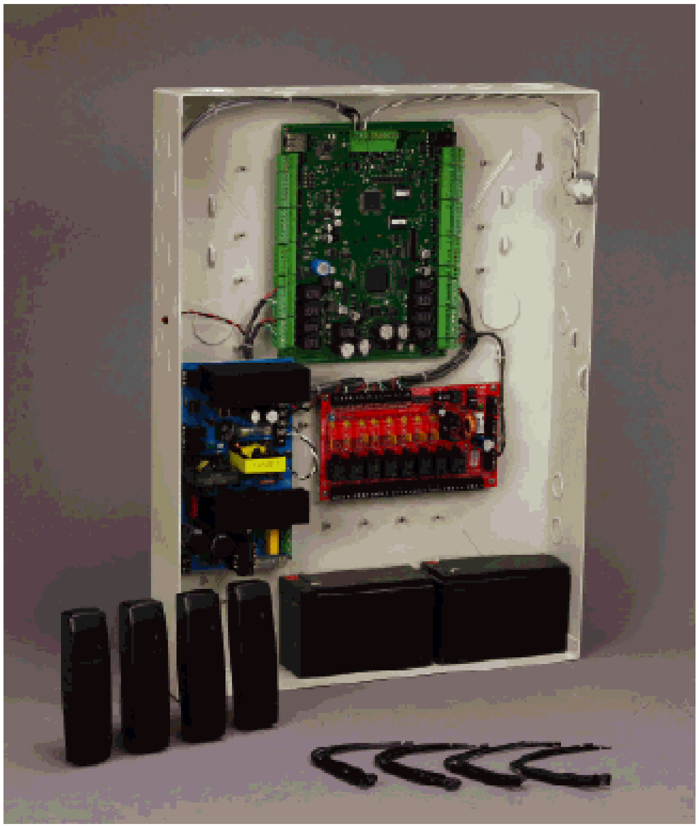
Honeywell



Honeywell NetAXS™

NX4L1

Access Control Unit Installation Guide

July 2016

Ordering Information

Please contact your local Honeywell representative or visit us on the web at www.honeywellaccess.com for information about ordering.

Feedback

Honeywell appreciates your comments about this manual. Please visit us on the web at www.honeywellaccess.com to post your comments.

TABLE OF CONTENTS

NetAXS™ NX4L1 Installation Guide

NetAXS™ Standalone Operation

Recommended Wiring for NetAXS-4/NetAXS-123 Loops

LIST OF FIGURES

LIST OF TABLES

NetAXS™ NX4L1 Installation Guide

1.0 Notices

1.1 Warnings and Cautions

WARNING Fire Safety and Liability Notice: Never connect card readers to any critical entry, exit door, barrier, elevator or gate without providing an alternative exit in accordance with all fire and life safety codes pertinent to the installation. These fire and safety codes vary from city to city and you must get approval from local fire officials whenever using an electronic product to control a door or other barrier. Use of egress buttons, for example, may be illegal in some cities. In most applications, single action exit without prior knowledge of what to do is a life safety requirement. Always make certain that any required approvals are obtained in writing. Verbal approvals are not valid.

WARNING Honeywell never recommends using WIN-PAK or related products for use as a primary warning or monitoring system. Primary warning or monitoring systems should always meet local fire and safety code requirements. The installer must also test the system on a regular basis by instructing the end user in appropriate daily testing procedures. Failure to test a system regularly could make installer liable for damages to the end user if a problem occurs.

WARNING Earth ground all enclosures for proper installation.

WARNING Honeywell recommends only DC locks.

WARNING Personal injury or death could occur, and the equipment could be damaged beyond repair, if this precaution is not observed!

- Before installation, turn off the external circuit breaker which supplies power to the system, including door locks.
- Before connecting the device to the power supply, verify that the output voltage is within specifications of the power supply.
- Do not apply power to the system until after the installation has been completed.

CAUTION If any damage to the shipment is noticed, a claim must be filed with the commercial carrier responsible.

CAUTION Electrostatic discharge (ESD) can damage CMOS integrated circuits and modules. To prevent damage always follow these procedures:

- Use static shield packaging and containers to transport all electronic components, including completed reader assemblies.
- Handle all ESD sensitive components at an approved static controlled workstation. These workstations consist of a desk mat, floor mat and an ESD wrist strap. Workstations are available from various vendors.

1.2 Product Liability, Mutual Indemnification

In the event that a Customer receives a claim that a Product or any component thereof has caused personal injury or damage to property of others, the Customer shall immediately notify Honeywell in writing of all such claims. Honeywell shall defend or settle such claims and shall indemnify and hold the Customer harmless for any costs or damages including reasonable attorneys' fees which the Customer may be required to pay as a result of the defective Product or the negligence of Honeywell, its agents or its employees.

The Customer shall hold harmless and indemnify Honeywell from and against all claims, demands, losses and liability arising out of damage to property or injury to persons occasioned by or in connection with the acts or omissions of the Customer and its agents and employees, and from and against all claims, demands, losses and liability for costs of fees, including reasonable attorneys' fees in connection therewith.

1.3 Limited Warranty

All Products sold or licensed by Honeywell Access Systems (HAS) include a warranty registration card which must be completed and returned to HAS by or on behalf of the end user in order for Honeywell to provide warranty service, repair, credit or exchange. All warranty work shall be handled through the Customer which shall notify Honeywell and apply for a Return Merchandise Authorization (RMA) number prior to returning any Product for service, repair, credit or exchange. Honeywell warrants that its Products shall be free from defects in materials and workmanship for a period of one year from date of shipment of the Product to the Customer. The warranty on Terminals, Printers, Communications Products and Upgrade kits is 90 days from date of shipment. Satisfaction of this warranty shall be limited to repair or replacement of Products which are defective or defective under normal use.

Honeywell's warranty shall not extend to any Product which, upon examination, is determined to be defective as a result of misuse, improper storage, incorrect installation, operation or maintenance, alteration, modification, accident or unusual deterioration of the Product due to physical environments in excess of the limits set forth in Product manuals.

THERE ARE NO WARRANTIES THAT EXTEND BEYOND THIS PROVISION. THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE. NO REPRESENTATION OR WARRANTY OF THE DISTRIBUTOR SHALL EXTEND THE LIABILITY OR RESPONSIBILITY OF THE MANUFACTURER BEYOND THE TERMS OF THIS PROVISION. IN NO EVENT SHALL HONEYWELL BE LIABLE FOR ANY RE-PROCUREMENT COSTS, LOSS OF PROFITS, LOSS OF USE, INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES TO ANY PERSON RESULTING FROM THE USE OF HONEYWELL PRODUCTS.

1.4 Federal Communications Commission

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or re-locate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The user shall not make any changes or modifications to the equipment unless authorized by the Installation Instructions or User’s Manual. Unauthorized changes or modifications could void the user’s authority to operate the equipment.

For panels using the Ethernet connection, the cable clamp (HAS part number 3-000342) must be used for the panel to pass the FCC Part 15 Class B requirements. See “Installation“ on page 20 for clamp installation instructions.

1.5 Industry Canada

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du réglement sur le matériel brouilleur du Canada.

1.6 Underwriters Laboratories Incorporated

The NetAXS panel was approved by Underwriters Laboratories Incorporated for Access Control System Units - Category ALVY, UL294 standard. The NetAXS panel was approved as a standalone system. The input points only monitor the door position. The NetAXS panel is not intended as a Proprietary Alarm Unit - Category APOU, UL1076 standard.

The NetAXS panel was approved using the following Honeywell readers: OmniAssure™ OT30, OmniClass™ OM40 and OM55, and OmniProx™ OP30 and OP40.

Notes:

- All field wiring, except for the AC power input and the battery backup/charger wiring, is Class 2 power-limited.
- Communication between panels other than the NetAXS panel has not been evaluated by UL.
- UL has approved only the configurations shown in Section 5.1, "RS-485 Connection via PCI-2" on page 42, Section 5.2, "RS-485 Connection via NetAXS" on page 43, and Section 5.4, "RS-232 Connection" on page 46 of this guide. Because UL has approved the NetAXS panel only as a standalone system, the computer terminal, NetAXS gateway panel, and N-485_PCI-2 adapter appear in these sections only to illustrate the installation and programming of the NetAXS panel.
- UL has not evaluated the compatibility of downstream I/O devices (see Section 4.10, "Downstream I/O" on page 39) with the NetAXS panel.
- All wiring methods shall be performed in accordance with NFPA70, local codes and authorities having jurisdiction.
- This product must be mounted indoors only, installed within the protected premises.
- This product must be installed, serviced and tested once a year by a factory trained professional.
- All interconnecting devices must be UL Listed and Class 2 power-limited only.
- The minimum system configuration consists of Model NX4L1 and a Listed, compatible access control reader or keypad.
- The system shall not be installed in the fail secure mode unless permitted by the local authority having jurisdiction and shall not interfere with the operation of panic hardware.
- The model NX4L1 system is capable of providing 40 minutes of standby power.
- The model NX4L1 system is capable of being permanently connected to line voltage or alternatively a cord connection can be made. The cord shall be a minimum 6 ft. long and a SJ, SJT, or equivalent.

- The model NX4L1 control units are compatible with the following Listed reader heads:
    - Honeywell OmniAssure™ OT30
    - Honeywell OmniClass™ OM40
    - Honeywell OmniClass™ OM55
    - Honeywell OmniProx™ OP30
    - Honeywell OmniProx™ OP40

2.0 Introduction

2.1 Access Control Overview

An access control system protects and preserves an enterprise's resources by providing authentication, authorization, and administration services. Authentication is a process that verifies a user's identity. If the user is verified, the system then either grants or denies access to specific areas and resources. Administration includes the creation and modification of user accounts and access privileges.

An access control system consists of hardware and software, usually configured in a network environment over a standard network protocol. Access control units, readers, door strikes, and video and other devices, for example, are configured to control and monitor the access to a company site.

2.2 NetAXS Access Overview

A NetAXS access control system consists of a host system and NetAXS access control units that meet existing N-1000-III/IV specifications and that communicate with each other and with a variety of input and output devices over the RS-232 and RS-485 network protocols. See "System Configuration" on page 42 to view illustrations of the supported NetAXS system configurations. A NetAXS access control system is configured and maintained via either the host system or a web server using RS-232, RS-485, or Ethernet network protocols.

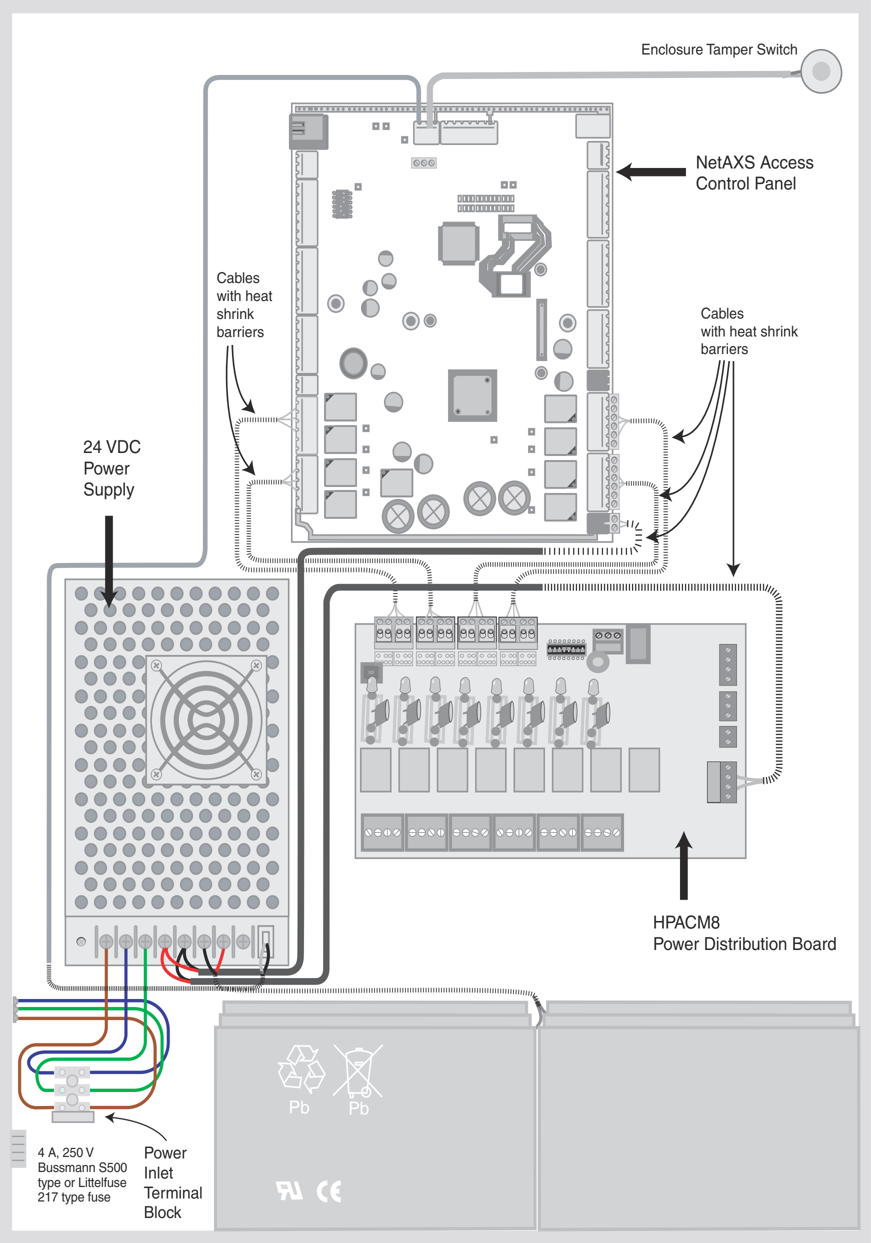
This document describes how to install and configure the NX4L1 access control unit.

3.0 Panel Components and Descriptions

The NX4L1 access control unit consists of a NetAXS panel control board, a power distribution module, a power supply, and batteries. The components are enclosed in a pre-wired cabinet. The power supply provides power for the panel control board, which is a four-reader panel providing access control for up to four doors.

The following figure shows the NX4L1 panel components.

Figure 1: NX4L1 Panel Components


Enclosure Tamper Switch
NetAXS Access Control Panel
Cables with heat shrink barriers
Cables with heat shrink barriers
24 VDC Power Supply
HPACM8 Power Distribution Board
Pb
Pb
4 A, 250 V Bussmann S500 type or Littelfuse 217 type fuse
Power Inlet Terminal Block

Note: Maintain at least 0.25-inches between the non-power-limited wiring (AC line voltage input wiring, 24 VDC wiring, battery backup/charger wiring, and battery-to-battery wiring) and all other wiring, which is power-limited Class 2 wiring.

3.1 NetAXS Access Control Unit

The NetAXS panel is a four-reader board that controls up to four doors by providing up to 14 inputs and 8 outputs. The NetAXS panel may be used as a standalone panel with independent card and transaction storage or, with a host software upgrade, as a fully monitored online access control device. The NetAXS panel also supports up to 30 downstream panels in a variety of network configurations. See Communications, page 32, for descriptions and illustrations.

Fourteen inputs are capable of four state supervision: Normal, Alarm, Short and Open. Eight inputs are used as door control with one input used for request to exit on each door and one input used for door status on each door. Supervised inputs for Tamper, External Power Fail and four Reader Tampers are supplied as well, and they can be used as additional inputs when not required for their default purpose.

CAUTION The NetAXS board must not be used to power locks. All locks must be powered through the relay board.

Real-Time Clock Protection

The panel RTC is backed up using a super capacitor. The super capacitor will power the real-time clock for one week in the absence of primary power or backup battery.

Memory Protection

The NetAXS panel continuously saves database and event information in non-volatile FLASH memory. This activity prevents the panel from losing data when power is lost.

Reader and AUX Power

Reader and AUX power is supplied at 12.4 VDC nominal with a maximum current distribution of 600 mA. The current can be distributed throughout the Reader Power or AUX Power in any configuration as long as the maximum draw is less than 600 mA: Reader 1 + Reader 2 + Reader 3 + Reader 4 + AUX Power < 600 mA. Maximum combined current of the two auxiliary outputs (if used without the four reader outputs) is 500 mA.

CAUTION AUX Power must not be used to power locks.

For NetAXS maximum current draw, refer to panel specifications.

3.2 Power Supply

The NX4L1 uses an internal 24 VDC nominal regulated power supply. The supply uses provides 24 VDC at 5 amps for the system power. The supply also charges and monitors the condition of the batteries. Wire the unswitched electrical power to the supply per the National Electrical Code as well as any local electrical codes, including the safety ground wire.

An AC input power indicator is supplied, and it is illuminated when AC input voltage is present. If the indicator is off, the AC input voltage is off, or too low to operate the system.

⚠ **CAUTION** De-energize the unit before servicing it. For continued protection against the risk of electric shock and fire hazard, replace the AC terminal block input fuse with the rating of 3.5 A, 250 V. The power supply in the NX4L1 is not serviceable by the customer and does not contain any serviceable parts. Do not open or remove the power supply cover.

3.3 Batteries

For the NX4L1, two 12 VDC, 7 Ah sealed lead-acid batteries (Honeywell order number 3-000066) wired in series must be used to have backup battery capability. The batteries will provide standby backup power, depending upon system configuration and activity. The batteries are wired in series (positive on one battery to negative on the other) and connected to the BATT + and BATT – terminals on the 24 VDC power supply in the NetAXS enclosure. When AC is lost, the power supply automatically switches to the backup batteries for continuous 24 VDC power. The power supply has deep discharge protection, and it can provide a Low Battery signal to the panel if it is connected to a supervised input on the NetAXS panel. Refer to the system wiring diagram for details. Replace the batteries every 2 to 2.5 years, or more often if the system has a high rate of backup use.

3.4 Enclosure

The enclosure is 450 mm (17.7 in.) wide, 607 mm (23.9 in.) high, 90 mm (3.54 in.) deep. The enclosure is shipped pre-wired.

3.5 Suppressors

Two suppressors (HAS number S-4) are required for each door lock. One suppressor is installed on the panel control board, and the second must be installed at the door lock.

4.0 Installation

Perform the following steps to install the NX4L1 panel:

WARNING Use a static strap whenever touching the panel to ensure protection from Electrostatic Discharge (ESD).

1. Review the panel layout, cable runs, and power needs.
2. Mount the enclosure at the proper location on the wall. Use appropriate anchors for the mounting material.
3. Run all I/O wires to the enclosure, and properly mark each wire for its use.
4. Run appropriate length three-wire cable to the enclosure power inlet terminal block. Ensure that the building earth ground wire is connected to the center terminal of the power inlet terminal block as shown on the wiring diagram inside the enclosure door. This wll complete the NX4L1 earth ground connection to the building electrical system. Earth ground for the power supply is established by the direct metal-to-metal contact to the enclosure. Do not remove any of the factory-installed hardware. Note that an Optional Power Connection kit (HAS part number 100-00049) is available for the NX4L1 panel. To install the Power Connection option, see "Installing the Optional AC Inlet" on page 21 for instructions. The power inlet terminal block can accommodate wire sizes up to 12 AWG. Wiring to a 20 amp branch circuit requires 12 AWG insulated copper wire. Wiring to a 15 amp branch circuit requires 14 AWG insulated copper wire. Connect the line, neutral, and earth ground wires to the appropriate terminal on the power inlet terminal block.

CAUTION Do not apply power at this time.

5. Remove each terminal plug one at a time to wire the properly labeled cables. See the wiring diagram (Figure 35 on page 63). Leave enough shield drain length to secure to the grounding stud. Also, maintain at least 0.25 inches between the non-power-limited wiring (AC line voltage input wiring, 12/24 VDC wiring, battery backup/charger wiring, and battery-to-battery wiring) and all other wiring, which is power-limited Class 2 wiring.

CAUTION Do not apply power at this time.

6. Connect the shield to the grounding studs.
7. Set DIP switch settings for the panel address (see Table 5 on page 38), and set J36 and J37 for communication termination and biasing (see "System Configuration" on page 42 and "Jumper Settings" on page 39).
8. Check all wiring at this time.

CAUTION Improper wiring can cause damage to the NetAXS at power up and result in a loss of warranty.

9. Apply power to the panel. The power-up sequence may take up to two minutes, after which the RUN LED blinks green. The RUN LED is located near Terminal Block (TB) 8. After the power-up sequence, check the LEDs to be sure the panel has powered up properly (see “LED Operation“ on page 58).
10. Configure the panel by following the instructions in the *NetAXS™ Access Control Unit User’s Guide.*
11. If you are using a battery backup function, place the two 7 Ah batteries in the enclosure with the battery terminals of each battery close to each other.
12. Attach the 4-inch battery-to-battery cable from the positive (red) terminal of one battery to the negative (black) terminal of the other battery. DO NOT CONNECT THE CABLE BETWEEN THE TERMINALS OF THE SAME BATTERY.
13. Attach the positive (red) power supply-to-battery cable to the remaining positive (red) battery terminal.
14. Attach the negative (black) power supply-to-battery cable to the remaining negative (black) battery terminal.
15. For panels using the Ethernet connection, the cable clamp (HAS part number 3-000342) must be used for the panel to pass the FCC Part 15 Class B requirements. Snap the clamp around any portion of the Ethernet cable that is inside of the enclosure.

4.1 Installing the Optional AC Inlet

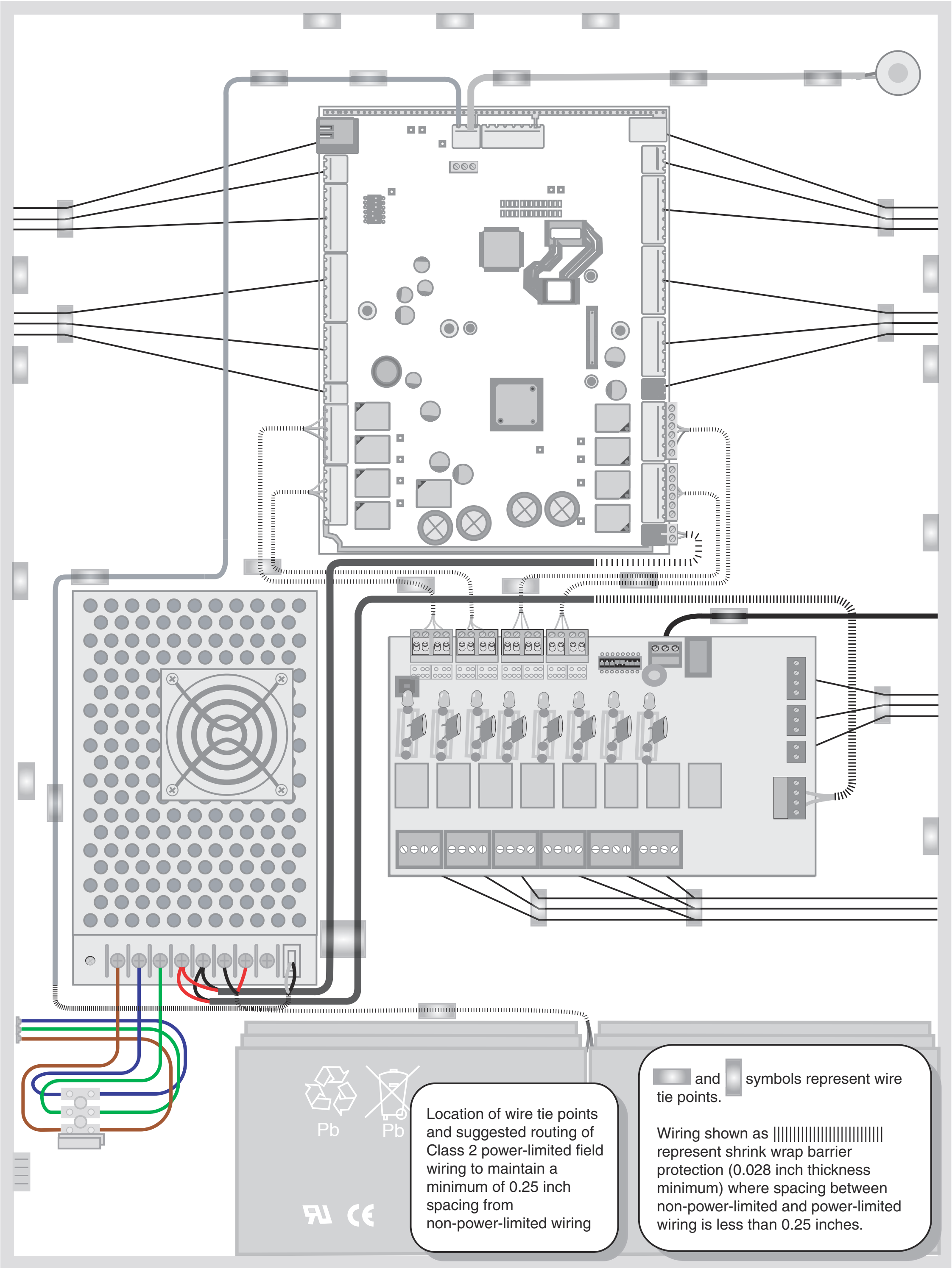
Perform these steps to install the optional AC inlet (HAS part number 100-00049):

1. Remove the knockout piece at the lower-left side of the enclosure.
2. Feed the AC inlet assembly wires through the opening from the outside.
3. Push the receptacle straight in, until it snaps into place.
4. Connect each colored wire to its corresponding color on the terminal block.
5. Plug the AC inlet unit’s power cord into the three-prong receptacle.
6. Plug the other end of the cable into a standard non-switched 115 VAC outlet.

Note: Use only a Honeywell-provided power cord (HAS part number 700-0109). UL has evaluated the use of this power cord with the optional AC inlet for the NX4L1.

4.2 Typing the Field Wiring in the NX4L1 Cabinet

Figure 2: Tying the Field Wiring in the NX4L1 Cabinet



Location of wire tie points and suggested routing of Class 2 power-limited field wiring to maintain a minimum of 0.25 inch spacing from non-power-limited wiring

▭ and ▯ symbols represent wire tie points.

Wiring shown as |||||||||||||||||||||||||||||| represent shrink wrap barrier protection (0.028 inch thickness minimum) where spacing between non-power-limited and power-limited wiring is less than 0.25 inches.

4.3 Cabinet Mounting

The following five figures show the back, top, bottom, right, and left views of the NetAXS panel cabinet. Each view includes the dimensions and knockout placement that you will need to mount the cabinet. See Table 1 on page 27 for dimensions of the conduit entries into the cabinet.

Figure 3: NetAXS Panel Cabinet, Back View

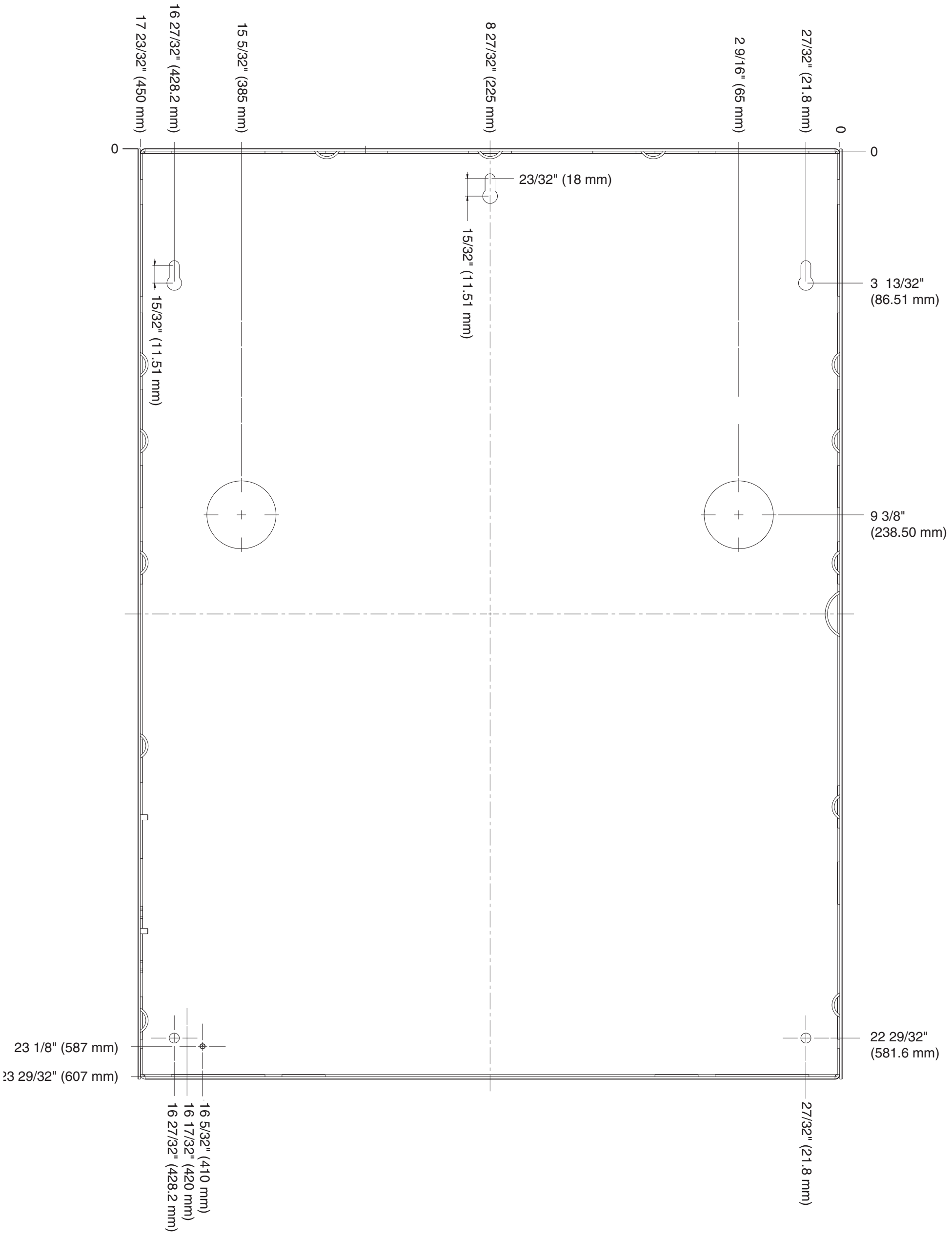


Figure 4: NetAXS Panel Cabinet, Top View

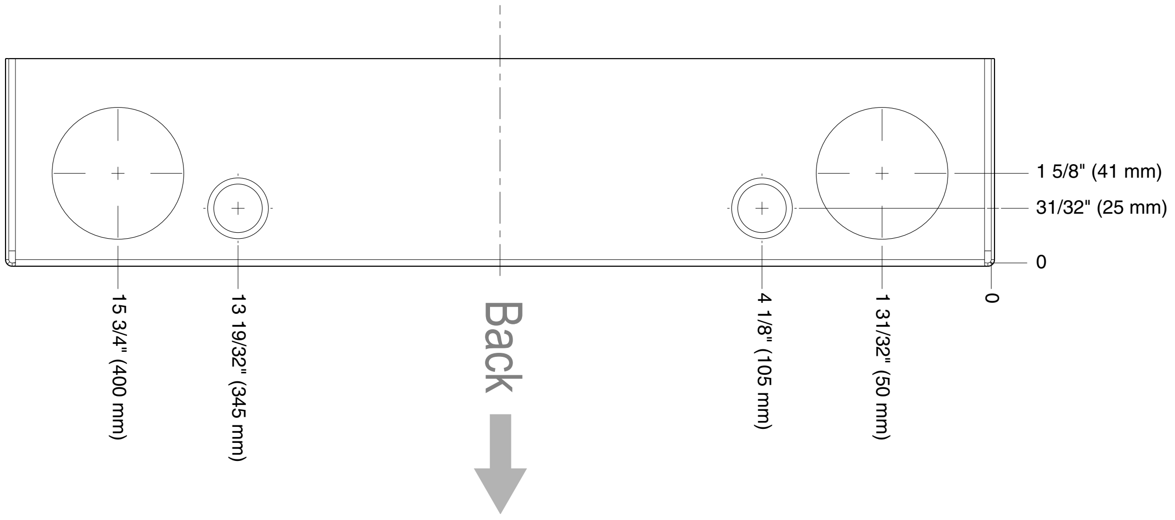


Figure 5: NetAXS Panel Cabinet, Bottom View

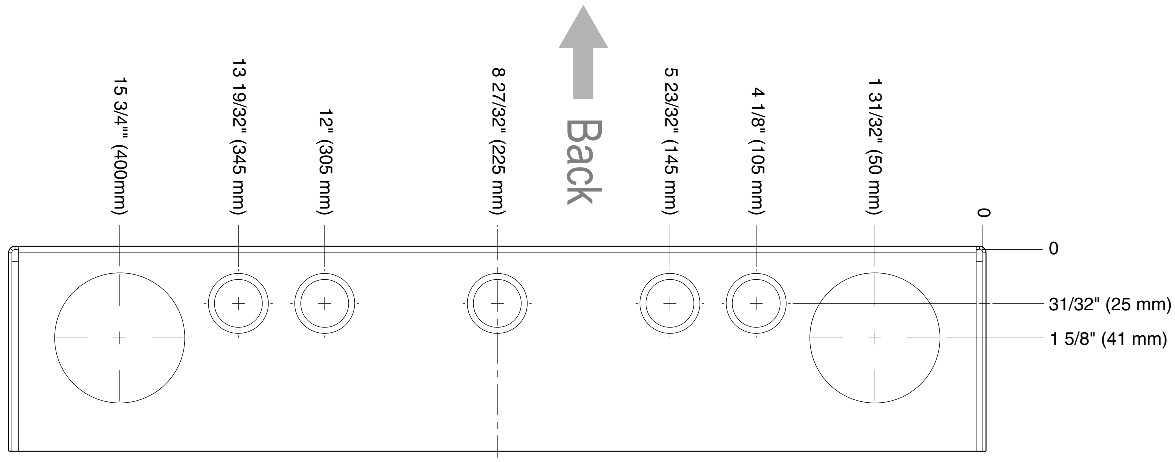


Figure 6: NetAXS Panel Cabinet, Left View

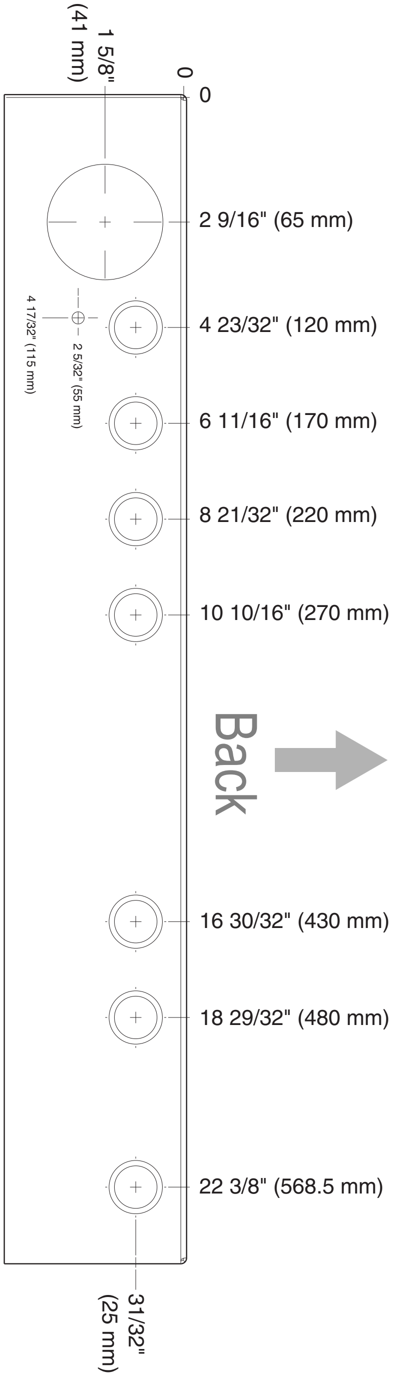


Figure 7: NetAXS Panel Cabinet, Right View

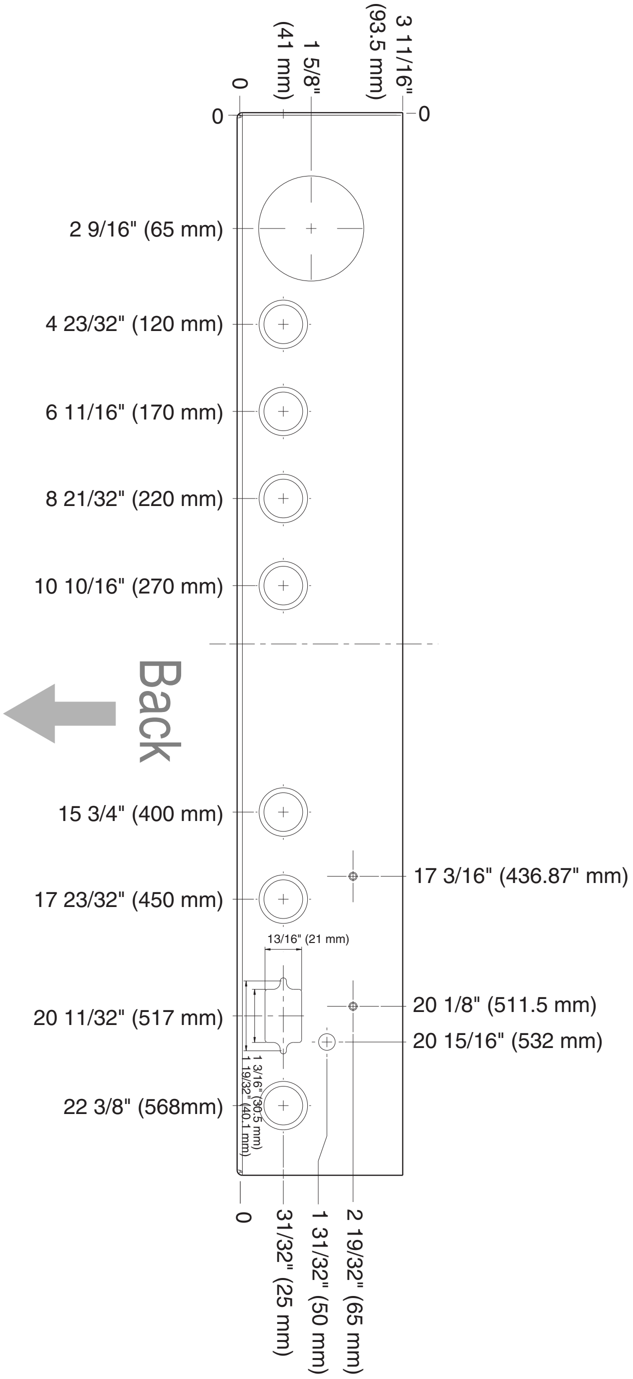


Table 1 lists the dimensions of the cabinet's conduit entries.

Table 1 Cabinet Electrical Entries

ENCLOSURE	CONDUIT 1/2" (12.7 mm)	CONDUIT 3/4" (19.0 mm)	CONDUIT 1" (25.4 mm)	CONDUIT 2" (50.8 mm)
Top	5	5	N/A	2
Bottom	2	2	N/A	2
Right Side	8	8	N/A	N/A
Left Side	6	6	N/A	N/A
Back	N/A	N/A	2	N/A

4.4 Reader Wiring

Each reader port supports a single 12-volt reader with Wiegand output format. Power to the readers is shared with the AUX Power ports TB3 and TB14. The maximum power draw is 600 mA for readers and AUX Power combined.

To fully utilize each reader port, a shielded 7-conductor cable (18–22 AWG) is required. The reader buzzer feature is not supported with NetAXS-4. Therefore, you can use the standard six-conductor cable. The cable shield should be grounded at the panel only. Grounding at both ends can cause ground loops which can be disruptive. The maximum recommended length of wiring is 500 feet per reader.

Table 2 Reader Wiring

Terminal	Wire Color	Wiegand Reader
TB5-1, 6-1, 11-1, 12-1	Brown	LED Control
TB5-2 6-2, 11-2, 12-2	Green	Wiegand Data 0 or Data
TB5-3, 6-3, 11-3, 12-3	White	Wiegand Data 1 or Clock
TB5-4, 6-4, 11-4, 12-4	Black	Common
TB5-5, 6-5, 11-5, 12-5	Red	12 VDC Power
TB5-6, 6-6, 11-6, 12-6	Variable	Tamper
TB5-7, 6-7, 11-7, 12-7	Variable	Buzzer

Note: Incorrect wiring of the reader to the panel can cause the panel to stop operating.

4.5 Supervised Input Wiring

The supervised inputs are located on TB4 and TB13 (Figure 8 on page 28). Input 1 through Input 8 may be configured for normally open or normally closed contacts as supervised or non-supervised. Inputs 13 and 14 are on TB8. All eight inputs have default functions, but they can be configured for general purpose inputs.

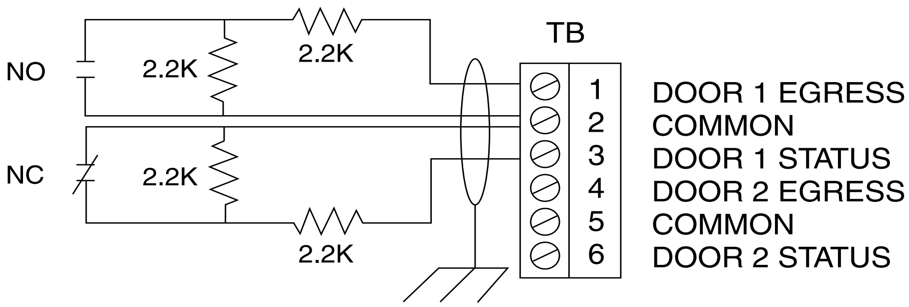
The following table identifies the default function for each terminal position.

Table 3 Default Supervised Input Assignments

Terminal Position	Default Function
TB4-1	Door 1 REX (Egress)
TB4-3	Door 1 Status
TB4-4	Door 2 REX (Egress)
TB4-6	Door 2 Status
TB8-1	External Power Supply AC FAIL
TB8-3	Panel Tamper
TB13-1	Door 3 REX (Egress)
TB13-3	Door 3 Status
TB13-4	Door 4 REX (Egress)
TB13-6	Door 4 Status
TB 5-6, 6-6, 11-6, 12-6	Optional supervised input if not used for a reader tamper

The following figure shows the typical wiring for a supervised input.

Figure 8: Typical Supervised Input Wiring Diagram



The figure above shows standard 2,200 ohm resistors. The NetAXS panel accepts 1,000, 2,200, 4,700, or 10,000 ohm values. Note that both resistors must have the same value. See the *NetAXS™ Access Control Unit User's Guide* for instructions on selecting resistor options.

In addition, the Tamper and External Power Fail, as well as the Reader and Panel tampers can be supervised and capable of being used as additional inputs if the default functionality is not needed. They also share a single common.

The wire used for the inputs should be shielded and cannot exceed 30 ohms over the entire length of the cable. Remember that the distance from the panel to the door must be doubled to determine the total resistance.

CAUTION The cable shield should be grounded only at the panel earth ground. Grounding at both ends can cause ground loops which can be disruptive.

CAUTION The system has not been verified for compliance with UL1076 Burglar Alarm units and systems.

4.6 NX4L1 Control Output Wiring

The NX4L1 provides a Power Distribution Output circuit board that is pre-wired to the eight relays on the control panel. Each panel relay controls the correspondingly numbered Power Distribution Output relay.

Relay 1 is defaulted for control of the Door 1 lock, Relay 2 is defaulted for the control of the Door 2 lock, Relay 3 is defaulted for the control of the Door 3 lock, and Relay 4 is defaulted for the control of the Door 4 lock. Relays 5–8 are used as auxiliary relays. Refer to the *NetAXS Access Control Unit User's Guide* for details on controlling the relay operations. The NX4L1 is wired to enable the internal nominal 24 VDC power supply to be used to power the access control door strikes/locks or other auxiliary loads. The voltage range of the relay outputs is 23.5 VDC to 25 VDC. 2A is the maximum the maximum total current for all relays and the maximum current for each relay. If the application requires a separate supply, refer to the Power Distribution Output board installation manual for details.

Each Power Distribution Board Output relay has a built-in fast-acting over current protection circuit. When the current through the relay output exceeds 2 amps, the output power will be interrupted and a yellow LED will illuminate to indicate which power output was interrupted. Each relay also has a red indicator LED, which indicates the relay state. If the relay is active, the LED is illuminated.

For field wiring, attach the negative terminal of the load to the NEG output terminal of the Power Distribution Output relay. Attach the positive load terminal to either the Normally Open or Normally Closed terminal of the Power Distribution Output relay. Refer to Figure 9 on page 31 for a wiring example.

CAUTION The cable used must be sized for the current load and should be shielded. The cable shield should be grounded at the panel only. Grounding at both ends can cause ground loops which can be disruptive. Do not bundle these wires with communication, reader, or supervised input wiring.

The Power Distribution Output board can be connected to an external Fire Alarm Control Panel (FACP). When the FACP input signal is active, it will turn off the selected relays on the Power Distribution Output board. An eight-position DIP switch is used to select which Power Distribution Output relays are affected by the FACP input. To make an output respond to the FACP input, move the associated DIP switch to the OFF position. To have the relay ignore the state of the FACP input, move the DIP switch to the ON position.

The Power Distribution Output board has a green LED that indicates the status of the external FACP input. The LED will turn on when the input is active and turn off when inactive.

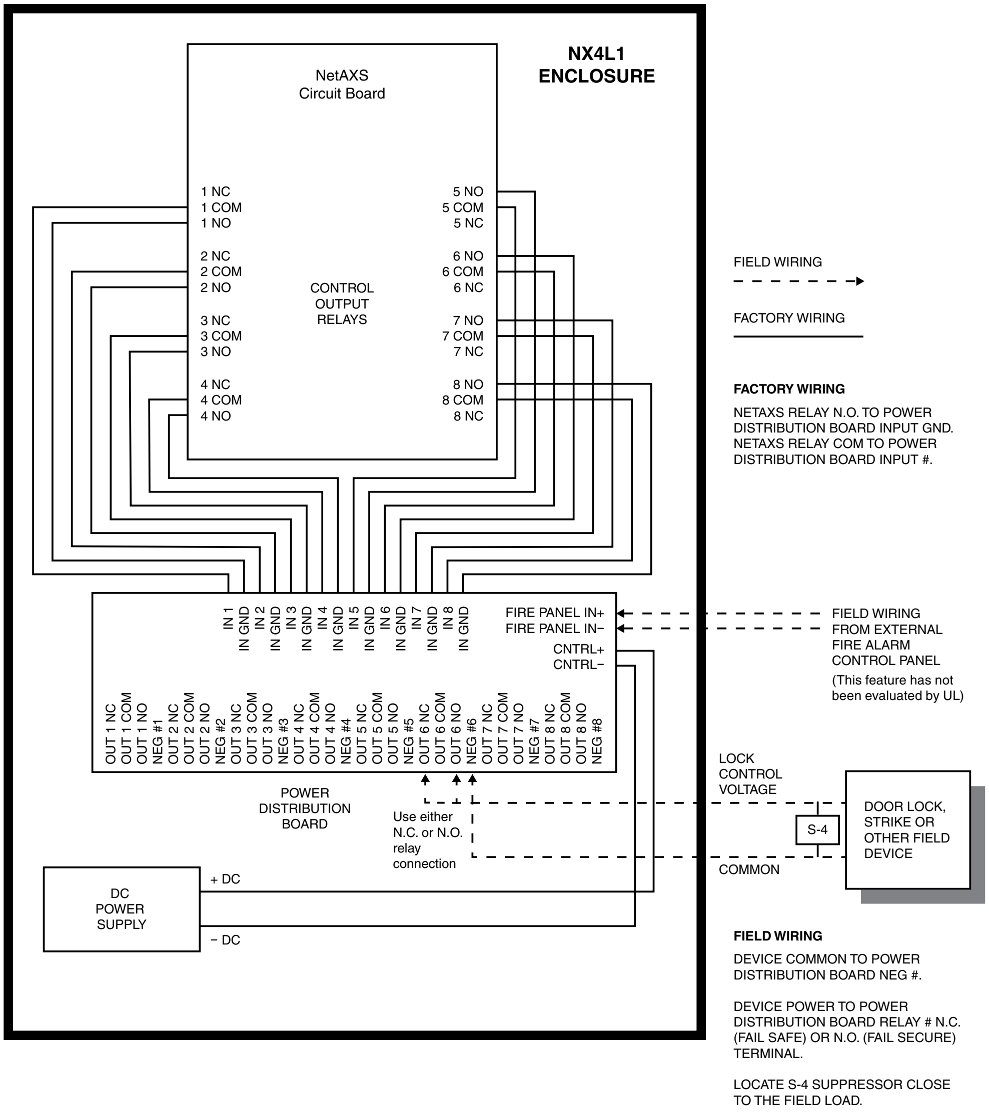
Table 4: NetAXS Relay and Power Distribution Board DIP Switch Associations

Default Function	**NetAXS Board Relay**	**Power Distribution Output Board Relay**	**Power Distribution Output Board DIP Switch**
Door 1	1	1	1
Door 2	2	2	2
Door 3	3	3	3
Door 4	4	4	4
Auxiliary	5	5	5
Auxiliary	6	6	6
Auxiliary	7	7	7
Auxiliary	8	8	8

The Power Distribution Output board has two dry contact outputs, FACP (fire) and power fail, that can be used to monitor the general condition of the system. The TRBL relay output is de-energized if the +24 VDC is off or if the over current protection circuit is active. The FACP relay output will de-energize if the external FACP input is active. Either one of these outputs can be optionally wired into the supervised inputs on the NetAXS panel and configured as two-state inputs.

The following figure shows the power distribution board field wiring.

Figure 9: Power Distribution Board Field Wiring



(This feature has not been evaluated by UL)

FACTORY WIRING

NETAXS RELAY N.O. TO POWER DISTRIBUTION BOARD INPUT GND.
NETAXS RELAY COM TO POWER DISTRIBUTION BOARD INPUT #.

FIELD WIRING

DEVICE COMMON TO POWER DISTRIBUTION BOARD NEG #.

DEVICE POWER TO POWER DISTRIBUTION BOARD RELAY # N.C. (FAIL SAFE) OR N.O. (FAIL SECURE) TERMINAL.

LOCATE S-4 SUPPRESSOR CLOSE TO THE FIELD LOAD.

4.7 Communications

CAUTION Do not route communication wires with power or locking devices.

Note: Because UL has approved the NetAXS panel only as a standalone system, the computer terminal, NetAXS gateway panel, and N-485_PCI-2 adapter appear in this section's figures only to illustrate the installation and programming of the NetAXS panel.

RS-232 Communications

The NetAXS panel communicates with a PC through a 50-foot RS-232 cable (HAS part number CBL50). Connect the RJ45 end of the cable to the jack on the NetAXS panel.

The cable is used to provide communication to a single panel. A second cable can be used with another NetAXS control panel connected to a second COM (communication) port, which would enable eight readers to be used, see Figure 11, RS-232 Configuration.

Figure 10 illustrates the connections for an RS-232, DB9 (9 pin) connector to the panel's RJ-45 serial port. Replacement cables can be obtained by contacting your Honeywell Access System Representative.

Figure 10: RJ-45 Serial Port

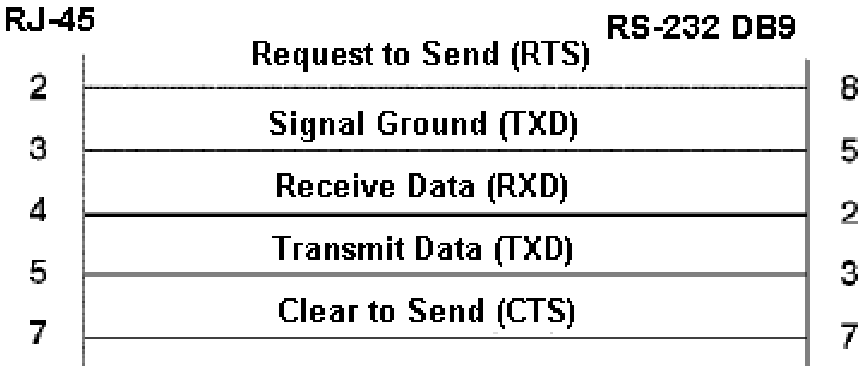
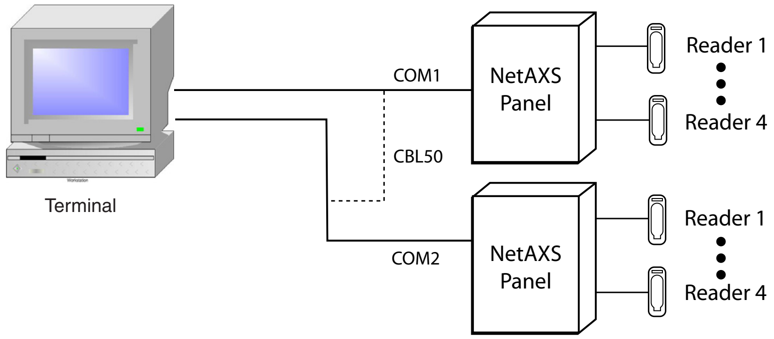


Figure 11: RS-232 Configuration



One NetAXS panel per COM port. Two COM ports possible.

RS-485 Communications

The NetAXS panel can reside on an existing RS-485 drop line hosted by either a NetAXS panel configured as a Gateway, or N-485-PCI-2, PCI-3, or N-485-HUB-2 (see Figure 12, Figure 13, and Figure 24). The interface allows the wiring of a multidrop communication network of up to 4,000 feet (1200 m) in length. Only one host converter device per drop line is supported.

Note: On a multidrop line, the Gateway panel and the PCI unit can have either end-point or interior positions. See Figure 20 on page 44 and Figure 21 on page 45.

DIP switch position 6 on the NetAXS panel selects whether the panel is a Gateway or Multidrop panel. The switch in the OFF position configures the panel as a Multidrop panel; ON configures a Gateway. The panel must be power cycled for a new switch setting to be recognized. DIP switch positions 1-5 are used to select the panel's address on the network. Refer to Table 5 for DIP switch setting information.

Connectors J36 and J37 are provided for supplying biasing and end-of-line termination for the RS-485 network. The board ships with all jumpers open. For a multidrop RS-485 line, you must close both J36 and J37 (terminated and biased) at the two end-point panels. At all other panels, leave J36 and J37 open. Both jumpers on a given panel must set the same. Note that biasing and termination on both ends are present. Use the jumpers on both ends of the RS-485 network.

