test Monitoring**. The *Test Monitoring* window displays (see Figure 7.6).



Item	Feature	Description
1	Tab Line	Open window tabs are displayed. The Common tab displays automatically and lists all test session events. Other tabs displaying history for individual nodes can be added (see Item 3 below).
2	Test Session Information Grid	Chronological list of test events for each node under test. • Click the column headings and then click the up/down arrows (⬍) to sort the column in ascending/descending order. • Right-click an event row to clear event, acknowledge, silence panel, and reset.
3	Monitor in New Tab	Right clicking a node label and clicking this option opens a separate history window for the selected node.
4	Test Session Summary	Displays the time remaining in the test session before the session ends and the total number of events in the session. On node-specific windows, the number of events for that node are displayed.
5	Scroll Bar	Slide the bar to view columns with additional data.

Figure 7.6 Test Monitoring Window

7.6 Security Log

Administrators are able to access the security log by going to **Menu > View > Security Log**. The log records the chronological history of such events as the following:

- User login and logout
- User added and deleted
- New networks
- Deleted networks
- Changes to Monitoring Profiles
- Changes to Control Profiles

Clicking on the column headings changes the order of the information. The TimeStamp column sorts by date and time and the columns containing text sort alphabetically.

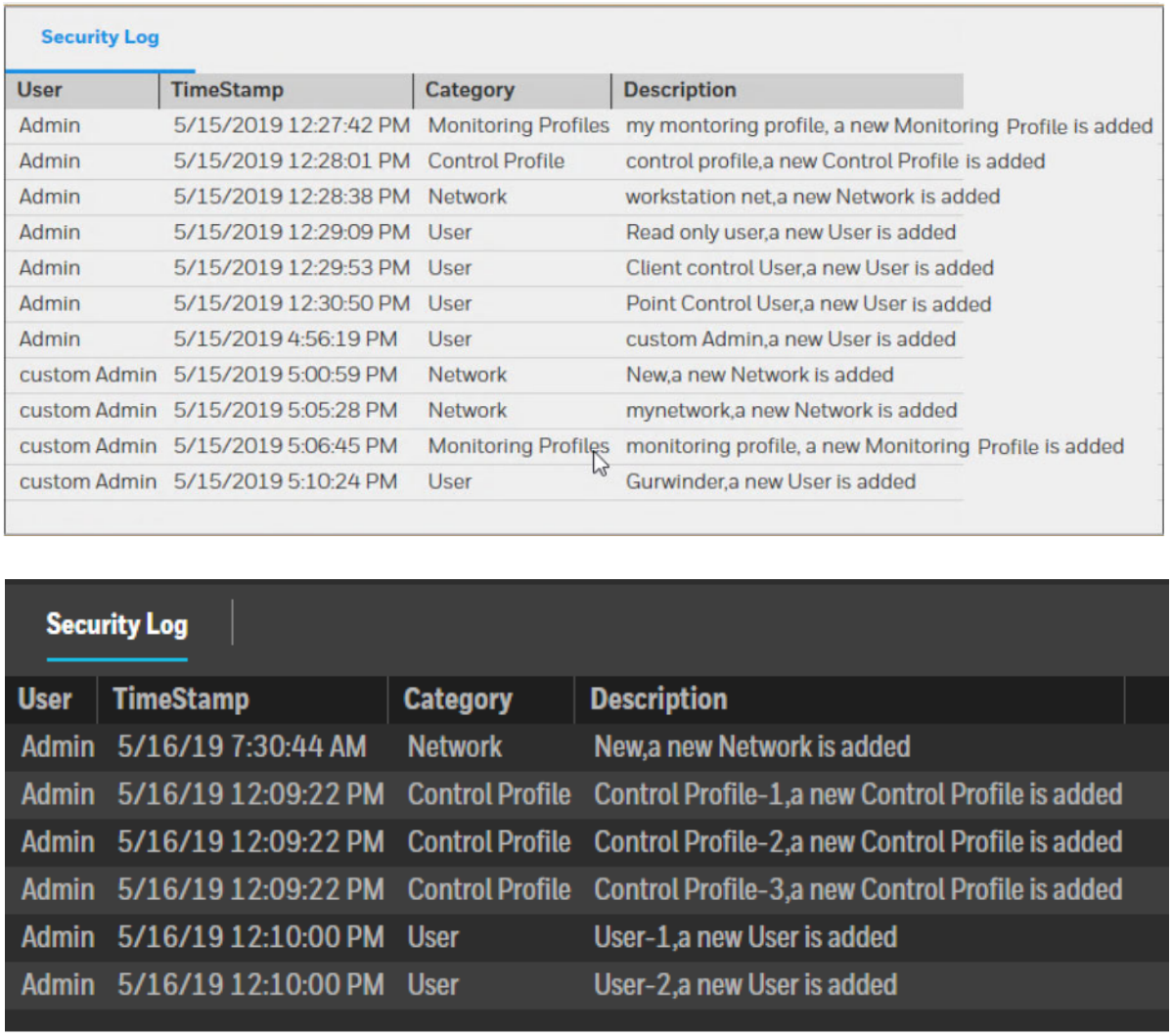


Figure 7.7 Workstation Security Log

Section 8 System Architecture

8.1 Overview

Workstations and gateways communicate over an Ethernet (TCP/IP) network. Gateways also communicate with other panels and fire alarm networks and protective equipment. Each gateway relays Ethernet protocol messages from the monitored equipment using the equipment's native protocol to the workstation. A workstation can support up to 200 gateways.

Example system architectures are described in the figures below.

