

Embedded NFN Gateway

NFN-GW-EM-3

Installation and Operation Manual



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.

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

The most common cause of life safety system malfunction is inadequate maintenance. To keep the entire life safety system in excellent working order, ongoing maintenance is required per the manufacturer's recommendations, and UL and NFPA standards. At a minimum, the requirements of NFPA 72 shall be followed. Environments with large amounts of dust, dirt, or high air velocity require more frequent maintenance. A maintenance agreement should be arranged through the local manufacturer's representative. Maintenance should be scheduled 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-D2-2016

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

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

Like all solid state electronic devices, this system may operate erratically or can be damaged when subjected to lightning induced transients. Although no system is completely immune from lightning transients and 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 radio-electriques depassant les limites applicables aux appareils numeriques de la classe A prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

HARSH™, NIS™, and NOTI-FIRE-NET are all trademarks; and Acclimate® Plus™, eVance®, 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.

© 2019 by Honeywell International Inc. All rights reserved. Unauthorized use of this document is strictly prohibited.

Software Downloads

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

Documentation Feedback

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

On-Line Help – Please include the following information:

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

Documents – Please include the following information:

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

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

Manual Usage

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

Table of Contents

Section 1 Product Overview	7
1.1: Operation	7
1.2: Functionality	7
1.3: Recommended Cybersecurity Practices	7
1.4: Required Software	7
1.5: Environmental Requirements	7
1.6: System Architecture.....	7
Figure 1.1 Direct Panel Architecture	7
Figure 1.2 Single NFN Network Architecture.....	8
Figure 1.3 Multiple NFN Networks Architecture.....	9
1.6.1: Redundancy	10
Figure 1.4 Redundant NFN-GW-EM-3s.....	10
1.7: IP Requirements.....	11
1.7.1: IP Port Settings	11
1.7.2: Bandwidth Usage.....	11
1.7.3: IP Restrictions.....	11
1.8: Agency Listings	12
1.8.1: Standards.....	12
1.8.2: Agency Restrictions and Limitations.....	12
1.9: Compatible Equipment	13
Table 1.1 Compatible Equipment	13
1.10: Upgrades	13
1.11: PCB Board Type Supported by Software Version 4.30 and Later	13
Section 2 Installation.....	14
2.1: Required Equipment	14
2.1.1: NFN-GW-EM-3 Assembly:.....	14
2.1.2: Network Components:	14
2.1.3: Customer Supplied Equipment:	14
2.2: Board Installation.....	15
Figure 2.1 NFS-320 Series Installation.....	15
Figure 2.2 NFS2-640 Series Installation.....	15
Figure 2.3 CHS-4L Installation.....	15
Figure 2.4 Securing the Board	15
2.3: Connections	16
2.3.1: Connecting to the NFN-GW-EM-3	16
Figure 2.5 NFN-GW-EM-3 Connections	16
Table 2.1 Connection Specifications	16
Figure 2.6 NFN-GW-EM-3 LEDs	17
Table 2.2 LED Definitions.....	17
2.3.2: Trouble Relay Connections	18
Figure 2.7 TB-1 Trouble Relay.....	18
2.3.3: Connecting to a Standard NCM.....	19
Figure 2.8 Routing Power and Communication to a Standard NCM	19
Table 2.3 Standard NCM Connections	19
2.3.4: Connecting to an HS-NCM	20
Figure 2.9 Routing Power and Communication to an HS-NCM.....	20
Table 2.4 HS-NCM Connections.....	20
2.3.5: Connecting to a Fire Alarm Control Panel (FACP).....	21
Figure 2.10 Connecting to an FACP.....	21
2.3.6: Connecting to the PNET-1 Surge Suppressor	21
Figure 2.11 Connecting to the PNET-1	21
2.4: System Power	22
Table 2.5 Power Requirements	22
2.5: Testing and Maintenance	22
Section 3 Configuration	23
3.1: Configuration Web Page.....	23
3.2: Configuring the NFN-GW-EM-3	23
3.2.1: Logging into the Web Page	23
3.2.2: Basic Configuration Tool Layout	24
Figure 3.1 Basic Configuration Tool Layout.....	24

3.2.3: Main Menus	25
Table 3.1 Main Menus	25
3.2.4: Product Information	26
Table 3.2 Product Information	26
3.2.5: Additional Properties	27
Table 3.3 Additional Properties	27
3.2.6: Node List	29
3.2.7: Error Log	29
Table 3.4 Error Log Descriptions	29
3.3: Security Certificate	29
Figure 3.2 Chrome Security Warning Example.....	29
3.4: Web Portal Setup	30
3.5: Client Monitoring	31
Table 3.5 Client Monitoring Use Cases	31
Appendix A Gateway Settings.....	32
A.1: Viewing Existing IP Settings	32
A.2: Resetting Factory Default Values	32

Section 1 Product Overview

1.1 Operation

The NFN-GW-EM-3 serves as a bridge between an ONYXWorks[®] Workstation or ONYX[®] FirstVision[™] and the connected Fire Alarm Control Panels (FACPs), NFN network, or high-speed NFN network.

The web portal feature serves as a bridge between eVance[®] and the connected FACPs, NFN network, or high-speed NFN network.

1.2 Functionality

The NFN-GW-EM-3 translates the protocols and facilitates communications between an ONYXWorks Workstation or ONYX FirstVision and the connected FACPs, NFN network, or high-speed NFN network; to protocols used by the workstation or FirstVision.

The web portal feature transmits network events and system information between eVance and the connected FACPs, NFN network, or high-speed NFN network. This information is used for maintenance purposes only.

1.3 Recommended Cybersecurity Practices

Highly recommended cybersecurity practices for the NFN-GW-EM-3 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 Required Software

Chrome[™] is required for use with the NFN-GW-EM-3.

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 15-27° C (60-80° F).

1.6 System Architecture

An Internet or Intranet IP network connection is used with the architectures described in [Figures 1.1, 1.2, and 1.3](#).