Note: If an RS-485 network has a NetAXS Gateway panel, no N1000-II, N1000-III, or N1000-IV are allowed on the same network. If they are added to a network with a NetAXS Gateway panel, they will not be able to communicate with the host computer.

Figure 12:   RS-485 Configuration via N-485-PCI-2 or PCI-3

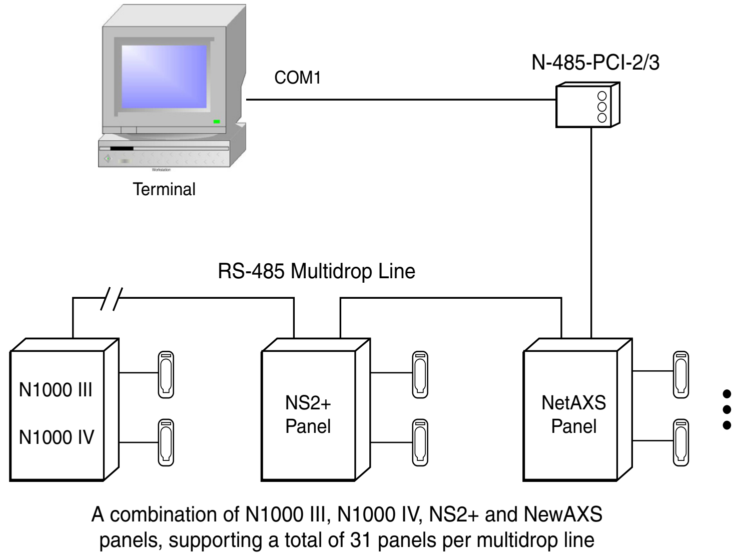
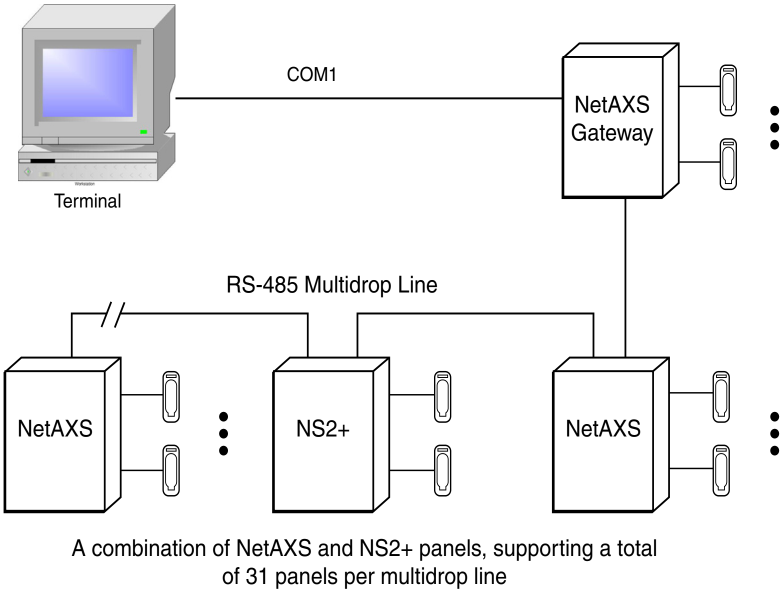
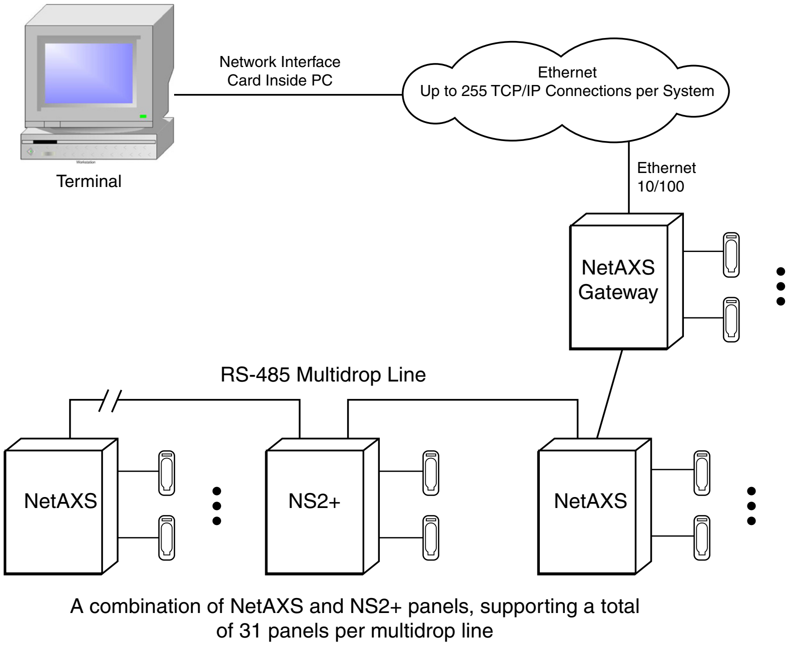

COM1
N-485-PCI-2/3
Terminal
RS-485 Multidrop Line
N1000 III
N1000 IV
NS2+
Panel
NetAXS
Panel
A combination of N1000 III, N1000 IV, NS2+ and NewAXS
panels, supporting a total of 31 panels per multidrop line

Figure 13:   RS-485 Configuration via NetAXS Gateway


COM1
Terminal
NetAXS
Gateway
RS-485 Multidrop Line
NetAXS
NS2+
NetAXS
A combination of NetAXS and NS2+ panels, supporting a total
of 31 panels per multidrop line

Ethernet TCP/IP Communications

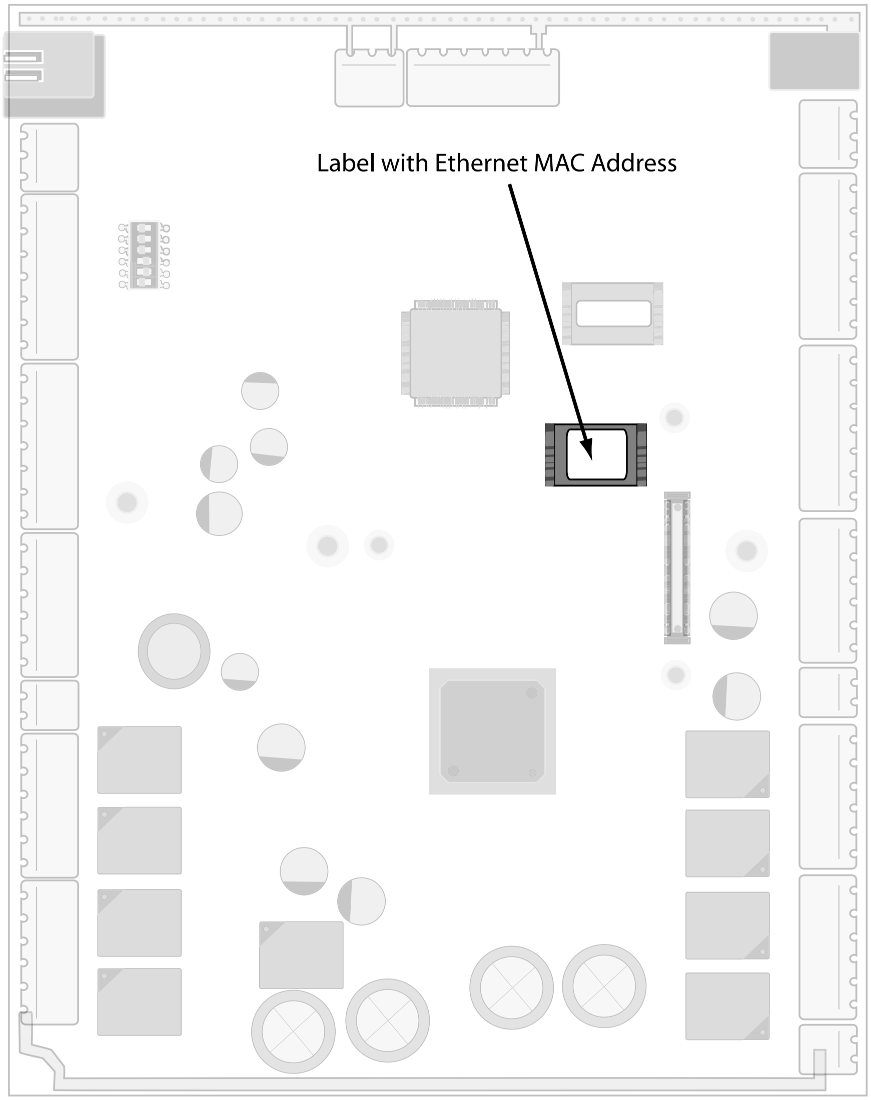
Figure 14: Ethernet TCP/IP Configuration


Network Interface
Card Inside PC
Ethernet
Up to 255 TCP/IP Connections per System
Terminal
Ethernet
10/100
NetAXS
Gateway
RS-485 Multidrop Line
NetAXS
NS2+
NetAXS
A combination of NetAXS and NS2+ panels, supporting a total
of 31 panels per multidrop line

Each NetAXS panel has a port for an Ethernet TCP/IP interface (see Figure 14, Ethernet TCP/IP Configuration). The Ethernet TCP/IP interface provides 10/100 Mbit Ethernet support for each panel. Up to 31 panels can be configured on each TCP/IP connection.

Figure 15 shows the location of the panel’s unique MAC ID.

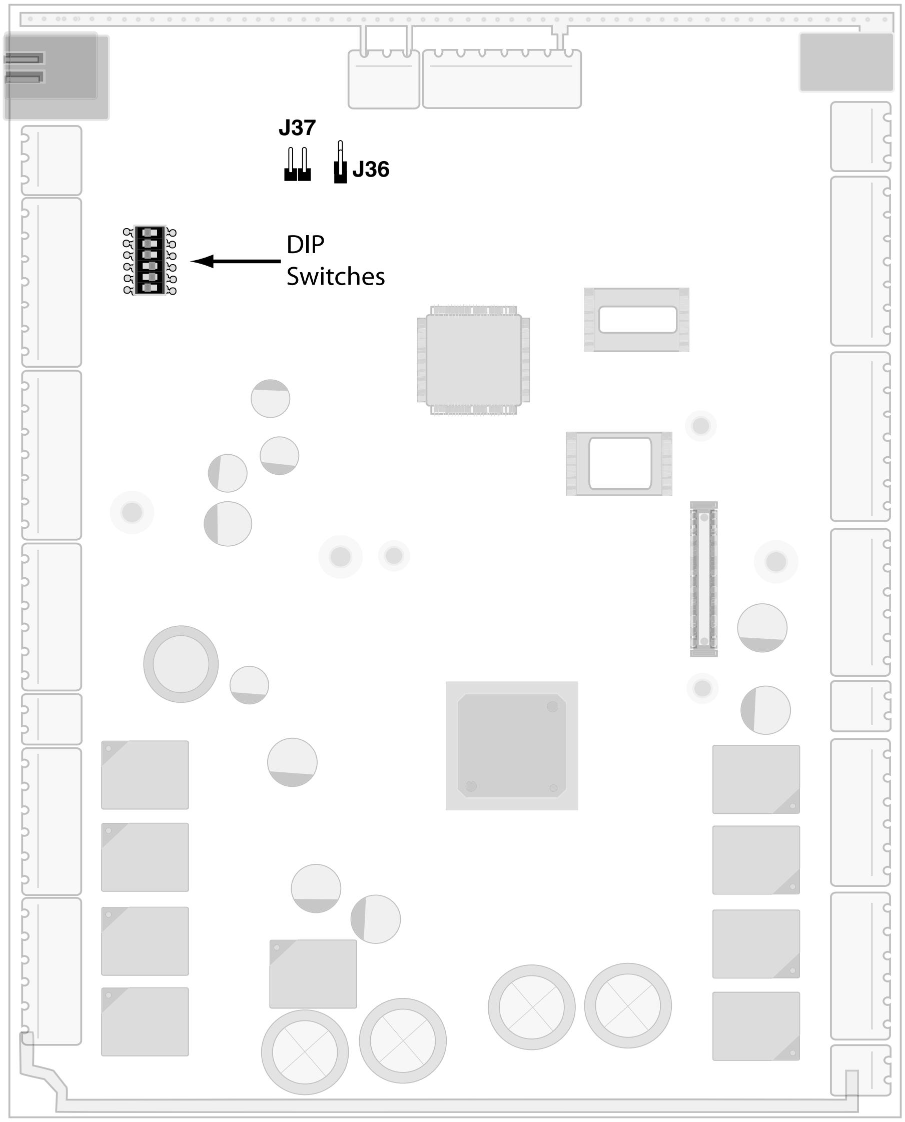
Figure 15: Ethernet MAC Address Location



4.8 DIP Switch Settings

Figure 16 locates the NX4L1 DIP switch panel and the J36 and J37 jumpers.

Figure 16: DIP Switch and Jumper Location



Use the following DIP switch configurations to set the panel address.

Table 5 DIP Switch Settings

S1	S2	S3	S4	S5	S6	Selection
on	off	off	off	off		Address 1 (default)
off	on	off	off	off		Address 2
on	on	off	off	off		Address 3
off	off	on	off	off		Address 4
on	off	on	off	off		Address 5
off	on	on	off	off		Address 6
on	on	on	off	off		Address 7
off	off	off	on	off		Address 8
on	off	off	on	off		Address 9
off	on	off	on	off		Address 10
on	on	off	on	off		Address 11
off	off	on	on	off		Address 12
on	off	on	on	off		Address 13
off	on	on	on	off		Address 14
on	on	on	on	off		Address 15
off	off	off	off	on		Address 16
on	off	off	off	on		Address 17
off	on	off	off	on		Address 18
on	on	off	off	on		Address 19
off	off	on	off	on		Address 20
on	off	on	off	on		Address 21
off	on	on	off	on		Address 22
on	on	on	off	on		Address 23
off	off	off	on	on		Address 24
on	off	off	on	on		Address 25
off	on	off	on	on		Address 26
on	on	off	on	on		Address 27
off	off	on	on	on		Address 28
on	off	on	on	on		Address 29
off	on	on	on	on		Address 30
on	on	on	on	on		Address 31
					off	NetAXS Multidrop
					on	NetAXS Gateway

Note: Address 0 is not a valid setting.

4.9 Jumper Settings

The NX4L1 panel control board includes jumpers 36 and 37, which set end-of-line termination and biasing for the Multidrop RS-485 Line.

The board ships with all jumpers set to OFF. For a Multidrop RS-485 Line, you must set both J36 and J37 to CLOSED (terminated and biased) at the two end-point panels. At all other panels, leave J36 and J37 at OPEN. Note that both jumpers on a given panel must either be OPEN or CLOSED.

4.10 Downstream I/O

Note: UL has not evaluated the compatibility of downstream I/O devices with the NetAXS panel.

In some applications, the number of system inputs or outputs exceeds the number that is standard on the NetAXS panel. The solution is to add a combination of NX4IN and NX4OUT modules external to the NetAXS enclosure on a dedicated RS-485 Downstream Input/Output (I/O) bus. A maximum of two NX4IN and a maximum of four NX4OUT for a total of six NX4IN/OUT modules can be added to the downstream bus.

An NX4IN module has 32 supervised, four-state inputs that are limited to 2,200 ohms resistance. The NX4OUT has two supervised inputs and 16 SPDT relay outputs. Each input is limited to 2,200 ohms resistance. Refer to the individual installation manuals for I/O wiring details.

The downstream I/O bus is wired into the NetAXS TB10 terminal block. The downstream bus has a fixed baud rate and communicates to the input and output modules using a polling technique.

Each NX4 input and output module needs to have a unique address for proper communication. Each one also has some configuration jumpers that need to be positioned correctly.

The following table lists the DIP switch and jumper settings for the input and output modules.

Table 6 NX4IN DIP Switch and Jumper Settings

Module	Setting	Value
NX4IN	DIP switches	Address (switches 1–6) - 1 or 2
		Baud rate (switches 7 and 8) - 7 = OFF, 8 = ON
		OP Mode (switches 9 and 10) - 9 = OFF, 10 = OFF

Table 6 NX4IN DIP Switch and Jumper Settings (continued)

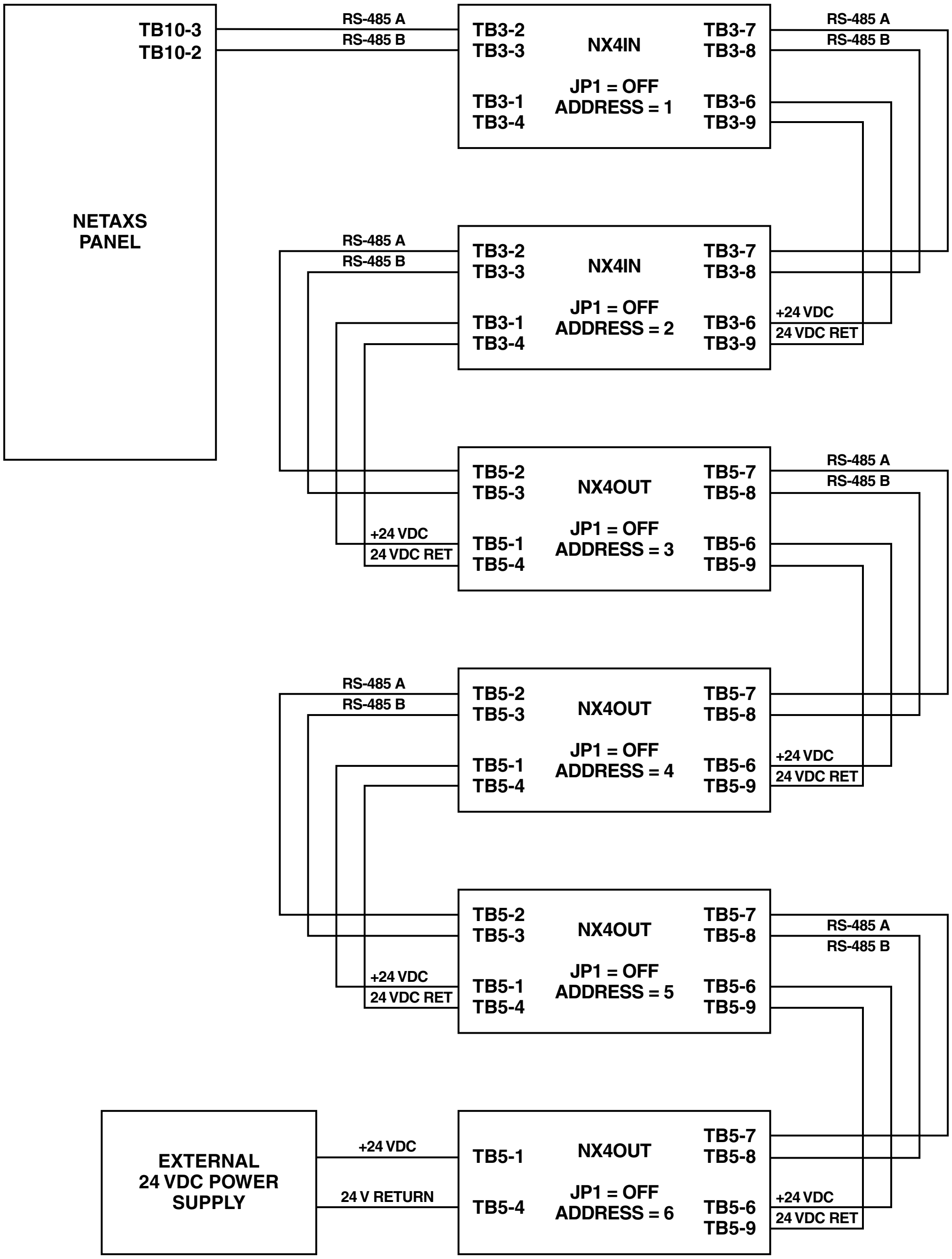
Module	Setting	Value
	Jumper settings	JP1 - CLOSED (if the module is the last module on the downstream bus), OPEN (if the module is not the last module on the downstream bus)
		JP2 - any setting
		JP3 - any setting
		JP4 - NORMAL (Positions 1 and 2)
NX4OUT	DIP switches	Address (switches 1–6) - 3 through 6
		Baud rate (switches 7 and 8) - 7 = OFF, 8 = ON
		OP Mode (switches 9 and 10) - 9 = OFF, 10 = OFF
	Jumper settings	JP1 - CLOSED, positions 2 and 3 (if the module is the last module on the downstream bus); OPEN, positions 1 and 2 (if the module is not the last module on the downstream bus)
		JP2 - NORMAL, positions 1 and 2

Note: If an NX4IN is not required in a system, start addressing the output modules at DIP switch 3. If an NX4IN is configured with an address other than 1 or 2, the NetAXS panel will not communicate with it. Likewise, if an NX4OUT is configured with an address other than 3 through 6, the NetAXS panel will not communicate with it.

The NetAXS board and the NX4L1 is not intended to provide either module power or module output load power for downstream I/O. A separate 24 VDC supply should be used to provide power to all downstream modules and output loads. For some installations, the noise immunity improves if the NetAXS common is connected to the 24 V Return wiring for the downstream modules. This connection is not needed for most installations.

The following figure shows the default downstream I/O system configuration with communication and power wiring.

Figure 17: Default Downstream I/O Configuration with Wiring



DEFAULT DOWNSTREAM I/O SYSTEM
CONFIGURATION WITH COMMUNICATION
AND POWER WIRING

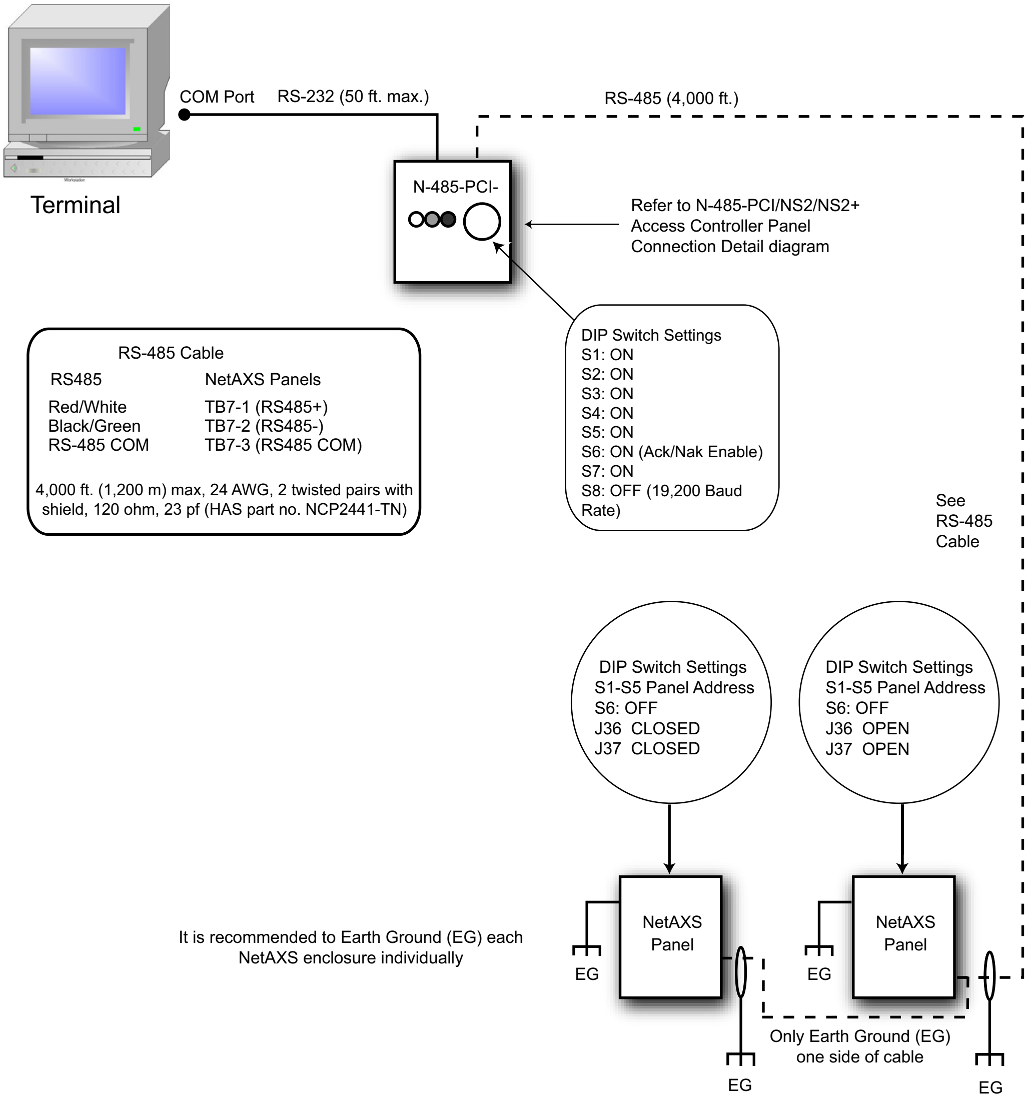
5.0 System Configuration

This section provides wiring diagrams for each of the NetAXS system configurations.

5.1 RS-485 Connection via PCI-2

This connection supports thirty-one NetAXS Access Controller panels for each drop line. Note that PCI-2 units can also be wired in interior, as well as in endpoint, positions. See Figure 20 on page 44 and Figure 21 on page 45. Because UL has approved the NetAXS panel only as a standalone system, the computer terminal, NetAXS gateway panel, and N-485_PCI-2 adapter appear in these sections only to illustrate the installation and programming of the NetAXS panel.

Figure 18: RS-485 Connection via PCI-2


Terminal
COM Port
RS-232 (50 ft. max.)
RS-485 (4,000 ft.)
N-485-PCI-
Refer to N-485-PCI/NS2/NS2+ Access Controller Panel Connection Detail diagram
See RS-485 Cable
NetAXS Panel
NetAXS Panel
EG
EG
EG
EG
It is recommended to Earth Ground (EG) each NetAXS enclosure individually
Only Earth Ground (EG) one side of cable

RS-485 Cable

RS485	NetAXS Panels
Red/White	TB7-1 (RS485+)
Black/Green	TB7-2 (RS485-)
RS-485 COM	TB7-3 (RS485 COM)

4,000 ft. (1,200 m) max, 24 AWG, 2 twisted pairs with shield, 120 ohm, 23 pf (HAS part no. NCP2441-TN)

DIP Switch Settings
S1: ON
S2: ON
S3: ON
S4: ON
S5: ON
S6: ON (Ack/Nak Enable)
S7: ON
S8: OFF (19,200 Baud Rate)

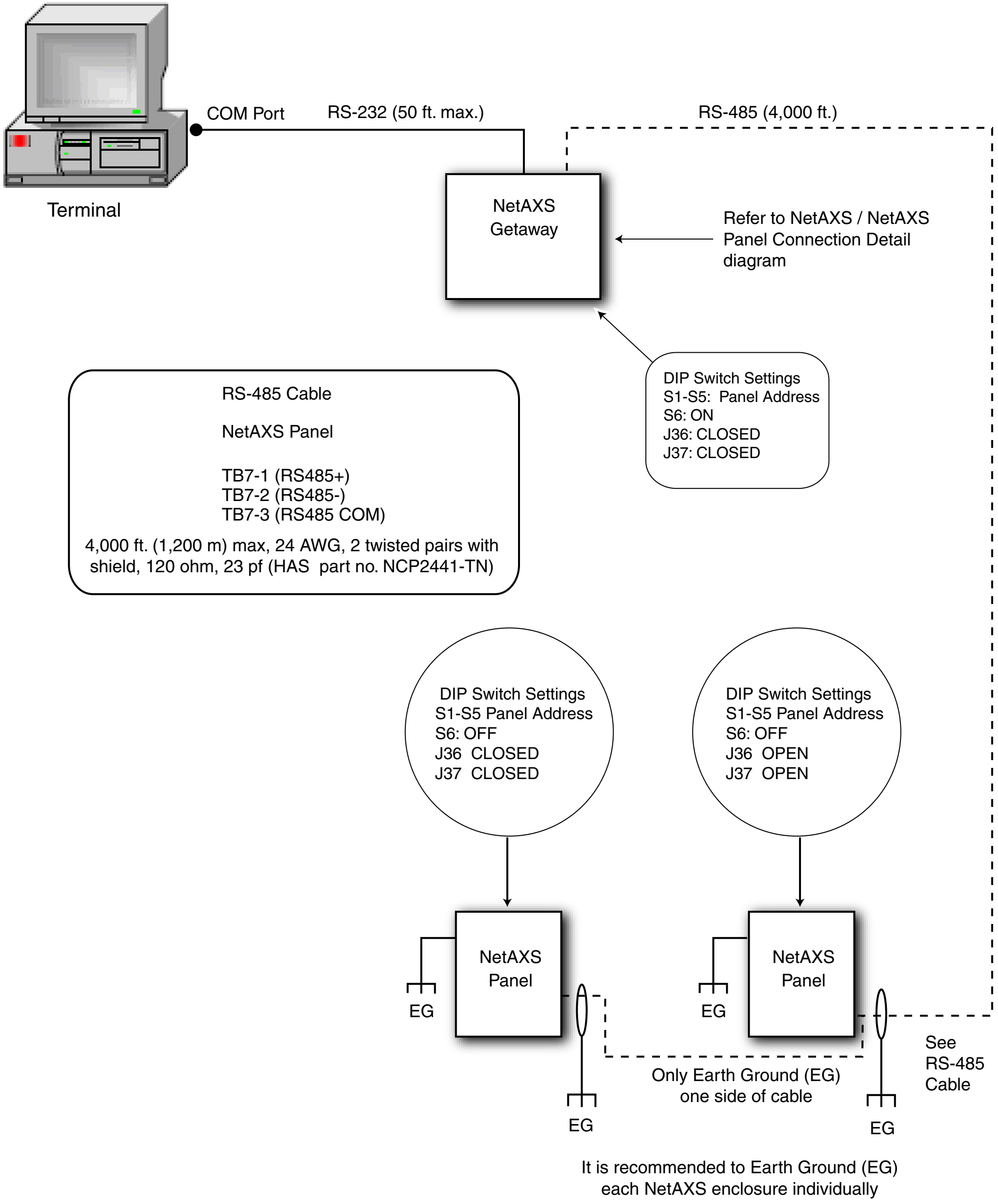
DIP Switch Settings
S1-S5 Panel Address
S6: OFF
J36 CLOSED
J37 CLOSED

DIP Switch Settings
S1-S5 Panel Address
S6: OFF
J36 OPEN
J37 OPEN

5.2 RS-485 Connection via NetAXS

This connection supports thirty-one NetAXS Access Controller panels for each drop line. However, because UL has approved the NetAXS panel only as a standalone system, the computer terminal and NetAXS gateway panel appear in this illustration only to show the installation and programming of the NetAXS panel.

Figure 19: RS-485 Connection via NetAXS



5.3 RS-485 Connections with Multidrop Panels at Both Ends of the Cable

You can connect Multidrop panels at both ends of an RS-485 cable via either a NetAXS panel or a PCI-2 device. This connection has not been approved by UL.

Figure 20: RS-485 Connection via NetAXS with Multidrop Panels at Both Ends

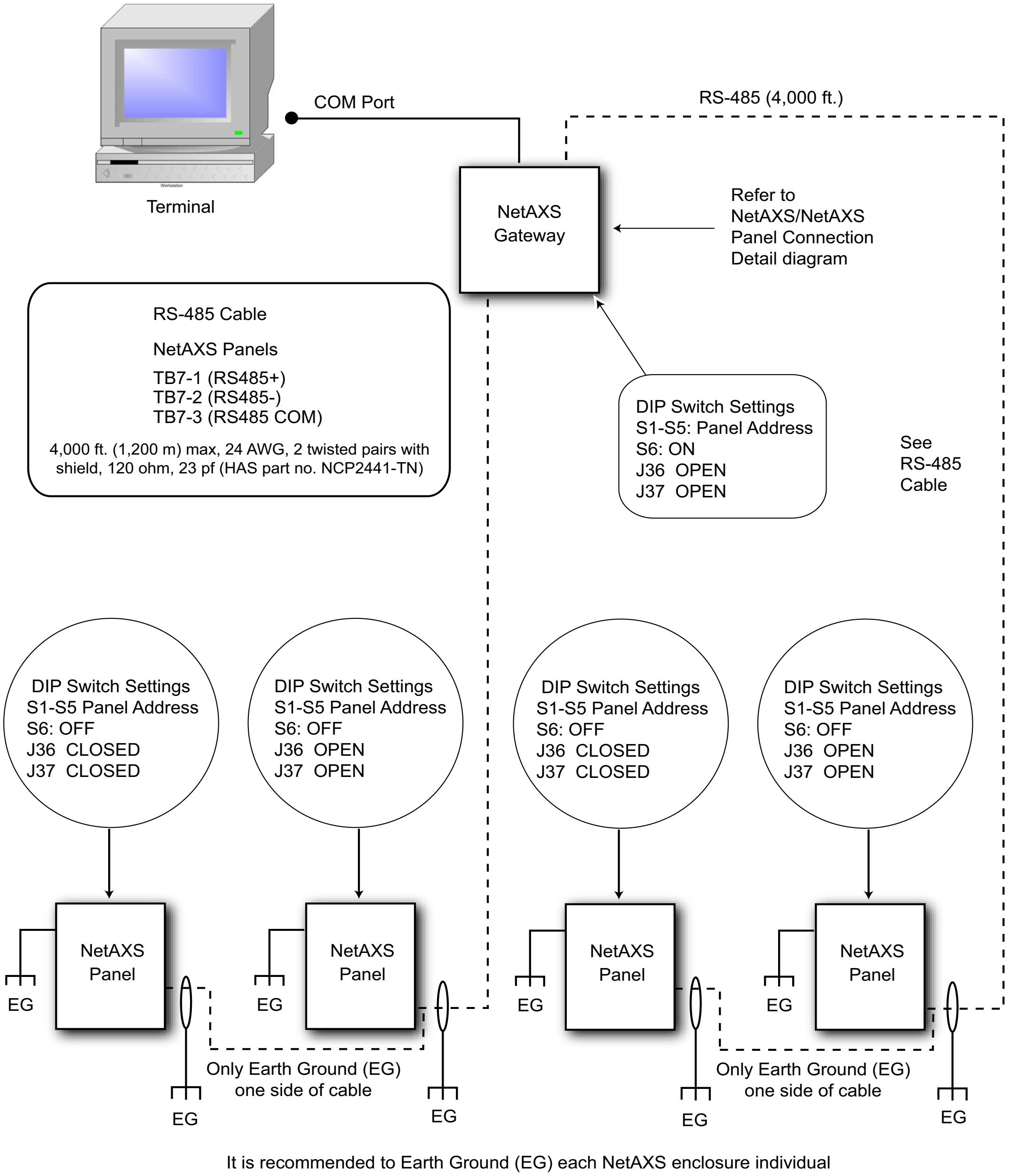
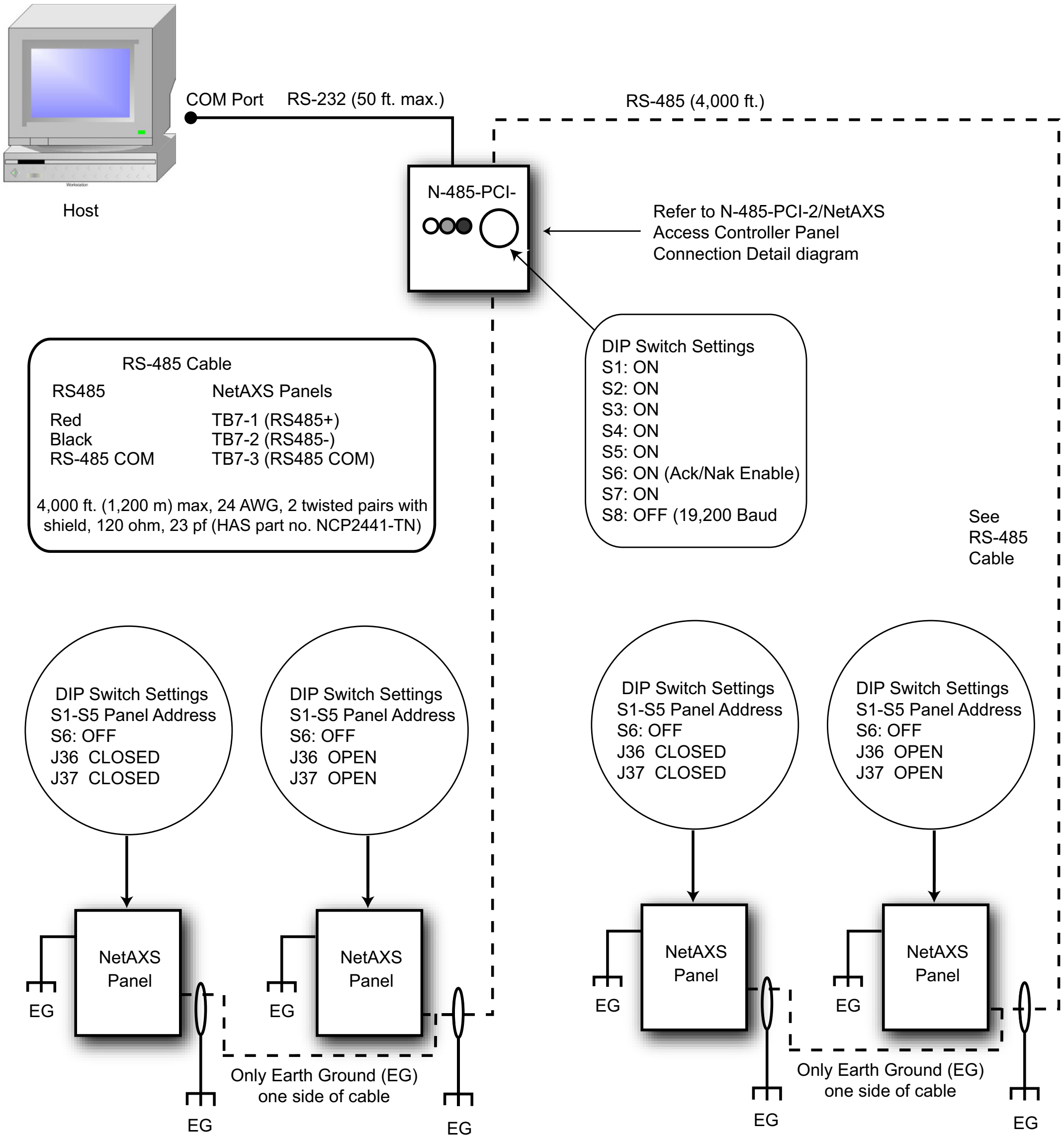


Figure 21: RS-485 Connection via PCI-2 with Multidrop Panels at Both Ends



RS-485 Cable

RS485	NetAXS Panels
Red	TB7-1 (RS485+)
Black	TB7-2 (RS485-)
RS-485 COM	TB7-3 (RS485 COM)

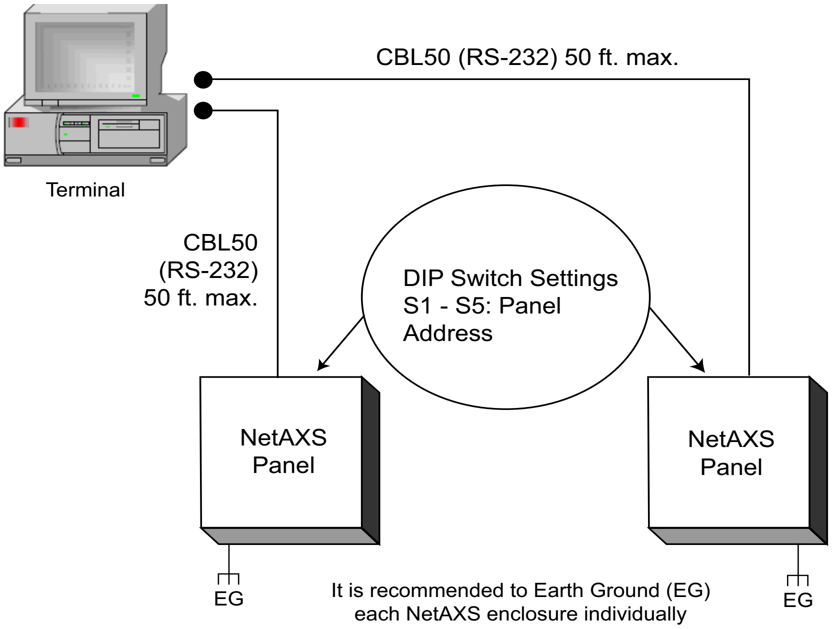
4,000 ft. (1,200 m) max, 24 AWG, 2 twisted pairs with shield, 120 ohm, 23 pf (HAS part no. NCP2441-TN)

It is recommended to Earth Ground (EG) each NetAXS enclosure individually

5.4 RS-232 Connection

This connection supports one NetAXS Access Controller panel for each COM port. It has been approved by UL. However, because UL has approved the NetAXS panel only as a standalone system, the computer terminal and NetAXS gateway panel appear in this section only to illustrate the installation and programming of the NetAXS panel.

Figure 22: RS-232 Connection



It is recommended to Earth Ground (EG) each NetAXS enclosure individually

CBL50 (RS-232)

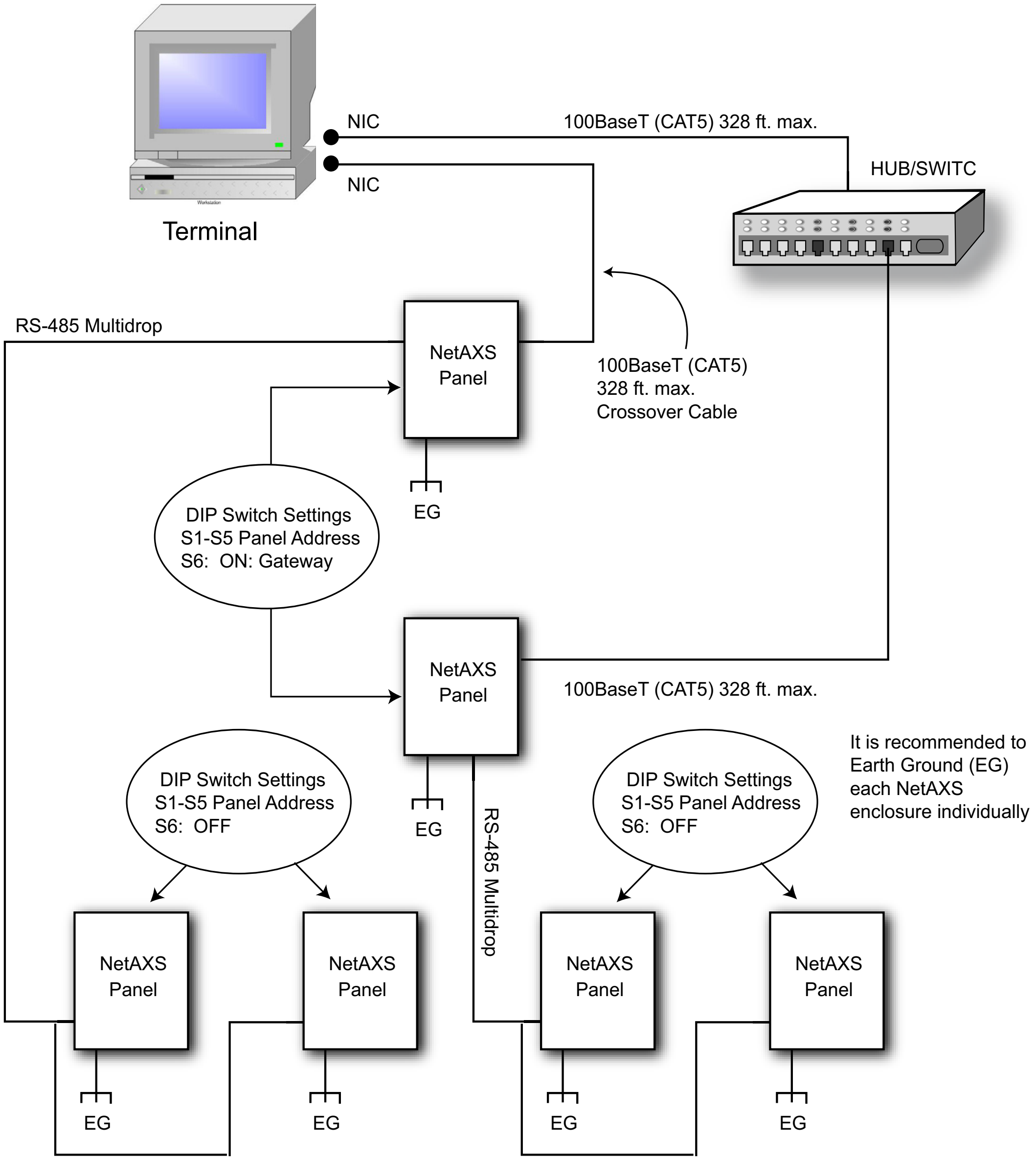
RS-232 (DB9)		RJ-45
8	← Request To Send (RTS) →	2
5	← Signal Ground (GND) →	3
2	← Receive Data (RXD) →	4
3	← Transmit Data (TXD) →	5
7	← Clear To Send (CTS) →	7

9-Pin COM 1 or COM 2 to RJ-45 on NetAXS Panel

5.5 Ethernet Connection

This connection supports a maximum of 255 IP connections per server. It has not been approved by UL.

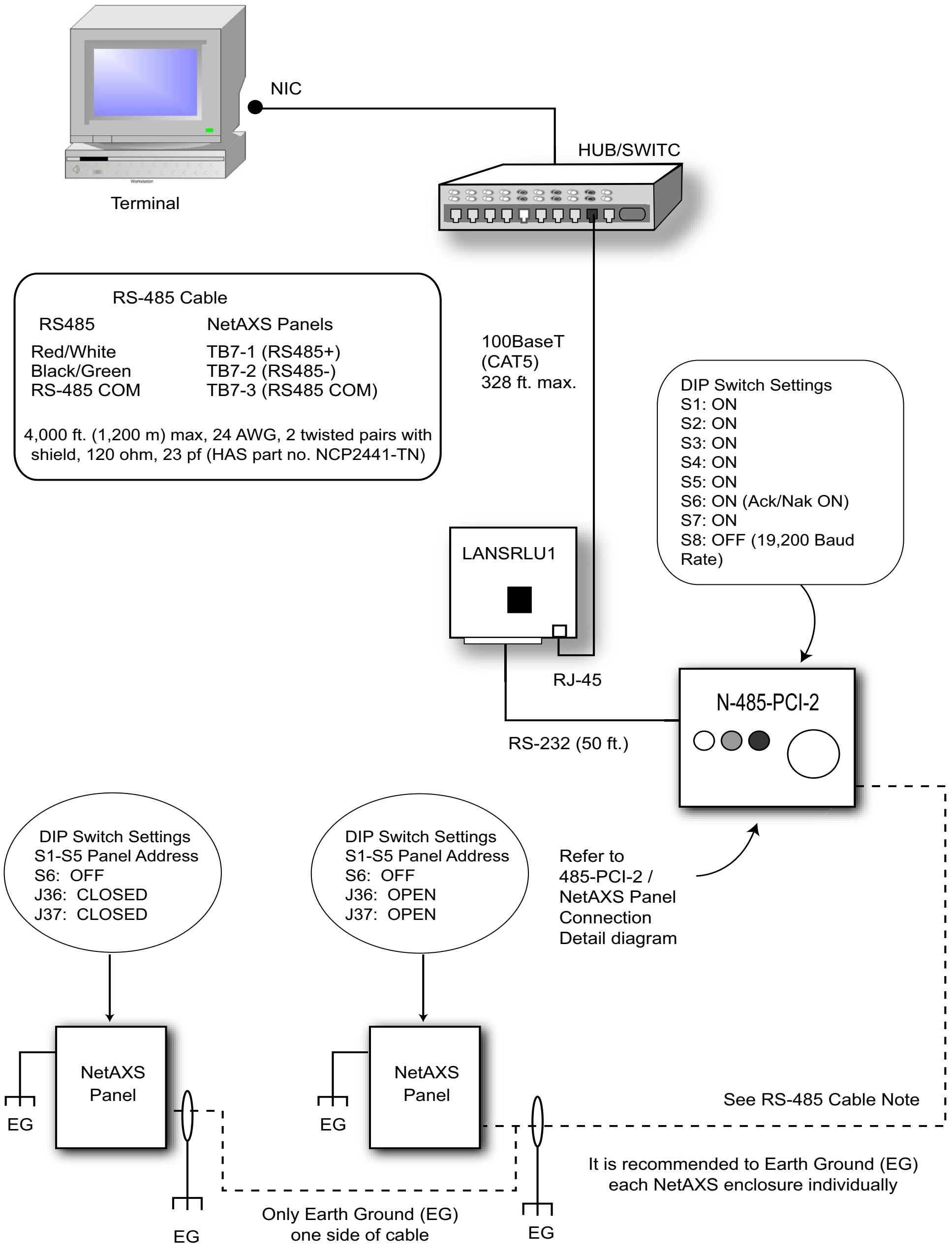
Figure 23: Ethernet Connection



5.6 LANSRLU1 Connection

This connection supports 31 panels for each drop line and a maximum of 255 IP connections. It has not been approved by UL.

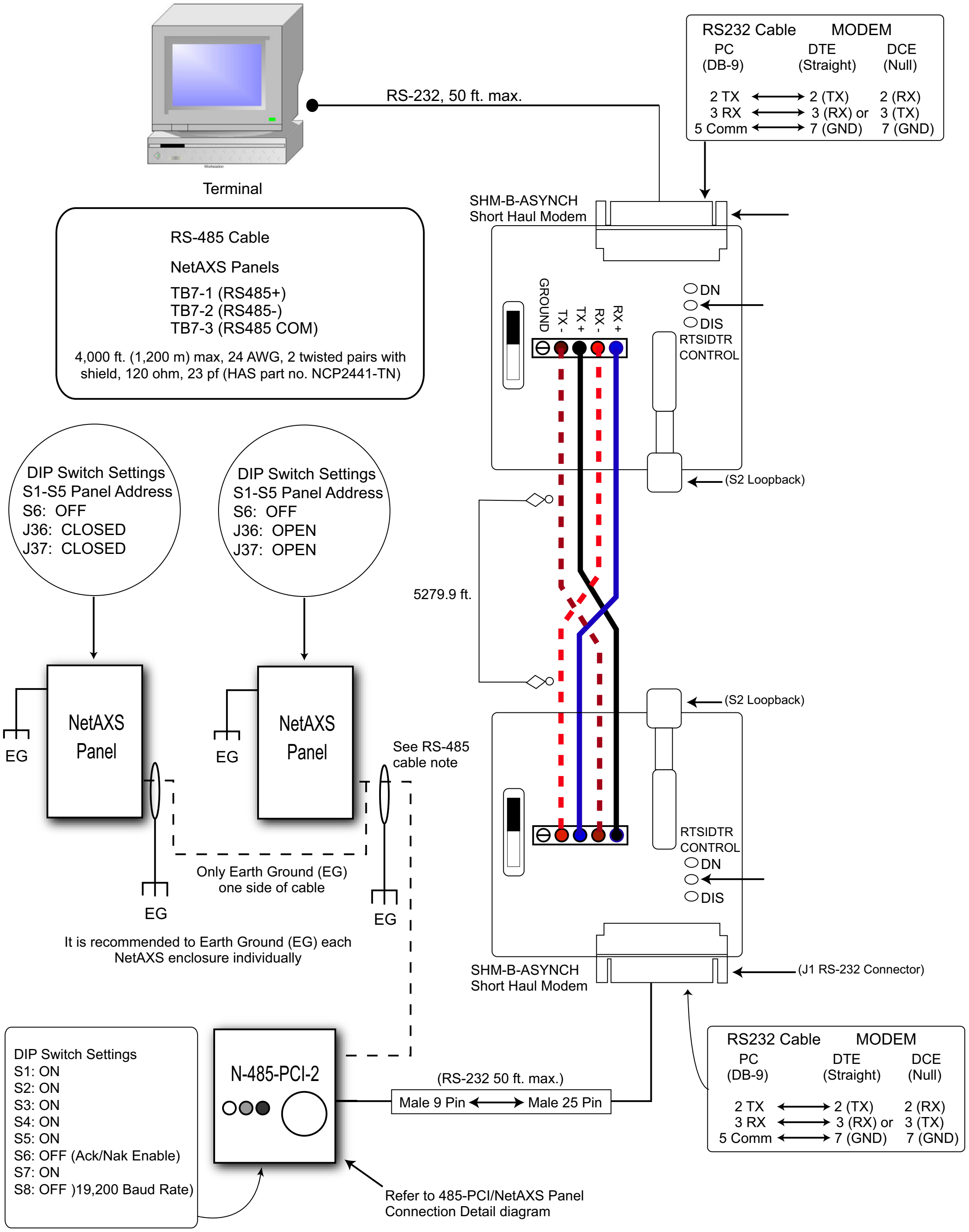
Figure 24: LANSRLU1 Connection



5.7 RS-485 Short Haul Modem Connection via PCI-2

This connection supports 31 NetAXS Access Controller panels for each drop line. It has not been approved by UL.