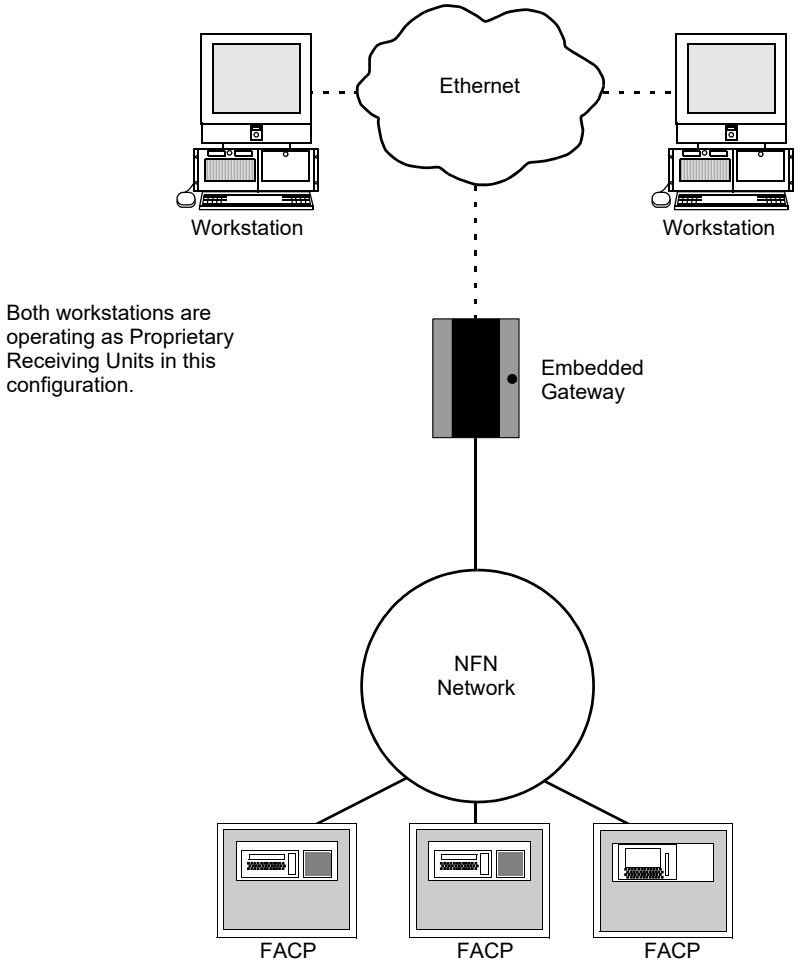


Figure 8.1 Basic ONYXWorks System Example

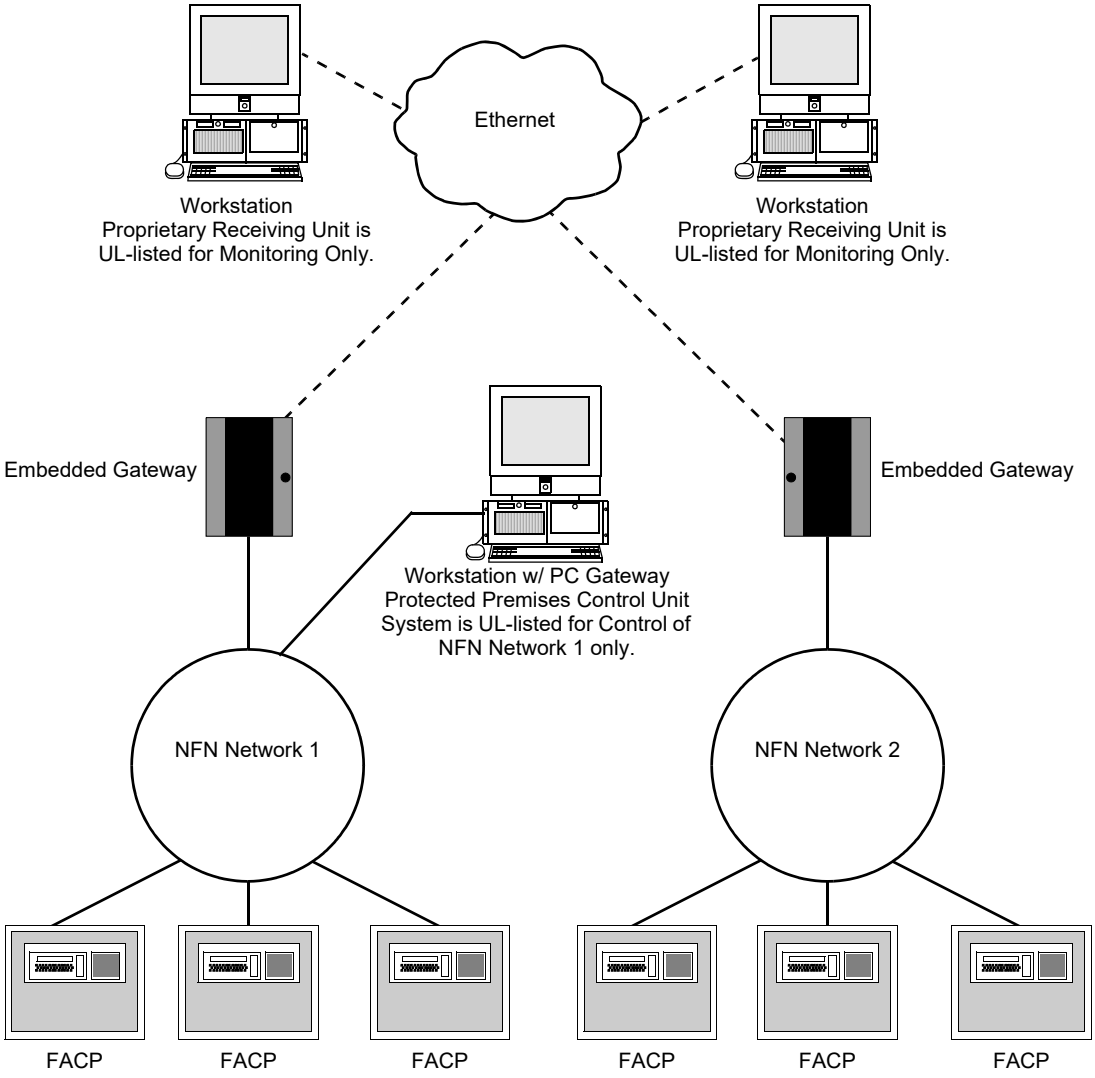


Figure 8.2 Advanced ONYXWorks System Example

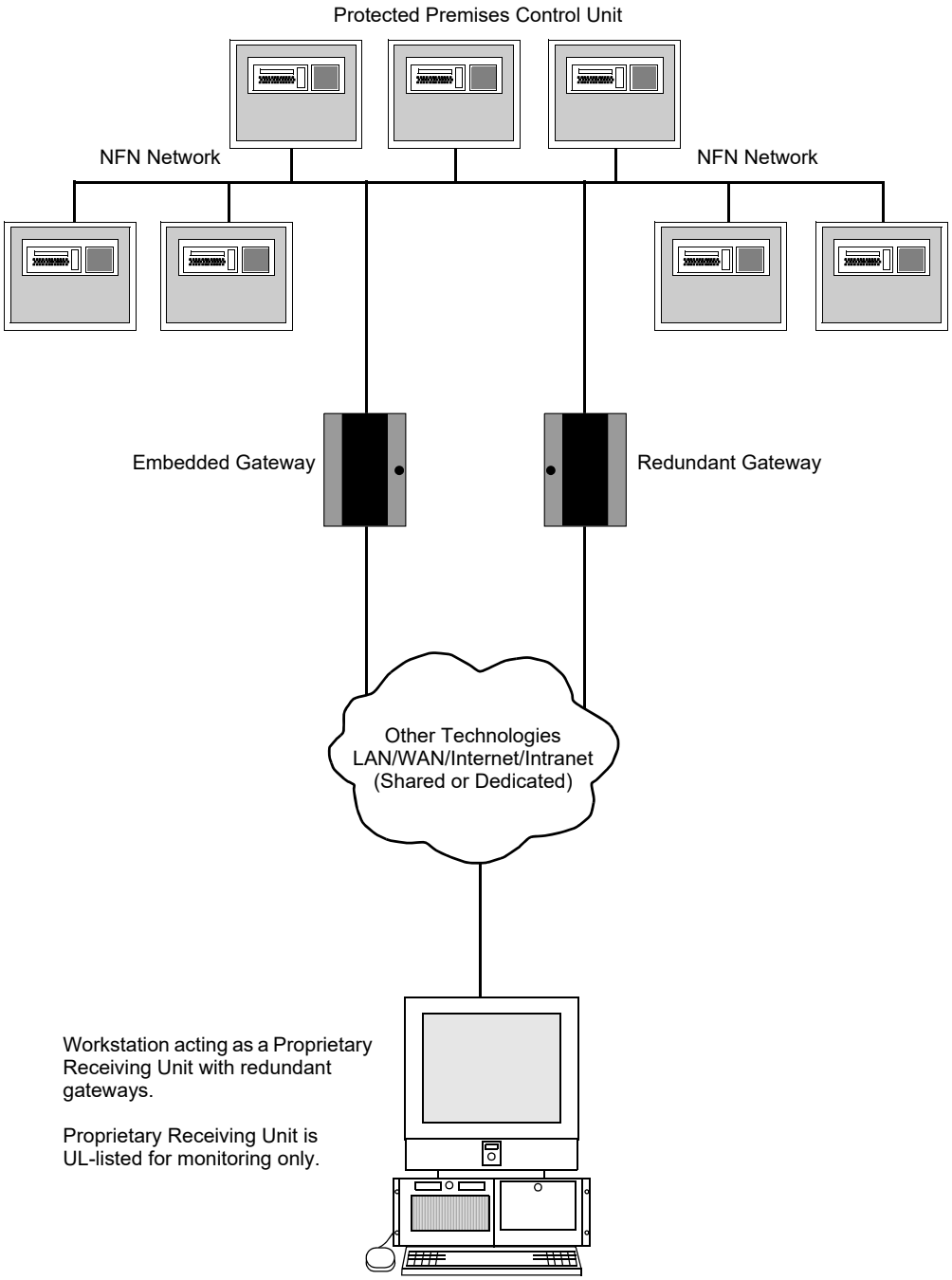


Figure 8.3 System with Redundant Gateway Example

8.2 Protected Premises Control Unit Overview

8.2.1 Architecture for Protected Premises Control Unit

In Protected Premises Control Unit (PPCU) mode, there must be one workstation and one NFN Gateway (see Figure 8.4). The NFN Gateway must be installed on the same PC that is running the workstation software application.

- When operating the workstation in PPCU mode, ULC requires it to be operated by trained personnel.
- If multiple gateways are present or required, the workstation software application must run as a Proprietary Receiving Unit.
- PPCU mode is to be used on a dedicated fire protective signaling network only.

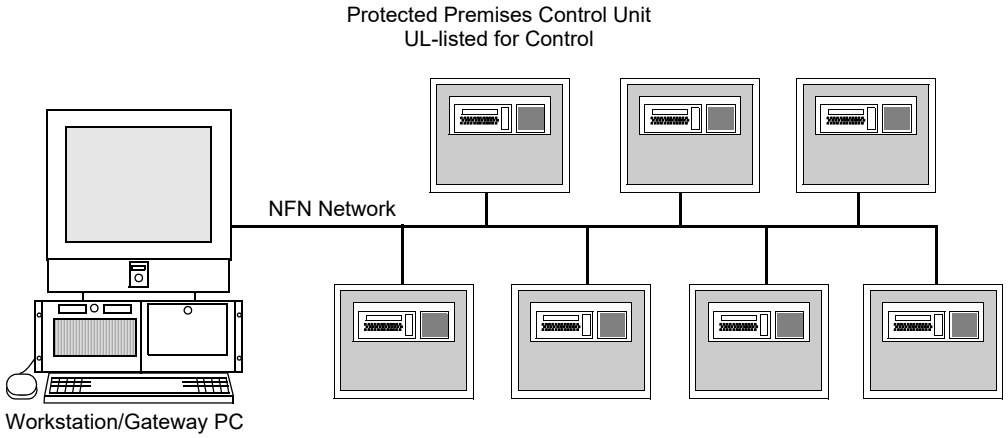


Figure 8.4 Example Protected Premises Control Unit Life Safety System

8.2.2 Event Handling Overview for Protected Premises Control Unit

The following features are provided by the workstation as a Protected Premises Control Unit:

- Block acknowledge of troubles, supervisory, and security events
- Always requires an individual acknowledgment of alarms
- Display and Command Center (DCC)

8.3 Proprietary Receiving Unit Overview

8.3.1 Architecture for Proprietary Receiving Unit

Proprietary Receiving Unit (PRU) fire alarm systems monitor the life safety systems of the protected premises that are under the same ownership. The proprietary receiving unit can be located at the protected premises or at multiple protected properties. Properties may consist of a single building, such as a high-rise building, or several buildings, such as a campus where multiple separate buildings report to a proprietary receiving unit owned and operated by the campus. The property may be contiguous or non-contiguous. If it is non-contiguous, it may consist of protected properties at remote locations. Codes do not limit the geographic distance that may exist between non-contiguous properties. This permits an owner to oversee protection features at geographically diverse locations from a single proprietary receiving unit.

When the ONYXWorks system is operating as a PRU, trained and competent personnel must be in constant attendance. Monitoring of life safety systems may include (but is not limited to) the proprietary receiving unit, power supplies, signal-initiating points, initiating point circuits, signal notification appliances, equipment for the automatic and permanent visual recording of signals, and equipment for initiating the operation of emergency building control services. ONYXWorks systems are permitted to be interconnected with other systems intended to make the premises safer.

In PRU mode, the ONYXWorks system supports up to 200 gateways. Multiple NFN and Receiver gateways are supported simultaneously and can be constantly supervised and communicating with the same workstation. They can also span the TCP/IP network and exist on multiple workstations or embedded hardware. The choice of which gateways to use and where they should be located is application specific and should be analyzed by a trained individual. See Figures 8.5 and 8.6 for examples of proprietary receiving unit system architecture.

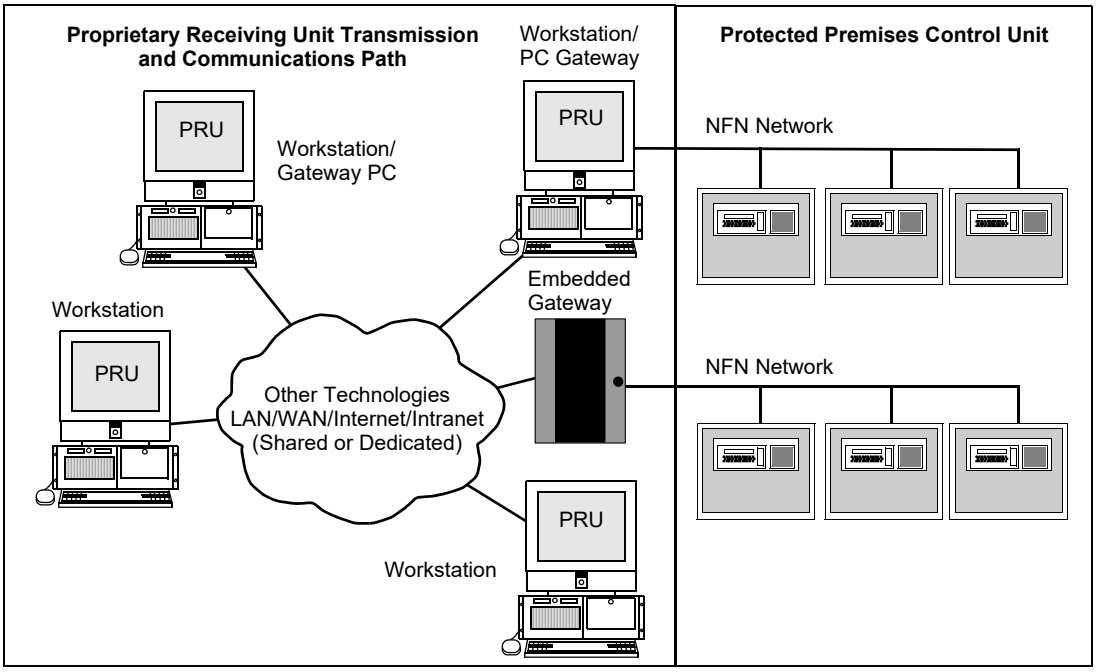


Figure 8.5 Proprietary Receiving Unit System - Example 1

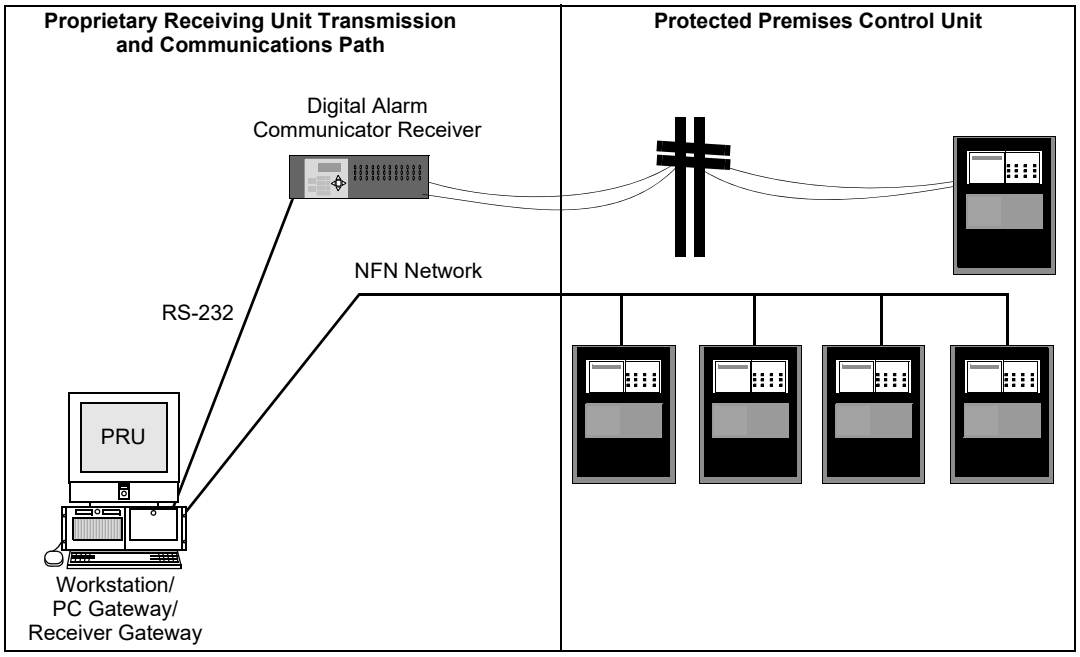


Figure 8.6 Proprietary Receiving Unit System - Example 2

8.3.2 Overview of Event Handling for Proprietary Receiving Unit

The workstation, operating as a Proprietary Receiving Unit, complies with NFPA-72 and UL 864. The following features are provided by the workstation software application operating as a PRU:

- Each change of state is individually acknowledged.
- The maximum duration between the initiation of an alarm signal at the protected premises, transmission of the signal, and subsequent display and recording of the alarm signal at the workstation does not exceed 90 seconds.
- Display rate of subsequent alarms at the workstation is equal to or faster than one complete signal every 10 seconds.
- Trouble signals and their restoration to normal are indicated within 200 seconds.

8.4 Protected Premises Control Unit vs. Proprietary Receiving Unit Event Handling

Events are displayed the same way whether the workstation is operating as a Protected Premises Control Unit or Proprietary Receiving Unit. For example:

- 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 displays 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 (*) is displayed prefixing the event in the New Events list.

However the workstation handles return-to-normal conditions and acknowledgments in a significantly different way, depending on operating mode as described in Table 8.1.

Table 8.1 Protected Premises Control Unit vs. Proprietary Receiving Unit Comparison

Action	Protected Premises Control Unit	Proprietary Receiving Unit
If an event is acknowledged at the Fire Alarm Control Panel (FACP), it is acknowledged at the workstation.	Yes	No
If an event is acknowledged at the workstation, it is acknowledged at the Fire Alarm Control Panel (FACP).	Yes*	Yes*
When an event returns to a normal state, it is removed from the New Event listing.	Yes	No
When an event returns to a normal state, it is acknowledged at the FACP.	Yes	No

* If the logged-in user has sufficient privileges.

Section 9 NetLogic

9.1 NetLogic Description

NetLogic is an application running on the workstation that can provide automated response(s) to events as they occur on any networks monitored by that workstation based on user-defined conditions. It receives messages from the ONYXWorks system and compares that data with user-defined conditions. When a match to a condition is found, the configured action is taken.

NetLogic functions only on workstations running in Proprietary Receiving Unit (PRU) operating mode.

CAUTION: USING NETLOGIC IS NOT APPROVED BY UL.

9.2 Changes in Fire System Database

Changing or deleting referenced nodes, points, or networks in the fire system database can cause NetLogic equations to fail. Any time you make changes to nodes, points, or networks in the fire system database using the Configuration Tool, check NetLogic equations and change them as necessary.