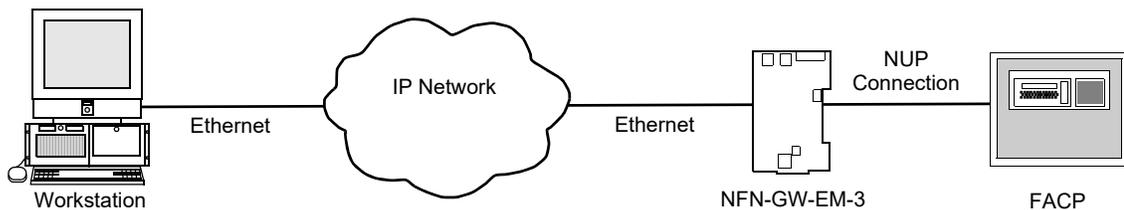


Figure 1.1 Direct Panel Architecture

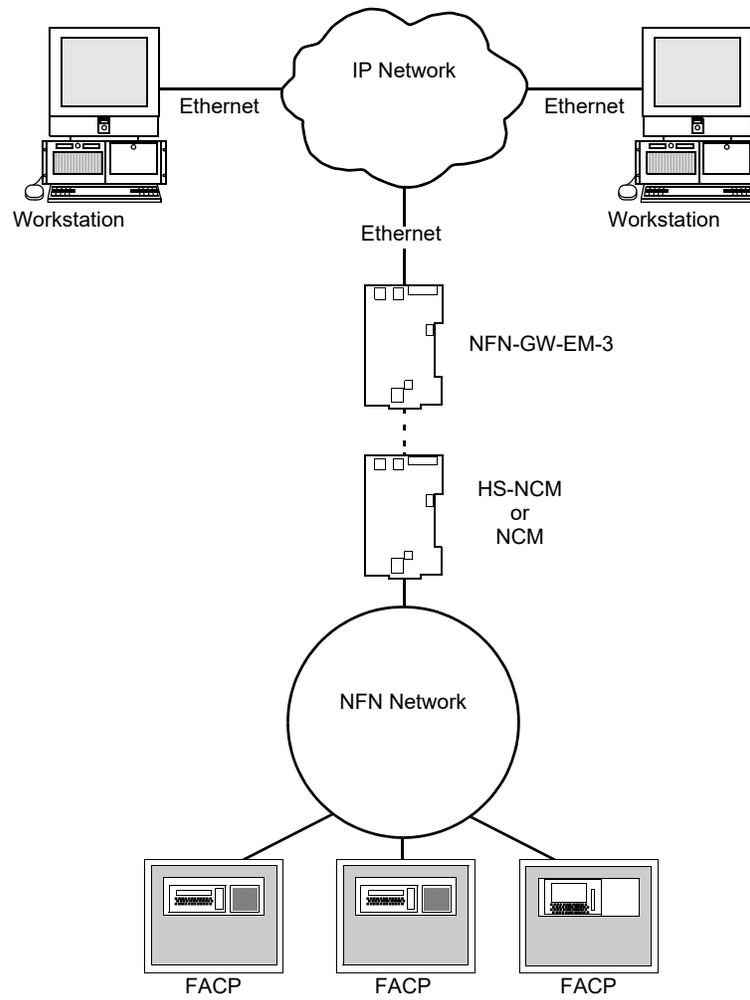


Figure 1.2 Single NFN Network Architecture

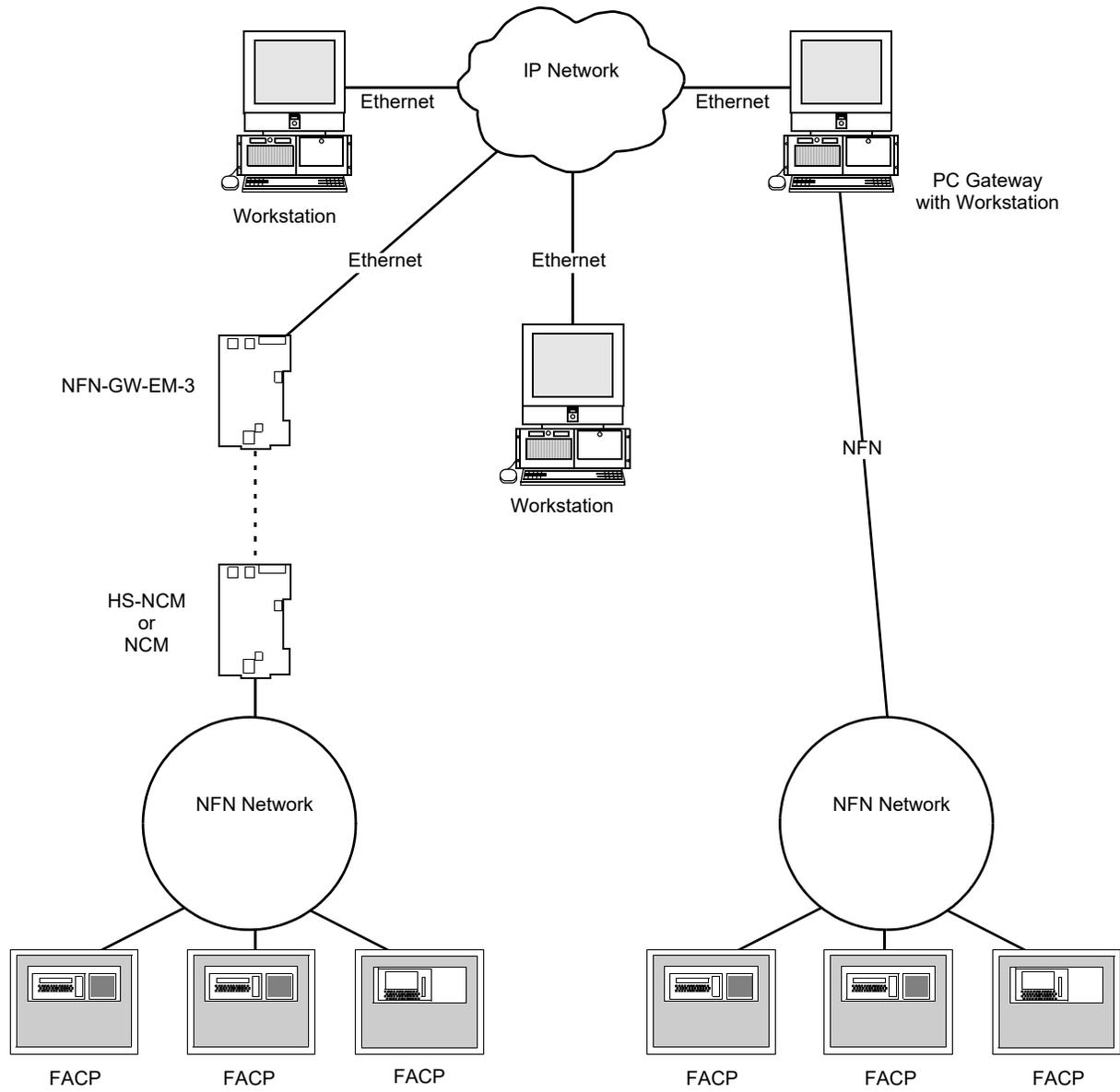


Figure 1.3 Multiple NFN Networks Architecture

1.6.1 Redundancy

A redundant gateway is a second gateway which communicates with an NFN network. If the main gateway cannot be reached, the system attempts to communicate with the network through the redundant gateway. For more information about configuring redundant gateways, refer to the *ONYXWorks Workstation Installation and Operation Manual*.

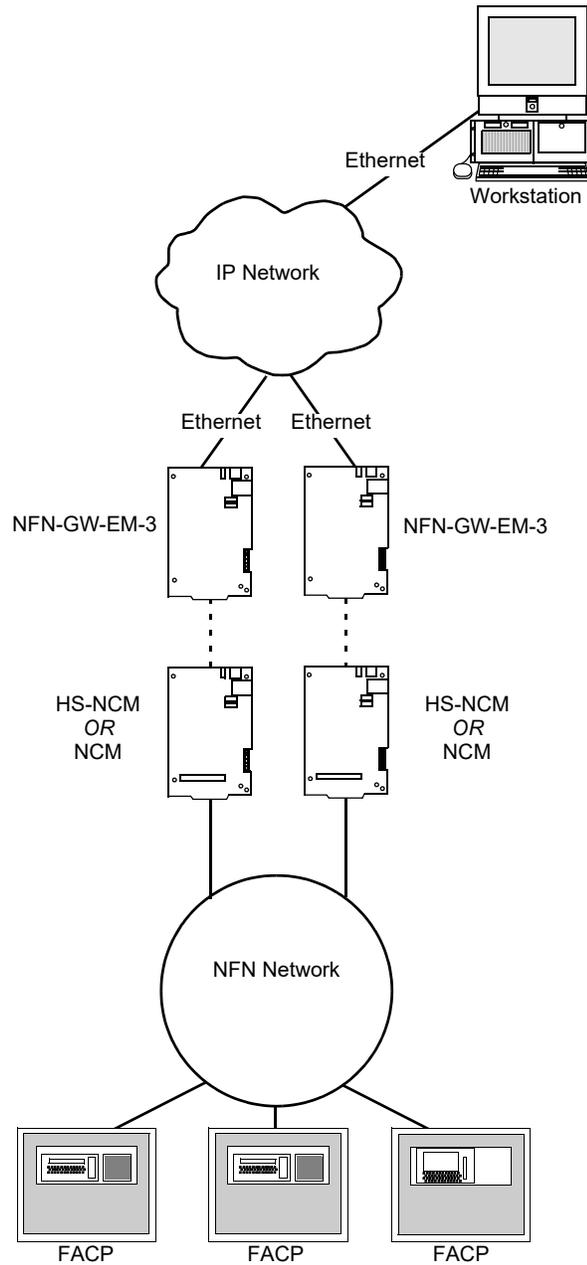


Figure 1.4 Redundant NFN-GW-EM-3s

1.7 IP Requirements

1.7.1 IP Port Settings

The following IP ports must be available to the NFN-GW-EM-3:

Port	Type	Direction	Purpose
53	UDP and TCP	Out	DNS resolution: The optional web portal feature in the NFN-GW-EM-3 must resolve www.evanceservices.com for communications to the eVance server.
80	TCP	In	Web Based Configuration
123	UDP	Out	SNTP
443	TCP	In/Out	HTTPS Communications: The NFN-GW-EM-3 will accept connections on port 443 for configuration of the NFN-GW-EM-3. Typically, this incoming connection is local to the site intranet and not externally from the Internet. The optional web portal feature in the NFN-GW-EM-3 will communicate out to the eVance server on the Internet (www.evanceservices.com) when configured for eVance operations.
2017	TCP	In	Connection from Workstation (Events and Commands)
4016	TCP	In	Upgrade for Embedded Gateway
5000	TCP	In	VeriFire Tools Access
5100	TCP	In	Voice Paging

1.7.2 Bandwidth Usage

Worst Case Sustained Bandwidth	No. Workstations	Bandwidth
Typical	50	2520 Bytes/Sec 20160 bit/Sec 0.020 Mb/Sec (Approx.)
Maximum	50+ Audio	14670 Bytes/Sec 117360 bit/Sec 0.118 Mb/Sec (Approx.)