Figure 25: RS-485 Short Haul Modem Connection via PCI-2



RS232 Cable	MODEM	
PC (DB-9)	DTE (Straight)	DCE (Null)
2 TX ⟷	2 (TX)	2 (RX)
3 RX ⟷	3 (RX) or	3 (TX)
5 Comm ⟷	7 (GND)	7 (GND)

RS-485 Cable

NetAXS Panels

TB7-1 (RS485+)
TB7-2 (RS485-)
TB7-3 (RS485 COM)

4,000 ft. (1,200 m) max, 24 AWG, 2 twisted pairs with shield, 120 ohm, 23 pf (HAS part no. NCP2441-TN)

DIP Switch Settings
S1-S5 Panel Address
S6: OFF
J36: CLOSED
J37: CLOSED

DIP Switch Settings
S1-S5 Panel Address
S6: OFF
J36: OPEN
J37: OPEN

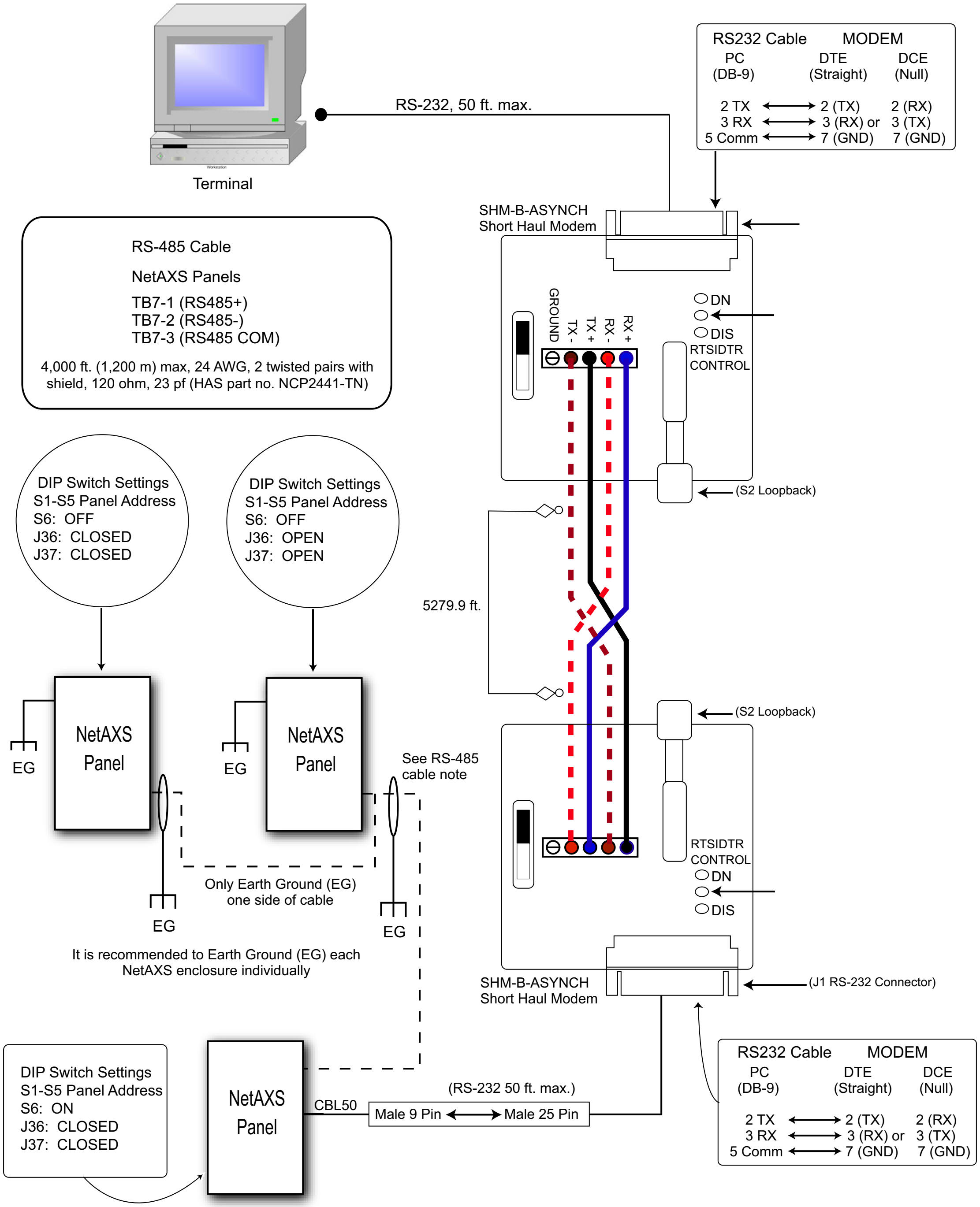
DIP Switch Settings
S1: ON
S2: ON
S3: ON
S4: ON
S5: ON
S6: OFF (Ack/Nak Enable)
S7: ON
S8: OFF)19,200 Baud Rate)

RS232 Cable	MODEM	
PC (DB-9)	DTE (Straight)	DCE (Null)
2 TX ⟷	2 (TX)	2 (RX)
3 RX ⟷	3 (RX) or	3 (TX)
5 Comm ⟷	7 (GND)	7 (GND)

5.8 RS-485 Short Haul Modem Connection via NetAXS

This connection supports 31 NetAXS Access Controller panels for each drop line. It has not been approved by UL.

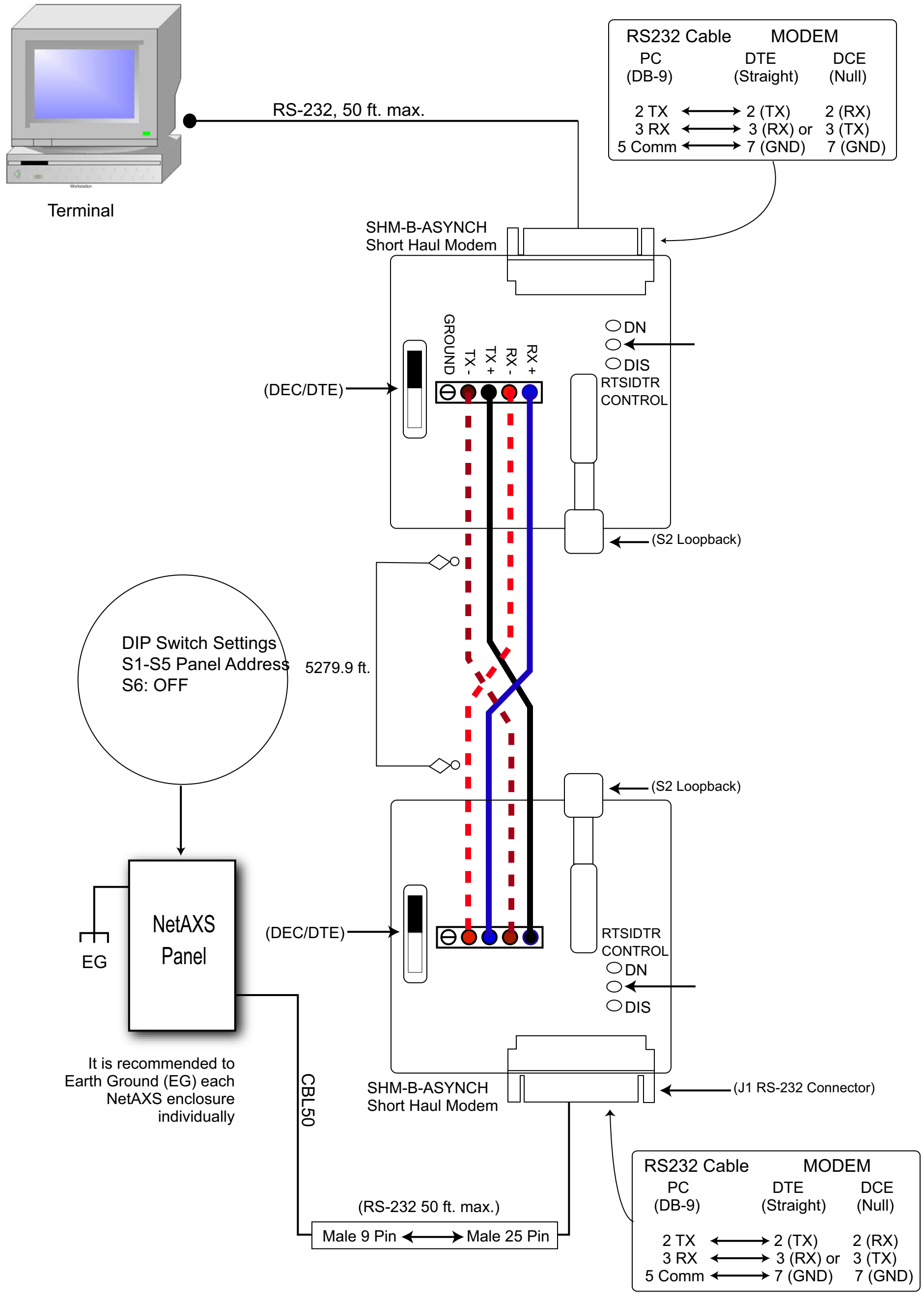
Figure 26: RS-485 Short Haul Modem Connection via NetAXS



5.9 RS-232 Short Haul Modem Connection

This connection supports one NetAXS Access Controller panel for each loop. It has not been approved by UL.

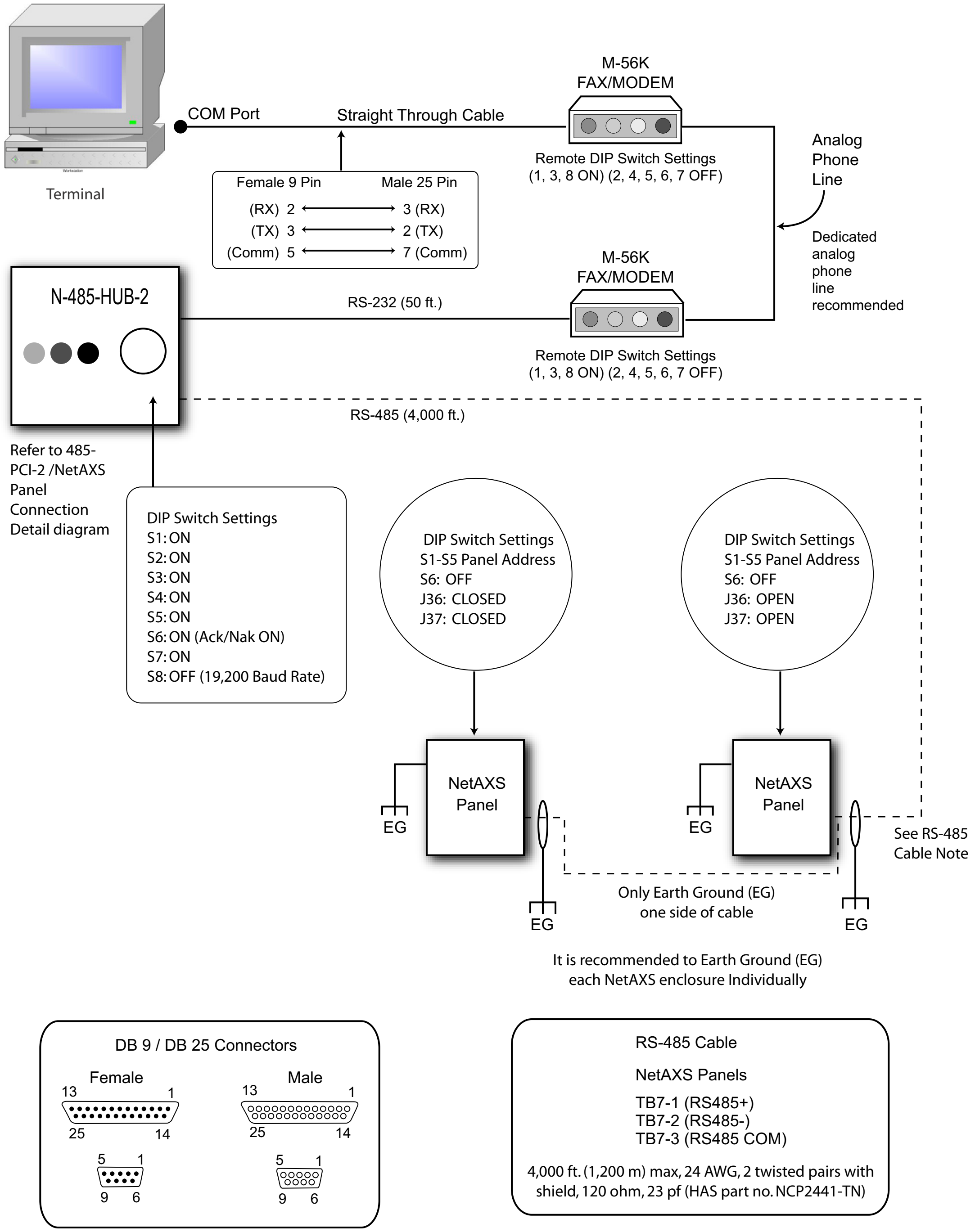
Figure 27: RS-232 Short Haul Modem Connection



5.10 M-56K Dial-up Modem, RS-485 Connection via Hub

This connection supports 31 NetAXS Access Controller panels for each drop line. It has not been approved by UL.

Figure 28: M-56K Dial-up Modem, RS-485 Connection via Hub



Remote DIP Switch Settings
(1, 3, 8 ON) (2, 4, 5, 6, 7 OFF)

Female 9 Pin	Male 25 Pin
(RX) 2	3 (RX)
(TX) 3	2 (TX)
(Comm) 5	7 (Comm)

Remote DIP Switch Settings
(1, 3, 8 ON) (2, 4, 5, 6, 7 OFF)

Refer to 485-PCI-2 /NetAXS Panel Connection Detail diagram

DIP Switch Settings
S1: ON
S2: ON
S3: ON
S4: ON
S5: ON
S6: ON (Ack/Nak ON)
S7: ON
S8: OFF (19,200 Baud Rate)

DIP Switch Settings
S1-S5 Panel Address
S6: OFF
J36: CLOSED
J37: CLOSED

DIP Switch Settings
S1-S5 Panel Address
S6: OFF
J36: OPEN
J37: OPEN

Only Earth Ground (EG)
one side of cable

It is recommended to Earth Ground (EG)
each NetAXS enclosure Individually

RS-485 Cable

NetAXS Panels

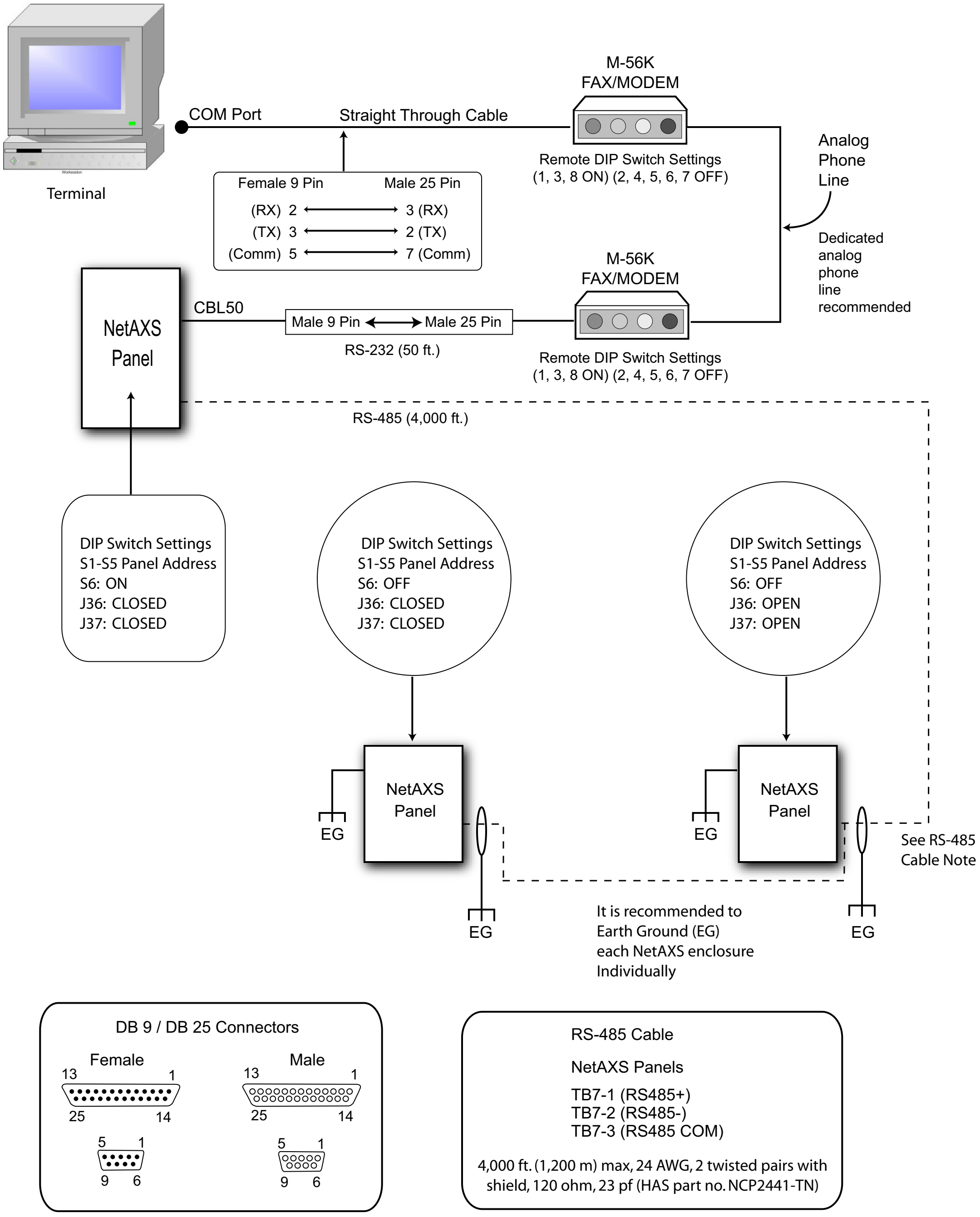
TB7-1 (RS485+)
TB7-2 (RS485-)
TB7-3 (RS485 COM)

4,000 ft. (1,200 m) max, 24 AWG, 2 twisted pairs with shield, 120 ohm, 23 pf (HAS part no. NCP2441-TN)

5.11 M-56K Dial-up Modem, RS-485 Connection via NetAXS

This connection supports 31 NetAXS Access Controller panels for each drop line. It has not been approved by UL.

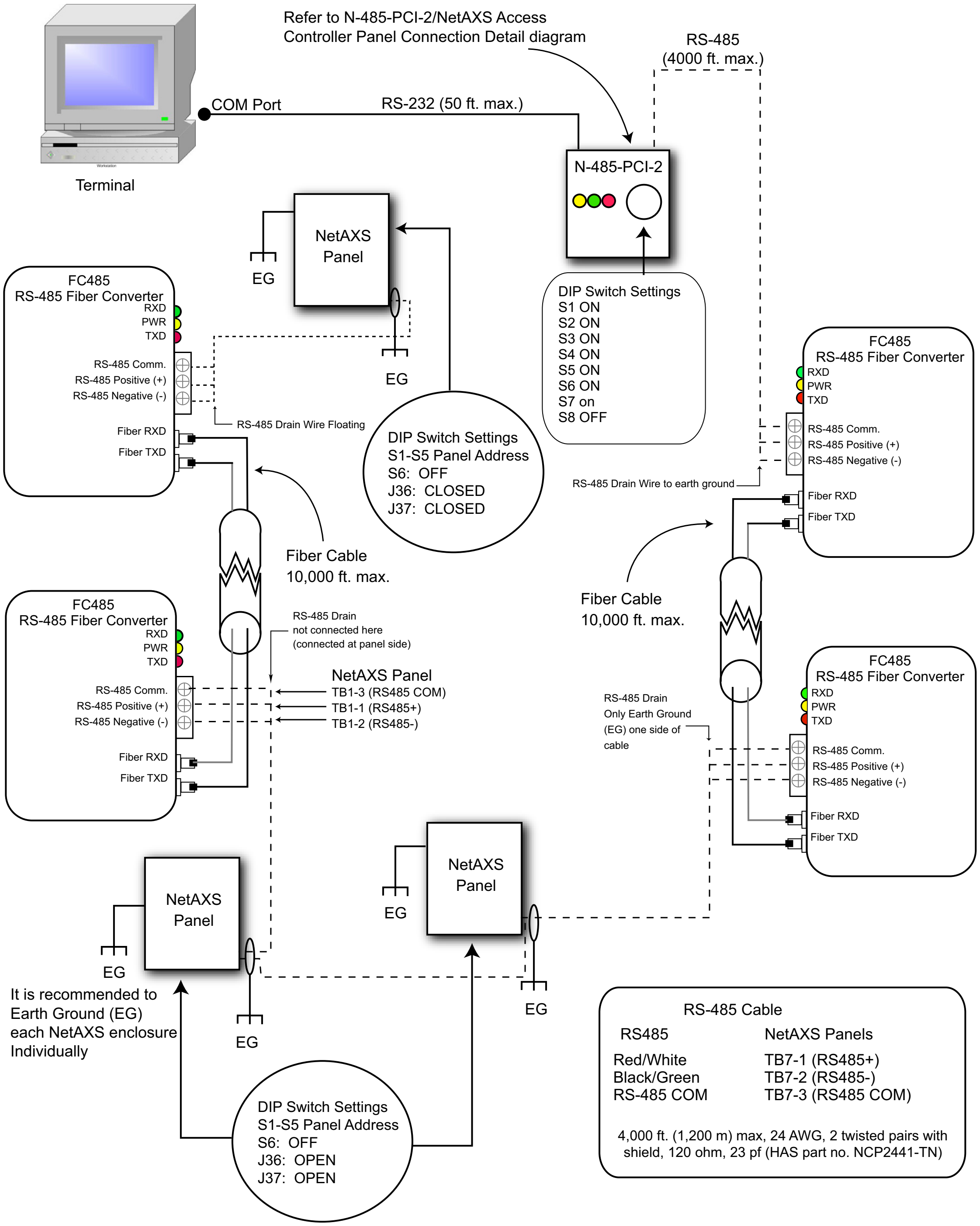
Figure 29: M-56K Dial-up Modem, RS-485 Connection via NetAXS



5.12 Fiber Converter to RS-485 Connection via PCI-2

This connection supports 31 NetAXS Access Controller panels for each drop line. It has not been approved by UL.

Figure 30: Fiber Converter to RS-485 Connection via PCI-2


Terminal
COM Port
RS-232 (50 ft. max.)
Refer to N-485-PCI-2/NetAXS Access Controller Panel Connection Detail diagram
RS-485 (4000 ft. max.)
N-485-PCI-2
NetAXS Panel
EG
FC485 RS-485 Fiber Converter
RXD
PWR
TXD
RS-485 Comm.
RS-485 Positive (+)
RS-485 Negative (-)
Fiber RXD
Fiber TXD
RS-485 Drain Wire Floating
RS-485 Drain Wire to earth ground
Fiber Cable 10,000 ft. max.
RS-485 Drain not connected here (connected at panel side)
NetAXS Panel
TB1-3 (RS485 COM)
TB1-1 (RS485+)
TB1-2 (RS485-)
RS-485 Drain Only Earth Ground (EG) one side of cable
It is recommended to Earth Ground (EG) each NetAXS enclosure Individually

DIP Switch Settings
S1 ON
S2 ON
S3 ON
S4 ON
S5 ON
S6 ON
S7 on
S8 OFF

DIP Switch Settings
S1-S5 Panel Address
S6: OFF
J36: CLOSED
J37: CLOSED

DIP Switch Settings
S1-S5 Panel Address
S6: OFF
J36: OPEN
J37: OPEN

RS-485 Cable

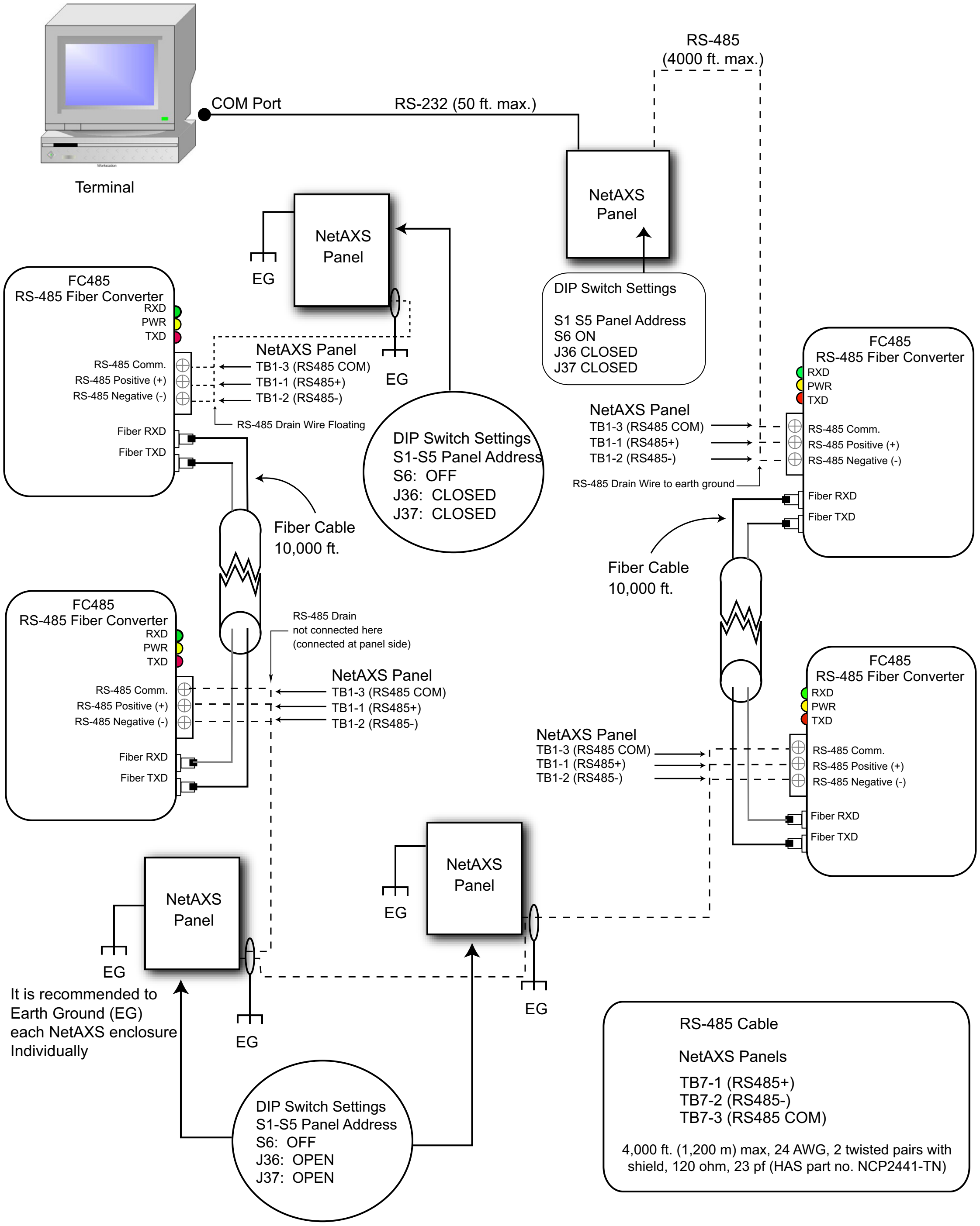
RS485	NetAXS Panels
Red/White	TB7-1 (RS485+)
Black/Green	TB7-2 (RS485-)
RS-485 COM	TB7-3 (RS485 COM)

4,000 ft. (1,200 m) max, 24 AWG, 2 twisted pairs with shield, 120 ohm, 23 pf (HAS part no. NCP2441-TN)

5.13 Fiber Converter to RS-485 Connection via NetAXS

This connection supports 31 NetAXS Access Controller panels for each drop line. It has not been approved by UL.

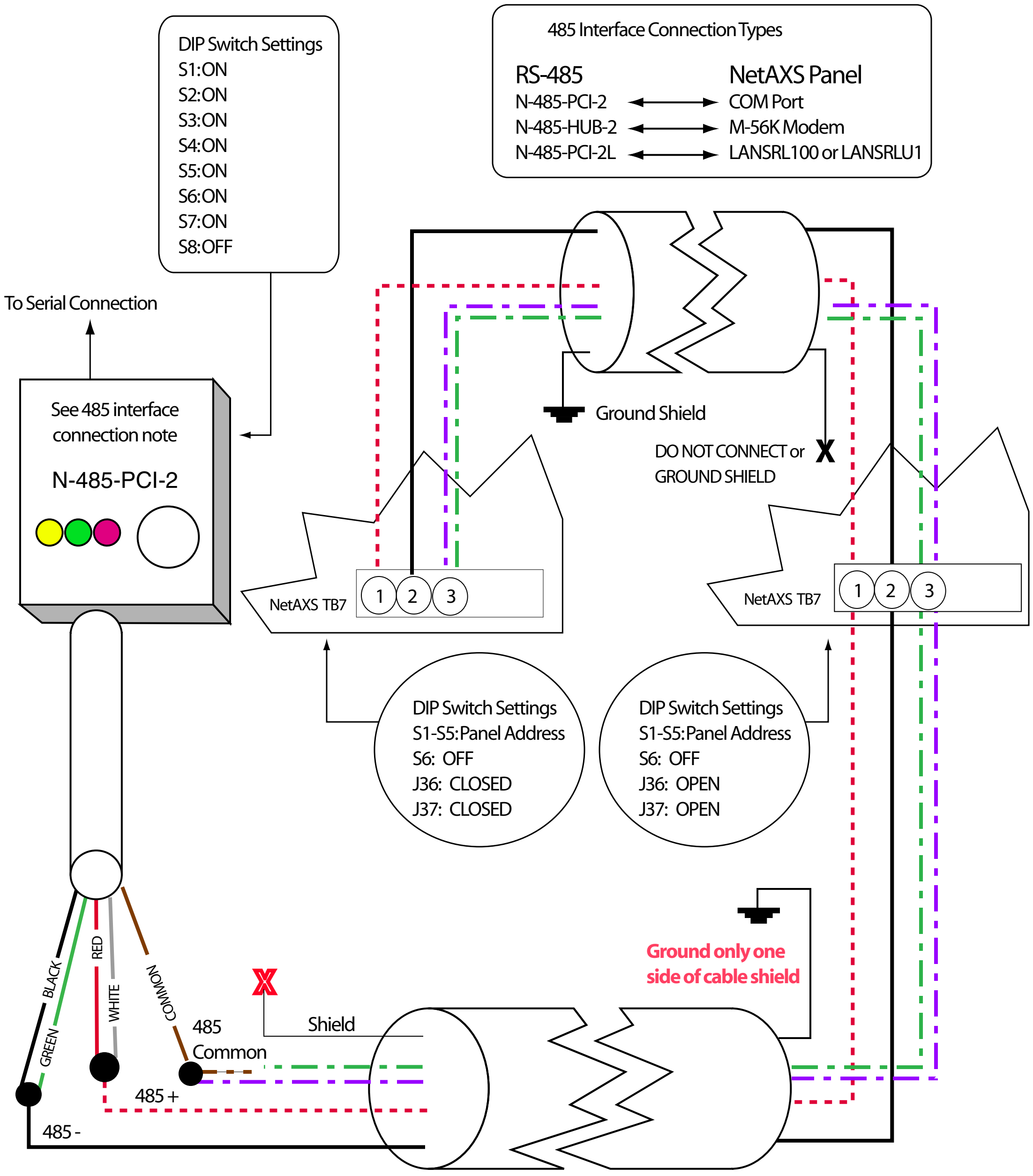
Figure 31: Fiber Converter to RS-485 Connection via NetAXS



5.14 N-485-PCI-2/NetAXS Access Controller Panel Connection Detail

This configuration has not been approved by UL.

Figure 32: N-485-PCI-2/NetAXS Access Controller Panel Connection Detail



485 Interface Connection Types

RS-485		NetAXS Panel
N-485-PCI-2	←→	COM Port
N-485-HUB-2	←→	M-56K Modem
N-485-PCI-2L	←→	LANSRL100 or LANSRLU1

DIP Switch Settings
S1:ON
S2:ON
S3:ON
S4:ON
S5:ON
S6:ON
S7:ON
S8:OFF

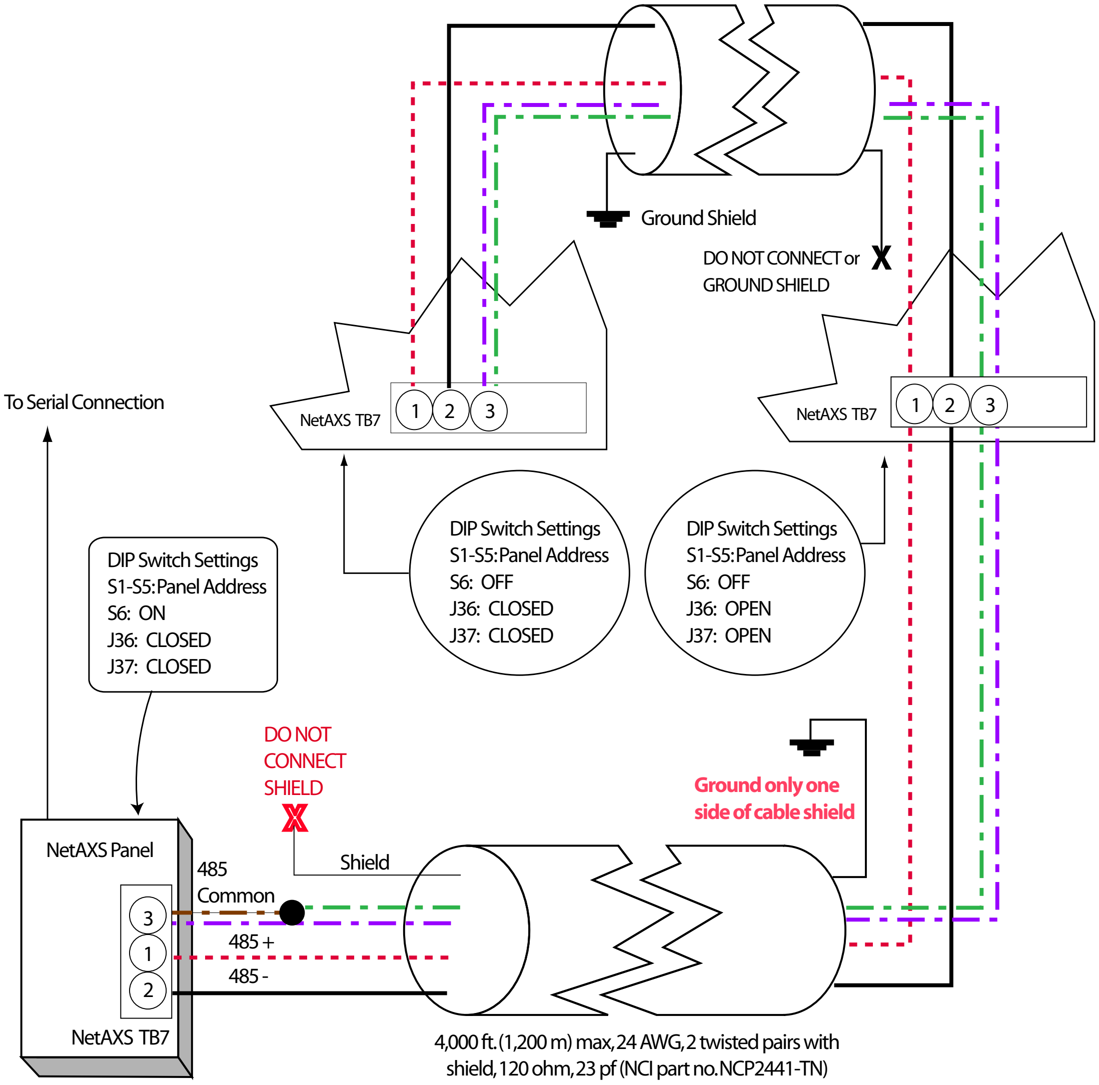
DIP Switch Settings
S1-S5:Panel Address
S6: OFF
J36: CLOSED
J37: CLOSED

DIP Switch Settings
S1-S5:Panel Address
S6: OFF
J36: OPEN
J37: OPEN

4,000 ft. (1,200 m) max, 24 AWG, 2 twisted pairs with shield, 120 ohm, 23 pf (HAS part no. NCP2441-TN)

5.15 NetAXS/NetAXS Access Controller Panel Connection Detail

Figure 33: NetAXS/NetAXS Access Controller Panel Connection Detail

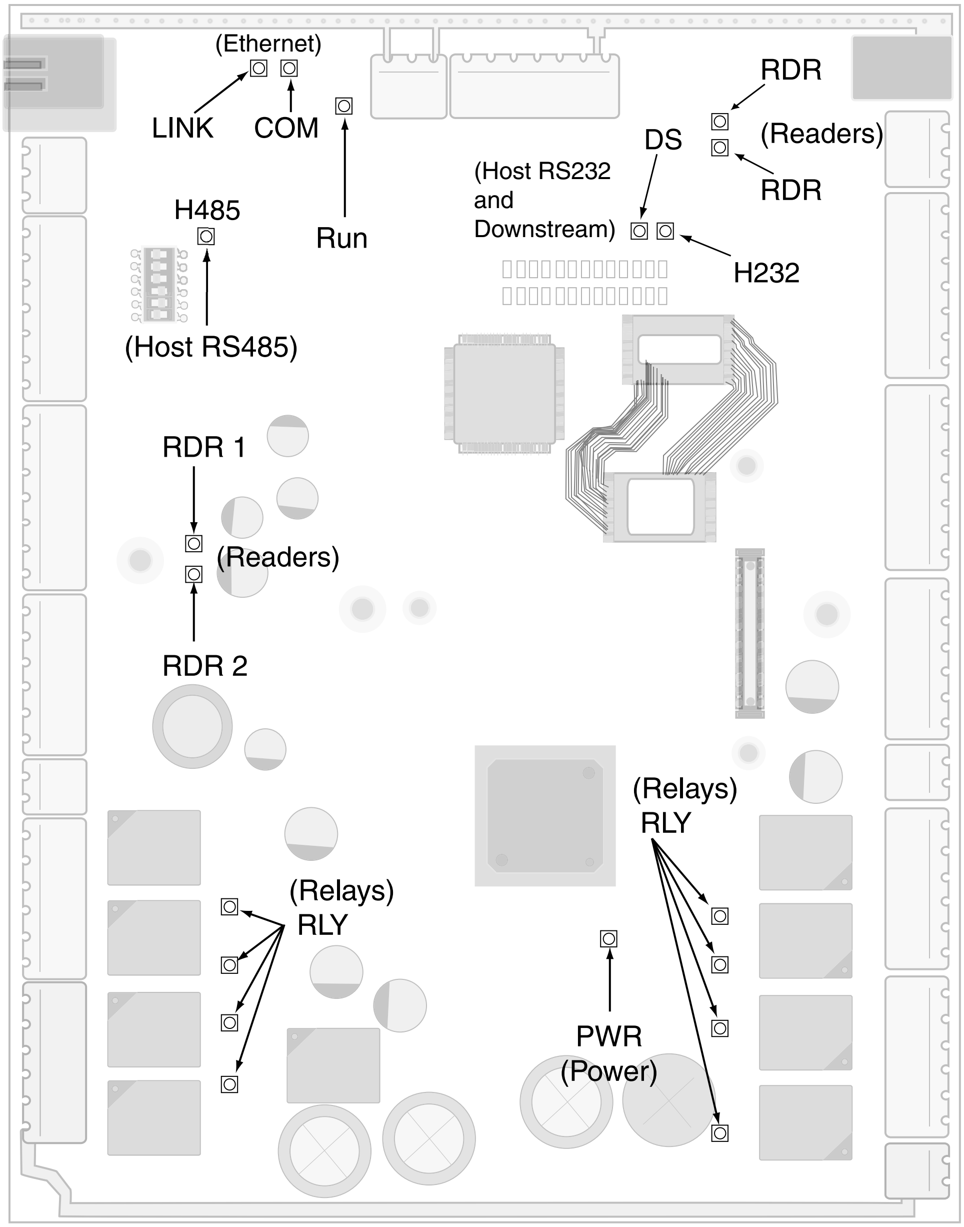


6.0 NetAXS Startup

6.1 LED Operation

When the panel wiring is complete, turn on the power. It might take a few minutes for the panel to complete the power-up sequence. When the board does initialize, verify that the appropriate LEDs identified in the following figure are in accord with the descriptions in Table 7 on page 59.

Figure 34: System, Relay and Power LEDs



The following table indicates the status associated with each LED.

Table 7 LED Status

LED	PWR	RUN	H485	H232	DS	COM	LINK	RLY	RDR
GREEN	Power OK	RUN Heart Beat	Multi-drop Receive Data	RS232 Receive Data	Down-stream Receive Data	100Mbit	Link OK	Relay Active	Flash at read
RED	N/A	N/A	Trans-mit Data	Trans-mit Data	Trans-mit Data	N/A	N/A	N/A	N/A
AMBER	N/A	N/A	TX & RX Data	TX & RX Data	TX & RX Data	N/A	TX & RX Data	N/A	N/A
OFF	Power Off	Mal-function	No Com	No Com	No Com	10Mbit	No Link	Relay Off	Normal

Note: The Ethernet/COM status LED will be green even if no cable is attached.

7.0 Hardware Specifications

7.1 Relay Contacts

Eight Form-C SPDT relays, 2 A @ 28 VDC (PTC limited).

7.2 Reader Interface

- Reader Power: 12 VDC nominal with 600 mA combined current between readers and AUX Power.
- Reader LED Output: Open collector driver capable of sinking up to 8 mA.
- Reader Tamper: Supervised or non-supervised input.
- Reader Data Input: TTL compatible inputs.
- Reader Buzzer Output (not supported with NetAXS-4): Open collector driver capable of sinking 8 mA at 15 VDC.

7.3 Maximum Output Loading

- Maximum current for any of the four reader outputs is 600 mA.
- Maximum current for any of the eight relay outputs on the HPACM8 is 2 A.
- Maximum battery charge current for the two batteries wired in series is 700 mA.
- Maximum combined current of the four reader outputs and the two auxiliary outputs is 600 mA.
- Maximum combined current of the two auxiliary outputs is 500 mA if no readers are being used.
- The HPACM8 total current including all outputs cannot exceed 2 A when powered by the internal NX4L1 power supply.

7.4 Common Connections

Common connections are all connected internally. They are not connected to the panel chassis.

7.5 Mechanical

- Enclosure Dimension: 17.7 in. (450 mm) W × 23.9 in. (607 mm) H × 3.54 in. (90 mm) D.
- Enclosure Weight:
  - With two batteries (including the door): 33.70 lb.
  - With one battery (including the door): 28.90 lb.
  - Without batteries (including the door): 24.25 lb.

7.6 Environment

- Temperature: 0°C to 49°C operating, –55°C to +85°C storage.
- Humidity: UL approved at 85%, non-condensing.

7.7 Communications and Wiring

Table 8 Communications and Wiring

Communication Type	Description	Maximum Panels	Maximum Distance: Feet (Meters)
Direct to COM Port			
CBL50, RS-232 Cable	9-pin to RJ-45	1	50 (15)
N-485-PCI-2	RS-485 9-pin to CPU	31	4,000 (1,220)
Modems			
M-9600-LA (LO)/ N-485-PCI-2	Lease-line Modem to RS-485	31	NA/4,000 (NA/122)
SHM-B-ASYNC/ N-485-PCI-2	Short-haul Modem to RS-485	31	5,280/4,000 (1,610/1,220)
SHM-B-ASYNC/CBL50	Short-haul Modem to RS-232	1	5,280/50 (1,610/15)
M-56K/N-485-HUB-2	Dial-up Modem to RS-485	31	NA/4,000 (NA/1,220)
Fiber			
FC485	Fiber converter to RS-485	31	10,000/4,000 (3,050/1,220)

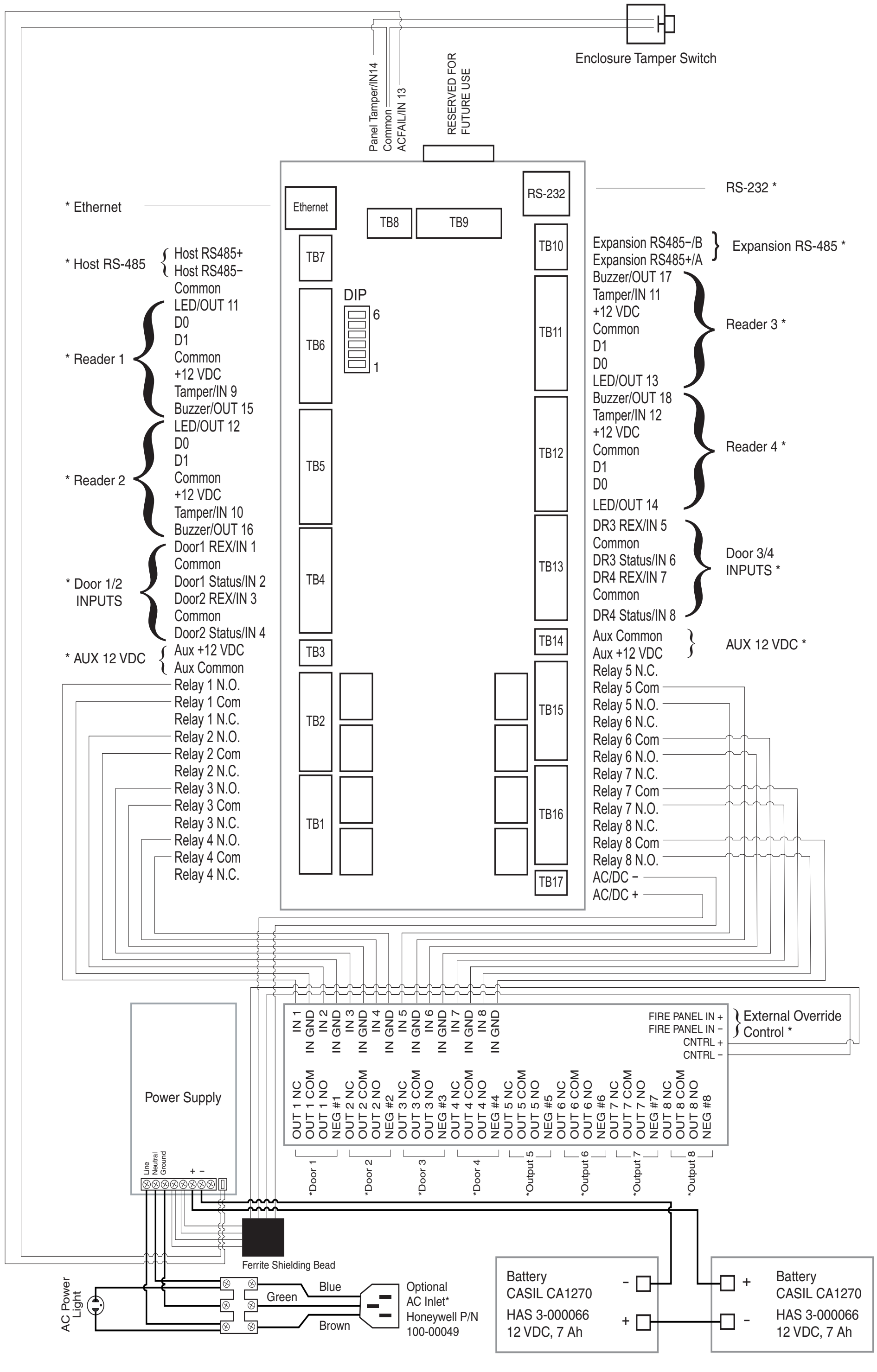
7.8 Reader Wiring

Table 9 Reader Wiring

Cable Specifications	Description	AWG	Maximum Distance: Feet (Meters)
Readers			
NC1861-BL	6 Conductor, Shielded	18	500 (153)
Alarm Input			
NC1821-GR	Twisted Pair, Shielded	18	2,000 (610)
Relay Outputs			
NC1821-GR	Twisted Pair, Shielded	18	2,000 (610)

7.9 NX4L1 Panel Wiring Diagram

Figure 35: NetAXS Panel Wiring Diagram



* Represents field wiring (Class 2 power-limited)

Note: Maintain at least 0.25-inches between the non-power-limited wiring (AC line voltage input wiring, 24 VDC wiring, battery backup/charger wiring, and battery-to-battery wiring) and all other wiring, which is power-limited Class 2 wiring.

8.0 Maintenance

Perform the following maintenance on the NetAXS enclosure:

- Change the lead-acid backup batteries (HAS part number 3-000066) every two to two-and-a-half years.

CAUTION Do not connect an uncharged battery to the panel.

- Oil the lock once per year
- The NX4L1 power supply contains no user replaceable parts. Do not remove or open the power supply cover.

WARNING Do not open or remove the power supply cover.

WARNING The NX4L1 power supply contains a non-replaceable input power line fuse. If this fuse opens, the power supply must be replaced.

- Use the following procedure to change the 4 A, 250 V, Bussmann type S500 or Littelfuse type 217 fuse in the power inlet terminal block.

WARNING Be sure to disconnect the AC power before removing the fuse holder from the power inlet terminal block.

WARNING To reduce the risk of fire, replace the fuse only with a 4 A, 250 V, Bussmann type S500 or Littelfuse type 217 fuse.

1. Disconnect the AC power.
2. Remove the fuse holder from the power inlet terminal block (see Figure 1 on page 17 to identify the location of the power inlet terminal block).
3. Replace the blown fuse in the lower section of the fuse holder with the new fuse. The upper section of the fuse holder provides a convenient location for a spare fuse.
4. Slide the fuse holder back into the power inlet terminal block.
5. Re-connect the AC power.

9.0 Troubleshooting

Table 10 Troubleshooting Problems and Solutions

Problem	Solution
The panel powers up, but it does not respond to any communication, cards reads, or input activation.	Ensure that the Address DIP switches are set to a value other than zero. Turn off the power (including battery), change the settings, and re-apply the power.
No communications exist with the Ethernet port.	Only a panel set to be a Gateway (DIP switch 6 = ON) will have communications on the Ethernet port. If you need to use that port to access the panel, turn off the power (including the battery), change the switch setting, and reapply the power. Note that if the panel is normally not a Gateway on a Multidrop communication bus, then the Host RS-485 connection (TB7) should also be disconnected while DIP switch 6 is ON. After completion of the Ethernet session, turn off the power (including the battery), change the switch setting, re-connect the Host RS-485 terminal block, and re-apply the power.
The IP address is incorrectly set to verify the value.	If you are connecting directly to a computer instead of going through a router or hub, use a cross-over Ethernet cable.
The N1000 panels on the Multidrop bus do not report.	N1000 panels will not communicate to a NetAXS panel that is configured as a Gateway. Replace all of the N1000 panels with NetAXS, or replace the Gateway panel with an N-485-PCI-2 device.
The BAD CRC counter is incrementing every minute.	Two or more panels on the Multidrop Bus have the same panel address. Verify that each panel has a unique address setting on DIP switch positions 1-5.
A drop line panel in standalone mode using RS-232 may unexpectedly fill its buffer.	The preferred solution is to configure the standalone panel through the web server as a Gateway and use the board PCI and AckNak communications. This also gives the user a more secure and reliable communications line. Another solution is to execute a new command that will allow the user to turn the Tesla flow control off: _U=<pn>_D (disable flow control) This prevents the panels from inadvertently filling their buffers. To turn the Tesla flow control back on: _U=<pn>_E (enable flow control)

Note: The NetAXS EOL network is AC-coupled. There is no resistance difference between the RS-485 positive and negative terminals if the EOL network is on or off (J36 and J37).

10.0 Technical Support

10.1 Normal Support Hours

Monday through Friday, 7:00 a.m. to 7:00 p.m. Central Standard Time (CST), except company holidays: 1-800-323-4576.

10.2 Web

For technical assistance, please visit http://www.honeywellaccess.com

NetAXS™ Standalone Operation A

1.0 Basic Standalone Operations

1.1 Card Read / Door Lock Operation

1. Present a card to a reader.
2. The reader sends the card number to a reader input on the panel.
3. The panel searches its database and:
    - If it is a valid card, then energize the door relay associated with the particular reader input. The card is valid when it is in the card database on the panel and the current time and date conforms to the time zone associated with the card.
    - If it is not a valid card, the door relay remains locked.

1.2 Door Egress / Door Lock / Door Status Operation

1. Activate the door egress input.
2. The panel energizes the door relay associated with the particular door egress input for a default time of 10 seconds.
3. If the door status goes from close to open to close again during the 10 second door open period, the door relay will be immediately de-energized.

2.0 Standalone Settings

2.1 NetAXS Panel Hardware Settings

- Configure the system with an RS-232 connection according to Figure 22 on page 46.
- Set DIP switches 1 through 5 to define the panel number (see Table 5 on page 38). Panel number 0 is not valid.
- Set DIP switch 6 to the OFF position to place the panel into the Multidrop mode.
- Use a personal computer's serial communications port (COM1 or COM2) and a terminal emulation program to configure the NetAXS™ panel for normal operation.

2.2 Communication Settings

- Baud Rate: 115200
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

2.3 Emulation Settings

- Echo typed characters locally: YES
- Line Delay: 500 milliseconds

2.4 Verifying Communications

1. Press the spacebar.
2. Press the carriage return <CR>. "S?" appear for every online panel and indicates proper communication between the terminal and panel.

3.0 Standalone Commands

CAUTION Use the following commands, in the order they are listed, to configure the NetAXS™ panel.

1. T command: Sets the panel's time
2. D command: Sets the panel's date
3. L command: Creates time zones for use by the cards
4. C command: Adds or deletes cards from the panel
5. W command: Program each input for either NO/NC and supervised or non-supervised operation
6. P command: Sets interlocks between input points and/or output points

Note: In all examples, the underscore character "_" indicates a space and <CR> indicates a carriage return.

3.1 T (Time) Command

```
_T=pn_hh:mm<CR>
```

Variables:

pn = panel number (1–31)
hh = hours (0–23) (Military time)
mm = minutes (00–59)

Example 1

```
_T=1_08:30<CR>
```

This command would set panel 1 to a time of 8:30 AM.

Example 2

```
_T=6_18:15<CR>
```

This command would set panel 6 to a time of 6:15 PM.

3.2 D (Date) Command

```
_D=pn_mm/dd/yyyy_day<CR>
```

Variables:

pn = panel number (1–31)
mm = month number (1–12)
dd = day number (1–31)
yyyy = year number (e.g., 2007, 1999, etc.)
day = day of week (1–7):

1 = Monday
2 = Tuesday
3 = Wednesday
4 = Thursday
5 = Friday
6 = Saturday
7 = Sunday

Note: The day of week setting is a hold-over from an old command. The panel using the mm/dd/yyyy information will automatically configure panel to the correct day of the week, regardless of the setting selected in day of week. But the command still requires a value to be entered in its place of 1–7.

Example 1

```
_D=1_01/09/2007_5<CR>
```

This command would set panel 1 to a date of 1/9/2007 and to Tuesday as the day of the week.

Example 2

```
_D=25_12/14/2009_7<CR>
```

This command would set panel 25 to a date of 12/14/2009 with a day of week being Monday.

3.3 L (Time Zone) Command

```
_L=pn_tz_h1:m1-h2:m2_days<CR>
```

Variables:

pn = panel number (1–31)
tz = time zone number (1–255)
h1 = start time zone: hours (00–23) (Military time)
m1 = start time zone: minutes (00–59)
h2 = end time zone: hours (00–23) (Military time)
m2 = end time zone: minutes (00–59)
days = days of week valid values as listed below:

1 = Monday
2 = Tuesday
3 = Wednesday
4 = Thursday
5 = Friday
6 = Saturday
7 = Sunday
0 = Holiday 1
8 = Holiday 2
9 = Holiday 3

Note: 00:00 is the earliest time possible and 23:59 is the latest time possible. A single time zone cannot be made to span midnight, through the use of extended commands we can simulate this. For more information, please seek the guidance of technical support.