9.3 Opening and Closing NetLogic

The Administrator must be logged into the workstation software application and NetLogic must be enabled (refer to 5.3.1, "General Tab") before it can be opened. Open NetLogic by selecting **Menu > Configure > NetLogic** in the workstation application (refer to 6.4.1, "Workstation Menus").

Close NetLogic by clicking the ‘X’ on upper right-hand corner of the NetLogic tab (if the window is docked) or window (if floating). A prompt asks if the user wants to save the changes.

9.4 NetLogic Window

NetLogic is programmed by writing Boolean equations which are logical statements where different conditions are joined by logical operators. Each condition refers to the normal or off-normal status of a defined device on the network. When the result of the equation is true, the associated action (e.g., flashing strobes, alarm, etc.) is carried out. If it is false, the action is not executed. More than one action can be associated with an equation.

In NetLogic, the equation conditions are set up on the Conditions tab and actions are set up on the Actions tab. These tabs are described below.

9.4.1 Conditions Tab

9.4.1.1 Conditions Tab Features

Figure 9.1 shows the features on the Conditions tab. Features are described in Table 9.1.

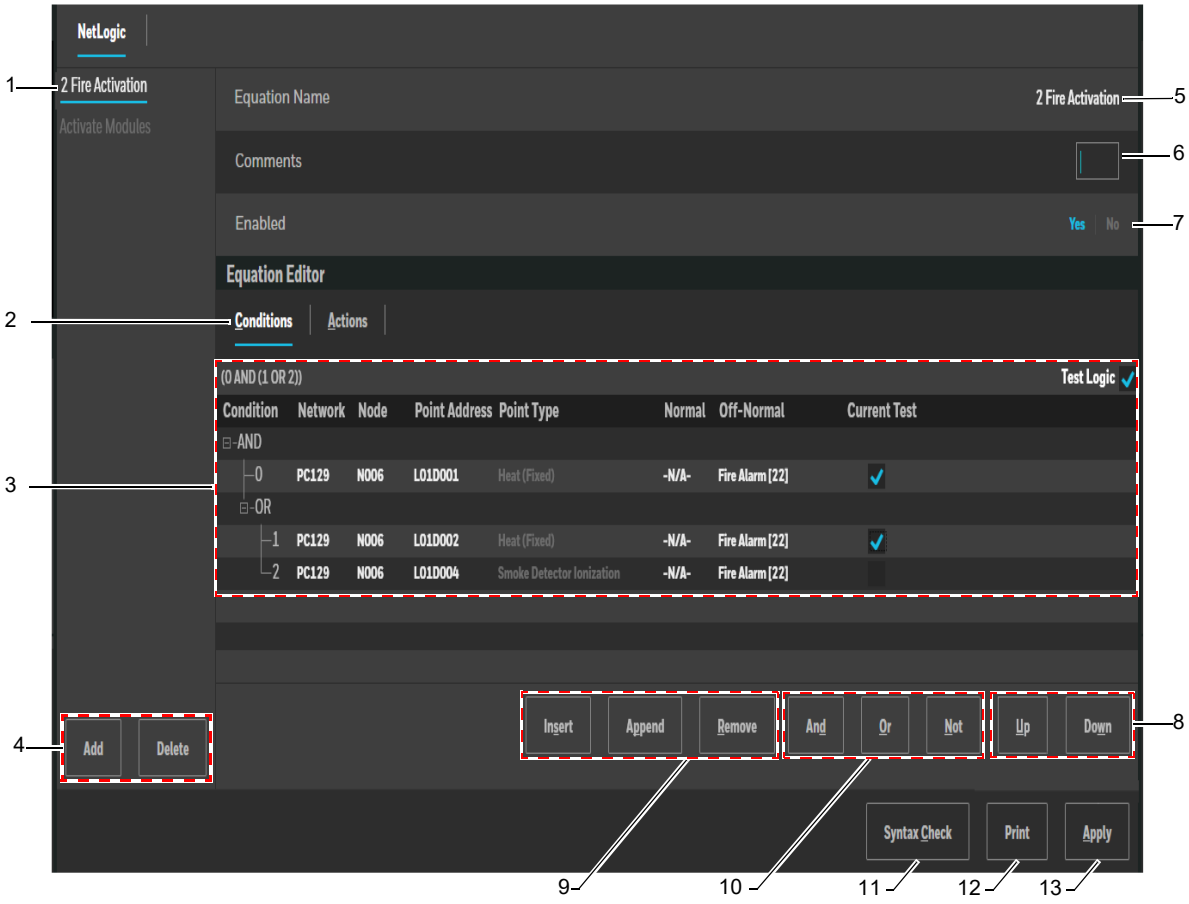


Figure 9.1 NetLogic Conditions Tab

Table 9.1 Conditions Tab Features

Item	Name	Description
1	**Equations List**	Displays the names of all saved equations. Blue underline indicates the currently displayed equation.
2	**Equation Editor Tabs**	• **Conditions** - Displays the equation editor window where the user creates and configures boolean equations. • **Actions** - Displays the actions window where the user configures the actions that will automatically occur if the conditions of the equation are met.
3	**Conditions Grid**	This is the workspace to append, insert, and edit conditions. Condition element columns can be resized by dragging the column boundary lines. Clicking within a column provides a drop-down list of available values. Refer to 9.4.2, "Conditions Grid" for additional information. **Note:** A DACR (receivers) gateway may be chosen as part of a condition, but no commands can be sent to it.
4	**Add/Delete Buttons**	• **Add** - Allows the user to create a new equation. • **Delete** - Deletes the equation selected in the equations list.
5	**Equation Name Field**	Displays the current equation name. Click within the field to change the name.
6	**Comments Field**	Enter up to 32,000 characters of text related to the current equation. Right-clicking the field displays a menu providing options for cut, copy, and paste. Alternately, Ctrl+X, Ctrl+C, and Ctrl+V can be used.
7	**Enabled/Disabled Field**	Using this feature, multiple conditions can be defined and tested over time without activating them and without interfering with other activated conditions. • **Yes** - Default. Enables the equation shown in the *Equation Name* field. • **No** - The equation shown in the *Equation Name* field is disabled.
8	**Level Buttons**	Level buttons control the precedence of conditions in the grid. • **Up** - Unindents the selected condition by removing it from its logic operator. • **Down** - Indents the selected condition by adding a logic operator. A level causes the placement of parentheses in the equation field and controls the order in which conditions are evaluated (i.e., precedence). NetLogic allows an item to be indented, or nested within up to two sets of parentheses. For more information, refer to 9.4.5, "Precedence Levels".
9	**Modifier Buttons**	These buttons are used to add and remove conditions in the conditions grid. Modifier buttons function as follows: • **Insert** - Inserts a new condition above the selected condition, except for the first condition on the grid. • **Append** - Adds a new condition below the last condition on the grid. • **Remove** - Removes the selected condition or logic operator. The appropriate operator button (Item 12 below) must be clicked after clicking the Insert and Append modifier buttons.
10	**Logical Operator Buttons**	These buttons add or modify the logical operator of a condition in the grid. The first condition is automatically assigned the “IF” operator. Click an operator button after clicking the Insert or Append button to assign an operator to the condition. To change the operator, select the current operator and click the desired button. Refer to 9.4.4, "Logical Operators" for additional information.
11	**Syntax Check Button**	Click to test the validity of the logic of the displayed condition. A results message displays. This does not test the equation on the network.
12	**Print Button**	Prints details of the current equation and associated actions on the local printer (if installed).
13	**Apply Button**	Applies the settings to the current equation.

9.4.2 Conditions Grid

9.4.2.1 Overview

Each condition of the equation is a collection of elements. Each element defined in a condition is made up of event criteria. When an equation is true, the related action is executed.

Clicking an element column provides a drop-down list of available values. The value ANY means that any value for that element is valid.

Example: If the network is specified, but the value "ANY" is used for all other elements in that condition, then any event that occurs on that network makes that condition true.

At least one element in the condition must have a specific value for that element to be valid.

Each element builds on its predecessor. For example, the network must be selected before a list of nodes can be provided. NetLogic uses information contained in the workstation database.

Example: When the network is defined, the values found in the node drop-down list are only those available for that network. Once a node is specified, the only values available for points are those found in that node.

9.4.2.2 Conditions Grid Features

Equations are set up on a grid on the Conditions tab. Features are displayed in Figure 9.2 and defined in Table 9.2.

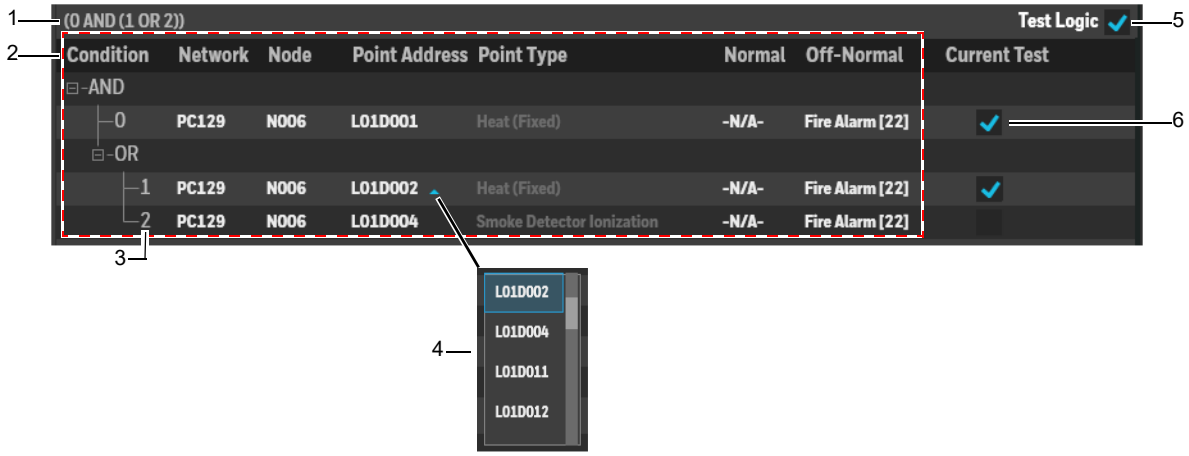


Figure 9.2 Conditions Grid Features

Table 9.2 Conditions Grid Definitions

Item	Element Name	Description
1	**Equation Field**	Shows the displayed condition(s) in simplified standard equation format with operators and parentheses, but replaces each full condition with its condition number in the grid. This display is dynamic, being updated as conditions and operators are added or modified.
2	**Conditions Grid**	Grid where each element of the equation is configured. Column headings describe the elements that may make up the condition. Elements are available by clicking within a column on a row and selecting the element from a drop-down list. The elements available in the drop-down list depend on the previous elements selected. Elements are defined as follows:
		Condition - The Boolean operator assigned to the condition.
		Network - Identifies the network on which the point resides.
		Node - The assigned node number for the point on the network.
		Point Address - The address of the point reporting the event. The point address may be selected from a drop-down list or manually entered.

Table 9.2 Conditions Grid Definitions *(Continued)*

Item	Element Name	Description
2	**Conditions Grid *(continued)***	**Point Type** - Defines the kind of point that is being monitored such as a card reader or pull station. When an event is received on a device, the workstation automatically updates the device to have the correct point type as defined by the gateway. **CAUTION: Manually Defined Point Types** - When designing an equation to respond to status changes in devices of a given point type, it is critical to provide the gateway-defined point type of each monitored device; not a manually defined point type (for example, if the point type has been changed using the workstation configuration tool).
		Normal - The point status description when it is in a normal state. **Note:** ANY is not available for the normal state.
		Off-Normal - The point status description when it is in an off-normal state. **CAUTION: Single-sided Events** - An asterisk beside a point status description in an element's drop-down list denotes a single-sided event. Single-sided events are events that do not have a matching back-to-normal status, such as a card swipe where a report is made that the swipe occurred, but there is no "unswipe" return-to-normal event reported. A single-sided event is cleared when it is acknowledged at the workstation, even though the circumstances which triggered it may still be true. Therefore, single-sided events should not be used in compound conditions (i.e., conditions which include the condition operators AND or AND NOT). Otherwise, acknowledging an event at the workstation could prevent an equation from triggering even though its criteria were true.
3	**Condition Number**	Ordinal number of the condition automatically assigned to the row in the grid.This number is used in the equation field to represent the condition in the equation.
4	**Drop-down List**	Click in a column in the row to display the list of available options. The options available depend on the settings made in a previous element column in the grid.
5	**Test Logic Indicator**	Indicates whether the conditions with *Current Test* checkboxes checked will activate the action configured on the Actions tab. • **Blue Check Mark** - Selected conditions will activate the action(s). • **No Check Mark** - Action(s) will not be performed. **Note:** The logic test does not test the equation on the network.
6	**Current Test**	• **Checked** - Makes the condition in that row TRUE. • **Unchecked** - Makes the condition in that row FALSE. Test results are indicated by the Test Logic Indicator.

9.4.2.3 Testing the Conditions

NetLogic is provided with a condition testing tool. The condition tester allows the logical functionality of each condition in the equation to be tested manually without affecting anything on the network.

The condition tester does not test for interaction between equations such as if another equation performs actions on the same output.

