Honeywell

NetAXS-123
Version 5.0
Access Control Unit User's Guide

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

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

Chapter 1 Getting Started

Chapter 2 Configuring via the Web Server

LIST OF FIGURES

LIST OF TABLES

(This page is left blank intentionally for double-sided printing.)

Getting Started

1

In this chapter...

1.1 Overview

The NetAXS-123 is a modular 1-, 2- or 3-Door access control system. A NetAXS-123 access control site is configured with a host system and access control units that exceed existing N-1000-III/IV, Pro Series specifications and approvals. These units also communicate with each other and with a variety of input and output devices. Each access control unit, or panel, has three reader ports. Each port can support two readers. For supported configurations, see Compatibility and Interoperation with Other Controllers, page 91.

You can communicate with the NetAXS-123 access control unit either through a host software system or by connecting to the web server through an Ethernet connection. This chapter describes how to connect to the web server.

1.2 Connecting to the Web Server

Notes:

- The NetAXS-123 web server is intended for supplementary and programming purposes only. It has not been evaluated by UL for use as a monitoring station.
- Web server is for supplementary and programming purposes only, and it has not been evaluated by UL for use as a monitoring station.

This section describes three configurations for connecting a computer to the NetAXS-123 web server:

- USB
- Ethernet through a web server direct connection
- Ethernet through a web server hub/switch connection

Note: The 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.

1.3 Setting up the USB Connection

Warning: Do NOT connect the USB cable to the panel until AFTER the drivers are installed.

Follow these steps to set up the NetAXS-123 USB connection.

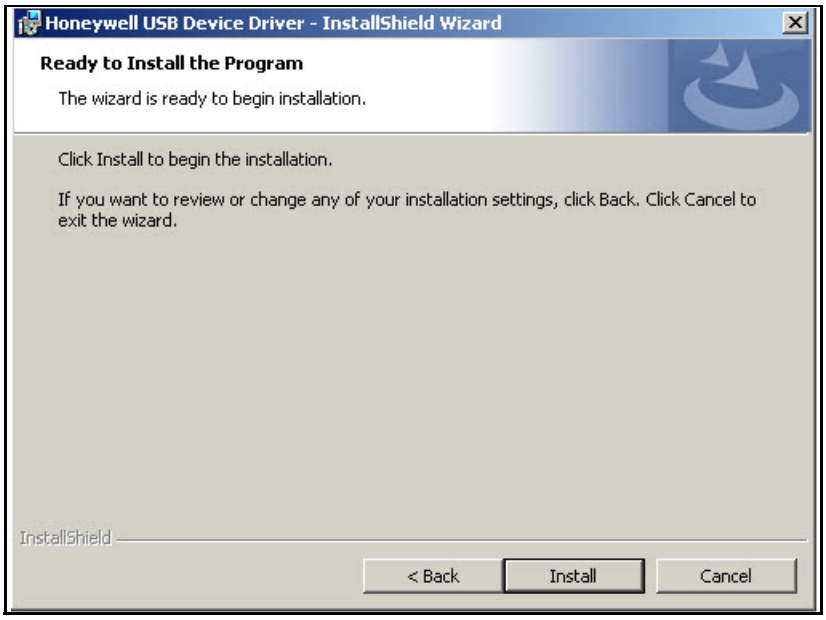
1. Insert the NetAXS-123 Product CD into your Windows-based computer. The NetAXS-123 product menu opens in the web browser.

   Note: If the product menu does not open automatically in your browser, right click on the **Start** button and select **Explore**. In the folder tree, find and click the CD drive that is reading the NetAXS-123 Product CD.

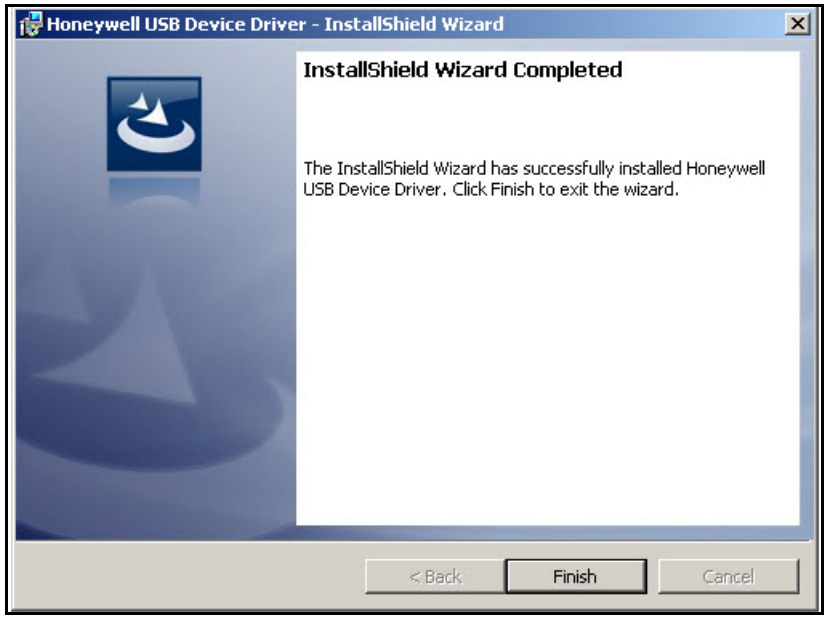
2. Click **Install USB Drivers** on the product menu to start the USB driver installation wizard.

3. Click **Next** to display the Ready to Install the Program screen.

Note: If confirmation dialog boxes pop up before or during the installation, click the appropriate boxes to allow or approve the installation.



4. Click **Install** to initiate the installation.
5. When the installation is complete, the closing screen appears:



6. Click **Finish**.
7. Connect the computer to the NetAXS-123 controller with a USB-A to Micro USB-B cable.
8. Turn on the power to the NetAXS-123 controller.

For login information, go to https://192.168.2.150.

1.4 Setting up an Ethernet Port

There are two options for connecting the panel to a PC via a web server:

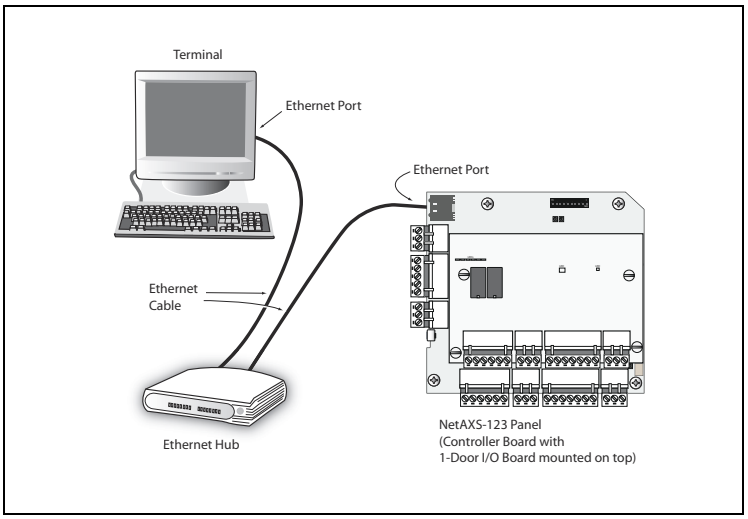
- Using a hub/switch connection
- Using a direct connection

Perform the following steps:

1. Connect your computer's Ethernet port to the panel's Ethernet Port using one of the two following methods:

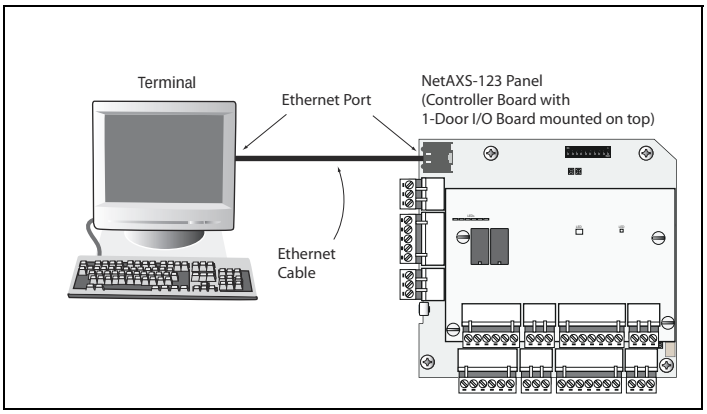
    a. For an Ethernet Hub connection, connect both the computer's Ethernet port and the panel's Ethernet port to an Ethernet hub with standard Ethernet patch cables.

Figure 1-1: NetAXS-123 Web Server Hub Connection



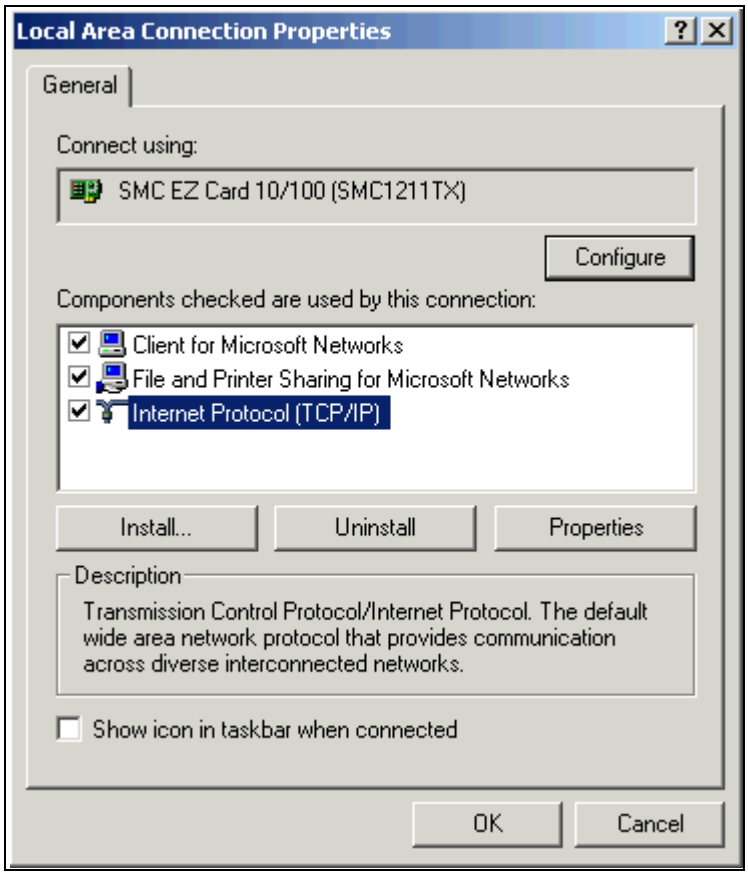
b. For a web server direct connection, connect the computer's Ethernet port directly to the panel's Ethernet port with either a crossover or an Ethernet cable.

Figure 1-2: NetAXS-123 Web Server Direct Connection



2. Configure the computer's network connection:
   a. Select **Start** > **Settings** > **Control Panel**.
   b. Click **Network and Dial-up Connections**.

c. Identify your local Ethernet connection (commonly labeled **Local Area Connection**), and right-click the icon to display the Local Area Connection Properties screen.



d. Highlight the Internet Protocol (TCP/IP) connection.

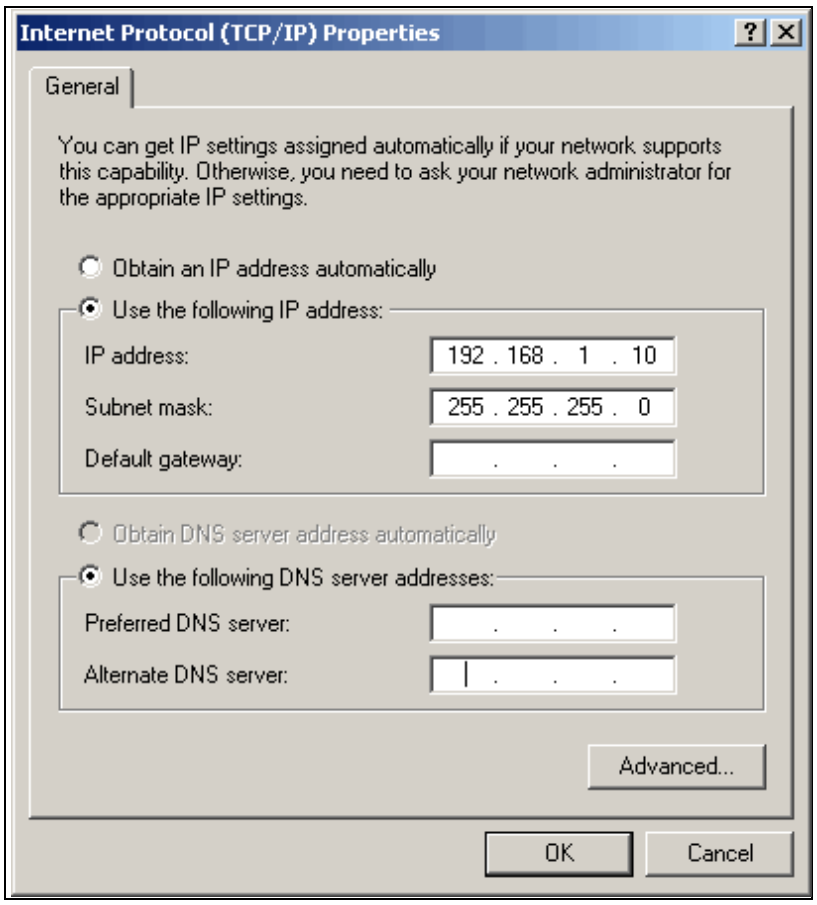
e. Click **Properties** to display your system's current Internet Protocol properties.

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.

f. Select "Use the following IP address."

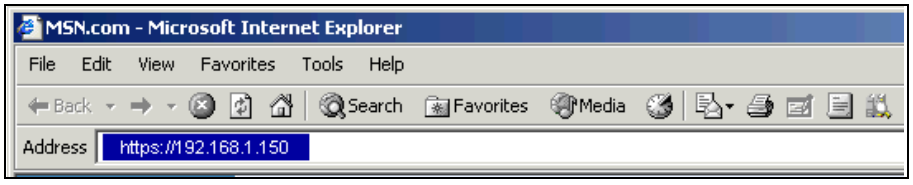
g. Enter "192.168.1.10" in the IP address field.

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



i. 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.



Caution: When connecting to the web using a browser, you must use **https://** for a secure connection. The standard http:// that is the default in most browsers will not work.

4. Press the **Enter** key to display the Honeywell NetAXS-123 login screen.

Note: If you are using Microsoft Internet Explorer 7 and you receive a certificate error message, follow these steps to clear it:

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.

c. Click **Certificate Error** at the top-right of the IP address. The "Untrusted Certificate" screen appears.

d. Click the **View Certificates** bar. The "Certificate Information" screen appears.

e. Click **Install Certificate**. The "Certificate Import Wizard" screen appears.

f. Click **Next** and follow the prompts; leave all settings at their default values. A Security Warning asks if you want to install the certificate.

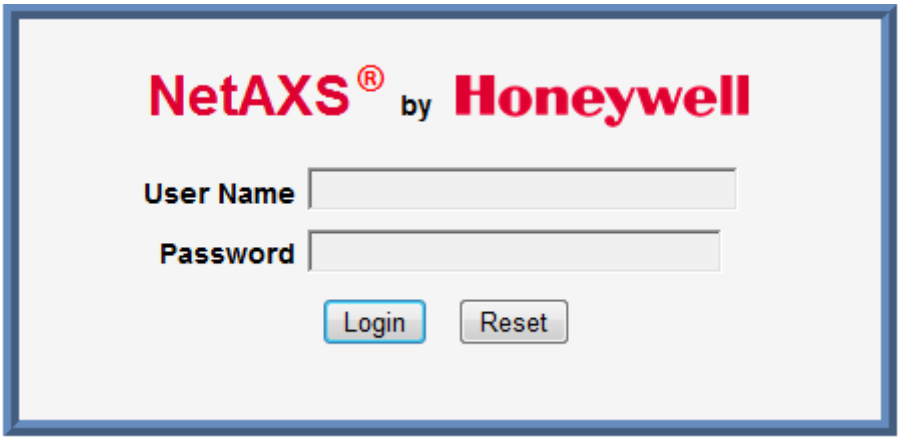
g. Click **Yes**. A Certificate Import Wizard message states "The import was successful."

h. Click **OK**. The Certification Information message appears again.

i. Click **OK**.

j. Close the web browser and re-open it.

k. Enter the IP address again into the URL box. The login screen appears without the certificate error.



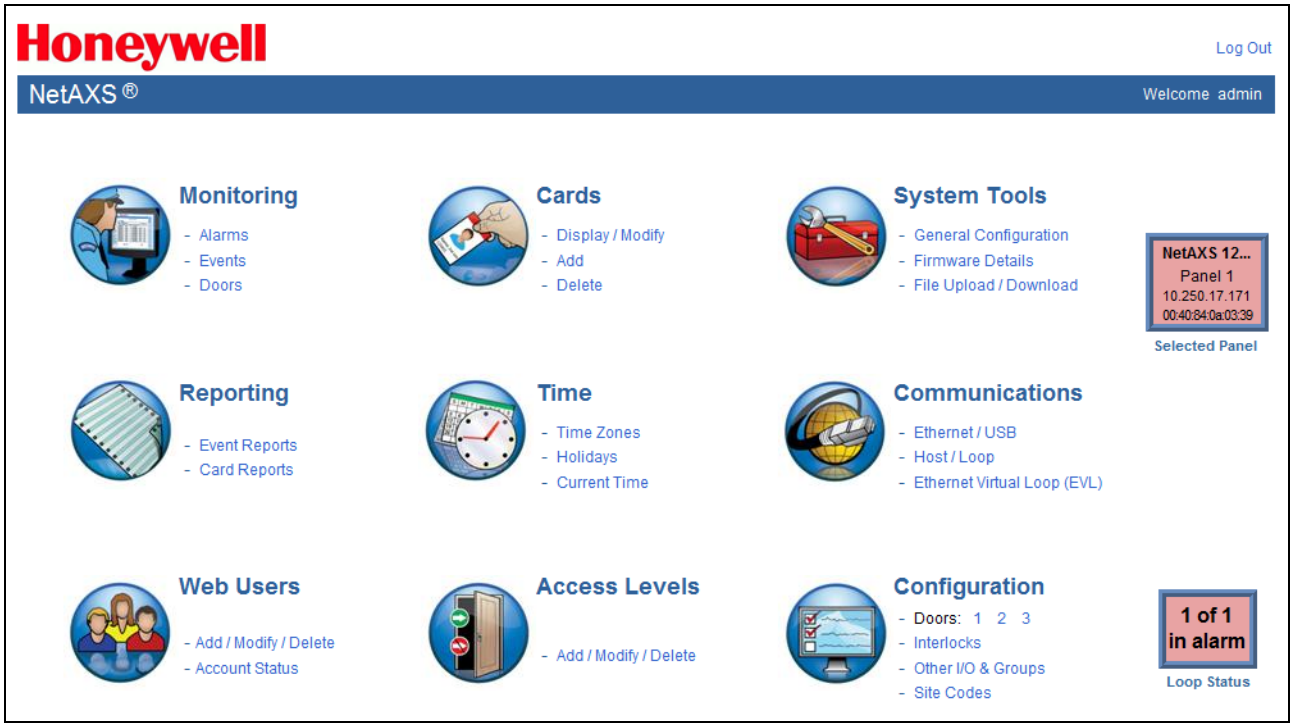
Note: For instructions on certificate errors regarding other supported browsers, see Appendix B, Clearing Cache and Certificate Errors.

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: 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 Configuring Users, page 85.

6. Click **Login** to display the NetAXS-123 Main Window, sometimes also referred to as the "Landing Page".

Figure 1-3: Landing Page



Note: The Panel Selection Frame on the right side of the screen shows the status of the selected Panel. When the gateway is configured to manage a loop of panels, the Panel Selection Frame may be used to select and view/configure other panels. See Panel Selection and Status, page 14, for more information.

1.5 Navigating the Landing Page

The opening screen displays icons representing the functions available.

Table 1-1: *Landing Page Icons*

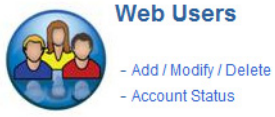
Icon	Description	For more information, see..
	View status monitoring	Monitoring System Status, page 111
	Generate event reports and card reports	Maintaining Cards, page 70 and Generating Reports, page 118
	Create, modify, and delete users, and checks account status	Configuring Users, page 85
	Manage cardholder cards	Maintaining Cards, page 70
	Configure time management	Time Zones Tab, page 46
	Manages access levels	Configuring Access Levels, page 68
	Provides file management functionality	Generating Reports, page 118

Table 1-1: *Landing Page Icons* (continued)

Icon	Description	For more information, see..
	Configure connectivity	Configuring the System, page 26
	Provides system configuration functionality[a]	Configuring the System, page 26

a. The number of doors shown next to this icon reflects the actual number of doors the panel is configured for. The example in the table displays a Controller Board with a 2-door input/output board (I/O board), thus resulting in a total of three doors. A Controller with a 1-door I/O board will report Doors: 1 2. A Controller without an I/O board lists only Door, no numbers.

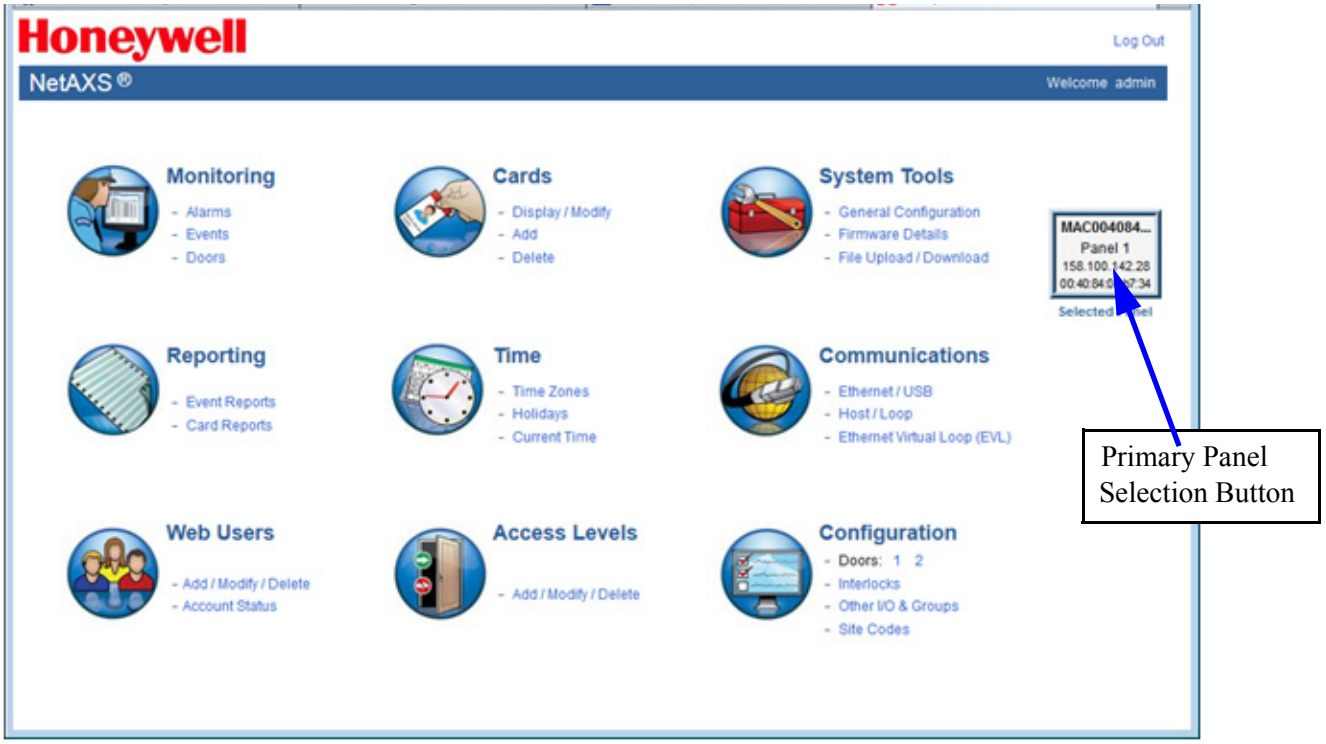
Note: To return to the home page at any time, simply click the Home Page icon. 