Example 1

```
_L=5_10_08:00-17:00_1_2_3_4_5<CR>
```

This command would configure panel 5 to add a time zone entry to time zone number 10 ranging from 8AM to 5PM and would be valid during Monday, Tuesday, Wednesday, Thursday, and Friday.

Example 2

```
_L=25_45_16:00-23:59_0_6_7_8_9<CR>
```

This command would configure panel 25 to add a time zone entry to time zone number 45 ranging from 4PM to 11:59PM and would be valid during Saturday, Sunday, Holiday, 1, 2, and 3.

3.4 C (Card Add) Command

```
_C=pn_code_time zone_dev<CR>
```

Variables:

pn = panel number (1–31)
code = card number (range depends on card format)
time zone = time zone number the card will follow (1–255)
dev = device numbers card will work with, see below:

1 = card reader #1
2 = card reader #2
3 = card reader #3
4 = card reader #4

Example 1

```
_C=6_12345_10_1_2_3_4<CR>
```

This command would configure panel 6 to add a card entry of 12345 to the panels database, that will be valid on reader 1, 2, 3, and 4 during the times and days specified by time zone 10.

Example 2

```
_C=18_52989_120_1_3<CR>
```

This command would configure panel 18 to add a card entry of 52989 to the panels database, that will be valid on reader 1 and 3 during the times and days specified by time zone 120.

3.5 C (Card Delete) Command

```
_C=pn_code<CR>
```

Variables:

pn = panel number (1–31)
code = card number (range depends on card format)

Example 1

```
_C=6_12345<CR>
```

This command would remove card 12345 from panel 6.

Example 2

```
_C=18_52989<CR>
```

This command would remove card 52989 from panel 18.

3.6 W (Input) Command

```
_W=pn_input_{SO|SC|NO|NC}<CR>
```

Variables:

SO: Supervised normally open
SC: Supervised normally closed
NO: Non-supervised normally open
NC: Non-supervised normally closed (default)

Example

_W=1_9_SO<CR>

Input 9 has been programmed as supervised, normally open on panel 1.

3.7 P (Interlock) Command

```
_P=pn_I/O_[number]_I/O[number]_{D|E|F|N|P}_
{D|E|F|N|P}<CR>
```

Parameters:

number: for an input number, the range is 1–96; for output, 0–78
D: De-energize
E: Energize
F: Follow
N: No action
P: Pulse

Example

```
_P=1_I_5_O_3_E_D
```

When Input 5 is triggered, Output 3 energizes.

When Input 5 returns to its normal state, Output 3 de-energizes.

3.8 Flow Control Disable/Enable Command

(Use this command only for a drop line panel using RS-232 in standalone mode)

_U=[panel name]_{D|E}

Parameters:

D: Disable
E: Enable

Example

```
_U=30_D
```

This disables the flow control on panel 30 and prevents the panel's buffers from filling. After a hard reset of the panel, the flow control is re-enabled.

4.0 NetAXS Panel Defaults

4.1 Reader Ports

The panel accepts a Wiegand serial data packet from the card reader. If the card is in the database, the associated relay is activated. If the card is not in the database, the relay state is unchanged.

The following are the default reader port to relay associations:

Reader Number	Controls...
1	Relay 1 (Output 1)
2	Relay 2 (Output 2)
3	Relay 3 (Output 3)
4	Relay 4 (Output 4)

4.2 Reader LED Outputs

The Reader LED output defaults to toggle the card reader LED from Red to Green for two seconds when a valid card is presented. No LED color change (other then a possible momentary change depending on reader used) occurs if the card is not in the database.

The following are the default reader LED port to output associations:

Reader LED	Controls...
Reader 1	Output 11
Reader 2	Output 12
Reader 3	Output 13
Reader 4	Output 14

4.3 Reader Tamper Inputs

The card readers have a Tamper signal wired to the NetAXS™ panel. This is a two-state input configured as a Normally Closed contact.

The following are the default Reader Tamper Input to Panel Input associations:

Tamper LED	Reports as...
Tamper 1	Input 9
Tamper 2	Input 10
Tamper 3	Input 11
Tamper 4	Input 12

4.4 Door Egress Inputs

The panel has a Request-To-Exit (egress) input for each door. The default condition is a two-state input configured as Normally Closed contact. When the egress input is active, the associated output relay will be active.

The following are the default egress input associations:

Egress input	Controls relay...	Panel input	Reports as...
1	1	SP1	Input 1
2	2	SP3	Input 3
3	3	SP5	Input 5
4	4	SP7	Input 7

4.5 Door Status Inputs

The panel has a Door Status input for each door. The default condition is a two-state input configured as a Normally Closed contact.

The following are the default door status input associations:

Door Status input	Panel input	Reports as...
1	SP2	Input 2
1	SP4	Input 4
1	SP6	Input 6
1	SP8	Input 8

4.6 ACFAIL and Panel Tamper Inputs

The panel has the following two additional generic inputs that can be used as generic inputs or as either External Power Fail or Enclosure Tamper inputs. The default condition is a two-state input configured as Normally Closed. Input 14 is a special case, since it reports in as two inputs (inputs 14 and 20). Input 14 can be used as a generic input, but input 20 is used for the Enclosure Tamper alarm. An active External Power Fail input indicates that the system is operating from the battery current, not from the primary input power. An inactive External Power Fail input indicates that the system is operating from the primary input power.

Generic input	Panel input	Reports as...
Generic/External Power Fail	SP9	Input 13
Generic/Enclosure Tamper	SP10	Inputs 14 and 20

4.7 Additional Generic Outputs

The panel has the following four additional generic form C relay outputs that can be programmed using the P command:

Relay output	Controls...
5	Output 5
6	Output 6
7	Output 7
8	Output 8

Recommended Wiring for NetAXS-4/NetAXS-123 Loops

B

1.0 Overview

This document provides the recommended RS-485 wiring for NetAXS-4 and mixed loop configurations.

The downstream controller boards communicate to the gateway controller board through an RS-485 interface. The interface allows for multidrop communication of up to 4,000 feet (1,200 m) total per port. Use two twisted pair (minimum 24 AWG) with shield, 120 ohm, 23 pf for communication. The default speed of this port is 38.4 Kbps but it can be upgraded to 115.2 Kbps.

The 485+ (A) is the positive side of the transmit and receive differential signal, the 485– (B) is the negative side. The COM or common is the signal ground. The RS-485 COM signal is connected on the NetAXS controller but not on the NetAXS-123 controllers.

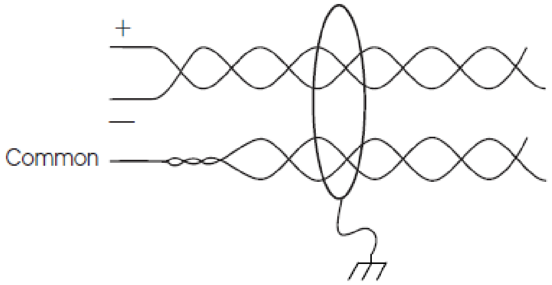
Note: This signal (RS-485 COM) must **NOT** be connected to chassis GND.

When daisy-chaining 485 ports together connect the 485+ (A) wires from the upstream and downstream boards to the 485+ (A) terminal and likewise, connect the 485– (B) wires from the upstream and downstream boards to the 485– (B) terminal. Using twisted pair for RS-485 communication wiring, use the first pair as your data pair, observing polarity. Twist the second pair together and use as the common.

See Figure B-1 on page 79 for reference.

Note: The common is not used on NetAXS-123 controllers. Connect the external drain shield to the appropriate earth ground on **one** end.

Figure B-1:   Twisted Pair



2.0 The Shield Wire

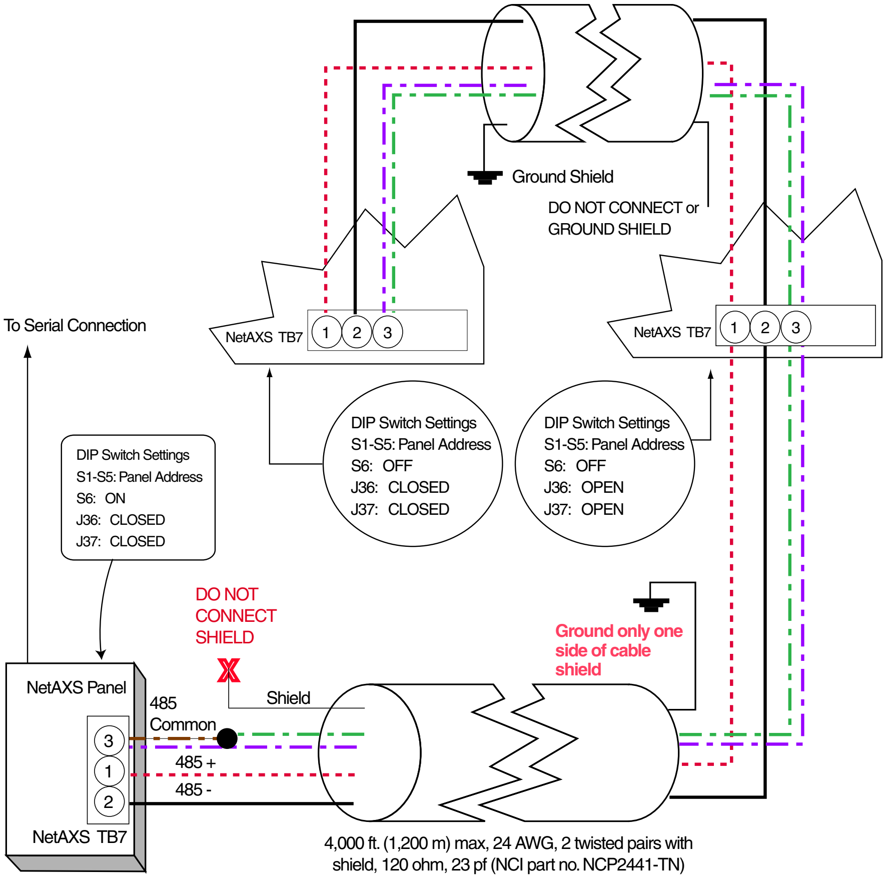
This shield can be used as normal in both the NetAXS-4 and NetAXS-123. If the environment is not electrically noisy, the shield can be left off. But in electrically noisy environments, the shield can be used grounding only one (1) end of the cable shield to prevent ground loops.

3.0 RS-485 Wiring for NetAXS-4 Loop

- The 485+ (A) of one controller is connected to 485+ (A) of the next controller using one wire of the first twisted pair.
- The 485– (B) of one controller is connected to 485– (B) of the next controller using the other wire of the first twisted pair.
- On a loop that contains all NetAXS-4 controllers, the 485 COM is connected. The second pair of the wires are twisted together and connected to 485 COM on the controller.
- The shield is only connected on one end of the cable, not both.

See Figure B-2 on page 81.

Figure B-2: RS-485 Wiring for NetAXS-4 Loop

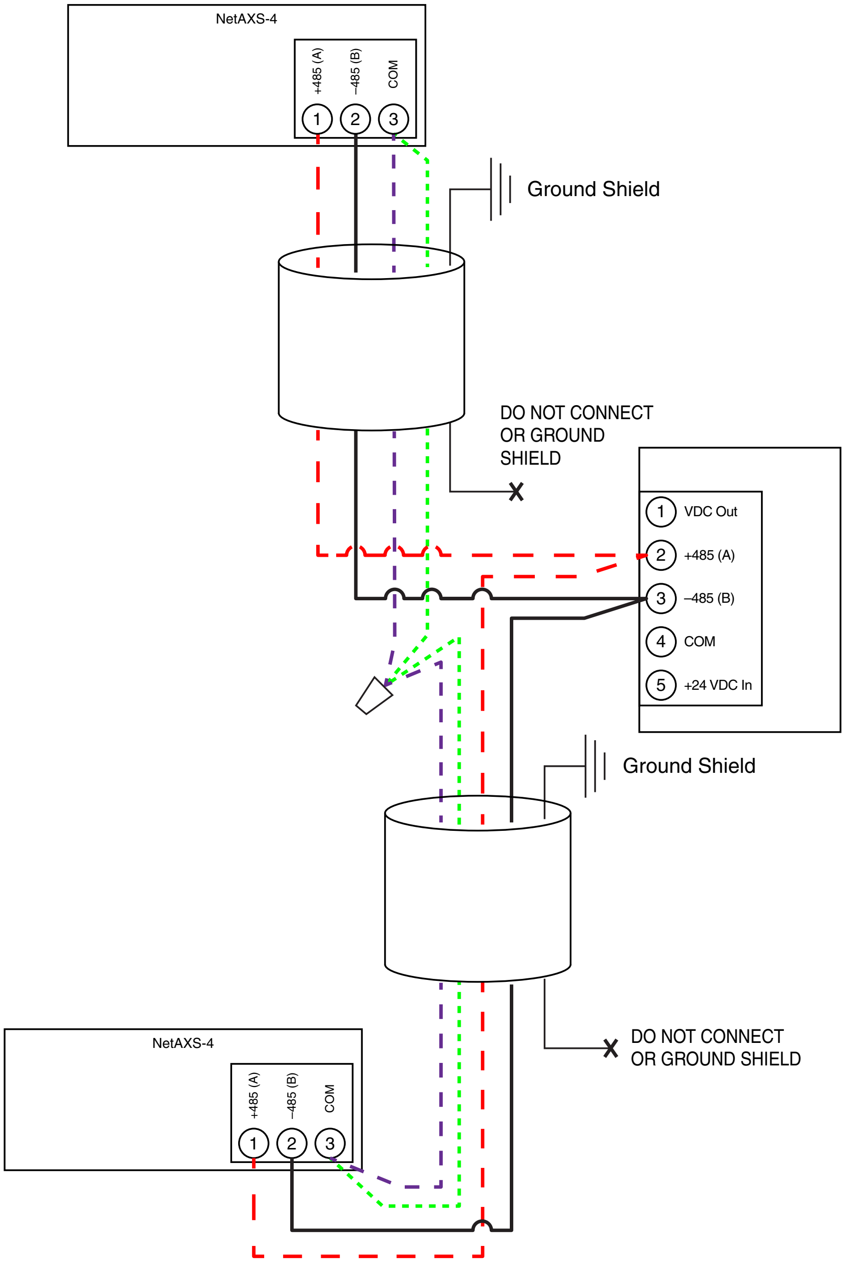


4.0 RS-485 Wiring for a Mixed Loop

- The 485+ (A) of one controller is connected to 485+ (A) of the next controller using one wire of the first twisted pair.
- The 485– (B) of one controller is connected to 485– (B) of the next controller using the other wire of the first twisted pair.
- On a loop that contains both NetAXS-123 and NetAXS panels (mixed loop), the second pair of the wires are twisted together and connected to the RS-485 COM on the next NetAXS-4 controller to the RS-485 COM of the next NetAXS-4 controller in the loop.
- Do not connect the RS-485 COM on the NetAXS-123 controllers. The RS-485 COM is bypassed on the NetAXS-123 controller.
- The shield is only connected on one end of the cable, not both.

See Figure B-3 on page 82.

Figure B-3: RS-485 Wiring for a Mixed Loop



Using twisted pair, the first pair (usually red and black wires) is connected to 485+ and 485– respectively. The second pair (usually green and white) are twisted together and connected to COM with the exception of the NetAXS-123 controller where the common is bypassed.

Note: In the above figure, the white wire is colored purple for easy viewing.

5.0 End of Line Termination

By default, the controllers are not terminated. If the controller is the last one on the 485 bus then it should be terminated. For more information, see the controller's installation guide.

- **NetAXS-123**: Place SW1 DIP switches 8 and 9 to the ON position to terminate.
- **NetAXIS**: Place jumpers across J36 and J37 to terminate.

Honeywell Access Systems
135 W. Forest Hill Avenue, Oak Creek, WI 53154
1-800-323-4576
www.honeywellaccess.com

Honeywell

NetAXS®

Access Control Unit User's Guide

If this panel is to be added to an existing loop, then all panels need to be upgraded. Please see www.honeywellaccess.com.

Document 800-04410V2, Revision A

Ordering Information

Please contact your local Honeywell representative or visit us on the web at www.honeywellaccess.com for information about ordering.

Feedback

Honeywell appreciates your comments about this manual. Please visit us on the web at www.honeywellaccess.com to post your comments.

CONTENTS

What's New in This Release

NetAXS® Access Control Unit User's Guide

Upgrading NetAXS® Firmware

LIST OF FIGURES

LIST OF TABLES

What’s New in This Release

Database import/export file password protected

Database file may be exported from the File Management screen in the Upload (from panel) section. The specific database files are: Cards and Common Configuraion, Cards, Common and Panel Configuration, and Panel Configuraion. These files should be encrypted, and when exporting a database file, a password will be required.

When import a database file, a password shall be validated if the import occurred on gateway panel that is not the same one used to export. No password is required if using the same gateway that created database, or if the imported database file was created from R3.4 or R3.5

Web events can be filtered by separate event types

Web events now can be filtered by separate event types. There are 8 web event types: Login, Logout, Unknown User, Bad Database Read, Disabled Account, Invalid Password Locked Account, Bad Database Write. After upgrading from R3.4 or R3.5, existing web events shall be split into the individual types.

Create SSL certificate request and import certificate

Ability to create SSL certificate request and import a certificate from a trusted Certificate Authority has been added. The panel is installed with a Panel Self Signed Certificate by default. The user can install a User Certificate by generatiing a SSL certificate request and then importing the SSL certificate from a Certificate Authority.

After a CSR (Certificate Signing Request) is generated, send the CSR to a trusted Certificate Authority. Then install this certificate from the CA (Certificate Authority). The panels certificate will change from Panel Self Signed Certificate to User Certificate. Both CSR and the certificate shall be preserved after a factory default of the panel; the certificate can be reactivated.

NetAXS® Access Control Unit User's Guide

1.0 Connecting to the Web Server

1.1 Overview

NetAXS® has an embedded web interface. This interface provides a means to configure, program, monitor one or more NetAXS® panels as a stand-alone access control system with no need for software to be installed on a separate computer. This stand-alone system can also be configured for use with a host based software. Host based system can provide additional feature and system wide enhancements such as photo ID badging, intrusion and video integration. Each access control unit, or panel, has four reader ports. See the *NetAXS® NX4L1 Installation Guide*, *NetAXS® NX4S1 Installation Guide*, or *NetAXS® NX4S2 Installation Guide* to view illustrations of the supported NetAXS® system configurations.

You can communicate with the NetAXS® access control unit either through a host software system or by connecting to the NetAXS® web server by an Ethernet connection. This section describes how to connect to the NetAXS® web server. Section 2.0 describes how to use the NetAXS® web interface after you are connected to the NetAXS® panel through the NetAXS® web server. Section 3.0 describes how to use the web server interface.

1.2 Connecting to the Web Server

This section describes how to connect a computer to the NetAXS® web server via Ethernet and Internet Explorer.

Notes:

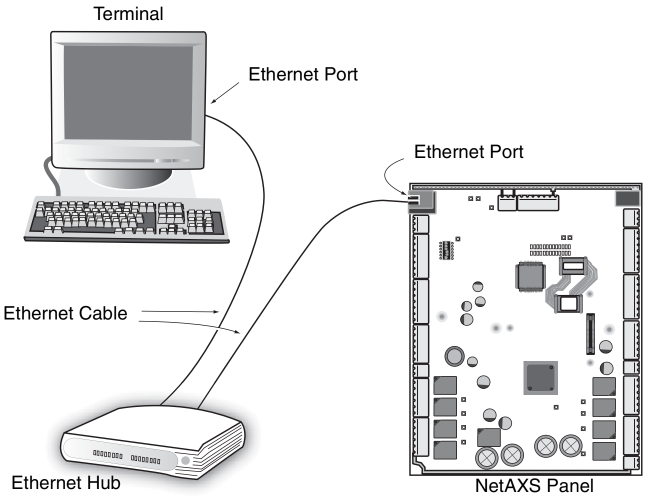
- The NetAXS® panel that you are connecting to the computer is the Gateway panel. DIP switch 6 on a Gateway panel must be set to ON for a successful connection.
- The Microsoft Windows™ screen captures used in this section reflect the Windows 7™ platform. If you are using another Windows™ platform, the screens will be somewhat different.

Perform the following steps:

1. Connect your computer's Ethernet port and the NetAXS® panel's Ethernet Port by using either of two methods:

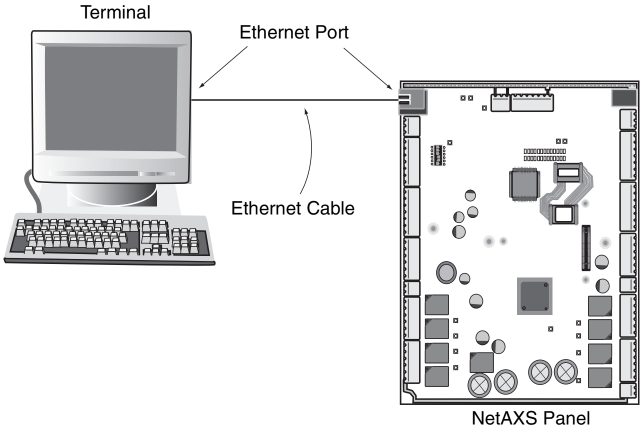
    a. Connect both the computer's Ethernet port and the NetAXS® panels Ethernet port to an Ethernet hub with standard Ethernet patch cables.

Figure 1: *NetAXS® Web Server Hub Connection*



    b. Connect the computer's Ethernet port directly to the NetAXS® panel's Ethernet port with an Ethernet cable.

Figure 2: NetAXS® Web Server Direct Connection

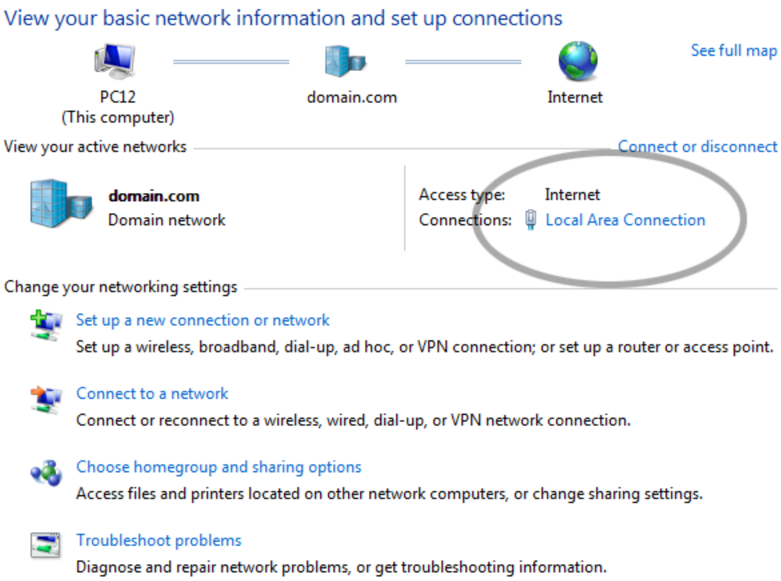


2. Configure the computer’s network connection:

   a. Select **Start > Control Panel**.

   b. Click **Network and Sharing Center**.

   c. Identify your local Ethernet connection, commonly labeled **Local Area Connection**.



View your basic network information and set up connections

View your active networks

domain.com
Domain network

Access type: Internet
Connections: Local Area Connection

Change your networking settings

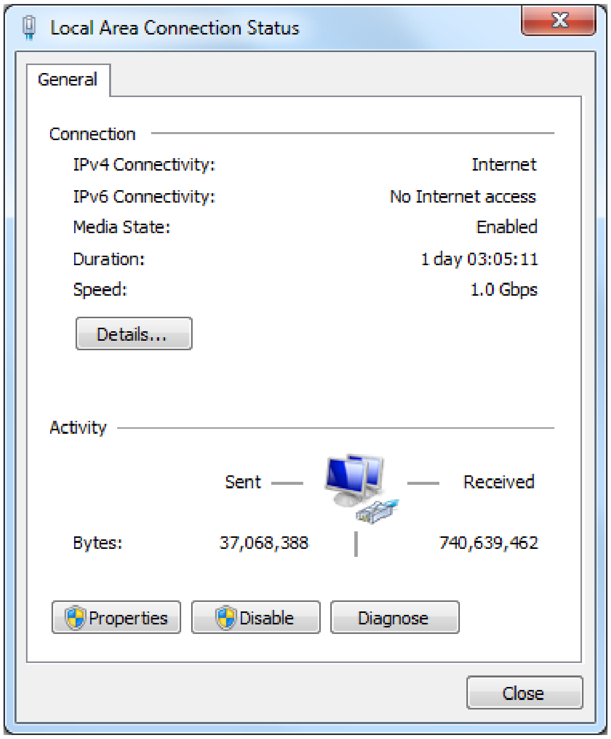
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

d. Click the link to display the Local Area Connection Status screen.



Local Area Connection Status

General

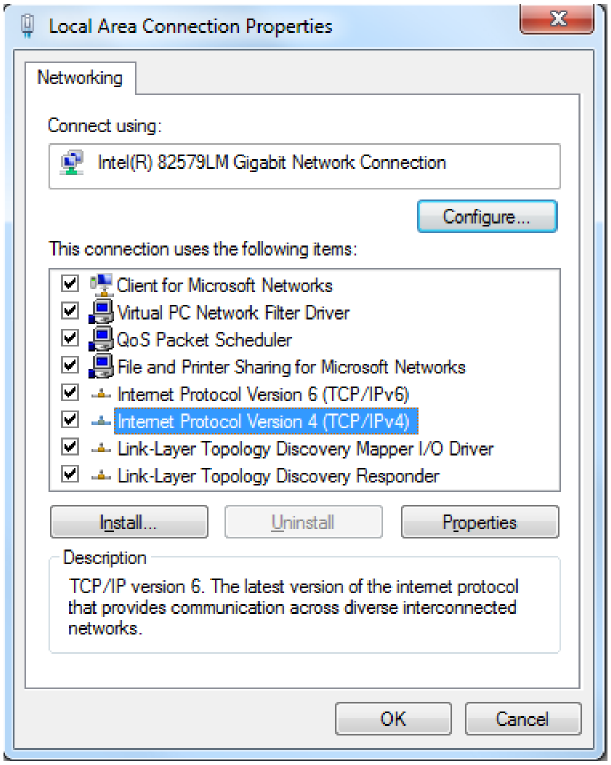
Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No Internet access
Media State:	Enabled
Duration:	1 day 03:05:11
Speed:	1.0 Gbps

Activity

	Sent	Received
Bytes:	37,068,388	740,639,462

e. Click **Properties** to display the Local Area Connection Properties screen.



Local Area Connection Properties

Networking

Connect using:

Intel(R) 82579LM Gigabit Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Virtual PC Network Filter Driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

f. Highlight the Internet Protocol Version 4 (TCP/IP) connection.

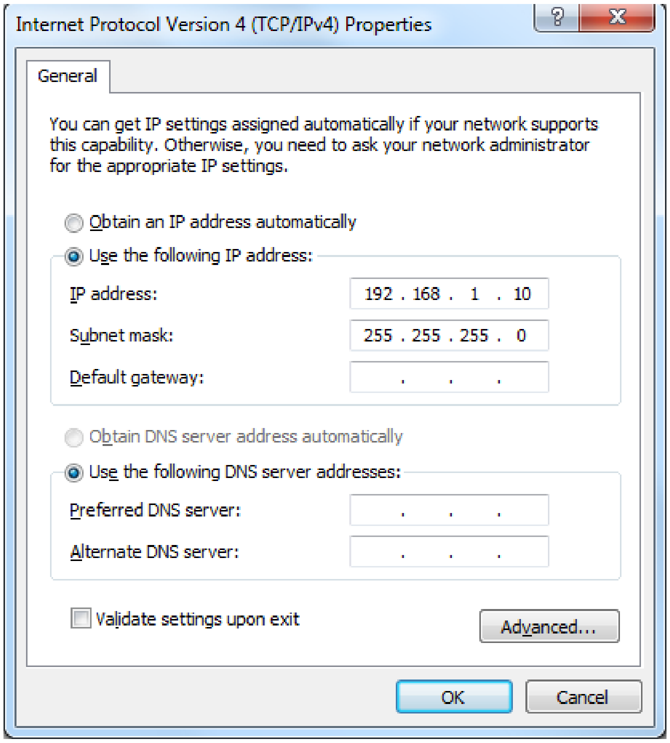
g. Click **Properties** to display your system's current Internet Protocol properties.

h. **Important:** Keep a record of your computer's current network configuration as it appears in this screen. You will need to re-instate this configuration later.

i. Select "Use the following IP address."

j. Enter "192.168.1.10" in the IP address field.

k. Enter "255.255.255.0" in the Subnet mask field.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

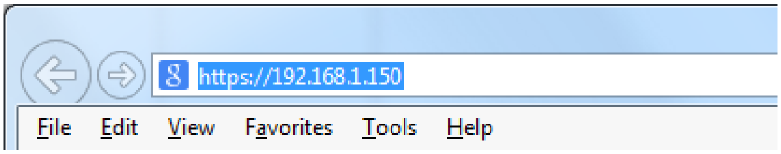
○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

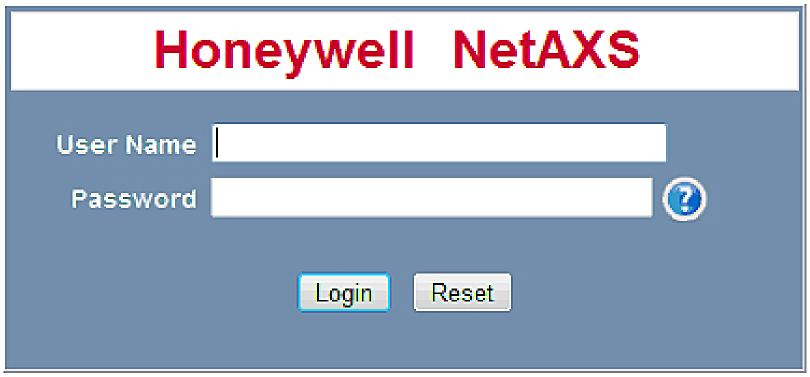
l. Click **OK** to accept the entries.

3. Open your browser (Internet Explorer shown below), and enter https://192.168.1.150 as the target address.



https://192.168.1.150

4. Press the **Enter** key to display the Honeywell NetAXS® login screen.



Note: If you are using Internet Explorer on windows, and you receive a certificate error message, follow these steps to login:

a. Enter the IP Address of the panel into the URL box.

b. Click **Continue to the website (not recommended)** to display the login screen.

Note: See the SSL section to request a certificate in SSL Certificate Management, page 68 .

5. Enter "admin" in the User Name field, and enter "admin" in the Password field. Both the user name and password are case-sensitive.

Note: 1. These steps were captured using Windows Internet Explorer, if using a different version of Windows and/or web browser, the steps maybe different.
2. You will be asked to change your password to a new password at this time. To do this, proceed to the instructions in Configuring Users , page 64 .

6. Click **Login** to display the NetAXS® main window. Note that the Select Panel column on the right edge of the screen displays all panels available to the computer. This list will include the gateway panel that you are connected to over Ethernet and any downstream panels connected via RS-485 to the Gateway panel.

Note: It is recommended that you change your default user name (admin) and password (admin) to a new user name and password at this time. To do this, proceed to the instructions in Steps to modify a user , page 67.

1.3 Reading the Select Panel

The Select Panel is located at the right margin of the NetAXS® web server main screen, shown in the preceding section. The presence of a number in one of the Select Panel cells indicates that its associated panel is online. For example, if you see a number 1 in a cell, this indicates that panel 1 is online. The combinations of size and color of the number and the color of the cell background indicate the panel's status, as shown in Table 1:

Notes:

- Holding the cursor over a cell also displays a popup message, which conveys the panel in that cell is online or selected.
- The Select Panel refreshes automatically when the panel's status changes.

***Table 1:** Reading the Select Panel*

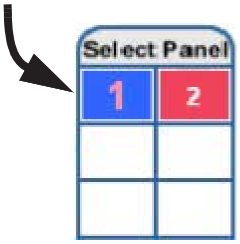
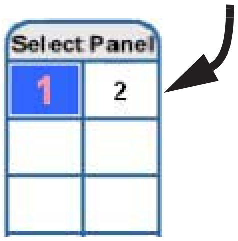
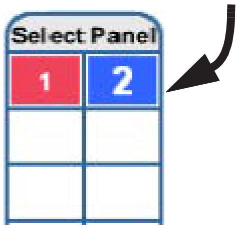
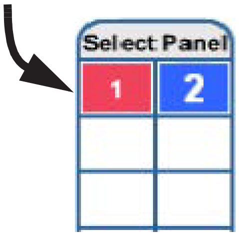
Cell Display	Status
Large red number on a blue background, such as "1" in the example below:  	Panel 1 is selected, and it has unacknowledged alarms.
Small black number on white background, such as "2" in the example below:  	Panel 2 is not selected and it has no unacknowledged alarms.

***Table 1:** Reading the Select Panel* (continued)

Cell Display	Status
Large white number on blue background, such as “2” in the example below: 	Panel 2 is selected, and it has no unacknowledged alarms.
Small white number on a red background, such as “1” in the example below: 	Panel 1 is not selected, but it does have unacknowledged alarms.

2.0 Configuring via the Web Server

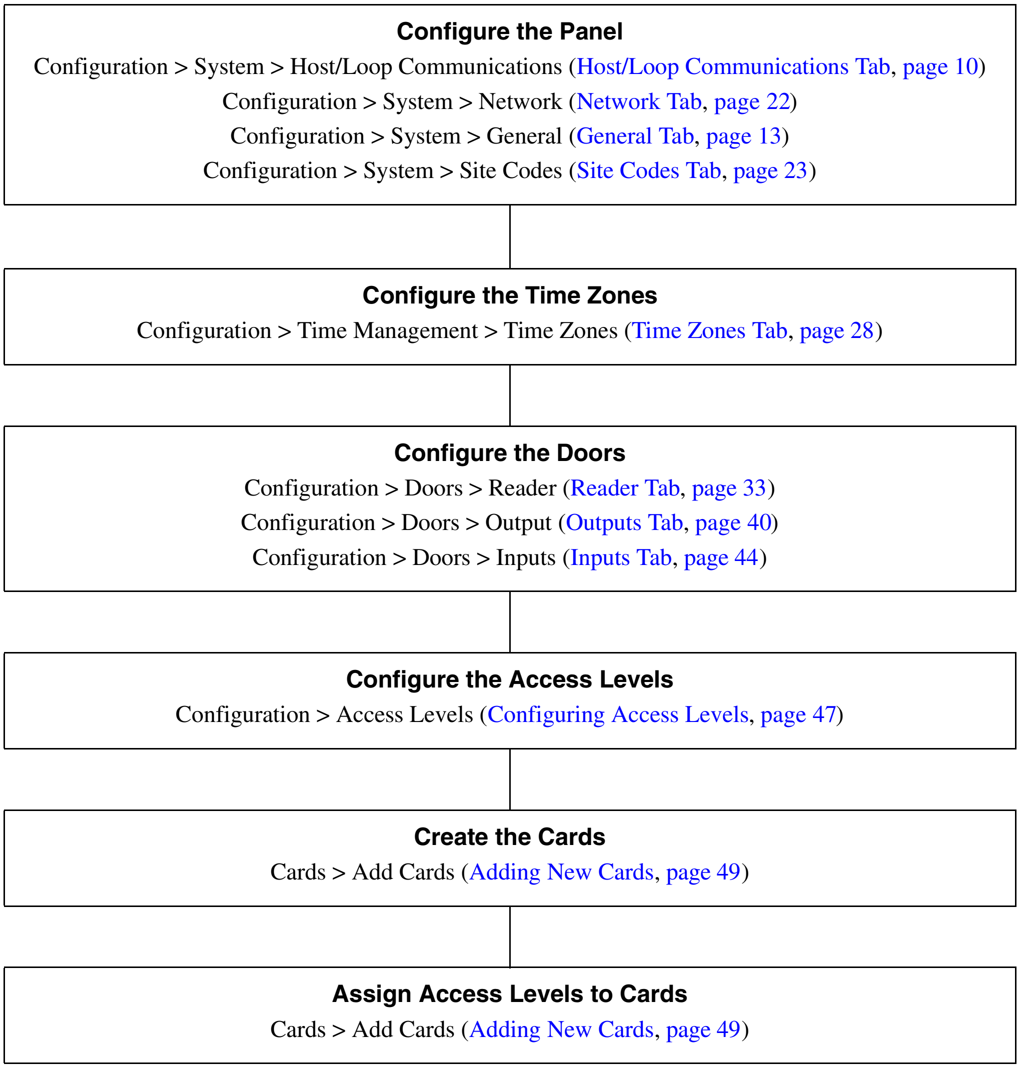
2.1 Overview

This chapter explains the NetAXS® configuration functions as accessed via the NetAXS® web server. These functions should be performed only by the NetAXS® system administrator or service personnel.

Caution: The sequence of NetAXS® configuration tasks is critical. If the sequence given below is not followed, the NetAXS® system cannot be successfully configured.

The flow chart in Figure 3 shows the order in which to perform the administrative functions.

Figure 3: *NetAXS® System Configuration Flow Chart*



Configure the Panel
Configuration > System > Host/Loop Communications (Host/Loop Communications Tab, page 10)
Configuration > System > Network (Network Tab, page 22)
Configuration > System > General (General Tab, page 13)
Configuration > System > Site Codes (Site Codes Tab, page 23)

Configure the Time Zones
Configuration > Time Management > Time Zones (Time Zones Tab, page 28)

Configure the Doors
Configuration > Doors > Reader (Reader Tab, page 33)
Configuration > Doors > Output (Outputs Tab, page 40)
Configuration > Doors > Inputs (Inputs Tab, page 44)

Configure the Access Levels
Configuration > Access Levels (Configuring Access Levels, page 47)

Create the Cards
Cards > Add Cards (Adding New Cards, page 49)

Assign Access Levels to Cards
Cards > Add Cards (Adding New Cards, page 49)

2.2 Configuring the System

2.2.1 Host/Loop Communications Tab

In order to maintain your NetAXS® system configuration or to monitor its status, you must connect to the NetAXS® panel by using one of two modes:

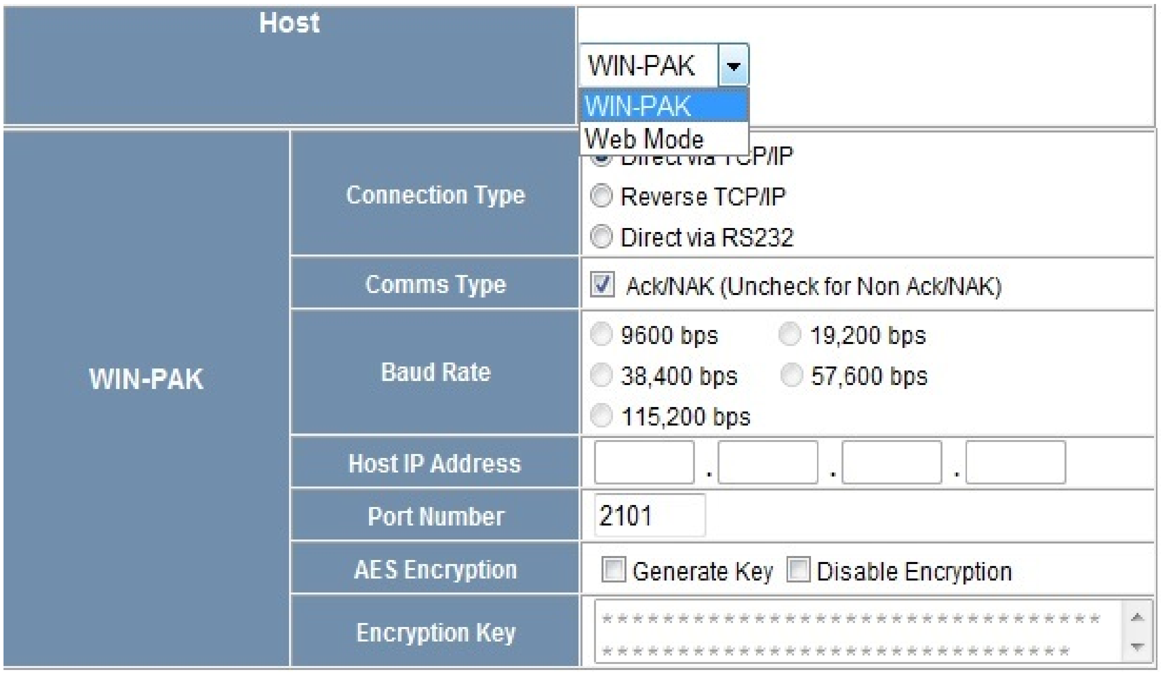
- Host mode (monitor only) — a host software system, such as WIN-PAK™, connects to the panel (through the NetAXS® gateway panel, which has an on-board PCI communications adapter), and it enables you to monitor the status of the NetAXS® system. The on-board PCI adapter functions as an interface between a host computer and one or more panels connected on the Multi-drop line.
- Web mode (configure and monitor) — the NetAXS® web server connects to the panel and enables you to configure the panel and monitor system status.

This tab enables you to select and configure the communication mode you will use to connect to the panel.

Note: A Gateway panel installed with release 3.5.x or newer of NetAXS® firmware cannot communicate fully with previous versions of NetAXS® that may be installed on existing panels. If your panels are running release 2 (v2.2.21 or older), they must be upgraded to release 3.

Click the **Host/Loop Communications** tab:

Figure 4: *Configuration > System > Host/Loop Communications*



Host		WIN-PAK ▾ WIN-PAK Web Mode
WIN-PAK	Connection Type	● Direct via TCP/IP ○ Reverse TCP/IP ○ Direct via RS232
	Comms Type	☑ Ack/NAK (Uncheck for Non Ack/NAK)
	Baud Rate	○ 9600 bps ○ 19,200 bps ○ 38,400 bps ○ 57,600 bps ○ 115,200 bps
	Host IP Address	___ . ___ . ___ . ___
	Port Number	2101
	AES Encryption	□ Generate Key □ Disable Encryption
	Encryption Key	******************************** ********************************

The Host/Loop Communications tab enables you to:

- Configure the following host settings:
  - Host selection (WIN-PAK or Web Mode)
  - Connection Type
  - Comms Type
  - Baud Rate
  - Host IP Address
  - Port Number
  - AES Encryption
  - Encryption Key
- Configure the loop baud rate for communication among downstream panels.

Steps: Use the descriptions in Table 2 to configure the settings:

Table 2: *Configuration > System > Host/Loop Communications Tab Field Descriptions*

Host/Loop	Setting	Description
WIN-PAK	Connection Type	Specifies the type of physical connection between the host and the Gateway panel. If you are connecting from a host software system such as WIN-PAK, select one of the following three connection options: **Direct via TCP/IP** — Host connects directly to the panel using the TCP/IP protocol. **Reverse TCP/IP** — Panel connects directly to the host system using the TCP/IP protocol. You must enter the host IP address in the Host IP Address field. **Direct via RS-232** — Host connects directly to the panel via the RS-232 protocol. If you will be connecting to the panel through the NetAXS® web server, select **Web Mode** from the Host drop down list.
	Comms Type	Specifies the type of communications. **Ack/NAK** — Provides a response (either an acknowledgement or a non-acknowledgement) in a transmission between the host and panel(s). This is the recommended communications type. **Non Ack/NAK** — Does not provide a response (either an acknowledgement or a non-acknowledgement) in a transmission between the host and panel(s). **Note:** This box is unchecked for Non-Ack/NAK.

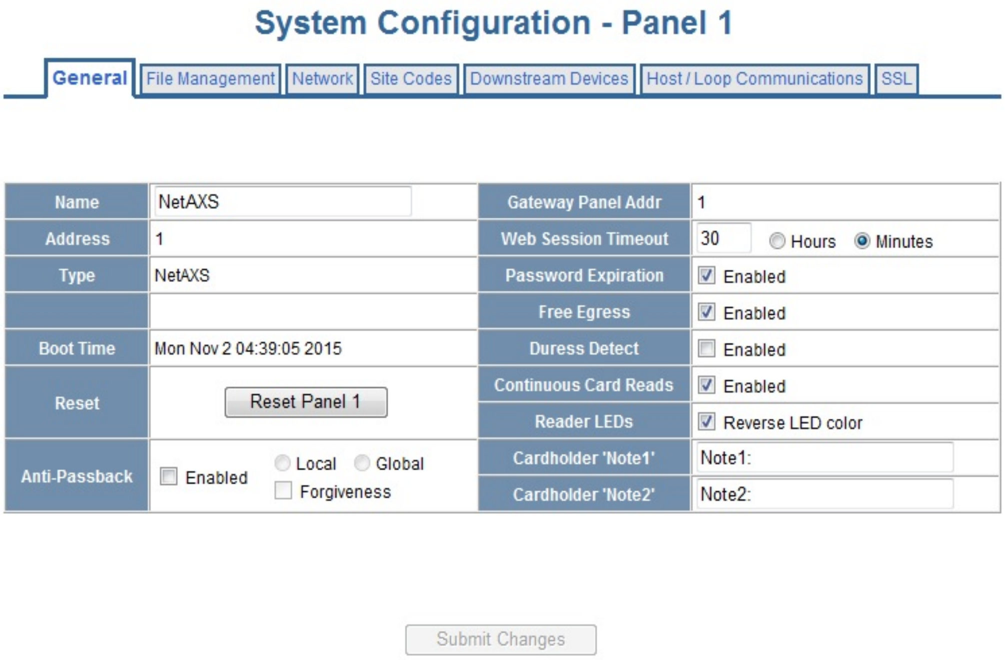
Table 2: *Configuration > System > Host/Loop Communications Tab Field Descriptions* (continued)

Host/Loop	Setting	Description
	Baud Rate	Specifies the transmission rate (bits per second) between the host and the panel.
	Port Number	Specifies the port number for the Ethernet port.
	Host IP Address	Enter the host system (or WIN-PAK server) IP address here if you selected **Reverse TCP/IP** in the Connection Type field on this screen.
	Generate Key	Enable this checkbox to create and display a new encryption key. **Note:** Whenever this button is enabled and the page is submitted, the new key must be entered in WIN-PAK.
	Disable Encryption	Check this boxto disable encrypted communication between NetAXS® Gateway and WIN-PAK Host. Disabling encryption creates an insecure system and is not recommended.
	Encryption Key	This is the password/key used to encrypt communications between the Gateway and WIN-PAK Host. Check on the **Generate Key** box to view and generate a new Encryption key. This password must be used in the Gateway configuration in the WIN-PAK Host. Copy and paste commands are allowed from NetAXS to WIN-PAK. Check on the **Generate Key** box to view and generate a new Encryption key.
Loop	Time Sync	Synchronizes the panel's time with the host's time. **Enabled** — Causes the panel(s) to be automatically time-synchronized with the host. This setting is in minutes, range 60 - 32767.
	Baud Rate	Specifies the transmission rate (bits per second) among the downstream NetAXS® panels on the loop. For NetAXS® downstream panels, it is recommended that you select 115,200.
	Force Baud Reset	Tells all downstream NetAXS® panels to change to the selected Downstream baud rate. This saves the user from having to go to each panel one by one.

2.2.2 General Tab

Click **Configuration > System** in the NetAXS® menu to display the System Configuration (General) screen:

Figure 5: *Configuration > System > General Tab*



System Configuration - Panel 1

Name	NetAXS	Gateway Panel Addr	1
Address	1	Web Session Timeout	30 ○ Hours ● Minutes
Type	NetAXS	Password Expiration	☑ Enabled
		Free Egress	☑ Enabled
Boot Time	Mon Nov 2 04:39:05 2015	Duress Detect	□ Enabled
Reset	Reset Panel 1	Continuous Card Reads	☑ Enabled
		Reader LEDs	☑ Reverse LED color
Anti-Passback	□ Enabled ○ Local ○ Global □ Forgiveness	Cardholder 'Note1'	Note1:
		Cardholder 'Note2'	Note2:

The General Tab enables you to:

- Set the general configuration settings.
- Reset the panel.

Steps: Use the descriptions in Table 3 to configure the general settings, and click **Submit Changes**:

Table 3: *Configuration > System > General Tab Fields*

Parameter	Description
Name	Unique name that identifies the panel.
Address	Displays the address set by the panel's DIP switches.
Type	Displays "NetAXS" as the panel type.
Boot Time	Displays the time that power was applied to the NetAXS® panel.
Reset	Reboots the panel. A reset does not change the current configuration in the database.

***Table 3:** Configuration > System > General Tab Fields* (continued)

Parameter	Description
Anti-Passback	**Enabled** — Enables anti-passback, which prevents an entrant to an area from passing his card back to another potential entrant. **Local** — Enforces anti-passback only at doors configured locally to the panel controlling the original card read. **Global** — Enforces anti-passback at panels throughout the NetAXS® system (NetAXS® panels connected to a single Gateway) after a successful card read at any one of the system's readers. **Forgiveness** — Causes all system codes to be reset at midnight every day. This enables a cardholder who exited the building in the evening without using his card to use his card for entry the following morning.
Gateway Panel Addr	Displays the panel address of the Gateway panel, or the panel directly connected to the host system.
Web Session Timeout	Activates a web session timeout after the specified time period has elapsed. Define the time period either in minutes or in hours. Enter the number in the box, then select either minutes (3-59) or hours (1-12).
Free Egress	**Enabled** — Configures the panel for free egress. Reader 1 activates output 1, reader 2 activates output 2, reader 3 activates output 3, and reader 4 activates output 4. Inputs 1, 3, 5, and 7 are egress defaults that activate outputs 1, 2, 3, and 4, respectively. Inputs 2, 4, 6, and 8 are status defaults for outputs 1, 2, 3, and 4, respectively.
Duress Detect	**Enabled** — Enables the user to trigger an alarm or output device in times of duress, such as when the operator is forced to grant access against his will to an unauthorized person. This feature is available only when the reader is configured with a "Card and Pin" access mode (see Reader Tab, page 33). When this feature is enabled, you can configure an auxiliary output with a pulse time and connect it to a device with an interlock (see Outputs Tab, page 58 for the output configuration). During normal operation, the duress output does nothing. To energize the output, the cardholder presents his card to a reader that is configured for Card and PIN access (see Reader Tab, page 33). The cardholder then enters a PIN that is either one number higher or one number lower than his correct PIN. For example, if his PIN is 2222, the cardholder would enter either 2221 or 2223. Even though the PIN is incorrect, the door will still open normally, but the duress output pulses and an alarm is generated. In this way, the cardholder notifies others without detection by the unauthorized person. **Note:** A PIN ending in 0 (for example, 2320) will only trip a duress output when a 1 is used in place of the 0 (for example, 2321).

Table 3: *Configuration > System > General Tab Fields* (continued)

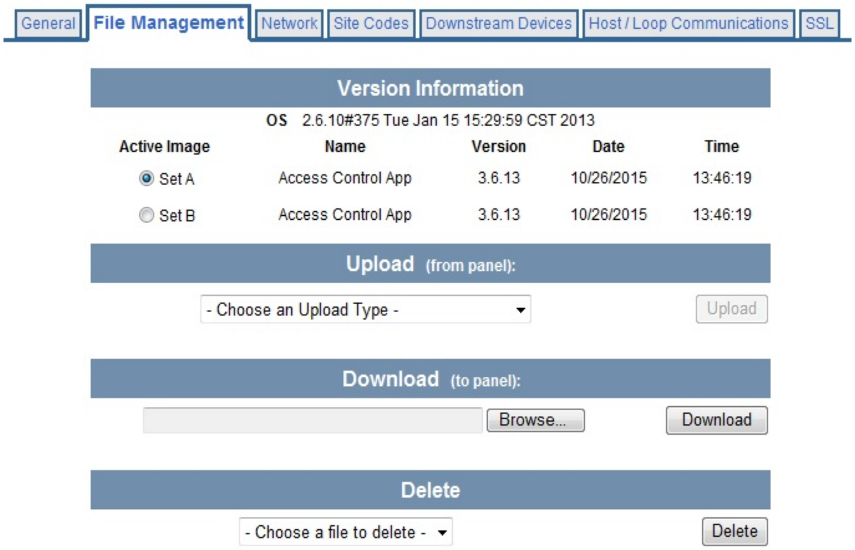
Parameter	Description
Continuous Card Reads	**Enabled** — Enables continuous card reading while the output is being energized. When this option is not enabled, a reader will not be able to read a second card during the pulsing of the output caused by the previous card read.
Reader LEDs	Identifies the color of a reader LED when a grant is authorized. Typically Green indicates the door is open and Red indicates that the door is locked. However, this can be toggled by changing the default setting.
Cardholder Note 1	Specifies any information field you might want to put on a card. For example, if you enter "Department" here, a field labeled "Department" appears on the card. The user who creates the card would then enter the cardholder's department name. See Adding New Cards, page 50.
Cardholder Note 2	Specifies any information field you might want to put on a card. For example, if you enter "Phone Number" here, a field labeled "Phone Number" appears on the card. The user who creates the card would then enter the cardholder's telephone number. See Adding New Cards, page 50.
Password Expiration	Default enable to remind user to change password after 180 days.

2.2.3 File Management Tab

2.2.3.1 Backing up and Restoring the NetAXS Panel

Click **System > File Management** to display the File Management screen:

Figure 6: *Configuration > System > File Management Screen*



Version Information

OS 2.6.10#375 Tue Jan 15 15:29:59 CST 2013

Active Image	Name	Version	Date	Time
● Set A	Access Control App	3.6.13	10/26/2015	13:46:19
○ Set B	Access Control App	3.6.13	10/26/2015	13:46:19

Upload (from panel):

- Choose an Upload Type - ▾ Upload

Download (to panel):

Browse... Download

Delete

- Choose a file to delete - ▾ Delete

To backup a secure, encrypted copy of the database tables:

Select one of the following types of upload from the **Upload** drop-down list:

- Card and Common Configuration data - uploads cards, time zones, card formats, holidays, access levels, and site codes in a proprietary internal format.