The tester functions by allowing the user to assign test states, true or false, to each condition. This allows the user to create several scenarios to analyze the accuracy of the condition before using it in a real situation.

Click on the indicator in the current test column of the condition grid (see Figure 9.2) to change the state of a condition: TRUE = green, or FALSE = black. The test logic indicator at the top-right of the grid indicates whether the logic of the equation components is valid (i.e., actions related to the equation would be executed if equation was enabled).

When analyzing an equation with several conditions, it is advisable to test them in many combinations of states to determine if the condition produces the desired effect.

9.4.3 Actions Tab

The actions tab is similar to the conditions tab in that it is used to identify the elements to be acted upon when the related equation is true. Unlike the conditions tab, wild-cards (i.e., ANYs) are not permitted. Every device must be fully defined. Like the condition grid, the value of each element is specified from a drop-down list.

In addition to the elements of the action grid, several other features can be defined to control action execution including delays, durations, and secondary inputs. Figure 9.3 shows the features on the Actions tab. Features are described in Table 9.3.

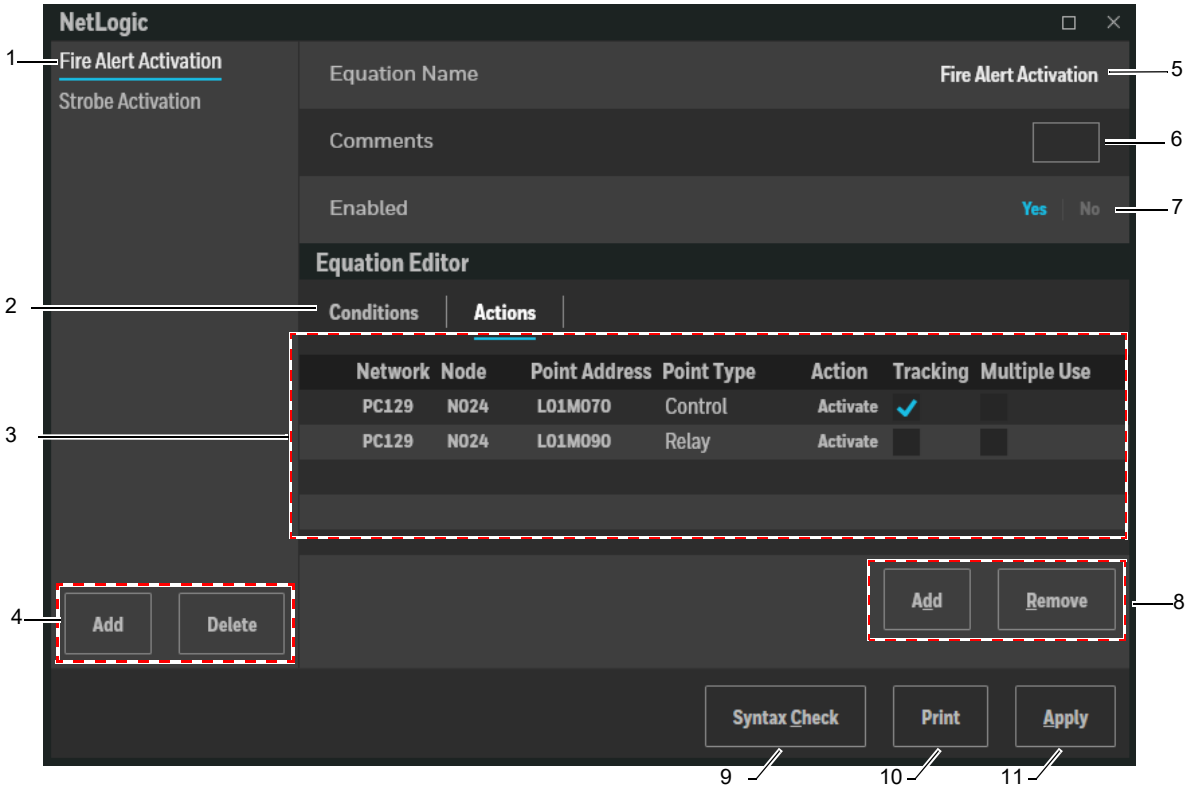


Figure 9.3 NetLogic Actions Tab

Table 9.3 Actions Tab Features

Item	Name	Description
1	**Equations List**	Displays the names of all saved equations. Blue underline indicates the current equation.
2	**Equation Editor Tabs**	• **Conditions** - Displays the equation editor window where the user creates and configures boolean equations. • **Actions** - Displays the actions window where the user configures the actions that will automatically occur if the conditions of the equation are met.
3	**Actions Grid**	This is the work space used to define and edit action elements. Action elements are defined in Table 9.4. Columns can be resized by dragging the column boundary lines. **Note:** A DACR (receivers) gateway may be may not be selected on this grid.
4	**Add/Delete Buttons**	• **Add** - Allows the user to create a new equation. • **Delete** - Deletes the equation selected in the equations list.
5	**Equation Name Field**	Displays the current equation name. Click within the field to change the name.
6	**Comments Field**	Enter up to 32,000 characters of text related to the current equation. Right-clicking the field displays a menu providing options for cut, copy, and paste. Alternately, Ctrl+X, Ctrl+C, and Ctrl+V can be used.
7	**Enabled/Disabled Field**	Using this feature, multiple conditions can be defined and tested over time without activating them and without interfering with other activated conditions. • **Yes** - Default. Enables the equation shown in the Equation Name field. • **No** - The equation shown in the Equation Name field is disabled.

Table 9.3 Actions Tab Features *(Continued)*

Item	Name	Description
8	**Editing Buttons**	Allow the user to add or remove actions on the actions grid. • **Add** - Inserts a blank line making space for a new action element. • **Remove** - Removes the line for the highlighted element.
9	**Syntax Check Button**	Click to test the validity of the logic for the equation. A results message displays. This does not test the equation on the network.
10	**Print Button**	Prints details of the current equation and associated actions on the local printer (if installed).
11	**Apply Button**	Applies the settings to the current equation.

Table 9.4 Action Elements

Element Name	Description
Network*	Select the network where the point resides from the drop-down list.
Node*	Select the assigned node number for the point on the network from the drop-down list.
Point Address*	Select the address of the point reporting the event.
Point Type*	Automatically populates depending on the point address selected.
Action	The command that will be sent to the device (output), either activate or deactivate, when a condition becomes TRUE. The choice of available actions is determined by the point type.
Tracking Checkbox	• **Checked** - When the condition becomes FALSE the opposite command for that point will be sent. In that way, a device may be turned on when the condition is TRUE, then automatically go back to normal when the condition becomes FALSE. If another equation is acting on an output of an equation that has returned to normal, then tracking will defer to the active equation, and the tracking command will not be sent out. This feature cannot be linked to a timer. Tracking allows an inverse command to be issued when the condition becomes FALSE, with no additional defined conditions. For example, if the action is to activate a point when the condition is met, a command to deactivate the point will be sent when the condition is no longer true. Tracking is not available for single-sided events and the user is notified by an on-screen message if tracking is selected when single-sided events have been defined. • **Unchecked** - Tracking is disabled.
Multiple Use Indicator	Automatically displays a blue check mark when another equation performs an action on the output defined on that line. When the check mark is present, the user can click on the indicator and get a list of other equations that use the same output. It is important to be aware of interactions to avoid undesired responses.
Note: Required elements are marked with an asterisk (*).	

9.4.4 Logical Operators

Boolean equations can be based on the results of the status of a single element. However, complex and specific equations can be built by joining multiple elements using logical operators. The main operators used are as follows:

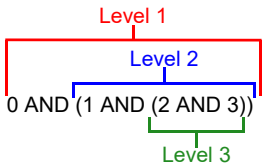
Table 9.5 Boolean Logical Operators

Operator	Description
AND	When AND is used, both conditions must be TRUE for the equation to be true. CAUTION: Using AND or AND NOT causes problems with equations involving single-sided events. For more information, refer to the Elements table in 2.5.2, “Building the Condition”.
OR	When OR is used, only one condition of the joined conditions must be TRUE for the equation to be true.
OR NOT	When OR NOT is used, either the first condition must be TRUE or the second condition must be FALSE for the equation to be true.
AND NOT	When AND NOT is used, the first condition must be TRUE and the second condition must be FALSE for the equation to be true
NOT	In the conditions grid, NOT is a toggle switch for operators in existing conditions. Highlight the condition field and click the Not button to modify the operator to include it. If NOT is already present in the highlighted operator, pressing the Not button removes it from the operator. NOT is actually a modifier used with a single element. When NOT is associated with a condition, then the monitored state of the element is reversed. Example: Input ON = TRUE is the same as NOT Input OFF = TRUE. CAUTION: Care should be exercised when using the NOT operator because any event except the one specified will cause the condition to be true. For example, if the input in the above equation is in TROUBLE, the input is NOT OFF, but should the action still be executed? These are the types of situations that must be considered. Generally NOT is used in conjunction with other elements.

9.4.5 Precedence Levels

Precedence defines the sequence of operations performed in an equation. In NetLogic, the order in which a condition is evaluated within an equation is determined by the placement of parentheses in the equation using the level buttons on the Conditions tab (see Figure 9.1). If levels are used in an equation, the innermost set of parenthetical elements is executed first, working outward until the entire condition has been evaluated.

NetLogic supports up to three levels of nested parentheses as shown below:

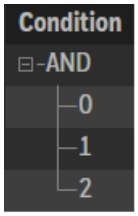


To group a condition or conditions in parentheses, click the condition number and click on the **Down** button to the left of the conditions grid. The condition is indented to the right of the operator above it making it a descendant. Every condition that is descended from the same parent will be grouped with that parent.

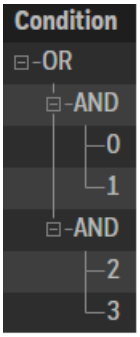
In order to view the condition grid as an equation, an equation field is provided in (Figure 9.1, Item 3) that displays the equation. Each number in the equation corresponds to the row number for the condition in the grid. For example: (0 AND 1) or (2 AND 3) or (4 AND 5). The equation field is updated as changes are made to the conditions grid.

Examples:

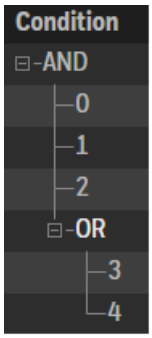
- **0 *AND* 1 *AND* 2 -** No precedence levels. Each condition is evaluated individually from left to right; first 0, then 1, then 2. The condition column in the grid looks like this:



- **(0 *AND* 1) *OR* (2 *AND* 3)** - First conditions 0 *AND* 1 are evaluated individually and compared with their operator. A result is obtained (true or false) for the set. Next conditions 2 *AND* 3 are evaluated in the same manner. Finally, the results of (0 *AND* 1) are "ORed" to the results (2 *AND* 3) and a result for the entire equation is obtained (true or false). The condition column in the grid looks like this:



- **0 *AND* 1 *AND* 2 *AND* (3 *OR* 4))** - First conditions 3 *AND* 4 are evaluated individually and compared with their operator. Next, Each condition is evaluated individually from left to right; first 0, then 1, then 2, then the result of (3 *AND* 4), and a result for the entire equation is obtained (true or false). The condition column in the grid looks like this:



9.5 NetLogic Entries in History Window

The entries listed in the following table are expected to appear in the workstation history window as NetLogic equations are running. The history window is accessed by selecting **Configure > View >History** in the workstation application.

Table 9.6 NetLogic Entries in Workstation History

Entry Text	Definition
Performing startup equation evaluation	Appears when the workstation is first started.
Equation '[EQUATION NAME]' has changed state to On, outputs are being evaluated	Appears when an equation is evaluated and becomes active.
Equation '[EQUATION NAME]' has changed state to Off, outputs are being evaluated	Appears when an equation is evaluated and is no longer active.
Equation '[EQUATION NAME]' has changed state, but equation is disabled (outputs are not evaluated)	Appears when an equation changes state, but the equation is disabled. The equation has to be manually disabled by the user.
Command 'Activate' is being sent to output '[OUTPUT DEVICE ADDRESS]'	Appears for each output when an equation is evaluated and becomes active.
Command 'Activate' is being reversed to output '[OUTPUT DEVICE ADDRESS]'	Appears for each output that is configured for Tracking, when an equation is evaluated and no longer active.
Output '[OUTPUT DEVICE ADDRESS]' cannot change state, it is still in a forced state by equation '[EQUATION NAME]	Appears when an equation is no longer active and tracking is configured for the output. The reverse command should be sent to the output, but will not because another equation is currently active that is also using the same output.

9.6 Troubleshooting Equations

Careful planning is essential to obtain the desired results from equations. While equations are being constructed and tested, problems may occur that can usually be resolved as described in the following table.

Table 9.7 Troubleshooting Equations

Problem	Resolution
The event that should trigger the action is not found.	• Verify NetLogic is communicating with the network. • Verify the desired event was actually sent.
The equation was not evaluated.	• Something in the equation does not match the event. • Compare the event received information with what is specified in the equation. • Verify the device has been programmed correctly.
The result of the equation is incorrect.	• Re-examine the actions of the equation.
Both items are found, but the action is still not carried out.	• Verify the address of the action is correct.



CAUTION: SINGLE-SIDED EVENTS

USING "AND" OR "AND NOT" CAUSES PROBLEMS WITH EQUATIONS INVOLVING SINGLE-SIDED EVENTS.