1.6 Panel Selection and Status

The right side of the NetAXS web interface is reserved for a panel selection and loop status display area. In previous releases, this was depicted as a 2x16 grid of 32 cells in which each cell represented a specific panel in the 485 loop. The cells conveyed the associated panel's status: whether its panel was online, offline, selected, unselected, 'in alarm' or not in alarm. Specific panels were selected by clicking its associated cell.

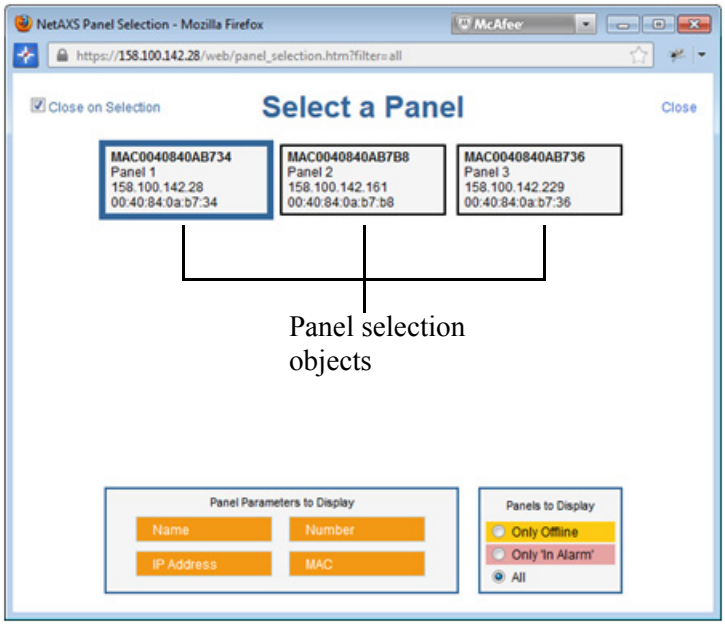
In NetAXS Release 5.0, the grid has been replaced with one to three panel selection buttons. The largest of them is the 'primary' panel selection button, which is always visible and displays information about the currently selected panel (see Figure 1-4, below).

Figure 1-4: Primary Panel Selection Button



When clicked, the primary panel selection button pops up a dialog box which displays the status of all the panels in the loop and allows selection of a different panel. A different panel may then be selected by clicking on the desired panel's selection object (see Figure 1-5, below).

Figure 1-5: Select a Panel Screen



Note: The currently selected panel is highlighted with a thick, dark blue border. Clicking on either of the other two panels causes them to be selected, at which time the dialog disappears. More about this dialog a little later.

There are two other panel selection buttons on the NetAXS web interface which are seen only during specific circumstances. These ‘secondary’ panel selection buttons become visible to notify the user when a panel has either gone into alarm or offline. When clicked, the secondary panel selection pushbuttons also bring up the panel selection dialog box, but with a display that is filtered by whichever secondary panel selection button was clicked. The two secondary panel selection buttons are the Alarm button and the Offline button.

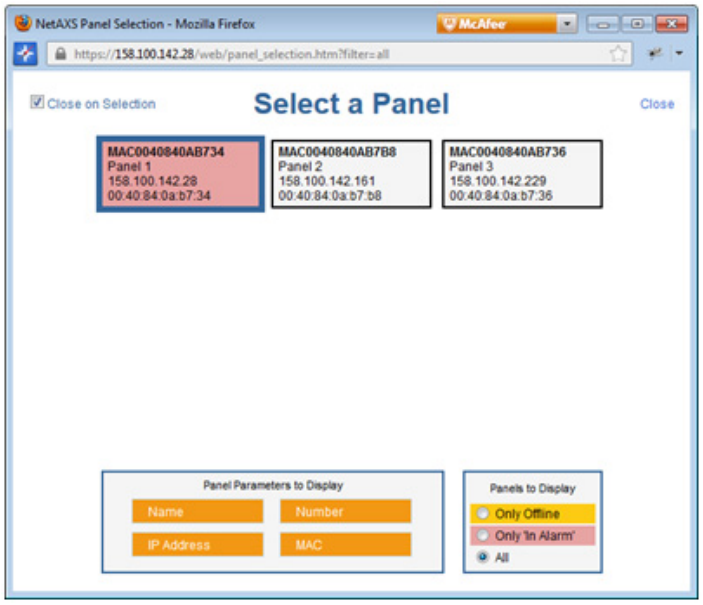
Below is an example of what would be seen when the selected panel – panel 1 – has gone into alarm. The background of the primary panel selection button becomes red in color and the Alarm secondary panel selection button becomes visible (see Figure 1-6).

Figure 1-6: Landing Page with Secondary Panel Selection Button

In this example we have 3 panels connected in an EVL loop. The currently selected panel has gone into alarm and the secondary panel selection button indicates that 1 of the 3 panels now has unacknowledged alarms.

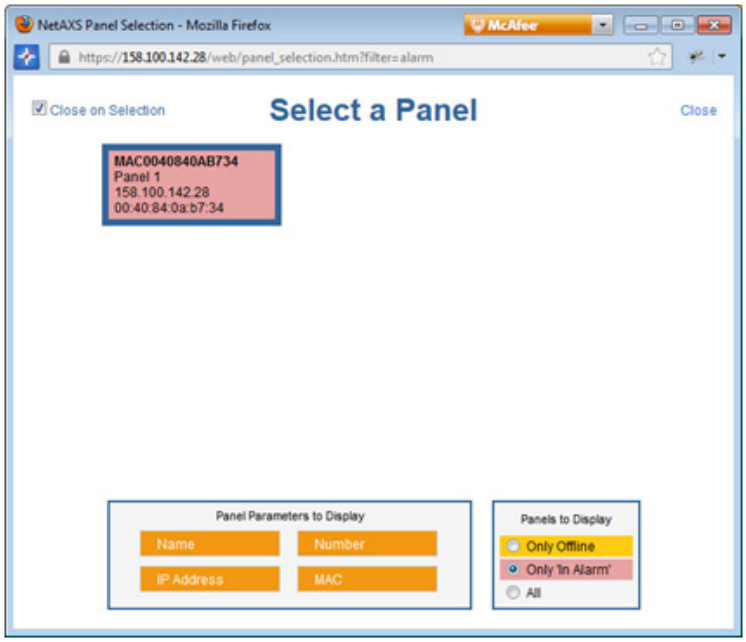
When the primary panel selection button is clicked, the panel selection dialog is brought up showing the status of all the panels in the loop. In this example, the background of the selected panel — panel 1 — is colored red, indicating that it is in alarm (see Figure 1-7).

Figure 1-7: Select a Panel Screen with Panel 1 In Alarm



If the secondary Alarm loop status button is clicked, the dialog would pop up showing only those panels in the EVL loop that are in alarm (see Figure 1-8).

Figure 1-8: Select a Panel Screen with Only In Alarm Panel Showing



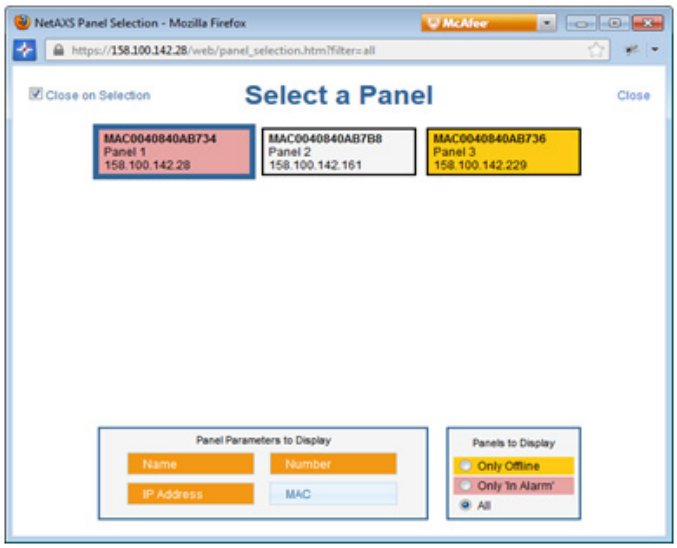
If a panel on the EVL loop goes offline, the other secondary loop status button becomes visible. Its background is colored yellow to indicate a panel has gone offline:

Figure 1-9: Landing Page with Secondary Panel Button Showing Offline

Here, the Offline secondary panel selection button indicates one of the three panels in our EVL loop has gone offline. Now, because there are only 2 panels online (only 2 of the 3 can still report alarms), the Alarm secondary panel selection button displays “1 of 2”.

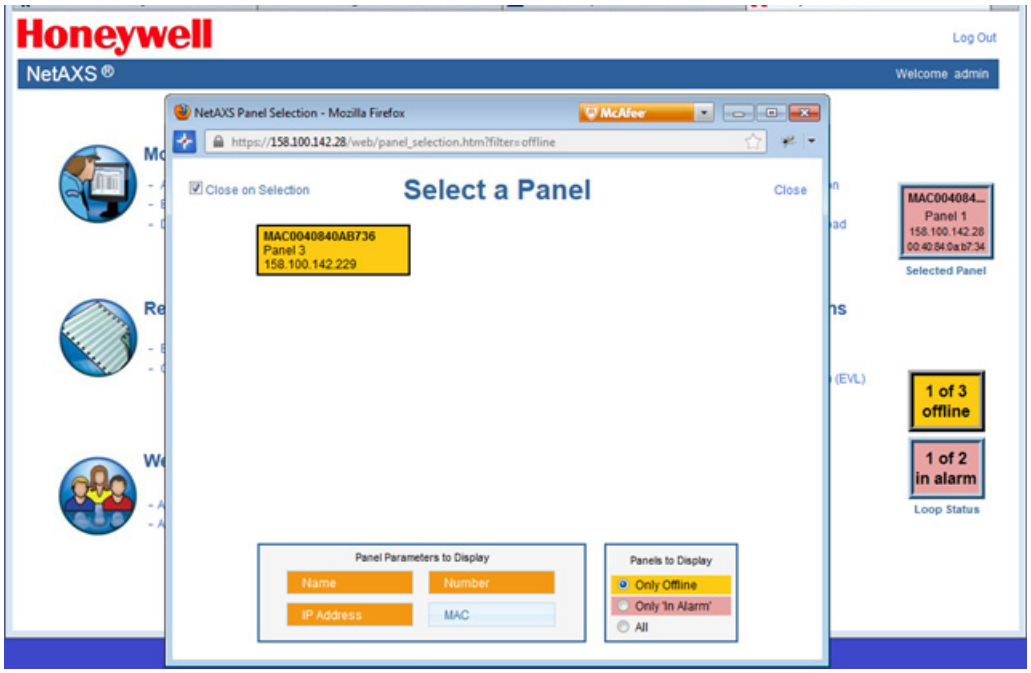
Clicking the primary panel selection button brings up the dialog showing the status of every panel in the loop, with the off line panel colored yellow (see Figure 1-10).

Figure 1-10: Select a Panel Screen with Panel 3 Offline



Clicking the Offline secondary panel selection button brings up the panel selection dialog filtered for only offline panels, as seen in Figure 1-11, below.

Figure 1-11: Select a Panel Screen with Only Offline

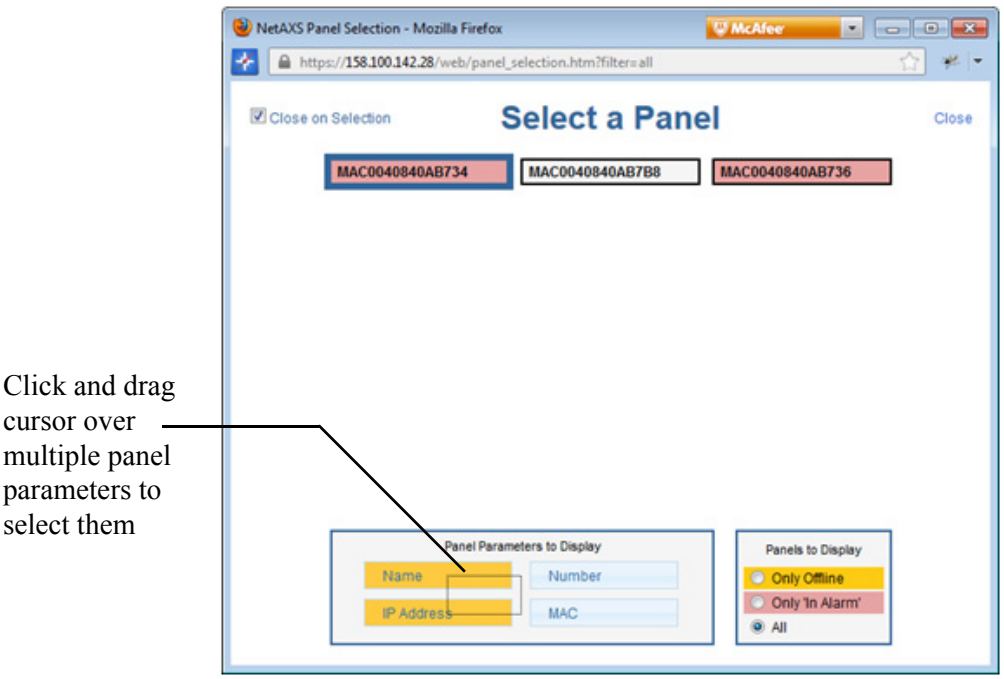


More About the Panel Selection Popup Dialog

There are two areas at the bottom of the panel selection dialog, each containing some controls. The area labeled **Panel Parameters to Display** controls the panel parameters displayed for each panel object in the dialog. Selections include panel name, panel number, IP address and MAC address. Clicking on any single one of them makes that the exclusive parameter displayed for each panel selection object. This mechanism was implemented in order to limit the number of parameters displayed for each panel selection object, and therefore more panels may be shown simultaneously on the dialog.

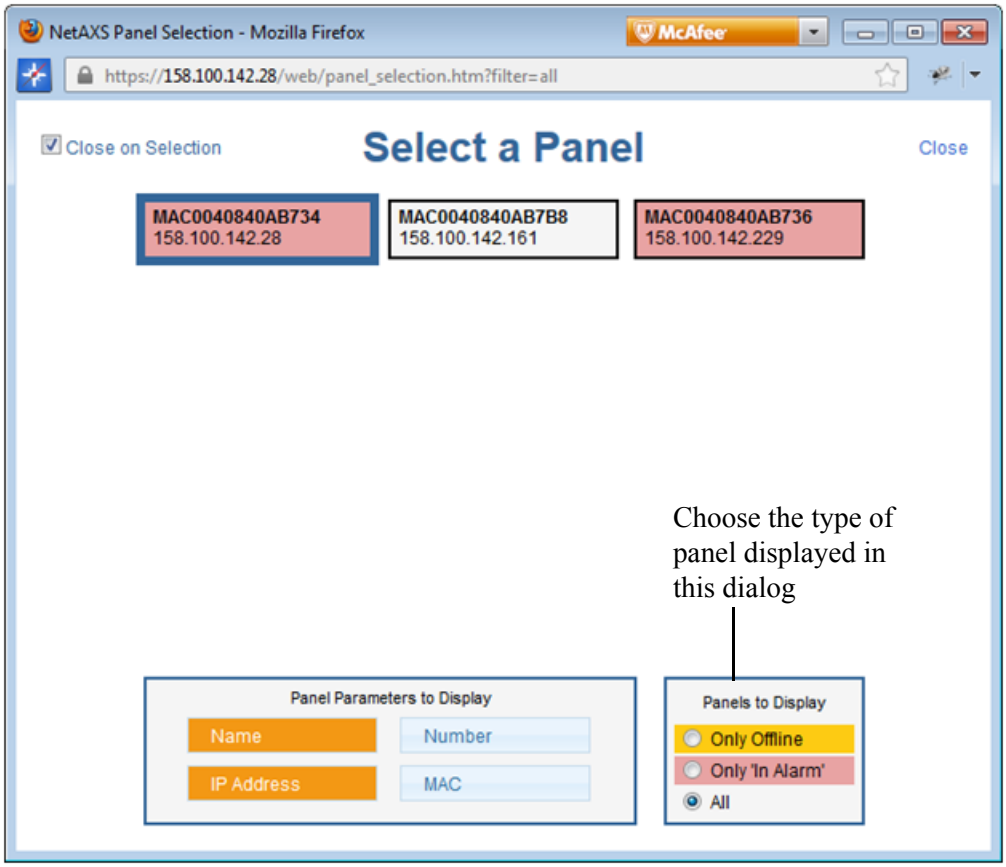
Multiple parameters can be displayed simultaneously either by clicking and dragging the mouse over the parameter display buttons as shown in Figure 1-12 or by pressing and holding the keyboard control key (**Ctrl**) while a selection is made. For example, below, the user chose only panel name to display but is now dragging the mouse to make multiple parameter selections.

Figure 1-12: Clicking and Dragging Mouse to Select Multiple Parameters



The type of panels to display in the dialog is also freely selectable anytime after the dialog is popped up (see Figure 1-13). Choosing “Only Offline”, “Only ‘In Alarm’” or “All” filters the display accordingly.

Figure 1-13: Select a Panel, Choose Type of Panel Displayed



(This page is left blank intentionally for double-sided printing.)

Configuring via the Web Server 2

In this chapter...

2.1 Overview

This chapter explains the NetAXS-123 configuration functions as accessed via the web server. These functions should be performed only by the system administrator or service personnel.

Caution: The sequence of NetAXS-123 configuration tasks is critical. If you do not follow the sequence described in Table 2-1, the system cannot be successfully configured.

Table 2-1: *Configuration Task Sequence*

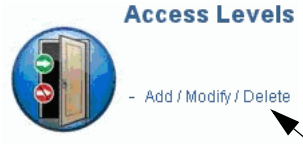
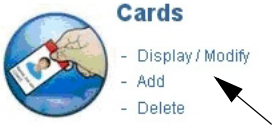
To perform this task...	Click this heading
1. Configure the panel: Host/Loop Communications Network General Site Codes	
2. Configure the time zones.	
3. Configure the doors: Readers Outputs Inputs	
4. Configure the access levels.	

Table 2-1: *Configuration Task Sequence* (continued)

To perform this task...	Click this heading
5. Create the cards and assign access levels.	
6. Modify access levels to cards.	

Note: This guide contains many screen captures. These screens have been captured on a Windows XP platform; they may look somewhat different, depending on your platform.

2.2 Configuring the System

2.2.1 Managing Configuration Data

This section provides an overview of how configuration data is managed on a system of panels interconnected via an RS-485 communications loop.

Some configuration data is common to all panels on the loop. When common data is entered, it is sent to and stored on all panels that are online at the time the data is entered. Common data includes:

- Time Zones
- Cards
- Card Formats
- Holidays
- Access Level Name and Number (access level details are panel-specific)
- System Configuration (Site Codes)

Other data is panel-specific and unique for each panel. Panel-specific data includes:

- Access Level Time Zone Reader Assignments
- Door/Reader Configuration
- System Configuration (General Tab)
- System Configuration (Firmware Details)
- System Configuration (Network) (IP addresses apply only to gateway panel)
- System Configuration (Host/Loop Communications) (applies only to gateway panel)
- Web Users (applies only to gateway panel)

If common data is modified when a panel is off-line, or if a new panel is attached to a loop after common data has been entered, the panel must be manually re-synchronized to obtain the common data. To resynchronize a new panel, you must upload a copy of the gateway panels common and card database and then download to the out-of-sync panel. See Section 5.1, "Backing up and Restoring the NetAXS-123" on page 114 for additional details.

2.2.2 Host/Loop Communications Tab

To maintain your NetAXS-123 system configuration or to monitor its status, you must connect to the panel using one of two modes:

- Host mode (monitor only) – a host software system, such as WIN-PAK™, connects to the panel (through the gateway panel, which has an on-board PCI communications adapter). It enables you to monitor the status of the system.
- Web mode (configure and monitor) – the web server connects to the panel and enables you to configure the panel and monitor system status.

The Host/Loop Communications tab enables you to:

- Select and configure the communication mode you will use to connect to the panel.
- Configure the following host settings:
  - Connection Type (Host or Web)
  - AES Encryption
  - Encryption Key
  - Comms Type
  - Port Number
  - Host IP Address
- Configure the loop:
  - Connection Type (485 or EVL)
    - RS485 — If Gateway provides access to RS485 loop
    - EVL — If Gateway provides access to Ethernet Virtual Loop
  - Time Sync (Enable—how often in minutes the gateway will broadcast its time to downstream panels)
  - Baud Rate (for communication among downstream panels)

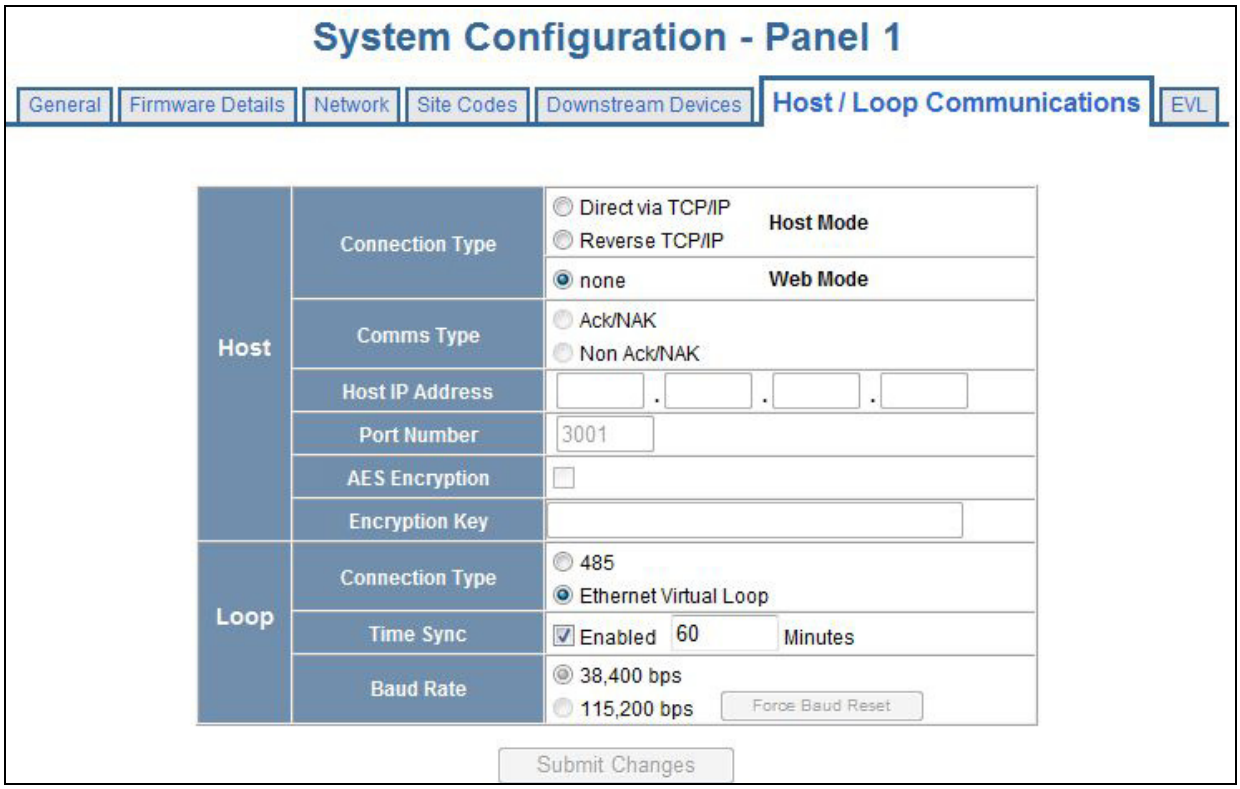
Note: When switching from EVL back to RS485 mode, all EVL Downstream controllers are automatically unregistered from the gateway so that they may be used again as RS485 DS controllers.