1.7.3 IP Restrictions

The following restrictions apply:

- Must have a static IP address. DHCP is not supported.
- The use of a NAT is not supported.
- Web access via an HTTP Proxy is not supported.

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 72 National Fire Alarm and Signaling Code

Underwriters Laboratories

- UL 864 Control Units for Fire Alarm Systems, Tenth Edition
- UL 1076 Proprietary Burglar Alarm Units and Systems, Fifth Edition (Certified Applications Only)
- UL 2017 General Purpose Signaling Devices and Systems, Second Edition
- UL 2572 Mass Notification Systems, Second Edition

Underwriters Laboratories Canada

- CAN/ULC S527-11 Standard for Control Units for Fire Alarm Systems, Third Edition
- CAN/ULC S559-13 Standard for 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
- NFPA 101 Life Safety Code

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 this product is sharing on-premises communication equipment, the shared equipment shall be “listed for the purpose”. “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 web portal feature is listed for supplementary use only.

1.9 Compatible Equipment

The NFN-GW-EM-3 is compatible with the following equipment.

Table 1.1 Compatible Equipment

Type	Equipment
Fire Panels:	<ul style="list-style-type: none"> • NFS-320 • NFS2-640 • NFS2-3030
Network Cards:	<ul style="list-style-type: none"> • NCM-W, NCM-F • HS-NCM-W, HS-NCM-SF, HS-NCM-MF, HS-NCM-WSF, HS-NCM-WMF, HS-NCM-MFSF
Workstation:	<ul style="list-style-type: none"> • ONXYWORKS-WS
Other Products:	<ul style="list-style-type: none"> • BACNET-GW-3 • CAP-GW • DVC • FIRSTVISION • LEDSIGN-GW • MODBUS-GW • NCA-2 • NCD • NWS-3 • VESDA-HLI-GW

1.10 Upgrades

When upgrading old versions of the NFN Gateway, 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 [Table 3.1, "Main Menus"](#) (Upgrade Firmware).
5. Click **Open**.

1.11 PCB Board Type Supported by Software Version 4.30 and Later

Software version 4.30 and later does not support EMPCA board types. Only EMPCB board types are supported.

Section 2 Installation

2.1 Required Equipment

2.1.1 NFN-GW-EM-3 Assembly:

The following components are shipped with the NFN-GW-EM-3:

- NFN-GW-EM-3 Printed Circuit Board
- Surge Suppressor (P/N PNET-1)
- NUP-to-NUP Cable (P/N 75577) - Used to connect the NFN-GW-EM-3 board to an NCM-W or NCM-F board or supported panel.
- Wire Leads-to-NUP Cable (P/N 75583) - Used to connect 24V power from the NFN-GW-EM-3 board to an NCM-W or NCM-F board.
- USB Cable (P/N 75665) - Used to connect the NFN-GW-EM-3 board to an HS-NCM board:
 - HS-NCM-W – HS-NCM-MF
 - HS-NCM-WMF – HS-NCM-SF
 - HS-NCM-WSF – HS-NCM-MFSF

2.1.2 Network Components:

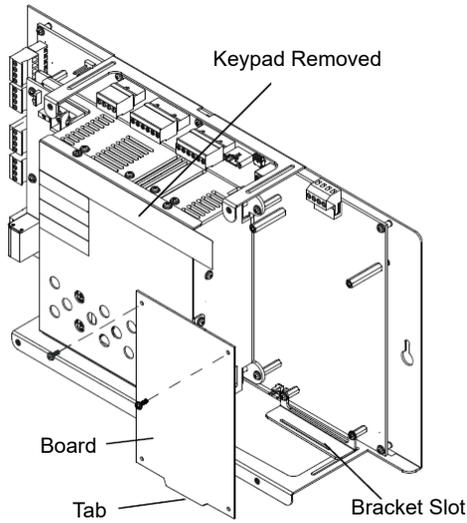
- High-speed Network Communication Module (HS-NCM) - Used to facilitate network communication between the NFN-GW-EM-3 and a High-Speed NFN network (sold separately)
OR
- Network Communication Module (NCM) - Used to facilitate network communication between the NFN-GW-EM-3 and an NFN network (sold separately)
OR
- Compatible FACP with NUP Port

2.1.3 Customer Supplied Equipment:

- Computer - Used to run a web browser to configure the NFN-GW-EM-3. Refer to [1.4, "Required Software"](#) for recommended browsers.
- Ethernet Patch Cable - Used for connecting the NFN-GW-EM-3 to Local Area Network (LAN).

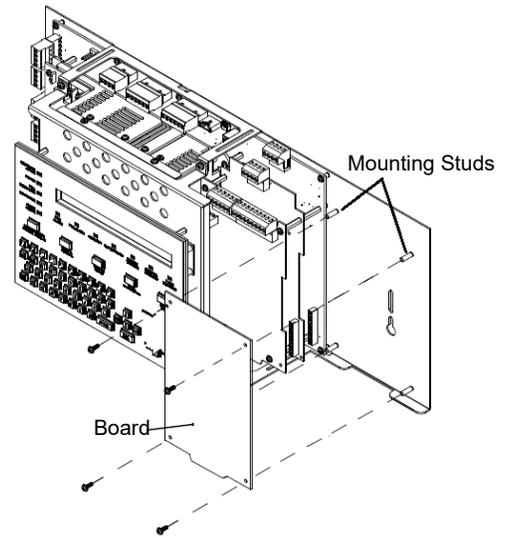
2.2 Board Installation

The NFN-GW-EM-3 may be installed in a CAB-3 or CAB-4 cabinet as shown below.



Install bracket on 1/2" standoffs. Place the board's tab in the bracket slot and screw the board to the top of the standoffs. May be stacked in front of or behind another board using standoffs of adequate length to clear the rear board.

Figure 2.1 NFS-320 Series Installation



Mount in 4th column of the NFS2-640 Series chassis. Mount chassis to backbox before installing the board in rear position. May be mounted in front of another board using standoffs of adequate length to clear the rear board.