Section 10 NOTIFY-IP

10.1 Operation

NOTIFY-IP is an optional feature that enables live paging to be performed from an ONYXWorks Workstation. The page may also be recorded and previewed before playing. Paging is restricted to one workstation at a time per target network or group of target networks.

NOTIFY-IP live pages participate in the DVC configured priority matrix and preempt or are preempted by other DVC inputs accordingly. NOTIFY-IP can trigger audio sequences on a Digital Voice Command module (DVC) to provide prerecorded output. In addition, NOTIFY-IP can be configured to activate zones during a page for use with Cooperative Control-By-Event (CCBE) equations.

When running on a workstation that is operating as a Proprietary Receiving Unit (PRU), NOTIFY-IP supports multiple gateways. NOTIFY-IP may be used for non-emergency general paging only or to play prerecorded voice messages.

NOTIFY-IP enables the workstation to operate as a Central Control Station (CCS) when participating as part of a Mass Notification System.

10.2 Functionality

NOTIFY-IP sends a message instructing the DVC(s) which speakers to activate based upon the audio group selected. The live voice input is digitized. NOTIFY-IP then sends the message to the DVC via an NFN Gateway or saves the message to a temporary audio file for previewing before it is sent to the DVC.

10.2.1 System Functions

The following tables provide information about the functional parameters of a NOTIFY-IP system.

Table 10.1 System Parameters (General Paging)

Parameter	Feature	Description
All Call, Evacuation, Inactive, and Alert Type Paging Groups	Message Route	Live Microphone to: • DVCs • Zones
	DVCs Supported	100 per group
	Zones Supported	100 per group
	Networks Supported	50
	Valid DVC Input(s)	N/A
Direct Paging Groups	Message Route	Live Microphone to: • DVCs • Zones
	PAM* Points Supported	100 per group
	Zones Supported	100 per group
	Networks Supported	50
	Valid DVC Input(s)	1037
Sequence Type Paging Groups	Message Route	Preconfigured Audio to: • PAM Points • DVCs Zones
	PAM Points Supported	100 per group
	DVCs Supported	100 per group
	Zones Supported	100 per group
	Networks Supported	50
	Valid DVC Input(s)	0031 to 1030 Inclusive
Paging Activation Icons	Icons to activate paging groups can be placed on any workstation screen.	
Network Limitation	Only one paging group at a time can be activated for a given network.	

Note: * Prioritized Audio Matrix.

Table 10.2 System Parameters (Mass Notification and Fire Paging)

Parameter	Feature	Description
All Call, Evacuation, Inactive, and Alert Type Paging Groups	Message Route	Live Microphone to: • DVCs • Zones
	DVCs Supported	100 per group
	Zones Supported	100 per group
	Networks Supported	1
	Valid DVC Input(s)	N/A
	Mode Required	PPCU
	Max. No. Emergency Groups	25
Direct Paging Groups	Message Route	Live Microphone to: • DVCs • Zones
	PAM Points Supported	100 per group
	Zones Supported	100 per group
	Networks Supported	1
	Valid DVC Input(s)	1035
	Mode Required	PPCU
	Max. No. Emergency Groups	25
Sequence Type Paging Groups	Message Route	Preconfigured Audio to: • PAM Points • DVCs • Zones
	PAM Points Supported	100 per group
	DVCs Supported	100 per group
	Zones Supported	100 per group
	Networks Supported	1
	Valid DVC Input(s)	0031 to 1030 Inclusive
	Mode Required	PPCU
	Max. No. Emergency Groups	25
Paging Activation Icons	Icons to activate paging groups can be placed on any workstation screen.	
Network Limitation	Only one paging group at a time can be activated for a given network.	

10.3 Agency Listings

10.3.1 Standards

The following standards apply to NOTIFY-IP:

■ **Compliance** - This product has been investigated to, and found to be in compliance with, the following standards:

National Fire Protection Association

- NFPA 72 National Fire Alarm and Signaling Code

Underwriters Laboratories

- UL 864 Control Units for Fire Alarm Systems, Tenth Edition
- UL 2572 Mass Notification Systems, Second Edition

■ **Installation** - This product is intended to be installed in accordance with the following:

Local

- AHJ Authority Having Jurisdiction

National Fire Protection Association

- NFPA 70 National Electrical Code
- NFPA 72 National Fire Alarm and Signaling Code

Underwriters Laboratories

- UL 681 Standard for Installation and Classification of Burglar and Holdup Alarm Systems

10.3.2 Agency Restrictions and Limitations

- NOTIFY-IP must be installed on a dedicated network.
- NOTIFY-IP is UL 864 listed for paging of life safety fire events, only when the workstation is operating in Protected Premises Control Unit (PPCU) mode.
- NOTIFY-IP is UL 2572 listed to perform Mass Notification All Call pages only. The workstation must be operating in PPCU mode.

10.4 UL 2572 Security Levels

NOTIFY-IP meets the UL 2572 security levels stated below:

Table 10.3 Security Levels

Level Type	Level
Communication Security	1
Stored Data Security	0
Access Control Security	2
Physical Security	1
Audit Control Security	0

10.5 Field Programmable Settings

Table 10.4 UL 2572 Field Programmable Settings - NOTIFY-IP

NOTICE TO USERS, INSTALLERS, AUTHORITIES HAVING JURISDICTION, AND OTHER INVOLVED PARTIES			
This product incorporates field-programmable software. In order for the product to comply with the requirements in the Standard for Control Units and Accessories for Fire Alarm Systems, UL 2572 certain programming features or options must be limited to specific values or not used at all as indicated below.			
Program feature or option	Permitted in UL 2572 (Y/N)	Possible Settings	Settings permitted in UL 2572
Inactivity Timeout	Yes	0 - 20 minutes (0 disables feature)	1 - 20 minutes

10.6 Compatible Equipment

10.6.1 Current Compatible Equipment

The equipment listed in the table below is compatible with NOTIFY-IP:

Table 10.5 Compatible Equipment

Type	Equipment	Description
Network Cards:	• NCM-W, NCM-F	• PCA: 3.60.6 or later • PCB: 10.2.2 or later
	• HS-NCM-MF • HS-NCM-SF • HS-NCM-W-2 • HS-NCM-WSF-2 • HS-NCM-WMF-2 • HS-NCM-MFSF	• Kernel: 1.2.4 or later • Firmware: 20.1.1 or later
Workstation:	• ONXYWORKS-WS	ONXYWorks Workstation
Network Gateways:	• NFN-GW-EM-3	Embedded NFN Gateway
	• NFN-GW-PC-W	PC NFN Gateway Card (wire connections)
	• NFN-GW-PC-F	PC NFN Gateway Card (fiber connections)
	• NFN-GW-PC-HNMF	High-speed PC NFN Gateway Card (multi mode fiber connections)
	• NFN-GW-PC-HNSF	High-speed PC NFN Gateway Card (single mode fiber connections)
	• NFN-GW-PC-HNW-2	High-speed PC NFN Gateway Card (wire connections)
Other Products:	• DVC	Version 6 or later

10.6.2 Legacy Compatible Equipment

The following equipment is listed as compatible with the NOTIFY-IP, but is no longer available.

Table 10.6 Legacy Compatible Equipment

Type	Equipment	Description
Network Cards:	• HS-NCM-W • HS-NCM-WSF • HS-NCM-WMF	• Kernel: 1.2.4 or later • Firmware: 20.1.1 or later
Network Gateways:	• NFN-GW-PC-HNW	NFN PC Gateway card (wire connections)

10.7 System Configuration

The following table describes the required and optional configurations needed to meet NOTIFY-IP's intended application.

Table 10.7 System Configuration

Accessory/Subassembly	Part Number	Description	Network Configuration
Network Cards	**Refer to Tables 10.5 and 10.6.**	Current UL-listed Network Cards	R
Workstation		Current UL-listed Workstation	R
Network Gateway		Current UL-listed Network Gateways	R[1]
DVC		Current UL-listed DVC	R
Audio Supervision Card	AUDIOSUP-MB-PCA	Audio Supervisor Main Board	R
Microphone	50105431-001	Desktop Microphone	R
Audio Cables (2)	50105239-001	Cable Assembly, Stereo, Male to Male, 3.5mm, 6" Long	R
DAA		Digital Audio Amplifier	R
Digital Audio Loop			R
Software License		Enables NOTIFY-IP feature.	R

Notes:

R = Required component for minimally functional system

O = Optional equipment

1 = For Life Safety Fire paging and when part of a Mass Notification System, one of the NFN PC Gateways listed in Tables 10.5 and 10.6 must be used.

10.8 Power Requirements

Power requirements for NOTIFY-IP are the same as for the workstation. Refer to 2.1.2, "System Power Requirements" for details.

10.9 Environmental Requirements

Environmental requirements for NOTIFY-IP are the same as for the workstation. Refer to 1.5, "Environmental Requirements" for details.

10.10 NOTIFY-IP System Architecture

10.10.1 Fire Network Only

When NOTIFY-IP is on an Ethernet TCP/IP network, the network must be a dedicated network. When operating on a fire network only system, the system must include:

- NOTIFY-IP
- ONYXWORKS-WS
- NFN Gateway
- DVC
- DAA

To be UL 864 compliant, the system must be configured as follows:

- The workstation must be in PPCU mode.
- The NFN Gateway used for paging must be installed in the same PC that is running the NOTIFY-IP software application.

CAUTION: REDUNDANT GATEWAY FAILURE DELAY

IF ONE OF THE REDUNDANT GATEWAYS FAILS DURING A PAGE, UP TO 30 SECONDS OF THE PAGE MAY BE LOST WHILE THE REDUNDANT GATEWAY TAKES CONTROL.

10.10.2 Combination Fire and Mass Notification Network

When NOTIFY-IP is operating on a fire network only system, the system must include:

- NOTIFY-IP
- ONYXWORKS-WS running in PPCU mode
- NFN PC Gateway
- DVC
- DAA

To be UL 2572 compliant, the system must be configured as follows:

- The workstation must be in PPCU mode.

10.11 Protected Premises Control Unit (PPCU) Mode Overview

10.11.1 Architecture for PPCU Mode

A workstation in PPCU mode that is running NOTIFY-IP, complies with the UL requirements for a Protected Premises Control Unit. Refer to Figure 10.1 for an example of system architecture for a workstation in PPCU mode.

NOTE: PPCU mode is NOT supported when a gateway other than the PC version of the NFN Gateway is used, or if there is more than one gateway in the ONYXWorks system.

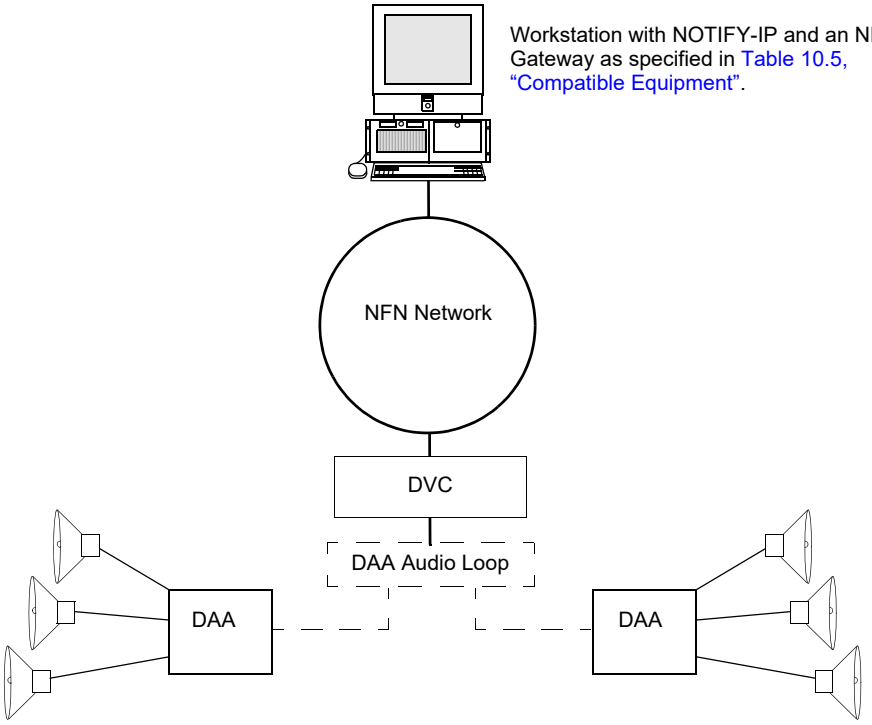


Figure 10.1 Example: NOTIFY-IP System Architecture (PPCU Mode)

10.11.2 PPCU Mode Agency Approval

In PPCU mode, ONYXWorks systems are classified as Protected Premises Control Units meeting UL requirements.

NOTES:

- NOTIFY-IP is not UL listed for paging from a workstation configured as a Central Control Station.
- NOTIFY-IP is UL-2572 listed for in-building paging.

10.12 Installation

10.12.1 Installing the Audio Supervision Card

Typically the workstation is ordered with the audio supervision card (ASC) already installed. However, if the card is being retrofitted into an existing workstation PC, install it as follows:

1. Close all applications and shut-down the PC.
2. Disconnect primary and backup power sources from the PC.
3. Open the PC's cover and locate a vacant PCI slot.
4. Remove the PCI slot cover saving the screw for reuse.
5. Insert the ASC's edge connector into the vacant PCI slot and secure the board with the screw.
6. Reinstall the cover on the PC.
7. Reconnect primary and backup power sources.