Note: When switching from EVL to RS485 mode, if the EVL gateway does not have communications with the DS controller, then the DS controller will remain an EVL controller until it is set back to factory defaults.

Note: Because of the unregistration on switching to RS485 mode, users may want to save the configuration database for later use in the event of a switch back to EVL mode.

Click **Communications > Host/Loop > Host/Loop Communications Tab** to display the Host/Loop Communications Tab.

Figure 2-1: *Communications > Host/Loop > Host/Loop Communications Tab*



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

Table 2-2: *Communications > Host/Loop > Host Loop Communications Tab Fields*

Host/Loop	Setting	Description
Host	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 initiates connection to panel. **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. Panel initiates connection to host. Panel currently does not support encryption. **None** – Select this if you are using web mode.
	Comms Type	Specifies the type of communications. **Ack/NAK** – Provides a response (either an acknowledgment or a non-acknowledgment) 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 acknowledgment or a non-acknowledgment) in a transmission between the host and panel(s). Normally used in troubleshooting only.
	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.
	Port Number	Specifies the port number for the Ethernet port (default is 3001). (Default for Reverse TCP/IP is 5001.)
	AES Encryption	Select this box to select encrypted communication between NetAXS-123 Gateway and WIN-PAK Host.
	Encryption Key	This is the password/key used to encrypt communications between Gateway and WIN-PAK Host. This password must also be entered on WIN-PAK Host.

Table 2-2: *Communications > Host/Loop > Host Loop Communications Tab Fields*

Host/Loop	Setting	Description
Loop	Connection Type	RS485 - If Gateway provides access to RS485 Loop EVL - If Gateway provides access to Ethernet Virtual Loop
	Time Sync	Synchronizes the gateway's time with the downstream panels. **Enabled** – Causes the gateway to automatically broadcast its time to downstream panels in order to time-synchronize the loop. This setting is in minutes, range 60-32767.
	Baud Rate	Specifies the transmission rate (bits per second) among the downstream panels on the loop. **Force Baud Reset** – Tells all downstream panels to change to the selected Downstream baud rate. This saves the user from having to go to each panel individually.

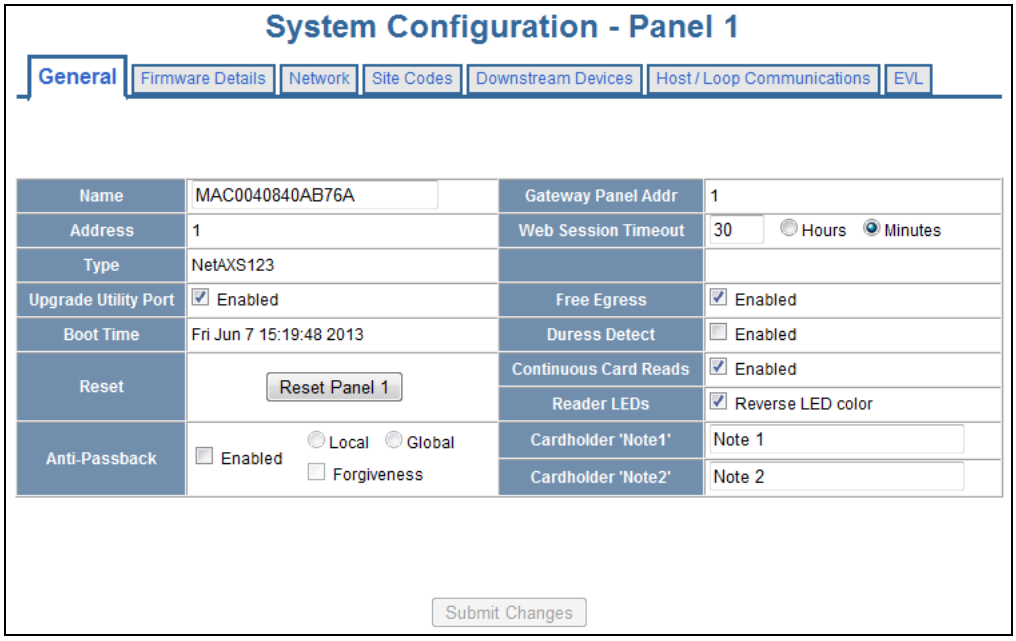
2.2.3 General Tab

The General Tab enables you to:

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

Click **System Tools > General Configuration** to display the System Configuration General tab:

Figure 2-2: *System Tools > General Configuration > General Tab*



Steps: Use the descriptions in Table 2-3 to configure the general settings, and click **Submit Changes**.

Table 2-3: *System Tools > General Configuration > General Tab Fields*

Parameter	Description
Name	Unique name that identifies the panel.
Address	When in EVL Mode, the Panel address is 1 DIPs 1-5 are unused. Displays the address set by the panel's DIP (dual in-line package) switches. See DIP Switch Settings (EVL Mode), page 38 for more complete information on DIP switch settings.
Type	Displays the panel type NetAXS-123.
Upgrade Utility Port	Controls whether a gateway or downstream panel can be updated through Ethernet from a Windows PC (default=enabled). See Upgrading NetAXS-123 Firmware, page 121, for details.
Boot Time	Displays the time that power was applied to the panel.

Table 2-3: *System Tools > General Configuration > General Tab Fields* (continued)

Parameter	Description
Reset	Reboots the panel. A reset does not change the current configuration in the database.
Anti-Passback	**Enabled** – Enables anti-passback, which requires a valid card for entry and exit. The card holder must use his/her card in the proper IN/OUT sequence. If the sequence is invalid, an anti-passback violation is generated and the card holder and is denied access. **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 system 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 card holder 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 (1-59) or hours (1-12).
Free Egress	**Enabled** – Configures the panel for free egress. When enabled (Default), the panel automatically configures inputs 1, 9, and 13 to act as egress inputs for Doors 1, 2, and 3 respectively. If disabled, those inputs 1, 9, and 13 can be used as general inputs.

Table 2-3: *System Tools > General Configuration > General Tab Fields* (continued)

Parameter	Description
Duress Detect	**Enabled** - Enables you to trigger an alarm event and, if configured, pulse an output device in times of duress, such as when the operator is forced to grant access against his will to an unauthorized person. Duress requires both a PIN value and Card number to be recognized, as described below. This feature is available only when the reader is configured with a "Card and Pin" access mode (see Reader A Tab, page 51). This parameter is set to **Disabled** by default. When this feature is enabled, a Duress Output option at the Door's Reader configuration (see Reader A Tab, page 51) is also enabled. You then need to assign the selected output--a Pulse time in Configuration - Other I/O. (See Outputs Tab, page 62 for the output configuration.) During normal operation, the duress output does nothing. To energize the output (for example, during a robbery), the card holder presents his card to a reader that is configured for Card and PIN access (see Reader A Tab, page 51). The card holder then enters a PIN that is either one number higher or one number lower than the correct PIN. 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).
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. This parameter is set to **Enabled** by default.
Reader LEDs	Identifies the color of a reader LED when a grant is authorized. When this parameter is enabled, the LED should be solid red and then turn green after two seconds (by default). This parameter is set to **Enabled** by default.
Cardholder ‘Note1’	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 card holder’s department name. See Adding New Cards, page 70.

Table 2-3: *System Tools > General Configuration > General Tab Fields* (continued)

Parameter	Description
Cardholder 'Note2'	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 card holder's telephone number. See Adding New Cards, page 70.

2.2.4 Firmware Details Tab

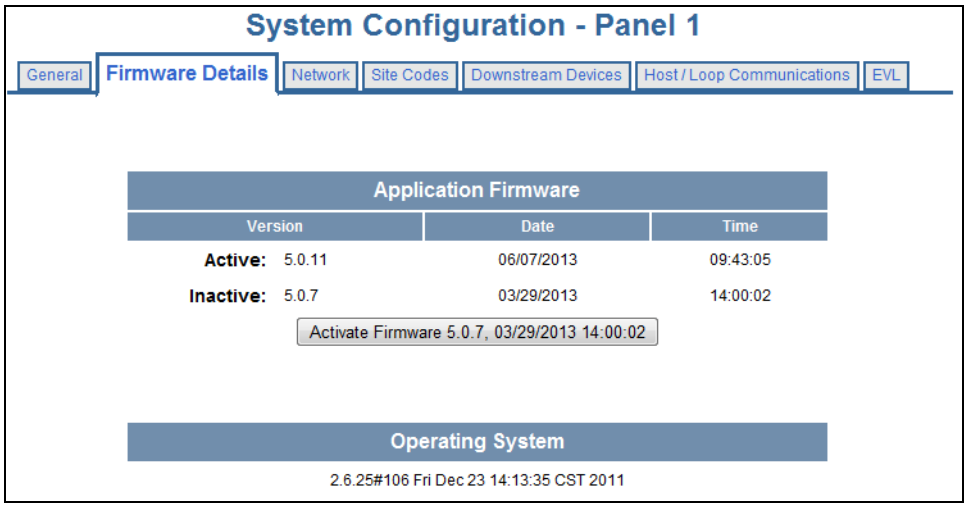
Firmware is software that is embedded in the NetAXS-123 boards. The firmware provides this web interface and all access control functionality. Periodically, the firmware is updated. The Firmware Details tab enables you to download new versions of the firmware, revert to a previous version of the firmware, upload and/or download cards, and configuration databases.

The Firmware Details tab enables you to:

- View the current firmware configuration.
- Revert to another firmware version.

Click **System Tools > Firmware Details** to display the Firmware Details tab:

Figure 2-3: *System Tools > Firmware Details Tab*



To revert to another firmware version:

1. Click **Activate Firmware** to select the firmware version to which you want to revert. The prompt "Switching to an alternate firmware set requires a panel reboot" appears.
2. Click **OK** to reboot the panel.

2.2.5 Network Tab

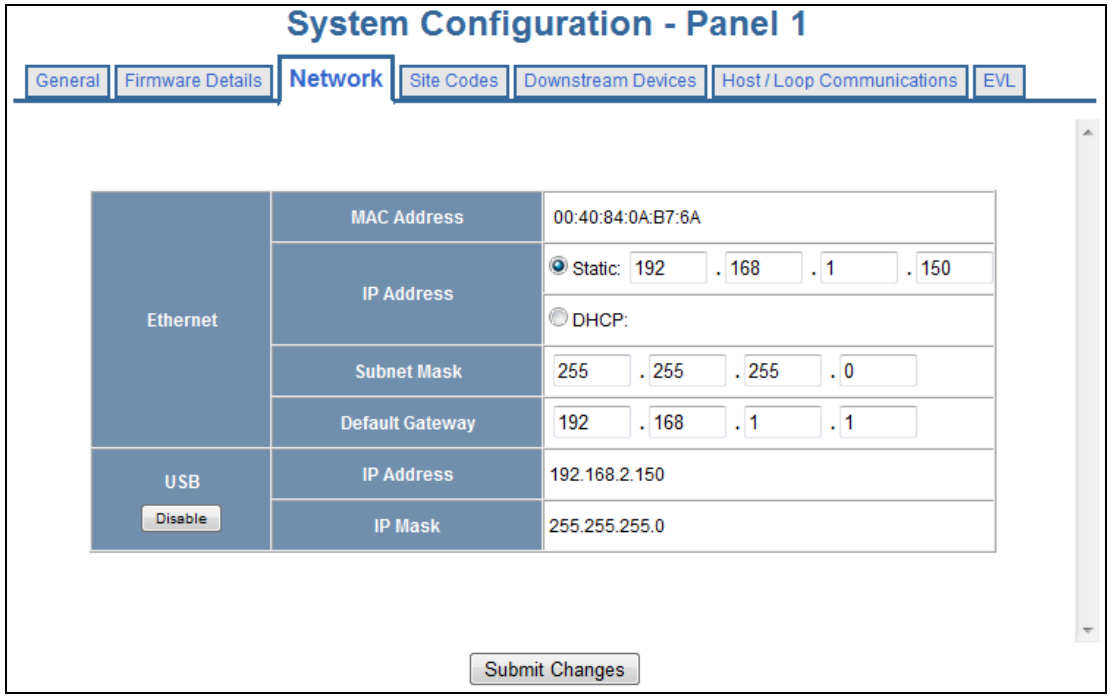
Your NetAXS-123 panel is physically configured in one of a number of possible network configurations. For the panel to function in any of these configurations, the other panels and devices in the network must know the panel's network addresses.

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.
- View, enable, and disable the USB configuration.
- View and edit the panel's USB address.
- View and edit the panel's USB IP Mask.

Click **System Tools > General Configuration** > **Network** Tab to display the Network tab:

Figure 2-4: *System Tools > General Configuration > Network Tab*



Note: Only the Gateway panels address may be modified using this screen. If a Gateway panel is demoted to a downstream controller by setting DIP switch 6 to OFF, the downstream panel will always obtain its IP address dynamically from a DHCP server.

2.2.6 Site Codes Tab

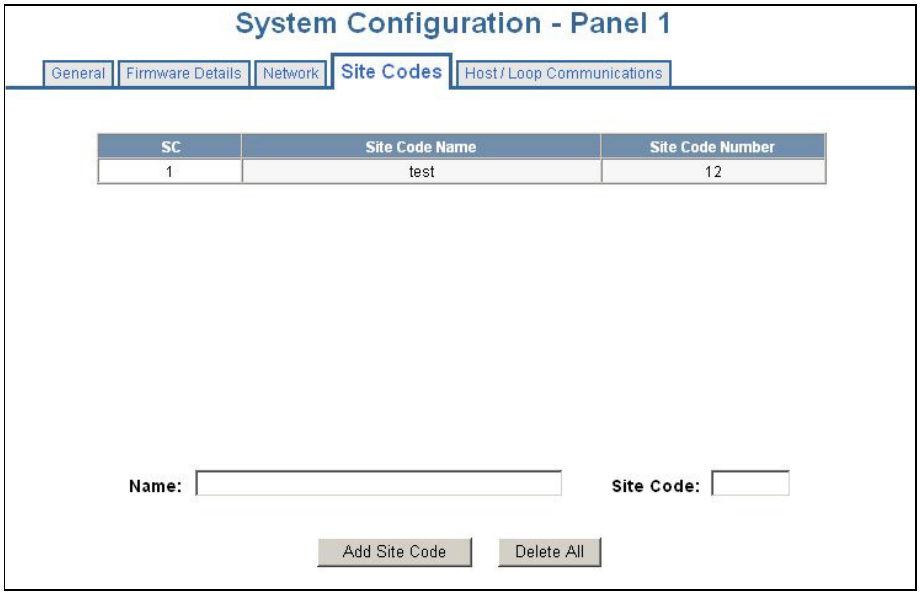
Site codes (also called facility codes) identify an enterprise's site with unique numbers for each site. You can create a maximum of eight site codes to serve as secondary IDs (in addition to the card number) on the card for additional validation.

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.

Click **System Tools > General Configuration > Site Codes** tab to display the Site Codes tab:

Figure 2-5: *System Tools > General Configuration > Site Codes Tab*

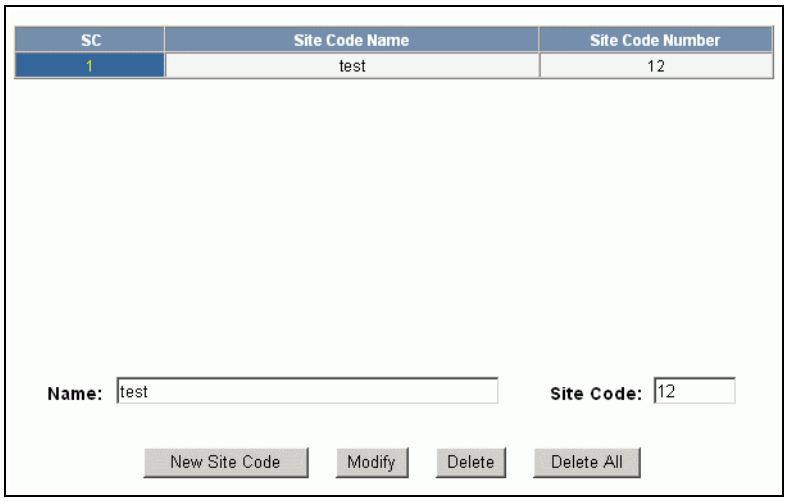


To create a site code:

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.

To modify a site code:

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



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.

To delete a site code:

1. In the Site Code Number 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.

To delete all site codes:

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

2.3 Configuring an Ethernet Virtual Loop

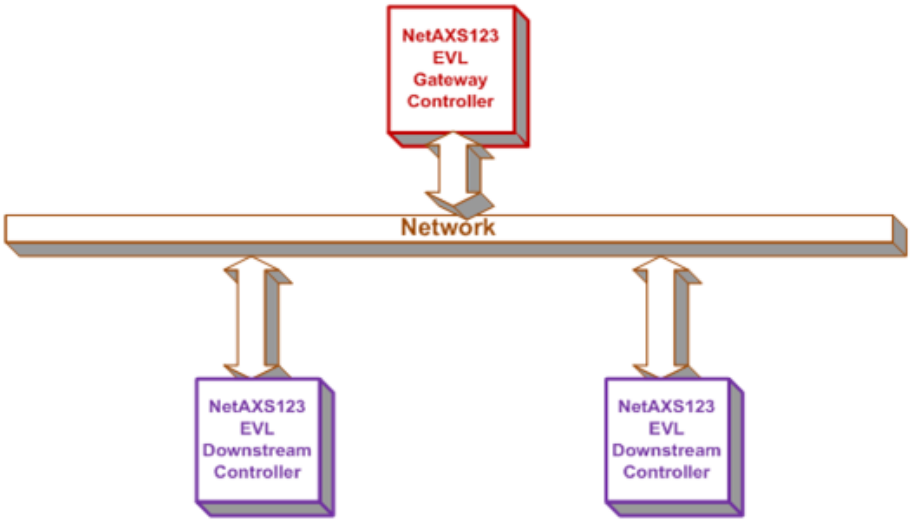
2.3.1 What is an Ethernet Virtual Loop?

An Ethernet Virtual Loop (EVL) allows a group of IP network connected NetAXS123 controllers to be managed as a group, through an embedded Web Server residing on one of the controllers.

Up to 16 controllers may be grouped into an Ethernet Virtual Loop.

The grouping is known as a Virtual Loop since the administration paradigm is similar to an RS-485 loop (featured in prior releases of the NetAXS firmware).

Figure 2-6: *Ethernet Virtual Loop System Diagram*



The EVL capability is new to NetAXS123. This section describes how to set up a Group of Ethernet connected panels to form an **Ethernet Virtual Loop** using the NetAXS123 Web Interface.

2.3.2 Panel Requirements

NetAXS123 panels must first be upgraded to Firmware Release 5.0.16 (or later). Installation instructions are provided in the document: Release Notes - NetAXS-123 Firmware Release 5.0.16.

2.3.3 Network Requirements

The controllers should be connected to a common IP sub-network that provides dynamic address assignment through DHCP.

2.3.4 DIP Switch Settings (EVL Mode)

When a NetAXS123 Panel is used in EVL mode, DIP switches 1-5 are not used to identify the panel. Instead, the panel is identified by its MAC address. When setting

up an EVL loop, it will be helpful to create a list of MAC addresses for all Panels and what doors they control. This will be useful later when the panels are configured.

It is recommended that DIP switches 1 through 5 be set as factory default:

- DIP switch 1: **ON**.
- DIP switches 2 through 5: **OFF**.

One of the controllers must be the Gateway controller. Select one of the EVL controllers as Gateway by setting DIP Switch 6 to **ON**.

The other controllers must have DIP switch 6 set to **OFF** and are known as Downstream controllers.

Table 2-4: *Gateway DIP Switch Settings (EVL Mode)*

DIP Switch	Setting
1	On
2	Off
3	Off
4	Off
5	Off
6	On
7-10	Off, On, On, Off

Table 2-5: *Downstream DIP Switch Settings (EVL Mode)*

DIP Switch	Setting
1	On
2	Off
3	Off
4	Off
5	Off
6	Off
7-10	Off, On, On, Off

2.3.5 Creating an Ethernet Virtual Loop

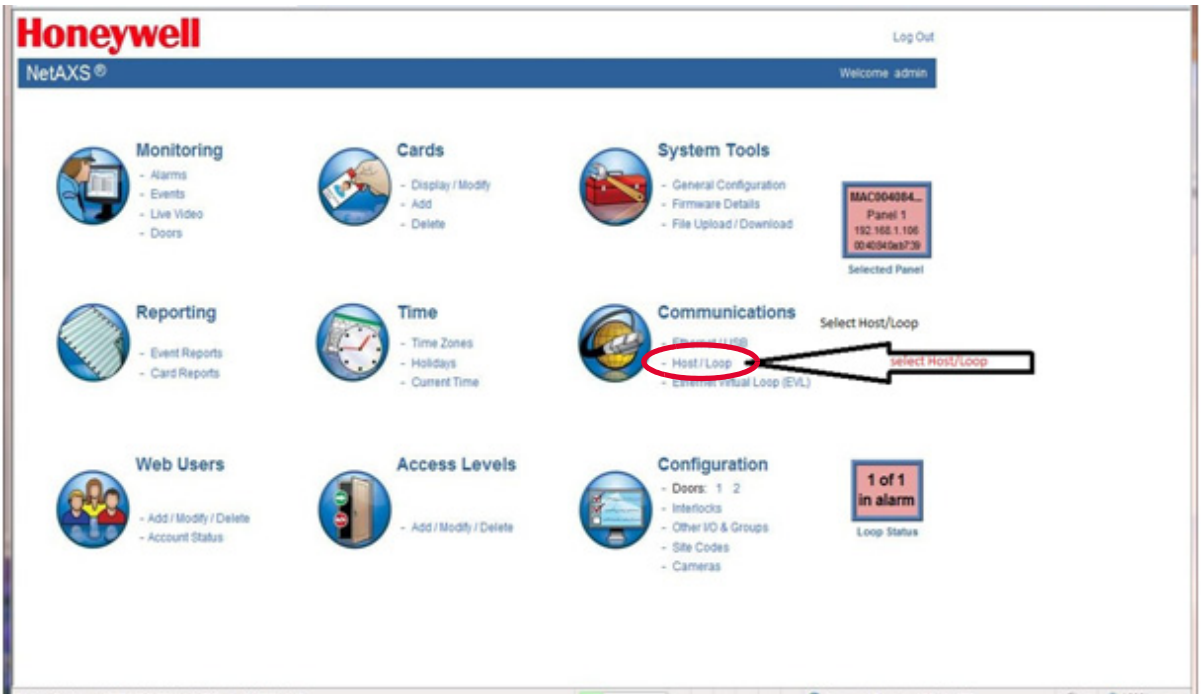
Connect all Controllers to a common IP network. The Downstream IP controllers must have DIP switch 6 set to **OFF**, and will be configured using the Gateway controller.