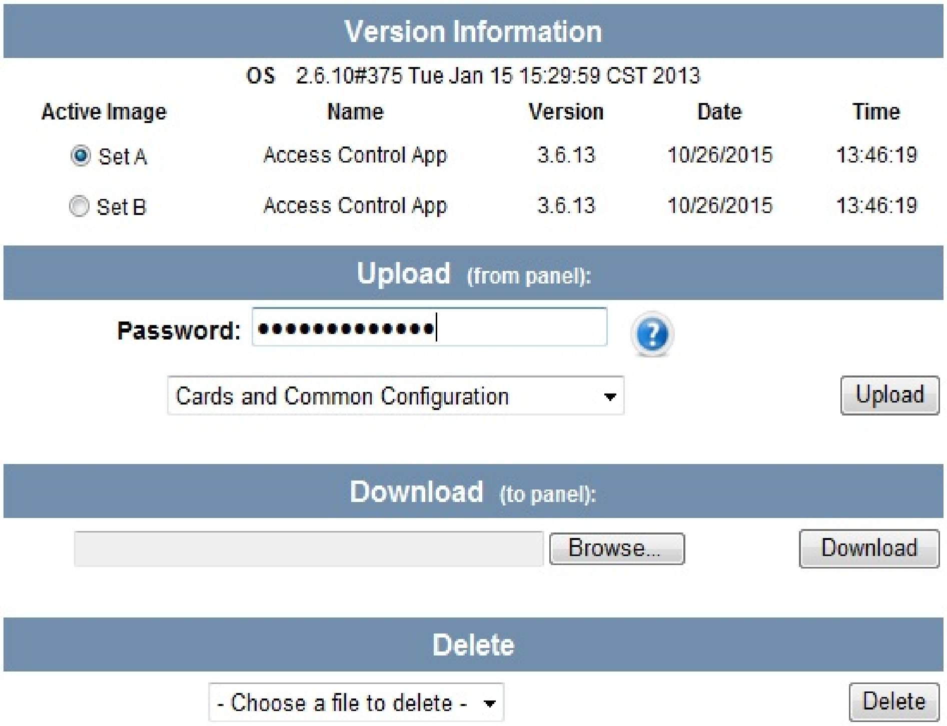
Caution: The card and common configuration data upload from an existing panel on a web-based loop should be used as the first download to a new panel added to the loop. This will configure the new panel so that its basic databases sync up with the existing panel.

- Panel Configuration data – uploads inputs, outputs, interlocks, readers, and panel configuration in a proprietary internal format.
- Card, Common, and Panel Confiduration data - uploads both the cards and panel configuration items in a proprietary internal format.

Example

To Upload a backup copy of Cards and Common:

Figure 7: *Uploading a Backup Copy of Cards and Common*



Version Information

OS 2.6.10#375 Tue Jan 15 15:29:59 CST 2013

Active Image	Name	Version	Date	Time
● Set A	Access Control App	3.6.13	10/26/2015	13:46:19
○ Set B	Access Control App	3.6.13	10/26/2015	13:46:19

Upload (from panel):

Password: •••••••••••••

Cards and Common Configuration

Enter a password. If you attempt to restore the file using the same gateway panel used to create the backup, then the password is not needed. However, if you need to restore the backup using a gateway panel that is not the one which created the backup, the password is required.

To back up (or upload) other data from the panel to the host system:

1. From the Upload drop-down list, select one of the following types of upload from the panel to the host system:

   - Card Report (Short) – uploads the Card Number, Last Name, First Name, Trace, VIP, Limited Use, Card Expiration, Temporary, Supervisor, and Access Level card values in a .CSV file.

   - Card Report (Long) – uploads the Card Number, Last Name, First Name, Trace, VIP, Limited Use, Card Expiration, Temporary, Supervisor, Access Levels, Site Codes, Number of Bits, Pin, Info 1, Info 2, Time Zones, Activation Date, Issue Level, APB State, and Control Device card values in a .CSV file.

     Note: This is the recommended card report for backups.

   - Alarms and Events Report – uploads the Date, Time, Event Type. Acknowledged Date, Acknowledged Time, and Message of Alarms/Events for alarms and events in a .CSV file.

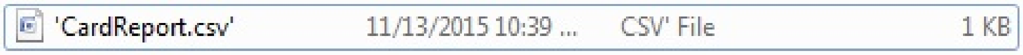
- Language: English (default), Spanish, French, Italian, Dutch, Czech and Chinese (simplified). This is a text file that uploads a language package that translates the text on all of the web screens for a user who has specified a language preference. Languages provided in the language package may not be deleted.

2. Click **Upload** to upload the data to the host PC or laptop. Follow the instructions to save a backup file on your PC. Be sure to give the backup file a useful name for easy identification and restoring.

Note: In order to have a full backup of the panel it is recommended to download the following files:

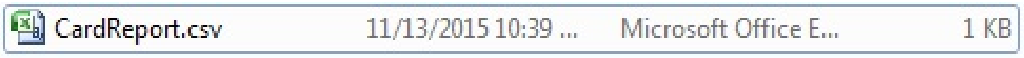
- Cards, Common and Panel Configuration
- Card Report (Long)

Note: When uploading and downloading .CSV files, check the file name to ensure it does not have an extra single quote.



'CardReport.csv' 11/13/2015 10:39 ... CSV' File 1 KB

If it does have an extra single quote, right click on 'CardReport.csv', select rename to delete the single quote, then the .CSV file likes this:



CardReport.csv 11/13/2015 10:39 ... Microsoft Office E... 1 KB

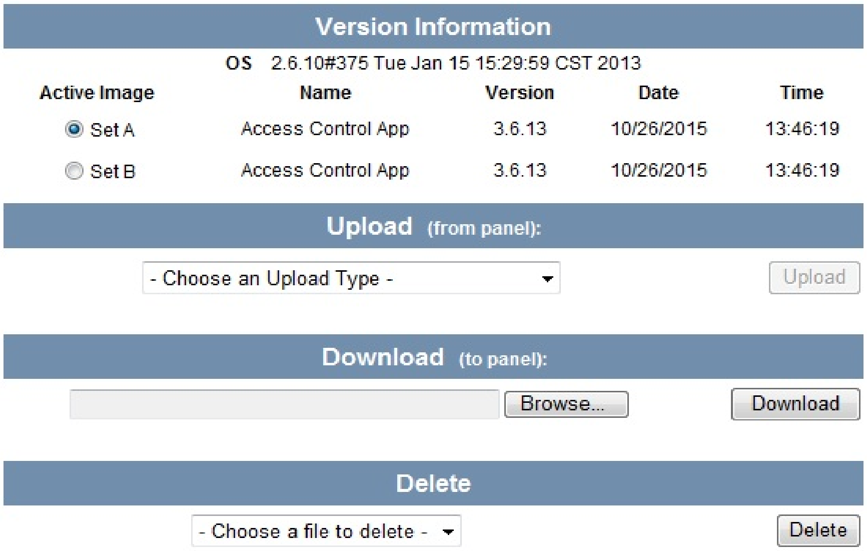
Important: Read Appendix A, Upgrading NetAXS Firmware before downloading to the panel.

When the download is completed, the panel is immediately rebooted. A status bar indicates the progress of the reboot.

To restore (or download) firmware:

1. Click **Browse** to locate the firmware file.
2. Click **Download**

Figure 8: *File Management Setting*



Version Information

OS 2.6.10#375 Tue Jan 15 15:29:59 CST 2013

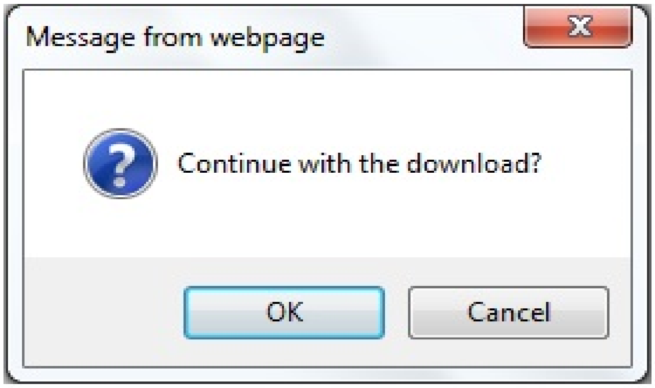
Active Image	Name	Version	Date	Time
● Set A	Access Control App	3.6.13	10/26/2015	13:46:19
○ Set B	Access Control App	3.6.13	10/26/2015	13:46:19

Upload (from panel):

Download (to panel):

Delete

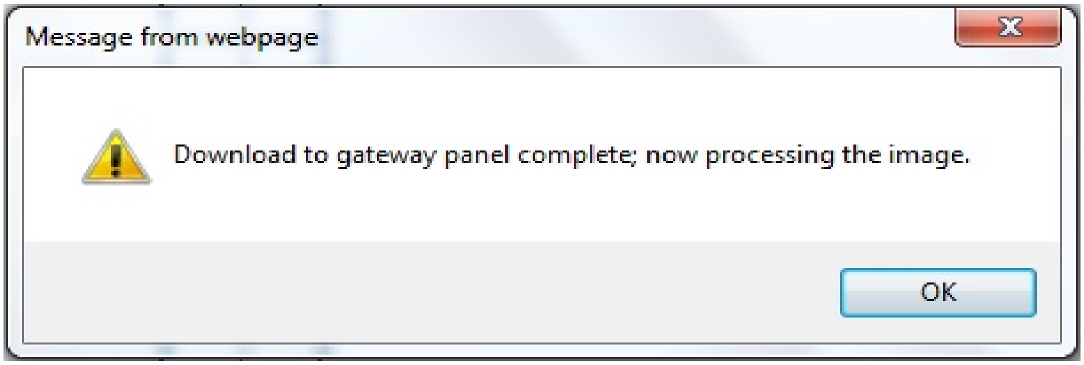
3. Click **OK** to continue with the download



Message from webpage

Continue with the download?

4. Click **OK** to processing the image



Message from webpage

Download to gateway panel complete; now processing the image.

To download a card database report (.CSV file) from the host system to the panel:

1. Click **Browse** to locate the .CSV file. This .CSV file is usually the Card Report (long) that was previously uploaded from the panel as a backup.
2. Click **Download** to download the file. If the file is in the correct report format, this message appears: "Would you like to append or replace the database? Access Control does not function while replacing a database, and updating may take several minutes." If the file is not in the correct report format, a message states the error condition.

   If the database update is successful, this message appears: "Update Successful. Restarting Access Control." If the database update is not successful, a message states the error condition.

To restore (or download) backup files from the host system to the panel:

1. Click **Browse** to locate the backup file.
2. Click **Download** to download the selected backup file.

Note: When restoring, if you attempt to restore file using the same gateway panel used to create the backup, then the password is not needed. However, if you need to restore the backup using a gateway panel that is not the one which created the backup, the password is required.

To delete language files:

1. From the Delete drop-down list, select the language file you want to delete.
2. Click **Delete** to delete the file.

2.2.3.2 Generating Diagnostic Report

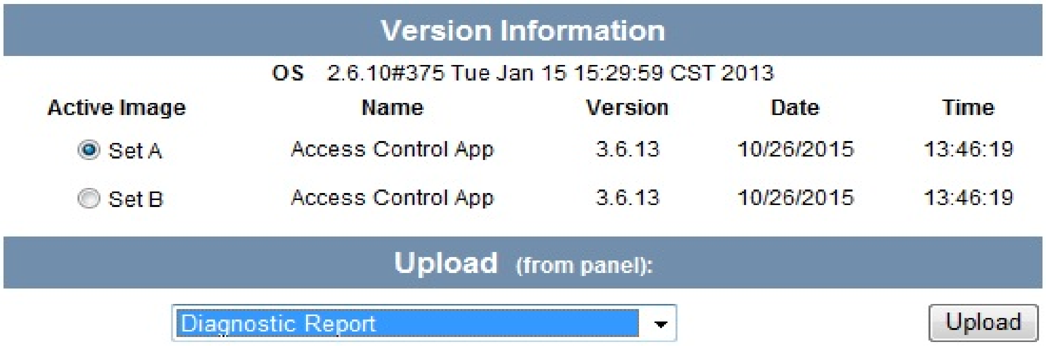
Troubleshooting information can be retrieved from the panel using this function. The report is not readable to the customer and is useful only as a tool to help Honeywell technical support troubleshoot certain unusual problems.

To generate a diagnostic report, select "Diagnostic Report" from the **Upload** drop-down menu on File Management Screen.

Click **Upload** button.

Save the file when prompted to do so.

Figure 9: *Generating a Diagnostic Report*



Version Information

OS 2.6.10#375 Tue Jan 15 15:29:59 CST 2013

Active Image	Name	Version	Date	Time
● Set A	Access Control App	3.6.13	10/26/2015	13:46:19
○ Set B	Access Control App	3.6.13	10/26/2015	13:46:19

Upload (from panel):

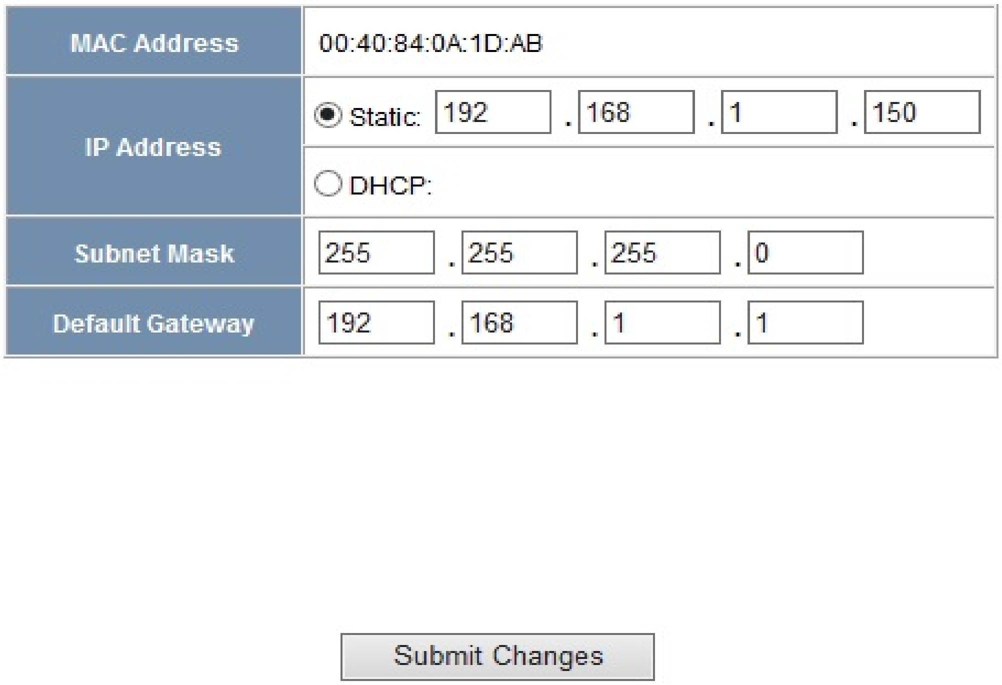
Diagnostic Report

2.2.4 Network Tab

Your NetAXS® panel is physically configured in one of a number of possible network configurations. See the "System Configuration" section in the *NetAXS® NX4L1 Installation Guide* and *NetAXS® NX4S1 Installation Guide* for illustrations of the supported network configurations. For the panel to function in any of these configurations, the other panels and devices in the network must know the panel's network addresses.

Click **Network** to display the Network tab:

Figure 10: *Configuration > System > Network Tab*



MAC Address	00:40:84:0A:1D:AB
IP Address	● Static: 192 . 168 . 1 . 150
	○ DHCP:
Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 1 . 1

The Network tab enables you to:

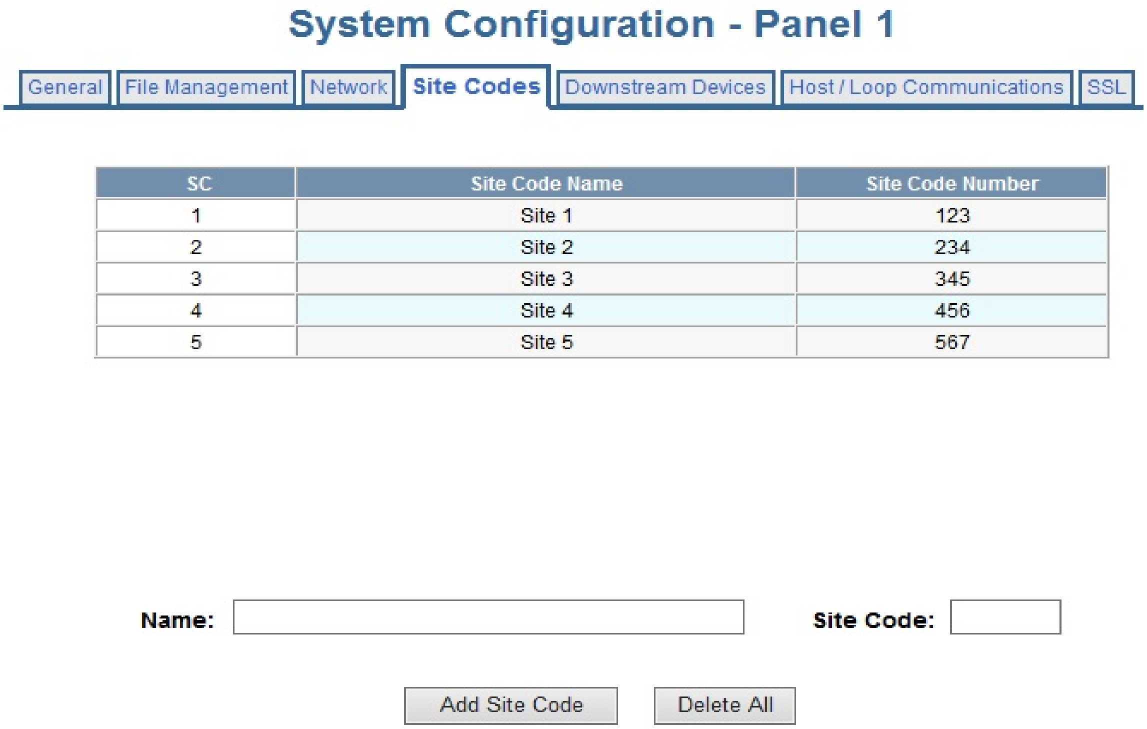
- View the panel's MAC address.
- View and edit the panel's IP address.
- View and edit the panel's subnet mask.
- View and edit the panel's default gateway.

2.2.5 Site Codes Tab

Site codes identify an enterprise's site. You can create a maximum of eight site codes to serve as secondary IDs (in addition to the card number) on the card for additional validation.

Click **Site Codes** to display the Site Codes tab:

Figure 11: *Configuration > System > Site Codes Tab*



SC	Site Code Name	Site Code Number
1	Site 1	123
2	Site 2	234
3	Site 3	345
4	Site 4	456
5	Site 5	567

The Site Codes tab enables you to:

- Create one or more site codes.
- View existing site codes.
- Modify an existing site code.
- Delete a selected site code.
- Delete all site codes.

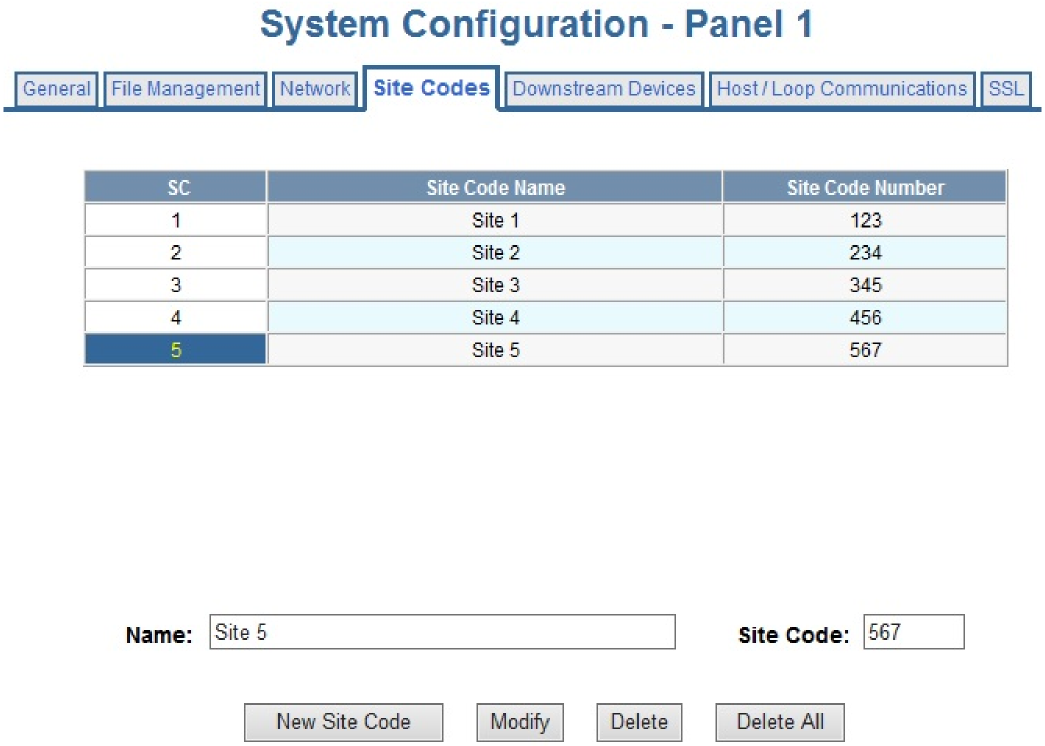
Steps to create a site code:

1. Enter a name for the site code in the Name field.
2. Enter a unique number (up to five digits) for the site code in the Site Code field.
3. Click **Add Site Code** to create the site code.

Steps to modify a site code:

1. Click the site code's number in the Num column to select the site code.

Figure 12: *Select Site Code Number*



System Configuration - Panel 1

SC	Site Code Name	Site Code Number
1	Site 1	123
2	Site 2	234
3	Site 3	345
4	Site 4	456
5	Site 5	567

Name: Site 5

Site Code: 567

2. Click **Modify** to display the Name and Site Code fields.
3. Modify the name or site code number as you desire, and click **Modify** again.

Steps to delete a site code:

1. In the Num column, click the number of the site you want to delete.
2. Click **Delete** to display a prompt.
3. Click **OK** to delete the site code.

Steps to delete all site codes:

1. Click **Delete All Codes** to display a prompt.
2. Click **OK** to delete the codes.

2.2.6 Downstream Devices Tab

The NetAXS® downstream devices provide the NetAXS® panel with additional inputs and outputs. The NetAXS® panel supports two downstream board types:

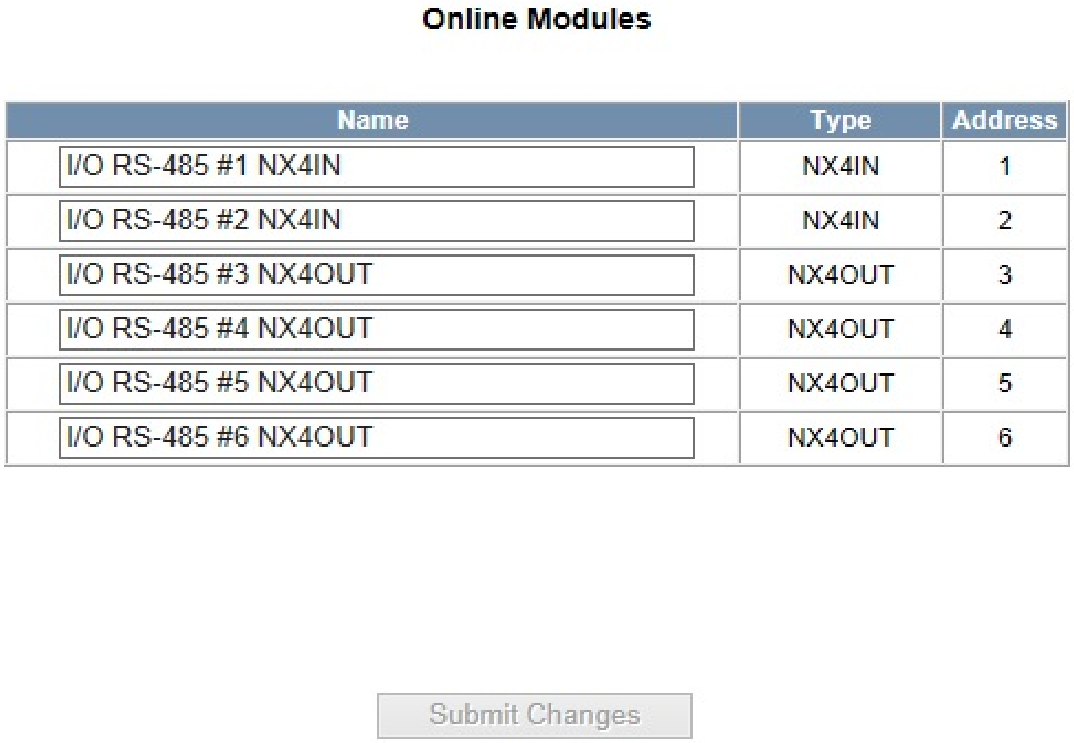
- NX4IN — Provides 32 supervised, four-state inputs that are limited to 2.2K ohms resistance. The NX4IN must be assigned network addresses 1 and 2.
- NX4OUT — Provides two supervised inputs and 16 SPDT relay outputs; each input is limited to 2.2K ohms resistance. The NX4OUT must be assigned network addresses 3-6.

Notes:

- The NX4IN and NX4OUT network addresses are set by the DIP switches on each board. Refer to the *NetAXS® NX4IN/NX4OUT Input/Output Configuration Guide* for more information about configuring the NX4IN and NX4OUT boards.
- A NetAXS® panel supports a maximum of six daisy-chained downstream boards — two NX4IN and four NX4OUT boards. The boards connect to the NetAXS® panel’s Downstream port (Terminal Block 10).

Click the **Downstream Devices** tab:

Figure 13: *Configuration > System > Downstream Devices Tab*



Online Modules

Name	Type	Address
I/O RS-485 #1 NX4IN	NX4IN	1
I/O RS-485 #2 NX4IN	NX4IN	2
I/O RS-485 #3 NX4OUT	NX4OUT	3
I/O RS-485 #4 NX4OUT	NX4OUT	4
I/O RS-485 #5 NX4OUT	NX4OUT	5
I/O RS-485 #6 NX4OUT	NX4OUT	6

The Downstream Devices tab enables you to:

- View and modify the names of the devices that communicate with the panel.
- View the types and addresses of the devices that communicate with the panel.

2.3 Configuring Time Management

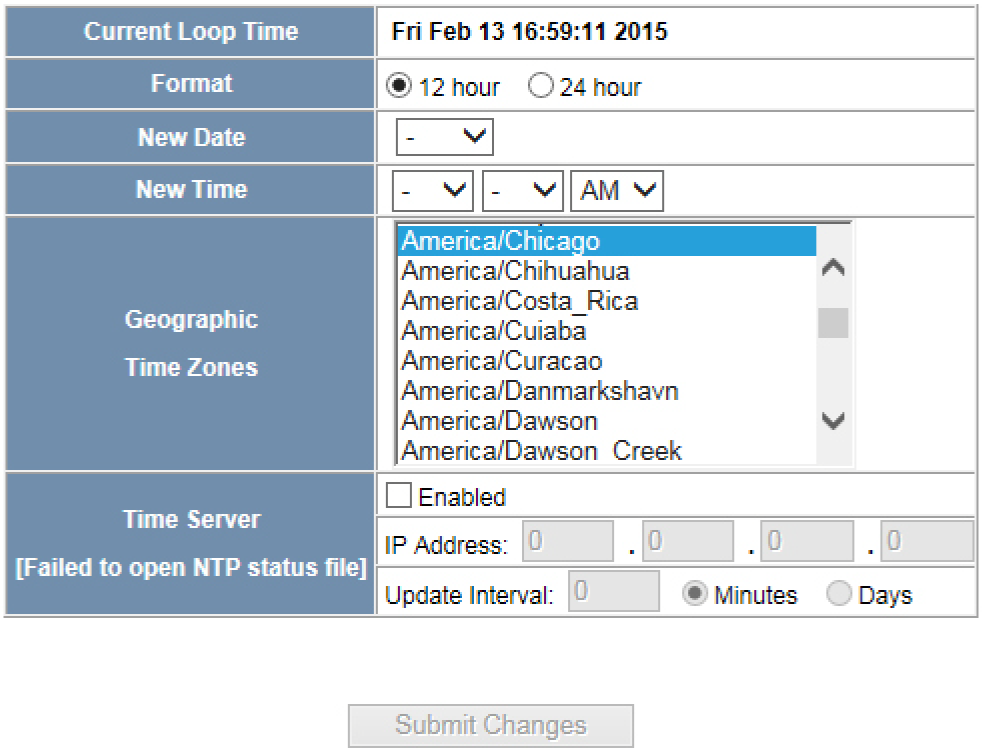
This set of time-related functions includes:

- Setting the current time by which the panel will function.
- Creating the time zones by which the panel will control the operation of the inputs, outputs, groups, readers, access levels, and cards through access levels.
- Defining the holiday schedule.

2.3.1 Current Time Tab

Click **Current Time** to display the Current Time screen:

Figure 14: *Configuration > Time Management > Current Time Tab*



Current Loop Time	Fri Feb 13 16:59:11 2015
Format	● 12 hour ○ 24 hour
New Date	-
New Time	- - AM
Geographic Time Zones	America/Chicago America/Chihuahua America/Costa_Rica America/Cuiaba America/Curacao America/Danmarkshavn America/Dawson America/Dawson_Creek
Time Server [Failed to open NTP status file]	□ Enabled IP Address: 0 . 0 . 0 . 0 Update Interval: 0 ● Minutes ○ Days

The Current Time tab enables you to:

- Set the current loop time.
- Specify the time format (12 hour/24 hour).
- Set a new date.
- Set a new time.
- Set the geographic time zone.
- Specify the time server being used.
- Force a time synchronization between the panel and the time server.

Steps: Use the descriptions in Table 4 to configure the time settings:

Table 4: *Configuration > Time Management Tab Field Descriptions*

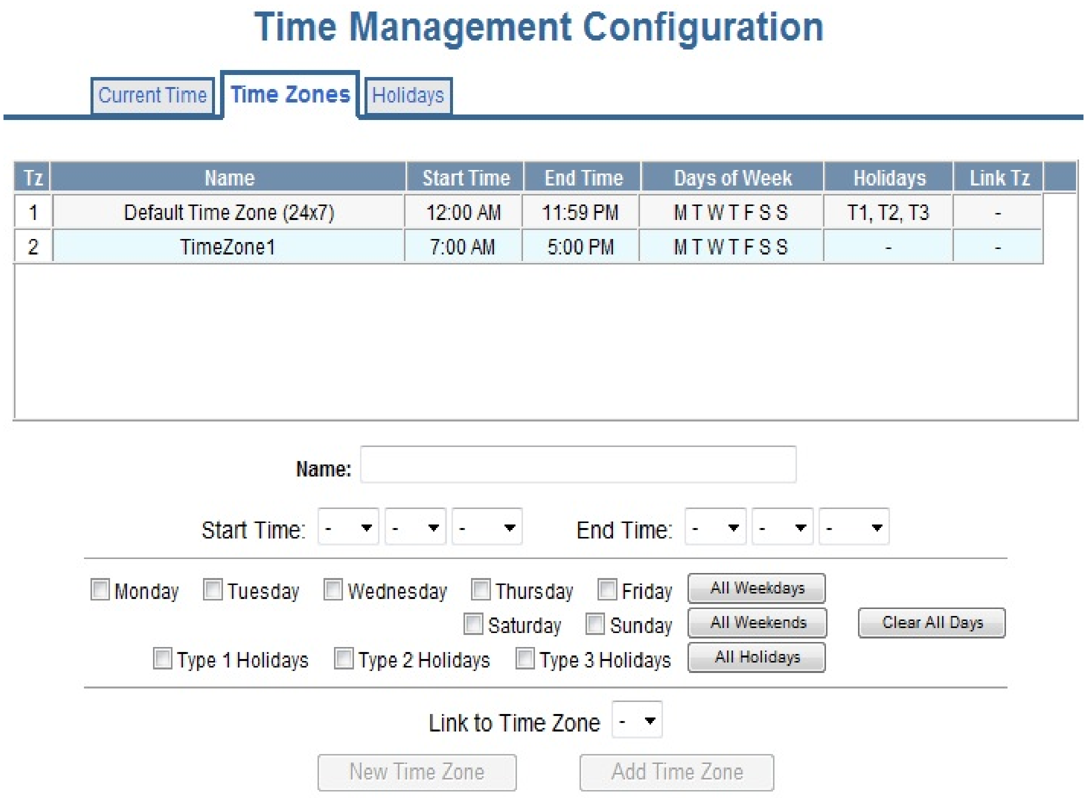
Setting	Description
Current loop time	Displays by default the current time setting in day/month/date/hour/minutes/seconds/year. For example: Fri Oct 31 07:16:27 2014.
Format	**12 hour** — The 24-hour day is divided into two 12-hour halves, a.m. and p.m.; each half is numbered 1-12. **24 hour** — The hours in the 24-hour day are numbered consecutively 0-23.
New Date	Specifies a new date to be the current date. Use the dropdown lists to set the month and date, and click the calendar icon to specify a different year.
New Time	Specifies a new time to be the current time. Use the dropdown lists to set the hour, minute, and AM or PM.
Geographic Time Zone	Select the geographic time zone in which the panel will operate. The time zones are written in the [continent/city] format. Find the appropriate continent, and then identify the city with the closest longitude to the panel's location. In the United States, you might find these time zone associations more familiar: Eastern Time: America/New York Central Time: America/Chicago Mountain Time: America/Denver Pacific Time: America/Los Angeles
Time Server	Enter the IP address of the machine whose time is used as the standard for all panels. **Enabled** — Select to enable the specified machine to be the active time server. **IP Address** — Enter the IP address of the time server. **Update Interval** — Specifies the interval of time between each automated synchronization. **Note:** Recommended value is once per day. The panel starts to update time as soon as it is enabled and successfully connects to the Time Server; it will continue to update according to the interval selected from that start point.

2.3.2 Time Zones Tab

The NetAXS® panel controls access by using time zones, or time schedules. Inputs, outputs, groups, readers, access levels, and cards through access levels are all configured with time zones by which they will be energized or de-energized, enabled or disabled. For example, you might assign a group of outputs to be energized from 12:00 a.m. to 6:00 a.m. every day. The 12:00 a.m. to 6:00 a.m., Monday through Sunday, time period is called a time zone. The Time Zones tab enables you to create the time zones you will use to configure your NetAXS® system.

Click **Time Zones** to display the Time Zones screen:

Figure 15: *Configuration > Time Management > Time Zones Tab*



Tz	Name	Start Time	End Time	Days of Week	Holidays	Link Tz
1	Default Time Zone (24x7)	12:00 AM	11:59 PM	M T W T F S S	T1, T2, T3	-
2	TimeZone1	7:00 AM	5:00 PM	M T W T F S S	-	-

The Time Zones tab enables you to:

- Create a new time zone.
- Modify a time zone.
- Delete a time zone.

Steps to create a time zone:

1. Enter the name of the new time zone in the **Name** field.
2. Enter a start time and an end time for the time zone.
3. Select the days of the week during which the time zone will be in effect.

4. If the time zone will be linked to another time zone, select the "linked to" time zone's number from the drop down list.

   ⚠ **Caution:** We recommend that you read the explanation of time zone linking below (see Linking Time Zones) before you link time zones. An example is provided to help you create the links successfully.

5. Click the **Add Time Zone** button.

Steps to modify a time zone:

1. In the Tz column, click the number of the time zone you want to modify.
2. Change the time zone settings as you desire.
3. Click the **Modify** button to accept the changes.

Steps to delete a time zone:

⚠ **Caution:** Do not delete a time zone that is currently in use.

1. In the Tz column, click the number of the time zone you want to delete.
2. Click the **Delete** button.
3. Click **OK** at the delete prompt.

Linking Time Zones

You assign each Time Zone a specific start time and end time. The maximum time range is from 12:00 a.m. to 11:59 p.m. Note that the time range cannot cross midnight. You can set this time range to be effective for any day of the week, including weekends (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday). These days can also include holidays, which are considered special days that take precedence over a standard day. Also, since Access Levels, Outputs, Inputs, Groups can only be given one Time Zone selection at a time, you can link Time Zones together to create bigger time zones that could not fit into a single Time Zone.

For example, suppose you must create a Cleaning Crew Time Zone. The time zone(s) are to be set up as follows: Monday-Friday 5 p.m.-1 a.m., Saturday and Sunday 8 a.m.-1 p.m., no holidays. This becomes three separate time zones, as follows.

Time Zone #	Time Range
2	Monday-Friday, 5 p.m.-11:59 p.m. (Remember, the time range cannot cross midnight, so 11:59 p.m. is the limit.)
3	Tuesday-Saturday, 12:00 a.m.-1:00 a.m.
4	Saturday-Sunday, 8:00 a.m.-1:00 p.m.

Note: Time Zone 1 is reserved as a default with a time range of 24 hours, seven days a week.

So, we need to add three time zones to the panel. Then, with the Link Time Zone feature, you can link them so that they all work together:

1. Add Time Zone 2 and select Monday, Tuesday, Wednesday, Thursday, and Friday. Enter a start time of 5:00 p.m. and an end time of 11:59 p.m. Leave the Link to Time Zone field blank.
2. Add Time Zone 3 and select Monday, Tuesday, Wednesday, Thursday, and Friday. Enter a start time of 12:00 a.m. and an end time of 1:00 a.m. In the Link to Time Zone field, select Time Zone 2 to link Time Zones 2 and 3 together.
3. Add Time Zone 4 and select Saturday and Sunday. Enter a start time of 8:00 a.m. and an end time of 1:00 p.m. In the Link to Time Zone field, select Time Zone 3 to link Time Zones 2, 3, and 4 together.

Linked in this way, Time Zone 4 tells the NetAXS® system that it is also to use Time Zone 3, and Time Zone 3 tells the system that it is to also use Time Zone 2. Since Time Zone 4 is the "start" of this linked chain, it is the Time Zone that would be operative for the Cleaning Crew Access Level. That is, the doors to which the cleaning crew would have access would be assigned Time Zone 4. And, by assigning them Time Zone 4, they would also have access during Time Zones 3 and 2 — because they are linked.

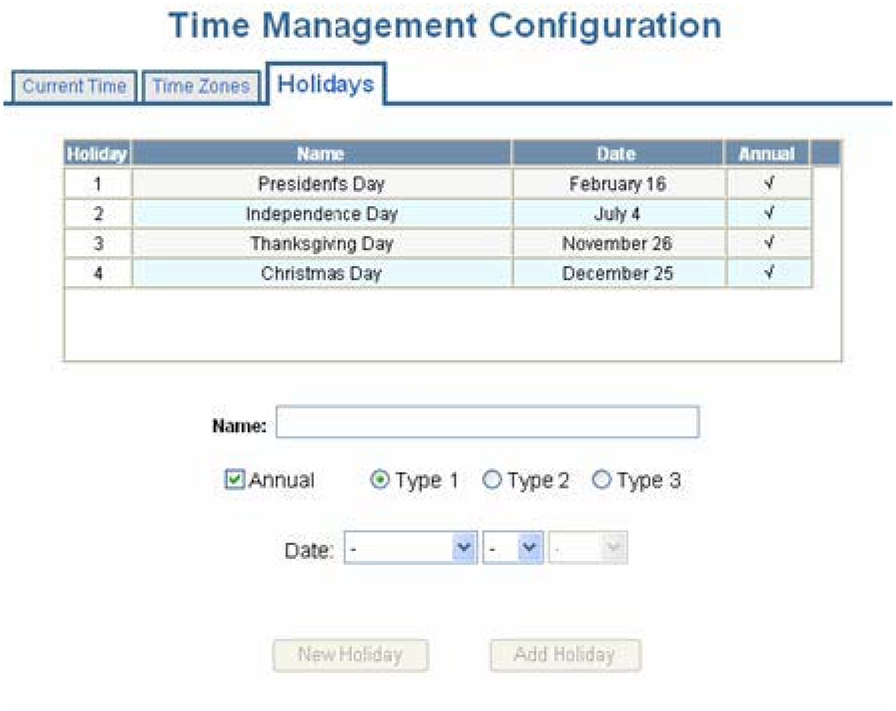
Note that in this example, Time Zone 2 is not linked to Time Zone 4. This is by rule. Time Zone links should start on one end and stop at other. If you link the start of a Time Zone chain to the end, you create a condition called a "circular interlock," which would cause your time zones to not function properly. The panel will send you a warning, should you try to create a circular interlock.

2.3.3 Holidays Tab

Holidays are days when no work is scheduled at the facility. These holidays are used in time zone configuration (see Time Zones Tab, page 28).

Click the **Holidays** tab:

Figure 16: *Configuration > Time Management > Holidays Tab*



Time Management Configuration

Holiday	Name	Date	Annual
1	Presidents Day	February 16	√
2	Independence Day	July 4	√
3	Thanksgiving Day	November 26	√
4	Christmas Day	December 25	√

Name:

☑ Annual ● Type 1 ○ Type 2 ○ Type 3

Date: - - -

The Holidays tab enables you to:

- Create a holiday.
- Modify a holiday.
- Delete a holiday.

Note: Holidays should be considered special days of a week. They are similar, but of higher rank than the standard Monday-Sunday. If a day programmed as a Holiday should occur in the panel, the panel will treat that day as the Holiday type, regardless of the actual day of the week (Monday-Sunday). During this Holiday, only Time Zones that contain that specific Holiday type will work. The Holiday allows users to further customize how the panel works. For example, the user can block access to a building on that day, or grant special access during that day.

Each Holiday added is considered a full day, extending from midnight to midnight. The options available when configuring a holiday are Annual, Type, Date and Year. While Annual is enabled, the date added as a Holiday will be a Holiday every year. This disables the Annual check box and allows a user to select a specific year, so that only during that date and year will the Holiday selection work.

While Annual is selected, the Year box is grayed out. The NetAXS can support three different Holiday Types (Type 1, Type 2, and Type 3), but a user can only select one type per day. Also of note, a single calendar day cannot be set for more than one type of Holiday. For example, the 4th of July could be a Type 1 Holiday, but then Type 2 and 3 would not be able to work on the 4th of July. Holidays or special events that require multiple days will require a Holiday entry for each date that is to be special. For example, Thanksgiving is usually two days, Thursday and Friday. Both of these days would require a separate Holiday date entry and use the same Holiday Type. Beyond that, Type 1, 2, and 3 can be configured any way you wish.

Steps to create a holiday:

1. Enter the name of the new holiday in the **Name** field (up to 25 characters).
2. If the holiday will occur annually, select the **Annual** checkbox.
3. Assign a type to the holiday, either Type 1, Type 2, or Type 3. The type you assign will map to a time zone configuration, and the holiday will be regarded according to the rules of that time zone (see Time Zones Tab, page 28).
4. Select the holiday's month and date from the drop down lists.
5. Click the **Add Holiday** button.

Steps to modify a holiday:

1. In the Holiday column, click the number of the holiday you want to modify.
2. Change the holiday settings as you desire.
3. Click the **Modify** button to accept the changes.

Steps to delete a holiday:

1. In the Holiday column, click the number of the holiday you want to delete.
2. Click the **Delete** button.
3. Click **OK** at the delete prompt.

2.4 Configuring the Doors

Each NetAXS® panel supports four doors. For each door, you must configure the readers, inputs, and outputs.

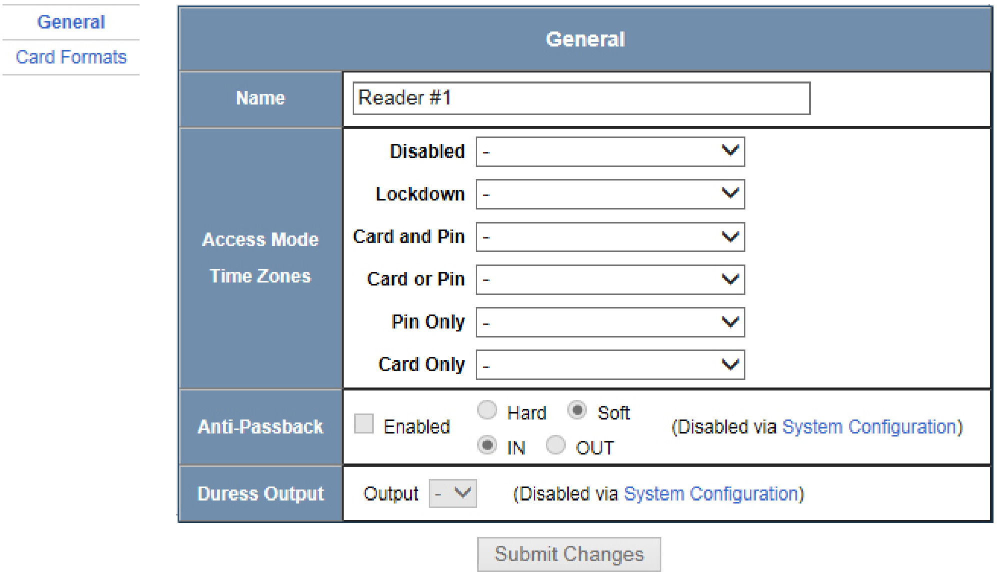
At **Configuration > Doors** in the task menu at the left margin of the NetAXS® screen, click 1 to display the Door Configuration screen for door 1. Follow the same procedures below for doors 2, 3, and 4 for each panel.

2.4.1 Reader Tab

A reader is a device that reads cards and either grants or denies access at the door.

Click the **Reader** tab:

Figure 17: *Configuration > Doors > Reader > General Tab*



General		
Name	Reader #1	
Access Mode Time Zones	Disabled	-
	Lockdown	-
	Card and Pin	-
	Card or Pin	-
	Pin Only	-
	Card Only	-
Anti-Passback	☐ Enabled	○ Hard ● Soft ● IN ○ OUT (Disabled via System Configuration)
Duress Output	Output -	(Disabled via System Configuration)

The Reader tab enables you to:

- Define the time zone during which the reader will be disabled. When the reader is disabled, neither exit nor entry by Card and PIN mode or Card or PIN mode is allowed. Also, free egress is not allowed.

Note: Should a conflict arise among the time zones set in the Access Mode Time Zones box on the Reader > General tab, priority is given to the time zone that is highest in the list of time zones displayed on the tab. Therefore, the Disabled time zone has highest priority, and the Card Only time zone has lowest priority.

- Define the time zone during which the reader will be in lockdown mode (see Time Zones Tab, page 28 for details about setting time zones). When the reader is in lockdown mode, entry is prevented but egress is still allowed. Only a VIP card can unlock the door.

- Define the reader's access mode (the combination of card and/or PIN entry required by the reader). Note that the access mode defined here for the door can be overridden by a card assigned with a VIP card type (see Adding New Cards, page 50 for information about assigning a VIP card type).
- Enable the Card Only, PIN Only, Card and PIN, and Card or PIN access modes with either the Supervisor or Escort rule:
  - Supervisor Rule: When the supervisor presents his card during the specified time zone just once, he gains access but does not enable access for non-supervisory personnel.
  - Escort Rule: This rule requires a supervisor escort for a non-supervisor.
- Configure the anti-passback feature. When enabled, the anti-passback feature prevents an entrant to an area from passing his card back to another potential entrant. Note that anti-passback must first be enabled at the **Configuration > System > General** screen (see General Tab, page 13).
- Specify the data format the reader must use to read the card data.
- Reconfigure a selected format's data layout.
- Select a Duress Output; Note that Duress Detect must first be enabled at the **Configuration > System > General** screen (see General Tab, page 13).

Steps:

1. Use the descriptions in Table 5 to configure the General reader settings.

Table 5: *Configuration > Doors > Reader Tab Descriptions*

Setting	Description
Access Mode	Specifies the validation conditions required at the door before access is granted. For each access mode, you must also select a time zone from the drop down list. The time zone is the schedule by which the access mode is effective. **Disabled** — Ignores all card reads (except from a VIP card), allows neither exit nor entry by Card-and-PIN mode or Card-or-PIN mode. Also, free egress is not allowed. **Lockdown** — Ignores all card reads (except from a VIP card), denies door entry but allows egress. **Card and Pin** — Grants access only with both a successful card read and a valid PIN entry at the door's keypad. You can perform the card read and PIN entry in either sequence. **You must make the second entry within 10 seconds of the first entry, in either sequence.** **Card or Pin** — Grants access with either a successful card read or a valid PIN number entry at the door's keypad. **Pin Only** — Grants access with only a valid PIN number entered at the door's keypad. **Card Only** — Grants access with only a successful card read. **Supervisor** — A mode that enables a supervisor to enter without allowing general access. When this mode is enabled, the reader LED changes color four times per second (usually red then green). When the supervisor presents his card during the time zone just once, he gains access but does not enable general access. If the supervisor presents his card again within 10 seconds, he enables general card access and the LED displays a steady red. After the supervisor presents his card twice to allow general card access, he can disable the general card access for the time zone by presenting his card again twice consecutively. The LED resumes rapid flashing between red and green. VIP cards do not need a supervisor card to gain access. **Escort** — A mode that requires a supervisor escort to allow entry by an employee card holder. When this mode is enabled, the reader LED changes color four times per second (usually red then green) and employees must be accompanied by a supervisor to gain entry. When the supervisor presents his card, the LED goes solid red for 10 seconds, pending an employee credential. When the employee credential is swiped within 10 seconds of the supervisor card swipe, the door opens to admit the employee and the LED returns to rapid flashing. If the time expires and there is no employee credential swipe, the LED returns to rapid flashing and the reader returns to escort mode. A supervisor can gain entry by simply swiping the card twice. Unlike Supervisor mode, the Escort mode when active cannot be disabled during its time zone; a supervisor is required for all employee access during Escort mode time zone. VIP cards do not need a supervisor card to gain access.

***Table 5:** Configuration > Doors > Reader Tab Descriptions* (continued)

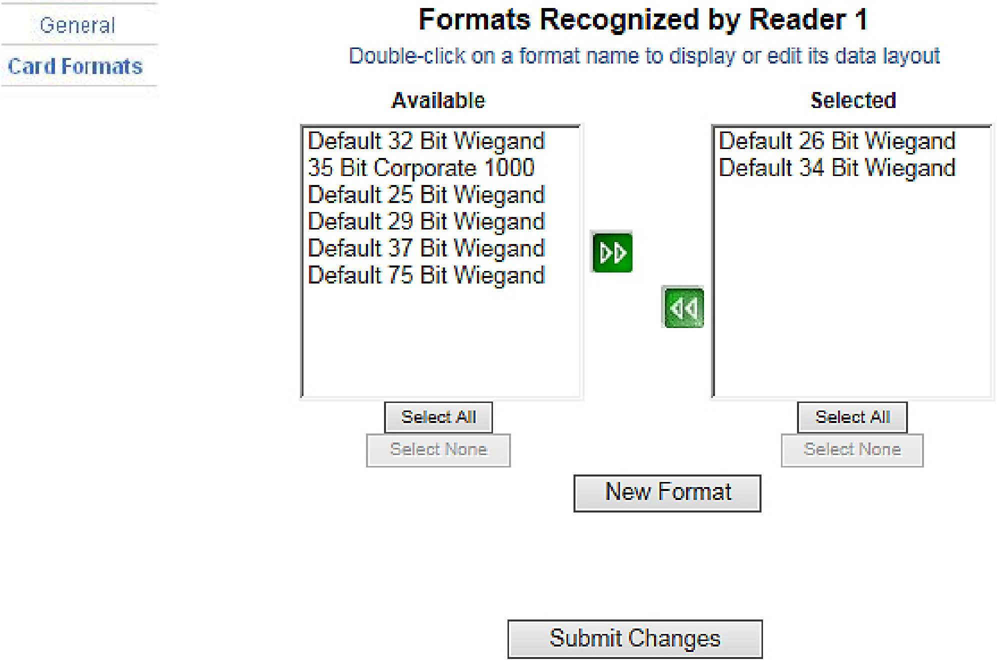
Setting	Description
Anti-Passback	Configures the anti-passback feature. Once configured under **Configuration > System > General** screen (see General Tab, page 13), the user enables the anti-passback feature on the reader, which requires a valid card for entry and exit. The card holder must use the card in the proper IN/OUT sequence — that is, a card swiped at an IN reader must then be swiped at an OUT reader, or vice versa — a card swiped at an OUT reader must then be swiped at an IN reader. If the user's IN/OUT sequence is invalid, then an anti-passback violation event is generated for the type of anti-passback chosen (Hard or Soft) and the card holder is either denied access (Hard) or allowed access (Soft). **Enabled** — Enables the anti-passback feature. **Hard** — Validates IN/OUT status before allowing entry. A second swipe of the card at the same type of reader (IN/OUT) causes a Hard anti-passback violation and the user is denied entry. **Soft** — Validates IN/OUT status before allowing entry. A second swipe of a card at the same type of reader (IN/OUT) causes a Soft anti-passback violation but the user is allowed entry. **Out** — Applies to readers located inside the anti-passback-controlled area. Card holders use these readers when attempting to exit the anti-passback-controlled area. **Note:** With anti-passback, limited use and trace cards do not apply. **In** — Applies to readers located outside the anti-passback-controlled area. Card holders use these readers when attempting to enter the anti-passback-controlled area.
Duress Output	Configures the output that will trip when a card holder enters a "duress PIN" at a keypad/card reader. A duress PIN is the PIN a user enters at a keypad when being forced (for example, during a robbery) to open a door. The card holder enters a PIN that is either one number higher or lower than the correct PIN. This PIN opens the door, but it also triggers the designated duress output and produces an alarm event. For example, if the PIN is 2222, the card holder would enter either 2221 or 2223. Even though the PIN is incorrect, the door will still open normally, but the duress output pulses and an alarm is generated. In this way, the card holder notifies others without detection by the unauthorized person. **Note:** A PIN ending in 0 (for example, 2320) will only trip a duress output when a 1 is used in place of the 0 (for example, 2321). The duress output feature requires the following: • "Duress" must be enabled on the **Configuration > System > General** tab. • A time zone must be selected for "Card and PIN" on the **Configuration > Doors > Reader** tab.

Note: Should a conflict arise among the time zones set in the Access Mode Time Zones box on the Reader > General tab, priority is given to the time zone that is highest in the list of time zones displayed on the tab. Therefore, the Disabled time zone has highest priority, and the Card Only time zone has lowest priority.

Note: The access mode defined here for the door can be overridden by a card assigned with a VIP card type. (See Adding New Cards, page 50 for information about assigning a VIP card type.)

2. Click **Card Formats** at the side of the tab. A card format tells the panel how the card number will be read. The panel supplies the format to the card readers. Then, the card readers can correctly read the card.