10.12.2 Connecting the Cables

Connect the cables as follows (see Figure 10.2):

1. Disconnect the PC speaker cable from the sound card and plug it into the speaker-out jack on the audio supervision card (ASC). The speaker-out cable must be connected in order for the workstation to provide supervision.
2. Connect the two 1/8" cables between the sound card and the ASC.
3. If necessary, connect the microphone cable leads to the 5-pin connector.
4. Connect the 5-pin connector into the ASC.

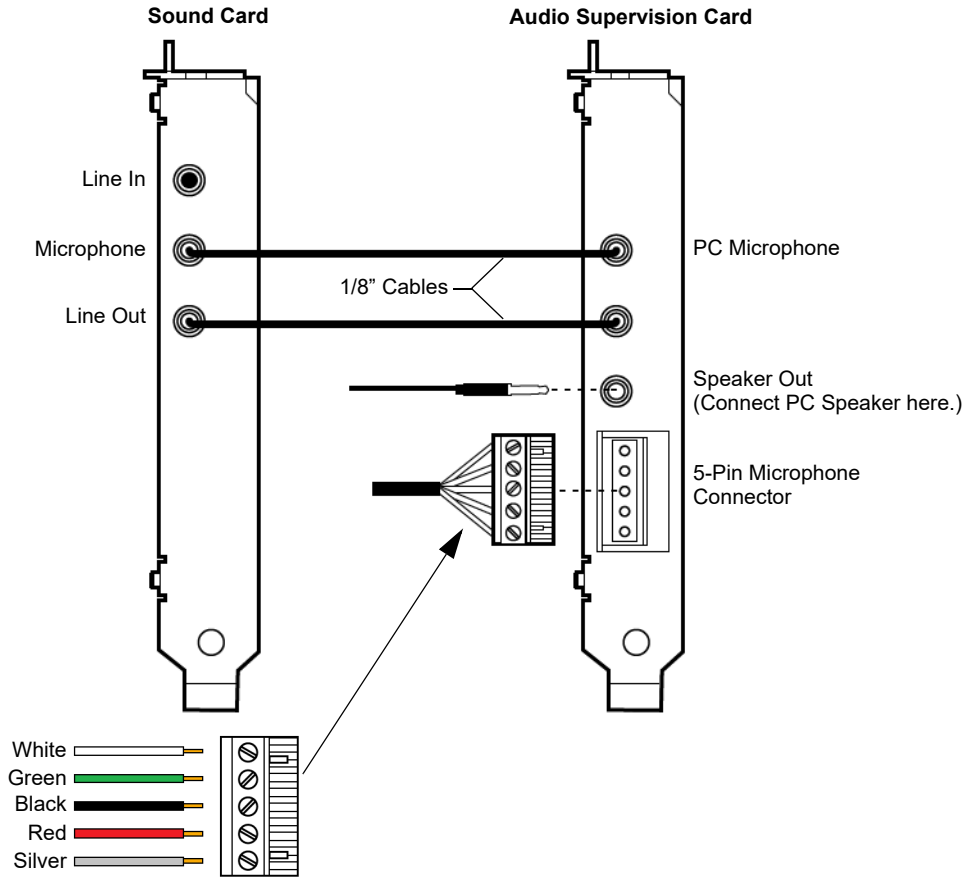


Figure 10.2 Sound Card and Audio Supervision Card Connections

10.12.3 Wiring Methods

Wiring methods used shall be in accordance with UL 681.

10.13 Voice Paging License

In order for NOTIFY-IP to operate, the workstation must be licensed for the Voice Paging feature. Refer to Appendix A, “Upgrades” for licensing information.

10.14 Configuration

10.14.1 Microphone Sound Level Settings

Configure the microphone sound level in Microsoft Windows as follows:

1. Click **Start** and type "**control panel**".
2. In the search results, select **Control Panel**.
3. Click **Hardware and Sounds**.
4. Under Sounds, select **Manager audio devices**. The Sound dialog box displays.
5. Click the **Recording** tab.
6. Double-click **Microphone**. The Microphone Properties dialog box displays.
7. Click the **Levels** tab and set "Microphone" to **100**.
8. Click **OK** and then click **OK** again in the Sound dialog box.

10.14.2 Workstation Configuration Tool Settings

The following settings for NOTIFY-IP are configured in the ONYXWorks Workstation configuration tool. From the workstation application, go to **Menu > Configure > Launch Configuration Tool**.

Table 10.8 Configuration Tool Settings for NOTIFY-IP

Location	Setting	Options	Description
System Options (System > System Options)	**Operating Mode**	Protected Premises Control Unit (PPCU)	NOTIFY-IP operates only in PPCU mode. All nodes on the system must also be set to PPCU mode.
	Mass Notification Priority	All panels, gateways, and workstations in the system must be set to the same setting.	
		MNS Higher than Fire	Mass Notification events have a higher priority than fire events.
		MNS Lower than Fire	Mass Notification events have a lower priority than fire events.
Users (System > Users)	**Allow Paging**	Yes	User has paging permission. **Note:** An Administrator has paging privileges by default.
		No	User does not have paging permission.
Audio Groups (Control > Audio Groups)		An audio group determines how NOTIFY-IP routes voice paging to a specific set of speakers. Refer to 10.15, "Audio Groups" for additional information.	
	Type	All Call	Sends the page to all audio devices on every DVC selected in the group.
		Evacuate	Sends the page only to points on a DVC that are already sounding an evacuation sequence.
		Inactive	Sends the page only to selected amplifiers with no active tasks. Select this group type for low priority pages only.
		Alert	Sends the page only to points on a DVC that are already sounding an alert sequence.
		Direct	Allows the user to individually specify speakers from the VeriFire database to receive the page by indicating their associated PAM point.
		Sequence	Allows the user to activate an audio sequence.The audio sequence must be loaded into a DVC before it can be imported by NOTIFY-IP.

10.15 Audio Groups

10.15.1 Creating an Audio Group

Perform the following steps to create an audio group:

1. Log in to the workstation if not already logged-in. Refer to 6.3.1, "Login".
2. Launch the configuration tool (**Menu > Configure > Launch Configuration Tool**).
3. Go to **Menu > Control > Audio Groups**. The Audio Groups screen displays.
4. Click the **Add** button.
5. Click on the **New** label in the *Name* field and enter a unique name for the audio group.
6. Select the desired group type (refer to Table 10.8) from the drop-down list.
7. Select the input (Mass Notification, Emergency, or General) from the drop-down list. Mass Notification only displays when the workstation is in PPCU operating mode.
8. Select the audio point(s) that are to be associated with the audio group from the tree displayed. Points that can be selected in the tree depends on the audio group type selected as follows:
   - For Inactive, Evacuate, Alert, or All Call audio group types, the user is able to select both DVCs and network zones.
   - For Sequence or Direct audio group types, the user is able to select both PAM Points and network zones.
9. Click **Exit**. The Audio Groups screen closes (audio groups are temporarily saved) and the configuration tool main screen displays.
10. To save the settings:
    - Go to **Menu > File > Save** (save without closing the configuration tool), or
    - Go to **Menu > File > Exit** and click **Yes** to close the configuration tool, save settings and synchronize the system.

10.15.2 Modifying an Audio Group

Modify audio group settings as follows:

1. Open the Audio Groups screen (refer to 10.15.1, "Creating an Audio Group").
2. Select the audio group to be changed from the list at the left-hand side of the screen.
3. Change the settings as desired.
4. Save the settings.

10.15.3 Creating Audio Buttons

Perform the following steps to create audio buttons on the floor plan screen. Audio buttons should be created after configuring the audio group(s).

1. Launch the configuration tool and navigate to the screen on which the audio button is to be placed using the navigation pane on the left-hand side of the configuration tool main screen.
2. Perform one of the following:
   - Click the **Add** menu and select **Audio Button**, or
   - Click the audio button icon ( ) in the tool bar.

   The Audio Button dialog box displays.
3. Click on the default caption for the audio button and enter a unique button caption (if desired).
4. Select the audio group to be associated with the button from the drop down list.
5. Click **OK**. The audio button displays in the graphics window.
6. Resize and move the audio button as desired (refer to 10.15.4, "Manipulating Audio Buttons").

10.15.4 Manipulating Audio Buttons

The table below describes the ways the audio button can be manipulated in the graphics window:

Table 10.9 Manipulating Audio Buttons

Operation	Procedure
Cut	Select the button(s) and: • Press **Ctrl + X**, or • Right-click the button and select **Cut**.
Copy	Select the button(s) and: • Press **Ctrl + C**, or • Right-click the button and select **Copy**.
Paste	Click within the graphics screen and: • Press **Ctrl + V**, or • Right-click and select **Paste**.
Button Selection	**Single Button**: Click the button in the graphics screen. Graphic handles appear. **Multiple Buttons**: • Click the first button, hold down the Shift key, and click the other buttons, or • Use the select tool ( ) to draw a selection box around the buttons. Graphic handles appear indicating selection.
Move	Select the button(s) and drag the button(s) to the desired location.
Resize	Select the button(s) and perform one of the following: • Drag a button graphic handle to the desired size. Each selected button is resized. To proportionally resize the button, drag a corner handle diagonally. • Right-click a button and select **Resize Selected Point(s) To...**. Then use the +/- arrows or type the desired size in the field provided. Each selected button is proportionally resized.
Delete	Select the button(s) and: • Press the **Delete** key, or • Right-click a button and select **Delete Object(s)**. Respond to the confirmation prompt that displays.
View/Change Properties	Right-click a button and select **Properties...**. The Audio Button properties dialog box displays. Change the button caption or associated audio group as desired.
Undo	Undo a change by: • Pressing **Ctrl + Z**, or • Click the Edit menu and select **Undo**.
Redo	To reverse the action of an Undo command, click the **Edit** menu and select **Redo**.

10.16 Voice Paging

Voice paging is only available when the user is logged in to the workstation and audio groups have been created. For more information, refer to 10.15, "Audio Groups".

10.16.1 Preparing to Page

NOTE: The workstation used for voice paging must have an audio driver installed or NOTIFY-IP returns the message, “Audio driver failed to initialize.”

Perform the following steps to prepare to make a page with NOTIFY-IP:

1. Initiate voice paging using one of the following methods:
   - Click an audio button on the floor plan graphics screen.
   - Click an audio group link in the Emergency Audio pane (Menu > View > Emergency Audio).
   - Click an audio group link in the General Audio pane (Menu > View > General Audio).

   A paging dialog box displays depending on the type of audio group:
   - The Live Microphone dialog box opens for All Call, Evacuate, Inactive, Alert, or Direct type audio groups.
   - The Stored Sequence dialog box displays for Sequence type audio groups.

   For all audio group types, the paging priority shown in the dialog box is that of the input channel on the DVC.
2. Make the page using one of the methods described in 10.16.2 to 10.16.4.

10.16.2 Making a Live Page

1. In the Live Microphone dialog box, click **Start Paging** to begin live paging.
2. Speak into the microphone to page.
3. Click **Stop Paging** when finished.
4. Click **Cancel** to close the dialog box.

10.16.3 Previewing the Live Page Before Broadcast

1. In the Live Microphone dialog box, click the **Preview Mode** button to record a message. The Record Message dialog box displays.
2. Click **Record** to begin recording a page.
3. Speak into the microphone to record the page.
4. Click **Stop** when finished recording.
5. Click **Play** to hear a preview of the recorded page.
6. Proceed as follows:
   a. If the recording is satisfactory, go to Step7.
   b. To re-record the page, repeat Steps 2 to 6.
7. Use the up and down arrows to select the number of times for a recorded page to automatically repeat up to nine times.
8. Click **Start Paging** to begin broadcasting the recorded page for the set number of repeat pages. Click **Stop Paging** to stop broadcasting the recorded page before the set number of repeat pages has been completed.
9. Click **Cancel** to close the dialog box.

10.16.4 Making a Sequence Type Page

1. In the Stored Sequence dialog box, click **Start Paging** to begin broadcasting the stored audio sequence.
2. To stop the sequence, click **Cancel**.

10.17 Paging Status Indicators

The following indicators are visible on the right-hand side of the workstation graphic area only if emergency audio is configured:

Table 10.10 Paging Status Indicators

Icon	Appearance	Definition
Primary Icons		
	Black background and all speakers are gray.	Page not active (normal).
	Black background and middle speaker is green.	One or more of the outputs in the group has been activated by a page from a different group. Refer to Table 10.12.
	Black background with all speakers green.	This workstation is actively paging.
Supplementary Icons		
	Yellow triangle with black exclamation symbol.	When this symbol is displayed with one of the icons above, a trouble has occurred on one or more of the points in this group.
	Red circle with white horizontal bar.	When this symbol is displayed with one of the icons above, paging is unavailable to one or more outputs in the audio group due to use by an input with a higher priority.