1. Log into NetAXS123 Gateway Panel from a browser through the USB (192.168.2.150).

   Instructions may be found in Setting up the USB Connection, page 4.

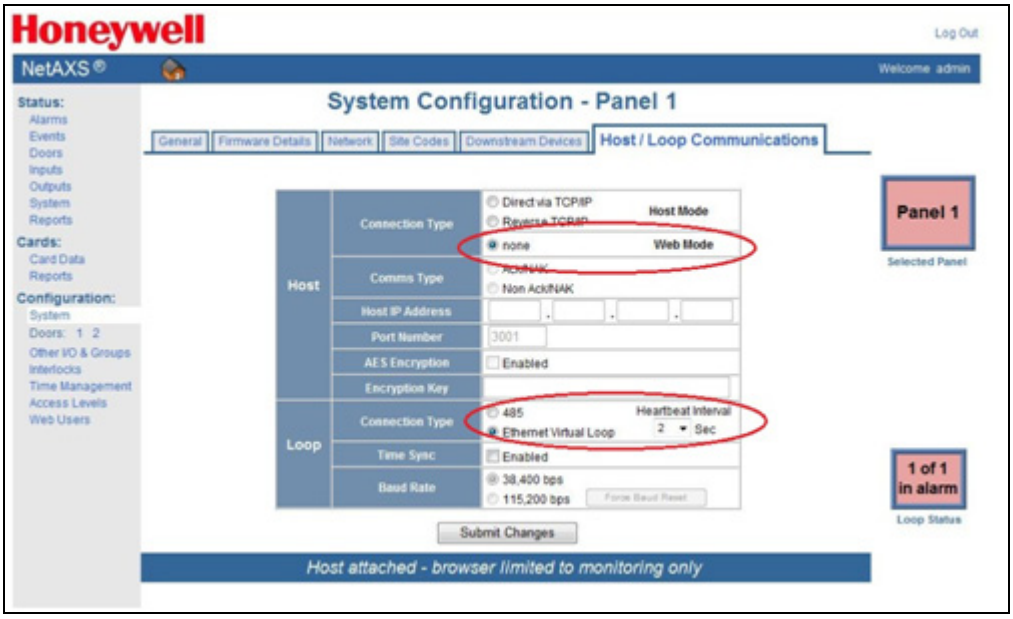
2. Navigate to Host/Loop Communications Screen.

Figure 2-7: *Landing Page with Selecting Host/Loop*



3. Set up Communication attributes (see Figure 2-8):
   a. Select **Web Mode** as **Host Connection Type**.
   b. Select **Ethernet Virtual Loop** as **Loop Connection Type**.
   c. **Submit Changes**, then **Reboot** when prompted.

Figure 2-8: *Host/Loop Communications Set for EVL*



4. Log into NetAXS123 panel.

   Instructions may be found in Setting up an Ethernet Port, page 6.

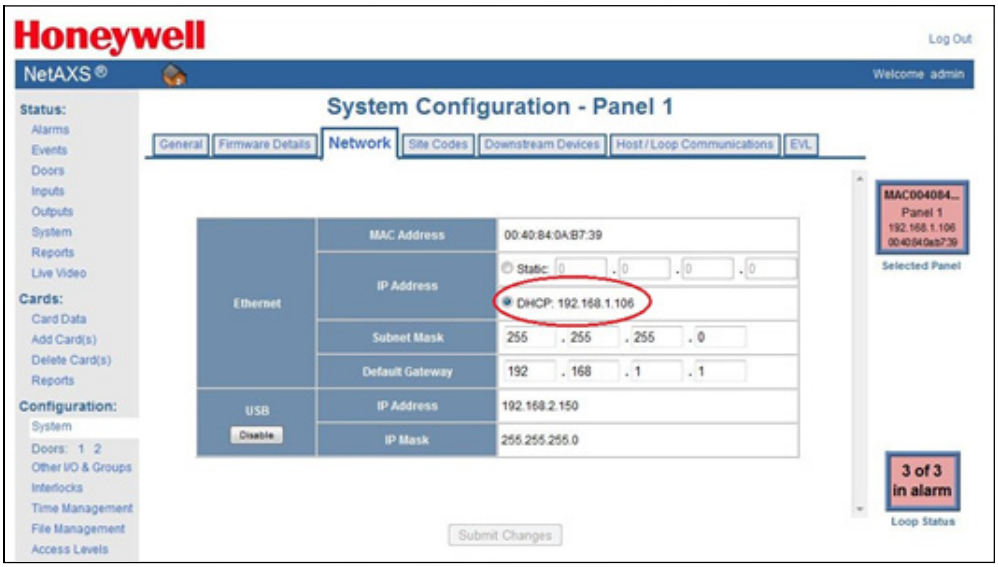
5. Set up Network Configuration (see Figure 2-9):

   a. Navigate to the **Network** tab.

   b. Select DHCP or enter Static IP address assigned to Gateway Panel.

   c. Submit Changes, then Reboot when prompted.

Figure 2-9: *Network Configuration for EVL*



6. Log into Gateway controller from browser.

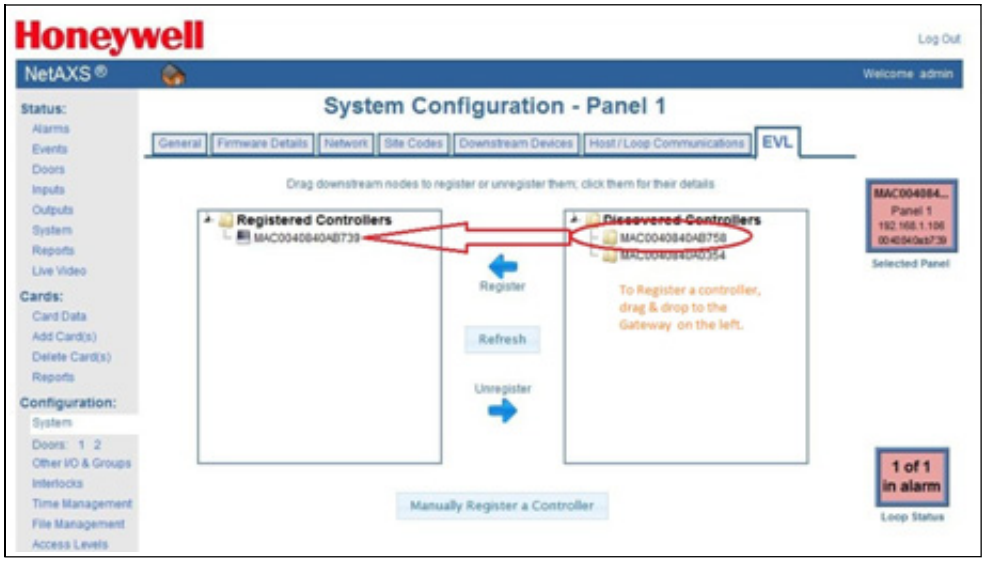
   Instructions may be found in Setting up an Ethernet Port, page 6.

7. Register Downstream EVL controllers (see Figure 2-10):

   a. Navigate to the **EVL** tab.

   b. Drag & Drop controllers listed on the right to the left (on TOP of the gateway controller) as shown in Figure 2-10.

Figure 2-10: *Registering Downstream Controllers*



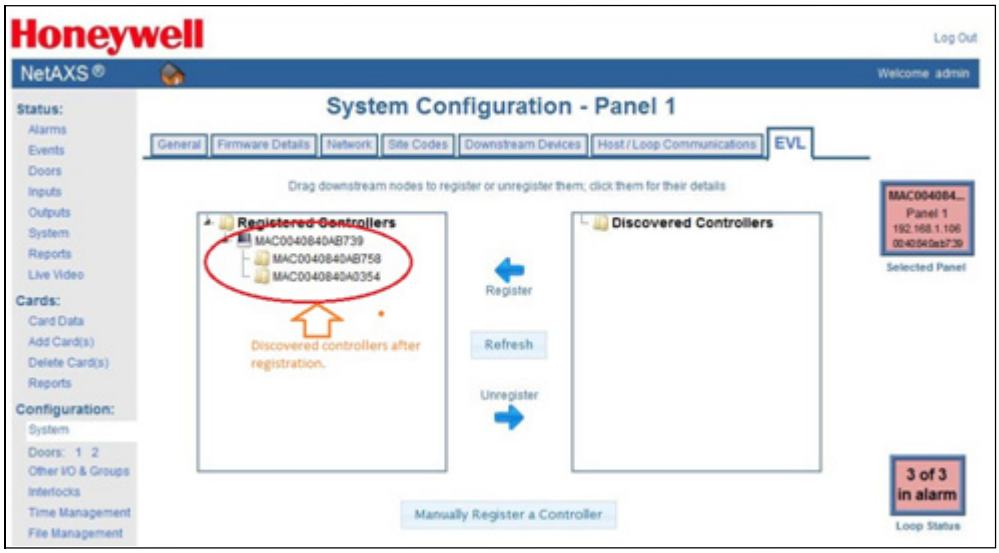
   c. Repeat step b) for all controllers to be registered.

Note: This screen is not dynamic. If a new panel becomes operational after the screen is rendered, you will need to click **REFRESH** for it to appear in the **Discovered Controllers** pane.

   d. After registration, the Downstream controllers will be listed under **Registered Controllers** (see Figure 2-11). The **Loop Status** box will show the status of all Controllers (including the Gateway).

Note: After controllers are registered, they may be highlighted as yellow, indicating that the controller is not yet connected. Once connected, you may need to refresh the screen to clear the highlighting.

Figure 2-11: *Downstream Controllers Now Registered*



You have now finished creating an Ethernet Virtual Loop.

2.4 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.

2.4.1 Current Time Tab

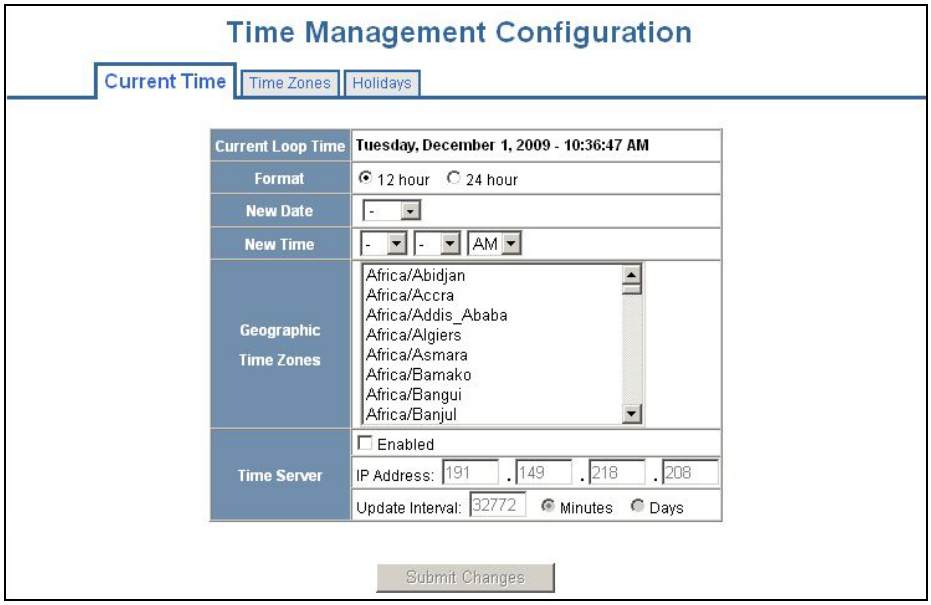
The Current Time tab displays time management configuration settings.

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 IP address of the time server being used.
- Force a time synchronization between the panel and the time server.

Click **Time > Current Time > Current Time** tab to display the Current Time tab:

Figure 2-12: *Time > Current Time > Current Time Tab*



Steps: Use the descriptions in Table 2-6 to configure the time settings:

Table 2-6: *Time > Current Time > Current Time Tab Fields*

Setting	Description
Current Loop Time	Displays by default the current time setting in Day / Month Date / Year - HH:MM:SS AM/PM
Format	**12 hour** – The 24-hour day is divided into two 12-hour halves, AM and PM; each half is numbered 1-12. **24 hour** – The hours in the 24-hour day are numbered consecutively 0-23. **Note**: Format does not affect Alarms and Events Display format as they are always reported in 24-hour time format.
New Date	Specifies a new date to be the current date. Use the drop-down 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 drop-down lists to set the hour, minute, and AM or PM.
Geographic Time Zones	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 Time Server that the Gateway will poll to update its time. **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. 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.

2.4.2 Time Zones Tab

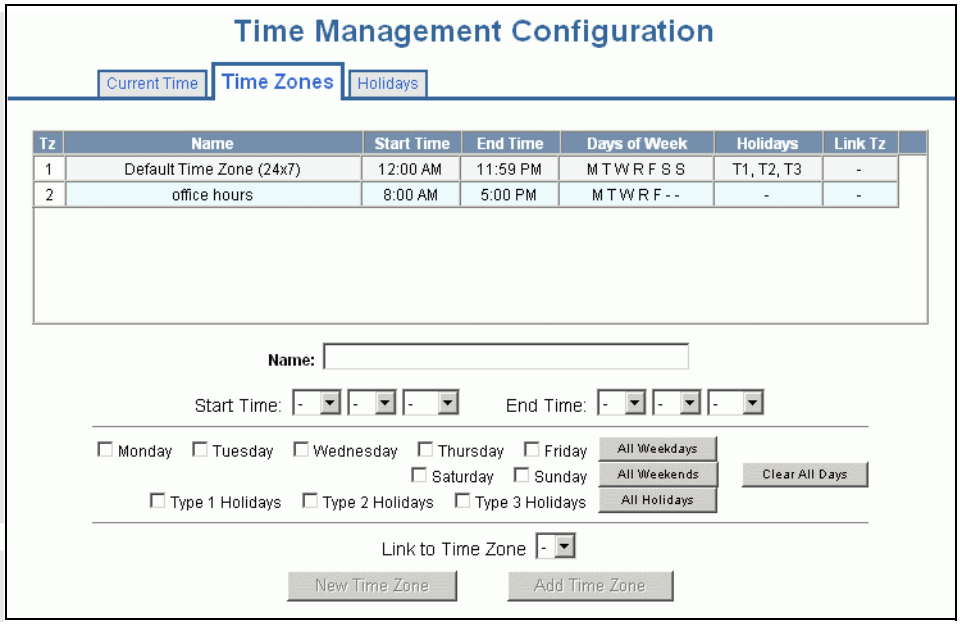
The NetAXS-123 panel controls access by using time zones, or time schedules. Inputs, outputs, readers, access levels, and cards through access levels are all configured with time zones by which they will be energized or de-energized, enabled or disabled. For example, you might assign a group of outputs to be energized from 12:00 AM to 6:00 AM. every day. The 12:00 AM to 6:00 AM, Sunday through Saturday, time period is called a time zone.

The Time Zones tab enables you to:

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

Click **Time > Time Zones > Time Zones** tab to display the Time Zones tab:

Figure 2-13: *Time > Time Zones > Time Zones Tab*



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 before you link time zones. An example is provided to help you create the links successfully.

5. Click **Add Time Zone**.

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 **Modify** to accept the changes.

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 **Delete**.
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 AM to 11:59 PM. 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, and Inputs 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.

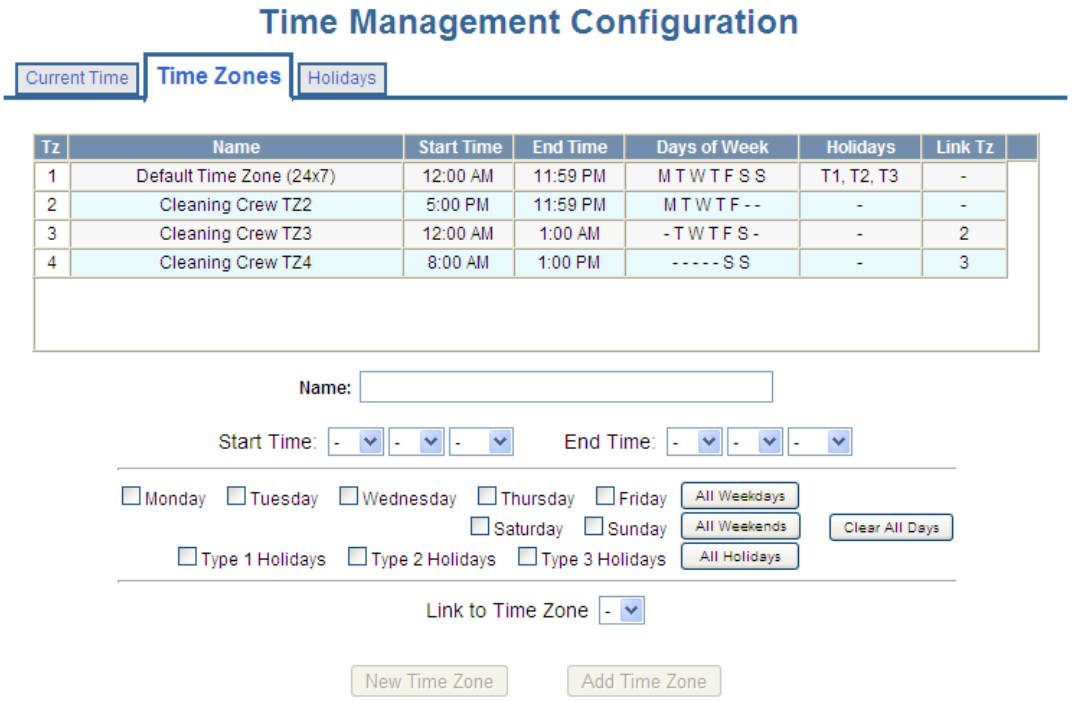
For example, suppose you must create a Cleaning Crew Time Zone. The time zone(s) are to be set up as follows: Monday-Friday 5 PM -1 AM, Saturday and Sunday 8 AM-1 PM, no holidays. This becomes three separate time zones, as follows.

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

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

So, you 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 PM and an end time of 11:59 PM. 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 AM and an end time of 1:00 AM. 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 AM and an end time of 1:00 PM. 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-123 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.

2.4.3 Holidays Tab

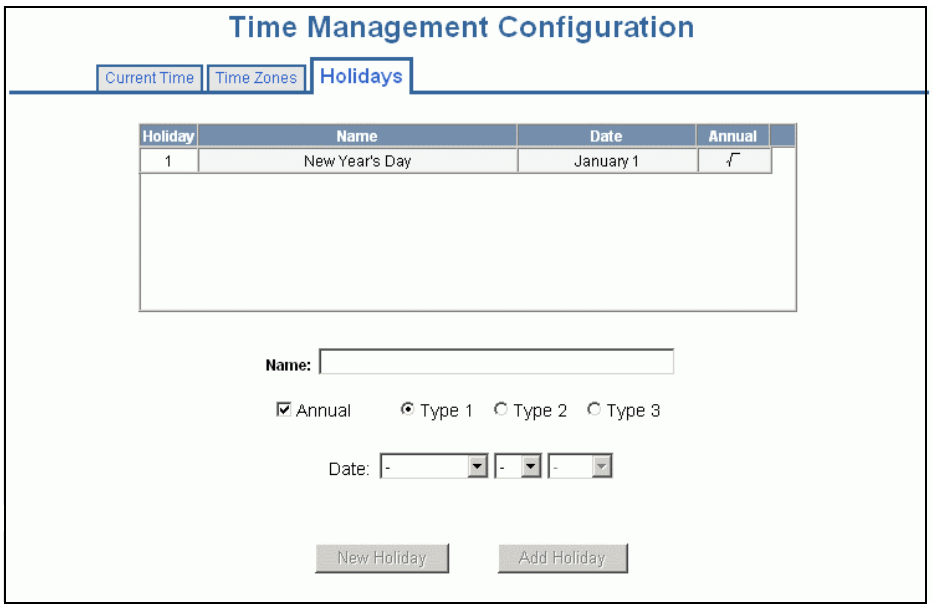
Holidays are considered special days of a week. They are similar, but of higher rank than the standard Monday-Sunday. If a day programmed as a Holiday should occur in the panel, the panel will treat that day as the Holiday type, regardless of the actual day of the week (Monday-Sunday). During this Holiday,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

The Holidays tab enables you to:

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

Click **Time > Holidays > Holidays** tab to display the Holidays tab:

Figure 2-14: *Time > Holidays > Holidays Tab*



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** check box.
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 46).
4. Select the holiday's month and date from the drop-down lists.
5. Click **Add Holiday**.

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 panel can support three different Holiday Types (Type 1, Type 2, and Type 3), but a user can only select one type per day. Also, note that 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.

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 **Modify** to accept the changes.

To delete a holiday:

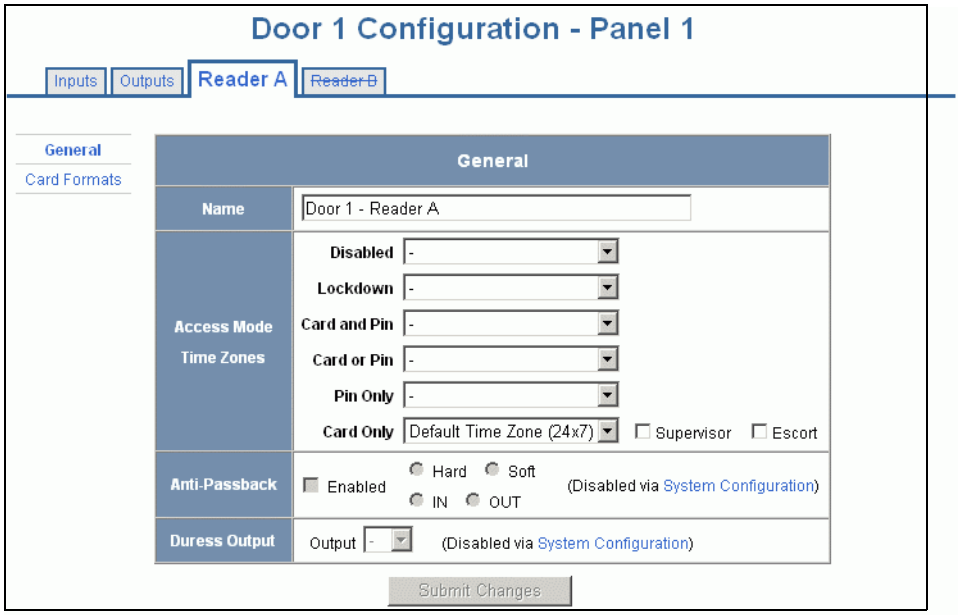
1. In the Holiday column, click the number of the holiday you want to delete.
2. Click **Delete**.
3. Click **OK** at the delete prompt.

2.5 Configuring the Doors

Each panel supports from 1-3 doors. For each door, you must configure the readers, inputs, and outputs.

Click **Configuration > Doors: 1** to display the Door Configuration screen for door 1.

Figure 2-15: *Configuration > Doors: > 1 > Reader A Tab*



Follow the same procedures described below to set up doors 2 and 3 if your setup includes them.