Figure 18: *Configuration > Doors > Reader > Card Formats Tab*



General
Card Formats

Formats Recognized by Reader 1

Double-click on a format name to display or edit its data layout

Available:
- Default 32 Bit Wiegand
- 35 Bit Corporate 1000
- Default 25 Bit Wiegand
- Default 29 Bit Wiegand
- Default 37 Bit Wiegand
- Default 75 Bit Wiegand

Selected:
- Default 26 Bit Wiegand
- Default 34 Bit Wiegand

3. Use the descriptions in Table 6 to select card formats.

Table 6: *Configuration > Doors > Reader > Card Format Fields*

Setting	Description
Available (column)	Lists all the formats in the panel. All formats, new ones as well as the eight default formats, are listed under Available. This information allows all readers by default to use all formats to try and decipher card reads. The reader will then use every Available format(s) to decipher incoming card reads. Any cards swiped with formats that do not match the Available format(s) are then reported as an Invalid Format event.
Selected (column)	Lists specific formats selected by the user from the Available list that the reader should use to decipher card reads. As soon as a single format is placed in the Selected column, the reader begins to use only the selected format, ignoring any unselected formats in the Available list. Cards swiped with formats that do not match the Selected format(s) are then reported as an Invalid Format event, even if the format is in the Available list. This selection is on a per reader basis--that is, each reader can have its own selected formats. Selections at one reader do not affect another reader.

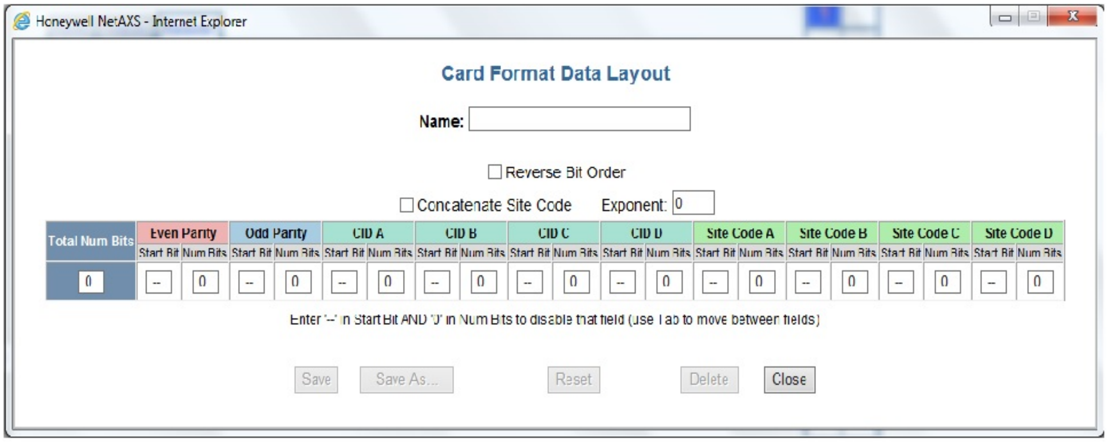
Note: The user should never add in more than one format using the same number of bits. If you need more information, please contact Technical Support.

4. Click to highlight each desired card format listed in the Available box, and click the green right arrow ⏩ button to move the format(s) into the Selected box.

Note: If you select no formats, the reader will function in legacy mode and the reader interprets the panel's formats. If you select a subset of formats for a given reader, the reader will interpret only those formats and ignore formats that are not selected.

5. Click **Submit Changes**.

6. If you want to create a new card format, click the **New Format** button to display an empty Card Format Data Layout screen:



Card Format Data Layout

Name:

□ Reverse Bit Order

□ Concatenate Site Code   Exponent: 0

Total Num Bits	Even Parity		Odd Parity		CID A		CID B		CID C		CID D		Site Code A		Site Code B		Site Code C		Site Code D	
	Start Bit	Num Bits	Start Bit	Num Bits	Start Bit	Num Bits	Start Bit	Num Bits	Start Bit	Num Bits	Start Bit	Num Bits	Start Bit	Num Bits	Start Bit	Num Bits	Start Bit	Num Bits	Start Bit	Num Bits
0	--	0	--	0	--	0	--	0	--	0	--	0	--	0	--	0	--	0	--	0

Enter '--' in Start Bit AND '0' in Num Bits to disable that field (use Tab to move between fields)

7. Use the field descriptions given in Table 7 to define the layout and click **Save**.

Note: To disable a field, enter "--" in the Start Bit box and "0" in the Num Bits box.

Table 7: *Configuration > Doors > Reader > Card Format Fields*

Setting	**Description**
Name	Displays the name by which the format will be listed in the Card Formats tab. The name is user-defined.
Reverse Bit Order	Returns the message from the reader in reverse bit order (least significant bit first and most significant bit last).

Table 7: *Configuration > Doors > Reader > Card Format Fields* (continued)

Setting	Description
Concatenated Site Code	When enabled, it is used with the Exponent field to combine the site code and Card ID into a new unique number. Mainly used when a site requires the use of more than 8 different site codes.
Exponent	This option is available only when the Concatenate Site Code box is checked. To generate a card's new ID, use this box to insert the desired number of zeroes to be added to the right-hand side of the Site Code value. Then add the card ID to calculate the card's new ID. For example, a 26-bit card has a site code of 123 and the card ID is 637. When the Concatenate Site Code is enabled with an exponent of 4, 4 zeroes are added to the right-hand side of the site code. The result is a final value of 1230000. This newly modified site code value is then added to the number that the panel has read as the card's ID — that is, 1230000 + 637 = 1230637. The newly combined number becomes the card's new ID value.
Total Num Bits	Lists the total number of bits on the card.
Even Parit	Lists where on the card that even parity is being observed. **Start Bit** – First bit in the card where even parity begins. **Num Bits** – Number of bits to the right of the start bit, including the start bit, to include in the even parity check.
Odd Parity	Lists where on the card that odd parity is being observed. **Start Bit —** first bit in the card where odd parity begins. **Num Bits** — Number of bits to the right of the start bit, including the start bit, to include in the odd parity check.
CID A	Lists where on the card the Card ID A is listed. **Start Bit** — first bit in the card where card ID begins. **Num Bits** — Number of bits to the right of the start bit, including the start bit, that comprise the card ID. Most formats require only CID A, and not CID B, C, or D.
CID B	Lists where on the card the Card ID B is listed. **Start Bit** — first bit in the card where card ID begins. **Num Bits** — Number of bits to the right of the start bit, including the start bit, that comprise the card ID. Most formats require only CID A, and not CID B, C, or D.
Card ID C	Lists where on the card the Card ID C is listed. **Start Bit** — first bit in the card where card ID begins. **Num Bits** — Number of bits to the right of the start bit, including the start bit, that comprise the card ID. Most formats require only CID A, and not CID B, C, or D.

Table 7: *Configuration > Doors > Reader > Card Format Fields* (continued)

Setting	Description
Card ID D	Lists where on the card the Card ID D is listed. **Start Bit** — first bit in the card where card ID begins. **Num Bits** — Number of bits to the right of the start bit, including the start bit, that comprise the card ID. Most formats require only CID A, and not CID B, C, or D.
Site Code A	Lists where on the card the Site Code A is listed. Consult the card manufacturer for detail on the card detail. **Start Bit** — first bit in the card where the card's Site Code begins. **Num Bits** — Number of bits to the right of the start bit, including the start bit, that comprise the Site Code. Most card formats require only Site Code A.
Site Code B	Lists where on the card the Site Code B is listed. Consult the card manufacturer for detail on the card detail. **Start Bit** — first bit in the card where the card's Site Code begins. **Num Bits** — Number of bits to the right of the start bit, including the start bit, that comprise the Site Code. Most card formats require only Site Code A.
Site Code C	Lists where on the card the Site Code C is listed. Consult the card manufacturer for detail on the card detail. **Start Bit** — first bit in the card where the card's Site Code begins. **Num Bits** — Number of bits to the right of the start bit, including the start bit, that comprise the Site Code. Most card formats require only Site Code A.
Site Code D	Lists where on the card the Site Code D is listed. Consult the card manufacturer for detail on the card detail. **Start Bit** — first bit in the card where the card's Site Code begins. **Num Bits** — Number of bits to the right of the start bit, including the start bit, that comprise the Site Code. Most card formats require only Site Code A.

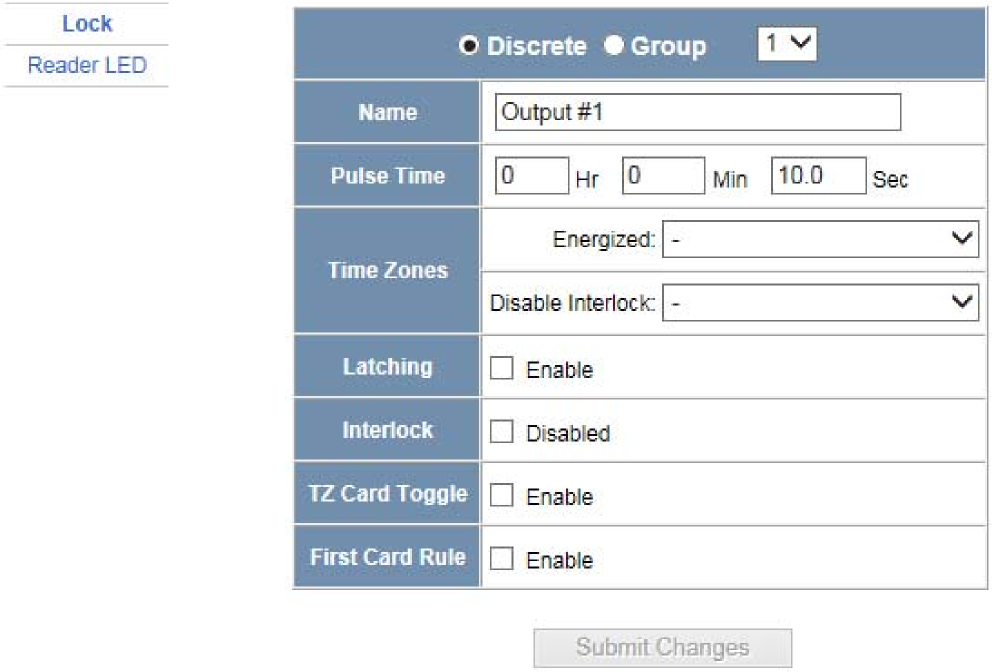
7. If you want to change an existing card format's data layout, double-click the format's name on the list of existing formats to display the Card Format Data Layout screen. Use the descriptions in the table above to edit the layout's fields. Then, click **Update** (to save in the format's current name) or **Save as** (to save with a different format name) to save the edited format. To return to the default settings for the card format, click **Reset**. To delete the card format, click **Delete**.

2.4.2 Outputs Tab

An output, or output relay, is a switch on the panel that either energizes or de-energizes or pulses an output device, such as a door lock or an LED. For example, a successful card read at a reader (input device) causes the output relay switch on the panel board to change the normal state of a door lock (output device), so that the normally locked door strike releases and permits entry. This tab configures the lock and reader LED output relays, either as individual (discrete) outputs or groups of outputs.

Click the **Outputs** tab. The Lock > Discrete tab window appears, enabling you to configure an individual lock output. Select the output number in the dropdown list at the top of the screen. Note that lock and reader LED outputs are associated with each of the four doors on a NetAXS® panel.

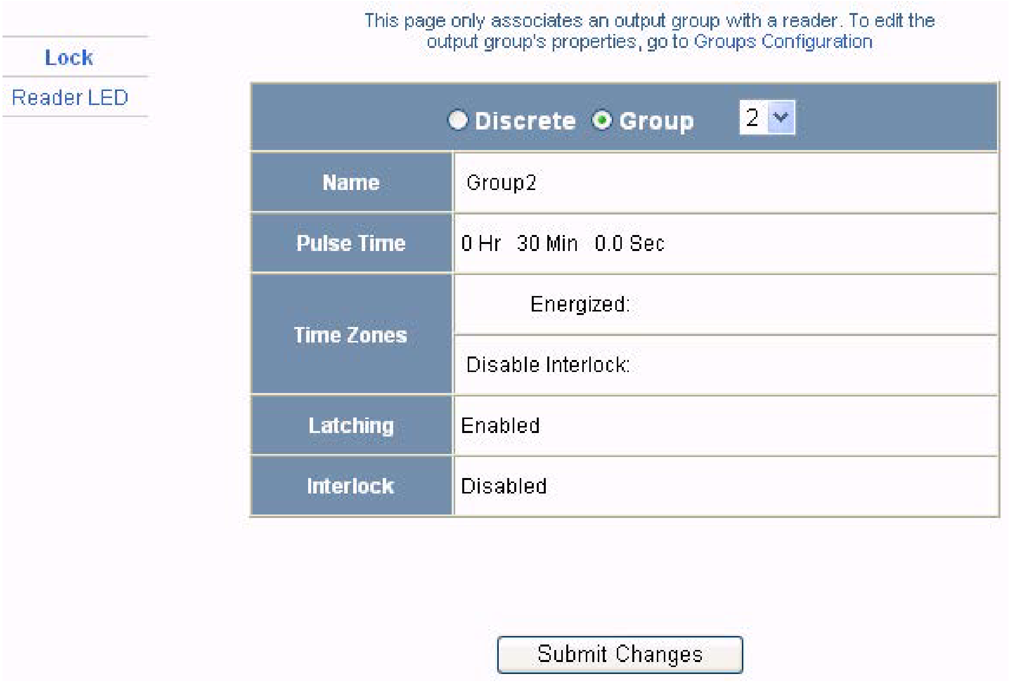
Figure 19: *Discrete Lock Output Configuration*



● Discrete ● Group	1
Name	Output #1
Pulse Time	0 Hr 0 Min 10.0 Sec
Time Zones	Energized: - Disable Interlock: -
Latching	□ Enable
Interlock	□ Disabled
TZ Card Toggle	□ Enable
First Card Rule	□ Enable

To view a configuration of a group of outputs, click **Group** and select the group number from the dropdown list at the top of the screen. The group configuration appears. Note that you can only view the group configuration from this screen. To edit the Group configuration, click **Configuration > Other I/O & Groups** in the side panel.

Figure 20: *Configuration > Doors > Outputs > Group Tab > Lock*

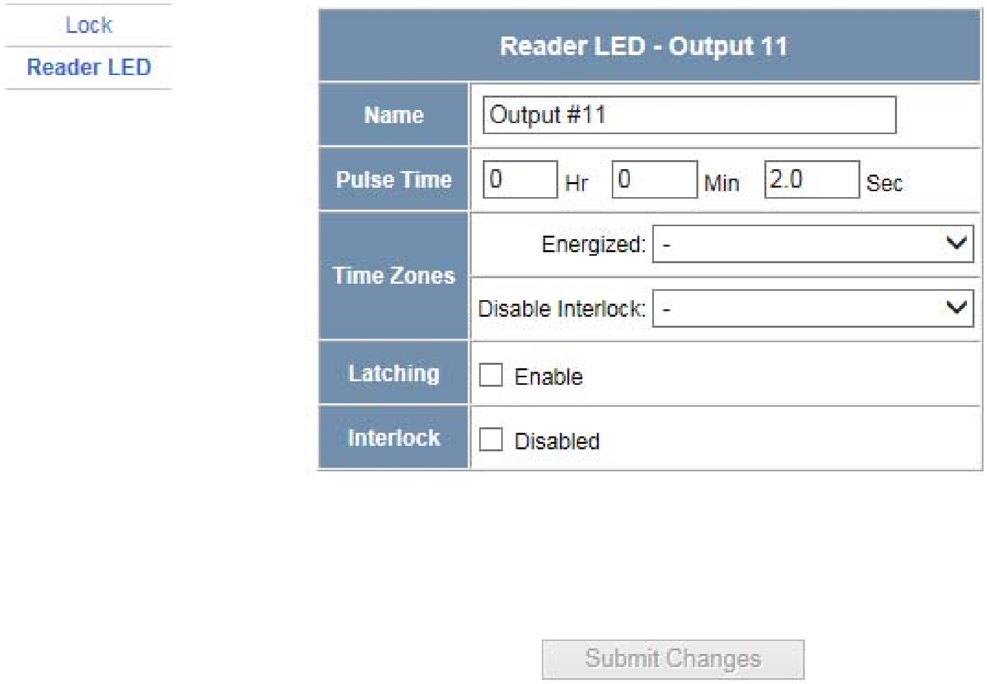


This page only associates an output group with a reader. To edit the output group's properties, go to Groups Configuration

○ Discrete ● Group 2

Name	Group2
Pulse Time	0 Hr 30 Min 0.0 Sec
Time Zones	Energized:
	Disable Interlock:
Latching	Enabled
Interlock	Disabled

The LED Reader dialog box enables you to configure the Reader LED:



Reader LED - Output 11

Name	Output #11	
Pulse Time	0 Hr 0 Min 2.0 Sec	
Time Zones	Energized:	-
	Disable Interlock:	-
Latching	□ Enable	
Interlock	□ Disabled	

The Outputs tab enables you to:

- Configure the following for each of the door's output locks and reader LEDs:
  - Name
  - Pulse time
  - Time zones
  - Latching
  - Interlock
  - Time zone card toggle
  - First card rule

Steps: Use the descriptions in Table 8 to configure each individual lock or Reader LED:

Table 8: *Configuration > Doors > Output Tab Field Descriptions*

Setting	Description
Name	Enter a unique name to identify the device.
Pulse Time	Specifies the duration for which the device will assume abnormal status. For example, it specifies how long a horn will sound or a door strike will remain released. The maximum number of hours is 1. When the hour field is blank, the maximum number of minutes is 59. When 1 is entered in the hour field, the maximum number of minutes is 45 and the maximum number of seconds is 59.9. The sum of all three units comprises the pulse time. Note that you can express seconds in tenths of a second.
Time Zones	Specifies two schedules: • **Energized** — sets the period during which the output switches are automatically energized. • **Disable Interlock** — sets the period during which the interlock, a programmed interaction between selected inputs, outputs and groups will be disabled. During the selected Time Zone this point ignores all interlock actions to it, effectively disabling it from being a Reacting Component during the Time Zone. Outside of the Time Zone the point will react to interlocks as expected.
Latching	When selected, this toggles a relay with either a valid card, interlock, or manual pulse.
Interlock	Enables you to disable the interlock, or programmed interaction between two points. When enabled, this point ignores all interlock actions to it, effectively disabling it from being a Reacting Component.
TZ Card Toggle	Requires, like the First Card Rule, a valid card read within the time zone to enable the time zone (period in which doors are unlocked) to take effect. Unlike the First Card Rule, however, the user can swipe the card a second time to return the doors to a locked state. Note that both TZ Card Toggle and First Card Rule cannot be enabled at the same time.
First Card Rule	Requires a valid card read within the time zone to enable the time zone (period in which doors are unlocked) can take effect. Note that both TZ Card Toggle and First Card Rule cannot be enabled at the same time.

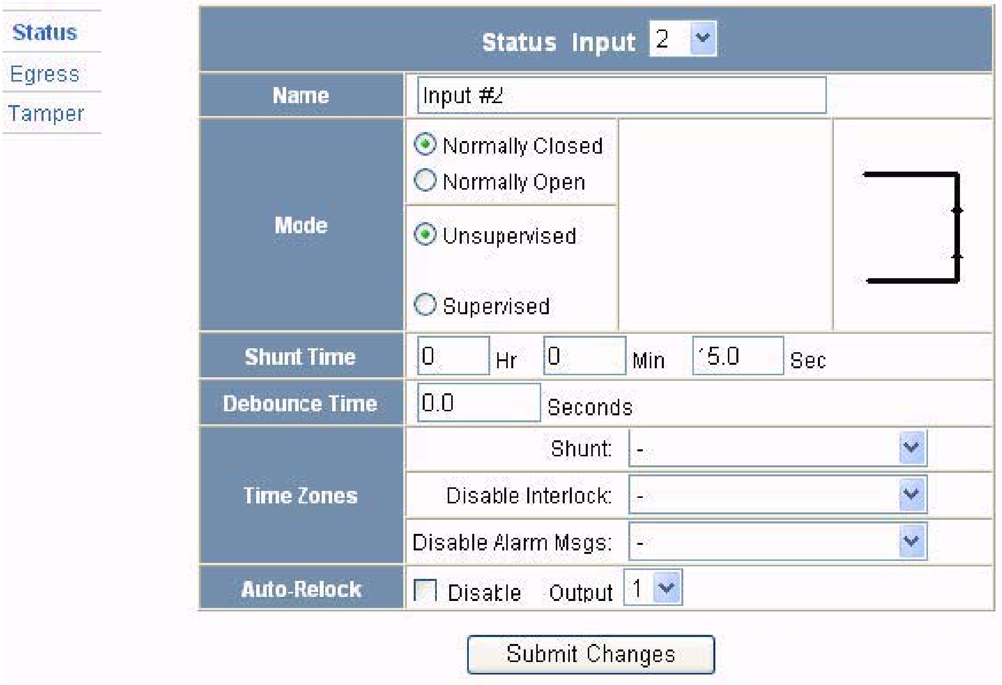
2.4.3 Inputs Tab

Three inputs are associated with each of the four doors on a NetAXS® panel:

- Status — Provides the following door status information.
- Egress — Allows the door to open or close normally without generating an alarm.
- Tamper — Reports abnormal handling of the reader device or wiring.

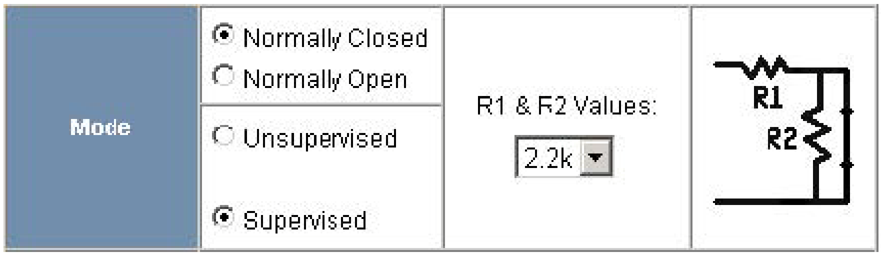
Click to display the **Inputs** tab:

Figure 21: *Configuration > Doors > Inputs Tab*

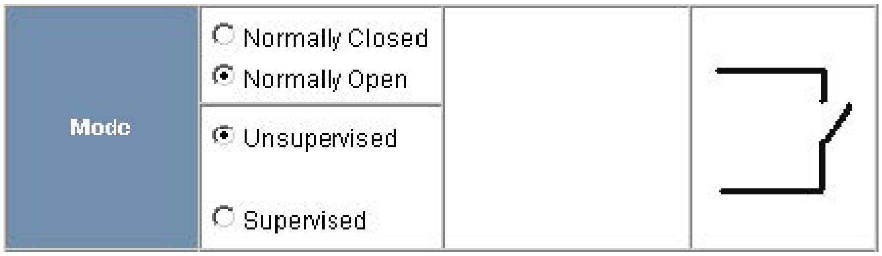


Status Input	2
Name	Input #2
Mode	● Normally Closed ○ Normally Open ● Unsupervised ○ Supervised
Shunt Time	0 Hr 0 Min 15.0 Sec
Debounce Time	0.0 Seconds
Time Zones	Shunt: - Disable Interlock: - Disable Alarm Msgs: -
Auto-Relock	□ Disable Output 1

Note that there are four possible Mode configurations. Shown in the screen above is the Normally Closed/Unsupervised Mode. The following screens show the remaining modes:



Mode	
	● Normally Closed ○ Normally Open ○ Unsupervised ● Supervised
R1 & R2 Values:	2.2k

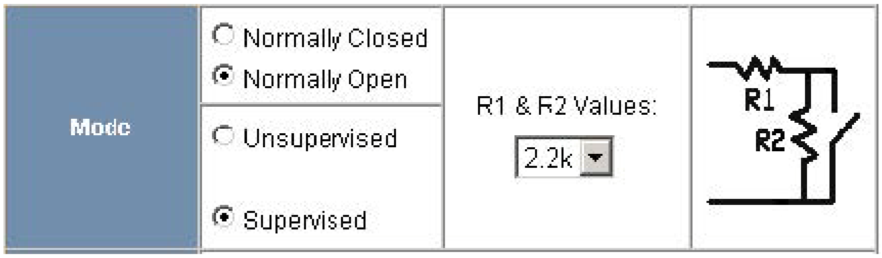


Mode

○ Normally Closed
● Normally Open

● Unsupervised

○ Supervised



Mode

○ Normally Closed
● Normally Open

○ Unsupervised

● Supervised

R1 & R2 Values: 2.2k

The Inputs tab enables you to:

- Define the Status, Egress, and Tamper inputs' access modes.
- Specify the Status, Egress, and Tamper shunt time, or the period of time the door's normal state will be ignored.
- Specify the Status, Egress, and Tamper debounce time, or the period of time the input must remain in its new state before it is recognized as being in the new state.
- Specify the time zones for the Status, Egress, and Tamper inputs.
- Enable or disable Auto-Relock for the Status inputs.

Steps: Use the descriptions in Table 9 to configure the Status, Egress, and Tamper inputs, then click **Submit Changes**:

***Table 9:** Configuration > Doors > Inputs Tab Field Descriptions*

Setting	Description
Mode Name	**Normally Closed** — Specifies that the input's normal state is closed (default). **Normally Open** — Specifies that the input's normal state is open. **Unsupervised** — Specifies that the input's electrical circuit is wired in one path without alternative paths supervised by resistors (default). **Supervised** — Specifies that the input's electrical circuit is wired with alternative paths supervised by resistors. **R1 & R2 Values** — Specifies the resistor values being used in the supervised modes. The drop-down menu lists the following values: 1K ohms, 2.2K ohms, 4.7K ohms, or 10K ohms. The default is 2.2K.
Shunt Time	Specifies the amount of time for which the inputs will be shunted, or de-activated. The maximum number of hours is 1. When the hour field is blank, the maximum number of minutes is 59. When 1 is entered in the hour field, the maximum number of minutes is 45 and the maximum number of seconds is 59. The sum of all three units comprises the shunt time. Note that you can express seconds in tenths of a second.
Debounce Time	Specifies the period of time the input must remain in a new state before generating an alarm. For example, with a 5-second debounce time selected, if a Normal state is changed to Alarm, the state must remain in Alarm for five consecutive seconds before an alarm is generated. The allowable range for debounce time is 0 to 6553.5 seconds.
Time Zones	**Shunt** — Specifies the time period during which the input will be ignored. **Disable Interlock** — Specifies the time period during which the programmed action on this input from another point will be disabled. **Disable Alarm Msgs** — Specifies the time period during which Alarm and Normal will not be reported, but Short and Cut will be reported.
Auto-Relock	Causes the door to re-lock immediately when the door status switch closes after entry. The output relay that controls the door strike de-energizes when the associated input returns to normal state instead of remaining energized for the duration of the pulse time. To enable Auto-Relock, de-select the **Disable** checkbox, and select the associated output from the drop down list.

2.5 Configuring Access Levels

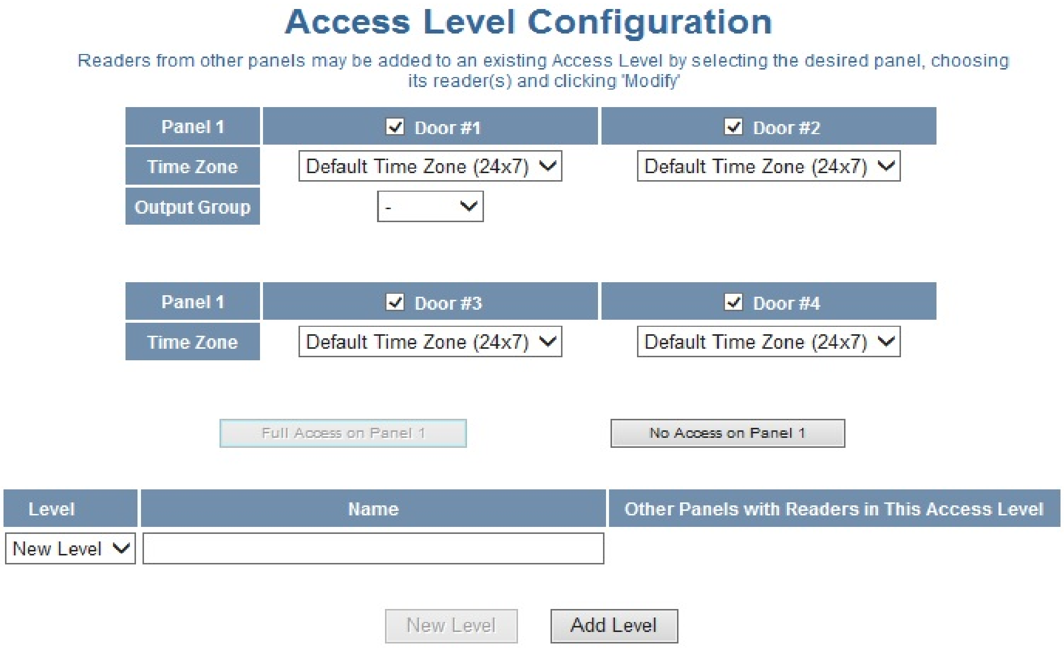
Every card is assigned an access level. The access level specifies the time zone, or time schedule, during which the card holder can be granted access at a specific door. For example, an access level embedded in an employee's card might allow the employee to enter the facility only through door 2 from 6:00 a.m. to 6:00 p.m., Monday through Friday.

This section explains how to create the access levels that subsequently can be assigned to cards.

Note: Since an access level is defined by door and time zone configurations, you must configure the door (see Configuring the Doors, page 33) and the time zone (see Configuring Time Management, page 26) before configuring an access level.

Click **Access Levels** to display the Access Level Configuration screen:

Figure 22: *Configuration > Access Levels*



Access Level Configuration

Readers from other panels may be added to an existing Access Level by selecting the desired panel, choosing its reader(s) and clicking 'Modify'

Panel 1	☑ Door #1	☑ Door #2
Time Zone	Default Time Zone (24x7)	Default Time Zone (24x7)
Output Group	-	

Panel 1	☑ Door #3	☑ Door #4
Time Zone	Default Time Zone (24x7)	Default Time Zone (24x7)

Level	Name	Other Panels with Readers in This Access Level
New Level		

The group drop-down is available if groups are added to panel or not. However, the drop down is not populated until group(s) is added. For more details on groups see Configuring Other I/O & Groups Tab, page 55.

Note: Output Groups are only selectable on Door 1.

The Access Levels screen enables you to:

- Create an access level.
- Modify an access level.
- Delete an access level.
- Set a Time Zone for each door.

Steps to create an access level:

1. Select the door(s). The access level will allow access only at the door(s) you select here.
2. Enter the name of the access level in the **Name** field. This should be a unique name that identifies the general user group.
3. Select the time zone you want from the drop down list in the **Time Zone** field. The access level will allow access to the card holder only during this time zone.
4. Click the **Add Level** button.

Steps to assign a Time Zone to a door:

1. Select the checkbox next to the door you desire. The Time Zone field appears.
2. From the Time Zone dropdown list, select the Time Zone you want to assign to the door. Note that a Time Zone must be configured in **Configuration > Time Management** before it appears in the dropdown list.

Steps to modify an access level:

1. From the drop down list in the Level field, select the number of the access level you want to modify.
2. Make the desired modifications.
3. Click the **Modify** button.

Steps to delete an access level:

1. Select the number of the access level you want to delete from the drop down list in the **Level** field.
2. Click the **Delete** button.
3. Click **OK** at the prompt to delete the access level.

⚠ Note that when you create an access level for a panel in a loop configuration, you must manually configure this access level at each panel in the loop. For example, suppose you have three panels in a loop, and you add a Master Access level to panel 1 and you configure readers 1-4 on panel 1 with this access level. When you save the access level configuration at panel 1, the access level is automatically copied to panels 2 and 3. However, the readers at panels 2 and 3 are not yet configured. So you still must go to panels 2 and 3 to assign the access level to the readers at these panels. To do this, navigate back to the Select Panel on the NetAXS® main screen, select the next panel in the loop, and configure that panel's doors according to the instructions in this section.

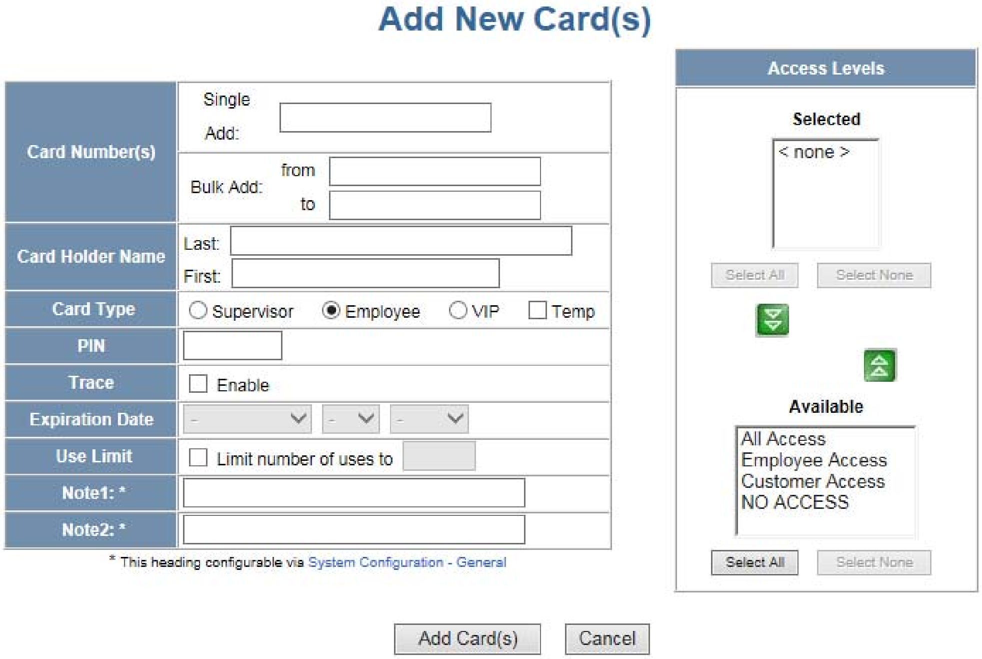
2.6 Maintaining Cards

A card is encoded with a unique number and the card holder's rights to access NetAXS® system resources. For example, in addition to its unique number, a card would allow the card holder to be granted access to certain doors during a certain time of day.

2.6.1 Adding New Cards

Click **Cards > Add Card(s)** to display the Add New Card(s) screen:

Figure 23: *Cards > Add Cards*



Add New Card(s)

Card Number(s)	Single Add: ____ Bulk Add: from ____ to ____
Card Holder Name	Last: ____ First: ____
Card Type	○ Supervisor ● Employee ○ VIP □ Temp
PIN	____
Trace	□ Enable
Expiration Date	- - -
Use Limit	□ Limit number of uses to ____
Note1: *	____
Note2: *	____

* This heading configurable via System Configuration - General

Access Levels

Selected: < none >

Available: All Access, Employee Access, Customer Access, NO ACCESS

The Add New Card(s) screen enables you to:

- Create cards encoded with the following information:
  - Card number(s)
  - Card holder name (first and last names)
  - Card type
  - Personal Identification Number (PIN)
  - Trace capability
  - Expiration date
  - Use limits
  - Card holder note 1
  - Card holder note 2
  - Access levels

Steps: Use the field descriptions in Table 10 to complete the card fields and click **Add Card(s):**

Table 10:*Cards > Add Cards Field Descriptions*

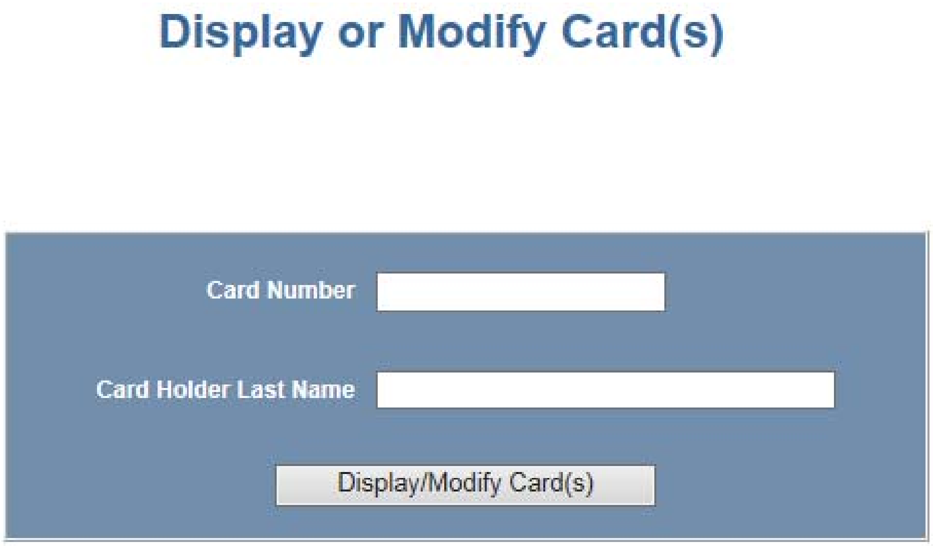
Field	Description
Card Number(s)	Specifies the unique number by which the card holder will be identified. A card number is required. Up to a 20-digit card number can be entered (64-bit) with a maximum value of 18446744073709551615.
Card Holder Name	Identifies the card holder. A card holder first and last name is required. Each name can have up to 15 characters for the first name and 20 characters for the last name.
Card Type	Specifies whether the card holder is a Supervisor, Employee, or a VIP. A temporary (Temp) flag can be set for each type of card holder. When the Temp flag is enabled, the expiration date becomes an active field. Note that the Temp box is active when the panel is configured for visitor cards in **Configuration > System > General** (see General Tab, page 13). A card type is required. Once a VIP card is added to the database it can gain access to any door regardless of the access level. VIP card can also bypass Displays, Anti-Passback, Disabled Reader Mode, Duress, Limited Use, Lockdown Reader Mode, Site Code, and Temporary Use.
PIN	Specifies the Personal Identification Number (PIN) for the card holder. A PIN is optional; however, if the door reader is configured to require PIN identification (see Reader Tab, page 33), then you must create a PIN for the card holder here. The PIN number has a maximum of six digits. Preceding zeros are allowed in a PIN number.
Trace	Sends an alarm message to the alarm monitor whenever a card with trace enabled is presented at a reader. This feature provides a trace of the cardholder's path through the facility.
Expiration Date	Specifies the date that a temporary card is de-activated.
Use Limits	Specifies the number of times a card may be read at a card reader to which it has valid access. Specify the number-of-uses limit as the number of times access may be granted. A maximum of 255 uses is allowed.
Note 1	Provides a user-defined field. See Configuring the System, page 10 for information about how this field is defined for the Add New Card template.
Note 2	Provides a user-defined field. See Configuring the System, page 10 for information about how this field is defined for the Add New Card template.
Access Levels	Specifies the time zone or time schedule during which the card holder can be granted access at a specific reader. A card may support more than one access level. Should two or more access levels have overlapping times on a card; the card will reflect a combination of the selected access levels. For example, Card 12345 is given Access Levels 1 and 2. Access Level 1 is Monday to Friday 9 a.m.-5 p.m. and Access Level 2 is Monday to Saturday 3 p.m.-11 p.m. When these times are combined, card 12345 provides access Monday to Friday 9 a.m.-11 p.m. and Saturday 3 p.m.-11 p.m.

2.6.2 Displaying and Modifying Cards

Use this function to display specified cards and modify them.

Click **Cards > Card Data** to display the search screen with which you can find and display specified cards.

Figure 24: *Cards > Card Data*



The Display or Modify Card(s) screen enables you to:

- Display cards by searching on any of the following keys:
  - Card number
  - Card holder’s last name
- Modify the displayed card(s)

Steps:

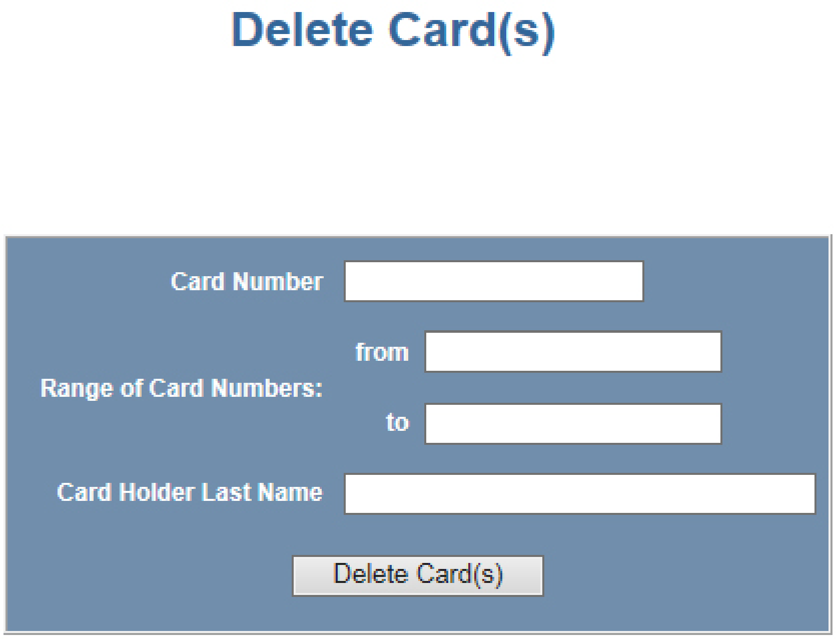
1. Enter a value for either of the search keys (card number or cardholder last name).
2. Click the **Display/Modify Card(s)** button. The cards specified in step 1 appear.
3. Use the field descriptions given in Table 9 on page 51 to complete the card fields and click **Submit Modification(s).**

Note: If no card is specified, the screen displays a list of all cards in the system.

2.6.3 Deleting Cards

Click **Cards > Delete Card(s)** to display the Delete Cards screen:

Figure 25: *Cards > Delete Cards*



The Delete Card(s) screen enables you to:

- Delete cards retrieved by any of the following keys:
  - Card number
  - Range of card numbers
  - Card holder's last name

Steps:

1. Enter a value for any of the search keys (card number, card number range, or cardholder name).
2. Click **Delete Card(s)** to delete all cards matching the search keys you entered.
3. Click **OK** at the prompt to delete the card.

2.6.4 Displaying Reports

Use this function to display a report of all cards and card data. You can display the cards either by the cardholder's last name or by the card number.

Click **Cards > Reports** to display the Card Reports screen.

The Card Reports screen enables you to:

- View card records by the cardholder's last name.
- View card records by the cards' numbers.

Steps:

1. Click the By Name tab to display the card records by the cardholders' last names.
2. Click the By Number tab to display the card records by the cards' numbers.

Note: The card report shows only the leftmost side of the display. This screen is very wide, so use the scroll bar across the bottom to access the remaining columns on the right.

3. Use the descriptions given in Table 11 to read the card records (see Adding New Cards, page 50 for more information about card data):

Table 11: *Cards > Reports Field Descriptions*

Field	**Description**
Card Number	Shows the card number.
Last	Shows the cardholder's last name.
First	Shows the cardholder's first name.
PIN	Shows the Personal Identification Number (PIN) for the card holder. The PIN number has a maximum of six digits.
Access Level	Shows the access level(s) configured for the cardholder. An access level specifies the time zone, or time schedule, during which the card holder can be granted access at a specific door. See Configuring Access Levels, page 48 for more information about access levels. To determine an access level's defined hours, click **Configuration > Access Levels** to display the Access Level Configuration screen.
Type	Shows the card type. The card type specifies whether the card holder is configured as a supervisor (Supervisor), employee (Employee), a VIP (VIP).

***Table 11:** Cards > Reports Field Descriptions* (continued)

Field	Description
Temp	Indicates (with a check mark) that the card is a temporary card.
Activation Date	Shows the date the card was activated.
Expiration Date	Shows the date the card expires.
Use Limit	Indicates the number of times the card will be granted access.
APB State	Indicates whether or not anti-passback is enabled on the card.
Note 1	Displays informational text that may have been entered in the Note 1 field.
Note 2	Displays informational text that may have been entered in the Note 2 field.

2.7 Configuring Other I/O & Groups Tab

The NetAXS® panel provides up to 14 inputs and eight outputs. Two of the inputs and four of the outputs are "other" inputs and outputs, because you can use them for other than door lock/unlock functions. This section explains how to configure these other inputs, outputs, and groups (for pulse and time zone).

2.7.1 Inputs Tab

This tab enables you to configure other input devices on inputs 13 and 14 on Terminal Block 8, and on the inputs on downstream NX4IN boards daisy-chained to Terminal Block 10. The downstream inputs are numbered 25-96.

Note: The NetAXS® panel supports two downstream board types:

- NX4IN — Provides 32 inputs and no outputs.
- NX4OUT — Provides two inputs and 16 outputs.

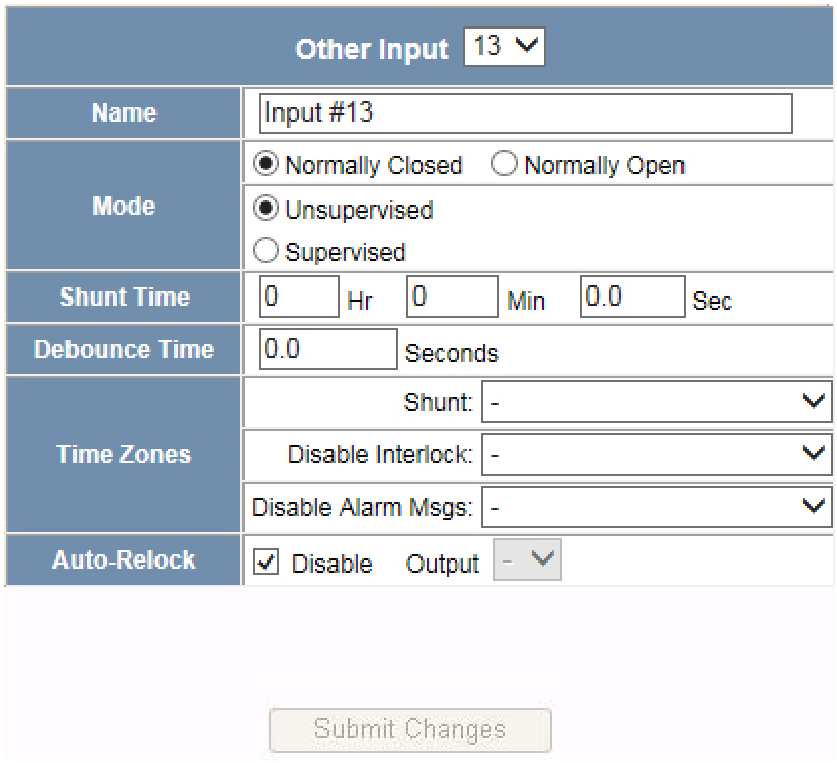
A NetAXS® panel supports a maximum of six daisy-chained downstream boards — two NX4IN boards and four NX4OUT. An NX4IN module has 32 supervised, four-state inputs that are limited to 2.2K ohms resistance. The NX4OUT has two supervised inputs and 16 SPDT relay outputs; each input is limited to 2.2K ohms resistance. Each board is configured with a unique address in the **Configuration > System > Downstream Devices** tab (see Downstream Devices Tab, page 25).

On panels with internal power supply, the Power Fail input generates an alarm when primary power is lost as indicated by the power supply. The Panel Tamper input generates an alarm when the NetAXS® cabinet has been forced open. The Downstream inputs are available for general use.

Note: You can also configure the Power Fail and the Panel Tamper inputs for general use, if you choose not to wire them for power and tamper detection.

Click **Inputs** to display the Inputs screen:

Figure 26: *Configure > Other I/O & Groups > Inputs Tab*



Other Input 13

Name	Input #13
Mode	● Normally Closed ○ Normally Open ● Unsupervised ○ Supervised
Shunt Time	0 Hr 0 Min 0.0 Sec
Debounce Time	0.0 Seconds
Time Zones	Shunt: - Disable Interlock: - Disable Alarm Msgs: -
Auto-Relock	☑ Disable Output -

The Input tab enables you to:

- Configure the mode, debounce time, and time zones for another input (input 13 and input 14).
- Configure the mode, shunt time, debounce time, time zones, and auto-relock for the downstream inputs provided by downstream input/output boards (NX4IN or NX4OUT).

Steps: Use the descriptions in Table 12 to configure other panel inputs and downstream inputs:

Table 12: *Configuration > Other I/O & Groups > Inputs Tab Field Descriptions*

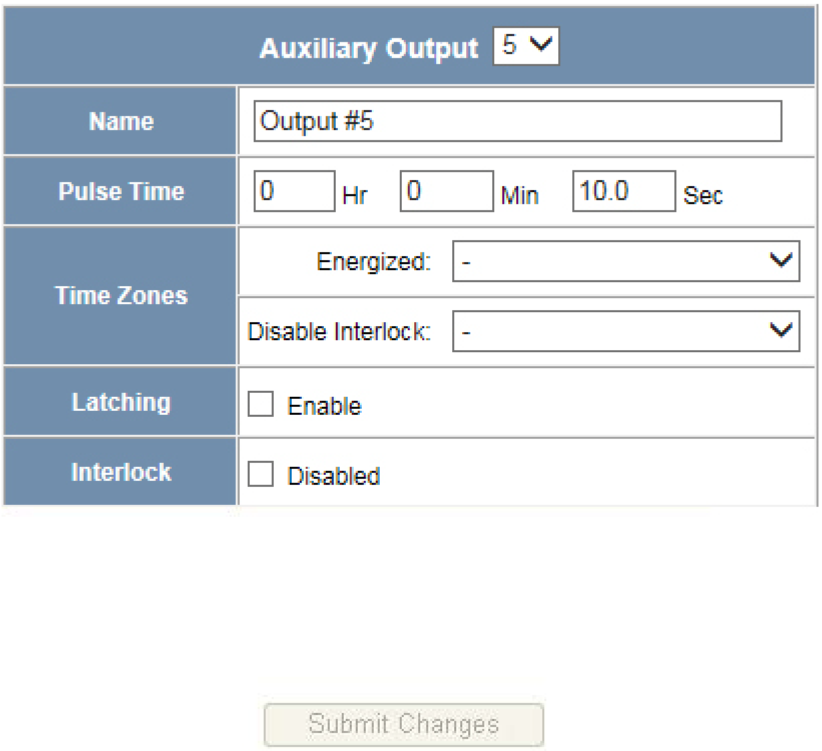
Setting	Description
Name	Enter a unique name to identify the device up to 25 characters.
Mode	**Normally Closed** — Specifies that the input's normal state is closed. **Normally Open** — Specifies that the input's normal state is open. **Unsupervised** — Specifies that the input's electrical circuit is wired in one path without alternative paths supervised by resistors. **Supervised** — Specifies that the input's electrical circuit is wired with alternative paths supervised by resistors.
Shunt Time	Specifies the amount of time for which the inputs will be shunted, or de-activated. The maximum number of hours is 1. When the hour field is blank, the maximum number of minutes is 59. When 1 is entered in the hour field, the maximum number of minutes is 45. The sum of all three units comprises the shunt time. Note that you can express seconds in tenths of a second.
Debounce Time	Specifies the period of time the input must remain in a new state before generating an alarm. For example, if a Normal state is changed to Alarm and the Debounce time is set to 5.0, the state must remain in Alarm for five seconds before an alarm is generated.
Time Zones	**Shunt** — Specifies the time period during which the input will be ignored. **Disable Interlock** — Specifies the time period during which the programmed action on this input from another point will be disabled. During the selected Time Zone, this point ignores all interlock actions to it, effectively disabling it from being a Reacting Component during the Time Zone. Outside of the Time Zone the point will react to interlocks as expected. **Disable Alarm Msgs** — Specifies the time period during which "Alarm" and "Normal" will not be reported, but "Short" and "Cut" will be reported.
Auto-Relock	Causes the door to re-lock immediately when the door status switch closes after entry. The output relay that controls the door strike de-energizes when the associated input returns to normal state instead of remaining energized for the duration of the pulse time. To enable Auto-Relock, de-select the **Disable** checkbox, and select the associated output from the drop down list.

2.7.2 Outputs Tab

This tab enables you to configure the four NetAXS® auxiliary outputs (outputs 5-8) that are physically located on the panel board, and the outputs on downstream NX4OUT boards daisy-chained to Terminal Block 10. A NetAXS® panel supports a maximum of four NX4OUT boards, and each board provides two inputs and 16 outputs. The downstream outputs are numbered 17-80.

Click **Outputs** to display the Auxiliary Output screen for the on-board outputs:

Figure 27: *Configure > Other I/O & Groups > Outputs Tab*



Auxiliary Output 5

Name	Output #5
Pulse Time	0 Hr 0 Min 10.0 Sec
Time Zones	Energized: -
	Disable Interlock: -
Latching	□ Enable
Interlock	□ Disabled

The Outputs tab enables you to:

- Configure the following for each of the auxiliary outputs — on board the panel as well as downstream:
  - Name
  - Pulse Time
  - Time Zones
  - Latching
  - Interlock

Steps: Use the descriptions in Table 13 to configure each output device:

Table 13: *Configuration > Other I/O & Groups > Outputs Tab > Fields*

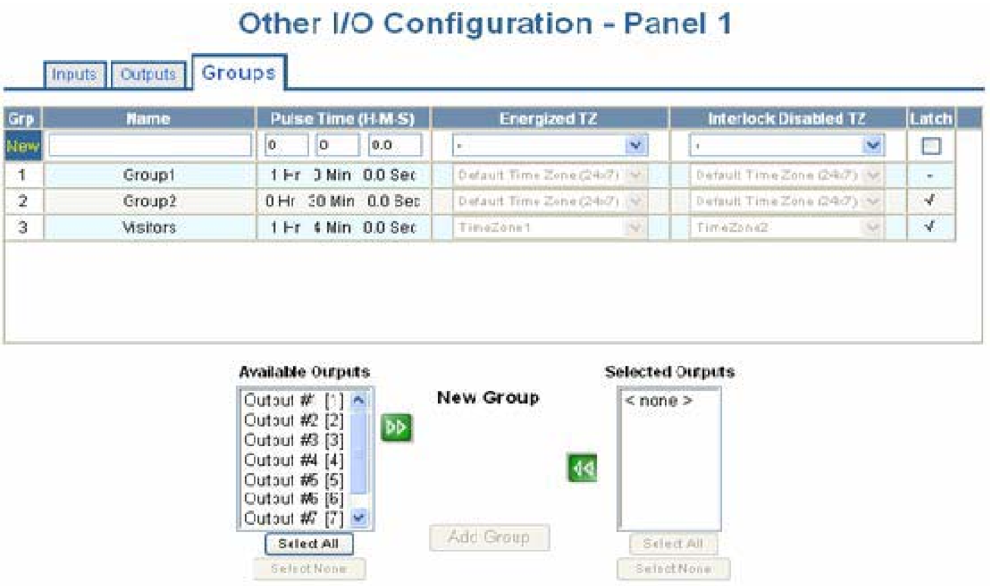
Setting	Description
Name	Enter a unique name to identify the device up to 25 characters in length.
Pulse Time	Specifies the duration for which the device will assume abnormal status. For example, it specifies how long a horn will sound or a door strike will remain released. The maximum number of hours is 1. When the hour field is blank, the maximum number of minutes is 59. When 1 is entered in the hour field, the maximum number of minutes is 45. The sum of all three units comprises the pulse time. Note that you can express seconds in tenths of a second.
Time Zones	Specifies two schedules: • **Energized** — sets the period during which the output is automatically energized. • **Disable Interlock** — sets the period during which the interlock, a programmed interaction between selected inputs and outputs, will be disabled. During the selected Time Zone this point ignores all interlock actions to it, effectively disabling it from being a Reacting Component during the Time Zone. Outside of the Time Zone the point will react to interlocks as expected.
Latching	Toggles the state of the outputs between energized and de-energized status upon every activation (code use, interlock, or manual pulse).
Interlock	Enables you to disable the interlock, or programmed interaction between two points.