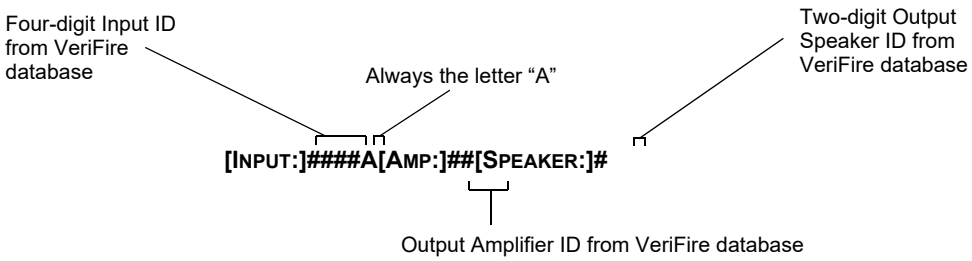
10.18 Troubleshooting

10.18.1 Configuration Problems

10.18.1.1 Problems with Audio Point Selection

PROBLEM: I want to configure an audio point, but it is not listed.

EXPLANATION: Check the audio group type. Different group types allow for different audio points to be configured (refer to Table 10.11). PAM addressing is complex. A single PAM point specifies both the input source (e.g. live microphone, sequence) and output amp and speaker. The input source of the PAM selected must match the input type expected for the selected audio group type. PAM address format is as follows:



For example, **1035A011** = input 1035, Amp 1, Speaker 1. This point would be used for a 'Direct' group, since input 1035 is always used for direct paging.

Table 10.11 Valid Audio Point Configurations

Audio Group Type	Audio Points Available
All Call	DVCs and network zones only.
Evacuate	• Nodes only. • DVC selects which PAM points to activate based on internal logic. Refer to “Audio Group Types” in Table 10.8 for selection criteria.
Inactive	
Alert	
Direct	PAM points are constrained to input: • Input 1035 for fire emergency paging. • Input 1037 for non-emergency paging. Outputs may be independently selected by amplifier and speaker ID.
Sequence	PAM points constrained to inputs between 0031 and 1030 inclusive. **Note:** Input 0031 corresponds to Sequence 1 in the DVC. For all sequence numbers add 30 to determine input number.

10.18.1.2 Missing Audio Points

PROBLEM: DVCs or their PAM points are not listed in selectable audio points.

SOLUTION: First refer to 10.18.1.1, "Problems with Audio Point Selection". If this does not help, the configuration tool most likely does not have knowledge of the desired point(s). You have two options:

- Add the point manually.
- Import the DVC’s Verifire database. If there are problems importing the database, make sure the DVCs database version is up to date. If not, update the panel database using Verifire Tools and try again.

10.18.2 Activation Problems

The following table describes possible problems related to activation:

Table 10.12 Activation Problems

Problem Reported	Problem	Definition
After Paging		Any problems which occur during the page are reported upon completion.
	Network Disconnected	No communication to target network. This may indicate that a gateway is the wrong version. Note that all gateways using paging must be version 3.18 or later.
	Preempted by DVC	The DVC was already paging or an input with a higher priority was activated on the DVC during the page.
	Preempted by another Workstation	Another workstation was already paging.
	Audio Inactive	No microphone input was detected for 30 seconds. Check the microphone input.
	Trouble	The desired DVC was in a Trouble state.
Problems Reported During or After Paging		These problems can occur either before of after the page.
	All Networks Disconnected	Possible IP trouble. Check local IP connection. Also see “Network Disconnected,” above.
	The Audio Group is empty	Bad configuration. Refer to 10.15.1, "Creating an Audio Group" for configuration information.
	Audio driver failed to initialize	Correct driver may not be installed.
	Sound driver does not support paging	Make sure the workstation is running on an approved workstation PC.

10.18.3 Problems Involving Group Types

PROBLEM: Evacuate or Alert pages do not work as expected.

EXPLANATION: Evacuate and Alert pages are set up in order to override Evacuate or Alert sequences set up by the DVC. An Evacuate or Alert page will not sound unless a DVC is already sounding a sequence which is set up as the corresponding type (Evacuate or Alert).

10.18.4 Group Type Hierarchy

Group type hierarchy is as follows:

- All-Call pages take over the entire DVC.
- Sequence and Direct pages take control of the speakers specified in their PAM points.
- Evacuate pages take control of speakers actively engaged in an Evacuate sequence.
- Alert pages take control of speakers actively engaged in an Alert sequence.
- Inactive pages sound on any speakers on the DVC which are not currently being paged.

All live pages participate in the DVC’s configured priority matrix and preempt or are preempted by other DVC inputs accordingly.

Appendix A Upgrades

A.1 Software Version 4 Upgrade Overview

When upgrading to software version 4, the following considerations apply:

- Windows 10 Pro or Enterprise 64-bit is required to operate version 4 of the workstation software.
- Version 4 of the workstation software is only compatible with the UL and ULC listed PCs purchased since January 2015. The part number for compatible UL and ULC workstation is 51-HFS12-001 and is displayed on a label on the back of the workstation.
- Versions 4.10 - 4.22/4.23 of the workstation software only support embedded gateways that are running on HS-GW-EM or HS-GW-EMPCB hardware.
- Versions 4.30 and higher of the software only support embedded gateways which are running on HS-GW-EMPCB hardware.
- Hardware information may be viewed from the gateway configuration tool as follows:
  a. Log into the gateway. The gateway configuration tool displays.
  b. View the gateway Board Type property. If the Board Type property value is not listed due to an older version of the software, contact Technical Support.
- With Version 4, FirstVision units operate on the same platform as the workstation and are required to run on the same software version as the workstation. Refer to the FirstVision *Installation and Operation Manual* (P/N LS10079-000NF-E) for Version 4 upgrade instructions.
- Version 4 of the software does not support Echelon Gateways or any NION hardware.
- Version 4 of the workstation only supports upgrades from version 3.x. In addition, the upgrade does not support the following systems:
  – NCS
  – UniNet2000
  – VGAS
  – Any other additional software
- When upgrading old versions of the NFN Gateway, it may be necessary to use the "Download Utility" that is installed along with the workstation software. Proceed as follows:
  1. In Windows 10, go to **Windows Start Menu > All apps > Facilities Monitoring > Download Utility**.
  2. Enter the gateway IP address.
  3. Click the File Name field. An Open dialog box displays containing the archive files installed on the workstation PC.
  4. Select appropriate archive file from the list. The archive file name information is described in the NFN Gateway manual (refer to Main Menus - Upgrade Firmware).
  5. Click **Open**.

A.2 Upgrade Decision Matrix

The version of the software and the hardware for an existing workstation system determines the process for upgrading to version 4. Select the applicable upgrade procedure using the following table:

Table A.1 Software Upgrade Decision Matrix

Current Condition	Perform...
If the workstation software is version 3.x and an Echelon gateway is configured in the system...	A.3
If the UL/ULC listed workstation PC was purchased prior to January 2015 and is running workstation software 3.x...	A.4
If the UL/ULC listed PC was purchased since January 2015 and is running workstation software 3.18 or later...	A.5
If updating workstation software from Matrix v. 4.52 to 4.60 and higher...	A.6

A.3 Upgrading Systems with Echelon

Since this PC was purchased prior to January 2015, it does not support version 4.X of the workstation software and the Windows 10 operating system. The general procedure for this upgrade is to back up the data from the PC, restore the data on the new PC, and migrate existing points from the Echelon Gateway to an NFN Gateway. The steps for this upgrade are as follows:

1. Follow procedure in 7.1.1, "Backing Up the Database" to back up the existing data.
2. Follow procedure 7.1.2, "Restoring a Backed-Up Database" to restore the data on the new PC.
3. If the system contained an Echelon Gateway and NIONs, the Migrate Node option in the workstation configuration tool must be used. Proceed as follows:
   a. From the workstation, open **Menu > Configure > Launch Configuration Tool**.
   b. In the configuration tool, go to **Menu > Monitoring > Networks**. The Networks window displays.
   c. Click the node label in the navigation tree, and click the **Migrate Node** button.The Migrate Node window displays.
   d. Select the network to which the node is to be migrated and enter a unique node number for the node.
   e. Click **OK**.
4. Upgrade the embedded gateways.

   If the embedded gateway, running on the HS-GW-EM or HS-GW-EMPCB hardware, is running software prior to version 3.18, it must first be upgraded to version 3.18 before it will upgrade to any later version.

   NOTE: Software versions 4.30 and higher only supports HS-GW-EMPCB hardware.

5. When ready to activate the workstation license, perform steps in Section 3, "Workstation License Activation".

A.4 Upgrading Systems with an Older PC and WS Software 3.X

Since this PC was purchased prior to January 2015, it does not support version 4.X of the workstation software and the Windows 10 operating system. The general procedure for this upgrade is to back up the data from the existing PC and then restore the data on the new PC. The steps for this upgrade are as follows:

1. Perform the procedure in 7.1.1, "Backing Up the Database" to back up the existing data.
2. Perform the procedure 7.1.2, "Restoring a Backed-Up Database"to restore the data on the new PC.
3. Upgrade the embedded gateways.

   If the embedded gateway, running on the HS-GW-EM or HS-GW-EMPCB hardware, is running software prior to version 3.18, it must first be upgraded to version 3.18 before it will upgrade to any later version.

   NOTE: Software versions 4.30 and higher only support HS-GW-EMPCB hardware.

4. When ready to activate the workstation license, perform steps in Section 3, "Workstation License Activation".

A.5 Upgrading Systems with UL-listed PCs Purchased after January 2015

A.5.1 Overview

Licensing of workstations is now performed using the Flexera Cloud-based application. To upgrade to the latest workstation software, USB key (dongle) based licensing must be converted to Cloud-based licensing via the Honeywell Connected Life Safety Services (CLSS) Web portal.

Upgrading the workstation software license consists of the following main processes:

- Installing the Key Migrator utility on the workstation PC in order to view and capture the information required for the upgrade.
- Recording the workstation to be upgraded on the CLSS Web portal.
- Migrating the license from USB key (dongle) based license to a Cloud-based license and inactivating the USB key.
- Downloading and installing the new software version on the workstation.

A.5.1.1 Prerequisites

Prerequisites include the following:

- If the workstation software is v3.x, Upgrade Kit P/N WIN10-UG is required to upgrade the workstation.
- Internet connection is required for software download and license generation.
- There must be at least one person with permissions to log into the CLSS Web Portal.
- The workstation database should be backed up as specified in 7.1.1, "Backing Up the Database".

A.5.1.2 Personnel - Information Transfer

The upgrade process is performed by trained ESD technicians. Examples:

- There can be a single technician who has administrator-level privileges and access to the Honeywell CLSS Web Portal and can perform all of the upgrade steps.
- There can be a team of two technicians; one at the worksite and one at another location who has administrator-level privileges and permissions to access to the Honeywell CLSS Web Portal. Information and files needed for the upgrade is transmitted between the two technicians.

Information transfer (if necessary) can be accomplished using convenient methods as determined by the personnel doing the upgrade and the type of information being transmitted such as:

- Email
- Smart Phone
- Text Message
- USB Flash Drive

A.5.2 Gathering Workstation Information

On the workstation go to **Help > About** and note the following for later use:

- Current Software Version
- Dongle Serial #

A.5.3 Recording Workstations in the CLSS Portal and Generating the License File

Prior to upgrading the workstation software license, the workstation PC must be recorded in the Honeywell CLSS Web portal. The technician recording the PC must have the following information for each workstation PC to be recorded:

- Workstation Brand
- From the **Help > About** on the workstation PC:
  - Serial number of the dongle
  - Software version currently on the workstation
- From Key Migrator Utility:
  - Workstation ID number
  - Feature ID (Code)



NOTE: For efficiency, it is recommended all Customer workstations at a site that require upgrade should be recorded before migrating licenses.

Record the workstation PC to be licensed as follows:

1. Using an Internet browser, go to fire.honeywell.com. The Honeywell CLSS Web Portal home page displays.
2. Log in as follows:
   a. Click **Sign In** (top right of the screen).
   b. Double-click the appropriate user account.
   c. Enter your username and password, and then click **Sign In**. The *All Customers* page displays.
3. At the left side of the screen, click the **Feature Activation** icon . The *Feature Activation* screen displays.

4. Click on **All Customers**. The *Select Customer/Site/Building* screen displays.
5. Select the Customer from the list. Then click **Apply**. The *Feature Activation* screen for the selected customer displays.
6. Click **Workstations** and then on **ADD WORKSTATION** tab.
7. Select **Record an Existing Workstation to Upgrade** and click **NEXT**. The *Add Workstation* screen displays where information about the workstation PC to be upgraded must be entered.
8. Provide the following information:
   - Enter/paste the dongle (USB key) serial number
   - Select the workstation PC brand from the drop-down list.
   - Select the hardware type (UL Listed or Customer PC) from the drop-down list. (Note: This may auto-populate depending on the brand.)
   - Select the software version currently on the workstation PC from the drop-down list.
   - Select the site from the drop-down list (if any).
   - Select the building from the drop-down list (if any).
9. Click **ADD**. A success message displays. Details about the workstation are shown.
10. Click the **DOWNLOAD UPGRADE UTILITY** link. The Download Center web page displays.
11. Search for and select the Key Migrator Utility and click **DOWNLOAD**. The utility is downloaded to the local PC *Downloads* folder.
12. Proceed as follows:
    - If the local PC is the workstation to be upgraded, go to step 13.
    - If the local PC is not the workstation to be upgraded, transport/send the Key Migrator utility to the worksite, and load the file on the workstation to be upgraded. Then go to step 13.
13. Ensure the dongle is connected to the workstation PC and then browse to and open the Key Migrator utility. The utility reads the information on the dongle and workstation PC and populates the fields in the Key Migrator window (see Figure A.1).