2.5.1 Reader A Tab

A reader is a device that reads cards and sends the card data to the panel. The NetAXS-123 supports two readers per door. Reader B may be activated and de-activated by the user.

The Reader A tab enables you to:

- Name the Reader.
- Define a time zone during which the reader will follow one or more of the access modes below:
  - Disabled
  - Lockdown
  - Card and PIN
  - Card or Pin
  - PIN Only
  - Card Only
- Further define the Card Only, PIN Only, Card and PIN, and Card or PIN access modes

- Configure reader for anti-passback.
- Specify the card formats the reader must use to read the card data.
- Add, edit, and delete card formats.

Click **Reader A** to display the Reader A tab (see Figure 2-15).

Steps:

1. Use the descriptions in Table 2-7 to configure the General reader settings.

Table 2-7: *Configuration > Doors > 1 > Reader A Tab Fields*

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** – Disabled mode puts the reader in a state where all card reads are ignored, with the exception of a VIP card, which is allowed access. Contact and Egress will report, but Egress will not cause the door to open. **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 entry at the door's keypad. **Pin Only** – Grants access with only a valid PIN 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 access and the LED displays a steady red. After the supervisor presents his card twice to allow general access, he can disable the general 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.

Table 2-7: *Configuration > Doors > 1 > Reader A Tab Fields* (continued)

Setting	Description
Access Mode (continued)	**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.
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.

Table 2-7: *Configuration > Doors > 1 > Reader A Tab Fields* (continued)

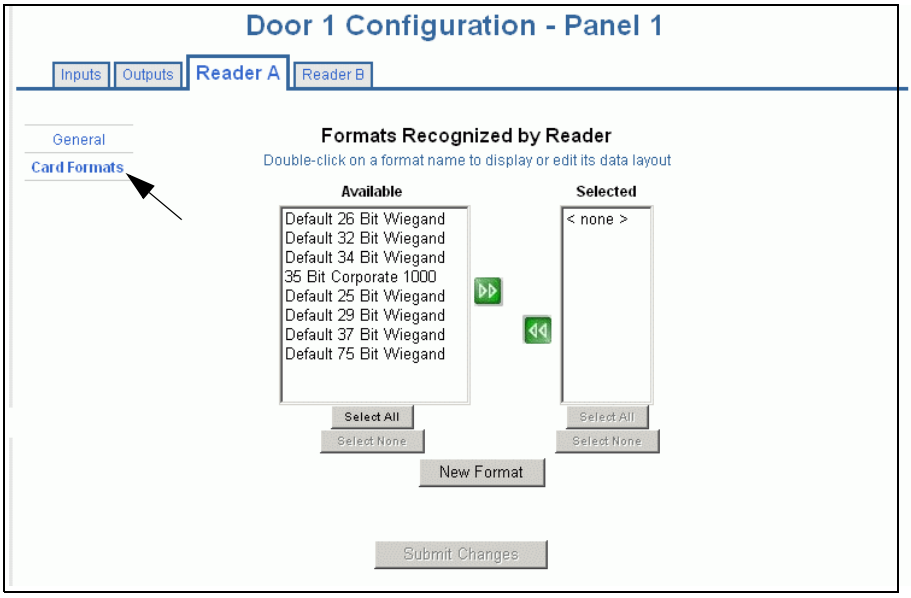
Setting	Description
Anti-Passback	Configures the anti-passback feature. Once configured under Configuration > System > General screen (see General Tab, page 30), the user enables the anti-passback feature on the reader, which requires a valid card for entry and exit. The card holder must use the card 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. **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.

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 70 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 2-16: *Configuration > Doors: > 1 > Reader A Tab > Card Formats*



3. Use the descriptions in Table 2-8 to select card formats.

Table 2-8: *Configuration > Doors: > 1 > Reader A Tab > 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.

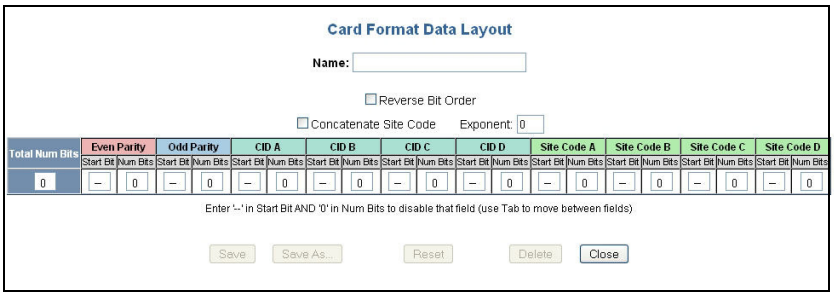
4. Click to highlight each desired card format listed in the Available box, and click the green right arrow button to move the format(s) into the Selected box.

Note: If you select no formats, the reader will use all available formats (up to 128) as described for the Available setting in Table 2-8. 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, as described for the Selected setting in Table 2-8.

5. Click **Submit Changes.**

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

Figure 2-17: *Card Format Editing Screen*



7. Use the field descriptions in Table 2-9 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 2-9: *Configuration > Doors: > 1 > Reader A > 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).
Concatenate 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.

Table 2-9: *Configuration > Doors: > 1 > Reader A > Card Format Fields*

Setting	Description
Even Parity	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. If the Card ID of the card format has multiple parts, CIDs B, C, and D may be used to specify which parts are to be concatenated to form the Card ID.
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.
CID 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.
CID 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.

Table 2-9: *Configuration > Doors: > 1 > Reader A > Card Format Fields*

Setting	Description
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.

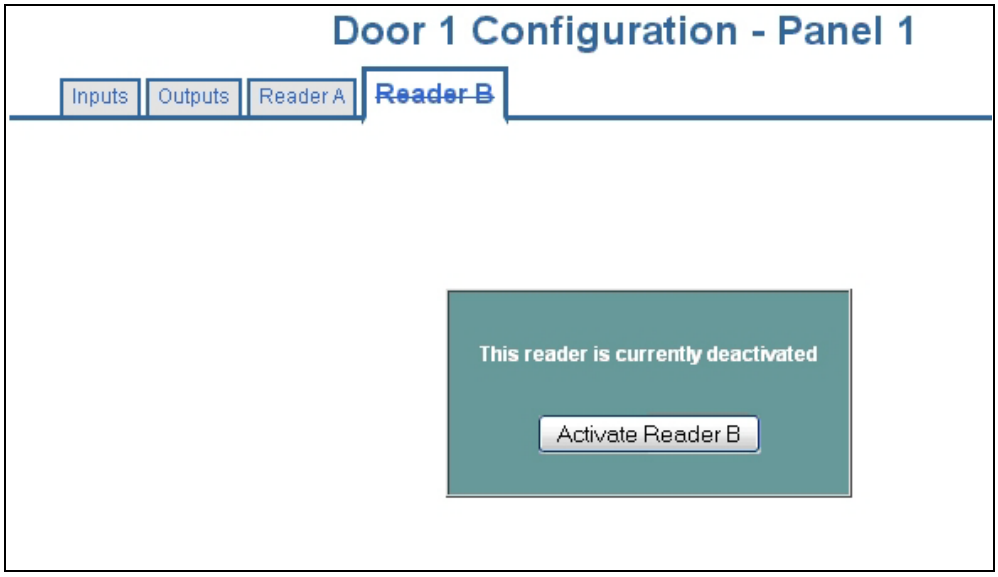
8. If you want to change an existing card format's data layout, double-click the format's name on the list of existing formats to display the Card Format Data Layout screen. Use the descriptions in the table above to edit the layout's fields. Then, click **Save** (to save in the format's current name) 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**.

2.5.2 Reader B Tab

When Reader B is activated, Reader A and Reader B may be multiplexed to the same reader port. Multiplexed readers must support hold lines and be wired according to guidelines in the Installation Guide. The multiplexed reader configuration supports readers on opposite sides of the same door, and the readers must be assigned the same Egress and Status Inputs (if configured). Multiplexed readers may also be assigned the same door lock.

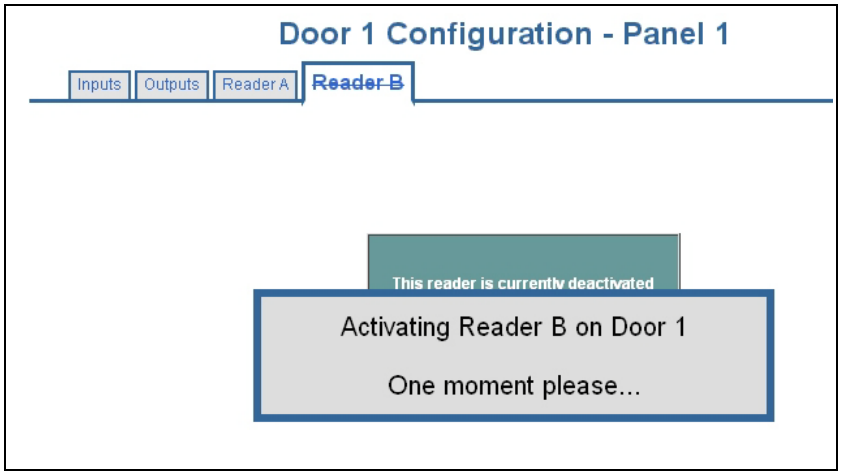
On the Reader A tab, click the **Reader B** tab to display the Reader B tab.

Figure 2-18: *Configuration > Doors: > 1 > Reader B Tab*



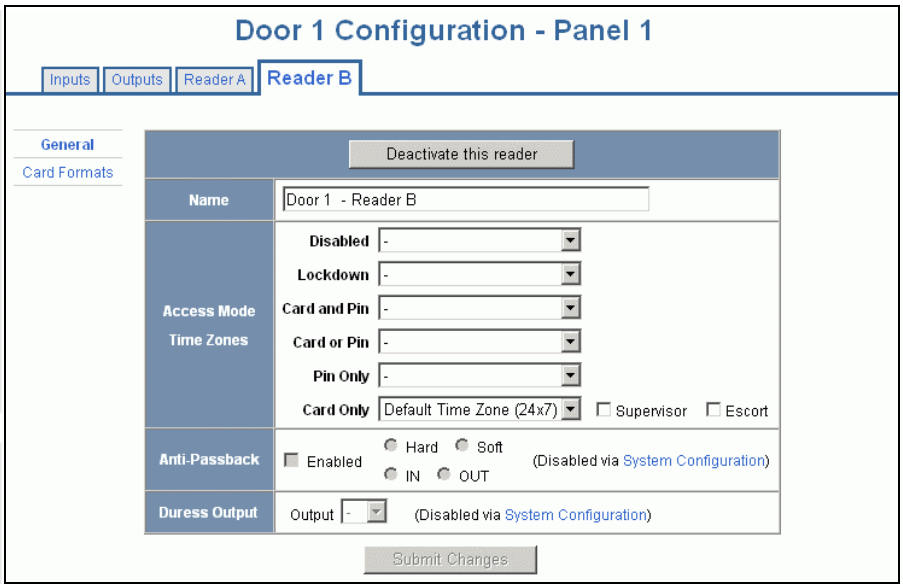
Click **Activate Reader B** to display the following "activation in-progress" screen:

Figure 2-19: *Reader B Activation In-Progress Message*



When Reader B is fully activated, the system displays the following screen:

Figure 2-20: *Reader B Fully Activated*



Note: The Supervisor and Escort mode settings checked for Reader A also apply to Reader B. However, these settings can be edited only on the Reader A tab—they cannot be edited on the Reader B tab.

Click **Deactivate this reader** to deactivate Reader B.

2.5.3 Outputs Tab

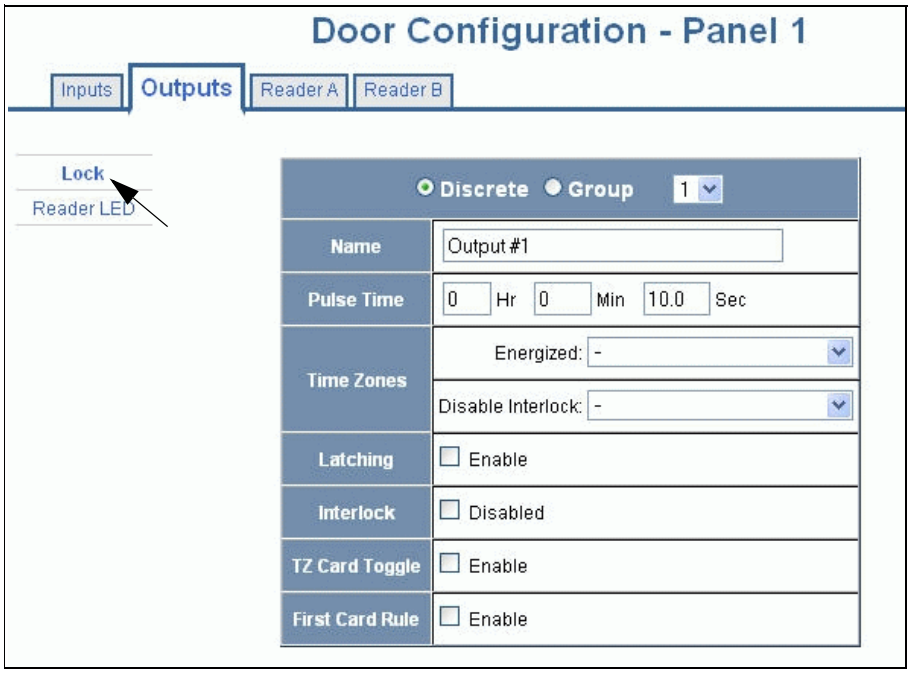
An output, or output relay, acts like a switch on the panel that either energizes or de-energizes or pulses an output device, such as a door lock or an LED. For example, a successful card read at a reader (input device) causes the output relay switch on the panel board to change the normal state of a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

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

Click **Configuration > Doors: > 1 > Outputs** tab to display the Outputs tab. The **Lock > Discrete** tab appears, enabling you to configure an individual lock output. Select the output number in the drop-down list at the top of the screen. Note that lock and reader LED outputs are associated with each of the doors on a NetAXS-123 panel.

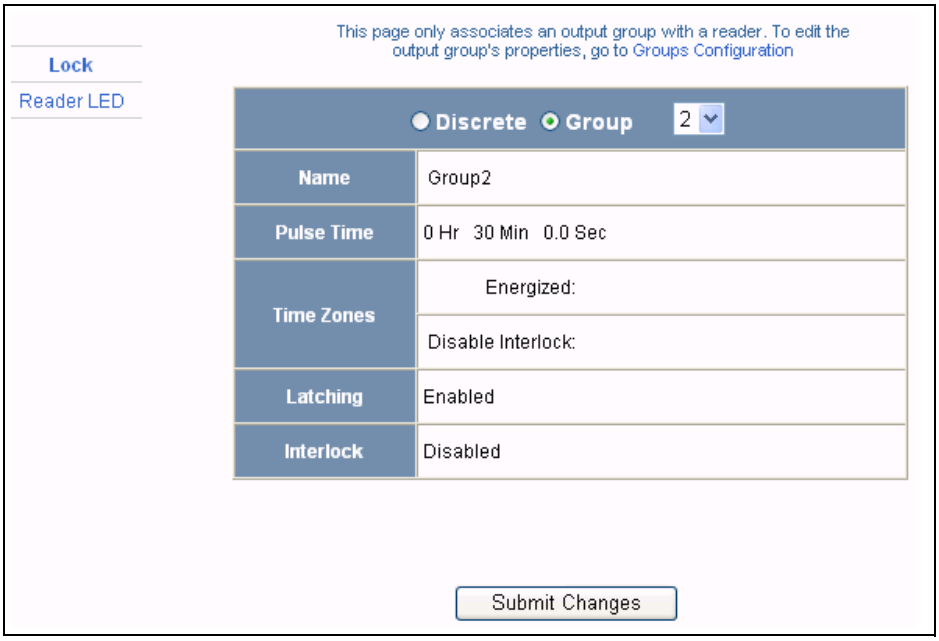
Figure 2-21: *Configuration > Doors > Outputs > Lock > Discreet*



To view a configuration of a group of outputs, click **Group** and select the group number from the drop-down list at the top of the screen. The group configuration

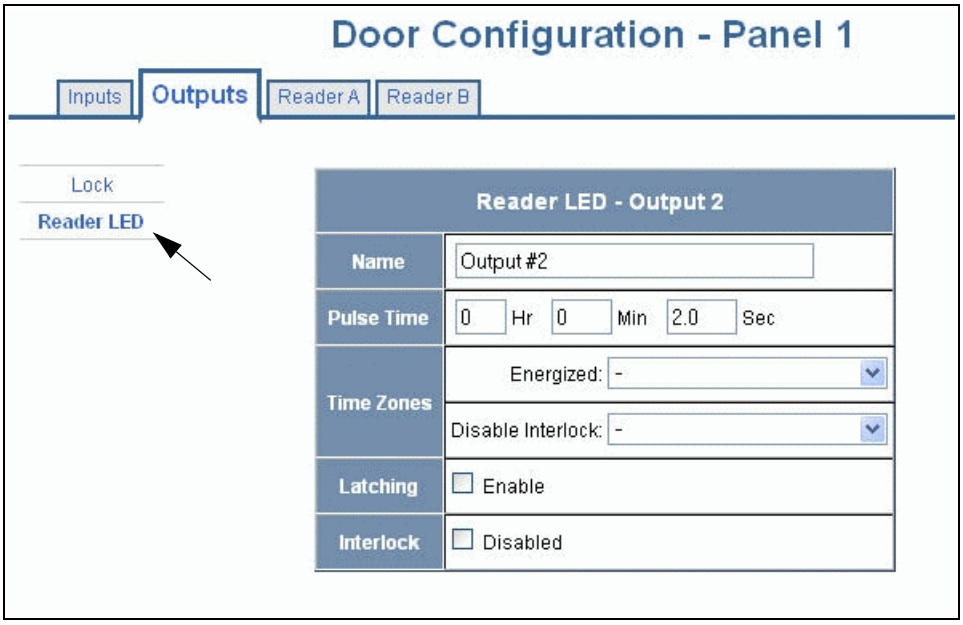
screen appears. Note that you can only *view* the group configuration from this screen. To *edit* the Group configuration, click **Configuration > Other I/O & Groups** link on the left side of the page.

Figure 2-22: *Configuration > Doors > Outputs > Lock > Group*



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

Figure 2-23: *Configuration > Doors: > 1 > Outputs Tab > Reader LED Dialog Box*



Steps: Use the descriptions in Table 2-10 to configure each individual lock or Reader LED:

Table 2-10: *Configuration > Doors: > 1 > Outputs Tab > Reader LED Dialog Box Fields*

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 is 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	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. 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. Appears only when the Lock option is selected.
First Card Rule	Requires a valid card read within the time zone to enable the time zone (period in which doors are unlocked) to take effect. Note that both TZ Card Toggle and First Card Rule cannot be enabled at the same time. Appears only when the Lock option is selected.

2.5.4 Inputs Tab

Four inputs are associated with each of the doors on a NetAXS-123 panel:

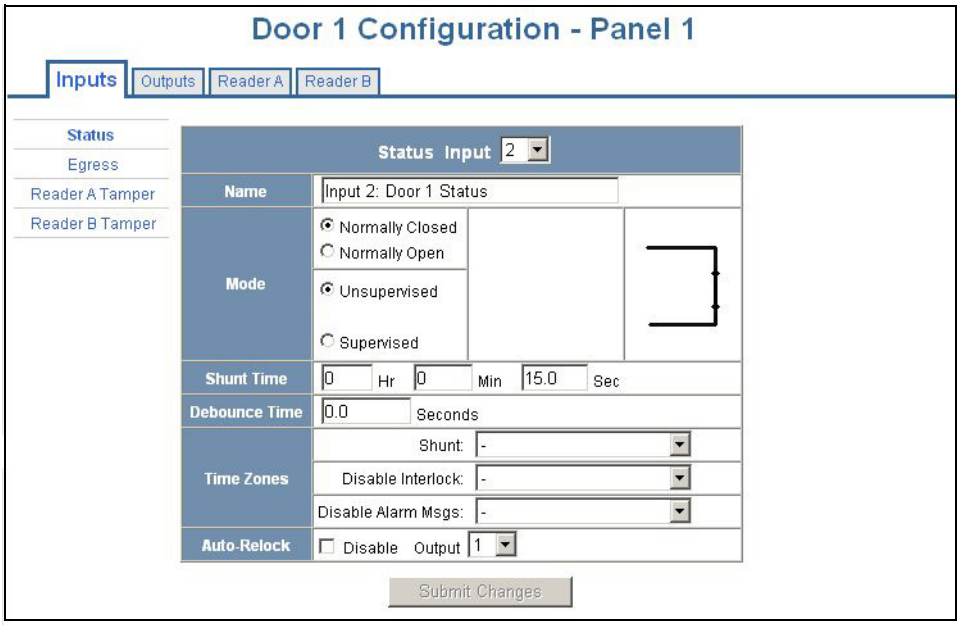
- Status – Provides door status information.
- Egress – Allows the door to open or close normally without generating an alarm.
- Tamper A – Reports abnormal handling of the reader device or wiring for Reader A.
- Tamper B – Reports abnormal handling of the reader device or wiring for Reader B.

The Inputs tab enables you to:

- Define the Status, Egress, and Tamper input 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.

Click **Inputs** to display the Inputs tab:

Figure 2-24: *Configuration > Doors: > 1 > Inputs Tab > Status*



There are four possible Mode configurations. Figure 2-24 shows the Normally Closed/Unsupervised Mode. The following screens show the remaining modes:

Figure 2-25: *Input Status Mode - Normally Open - Unsupervised Mode*

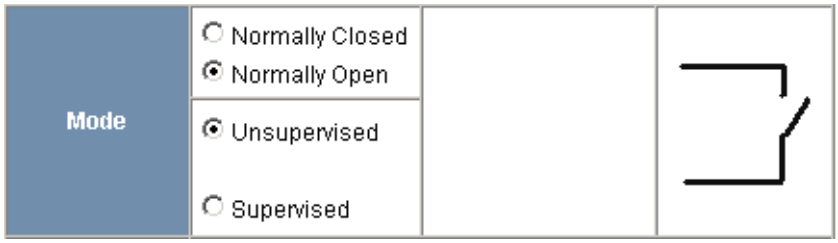


Figure 2-26: *Input Status Mode - Normally Closed - Supervised Mode*

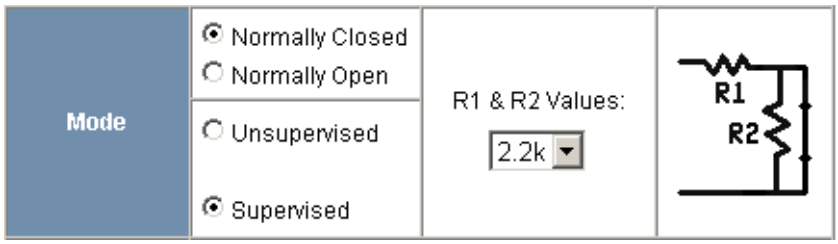
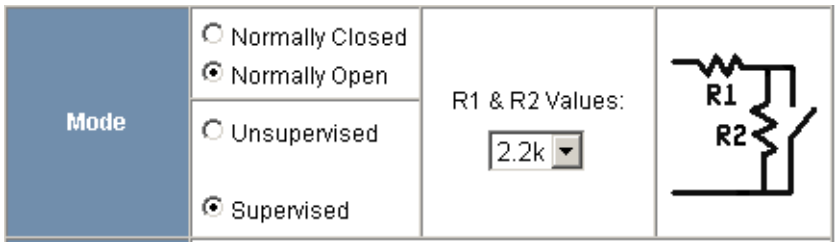


Figure 2-27: *Input Status Mode - Normally Open - Supervised Mode*



Steps: Use the descriptions in Table 2-11 to configure the Status, Egress, and Tamper inputs, then click **Submit Changes**:

Table 2-11: *Configuration > Doors: > 1 > Inputs Tab Fields*

Setting	Description
Name	Enter a unique name to identify the device.
Mode	**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.
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.