Figure 2.2 NFS2-640 Series Installation

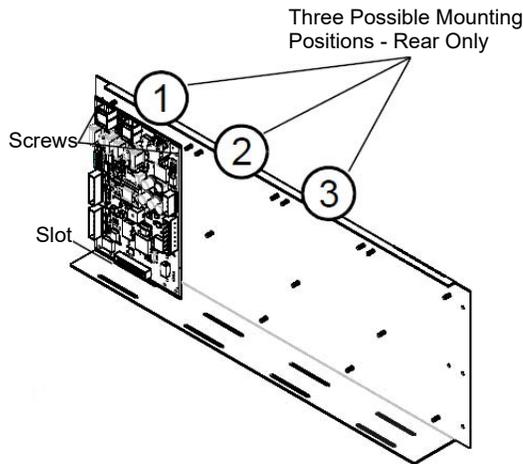


Figure 2.3 CHS-4L Installation

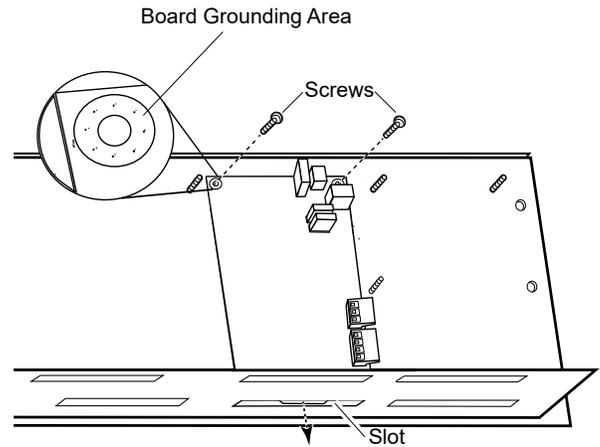


Figure 2.4 Securing the Board

2.3 Connections

2.3.1 Connecting to the NFN-GW-EM-3

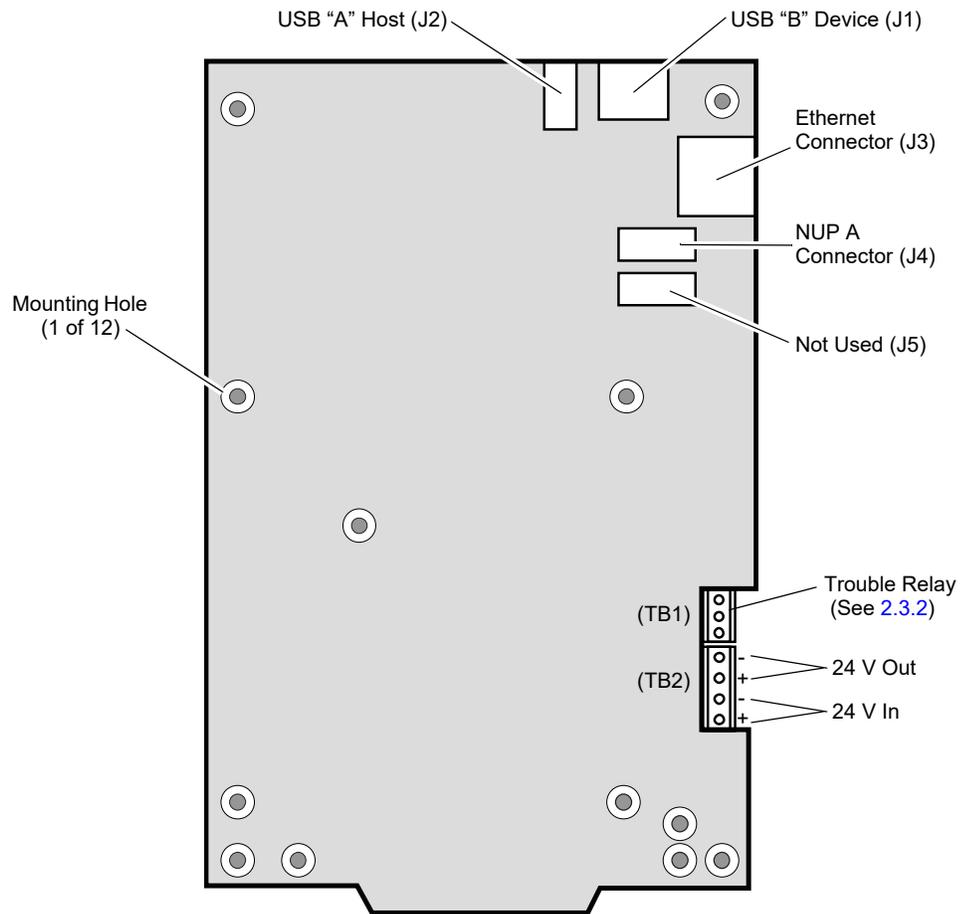


Figure 2.5 NFN-GW-EM-3 Connections

Table 2.1 Connection Specifications

Reference Designator	Description	Circuit Class	Specifications
TB1	Trouble Relay	2	Nominal Switching Capacity: 1 Amp @ 30 VDC 1.0 Power Factor Relay Type: Common
TB2	DC Power	2	Power Source - FACP or UL 1481 listed 24 VDC regulated power supply Nominal Voltage: 24 VDC, Regulated Current: 125 mA Locate in same cabinet or use close nipple fitting
J1	USB B	2	Locate in same cabinet or use close nipple fitting
J2	USB A	2	Locate in same cabinet or use close nipple fitting
J3	Ethernet	2	Line Impedance 100 ohm Max Distance 328.083 ft. (100 m)
J4	NUP A	2	RS-232 Locate in same cabinet or use close nipple fitting
<ul style="list-style-type: none"> All wiring from the power supply is power limited, and a separation of at least 1/4-inch (6.35 mm) must be maintained between power limited and non-power limited wiring. All interconnects are power limited. Ethernet connections are power limited and supervised except for ground faults. 			

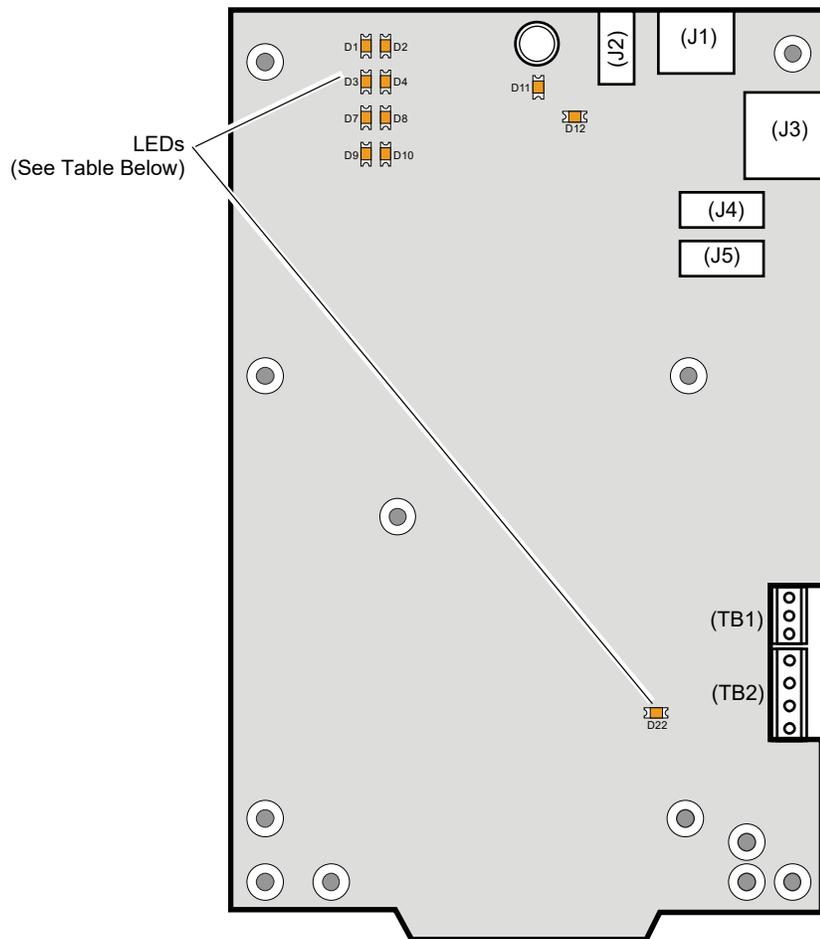


Figure 2.6 NFN-GW-EM-3 LEDs

Table 2.2 LED Definitions

Reference Designator	Label	Description
D1	ACTIVE	Active/Lit indicates that WinCE is running.
D2	NUPA RX	Blinks when data is received on the NUP A port (J4).
D3	PROGRAM	Not Used
D4	NUPB RX	Not Used
D7	USB B	Active/Lit indicates a device is connected to the USB B port (J1).
D8	NUPA TX	Blinks when data is sent on the NUP A port (J4).
D9	USB A	Active/Lit indicates a device is connected to the USB A port (J2).
D10	NUPB TX	Not Used
D11	DATA	Blinks to indicate data transmission to or from the Ethernet port (J3).
D12	LINK	Active/Lit indicates an Ethernet connection.
D22	WDT FAIL	Active/Lit indicates the system has undergone a reset due to a Watchdog circuit activating.

2.3.2 Trouble Relay Connections

The NFN-GW-EM-3 can be supervised by using an input module on an FACP. During normal operation (when the NFN-GW-EM-3 is not detecting an error) it activates the internal relay. When the relay is active, the input module detects the end-of-line resistor. When the NFN-GW-EM-3 detects an error, it deactivates the internal relay and posts an event to the error log (refer to 3.2.7, "Error Log"). This breaks the connection across the end-of-line resistor causing the input module to detect a trouble. This also occurs if the NFN-GW-EM-3 does not have power.