2.7.3 Groups Tab

This tab enables you to configure outputs in groups. For example, you might want a group of horns in your facility to sound for the same duration or to be enabled or disabled according to the same schedule, or time zone. You might want a group of doors to be energized or de-energized during the same time zone. A NetAXS® web server supports up to 64 output groups.

Click **Groups** to display the Groups screen:

Figure 28: *Configure > Other I/O & Groups > Groups Tab*



Other I/O Configuration - Panel 1

Grp	Name	Pulse Time (H-M-S)	Energized TZ	Interlock Disabled TZ	Latch
New		0 0 0.0	-	-	□
1	Group1	1 Hr 0 Min 0.0 Sec	Default Time Zone (24x7)	Default Time Zone (24x7)	-
2	Group2	0 Hr 30 Min 0.0 Sec	Default Time Zone (24x7)	Default Time Zone (24x7)	✓
3	Visitors	1 Hr 4 Min 0.0 Sec	TimeZone1	TimeZone2	✓

Available Outputs
Output #1 [1]
Output #2 [2]
Output #3 [3]
Output #4 [4]
Output #5 [5]
Output #6 [6]
Output #7 [7]

New Group

Selected Outputs
< none >

The Groups tab enables you to:

- Associate any of the panel's eight output relays in one or more groups.
- Configure the following for each group:
  - Pulse Time
  - Energized TZ (Time Zone)
  - Interlock Disabled TZ (Time Zone)
  - Latch

Steps: Use the descriptions in Table 14 to configure each group:

Table 14: *Configuration > Other I/O & Groups > Groups Tab Field Descriptions*

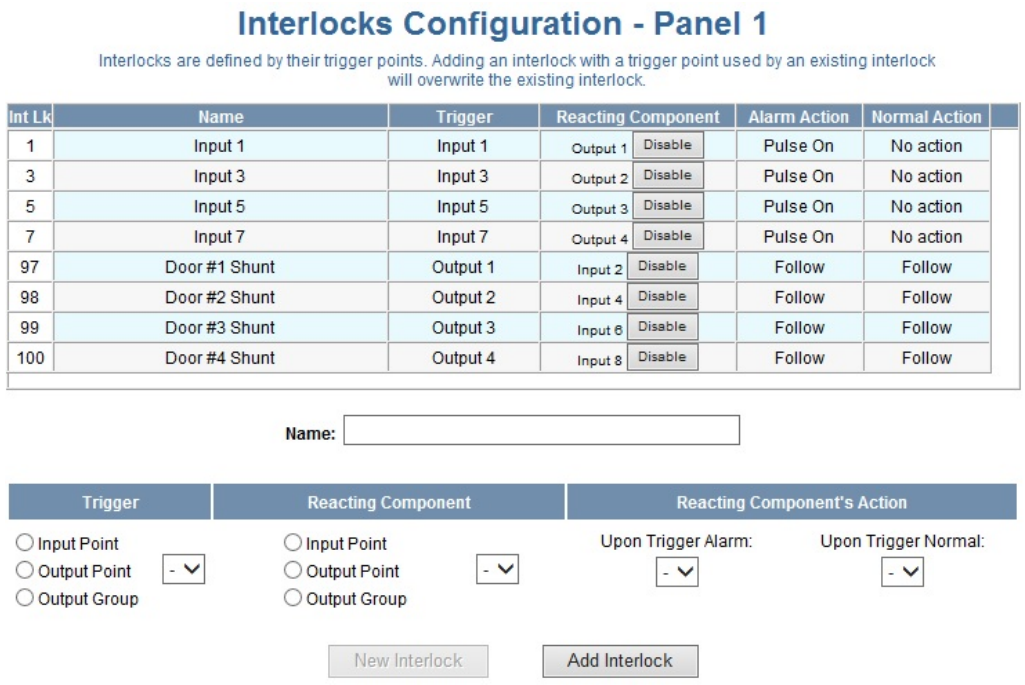
Setting	Description
Name	Enter a unique name to identify the group up to 25 characters.
Pulse Time	Specifies the duration for which the device will assume abnormal status. For example, it specifies how long a horn will blow or a door strike will remain released. The maximum number of hours is 1. When the hour field is blank, the maximum number of minutes is 59. When 1 is entered in the hour field, the maximum number of minutes is 45. The sum of all three units comprises the pulse time. Note that you can express seconds in tenths of a second.
Energized TZ	Specifies the period during which the group of output relays are automatically energized.
Interlock Disabled TZ	Specifies the period during which the interlocks that control the group's outputs will be disabled.
Latch	Toggles the state of the outputs between energized and de-energized status upon every activation (code use, interlock, or manual pulse).

2.8 Configuring Interlocks

An interlock is a programmed connection between two points. The interlock causes an input point, output point, or group of output points to act in a specified manner when another input point, output point, or group of output points changes its state. An action on one point causes a reaction from a second point on the same panel or attached downstream board. For example, when a motion detector (input) detects movement, it causes a horn (output) to sound.

Click **Interlocks** to display the Interlocks Configuration screen:

Figure 29: *Configure > Interlocks*



Interlocks Configuration - Panel 1

Interlocks are defined by their trigger points. Adding an interlock with a trigger point used by an existing interlock will overwrite the existing interlock.

Int Lk	Name	Trigger	Reacting Component	Alarm Action	Normal Action
1	Input 1	Input 1	Output 1 Disable	Pulse On	No action
3	Input 3	Input 3	Output 2 Disable	Pulse On	No action
5	Input 5	Input 5	Output 3 Disable	Pulse On	No action
7	Input 7	Input 7	Output 4 Disable	Pulse On	No action
97	Door #1 Shunt	Output 1	Input 2 Disable	Follow	Follow
98	Door #2 Shunt	Output 2	Input 4 Disable	Follow	Follow
99	Door #3 Shunt	Output 3	Input 6 Disable	Follow	Follow
100	Door #4 Shunt	Output 4	Input 8 Disable	Follow	Follow

Name:

Trigger	Reacting Component	Reacting Component's Action
○ Input Point ○ Output Point - ○ Output Group	○ Input Point ○ Output Point - ○ Output Group	Upon Trigger Alarm: - Upon Trigger Normal: -

The Interlocks screen enables you to:

- Create, modify, and delete interlocks.
- Enable or disable existing interlocks.

Steps to create an interlock:

1. Click the **New Interlock** button to display the screen.
2. Use the descriptions in Table 15 to configure the interlock:

Table 15: *Configuration > Interlocks > Field Descriptions*

Interlock element	Description
Trigger	Specifies the input, output, or output group for which a change of state will cause a reaction from another input, output, or group. If Trigger = Inputs, then triggers 1-88* will have an interlock link (Int Lnk) number from 1-96. If Trigger = Outputs, then outputs 1-80* will have an interlock link (Int Lnk) number from 97-184. If Trigger = Groups, then groups 1-64* will have an interlock link (Int Lnk) number from 185-250. Use the drop-down list to specify the number of the input or output. * **Note:** Additional Input/Output/Group points are achieved with the addition of NX4IN and NX4OUT downstream devices.
Reacting Component	Specifies the input, output, or output group that will react to a change of state from the trigger point. Use the drop-down list to specify the number of the input or output.
Reacting Component's Action	**Upon Trigger Alarm** — Specifies the reacting component's action when the trigger's change of state occurs. Select the action from the Upon Trigger Alarm drop-down list. **Upon Trigger Normal** — Specifies the reacting component's action when the trigger's change of state occurs. Select the action from the Upon Trigger Normal drop-down list. Following are the available actions in the drop-down lists: When Reacting Component = Input, then actions are **No Action**, **Shunt**, **Unshunt**, **Timed Shunt**, **Follow**, and **Invert Follow**. When Reacting Component = Output or group, then actions are **No Action**, **Energize**, **De-Energize**, **Pulse On**, **Pulse Off**, **Follow**, and **Invert Follow**. Interlocking is an advanced functionality. Contact Technical Support for information on how to use it.

3. Click the **Add Interlock** button to create the interlock.

Steps to delete an interlock:

1. In the Int Lk column, click the number of the interlock you want to delete.
2. Click the **Delete Interlock** button to display the Delete Interlock screen, and click **OK** to complete the deletion.

Steps to enable/disable an interlock:

1. To enable an interlock, click the **Enable** button.
2. To disable an interlock, click the **Disable** button.

Note: You may not modify an interlock, but you can overwrite an existing interlock by adding a new interlock. However, the new interlock must have the same trigger input as the existing interlock, otherwise the existing interlock will not be overwritten.

2.9 Configuring Users

A user is one who will be using the NetAXS® software interface in one or morefunction roles.

The User Configuration screen enables you to:

- Create a user.
- Modify a user.
- Delete a user.
- Enable or disable a user account.
- View the user's current login status, either logged in or logged out.

Table 16 lists the functions that each user type can perform.

Table 16: *User Functions*

Function	Operator	Service	Administrator
View alarms/events	✓	✓	✓
Acknowledge alarms	✓	✓	✓
View panel I/O status	✓	✓	✓
Control I/O points	✓	✓	✓
Generate reports	✓	✓	✓
View card database	✓	✓	✓

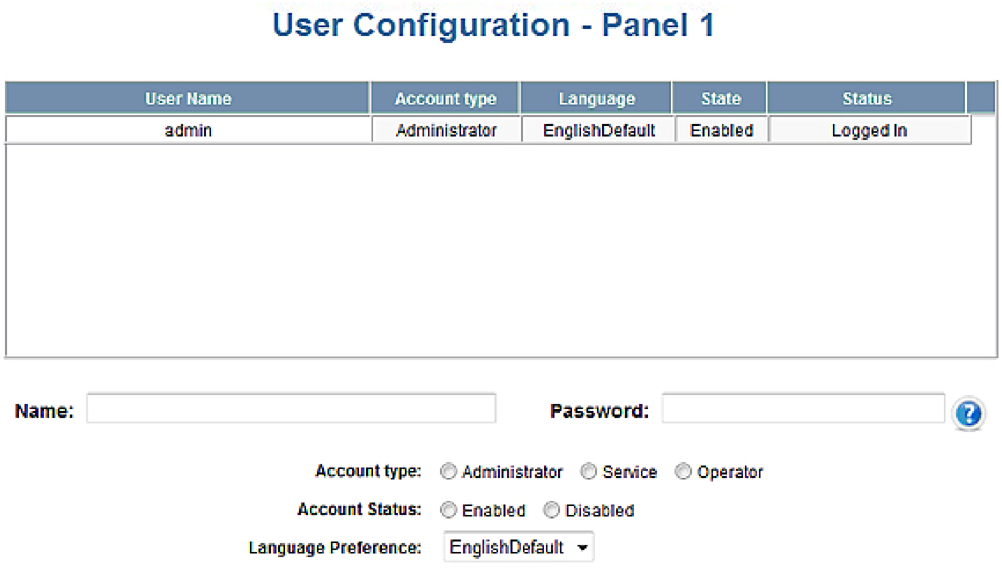
Table 16: *User Functions*

Function	Operator	Service	Administrator
Create, modify, delete cards		✓	✓
View all configurations		✓	✓
Create, modify, delete configurations			✓
Perform uploads/downloads			✓
Manage own user account	✓	✓	✓
Manage all user accounts			✓

Note: These are users rights when the panel is in Web Mode. Some rights become more limited when the panel is in Host Mode.

Click **Users** to display the User Configuration screen:

Figure 30: *Configuration > Users*



User Configuration - Panel 1

User Name	Account type	Language	State	Status
admin	Administrator	EnglishDefault	Enabled	Logged In

Name:

Password:

Account type: ○ Administrator ○ Service ○ Operator

Account Status: ○ Enabled ○ Disabled

Language Preference: EnglishDefault

Your password must meet the following minimum requrements:

1. Shall only consist of alpha, numeric, and symbol characters.
2. Shall contain at least 1 character from each of the following 4 character types:
   - lower-case letters (a-z)
   - UPPER CASE letters (A-Z)
   - numbers (0-9)
   - the symbols !, @, #, $, %, ^, &, (and).
3. Shall contain a minimum of 8 and a maximum of 16 characters.
4. Shall not contain a consecutive string of 3 or more repeated characters.
5. Shall not contain the name of the user's account type ('admin', 'service' or 'operator').
6. If you fail to successfully login after 5 consecutive attempts (Retry Limit Exceeded), account will be locked out for 30 minutes. Any login attempt with the locked out account, within the timeout period, will restart the 30 minute lock-out period.

The User Configuration screen enables you to:

- Create, modify, delete cards
- View all configurations
- Create, modify, delete configurations
- Perform uploads/downloads
- Manage own user account
- Manage all user accounts.

Steps to create a user:

1. Click the **New User** button.
2. Enter the user's name in the **Name** field (range 5-25 characters).
3. Enter a unique password in the **Password** field (range 8-16 characters). Note that a duplicate password will not be accepted.
4. Select the type in the **Account Type** field.
5. Select the Account Status:
   - Enabled — Activates the user account (the user can log in).
   - Disabled — De-activates the user account (the user cannot log in).
6. Select the user's Language Preference from the dropdown list.
7. Click the **Add User** button.

Steps to modify a user:

1. In the **User Name** field, click the name of the user you want to modify.
2. Change the name, password, account type, or account status.
3. Click the **Modify** button.

Steps to delete a user:

1. In the User Name column, click the user account you want to delete.
2. Click the **Delete** button.
3. Click **OK** at the prompt to delete the user account.

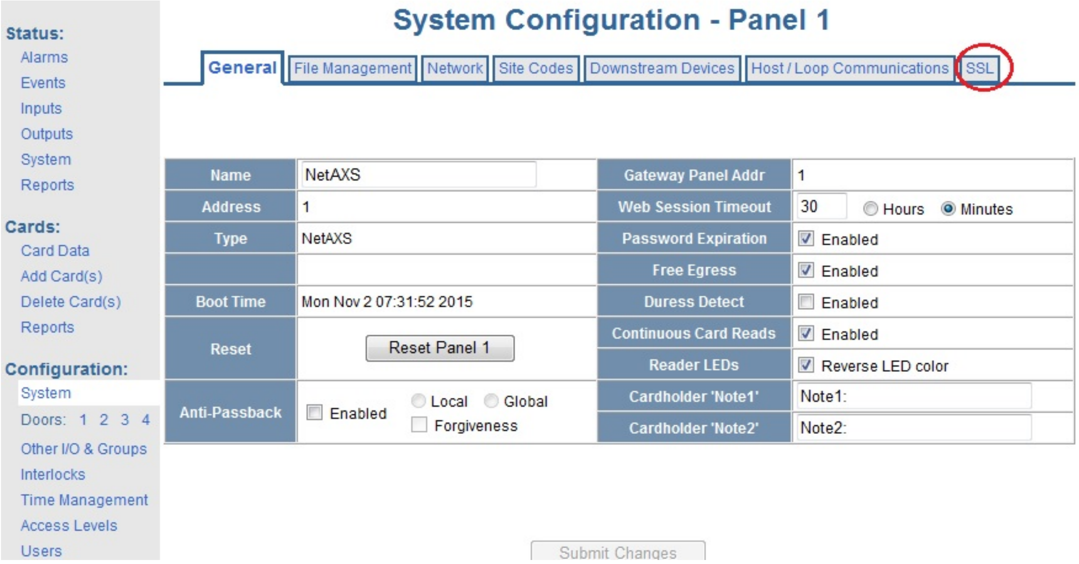
Note: All user passwords will expire after a period of six months; the users will be prompted to change password upon login.

2.10 SSL Certificate Management

2.10.1 Requesting a Certificate

To request a Certificate, Click **SSL Certificate** on Configuration/System:

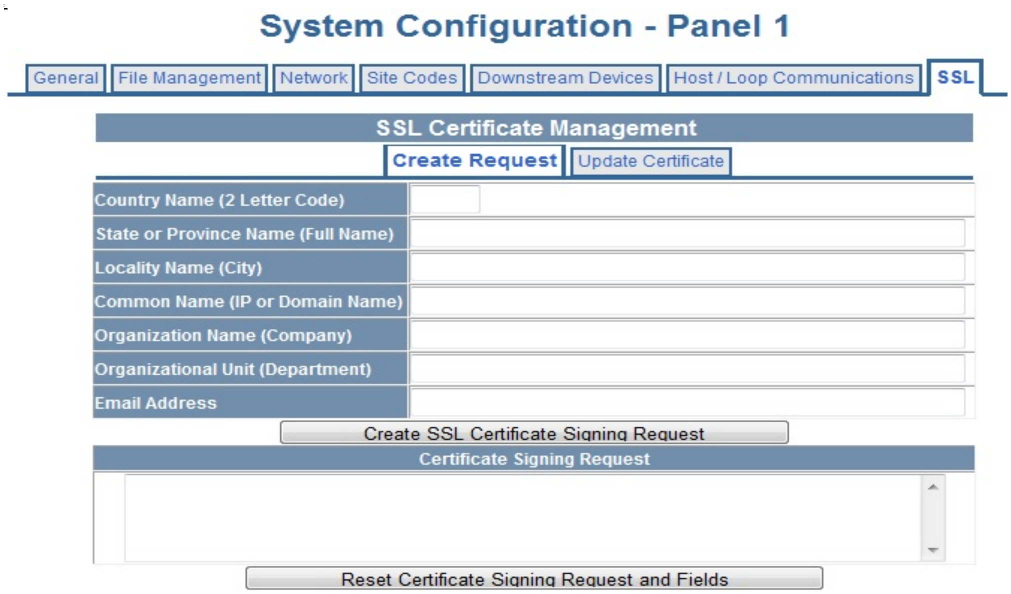
Figure 31: *Configuration > System > SSL*



Name	NetAXS	Gateway Panel Addr	1
Address	1	Web Session Timeout	30 ○ Hours ● Minutes
Type	NetAXS	Password Expiration	☑ Enabled
		Free Egress	☑ Enabled
Boot Time	Mon Nov 2 07:31:52 2015	Duress Detect	□ Enabled
Reset	Reset Panel 1	Continuous Card Reads	☑ Enabled
		Reader LEDs	☑ Reverse LED color
Anti-Passback	□ Enabled ○ Local ○ Global □ Forgiveness	Cardholder 'Note1'	Note1:
		Cardholder 'Note2'	Note2:

Enter the Certificate Information into the Create Request Form, then Click **Create SSL Certificate Signing Request.**

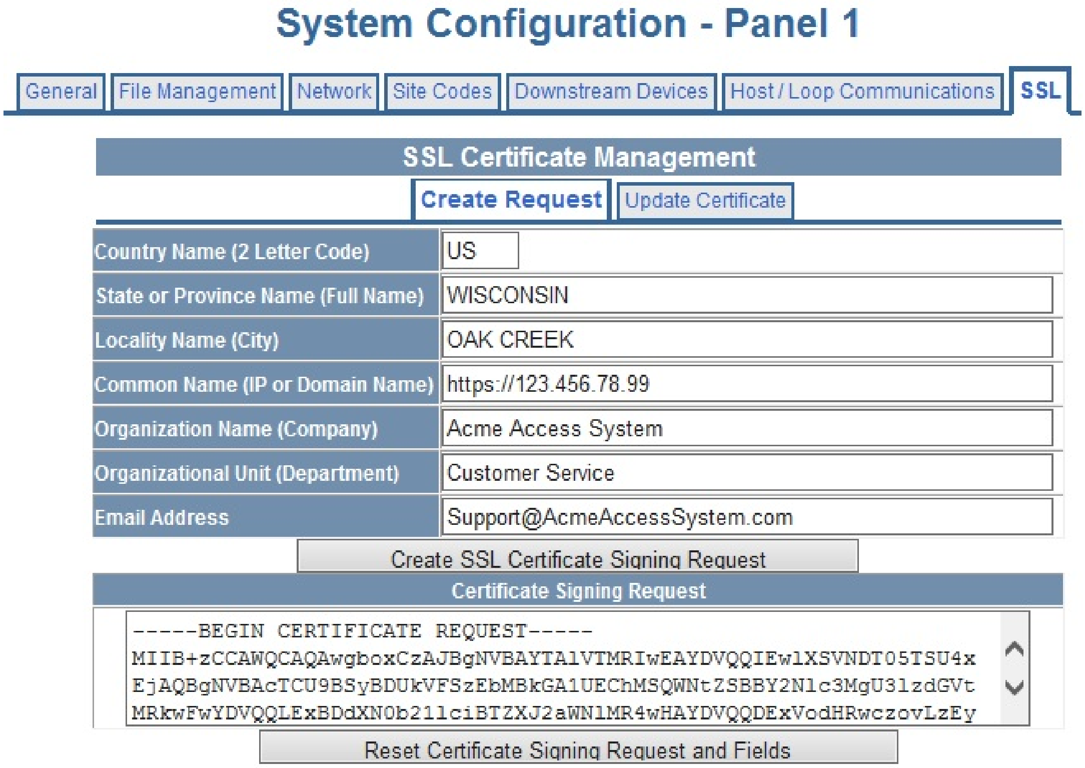
Figure 32: *Create SSL Certificate Signing Request*


System Configuration - Panel 1
General
File Management
Network
Site Codes
Downstream Devices
Host / Loop Communications
SSL
SSL Certificate Management
Create Request
Update Certificate
Create SSL Certificate Signing Request
Certificate Signing Request
Reset Certificate Signing Request and Fields

Country Name (2 Letter Code)	
State or Province Name (Full Name)	
Locality Name (City)	
Common Name (IP or Domain Name)	
Organization Name (Company)	
Organizational Unit (Department)	
Email Address	

The text box will get populated with text that serves as the "Certificate Signing Request" (CSR). This is the information that you must provide (copy/paste) to the Certificate Authority (CA) of your choice. It will be used to generate the CA provided certificate.

Figure 33: *CSR Information*


System Configuration - Panel 1
General
File Management
Network
Site Codes
Downstream Devices
Host / Loop Communications
SSL
SSL Certificate Management
Create Request
Update Certificate

Country Name (2 Letter Code)	US
State or Province Name (Full Name)	WISCONSIN
Locality Name (City)	OAK CREEK
Common Name (IP or Domain Name)	https://123.456.78.99
Organization Name (Company)	Acme Access System
Organizational Unit (Department)	Customer Service
Email Address	Support@AcmeAccessSystem.com

Create SSL Certificate Signing Request
Certificate Signing Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB+zCCAWQCAQAwgboxCzAJBgNVBAYTA1VTMRIwEAYDVQQIEw1XSVNDT05TSU4x
EjAQBgNVBAcTCU9BSyBDUkVFSzEbMBkGA1UEChMSQWNtZSBBY2Nlc3MgU3lzdGVt
MRkwFwYDVQQLExBDdXN0b21lciBTZXJ2aWNlMR4wHAYDVQQDExVodHRwczovLzEy
```

Note: For the Common Name field, check with your Certificate Authority first to confirm which one is needed to create CSR, IP or Domain name.

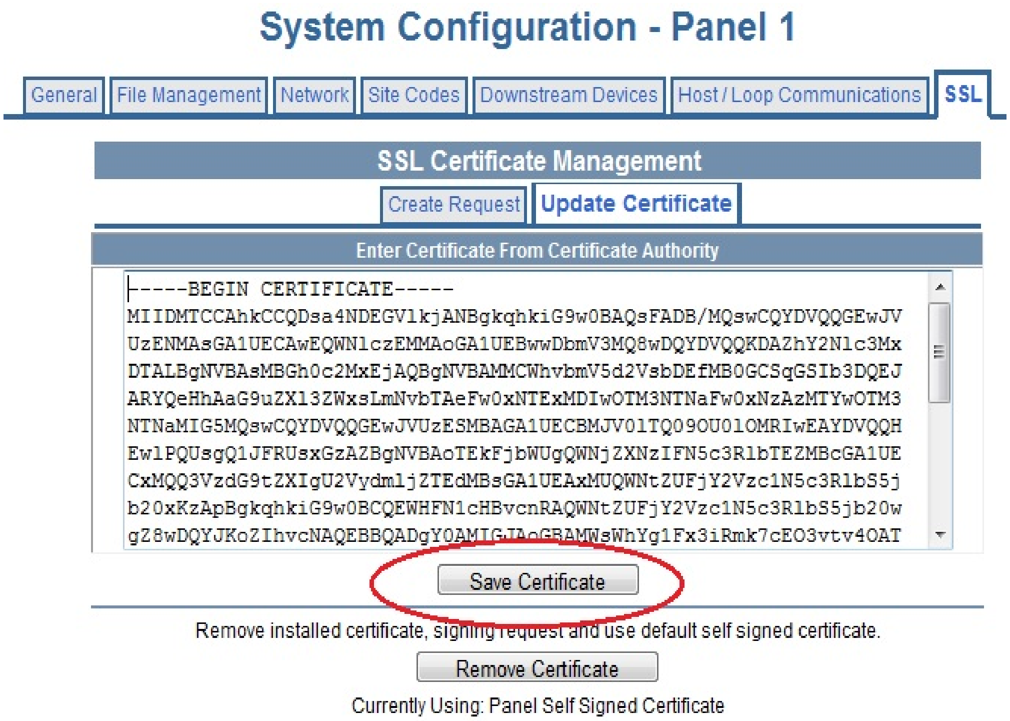
2.10.2 Installing a CA Provided Certificate Key

Your Certificate Authority (CA) will provide you with a certificate key.

- Select the Update Certificate tab, and paste the CA provided certificate key into the text box.
- Click the **Save Certificate** button.

This will restart the embedded web server and begin using the CA provided certificate.

Figure 34: *Updating a Certificate*



System Configuration - Panel 1

General
File Management
Network
Site Codes
Downstream Devices
Host / Loop Communications
SSL
SSL Certificate Management
Create Request
Update Certificate
Enter Certificate From Certificate Authority

```
-----BEGIN CERTIFICATE-----
MIIDMTCCAhkCCQDsa4NDEGVlkjANBgkqhkiG9w0BAQsFADB/MQswCQYDVQQGEwJV
UzENMAsGA1UECAwEQWNlczEMMAoGA1UEBwwDbmV3MQ8wDQYDVQQKDAZhY2Nlc3Mx
DTALBgNVBAsMBGh0c2MxEjAQBgNVBAMMCWhvbmV5d2VsbDEfMB0GCSqGSIb3DQEJ
ARYQeHhAaG9uZXl3ZWxsLmNvbTAeFw0xNTExMDIwOTM3NTNaFw0xNzAzMTYwOTM3
NTNaMIG5MQswCQYDVQQGEwJVUzESMBAGA1UECBMJV01TQ09OU01OMRIwEAYDVQQH
Ew1PQUsgQ1JFRUsxGzAZBgNVBAoTEkFjbWUgQWNjZXNzIFN5c3RlbTEZMBcGA1UE
CxMQQ3VzdG9tZXIgU2VydmljZTEdMBsGA1UEAxMUQWNtZUFjY2Vzc1N5c3RlbS5j
b20xKzApBgkqhkiG9w0BCQEWHFN1cHBvcnRAQWNtZUFjY2Vzc1N5c3RlbS5jb20w
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMWsWhYg1Fx3iRmk7cEO3vtv4OAT
```

Remove installed certificate, signing request and use default self signed certificate.

Currently Using: Panel Self Signed Certificate

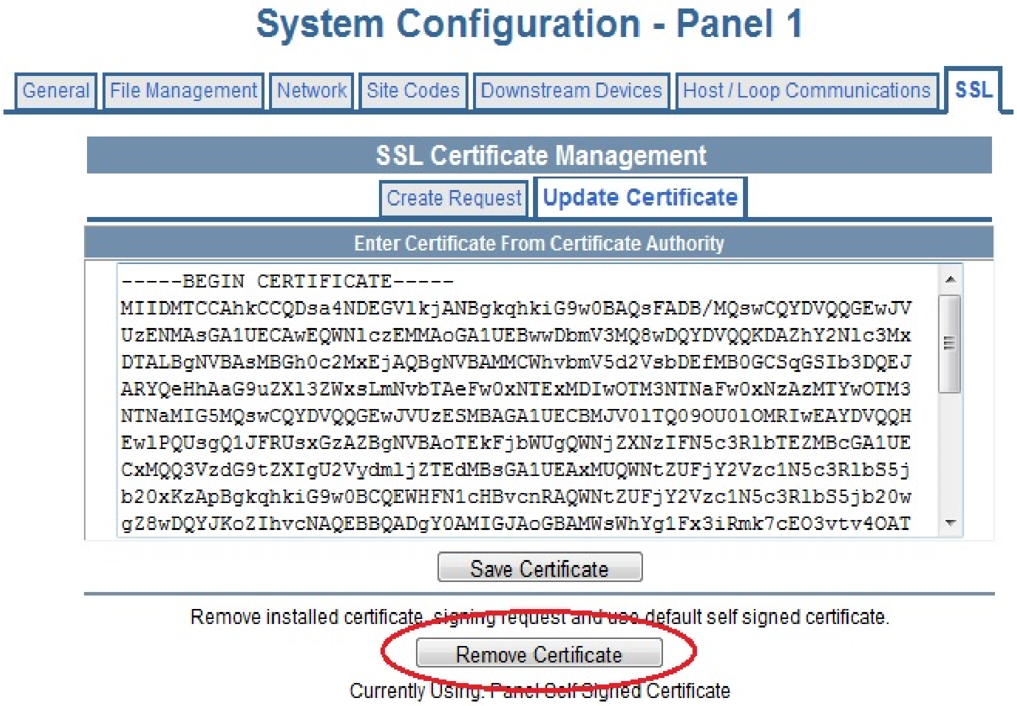
2.10.3 Removing a CA Provided SSL Certificate

From the SSL Certificate Management screen:

- Click the **Remove Certificate** button.

This action will remove the CA certificate, and cause the panel to use a default self-signed certificate.

Figure 35: *Removing a Certificate*


System Configuration - Panel 1
General
File Management
Network
Site Codes
Downstream Devices
Host / Loop Communications
SSL
SSL Certificate Management
Create Request
Update Certificate
Enter Certificate From Certificate Authority
Save Certificate
Remove Certificate