Table 2-11: *Configuration > Doors: > 1 > Inputs Tab Fields* (continued)

Setting	Description
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** check box, and select the associated output from the drop-down list.

2.6 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 AM to 6:00 PM, Monday through Friday.

The Access Levels screen enables you to:

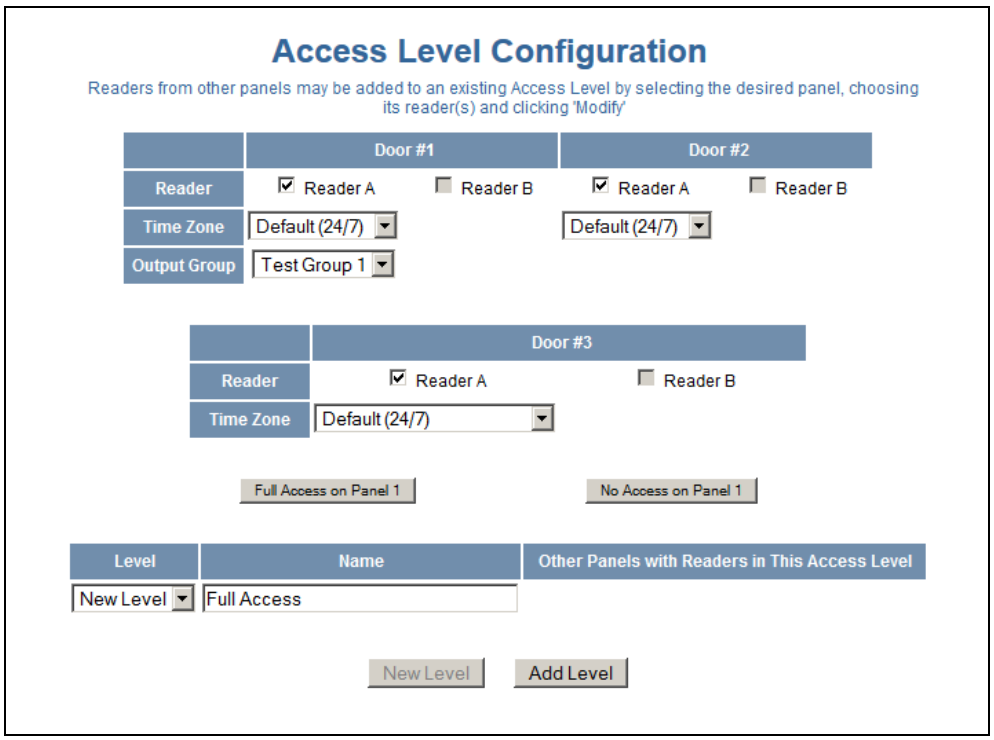
- Select Reader A and/or Reader B for each door. Note that if a reader is disabled, that reader's check box will also be disabled.
- Create an access level.
- Modify an access level.
- Delete an access level.
- Set a Time Zone for each door.
- View other panels with readers in this access level.

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 51) and the time zone (see Configuring Time Management, page 44) before configuring an access level.

Click **Access Levels > Add/Modify/Delete** to display the Access Level Configuration screen:

Figure 2-28: *Access Levels > Add/Modify/Delete*



In this figure, each Door only has Reader A enabled and Reader B grayed out. Readers that are grayed out indicate to the user that they are deactivated.

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, page 77.

Note: Output Groups are only selectable on Door 1.

To create an access level:

1. Select the door(s). The access level allows 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 allows access to the card holder only during this time zone.
4. Click **Add Level**.

To assign a Time Zone to a door:

1. Select the check box for the reader you desire. The Time Zone field appears.

2. From the Time Zone drop-down 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 drop-down list.

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 **Modify**.

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 **Delete**.
3. Click **OK** at the prompt to delete the access level.

Caution: 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 1-3 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 readers to the access level at these panels. To do this, click on the desired panel, and configure that panel's access level according to the instructions in this section.

2.7 Maintaining Cards

A card is encoded with a unique number and the card holder's access level grants rights to access 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.

2.7.1 Adding New Cards

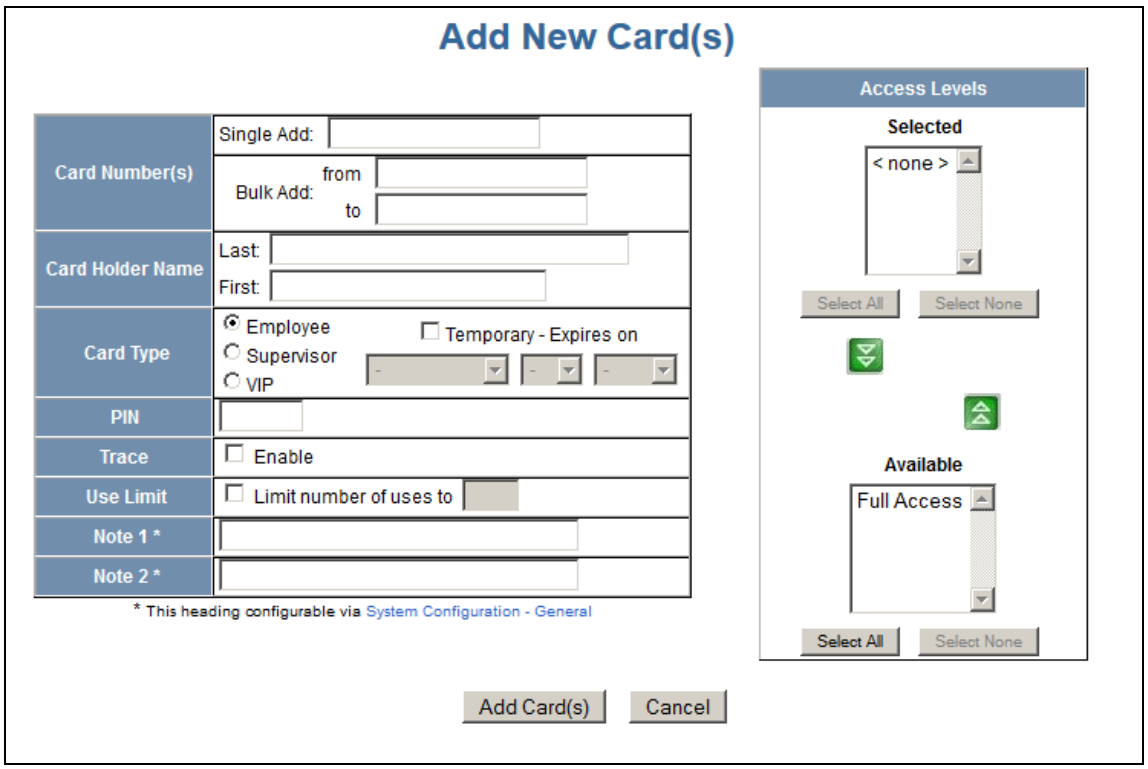
The Add New Card(s) screen enables you to:

- Create cards encoded with the following information:
  - Card Number(s)
  - Card Holder Name (first and last names)
  - Card Type
  - Personal Identification Number (PIN)
  - Trace
  - Expiration Date
  - Use Limit
  - Note 1

– Note 2
– Access levels

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

Figure 2-29: *Cards > Add*



Steps: Use the field descriptions in Table 2-12 to complete the card fields and click **Add Card(s)**:

Table 2-12: *Cards > Add Cards Fields*

Field	Description
Card Number(s)	Specifies the unique number by which the card holder will be identified. A card number is required.
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.

Table 2-12: *Cards > Add Cards Fields*

Field	Description
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 30). A card type is required.
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 A Tab, page 51), then you must create a PIN for the card holder here. The PIN has a maximum of six digits.
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 card holder's path through the facility.
Expiration Date	Specifies the date that a temporary card is de-activated.
Use Limit	Specifies the number of times a card can be used before it expires. Specify the number-of-uses limit as the number of times access may be granted.
Note 1	Provides a user-defined field. See Configuring the System, page 26 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 26 for information about how this field is defined for the Add New Card template.
Access Level(s)	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 9am-5pm and Access Level 2 is Monday to Saturday 3pm-11pm. When these times are combined, card 12345 provides access Monday to Friday 9am-11pm and Saturday 3pm-11pm.

2.7.2 Displaying and Modifying Cards

Use this function to display specified cards and modify them.

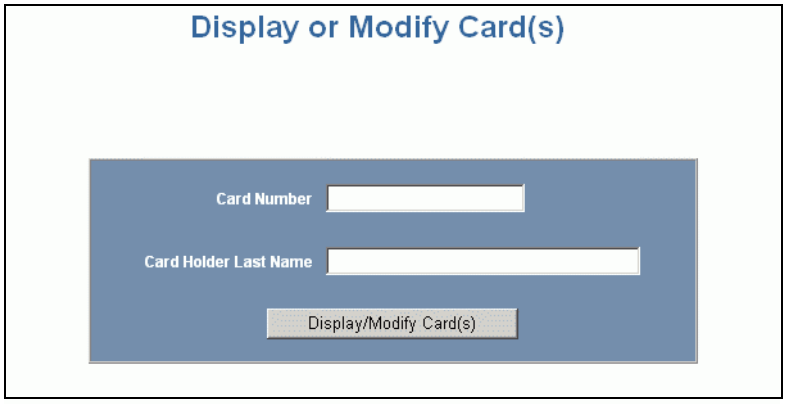
The Display or Modify Card(s) screen enables you to:

- Display cards by searching on any of the following keys:

  - Card number
  - Card Holder's last name
- Modify the displayed card(s)

Click **Cards > Display/Modify** to display the search screen with which you can find and display specified cards.

Figure 2-30: *Cards > Display/Modify*



To display or modify a card:

1. Enter a value for either of the search keys (card number or card holder last name).
2. Click **Display/Modify Card(s)**. The cards specified in step 1 appear.
3. Use the field descriptions in Table 2-12 on page 71 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.

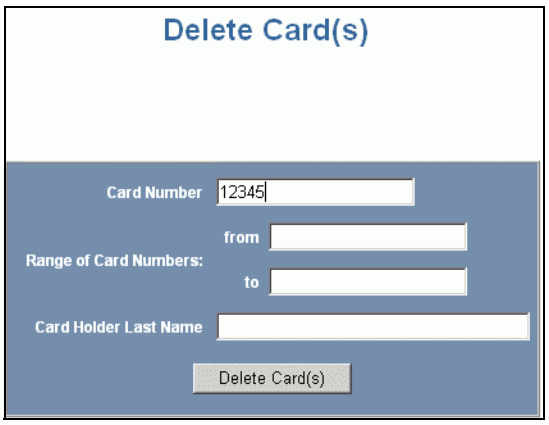
2.7.3 Deleting Cards

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

Click **Cards > Delete** to display the Delete Cards screen:

Figure 2-31: *Cards > Delete*



To delete a card:

1. Enter a value for any of the search keys (card number, card number range, or card holder 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.

2.7.4 Displaying Reports

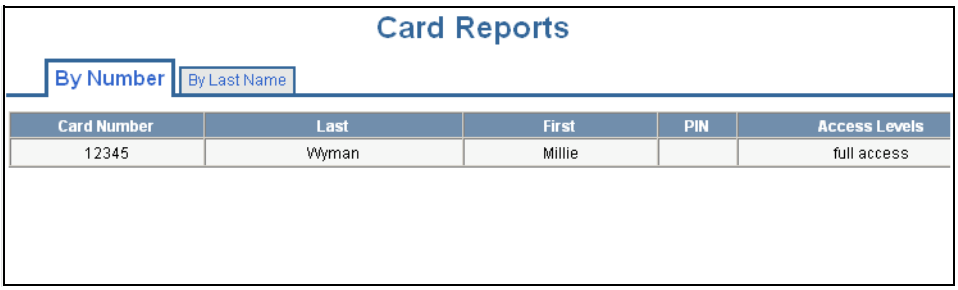
Use this function to display a report of all cards and card data. You can display the cards either by the card holder's last name or by the card number.

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

The Card Reports screen enables you to:

- View card records by the card holder's last name.
- View card records by the cards' number.

Figure 2-32: *Reporting > Card Reports*



To display a report:

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

Note: The display in Figure 2-32 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.

Note: For more information on importing/exporting card reports, see Chapter 5, File Management.

3. Use the descriptions in Table 2-13 to read the card records (see Adding New Cards, page 70 for more information about card data):

Table 2-13: *Reporting > Card Reports Fields*

Field	Description
Card Number	Shows the card number.
Last	Shows the card holder's last name.
First	Shows the card holder's first name.
PIN	Shows the Personal Identification Number (PIN) for the card holder. The PIN has a maximum of six digits.
Access Levels	Shows the access level(s) configured for the card holder. 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 68 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), or a combination of these types.
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 the card is IN the anti-passback area or OUT of the anti-passback area.
Note1:	Displays informational text that may have been entered in the Note 1 field.
Note2:	Displays informational text that may have been entered in the Note 2 field.

2.8 Configuring Other I/O & Groups

This section explains how to configure "other" inputs, outputs and groups on the NetAXS-123 panel. They are called "other" inputs, outputs and groups because you can use them for things other than door lock/unlock functions. This section explains how to configure these other inputs, outputs, and groups (for pulse and time zone).

2.8.1 Inputs Tab

This tab enables you to configure other input devices on inputs 5 and 6 or other inputs that have been disassociated from their doors.

When using power supplies with power fail output, the power fail output can be wired to input 6. When the power supply loses power and switches to battery, input 6 is activated and a Power Fail alarm is generated. If input 6 is not activated in this capacity, you can use it for other configurations.

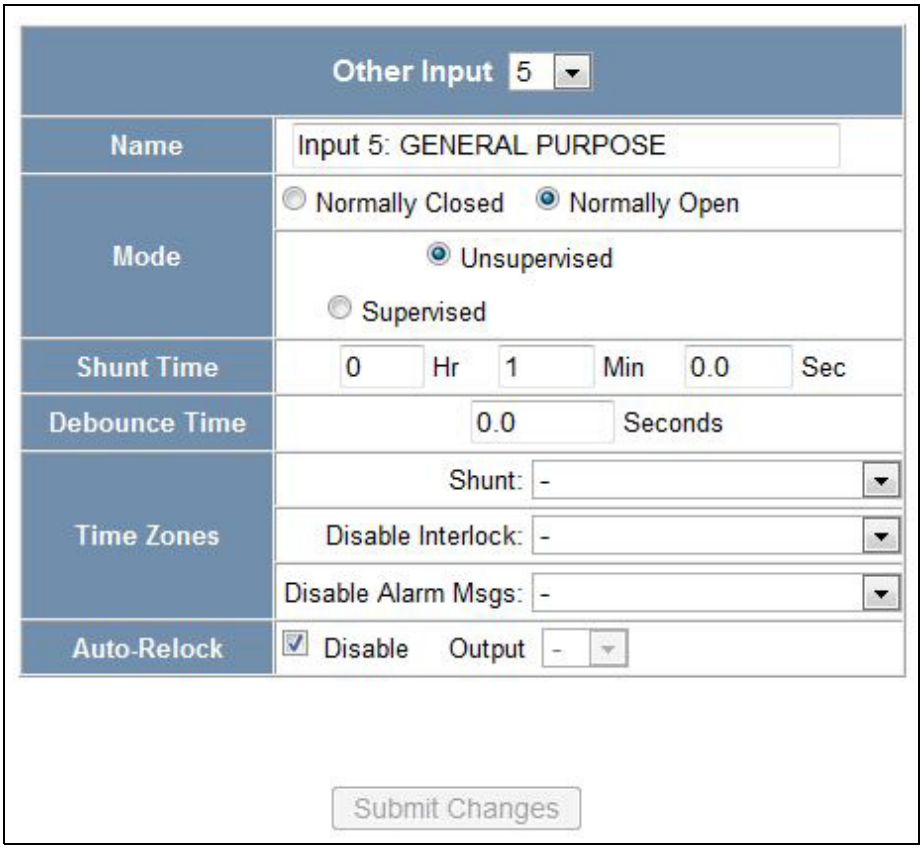
Note: You can also configure the Power Fail inputs for general use, if you choose not to wire them for power detection.

The Input tab enables you to:

- Configure
  - Mode
  - Shunt Time
  - Debounce Time
  - Time Zones
  - Auto-Relock

Click **Configuration > Other I/O & Groups > Inputs** tab to display the Inputs screen:

Figure 2-33: *Configuration > Other I/O & Groups > Inputs Tab*



Steps: Use the descriptions in Table 2-14 to configure other panel inputs and downstream inputs.

Table 2-14: *Configuration > Other I/O & Groups > Inputs Tab Fields*

Setting	Description
Name	Enter a unique name to identify the device.
Mode	**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.
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.
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** check box, and select the associated output from the drop-down list.

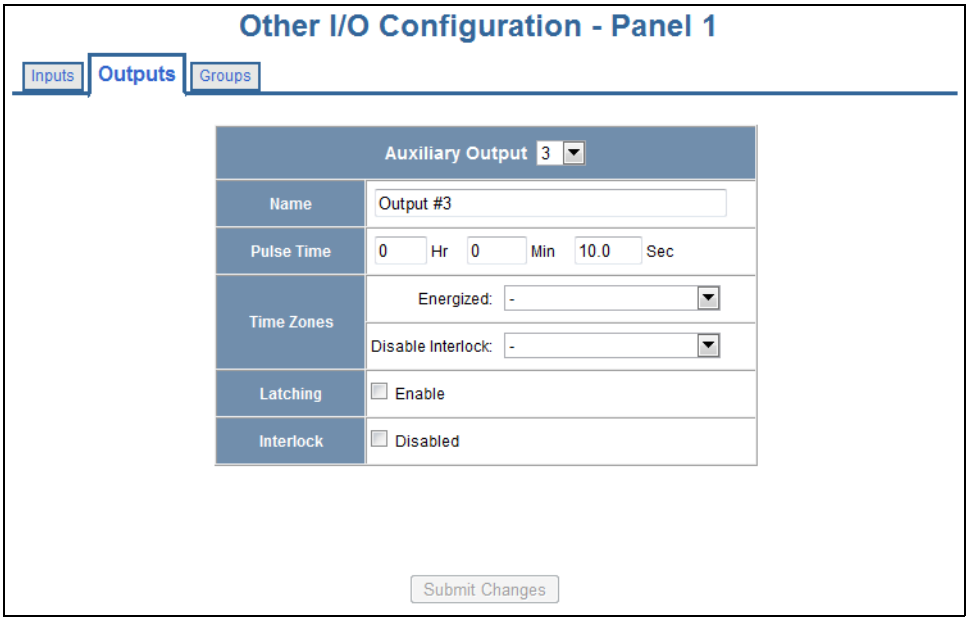
2.8.2 Outputs Tab

The Outputs tab enables you to:

- Configure the following for each of the auxiliary outputs:
  - Name
  - Pulse Time
  - Time Zones
  - Latching
  - Interlock

Click **Configuration > Other I/O & Groups > Outputs tab** to display the Auxiliary Output screen for the on-board outputs:

Figure 2-34: *Configuration > Other I/O & Groups > Outputs Tab*



Steps: Use the descriptions in Table 2-15 to configure each output device.

Table 2-15: *Configuration > Other I/O & Groups > Outputs Tab Fields*

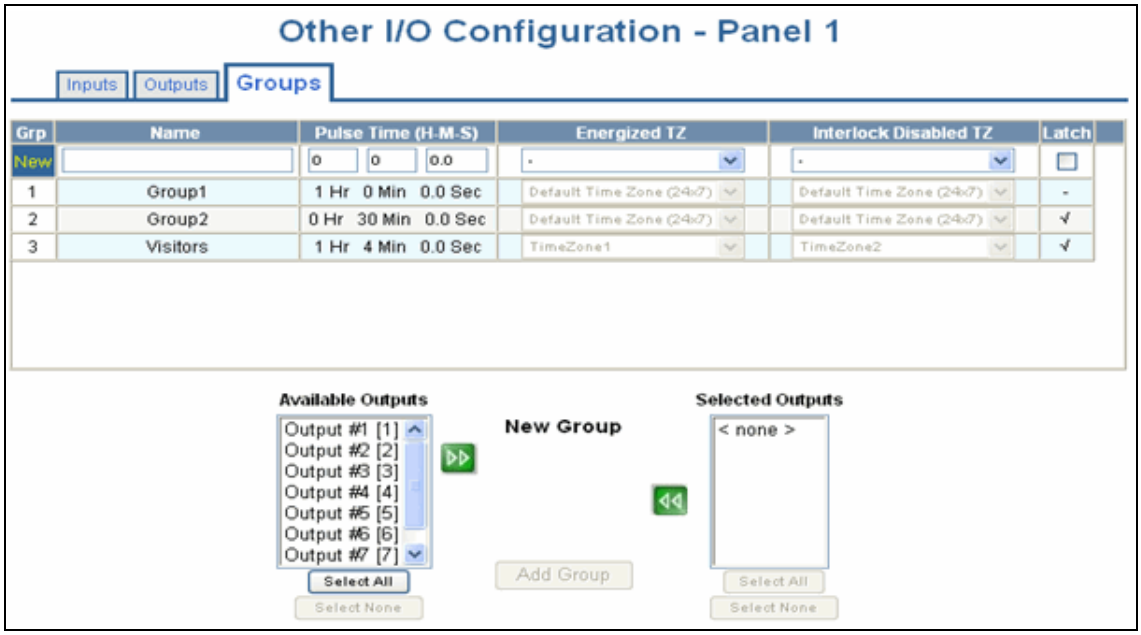
Setting	Description
Name	Enter a unique name to identify the device.
Pulse Time	Specifies the duration for which the device will assume abnormal status. For example, it specifies how long a horn will sound or a door strike will remain released. The maximum number of hours is 1. When the hour field is blank, the maximum number of minutes is 59. When 1 is entered in the hour field, the maximum number of minutes is 45. 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.

2.8.3 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-123 web server supports up to 64 output groups.

Click **Groups** to display the Groups screen (see Figure 2-35).

Figure 2-35: *Configuration > Other I/O & Groups > Groups Tab*



The Groups tab enables you to:

- Associate any of the panel's 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 2-16 to configure each group.

Table 2-16: *Configuration > Other I/O & Groups > Groups Tab Fields*

Setting	Description
Name	Enter a unique name to identify the group.
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.
Energized TZ	Specifies the period during which the group of output relays are automatically energized.

Table 2-16: *Configuration > Other I/O & Groups > Groups Tab Fields* (continued)

Setting	Description
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).