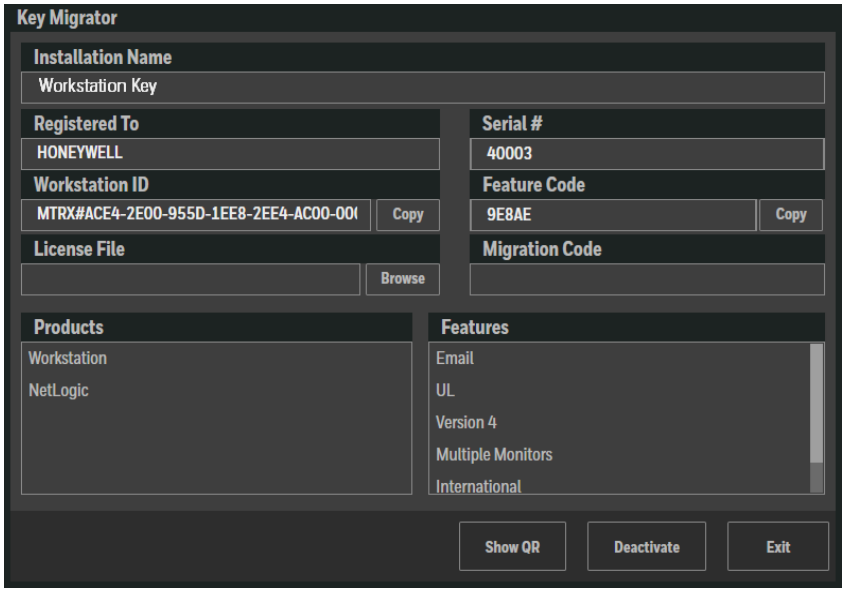


Figure A.1 Key Migrator Utility Window

14. Capture the following information for use in subsequent steps:
    - Feature Code
    - Workstation ID

    To capture this information you can, for example:
    - Click the **Copy** buttons next to the Workstation ID and Feature Code fields to copy the information to the clipboard. If necessary, the serial number can also be selected and copied (Ctrl + C).
    - Take a photo of the Key Migrator window with a smart phone.

    This information can then be pasted/entered directly into fields in the CLSS portal if there is Internet access on the workstation PC or transported/transmitted to a PC with CLSS portal access.
15. Click **UPGRADE NOW**. The *Upgrade Workstation-Workstation Details* tab displays.
16. Enter/paste the **Workstation ID #** and **Feature ID** (from the Key Migrator) in the fields provided and click **Next**. The *Feature Selection* tab displays the features currently applied to the workstation.
17. Click **Next**. The *License Generation Tab* displays.

18. Select **Upgrade License** and click **UPGRADE**. A success message indicates a successful upgrade and a summary page displays for the workstation.
19. Click **Download License**. The license file (.bin) is downloaded to the local PC's *Downloads* folder.
20. Browse to the *Downloads* folder on the local PC, copy the license and software files, and:
    - If the CLSS Web portal is accessed using a non-workstation PC, send the files to the worksite on a USB flash drive or as an email attachment. Then go to A.5.4, "Upgrading the License on the Workstation".
    - If the CLSS Web portal is accessed on the workstation PC, go to A.5.4, "Upgrading the License on the Workstation".

A.5.4 Upgrading the License on the Workstation

A.5.4.1 Prerequisites

- The Key Migrator utility must be installed on the workstation to be upgraded. Refer to A.5.2, "Gathering Workstation Information"
- The workstation PC must be recorded in the CLSS portal (see A.5.3, "Recording Workstations in the CLSS Portal and Generating the License File").
- The license upgrade (.bin) file must be installed on the workstation PC.
- The USB key (dongle) must be connected to the workstation PC.

A.5.4.2 License Migration Procedure

Migrate the license on the workstation PC as follows:

1. Exit the workstation application (if running).
2. Open the Key Migrator utility (see Figure A.2) on the workstation PC (**Start >** type **Key Migrator**).

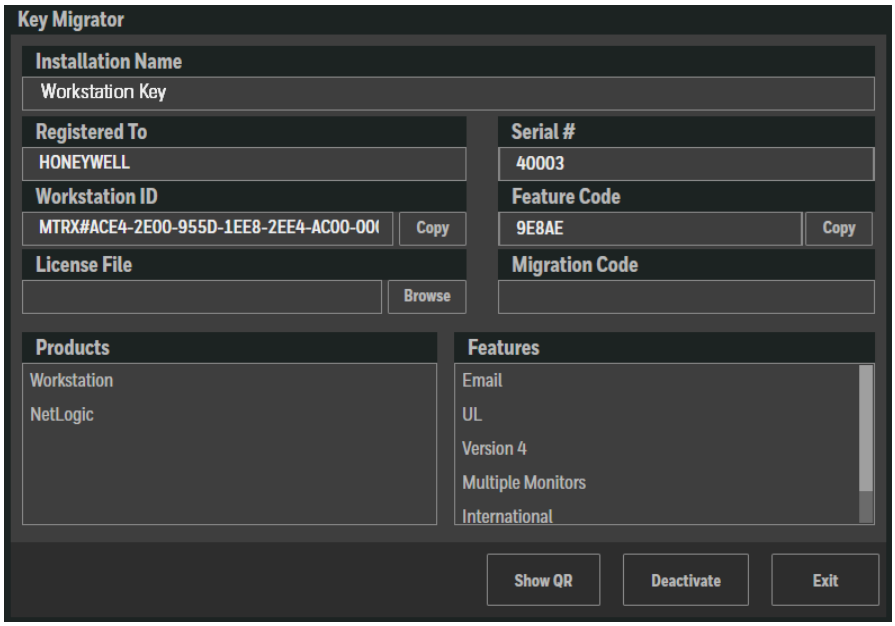


Figure A.2 Key Migrator Window

3. Click **Browse** next to the *License File* field and navigate to the location of the license upgrade file (.bin).
4. Double-click the license file. The filename displays in the Key Migrator *License File* field.
5. Click the **Deactivate** button. The *Migration Code* field populates, a Notepad file (.txt) is generated and stored on the workstation PC, and the dongle is deactivated. The Notepad file contains the Workstation ID, Feature Code, and the Migration Code and may be saved in workstation records for future reference.
6. Remove the USB key from the Workstation PC.
7. Go to A.5.5, "Downloading the Workstation Software".

A.5.5 Downloading the Workstation Software

During an upgrade, the latest software must be downloaded and then loaded on the workstation PC at the worksite. Download the software through the CLSS Portal as follows:

1. Using an Internet browser, go to fire.honeywell.com. The Honeywell CLSS portal displays.
2. Log in as follows:
   a. Click **Sign In**.

b. Double-click the appropriate user account.

c. Enter the account password and click **Sign in**. The CLSS main window for the selected account displays.

3. At the left side of the screen, click the **Feature Application** icon . The feature activation screen for the selected customer displays.
4. Click on **Workstations**.
5. At the top-right side of the screen, click the **All Customers** button and select the customer name/building from the list. Then click **Apply**. The feature activation screen for the selected facility displays showing details about any workstations at the site.
6. Click **PACKAGES**. The login screen for your brand's ESD website displays
7. Enter the username and password and click **Sign in**.
8. Download the applicable workstation application software for the brand.
9. Install the software on the workstation PC.
10. Go to A.5.6, "Final Steps".

A.5.6 Final Steps

1. Click the Windows **Start** icon on the workstation PC and type **License Manager**.
2. Double-click the **License Manager** app.
3. In License Manager (see Figure A.3):

a. Click the browse button (**…**).

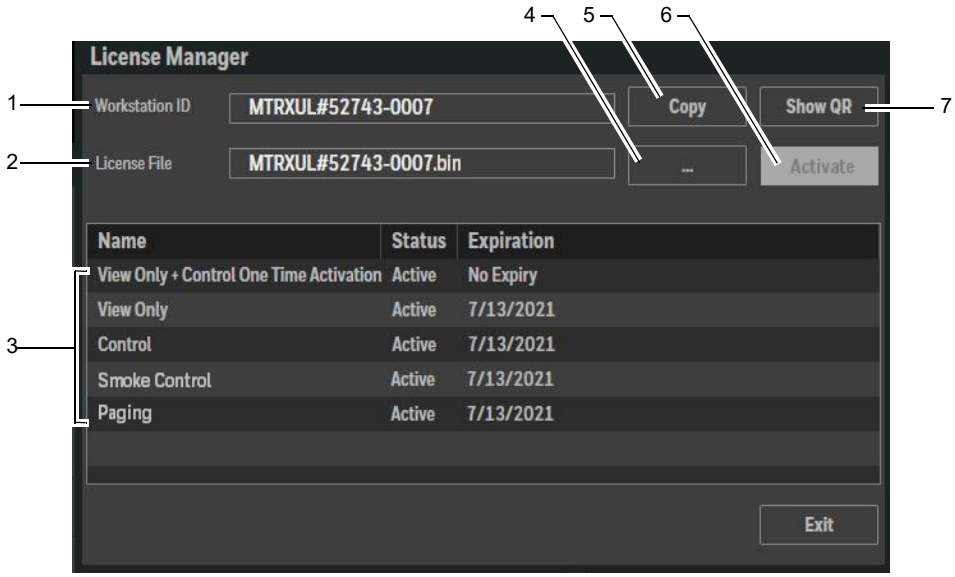
b. Navigate to the location of the license file.

c. Double-click on the license filename (.bin extension).

d. Enter the migration code from the text (.txt) file created in the A.5.4.2, "License Migration Procedure" when prompted and click **OK.** The filename displays in the License File field.

e. Click **Activate**. A message in the License Manager window indicates successful license activation. Click **OK**. The licensed features are displayed in the features list. Once activated, the software license is valid for 5 years.

f. When finished, click **Exit**.



Item	Feature	Description
1	Workstation ID	Auto-generated ID number of the workstation to be licensed.
2	License File	Displays the license file name.
3	Features List	Displays the licensed features active on the workstation and their status.
4	Browse Button	Click to browse to the location of the license file (.BIN).
5	Copy Button	Copies the Workstation ID to the clipboard.
6	Activate Button	Click to activate the selected license file.
7	Show QR	Displays the Workstation ID QR code to scan with a mobile device.

Figure A.3 License Manager Layout

4. Launch the workstation application from Windows 10 as follows:
   a. Click the Windows **Start** icon.
   b. Type "**workstation**" in the search field and **Enter**.
   c. Click the workstation application link in the search results window. The workstation application launches.
5. Log into the workstation and verify that the licensed features are activated. If not, contact Technical Support.

NOTE: Once the license file (.bin) file has been successfully used, it can be deleted from the workstation, if desired.

6. Perform the procedure 7.1.2, "Restoring a Backed-Up Database"to restore the data on the new PC.
7. Upgrade the embedded gateways.
   If the embedded gateway, running on the HS-GW-EM or HS-GW-EMPCB hardware, is running software prior to version 3.18, it must first be upgraded to version 3.18 before it will upgrade to any later version.

NOTE: Software versions 4.30 and higher only support HS-GW-EMPCB embedded gateway hardware.

A.6 Upgrading Matrix v. 4.52 Workstation to v. 4.60

Perform the upgrade as follows:

1. Perform the procedure in 7.1.1, "Backing Up the Database" to back up the existing data.
2. Exit the workstation application.
3. Download the Matrix v. 4.60 workstation application and the OWDOCS.exe documentation file from the NOTIFIER website onto the PC. Proceed as follows:
   - If software download is being performed on the workstation PC, navigate to the *Downloads* folder and double click the workstation application setup.exe file. Then go to step 4.
   - If software download is being performed on a non-workstation PC, navigate to the *Downloads* folder and copy the workstation application and documentation OWDOCS.exe file to a USB drive for transport to the workstation PC. Copy the downloaded files from the USB drive onto the workstation PC and double-click the workstation application setup.exe file. Then go to step 4.
4. Click **Yes** to the "allow changes to computer" message that displays.
5. Follow the on-screen prompts to allow the software installation to proceed. Accept all software licensing agreements. Additional installation wizards may appear during the installation that may include:
6. Microsoft Access Database Engine Installation Wizard - Click **OK** to proceed.
7. Facilities Monitoring - InstallShield Wizard - Click **Finish** to proceed. A computer restart message displays.
8. Click **Yes**. The computer restarts.
9. Navigate to the *Downloads* folder on the workstation PC's C:Drive and double-click the EXE file with a filename that begins with "OWDOCS" to install the user documentation onto the PC at C:\FacilitiesMonitoring\Documentation.
10. Launch the workstation application from Windows 10 as follows:
    a. Type "**workstation**" in the search field and **Enter**.
    b. Click the workstation application link in the search results window. The workstation application launches.
11. Log into the workstation application. If prompted to change the password, enter a new password with the following characteristics:
    - 8 characters maximum
    - Must have at least 1 uppercase letter, 1 numeric character, and one special character
12. Click **OK**. The workstation application opens.
13. Verify that the workstation is operating properly.

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

NOTIFIER
12 Clintonville Road
Northford, CT 06472-1610 USA
203-484-7161
www.notifier.com

NOTIFIER®
by Honeywell