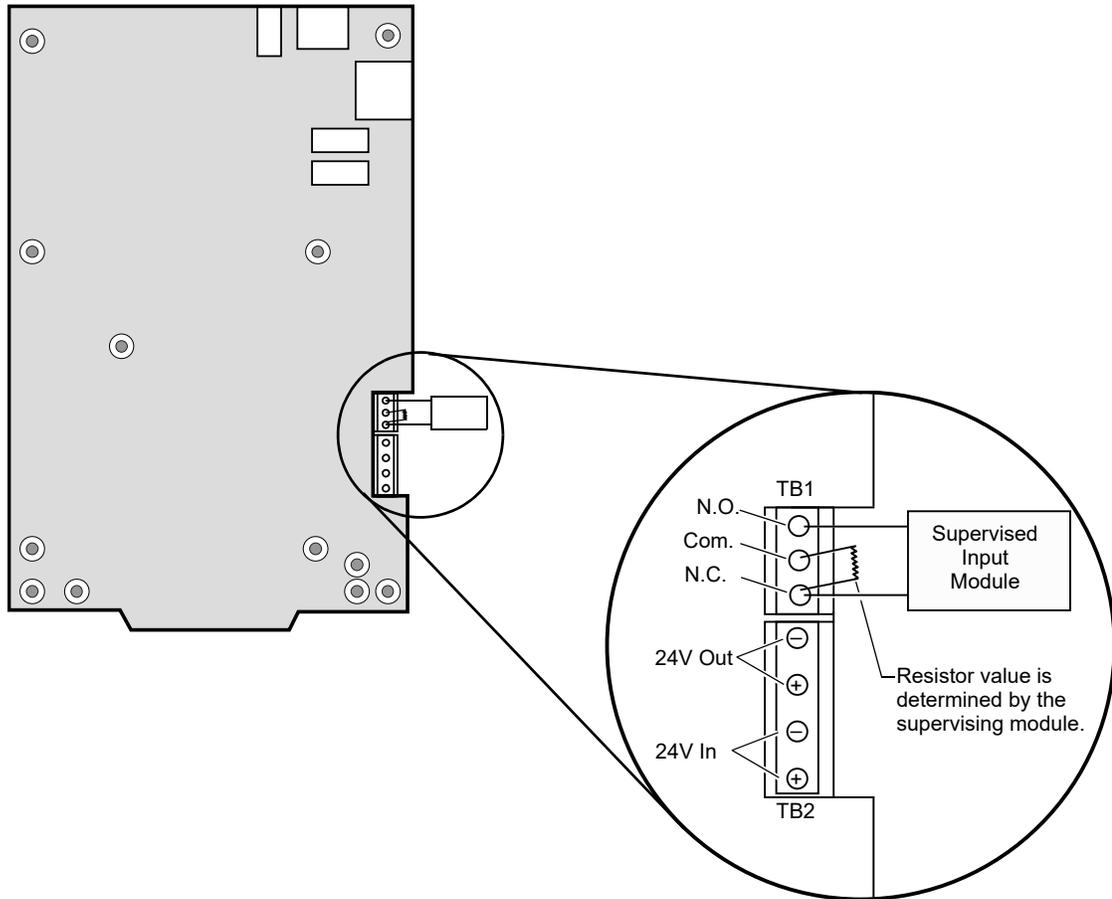


Figure 2.7 TB-1 Trouble Relay

2.3.3 Connecting to a Standard NCM

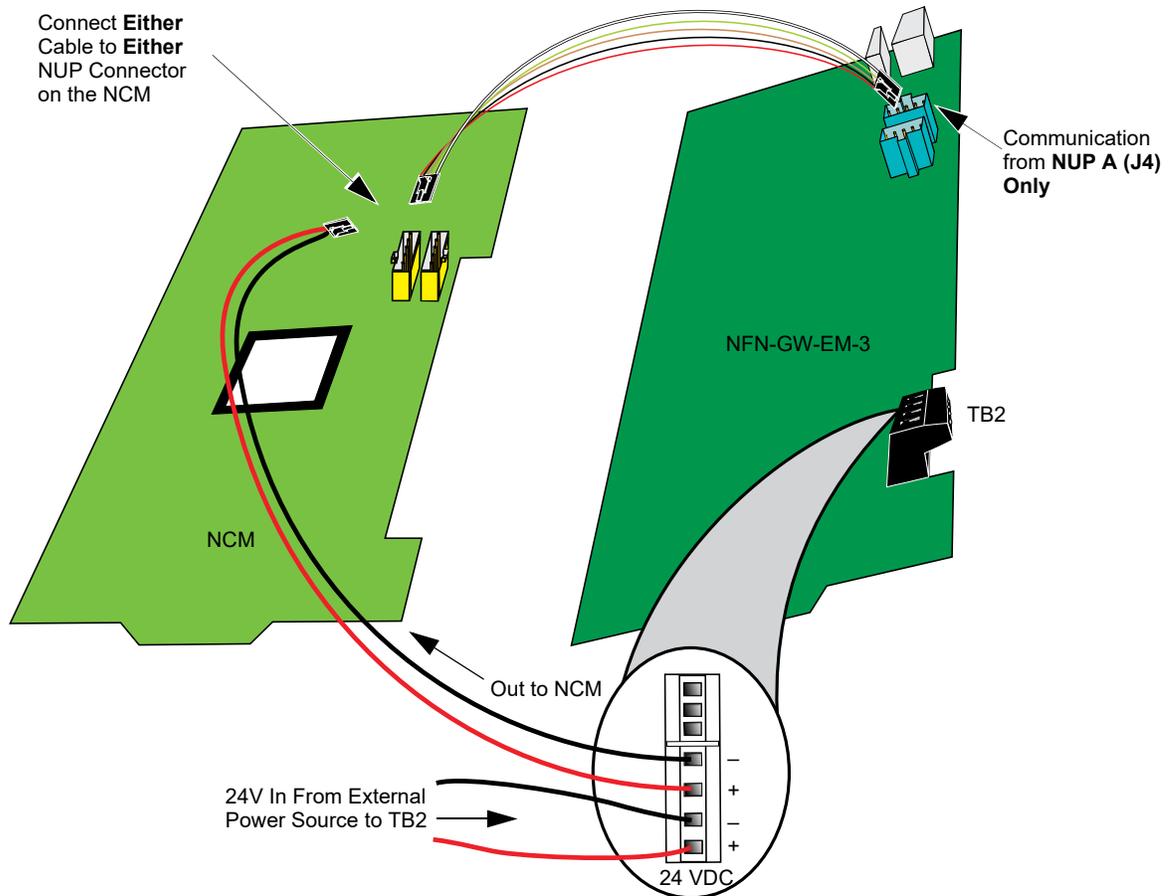


Figure 2.8 Routing Power and Communication to a Standard NCM

Table 2.3 Standard NCM Connections

Type	Connection
NCM-W	Twisted pair wire
NCM-F	Fiber-optic cable

2.3.5 Connecting to a Fire Alarm Control Panel (FACP)

Panel is shown for illustrative purposes only. The NFN-GW-EM-3 is mounted within the FACP cabinet and connected with the NUP connection located on the FACP.