```
-----BEGIN CERTIFICATE-----
MIIDMTCCAhkCCQDsa4NDEGVlkjANBgkqhkiG9w0BAQsFADB/MQswCQYDVQQGEwJV
UzENMAsGA1UECAwEQWNlczEMMAoGA1UEBwwDbmV3MQ8wDQYDVQQKDAZhY2Nlc3Mx
DTALBgNVBAsMBGh0c2MxEjAQBgNVBAMMCWhvbmV5d2VsbDEfMB0GCSqGSIb3DQEJ
ARYQeHhAaG9uZXl3ZWxsLmNvbTAeFw0xNTExMDIwOTM3NTNaFw0xNzAzMTYwOTM3
NTNaMIG5MQswCQYDVQQGEwJVUzESMBAGA1UECBMJV01TQ09OU01OMRIwEAYDVQQH
Ew1PQUsgQ1JFRUsxGzAZBgNVBAoTEkFjbWUgQWNjZXNzIFN5c3RlbTEZMBcGA1UE
CxMQQ3VzdG9tZXIgU2VydmljZTEdMBsGA1UEAxMUQWNtZUFjY2Vzc1N5c3RlbS5j
b20xKzApBgkqhkiG9w0BCQEWHFN1cHBvcnRAQWNtZUFjY2Vzc1N5c3RlbS5jb20w
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMWsWhYg1Fx3iRmk7cEO3vtv4OAT
```

Remove installed certificate, signing request and use default self signed certificate.

Currently Using: Panel Self Signed Certificate

3.0 Configuring via WIN-PAK

3.1 Overview

If you are using WIN-PAK XE/SE/PE 3.3 and newer or WIN-PAK CS 4.2 and newer you may skip this section since NetAXS is natively supported in these versions.

This section explains the NetAXS® configuration functions as accessed via the Quick Start Wizard (QSW) for WIN-PAK versions prior to WIN-PAK XE/SE/PE 3.3. The QSW creates the ADV options and adds the panel to the Control Map and the Master Access Level. It is strongly recommended to upgrade from these older WIN-PAK versions to the current WIN-PAK release. Doing so will provide optimum performance and security.

When the System Configuration is set up for host support you will see a notice on the bottom of the Browser indicating that the browser functions are limited. You will be able to view but not make any database changes once WIN-PAK takes control.

These functions should be performed only by the NetAXS® system administrator or service personnel.

Notes:

- WIN-PAK 2.0, release 4, uses the same steps provided in this section to configure NetAXS®; however, its screens are not exactly the same.
- NetAXS® cannot be added to WIN-PAK PRO Release 4 or older.
- For a new Site installation, or for adding to an existing Site, follow the procedures in this section as you would when you add an N-1000-IV-X panel. One exception to this is that the NetAXS® panel does not support the use of the C-100-A1 (20ma current loop installations). Therefore, when you select the Loop type, 485 ACK<-NAK is the only supported type. Direct is reserved for NS2P; C-100 is not supported.
- If the NetAXS® panel is configured as a Gateway panel, it appears to WIN-PAK as an N-485-PCI or N-485-HUB. Using the NetAXS® panel as a Gateway, you should not add N-1000/PW-2000 panels as a downstream panel to the NetAXS® gateway. The NetAXS® gateway is designed for more efficient downstream communications than what can be supported by the N-1000/PW2000 panels.

The NetAXS® Gateway panel's baud rate is set configured via the NetAXS® web server (see the *NetAXS® Access Control Unit Installation Guide* for instructions). When you set the Loop Type in the QSW to 485 ACK-NAK, you define the baud rate to be 19.2 kilobits per second. This baud rate and the panel's baud rate must match to communicate properly. For WIN-PAK SE or WIN-PAK PE systems, you can adjust the baud rate of the N-485 device to 115 kilobits per second for optimum performance.

3.2 Adding a New NetAXS® Panel

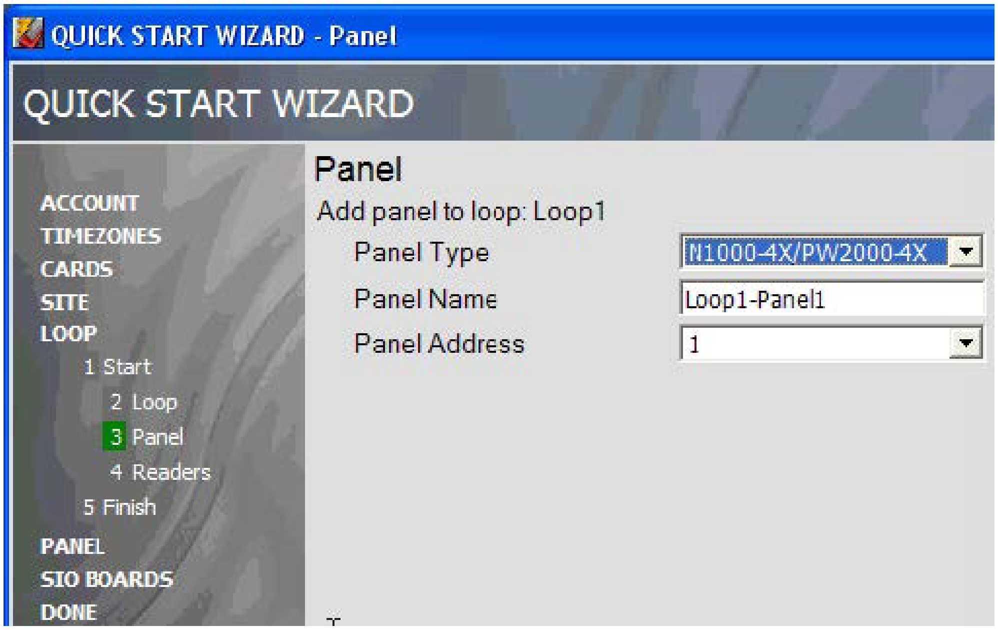
To add a NetAXS® panel, first create the panel in the WIN-PAK Quick Start Wizard, and then complete the configuration manually with the WIN-PAK Panel Configuration screen.

3.2.1 Creating the Panel with Quick Start Wizard

Add a new panel by selecting its Loop and configuring the following from the Quick Start Wizard Panel screen:

- Panel type (Select N1000-4X/PW2000-4X from the dropdown list)
- Panel name (Loop[Loop number]-Panel [Panel address])
- Panel address (Select from the dropdown list)

Figure 36: *Quick Start Wizard - Panel Screen*



Panel

Add panel to loop: Loop1

Panel Type: N1000-4X/PW2000-4X

Panel Name: Loop1-Panel1

Panel Address: 1

Note: Each panel on a communication loop must have a unique address. The address must correspond with the address that is set by DIP switches on the panel.

After adding the NetAXS® panel via the QSW, you must update the Reader and Input interlocks to match them with the default wiring of the NetAXS® panel. Proceed to Configuring the Panel Manually, page 74and make the necessary changes.

3.2.2 Configuring the Panel Manually

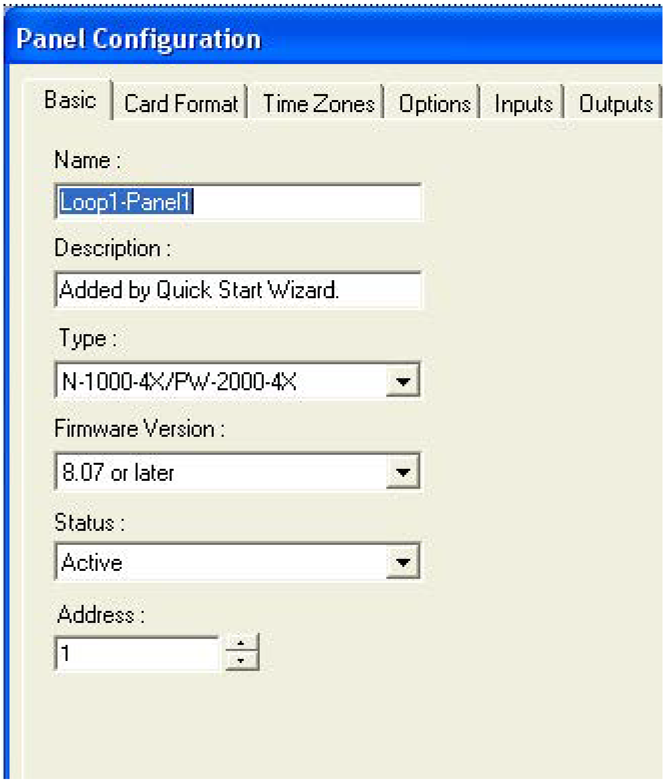
Use the WIN-PAK Panel Configuration screen to complete the NetAXS® panel configuration manually. All of the configuration screen options are supported for NetAXS® panel configuration, except where they are noted otherwise in this section.

Note: You cannot initialize the NetAXS® panel from the WIN-PAK Control Map until you complete the steps in this section.

If you are using the Device Map to add the NetAXS® panel manually, add it as you would an N-1000-IV-X panel.

1. Display the Basic tab of the WIN-PAK Panel Configuration screen. The Name, Description, and Type fields contain the entries selected in the Quick Start Wizard:

Figure 37: *WIN-PAK Panel Configuration Screen - Basic Tab*



Name : Loop1-Panel1

Description : Added by Quick Start Wizard.

Type : N-1000-4X/PW-2000-4X

Firmware Version : 8.07 or later

Status : Active

Address : 1

2. Enter the following selections for the remaining fields:

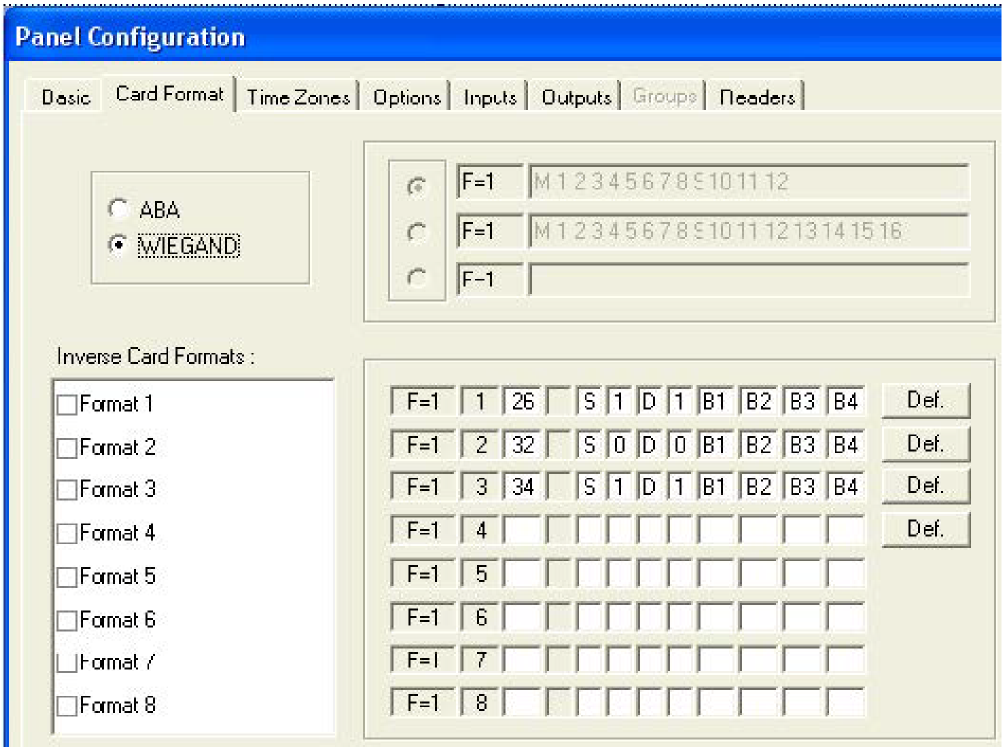
   – Firmware version — 8.07 or later.

   – Status — Active.

   – Address — Select the appropriate panel number.

3. Add the ADV.
4. Click **OK**.
5. Display and complete the Card Format tab:

Figure 38: WIN-PAK Panel Configuration Screen - Card Format Tab



○ ABA
● WIEGAND

● F=1 M 1 2 3 4 5 6 7 8 9 10 11 12
○ F=1 M 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
○ F-1

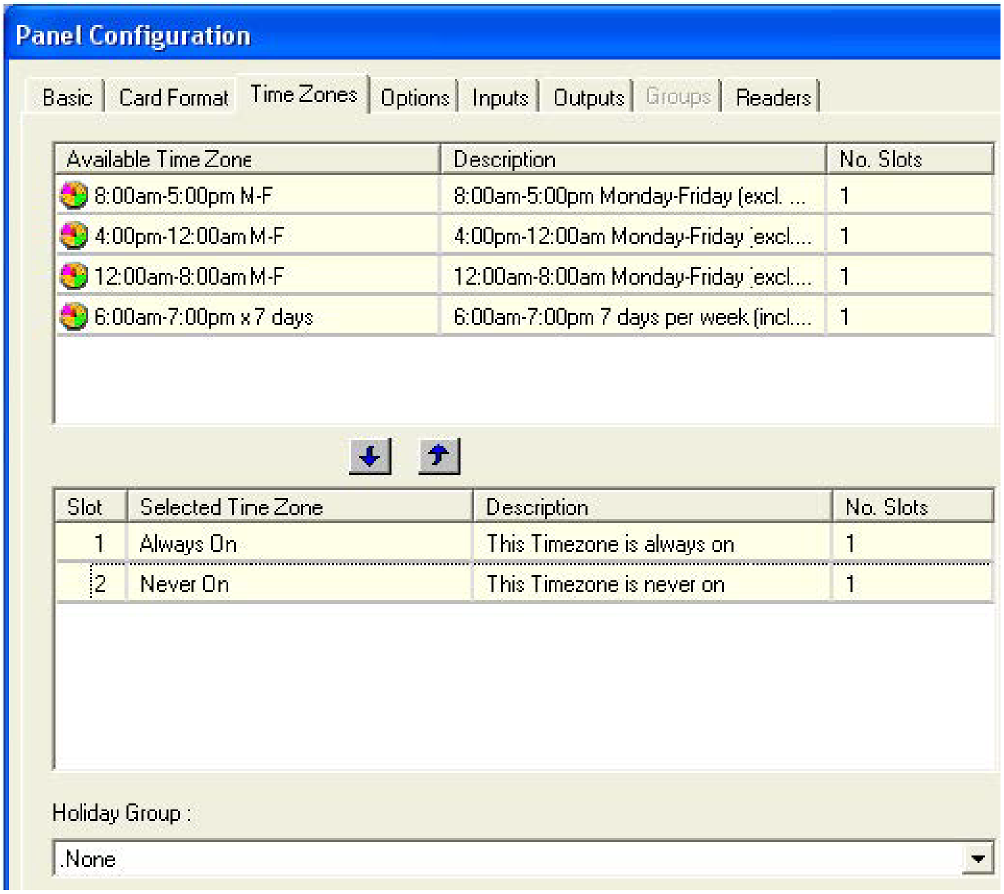
Inverse Card Formats :

□ Format 1
□ Format 2
□ Format 3
□ Format 4
□ Format 5
□ Format 6
□ Format 7
□ Format 8

F=1	1	26		S	1	D	1	B1	B2	B3	B4
F=1	2	32		S	0	D	0	B1	B2	B3	B4
F=1	3	34		S	1	D	1	B1	B2	B3	B4
F=1	4										
F=1	5										
F=1	6										
F=I	7										
F=1	8										

6. Display and complete the Time Zones tab:

Figure 39: *WIN-PAK Panel Configuration Screen - Time Zones Tab*



Available Time Zone	Description	No. Slots
8:00am-5:00pm M-F	8:00am-5:00pm Monday-Friday (excl. ...	1
4:00pm-12:00am M-F	4:00pm-12:00am Monday-Friday (excl....	1
12:00am-8:00am M-F	12:00am-8:00am Monday-Friday (excl....	1
6:00am-7:00pm x 7 days	6:00am-7:00pm 7 days per week (incl....	1

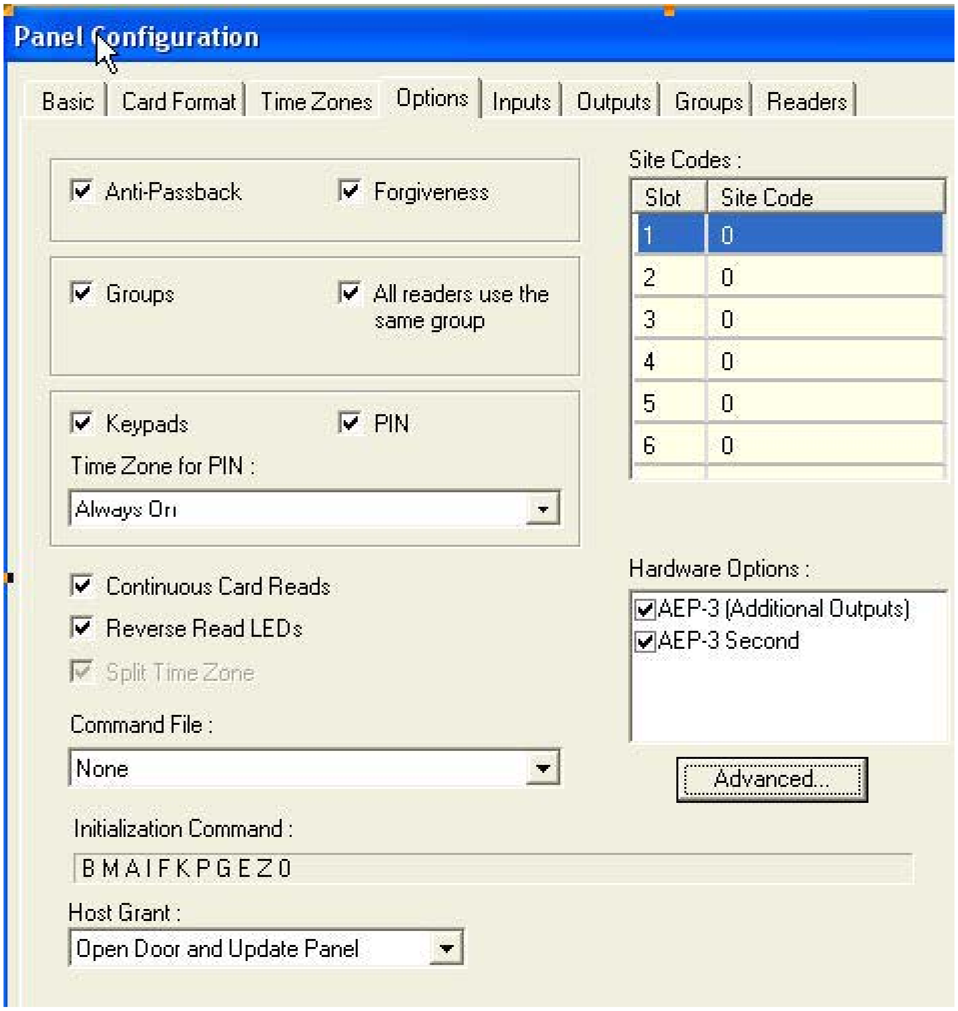
Slot	Selected Time Zone	Description	No. Slots
1	Always On	This Timezone is always on	1
2	Never On	This Timezone is never on	1

Holiday Group : None

Note: All Time Zones and Holidays are supported for a NetAXS® panel.

7. Display and complete the Options tab:

Figure 40: *WIN-PAK Panel Configuration Screen - Options Tab*



Panel Configuration

☑ Anti-Passback ☑ Forgiveness

☑ Groups ☑ All readers use the same group

☑ Keypads ☑ PIN

Time Zone for PIN : Always On

☑ Continuous Card Reads

☑ Reverse Read LEDs

☑ Split Time Zone

Command File : None

Initialization Command : B M A I F K P G E Z 0

Host Grant : Open Door and Update Panel

Site Codes :

Slot	Site Code
1	0
2	0
3	0
4	0
5	0
6	0

Hardware Options :

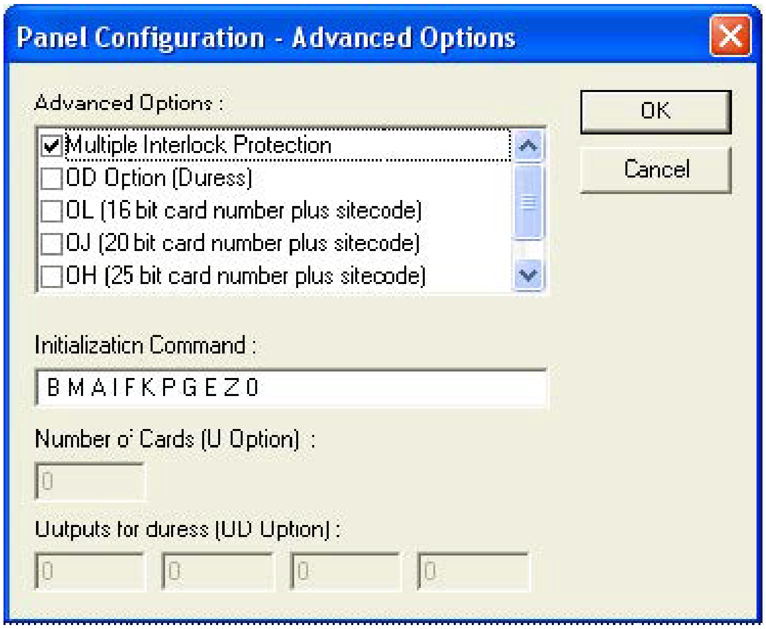
☑ AEP-3 (Additional Outputs)

☑ AEP-3 Second

Notes:

- All options are supported for a NetAXS® panel except the Advanced U option. When using Groups, you must select both AEP boards in the Hardware Options box. The NX4OUT board functions as two AEP-3 boards, and it provides outputs 17-32.
- You can select Keypads; however, the NetAXS® panel does not support the matrixed keypads (for example, KP-10, KP-12, or PR-PROXPRO-K2). The supported readers include the PR-PROXPRO-K (HU/5355AGK000 and OT35xx and OT36xx series readers and keypads).

8. Click the **Advanced** button to display the Advanced Options screen, and select the desired advanced options. Note that the Advanced U option is not supported for the NetAXS® panel.



Panel Configuration - Advanced Options

Advanced Options :

- ☑ Multiple Interlock Protection
- □ OD Option (Duress)
- □ OL (16 bit card number plus sitecode)
- □ OJ (20 bit card number plus sitecode)
- □ OH (25 bit card number plus sitecode)

Initialization Command : B M A I F K P G E Z 0

Number of Cards (U Option) : 0

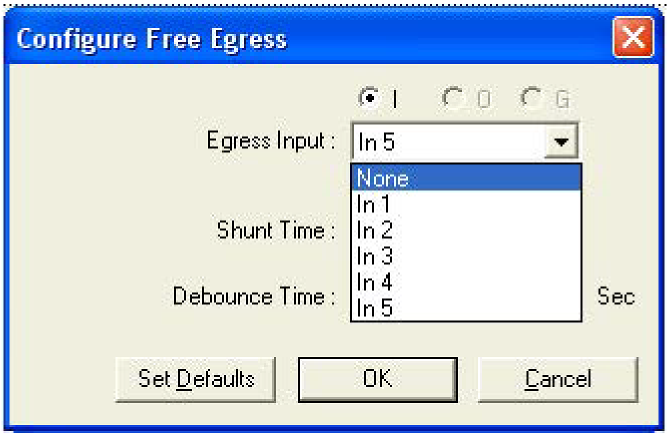
Outputs for duress (OD Option) : 0 0 0 0

9. Display and complete the Inputs tab. If you are using the NetAXS® inputs to monitor the door status or activate a request to exit, then you must reassign the interlocks as indicated below. If you are not using panel inputs for door status or egress, you only need to dissolve the interlocks. Note that if you do not dissolve the default N-1000-IV interlocks, an error will occur during NetAXS® panel initializations.

   All Inputs tab functions are available to NetAXS® configuration. However, not all inputs are available and their default functions have changed. NetAXS® supports inputs 1-14. The default functions are listed below. Their default values are assumed to be zero, unless otherwise noted. You must change the interlocking.

10. Use the following procedure to reassign the interlocks:

   a. Display the Readers tab, and then display the first input's configuration window. Select **None**, and click **OK**. This dissolves all input interlocks and changes the Shunt Time to 0. This allows the input to be properly redefined for use with NetAXS.



   b. Repeat the preceding step for each input for each reader on this tab.

   c. After all interlocks on all inputs for each reader have been dissolved, reassign the interlocks according to Table 17 below:

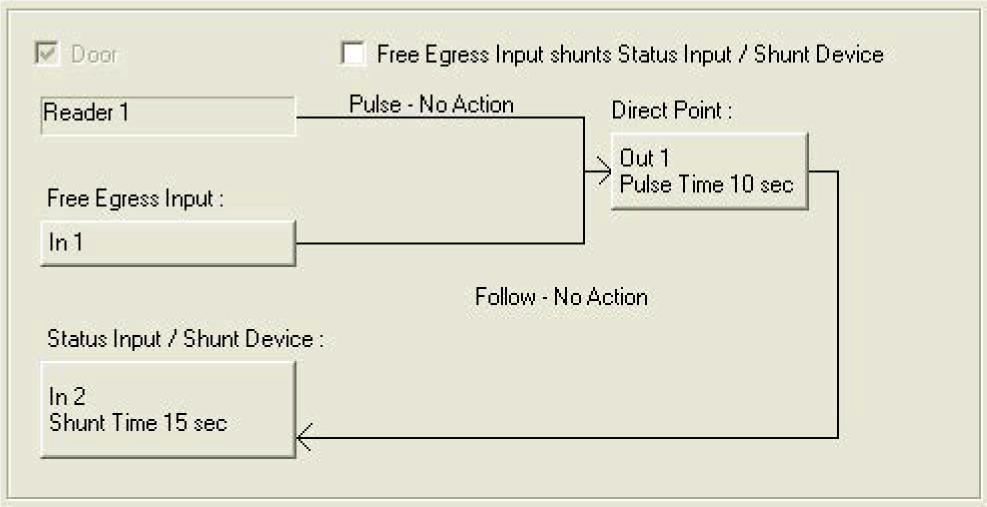
Table 17: *Interlock Reassignments for NetAXS®*

Interlock	Function
1	Door egress for Door 1
2	Door status switch for Door 1. Shunt time is 15 seconds.
3	Door egress for Door 2.
4	Door status switch for Door 2. Shunt time is 15 seconds.
5	Door egress for Door 3.
6	Door status switch for Door 3. Shunt time is 15 seconds.
7	Door egress for Door 4.
8	Door status switch for Door 4. Shunt time is 15 seconds.
9	Reader 1 tamper/auxiliary.
10	Reader 2 tamper/auxiliary.
11	Reader 3 tamper/auxiliary.

Table 17: *Interlock Reassignments for NetAXS®* (continued)

Interlock	Function
12	Reader 4 tamper/auxiliary.
13	Primary power status - external (or General input). There is also a system primary power alarm 17 that reports through the ADV and is not a wired port.
14	Tamper (or General input).

The screen captures shown below show the configuration for the default interlocking for a single door:



☑ Door

□ Free Egress Input shunts Status Input / Shunt Device

Reader 1

Pulse - No Action

Direct Point :

Out 1
Pulse Time 10 sec

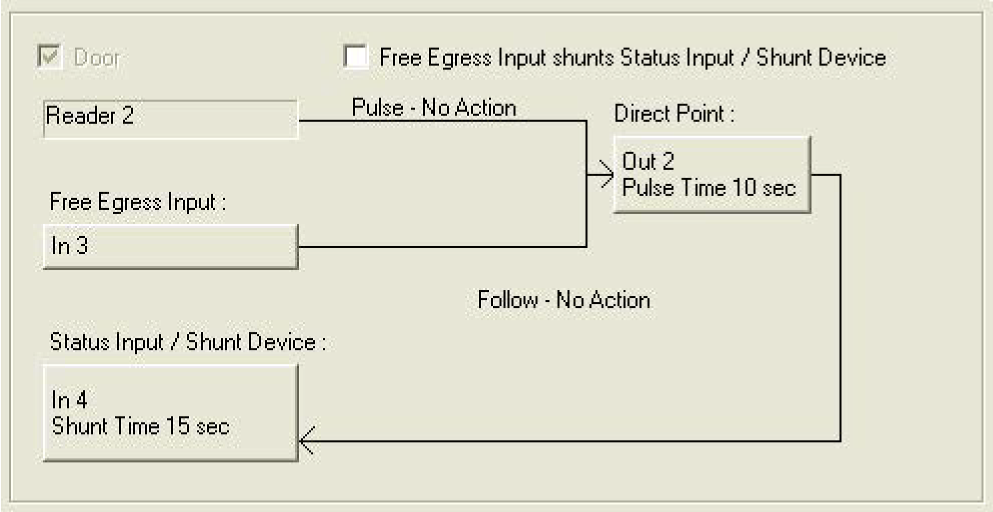
Free Egress Input :

In 1

Follow - No Action

Status Input / Shunt Device :

In 2
Shunt Time 15 sec



☑ Door

□ Free Egress Input shunts Status Input / Shunt Device

Reader 2

Pulse - No Action

Direct Point :

Out 2
Pulse Time 10 sec

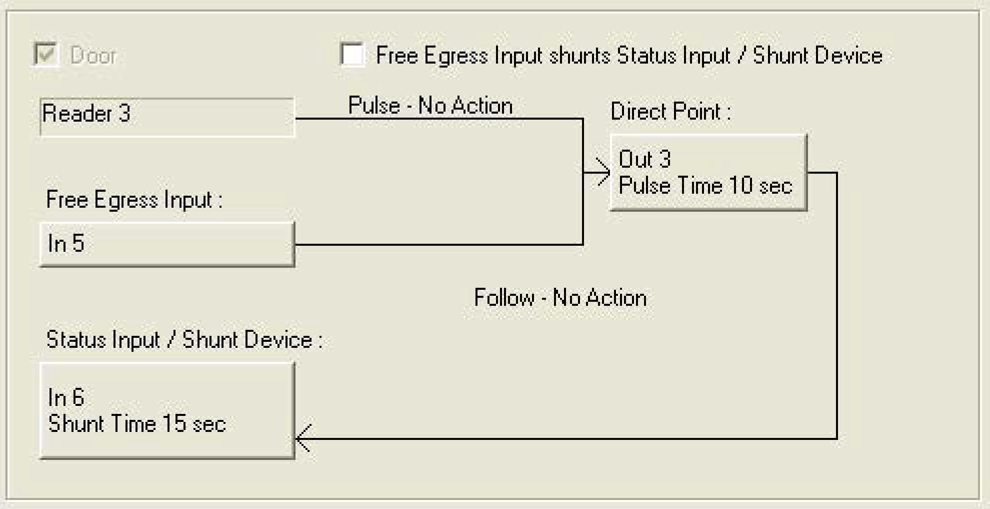
Free Egress Input :

In 3

Follow - No Action

Status Input / Shunt Device :

In 4
Shunt Time 15 sec



☑ Door

□ Free Egress Input shunts Status Input / Shunt Device

Reader 3

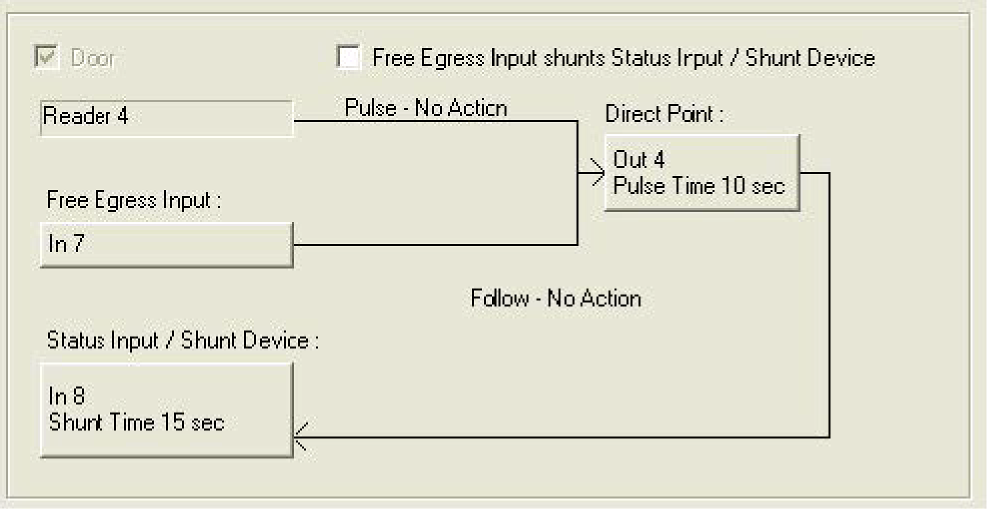
Pulse - No Action

Direct Point :
Out 3
Pulse Time 10 sec

Free Egress Input :
In 5

Follow - No Action

Status Input / Shunt Device :
In 6
Shunt Time 15 sec



☑ Door

□ Free Egress Input shunts Status Irput / Shunt Device

Reader 4

Pulse - No Acticn

Direct Point :
Out 4
Pulse Time 10 sec

Free Egress Input :
In 7

Follow - No Action

Status Input / Shunt Device :
In 8
Shunt Time 15 sec

11. The configuration of a NetAXS® panel via WIN-PAK is now complete. Configuration is optional on the Outputs and Groups tabs.

4.0 Monitoring NetAXS® Status

4.1 Overview

This section is written for the NetAXS® operator who will monitor the following NetAXS® status:

- Alarms — Alarms are events, or system transactions, that have been assigned alarm status. These often include events such as an invalid card read or a forced door.
- Events — Events are the recorded transactions of the NetAXS® system. For example, an event card found, number of users logged in.
- Inputs — Inputs are terminals located on the NetAXS® panel; the inputs are wired to input devices, such as a door-position switch.
- Outputs — Output relays are relays located on the NetAXS® panel that are connected to output devices, such as a door lock.
- System — This includes current capacities and limits.
- Reports — The system generates reports by Last Name and by Card Number.

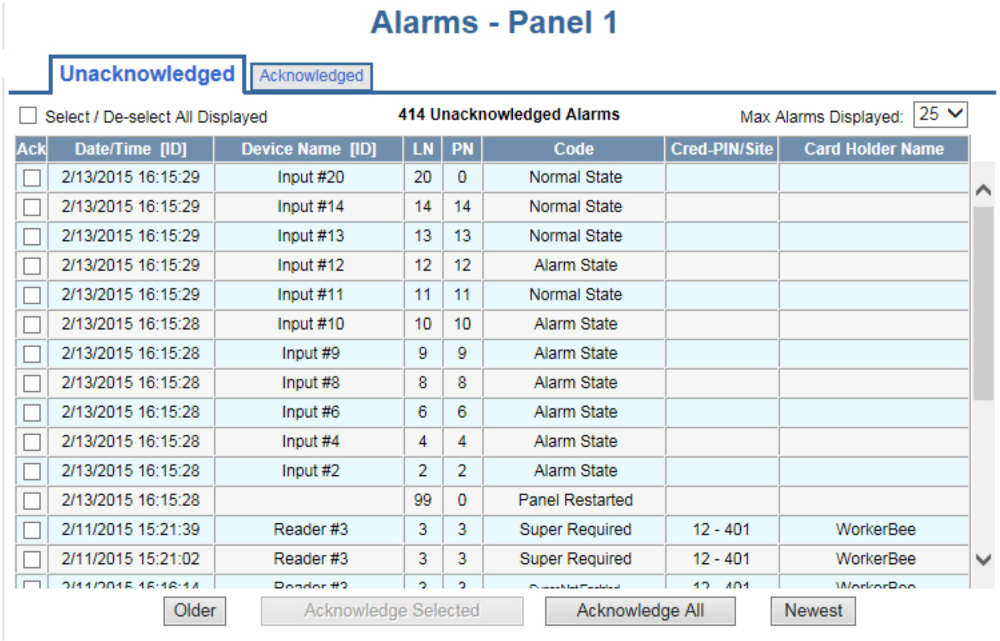
4.2 Monitoring Alarms

Alarms are viewed as system-generated messages that may indicate the need for user attention.

Note: From the drop down menu at the upper-right corner of each Alarms tab, you can configure the tab to display alarms in groups of 10, 25, 50, or 75.

Click **Status > Alarms** to display the Unacknowledged Alarms tab:

Figure 41: *Status > Alarms > Unacknowledged Tab*



☐ Select / De-select All Displayed

414 Unacknowledged Alarms

Max Alarms Displayed: 25

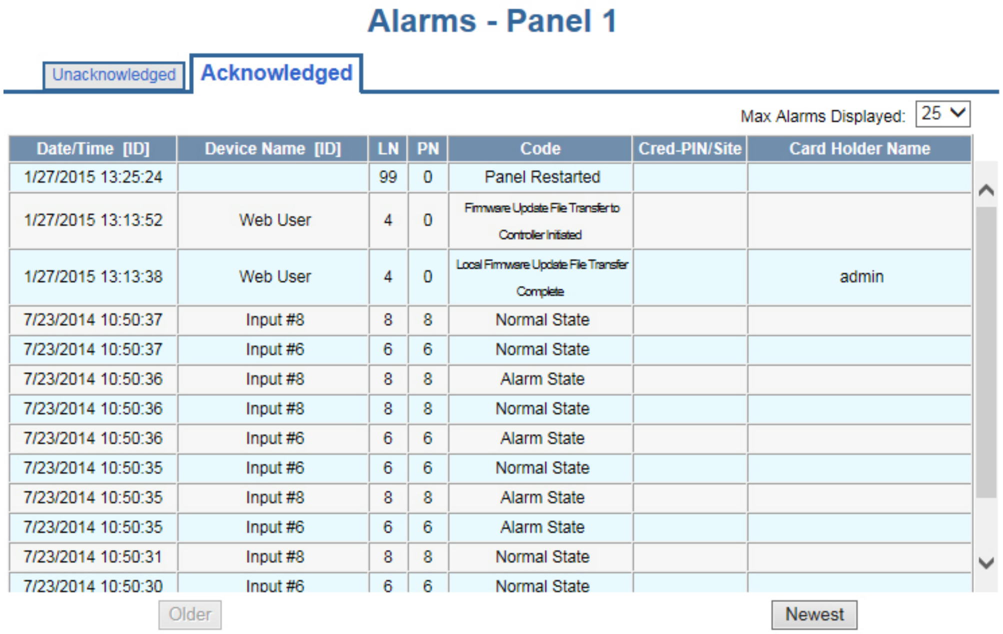
Ack	Date/Time [ID]	Device Name [ID]	LN	PN	Code	Cred-PIN/Site	Card Holder Name
☐	2/13/2015 16:15:29	Input #20	20	0	Normal State		
☐	2/13/2015 16:15:29	Input #14	14	14	Normal State		
☐	2/13/2015 16:15:29	Input #13	13	13	Normal State		
☐	2/13/2015 16:15:29	Input #12	12	12	Alarm State		
☐	2/13/2015 16:15:29	Input #11	11	11	Normal State		
☐	2/13/2015 16:15:28	Input #10	10	10	Alarm State		
☐	2/13/2015 16:15:28	Input #9	9	9	Alarm State		
☐	2/13/2015 16:15:28	Input #8	8	8	Alarm State		
☐	2/13/2015 16:15:28	Input #6	6	6	Alarm State		
☐	2/13/2015 16:15:28	Input #4	4	4	Alarm State		
☐	2/13/2015 16:15:28	Input #2	2	2	Alarm State		
☐	2/13/2015 16:15:28		99	0	Panel Restarted		
☐	2/11/2015 15:21:39	Reader #3	3	3	Super Required	12 - 401	WorkerBee
☐	2/11/2015 15:21:02	Reader #3	3	3	Super Required	12 - 401	WorkerBee
☐	2/11/2015 15:16:14	Reader #3	3	3	[illegible]	12 - 401	WorkerBee

Notes:

- You can display the oldest alarms first by clicking **Oldest**, or display the newest alarms first by clicking **Newest**. Click **Older** to scroll through the list by displaying the next oldest tab display of alarms.
- The Alarms screen dynamically refreshes when new alarms are generated.

Click the **Acknowledged** tab to display the acknowledged alarms:

Figure 42: *Status > Alarms > Acknowledged Tab*



Date/Time [ID]	Device Name [ID]	LN	PN	Code	Cred-PIN/Site	Card Holder Name
1/27/2015 13:25:24		99	0	Panel Restarted		
1/27/2015 13:13:52	Web User	4	0	Firmware Update File Transfer to Controller Initiated		
1/27/2015 13:13:38	Web User	4	0	Local Firmware Update File Transfer Complete		admin
7/23/2014 10:50:37	Input #8	8	8	Normal State		
7/23/2014 10:50:37	Input #6	6	6	Normal State		
7/23/2014 10:50:36	Input #8	8	8	Alarm State		
7/23/2014 10:50:36	Input #8	8	8	Normal State		
7/23/2014 10:50:36	Input #6	6	6	Alarm State		
7/23/2014 10:50:35	Input #6	6	6	Normal State		
7/23/2014 10:50:35	Input #8	8	8	Alarm State		
7/23/2014 10:50:35	Input #6	6	6	Alarm State		
7/23/2014 10:50:31	Input #8	8	8	Normal State		
7/23/2014 10:50:30	Input #6	6	6	Normal State		

Table 18 describes the information displayed on both the Unacknowledged alarms tab and Acknowledged alarms tab:

Table 18: *Status > Alarms Field Descriptions*

Column Head	Description
Ack (Unacknowledged tab only)	Enables you to select any or all of the alarms that you want to acknowledge. Note that acknowledging an alarm simply means that you acknowledge that the alarm exists; an acknowledgement does not mean action has been taken. To acknowledge an alarm, select the check box and click the **Acknowledge Selected Alarms** button. Note that you can select or de-select all of the alarms by selecting or de-selecting the Select/De-select All Displayed check box.
Date/Time [ID]	Provides the date and exact time the alarm was generated according to the panel's time.
Device Name [ID]	Identifies the device that generated the alarm.
LN	**Logical device number** — the unique name or number given to the alarm-generating device when the device was configured in **Configuration > Doors**.

Table 18: *Status > Alarms Field Descriptions* (continued)

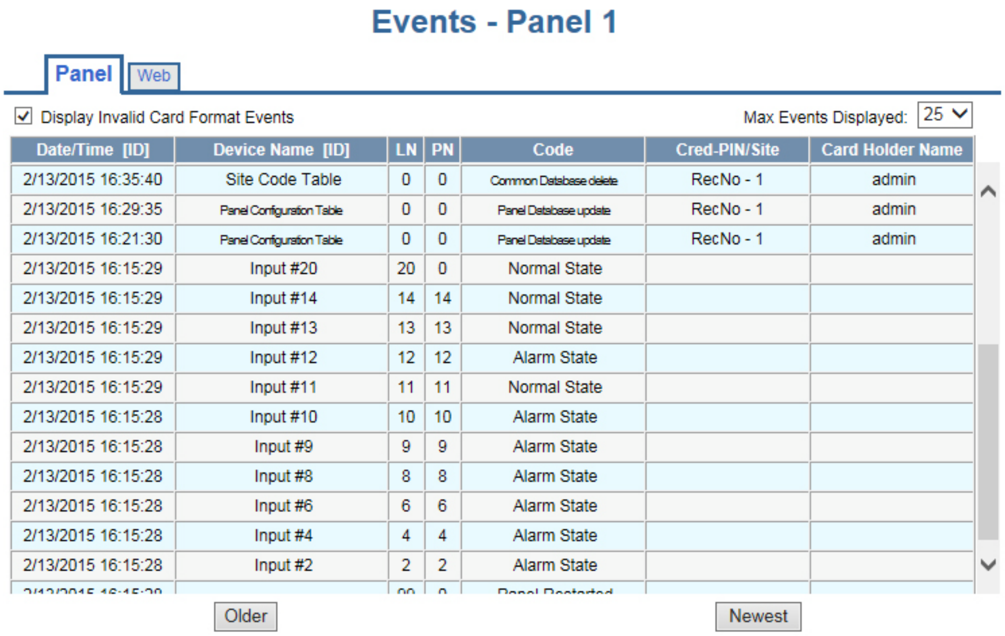
Column Head	Description
PN	**Physical device number** — the unique number assigned to the device on the NetAXS® board.
Code	Identifies the current state of the device that generated the alarm. For example, the possible states could include: • Normal State • Alarm State • Ajar State • Card Found • Card Not Found
Cred-PIN/Site	Identifies the card number, and either the PIN or site code number of the card. Reports only events that have an invalid Card Number, invalid Site Code, or invalid PIN. Invalid Cards are reported by themselves. Invalid Site Codes and invalid PINs are reported with the card number that was swiped along with them.
Card Holder Name	Identifies the last name of the card holder who energized the input device when the alarm was generated.

4.3 Monitoring Events

The Events page monitors both panel- and web-generated events. For example, a panel event is the reading of a card by a reader. A web event example is a user logon.

Click **Status > Events** to display the Panel event tab:

Figure 43: *Status > Events > Panel Tab*



Events - Panel 1

☑ Display Invalid Card Format Events

Max Events Displayed: 25

Date/Time [ID]	Device Name [ID]	LN	PN	Code	Cred-PIN/Site	Card Holder Name
2/13/2015 16:35:40	Site Code Table	0	0	Common Database delete	RecNo - 1	admin
2/13/2015 16:29:35	Panel Configuration Table	0	0	Panel Database update	RecNo - 1	admin
2/13/2015 16:21:30	Panel Configuration Table	0	0	Panel Database update	RecNo - 1	admin
2/13/2015 16:15:29	Input #20	20	0	Normal State		
2/13/2015 16:15:29	Input #14	14	14	Normal State		
2/13/2015 16:15:29	Input #13	13	13	Normal State		
2/13/2015 16:15:29	Input #12	12	12	Alarm State		
2/13/2015 16:15:29	Input #11	11	11	Normal State		
2/13/2015 16:15:28	Input #10	10	10	Alarm State		
2/13/2015 16:15:28	Input #9	9	9	Alarm State		
2/13/2015 16:15:28	Input #8	8	8	Alarm State		
2/13/2015 16:15:28	Input #6	6	6	Alarm State		
2/13/2015 16:15:28	Input #4	4	4	Alarm State		
2/13/2015 16:15:28	Input #2	2	2	Alarm State		

Notes:

- You can display the ewest events first by clicking **Newest**. Click **Older** to display the next oldest tab display of events.
- The Events screen dynamically refreshes when new events are generated.

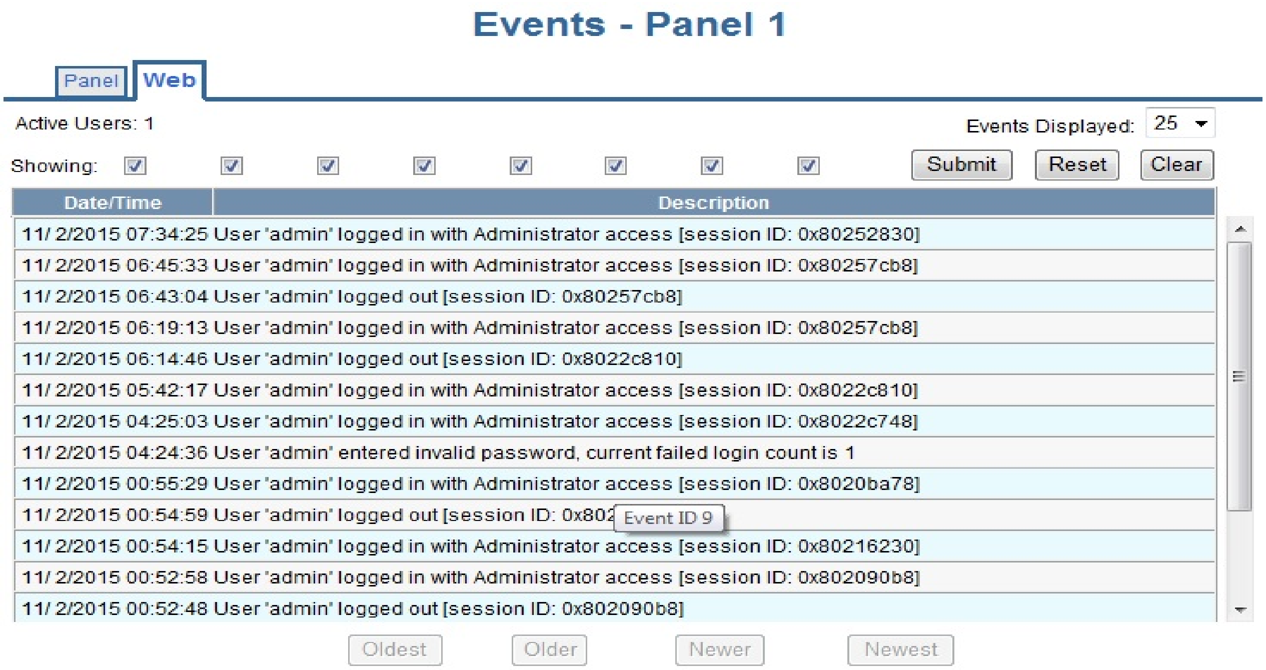
Table 19 describes the information displayed on the Panel events tab:

Table 19: *Status > Events > Panel Tab Field Descriptions*

Column Head	Description
Date/Time [ID]	Provides the date and exact time the event was generated, according to the panel's name.
Device Name [ID]	Identifies the device that generated the event.
LN	**Logical device number** — the unique name or number given to the event-generating device when the device was configured in **Configuration > Doors**.
PN	**Physical device number** — the unique number assigned to the device on the NetAXS® board.
Code	Briefly describes the event.
Cred-PIN/Site	Identifies the card number, and either the PIN or site code number of the card. Reports only events that have an invalid Card Number, invalid Site Code, or invalid PIN. Invalid Cards are reported by themselves. Invalid Site Codes and invalid PINs are reported with the card number that was swiped along with them.
Card Holder Name	Associates User, Card Holder, and raw data when applicable to a variety of events such as: • Valid Card reads • Invalid Site Code • Invalid PIN • Database Change **Note:** With respect to a card that does not have an associated format: The panel reads the card and converts its binary output into a single decimal number. This number is then reported in the Card Holder Name column along with the number of bits being listed in the Cred-PIN/Site column. Using this information, a user can determine the appropriate format for the card.

Click **Status > Events > Web** to display the Web events tab:

Figure 44: *Status > Events > Web Tab*



Active Users: 1

Events Displayed: 25

Showing: ☑ ☑ ☑ ☑ ☑ ☑ ☑ ☑

Date/Time	Description
11/ 2/2015 07:34:25	User 'admin' logged in with Administrator access [session ID: 0x80252830]
11/ 2/2015 06:45:33	User 'admin' logged in with Administrator access [session ID: 0x80257cb8]
11/ 2/2015 06:43:04	User 'admin' logged out [session ID: 0x80257cb8]
11/ 2/2015 06:19:13	User 'admin' logged in with Administrator access [session ID: 0x80257cb8]
11/ 2/2015 06:14:46	User 'admin' logged out [session ID: 0x8022c810]
11/ 2/2015 05:42:17	User 'admin' logged in with Administrator access [session ID: 0x8022c810]
11/ 2/2015 04:25:03	User 'admin' logged in with Administrator access [session ID: 0x8022c748]
11/ 2/2015 04:24:36	User 'admin' entered invalid password, current failed login count is 1
11/ 2/2015 00:55:29	User 'admin' logged in with Administrator access [session ID: 0x8020ba78]
11/ 2/2015 00:54:59	User 'admin' logged out [session ID: 0x802
11/ 2/2015 00:54:15	User 'admin' logged in with Administrator access [session ID: 0x80216230]
11/ 2/2015 00:52:58	User 'admin' logged in with Administrator access [session ID: 0x802090b8]
11/ 2/2015 00:52:48	User 'admin' logged out [session ID: 0x802090b8]

Note: 1. The number of active users is indicated in the upper left corner of the tab.

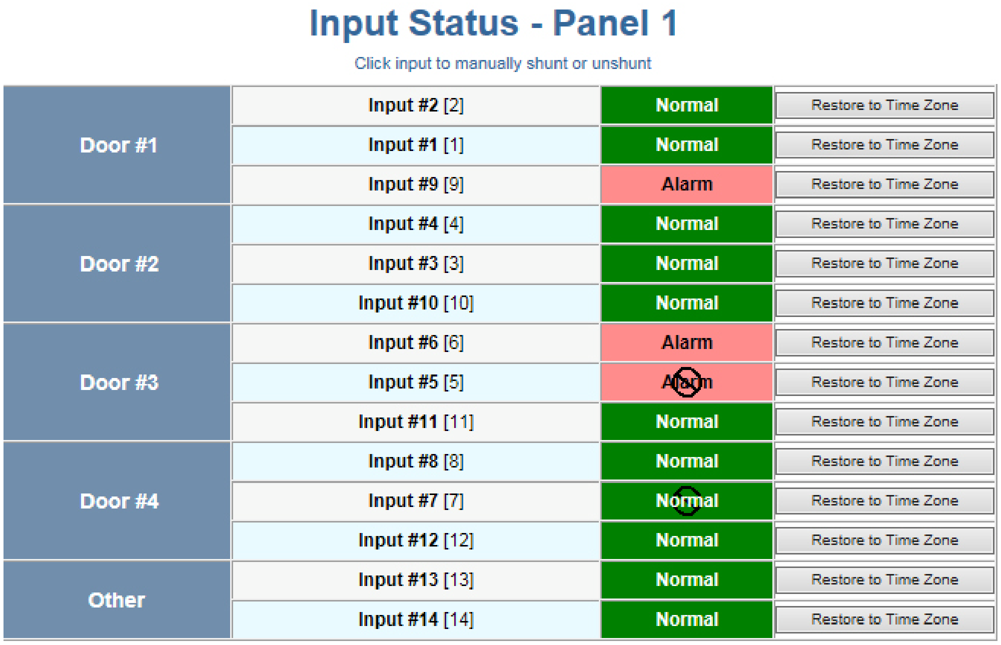
2. Select which Web Events to filter by selecting one or more checkboxes. Hover over each checkbox to display its filter type.

4.4 Monitoring Inputs

A NetAXS® panel supports door, panel, and auxiliary inputs. The door inputs provide egress and tamper status, the panel inputs provide power fail and tamper status, and the auxiliary inputs support any downstream status.

Click **Status > Inputs** to display the Input Status screen:

Figure 45: *Status > Inputs*



Input Status - Panel 1

Click input to manually shunt or unshunt

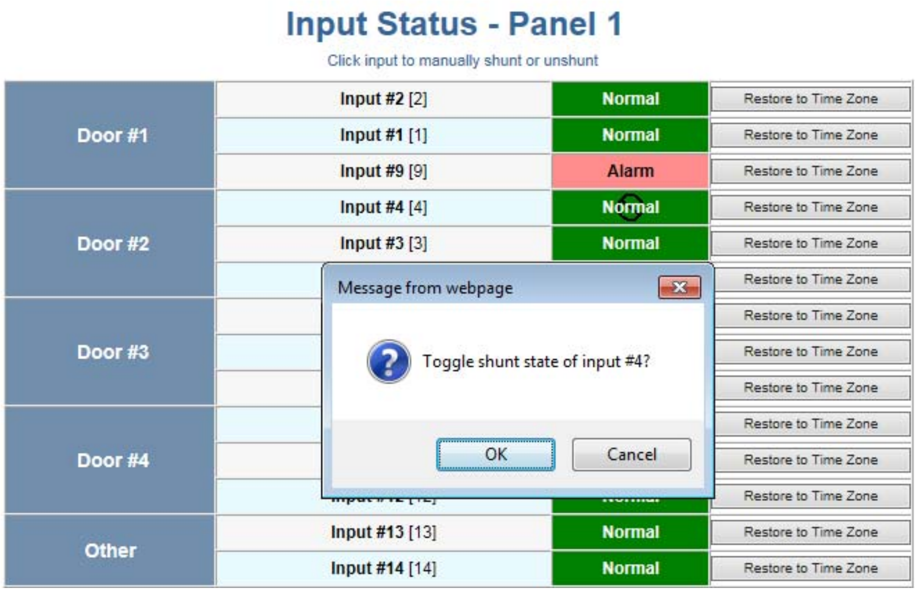
Door #1	**Input #2** [2]	Normal	Restore to Time Zone
	Input #1 [1]	Normal	Restore to Time Zone
	Input #9 [9]	Alarm	Restore to Time Zone
Door #2	**Input #4** [4]	Normal	Restore to Time Zone
	Input #3 [3]	Normal	Restore to Time Zone
	Input #10 [10]	Normal	Restore to Time Zone
Door #3	**Input #6** [6]	Alarm	Restore to Time Zone
	Input #5 [5]	Alarm	Restore to Time Zone
	Input #11 [11]	Normal	Restore to Time Zone
Door #4	**Input #8** [8]	Normal	Restore to Time Zone
	Input #7 [7]	Normal	Restore to Time Zone
	Input #12 [12]	Normal	Restore to Time Zone
Other	**Input #13** [13]	Normal	Restore to Time Zone
	Input #14 [14]	Normal	Restore to Time Zone

The Input Status screen enables you to:

- View the current status of each input (Normal, Alarm, Cut, Short, Shunted).
- Shunt or un-shunt any input. When an input is shunted, the alarm is de-activated. This is a way you can allow the input to grant access without falsely signalling an alarm. The default state of an input point is "un-shunted."
- Restore the input to its configured time zone. A time zone is a specified time period during which the input will be shunted and the alarm de-activated (see Configuring Time Management, page 26).

Steps:

1. To shunt or un-shunt an input, click the input name to display a prompt. Click OK to complete the shunt or un-shunt.



Input Status - Panel 1

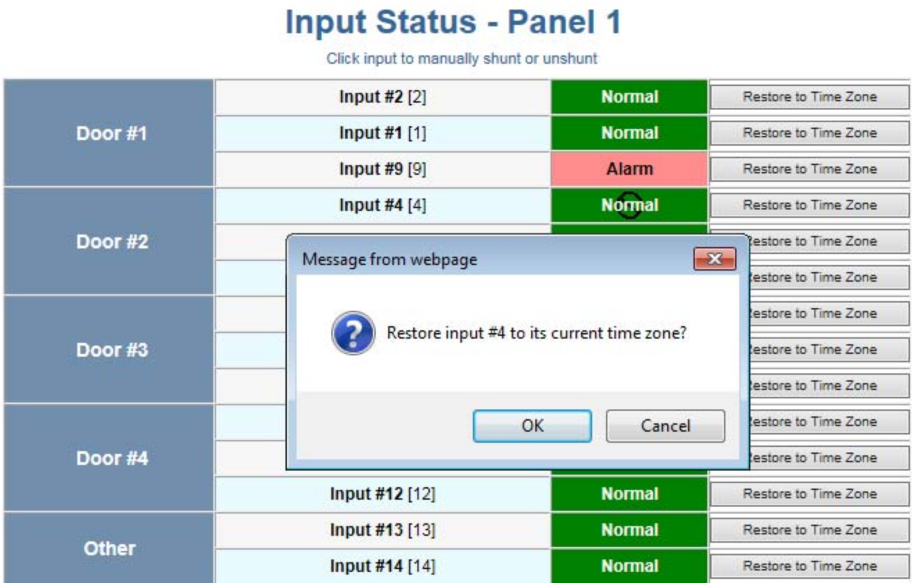
Click input to manually shunt or unshunt

Door #1	**Input #2** [2]	Normal	Restore to Time Zone
	Input #1 [1]	Normal	Restore to Time Zone
	Input #9 [9]	Alarm	Restore to Time Zone
Door #2	**Input #4** [4]	Normal	Restore to Time Zone
	Input #3 [3]	Normal	Restore to Time Zone
			Restore to Time Zone
Door #3			Restore to Time Zone
			Restore to Time Zone
			Restore to Time Zone
Door #4			Restore to Time Zone
			Restore to Time Zone
	Input #12 [12]	Normal	Restore to Time Zone
Other	**Input #13** [13]	Normal	Restore to Time Zone
	Input #14 [14]	Normal	Restore to Time Zone

Message from webpage

Toggle shunt state of input #4?

2. To restore the input to its shunt state based on its configured time zone, click the input's **Restore to Time Zone** button to display a prompt. Click **OK** to complete the restoration to the configured time zone.



Input Status - Panel 1

Click input to manually shunt or unshunt

Door #1	**Input #2** [2]	Normal	Restore to Time Zone
	Input #1 [1]	Normal	Restore to Time Zone
	Input #9 [9]	Alarm	Restore to Time Zone
Door #2	**Input #4** [4]	Normal	Restore to Time Zone
			estore to Time Zone
			estore to Time Zone
Door #3			estore to Time Zone
			estore to Time Zone
			estore to Time Zone
Door #4			estore to Time Zone
			estore to Time Zone
	Input #12 [12]	Normal	Restore to Time Zone
Other	**Input #13** [13]	Normal	Restore to Time Zone
	Input #14 [14]	Normal	Restore to Time Zone

Message from webpage

Restore input #4 to its current time zone?

Note: The Input Status screen dynamically refreshes when input status changes.

4.5 Monitoring Outputs

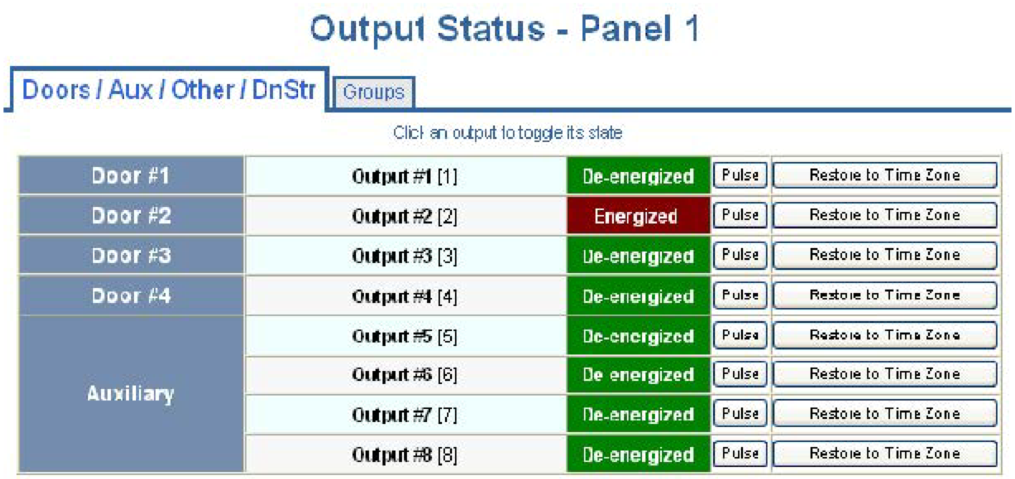
An output is an output device that changes its normal state when it is energized, pulsed, or time-zone controlled. For example, a successful card read at a reader pulses a door lock. The lock changes its normally locked state to an unlocked state and the cardholder opens the door.

A NetAXS® panel supports one output for each of its four doors. The panel also supports four additional outputs for auxiliary devices and 64 downstream outputs. Outputs can be configured singly as discrete outputs (see Outputs Tab, page 41 and Outputs Tab, page 58) or collectively as a group of outputs (Groups Tab, page 60).

Note: The Pulse and Restore to Time Zone buttons will only function when an output or group has a valid pulse time or a time zone assigned.

Click **Status > Outputs** to display the Doors/Aux/Other/DnStr tab of the Output Status screen:

Figure 46: *Status > Outputs > Doors/Aux/Other/DnStr Tab*

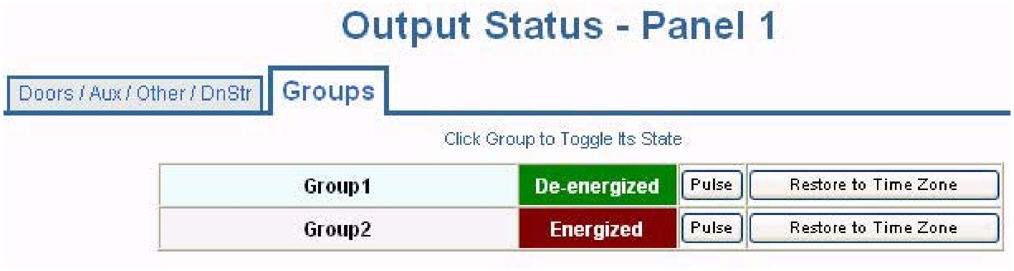


Click an output to toggle its state

Door #1	Output #1 [1]	De-energized	Pulse	Restore to Time Zone
Door #2	Output #2 [2]	Energized	Pulse	Restore to Time Zone
Door #3	Output #3 [3]	De-energized	Pulse	Restore to Time Zone
Door #4	Output #4 [4]	De-energized	Pulse	Restore to Time Zone
Auxiliary	Output #5 [5]	De-energized	Pulse	Restore to Time Zone
	Output #6 [6]	De-energized	Pulse	Restore to Time Zone
	Output #7 [7]	De-energized	Pulse	Restore to Time Zone
	Output #8 [8]	De-energized	Pulse	Restore to Time Zone

Click **Status > Outputs > Groups** to display the Groups tab of the Output Status screen:

Figure 47: *Status > Outputs > Groups Tab*



Output Status - Panel 1

Click Group to Toggle Its State

Group1	De-energized	Pulse	Restore to Time Zone
Group2	Energized	Pulse	Restore to Time Zone

The Output Status tab enables you to:

- View the current status of each output in the Discrete tab (Energized or De-energized).
- View the current status of each output group in the Groups tab.
- Energize or de-energize any output or group indefinitely.
- Pulse any output. This energizes the output or group for a configured period of time (see Outputs Tab, page 41).
- Restore the output to its configured time zone. A time zone is a specified time period during which the output will be energized. (see Configuring Time Management, page 26).

Steps:

1. To energize an output or group of outputs for an indefinite period of time, click the **De-energized** button to display a prompt. Click **OK** to complete the change to "Energized."

   To de-energize an output or group of outputs for an indefinite period of time, click the **Energized** button to display a prompt. Click **OK** to complete the change to "De-energized."

2. To Pulse an output or group of outputs for the configured period of time, click the **Pulse** button to display a prompt. Click **OK** to start the pulse. Note that the Pulse button will be greyed out if no output is attached.

3. To reset the output behavior according to its configured time zone, click the **Restore to Time Zone** button to display a prompt. Click **OK** to restore the time zone. Note that the **Restore to Time Zone** button will be greyed out if no output is attached.

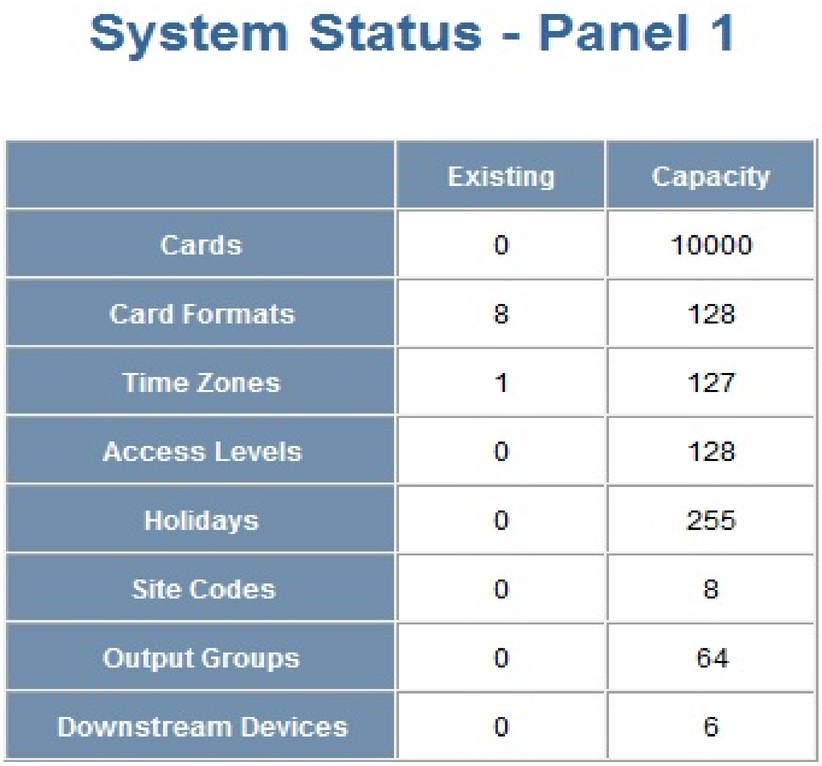
Note: The Output Status screen dynamically refreshes when the output status changes.

4.6 Monitoring System Status

This feature provides basic monitoring of objects in the NetAXS® system other than alarms, events, inputs, and outputs.

Click **Status > System** to display the System Status screen:

Figure 48: *Status > System*



System Status - Panel 1

	Existing	Capacity
Cards	0	10000
Card Formats	8	128
Time Zones	1	127
Access Levels	0	128
Holidays	0	255
Site Codes	0	8
Output Groups	0	64
Downstream Devices	0	6

The System Status screen enables you to:

View the following status of system objects other than alarms, events, inputs, and outputs:

- Number of currently configured instances of the object.
- Maximum number of object instances that can be configured.

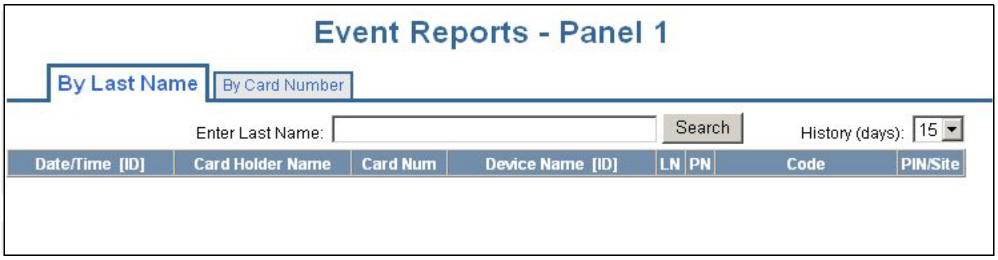
4.7 Generating Event Reports

The Event Report screen enables you to:

- Generate reports of card events by last name.
- Generate reports of card events by card number.

Click **Reporting > Event Reports** to display the Event Report screen.

Figure 49: *Status > Reports > By Last Name Tab*



Event Reports - Panel 1

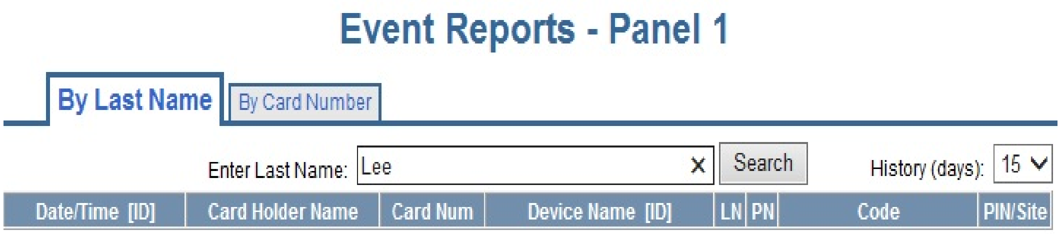
Enter Last Name:

History (days): 15

Date/Time [ID]	Card Holder Name	Card Num	Device Name [ID]	LN	PN	Code	PIN/Site

To generate an Event Report By Last Name:

1. Click the By Last Name tab and enter the card holder's last name in the Enter Last Name box, then click **Search**.



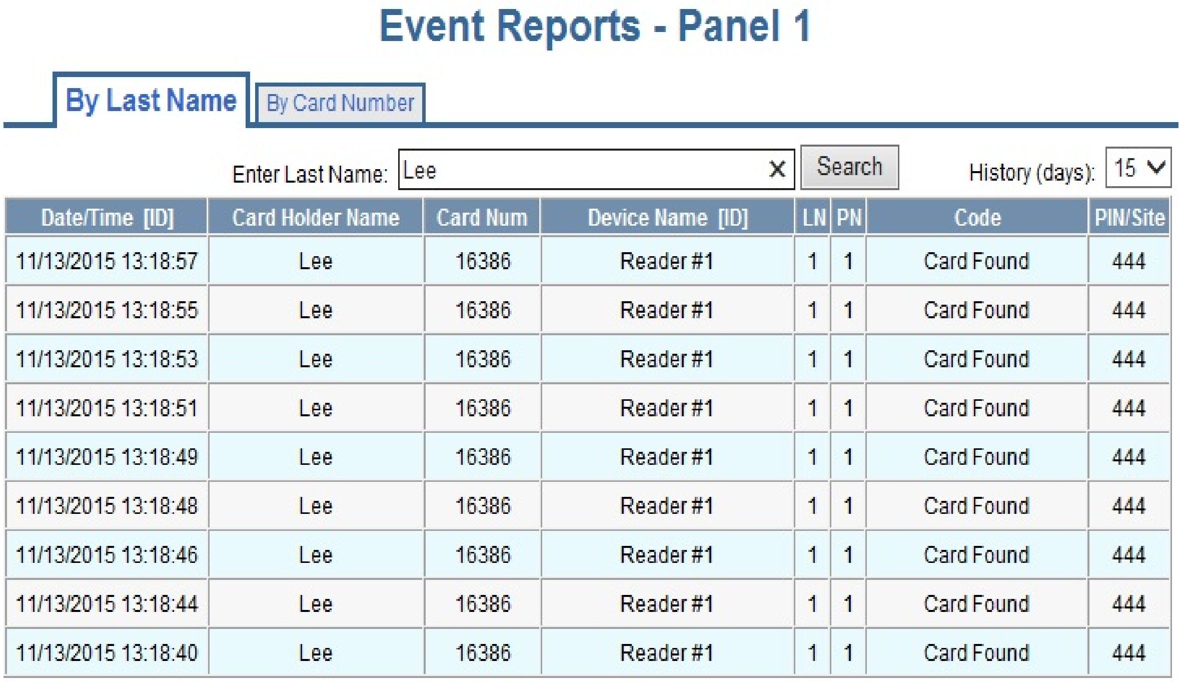
Event Reports - Panel 1

Enter Last Name: Lee

History (days): 15

Date/Time [ID]	Card Holder Name	Card Num	Device Name [ID]	LN	PN	Code	PIN/Site

2. Use the History (days) drop-down list to select the duration of days in history.



Event Reports - Panel 1

Enter Last Name: Lee

History (days): 15

Date/Time [ID]	Card Holder Name	Card Num	Device Name [ID]	LN	PN	Code	PIN/Site
11/13/2015 13:18:57	Lee	16386	Reader #1	1	1	Card Found	444
11/13/2015 13:18:55	Lee	16386	Reader #1	1	1	Card Found	444
11/13/2015 13:18:53	Lee	16386	Reader #1	1	1	Card Found	444
11/13/2015 13:18:51	Lee	16386	Reader #1	1	1	Card Found	444
11/13/2015 13:18:49	Lee	16386	Reader #1	1	1	Card Found	444
11/13/2015 13:18:48	Lee	16386	Reader #1	1	1	Card Found	444
11/13/2015 13:18:46	Lee	16386	Reader #1	1	1	Card Found	444
11/13/2015 13:18:44	Lee	16386	Reader #1	1	1	Card Found	444
11/13/2015 13:18:40	Lee	16386	Reader #1	1	1	Card Found	444

3. Use the descriptions in Table 20 to read the event records.

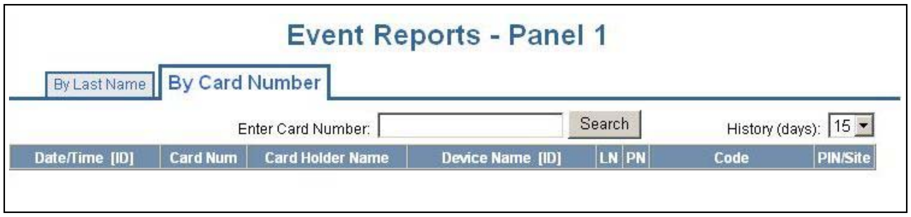
Table 20: *Status > Report Fields*

Setting	Description
Date/Time [ID]	Provides the date and exact time the event was generated, according to the panel's time.
Card Holder Name	Identifies the card holder.
Card Num	Specifies the unique number by which the card holder may be identified.
Device Name [ID]	Identifies the device that generated the event.
LN	**Logical Device Number** - A unique number starting at 1 that is assigned to an alarm generating point. This number is never duplicated on a Controller. There is one exception to this: Door Readers.
PN	**Physical Device Number** - A number at the board level that is assigned to a specific alarm generating point. System alarms such as reset which are not board-specific will report a value of 0. There is one exception to this: Door Readers.
Code	Identifies the current transaction generated by the card. For example, the possible transactions could include: • Card Found • Card Not Found • Time Zone Violation
PIN/Site	Identifies either the PIN or the site code number of the card. Only used to report an event that has an invalid Site Code or invalid PIN.

To generate an Event Report By Card Number:

1. Click on the By Card Number tab and enter the card number in the Enter Card Number box, then click **Search**.
2. Perform Steps 2 and 3 under generating an Event Report by Last Name.

Figure 50: *Event Reports By Card Number Example*



Event Reports - Panel 1

Enter Card Number:

History (days): 15

Date/Time [ID]	Card Num	Card Holder Name	Device Name [ID]	LN	PN	Code	PIN/Site

Upgrading NetAXS® Firmware

A

A.1 NetAXS® Upgrade Procedure

Please see product Release Notes for detailed instructions on how to upgrade panel firmware.

A.1.1 Clearing the Cache in the Internet Browsers Used by the NetAXS® Web Server

The NetAXS® panel supports Internet Explorer 8 (IE8) to IE11, and current Firefox version. For all browsers, we recommend that you clear the cache after a successful upgrade. Please follow your browser instructions to clear the cache.

INDEX

Honeywell Access Systems
135 W. Forest Hill Avenue
Oak Creek, WI 53154
United States
800-323-4576
414-766-1798 Fax
www.honeywellaccess.com

Specifications subject to change
without notice.

Document 800-04410V2, Revision A

Honeywell