2.9 Configuring Interlocks

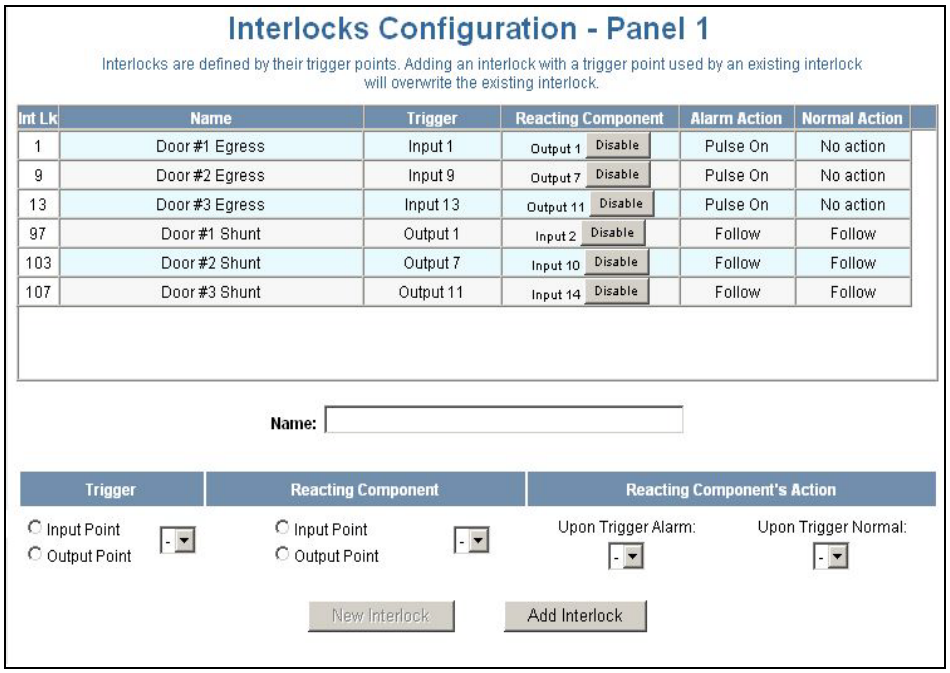
An interlock is a programmed connection between two points. The interlock causes an input point, output point, or group of output points to act in a specified manner when another input point, output point, or group of output points changes its state. An action on the trigger point causes a reaction on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

The Interlocks screen enables you to:

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

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

Figure 2-36: *Configuration > Interlocks*



To create an interlock:

1. Click **New Interlock** to display the screen.
2. Use the descriptions in Table 2-17 to configure the interlock:

Table 2-17: *Configuration > Interlocks Fields*

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 **Add Interlock** to create the interlock.

To delete an interlock:

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

To enable/disable an interlock:

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

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.

2.10 Configuring Users

A user is one who will be using the NetAXS-123 software interface in one or more functional 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 2-18 lists the functions that each user type can perform.

Table 2-18: *User Functions*

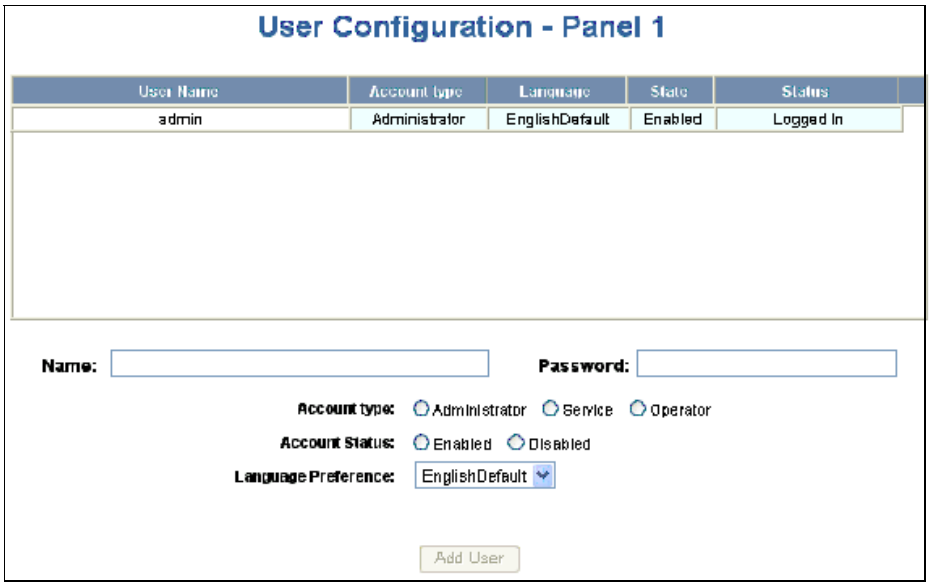
Function	Operator	Service	Administrator
View alarms/events	✔	✔	✔
Acknowledge alarms	✔	✔	✔
View panel I/O status	✔	✔	✔
Control I/O points	✔	✔	✔
Generate reports	✔	✔	✔
View card database	✔	✔	✔

Table 2-18: *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			✔

Click **Users & Accounts > Add/Modify/Delete** to display the User Configuration screen:

Figure 2-37: *Users & Accounts > Add/Modify/Delete*



To create a user:

1. Enter the user's name in the **Name** field (range 5-25 characters).
2. Enter a unique password in the **Password** field (range 5-25 characters). Note that a duplicate password will not be accepted.
3. Select the type in the **Account Type** field.
4. 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).

5. Select the user's Language Preference from the drop-down list.
6. Click **Add User**.

To modify a user:

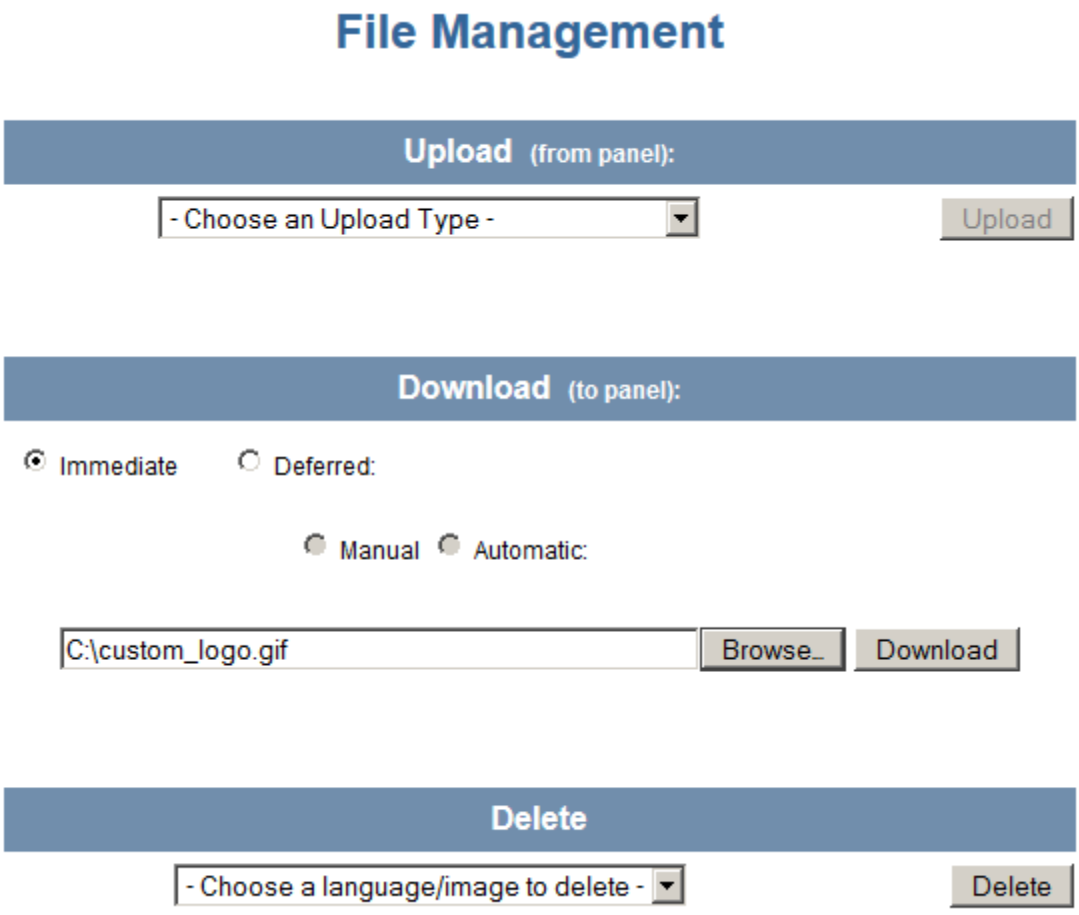
1. In the **User Name** field, click the name of the user you want to modify.
2. Change the name, password, account type, or account status.
3. Click **Modify**.

To delete a user:

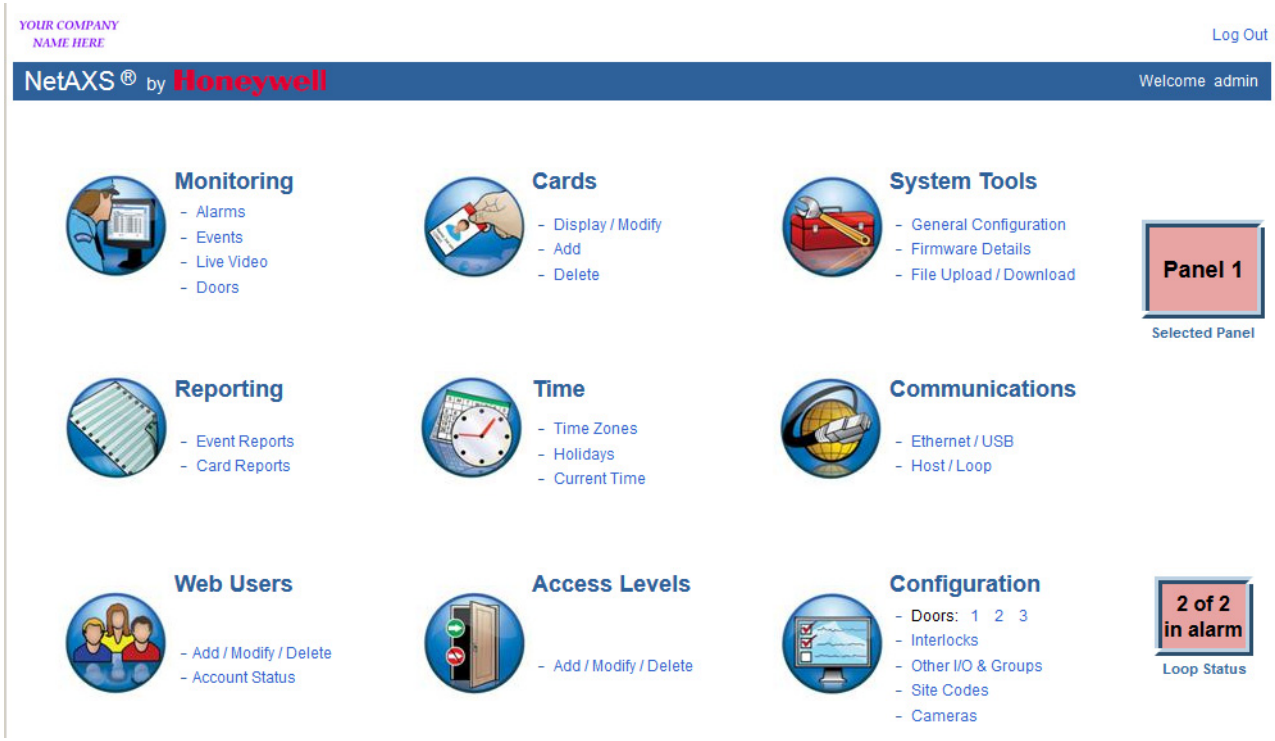
1. In the User Name column, click the user account you want to delete.
2. Click **Delete**.
3. Click **OK** at the prompt to delete the user account.

2.11 Adding a Custom Logo to NetAXS-123 Web Screens

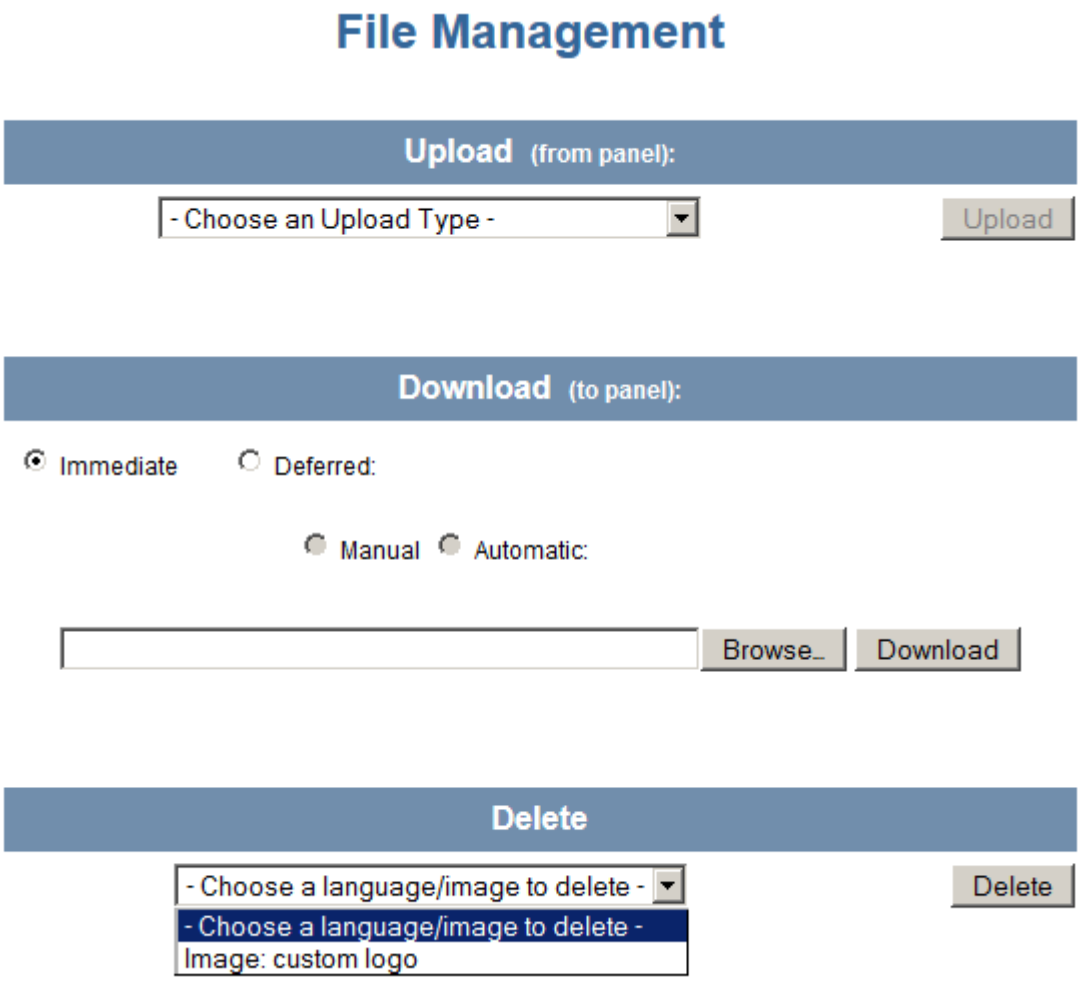
A custom logo may be downloaded into the panel using the **File Upload/Download** link under the **System Tools** heading on the landing page.



The logo must be a GIF image, must be named **custom_logo.gif**, and must have the dimensions of 414 x 181 pixels (W x H). If the image is of a different size, it may not display properly. Once downloaded, the new logo will appear upon the next login.



Subsequently, a new option will appear under the Delete section of the File Management page called Image: Custom Logo. Clicking the **Delete** button after choosing this option will delete the custom logo from the panel.



Compatibility and Interoperation with Other Controllers

3

In this chapter...

3.1 Introduction

The sections in this chapter outline the compatible versions of firmware, browsers and Host software (WIN-PAK) in conjunction with NetAXS123 R5.0.

Additional details regarding supported configurations may be found in the *NetAXS-123 Installation Guide.*

3.2 Configurations with NetAXS-123 R5.0 Gateway in EVL Mode

EVL is a virtual loop of panels connected via Ethernet.

This configuration must be managed via Web browser.

NetAXS-4 controllers not supported in this mode.

WIN-PAK is not supported in EVL mode for NetAXS-123 R5.0.

3.3 Configurations Using NetAXS-123 R5.0 Gateway in RS485 Mode

RS485 is based on physically wiring the panels in a loop.

This Configuration may be managed via WIN-PAK or Web browser.

Downstream RS485 Controllers may be:

- NetAXS-123 R5.0
- NetAXS-4 R3.4 (or higher)

3.4 Configurations Using PCI-3 Gateway/RS485 Loop

May be managed via WIN-PAK only.

Downstream Controllers may be:

- NetAXS-123 R5.0
- NetAXS-4 R3.4 (or higher)
- N-1000-III/IV, N-1000-III/IV-X
- NS2

3.5 WIN-PAK Supported:

The following versions of WIN-PAK support NetAXS-123 natively:

- WIN-PAK XE/SE/PE 3.3 build 670.21 or higher
- WIN-PAK CS 4.2 build 1017.33 or higher

For details, please consult the WIN-PAK customer documentation for configuring NetAXS-123 with WIN-PAK.

Versions of WIN-PAK earlier than R3.3 do not support NetAXS natively and are not recommended.

Customers using earlier versions of WIN-PAK are encouraged to upgrade to the version listed above or higher.

Note: NetAXS-123 Video functionality is not supported in WIN-PAK.

When R5.0 is used with WIN-PAK SE/PE 2.0, it must be set up as an N1000 III/IV-X. For details, please see *NetAXS-123 Access Control Unit User's Guide, Document 800-05168 Revision B, "Section 3.4 Setting up WIN-PAK"*.

3.6 Browsers Supported:

NetAXS-123 R5.0 is compatible with:

- Internet Explorer 8 (IE8)
- Internet Explorer 9 (IE9),
- Internet Explorer 10 (IE10), and
- Firefox (FF 19-21).

Note: Video functionality is not supported when using the Internet Explorer 10 and Firefox web browsers.

Monitoring NetAXS-123 Status 4

In this chapter...

4.1 Overview

This chapter is written for operators who monitor the following statuses:

- 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 system. For example, status of doors, database changes, invalid cards, valid cards, etc.
- Doors - Doors are a collection of inputs and outputs connected on the panel that are associated to reader(s).
- Inputs – Inputs are terminals located on the panel; the inputs are wired to input devices, such as door-position switches that monitor status of a door.
- Outputs – Output relays are relays located on the panel that are connected to output devices, such as a door lock or a siren.
- System – The system lists the current capacities and limits of the panel.
- Reports - The system generates reports by Last Name and by Card Number.

Note: NetAXS-123 has been evaluated for standalone use only. Monitoring features are supplementary only and have not been evaluated by UL.

4.2 Monitoring Alarms

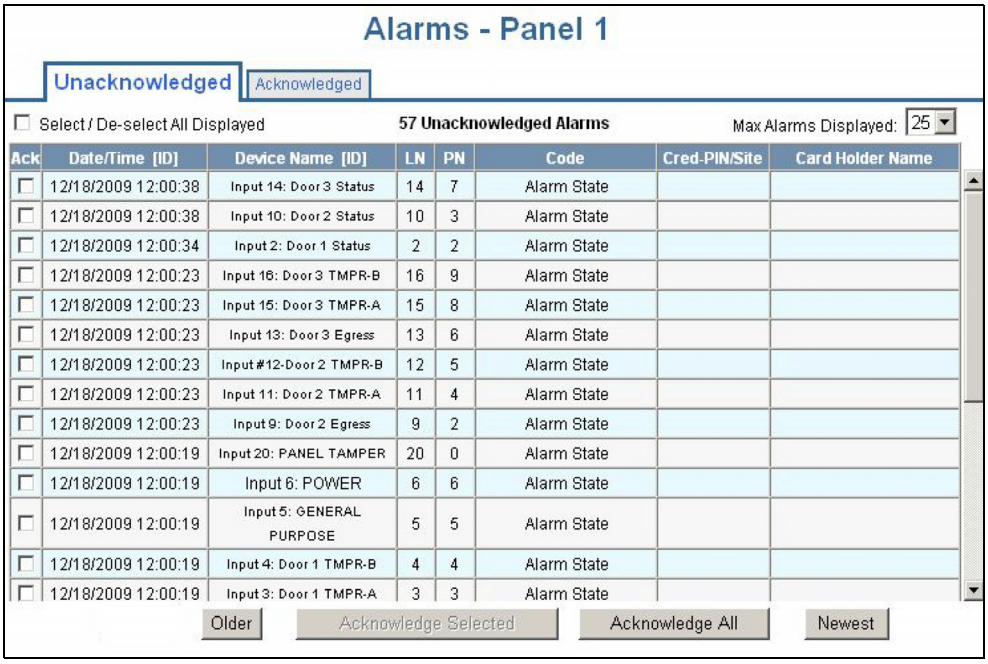
Note: NetAXS-123 is listed for access control only. No burglary applications have been investigated.

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

Note that 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 **Monitoring > Alarms** to display the Unacknowledged Alarms tab:

Figure 4-1: *Monitoring > Alarms > Unacknowledged Tab*



Ack	Date/Time [ID]	Device Name [ID]	LN	PN	Code	Cred-PIN/Site	Card Holder Name
☐	12/18/2009 12:00:38	Input 14: Door 3 Status	14	7	Alarm State		
☐	12/18/2009 12:00:38	Input 10: Door 2 Status	10	3	Alarm State		
☐	12/18/2009 12:00:34	Input 2: Door 1 Status	2	2	Alarm State		
☐	12/18/2009 12:00:23	Input 16: Door 3 TMPR-B	16	9	Alarm State		
☐	12/18/2009 12:00:23	Input 15: Door 3 TMPR-A	15	8	Alarm State		
☐	12/18/2009 12:00:23	Input 13: Door 3 Egress	13	6	Alarm State		
☐	12/18/2009 12:00:23	Input #12-Door 2 TMPR-B	12	5	Alarm State		
☐	12/18/2009 12:00:23	Input 11: Door 2 TMPR-A	11	4	Alarm State		
☐	12/18/2009 12:00:23	Input 9: Door 2 Egress	9	2	Alarm State		
☐	12/18/2009 12:00:19	Input 20: PANEL TAMPER	20	0	Alarm State		
☐	12/18/2009 12:00:19	Input 6: POWER	6	6	Alarm State		
☐	12/18/2009 12:00:19	Input 5: GENERAL PURPOSE	5	5	Alarm State		
☐	12/18/2009 12:00:19	Input 4: Door 1 TMPR-B	4	4	Alarm State		
☐	12/18/2009 12:00:19	Input 3: Door 1 TMPR-A	3	3	Alarm State		

Notes:

- You can display the newest alarms first by clicking **Newest**. Click **Older** to display 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 4-2: *Monitoring > Alarms > Acknowledged Tab*

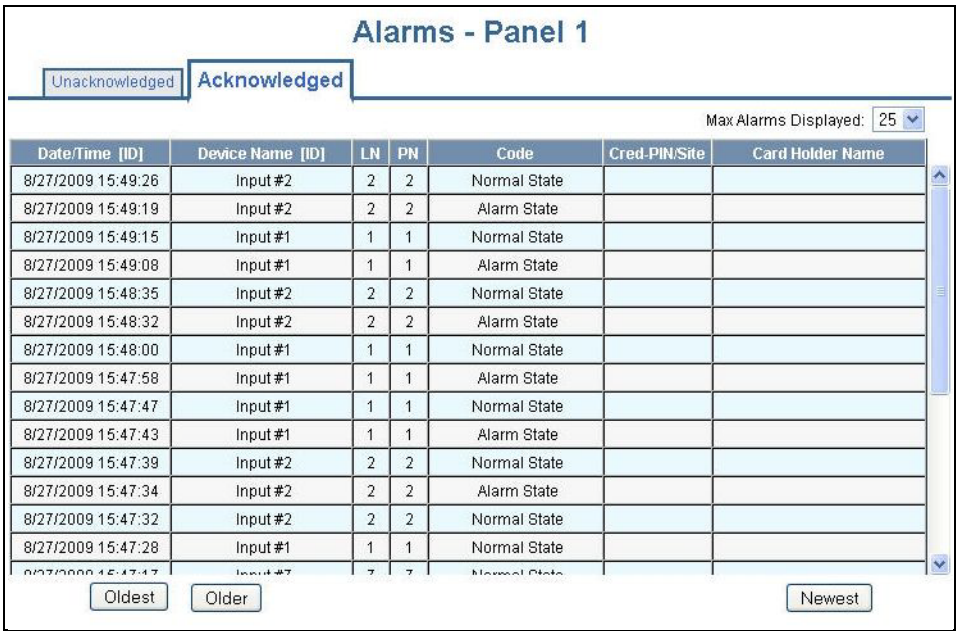


Table 4-1 describes the information displayed on both the Unacknowledged alarms tab and Acknowledged alarms tab:

Table 4-1: *Monitoring > Alarms Fields*

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 acknowledgment 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** – A unique number starting at 1 that is assigned to an alarm generating point. This number is never duplicated either on a Controller or its attached 1- or 2-door I/O board. There is one exception to this: Door Readers. For a list of common values, see Table 4-2.
PN	**Physical device number** – A number at the board level that is assigned to a specific alarm generating point. NetAXS-123 Controller starts at 1 and goes to 8, 1-Door I/O board as a new board goes from 1 to 4, and 2-door I/O board goes from 1 to 8. System alarms such as reset which are not board-specific will report a value of 0. There is one exception to this: Door Readers. For a list of common values, see Table 4-2.
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	Reports a Card Holder name on events where the Card Number is an actual card in the system.