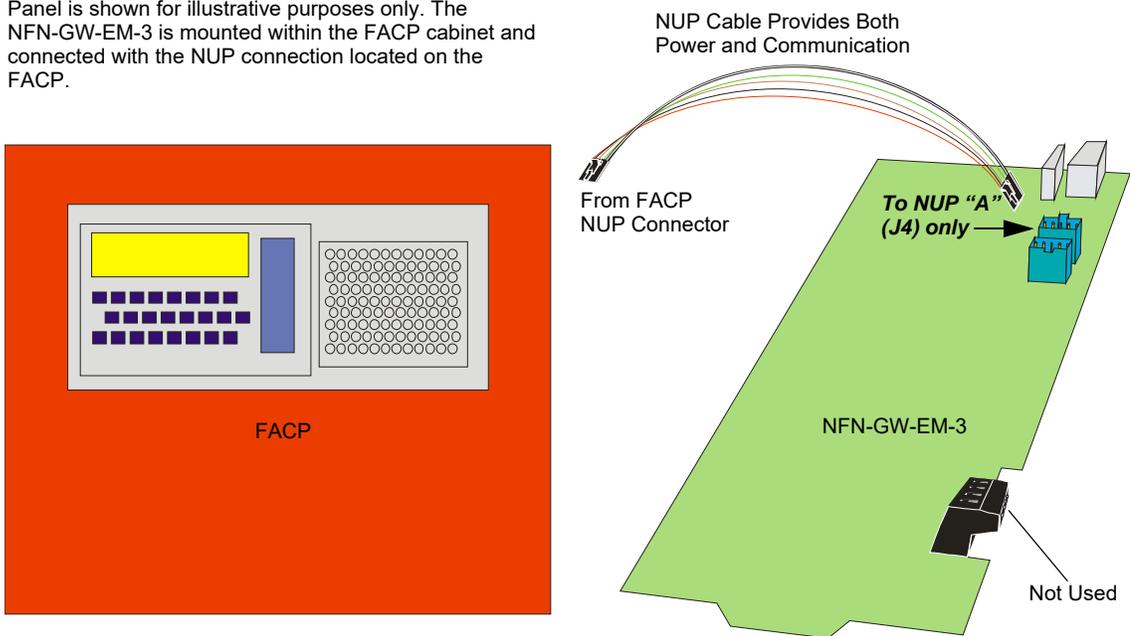


Figure 2.10 Connecting to an FACP

2.3.6 Connecting to the PNET-1 Surge Suppressor

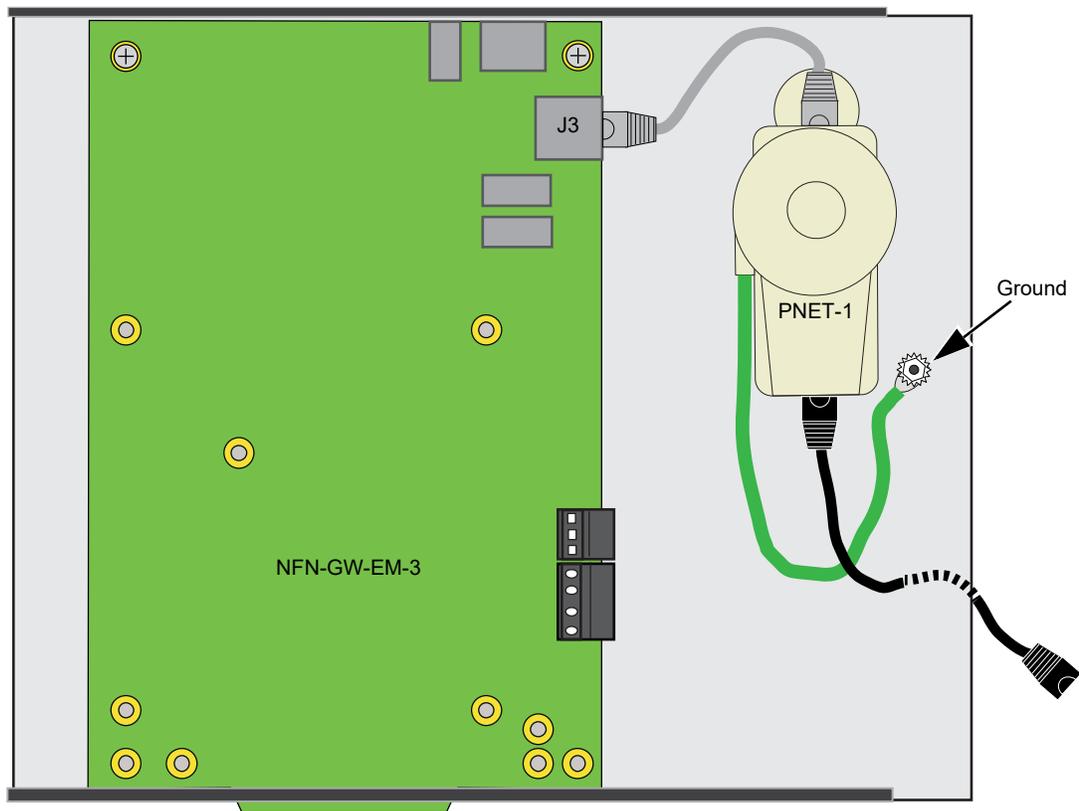


Figure 2.11 Connecting to the PNET-1

2.4 System Power

Table 2.5 Power Requirements

Power	Requirement
Input Voltage (Nominal)	24 VDC
Input Current @ 24 VDC	125 mA

2.5 Testing and Maintenance

Testing and maintenance should be performed according to the *Testing and Maintenance* section of NFPA-72 and CAN/ULC S536.

Section 3 Configuration

3.1 Configuration Web Page

Configuration of the NFN-GW-EM-3 is via a web page running on the NFN-GW-EM-3. Supported web browsers are listed in [1.4](#), "Required Software".

The following information applies to IP settings:

- Each NFN-GW-EM-3 is shipped with a default IP address of 192.168.1.2 and a default node number of 240.
- The computer used to configure the NFN-GW-EM-3 must be able to establish an IP connection to the gateway. Consult with a network administrator if unsure how to make this connection.
- Connecting more than one NFN-GW-EM-3 prior to reconfiguring the IP address will result in an IP address conflict.

Refer to [Appendix A](#), "Gateway Settings" for instructions on resetting and reviewing the IP settings of the NFN-GW-EM-3.

3.2 Configuring the NFN-GW-EM-3

3.2.1 Logging into the Web Page

Log into the NFN-GW-EM-3 as follows:

1. Start the web browser.
2. Navigate to the IP address of the gateway (**default http://192.168.1.2**).
3. If a security warning appears, select the option to continue anyway. Refer to [3.3](#), "Security Certificate" for more information.
4. Log into the web page:
 - a. If the password has already been established, enter the password and click **OK**.
 - b. If any of the following conditions is true, go to Step 5:
 - A new gateway from the factory.
 - An upgrade of a gateway from a previous version for which the password has not been set (i.e. still using the default password).
 - After a factory reset of the gateway.
5. To set a new password:
 - a. Enter the default password, 00000000 (eight zeros) and click **OK**. The Set Device Password dialog box appears.
 - b. Reenter the default password.
 - c. Enter a new password.
 - d. Reenter the new password to confirm.
 - e. Click **OK**.

3.2.2 Basic Configuration Tool Layout

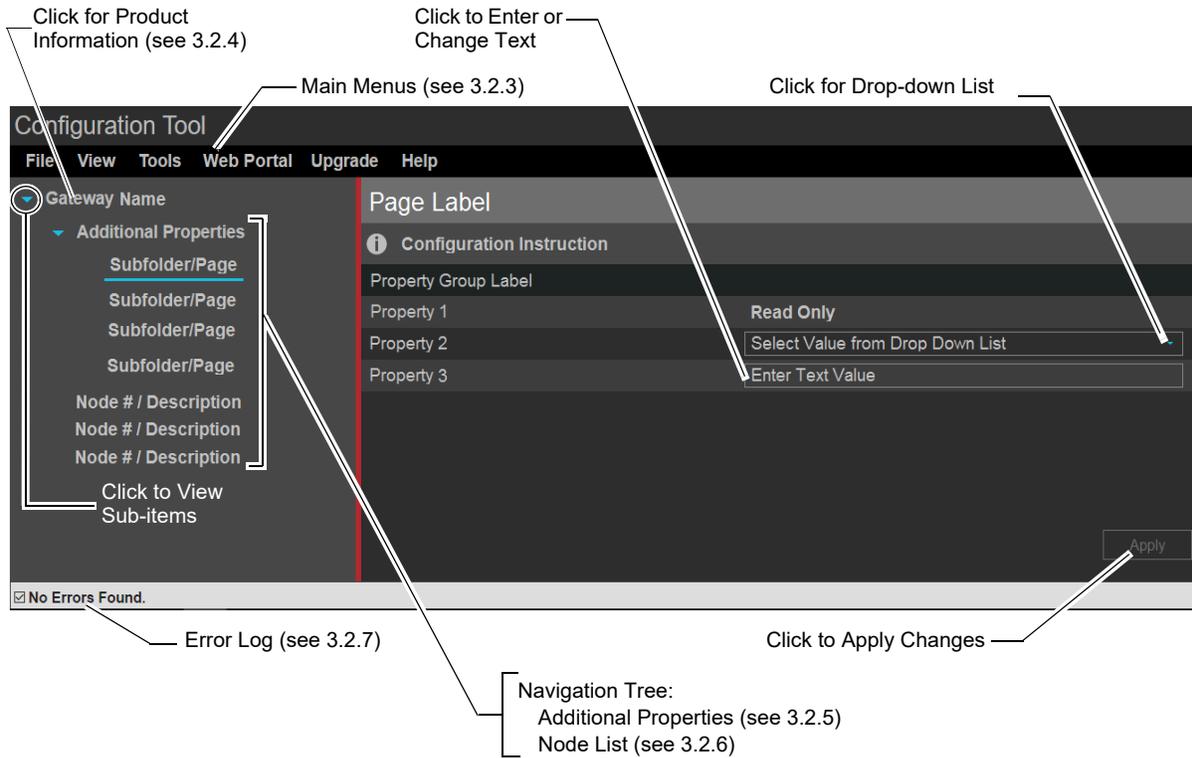


Figure 3.1 Basic Configuration Tool Layout

3.2.3 Main Menus

The following table describes the options available in the configuration tool main menus (see Figure 3.1).

Table 3.1 Main Menu

Menu	Option	Description
File	Reboot	Reboots the NFN-GW-EM-3.
View	History	Displays a window containing a historical list of error messages.
	Node Table	Displays a window containing software version information for all monitored nodes.
	Connected Clients	Displays a window containing IP address and description information for clients connected to the NFN-GW-EM-3.
Tools	Set Device Password	Displays a dialog box allowing the user to change the current password. <ul style="list-style-type: none"> • Passwords are case sensitive. • Alpha and numeric characters are supported. • Eight (8) characters minimum, 64 characters maximum.
	Backup...	Click to download a backup file (.bkp) from the gateway to the PC running the browser. Save or move the file to an appropriate location so it can be used, if necessary, to restore the gateway settings.
	Restore...	Browse to (or search for) the backup file on the PC running the browser. Click Open and then Send . An on-screen message indicates a successful restoration.
	Send PFX Key File	Opens a dialog box allowing the user to upload an SSL Certificate File. Browse for the file, enter the password (if required), and click Send. Refer to 3.3, "Security Certificate" .
	Auto Detect Nodes	Select to cause the gateway to automatically detect all connected nodes.
Web Portal	Commission Web Portal	Selecting this option causes the web portal to request the point information from the FACP(s) to update the information on the eVance server.
	Unregister Web Portal	Used prior to removing the web portal from the FACP connection.
Upgrade	Firmware	Opens the Send Archive File dialog box. Click the Choose button and select the filename that begins with " NGNUW " and has the extension ".AR". Click Open and then click Send . An on-screen message indicates a successful upgrade. It is recommended that the browser be restarted after the upgrade.
	Language	Displays a dialog box from which the user can navigate to, and select the desired language file.
Help	Legal	Displays legal information pertaining to the NFN-GW-EM-3.
	About	Displays version information pertaining to the NFN-GW-EM-3.
	Advanced Diagnostics	Used for informational/diagnostic purposes.

3.2.4 Product Information

The following information displays when initially opening the configuration tool. It can also be accessed by clicking the first entry in the navigation tree (see Figure 3.1).

Table 3.2 Product Information

Property	Value
Type	Displays the gateway type by name.
Brand	Displays brand information.
Version	Displays the gateway software version number.
Board Type	Displays the model of the gateway's printed circuit board.
Kernel Version	Displays additional software version information.
Boot Version	Displays additional software version information.
Current Time/Date	Displays the current time and date information after the gateway synchronizes the clock with the SNTP server.

3.2.5 Additional Properties

The Additional Properties folder is located in the navigation tree area of the configuration tool (see Figure 3.1). After configuring the settings, click **Apply** in the lower right corner of the window.

Table 3.3 Additional Properties

Navigation Tree Label	Property	Value
IP Address Settings	IP Address Settings	
	IP Address	Enter the IP address of the NFN-GW-EM-3. (Default is 192.168.1.2) Note: If a new IP address is entered, the user must enter the new IP address in the browser address bar to log into the gateway at its new address.
	SubNet Mask	Enter the subnet address of the NFN-GW-EM-3. (Default is 255.255.255.0)
	IP Gateway	Enter the IP address of the default gateway for the host network. (Default is 0.0.0.0)
	MAC Address	Displays the Media Access Control (MAC) address of the gateway Ethernet port and is not configurable.
	DNS Server Settings	
	Preferred DNS Server	Enter the IP address for the primary Domain Name System (DNS) server. A DNS entry is required by the NFN-GW-EM-3 for communications with the eVance server.
	Alternate DNS Server	Enter the IP address of the alternate DNS server.
Monitored Clients		Refer to 3.5, "Client Monitoring" for additional information.
	Add New...	<ul style="list-style-type: none"> • Yes: Automatically adds connecting clients to the list of monitored clients when they connect. • No: Does not allow new connecting clients to be added to the list.
	Client List	<ul style="list-style-type: none"> • Yes: The client will be monitored. • No: The client is not monitored. • Remove This Monitored Connection: Removes the client from the list of monitored clients. Note: Monitored clients labeled as "Incident Monitor" refer to FirstVision.
NFN Settings	Gateway Settings	
	Mode	Select the mode from the drop-down list. (Default is Proprietary Receiving Unit)
	System Password	Enter the unique value used to identify the gateways and workstations on the network. The system password is case-sensitive and limited to 20 characters. A default value is randomly assigned and must be changed to match the system password on the workstation PC.
	General Information	
	Connection Port	Displays the type of connection port used (Serial, USB, etc.).
	Connection Type	Describes how the gateway is connected to the NFN.
	NCM Version	Displays the NCM version number. NCM Version does not appear when there is no NFN connection.
	NCM Status Bits	Displays the NCM status, which can be: Piezo, UPS Failure, Network Fail Port A, Network Fail Port B, High Speed Audio, NCM Sniffer Mode Active, Local Connection Limit Exceeded, or None. NCM Status Bits does not appear if when there is no NFN connection.
	Fire Network Time Policy	Displays one of the following depending on the type of time synchronization used: <ul style="list-style-type: none"> • Send time: The NFN-GW-EM-3 sets the time on the NFN network. • Unsynced: The NFN-GW-EM-3 and NFN network are not synchronized with each other.

Table 3.3 Additional Properties (Continued)

Navigation Tree Label	Property	Value
NFN Settings (Continued)	Node Settings	
	Node	Enter the NFN node number of the NFN-GW-EM-3. (Default is 240)
	Panel Label	Enter panel label.
	Mass Notification Priority	<ul style="list-style-type: none"> Select None if Mass Notification is not used (default). Select Lower Than Fire if fire alarms have priority over Mass Notifications. Select Higher Than Fire if Mass Notifications have priority over fire alarms.
	Send Time to Panels	<ul style="list-style-type: none"> Selecting Yes enables the gateway to send the time to the FACPs on the NFN network. Selecting No prevents the gateway from sending time to the panels. (Default is No)
	Network Settings	
	Channel A Threshold	<ul style="list-style-type: none"> Select High for a high-noise NFN network. Select Low for a low-noise NFN network.
	Channel B Threshold	<ul style="list-style-type: none"> Select High for a high-noise NFN network. Select Low for a low-noise NFN network.
	Class X	<ul style="list-style-type: none"> Select Yes for a Class X Signaling Line Circuit (SLC) configured NFN network. Select No for a Class B SLC configured NFN network (default).
	SNTP Client Settings	Time Server Address
Time Zone Settings	GMT Reference	
	GMT Offset	Set the offset (hours and minutes) from Greenwich Mean Time (GMT). (Default is -5 hours, 00 minutes [Eastern Standard Time].)
	Observe Daylight Saving Time	Select one of the following from the drop-down list: <ul style="list-style-type: none"> Yes - The gateway observes Daylight Savings Time (DST). No - The gateway does not observe Daylight Savings Time.
	Time Zone Reference	Select the time zone standard from the drop-down list. (Default is US Standard.)
	DST Begin/DST End - Displays only when the "Other Standard" option is selected for the time zone reference.	
	Series Reference	Select the option (First to Fifth or Last) from the drop-down list.
	Day of Week	Select from the drop-down list.
	Month	Select from the drop-down list.
	Hour	Enter the hour in 24 hour time (0-23).
	Hour Reference	Select Local Time or GMT from the drop-down list.
Web Portal Setup		Configures the web portal feature for use with eVance. Requires the eVance user ID, password, unique web portal name, and web portal description. Utilizes predefined customers and buildings from eVance. See 3.4, "Web Portal Setup".

3.2.6 Node List

The node list is located in the navigation tree area of the configuration tool screen (see [Figure 3.1](#)). Click the desired node label to view information about that node. The information displayed is dependent on the node type. Labels for off-line nodes display in red text.

3.2.7 Error Log

The error log displays specific information when the NFN-GW-EM-3 detects a problem with the web portal connection. The following table defines the meaning of the label text.

Table 3.4 Error Log Descriptions

Label	Description
No Errors Found	The gateway is not reporting any web portal connection errors.
# Errors Found. Click here to view errors.	The gateway is reporting a web portal connection error. The number of errors is indicated in the label. Clicking the error label opens the Error Log that lists the date, time, and a description of the error(s).

When the error is corrected, the entry is removed from the log and the label at the bottom of the screen returns to its “No Errors Found” status. Information about the error is also recorded in the gateway history log (**View > History**).

3.3 Security Certificate

The NFN-GW-EM-3 communicates with the browser using secure communications facilitated by a self-signed security certificate. Using the self-signed security certificate will cause the browser to display warnings similar to the following:

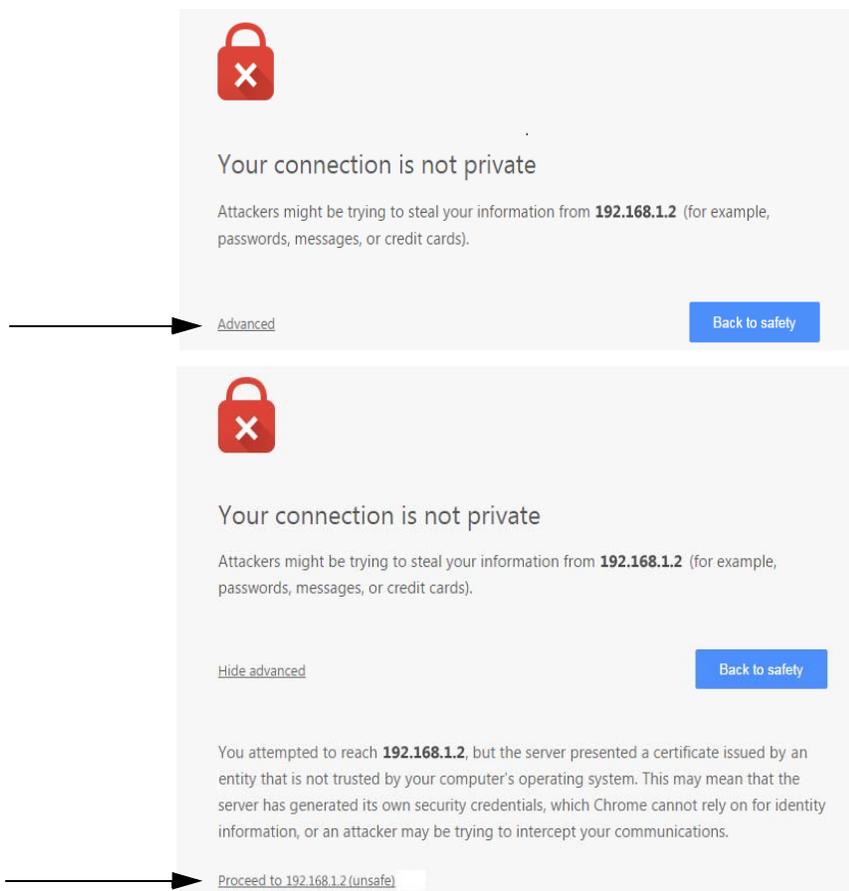


Figure 3.2 Chrome Security Warning Example

The browser warning is displayed upon each connection to the gateway. The warning may be removed by obtaining a security certificate from a security authority. The certificate may originate from a local certificate authority or a commercial certificate authority if the gateway is directly connected to the Internet with a unique IP address. Regardless of which type of certificate authority is selected, the IP

address of the gateway must be provided. The certificate is specific to the specified IP address. If the IP address is changed, a new certificate will be required. In addition, the certificates have an expiration date. Once the certificate expires, a new certificate needs to be sent to the gateway. If the certificate expires, a different warning is displayed by the browser.

The security certificate must be in the PFX format. The PFX file is uploaded to the gateway using the **Tools > Send PFX Key File** option in the gateway configuration tool. It may be necessary to install a file on each PC used to configure the gateway to fully resolve the security configuration.

The NFN-GW-EM-3 includes a self-signed security certificate. The certificate is generated with a three year expiration. In addition, the certificate is generated using the default IP address of the gateway, 192.168.1.2. A certificate authority may be used to create a valid certificate based on the IP address of the NFN-GW-EM-3. If a certificate authority is not available, a local IT administrator may use a security certificate generation application such as OpenSSL to generate the certificate.

The site network administrator may be able to assist with any additional details regarding security certificates.

3.4 Web Portal Setup

The NFN-GW-EM-3 web portal feature must have the correct time and date settings in order for it to establish communications with the eVance server. Ensure that a valid time server IP address or DNS server name has been entered and appropriate time zone settings have been made in the configuration tool's Additional Properties web page.

After each reboot, the web portal must communicate with the time server before it is able to connect to eVance.

To receive events and configuration information for use in tools such as the Inspection Manager and System Manager, the NFN-GW-EM-3 must be associated with a specific site as follows:



NOTE: The NFN-GW-EM-3 must be v. 4.00 or later and board type EMPCB to support System Manager.

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

3.5 Client Monitoring

The NFN-GW-EM-3 is able to monitor connected clients. When the NFN-GW-EM-3 detects a monitored client has disconnected, the NFN-GW-EM-3 deactivates the output relay. An active relay indicates that the client is operating properly. If power is disconnected from the gateway, the lack of the active relay results in a trouble on the connected monitor module.

The client monitoring feature operates as follows:

- When a client connects, the gateway adds the client to the list of supervised clients.
- The user may log into the gateway and deselect one of the clients which was automatically added to stop the gateway from supervising that particular client.
- The user may log into the gateway and deselect the option which forces the gateway to automatically add clients to the monitored clients list when it connects.

Use cases are covered in the following table:

Table 3.5 Client Monitoring Use Cases

Case	Procedure
Supervise all site clients at the gateways. No gateway configuration.	1. Connect the output relay to an input module on an FACP. 2. On the FACP, configure the input as a trouble (tracking recommended). Note: All clients at the site must have fixed IP addresses.
Supervise specific clients at the gateway.	1. Connect the monitored clients to the gateway. The clients must have fixed IP addresses. 2. Open the gateway's web-based configuration tool. 3. Deselect the option to automatically add and monitor clients as they connect. 4. Deselect any specific clients that do not need to be monitored (if any have been added). 5. If new clients are added and are to be monitored, re-enable the automatic addition/supervision and connect the new client(s). Once they have been added, turn off the automatic addition option.

Appendix A Gateway Settings



NOTE: The procedures in this appendix require the use of a USB flash memory drive.

A.1 Viewing Existing IP Settings

1. Connect the flash drive to the NFN-GW-EM-3.
2. Reboot the gateway.

A file is created that matches the configured IP address of the gateway, followed by the extension “.txt” (e.g., **192.168.1.2.txt**). If the file already exists on the drive, it will be altered to match the gateway configuration. The file contains additional information such as the MAC address of the gateway.

3. Connect the drive to a PC and view the files.

The flash drive should contain a file that matches the configured IP address of the gateway, followed by the extension “.txt” (e.g., **192.168.1.2.txt**). If the file already exists on the drive, it has been altered to match the gateway configuration. The file contains additional information such as the MAC address of the gateway.

A.2 Resetting Factory Default Values

1. Connect the flash drive to a PC and create a file named “**default.ldc**”. The contents of the file is not significant; however, ensure that the file does not have an additional hidden file extension. This file will be automatically deleted from the flash drive by the gateway.
2. Eject the flash drive from the PC.
3. Disconnect power from the gateway.
4. Disconnect the communication cable to the gateway USB port (if present) and connect the flash drive.
5. Reconnect the 24 VDC power supply to the gateway.
6. After approximately one minute, disconnect the flash drive from the USB port and (if necessary) reconnect the cable removed in Step 4.
7. Connect the flash drive to the PC and verify that the file named **192.168.1.2.txt** is on the drive.
 - If the file is on the flash drive, the reset has been accomplished.
 - If the file **is not** on the flash drive:
 - The flash drive may not have been connected during the reboot period or was removed early.
 - The flash drive is not seen as a valid drive by the hardware.
 - A software error has occurred and technical support may need to be contacted.

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