Table 4-2 displays the logical and physical numbers of common panel events for three doors.

Table 4-2: *Logical (LN) and Physical (PN) Numbers of Common Panel Events*

	Egress		**Status**		**Reader A Tamper**		**Reader B Tamper**		**Reader A**		**Reader B**	
	LN	PN	LN	PN	LN	PN	LN	PN	LN	PN	LN	PN
Door 1	1	1	2	2	3	3	4	4	1	1	5	5
Door 2	9	2	10	3	11	4	12	5	2	2	6	6
Door 3	13	6	14	7	15	8	16	9	3	3	7	7

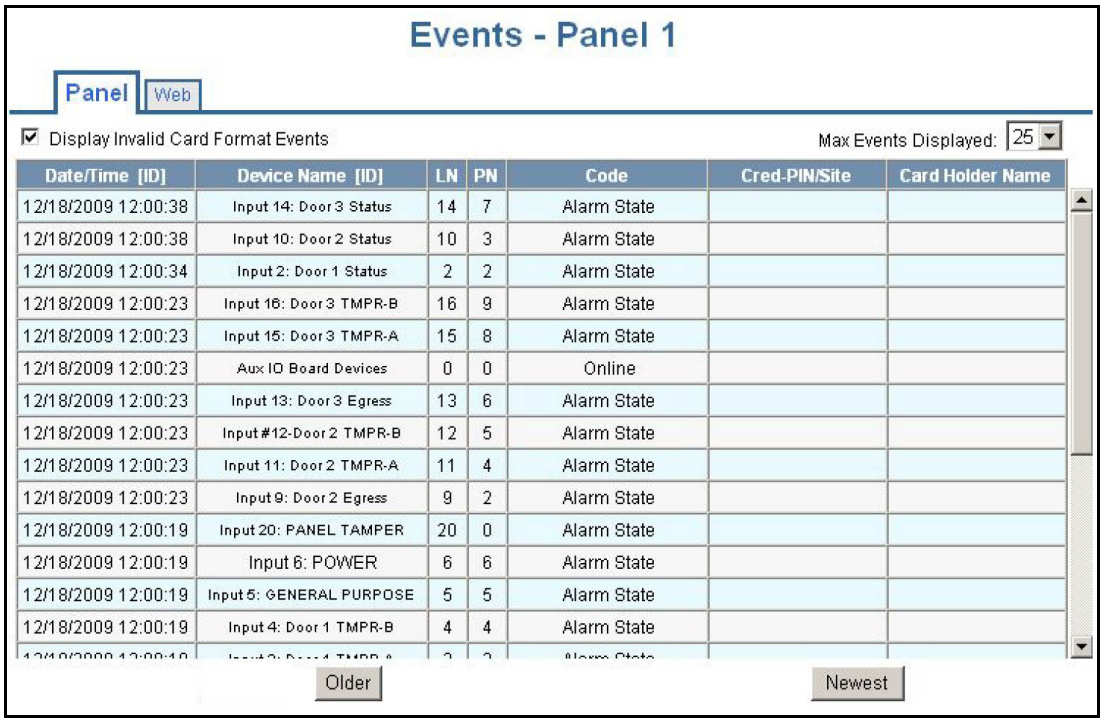
Note: The values listed in this table are based on defaults. For information on other values, contact Technical Support.

4.3 Monitoring Events

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

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

Figure 4-3: *Monitoring > Events > Panel Tab*



Date/Time [ID]	Device Name [ID]	LN	PN	Code	Cred-PIN/Site	Card Holder Name
12/18/2009 12:00:38	Input 14: Door 3 Status	14	7	Alarm State		
12/18/2009 12:00:38	Input 10: Door 2 Status	10	3	Alarm State		
12/18/2009 12:00:34	Input 2: Door 1 Status	2	2	Alarm State		
12/18/2009 12:00:23	Input 16: Door 3 TMPR-B	16	9	Alarm State		
12/18/2009 12:00:23	Input 15: Door 3 TMPR-A	15	8	Alarm State		
12/18/2009 12:00:23	Aux IO Board Devices	0	0	Online		
12/18/2009 12:00:23	Input 13: Door 3 Egress	13	6	Alarm State		
12/18/2009 12:00:23	Input #12-Door 2 TMPR-B	12	5	Alarm State		
12/18/2009 12:00:23	Input 11: Door 2 TMPR-A	11	4	Alarm State		
12/18/2009 12:00:23	Input 9: Door 2 Egress	9	2	Alarm State		
12/18/2009 12:00:19	Input 20: PANEL TAMPER	20	0	Alarm State		
12/18/2009 12:00:19	Input 6: POWER	6	6	Alarm State		
12/18/2009 12:00:19	Input 5: GENERAL PURPOSE	5	5	Alarm State		
12/18/2009 12:00:19	Input 4: Door 1 TMPR-B	4	4	Alarm State		

Notes:

- You can display the newest 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 4-3 describes the information displayed on the Events Panel tab:

Table 4-3: *Monitoring > Events > Panel Tab Fields*

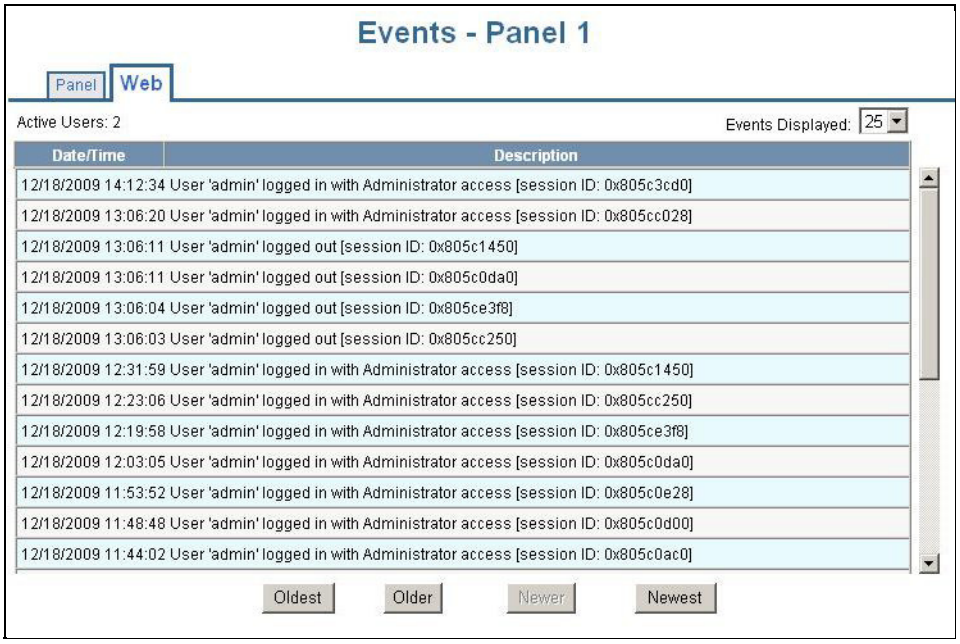
Column Head	Description
Date/Time [ID]	Provides the date and exact time the event was generated, according to the panel's time.
Device Name [ID]	Identifies the device that generated the event.
LN	**Logical device number** – A unique number starting at 1 that is assigned to an alarm generating point. This number is never duplicated either on a Controller or its attached 1 or 2 Door I/O board. There is one exception to this: Door Readers. For a list of common values, see Table 4-2.
PN	**Physical device number** – A number at the board level that is assigned to a specific alarm generating point. NetAXS-123 Controller starts at 1 and goes to 8, 1-Door I/O board as a new board goes from 1 to 4, and 2-door I/O board goes from 1 to 8. System alarms such as reset which are not board-specific will report a value of 0. There is one exception to this: Door Readers. For a list of common values, see Table 4-2.
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	Gives further details on valid and invalid card transactions. Also reports number of bits on cards that do not have associated format in panel, and database changes.

Table 4-3: *Monitoring > Events > Panel Tab Fields* (continued)

Column Head	Description
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 **Monitoring > Events > Web** tab to display the Web Events tab:

Figure 4-4: *Monitoring > Events > Web Tab*



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

4.4 Monitoring Doors

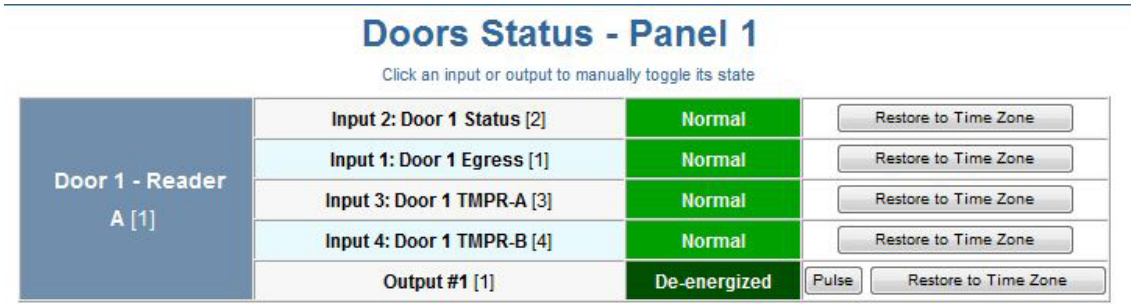
The panel supports 1, 2, or 3 doors. The door status screen provides status for each door's egress, status, and tamper and also status of the door lock relay.

The Door 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, its change of state is ignored. This way you can allow a door to be held open without signaling an alarm. The default state of an input point is "un-shunted."
- Restore the input to its time zone. A time zone is a specified time period during which the input will be shunted and the alarm de-activated (for time zone management, see Configuring Time Management, page 44).
- Pulse or energize the Door Lock relay.
- Restore the Door lock to its time zone.

Click **Monitoring > Door** to display the **Door Status** screen:

Figure 4-5: *Door Status Screen*



4.5 Monitoring Inputs

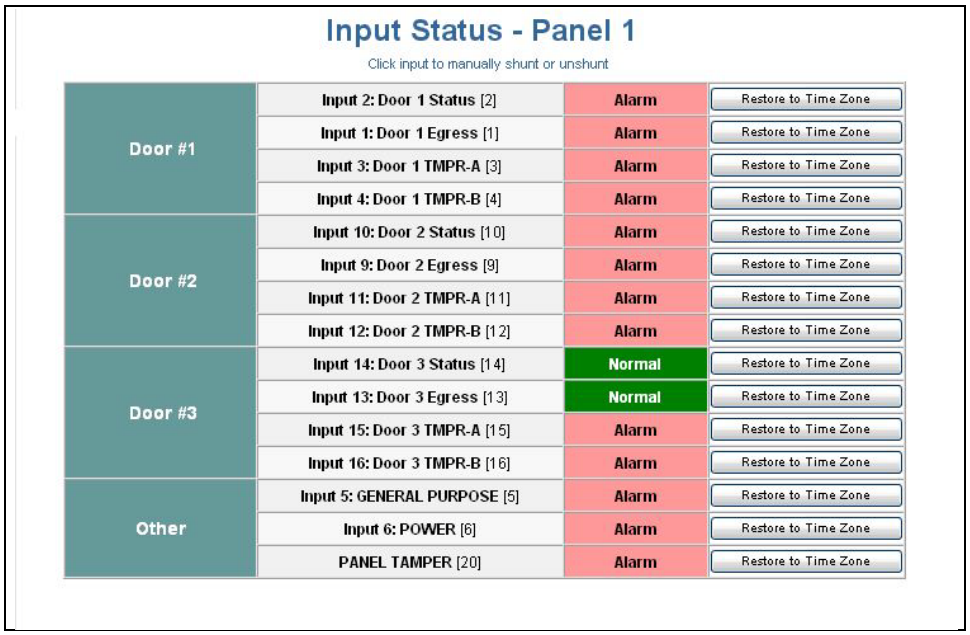
The panel supports door, panel, and auxiliary inputs. The door inputs provide egress, status, and tamper monitoring. The panel inputs provide power fail and tamper status. The auxiliary inputs support any monitoring devices connected.

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, its change of state is ignored. This way you can allow a door to be held open without falsely signalling an alarm. The default state of an input point is "un-shunted."
- Restore the input to its 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 44).

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

Figure 4-6: *Click Status > Inputs*



To shunt or un-shunt an input:

1. Click the input name to display a prompt.

2. Click **OK** to complete the shunt or un-shunt.

Figure 4-7: *Toggle Shunt State Dialog Box*

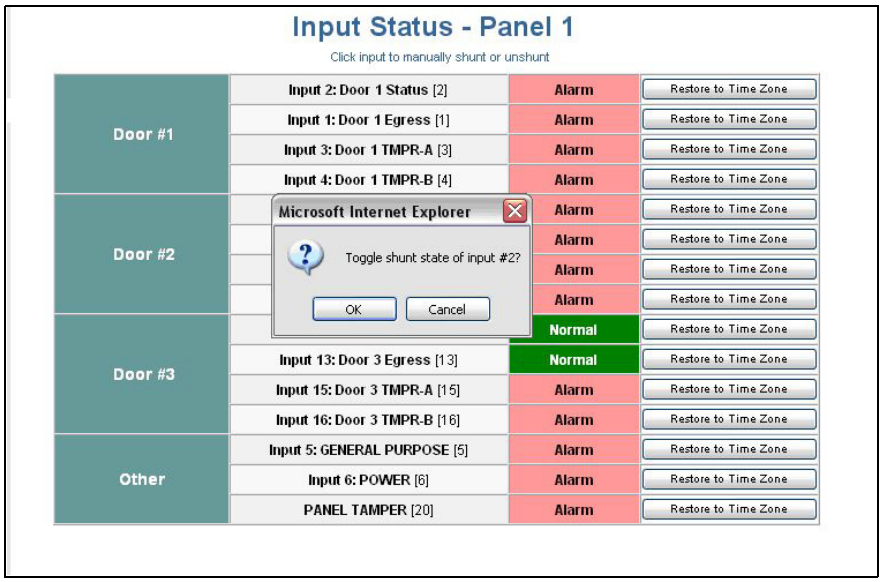
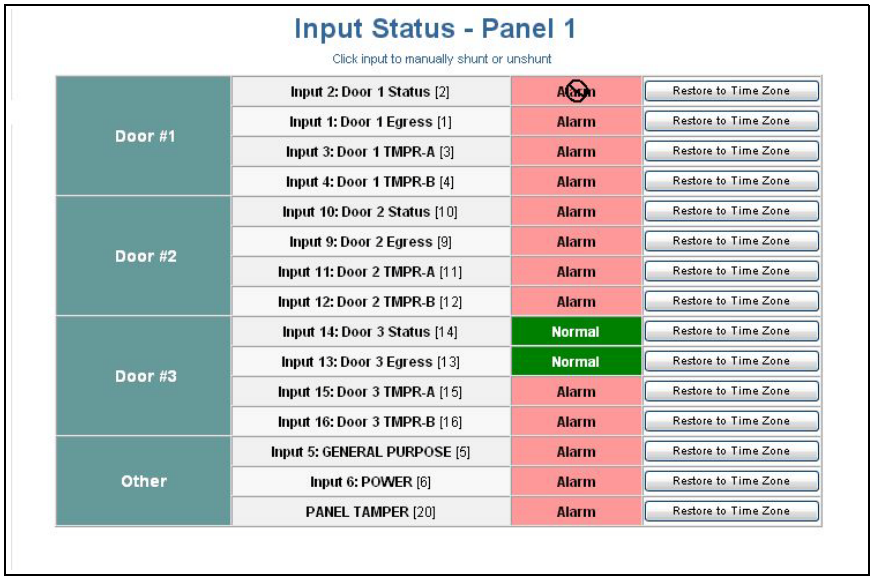


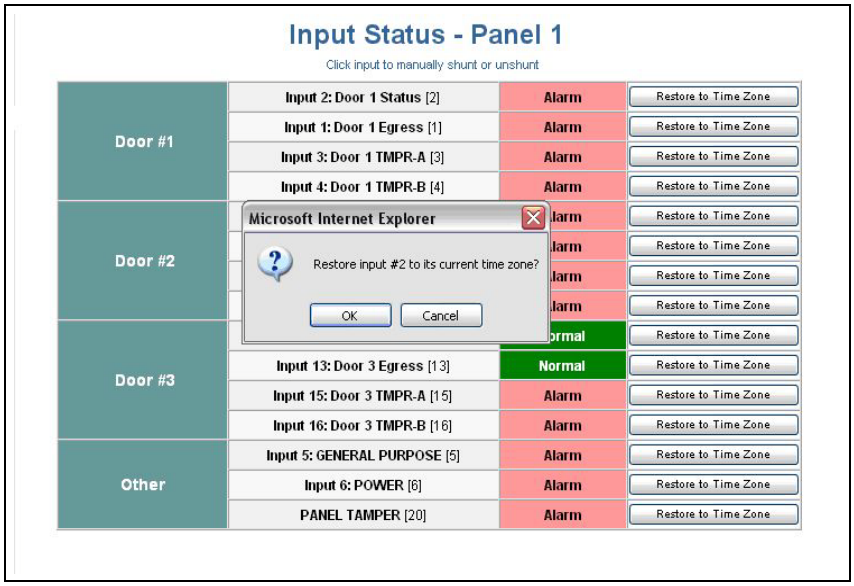
Figure 4-8 displays an example of a shunted input status.

Figure 4-8: *Shunted Input Status*



3. Click the input's **Restore to Time Zone** button to display a prompt to restore the input to its shunt state based on its current time zone. Click **OK** to complete the restoration to the current time zone.

Figure 4-9: *Time Zone Restore Dialog Box*



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

4.6 Monitoring Outputs

An output is a device that changes 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.

The panel supports one door output for each of its three doors. The panel also supports up to three additional auxiliary outputs. For example:

- 1 Door System = 1 Door Output and 1 Aux Output
- 2 Door System = 2 Door Outputs and 2 Aux Outputs
- 3 Door System = 3 Door Outputs and 3 Aux Outputs

Outputs can be configured individually as discrete outputs (see Outputs Tab, page 62 and Outputs Tab, page 62) or collectively as a group of outputs.

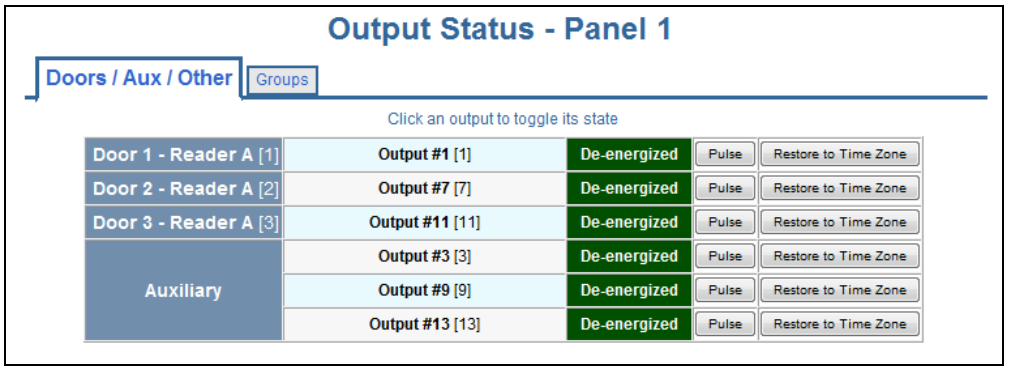
Note: The Pulse and Restore to Time Zone buttons will only function when an output or a group has a valid pulse time or a time zone assigned.

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 group of outputs in the Groups tab.
- Energize or de-energize any output or group indefinitely.
- Pulse any output or group. This energizes the output or group for a configured period of time (see Outputs Tab, page 62).
- 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 44).

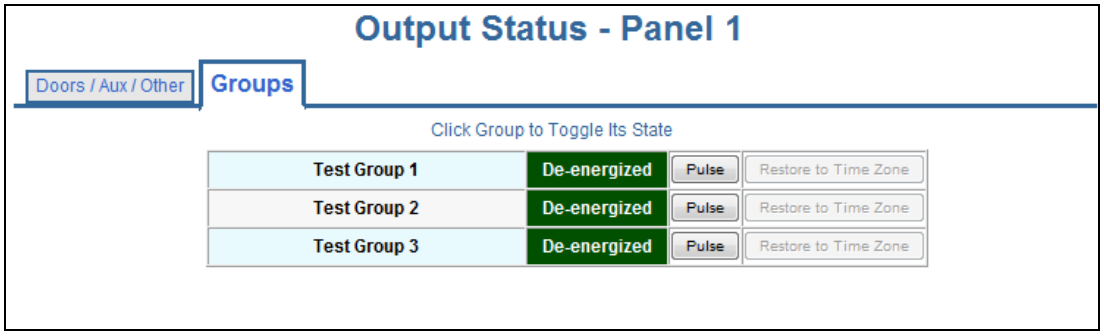
Click **Status > Outputs** to display the Doors/Aux/Other tab of the Output Status screen:

Figure 4-10: *Status > Outputs > Doors/Aux/Other Tab*



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

Figure 4-11: *Status > Outputs > Groups Tab*



To monitor output status:

1. To energize an output for an indefinite period of time, click the **De-energized** status button to display a prompt. Click **OK** to complete the change to "Energized."
2. To de-energize an output for an indefinite period of time, click the **Energized** status button to display a prompt. Click **OK** to complete the change to "De-energized."
3. To Pulse an output for the configured period of time, click the **Pulse** button to display a prompt. Click **OK** to start the pulse.
4. To reset the output to follow its configured time zone, click the **Restore to Time Zone** button to display a prompt. Click **OK** to restore the time zone.

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

4.7 Monitoring System Status

This feature provides current and maximum system capacities of the listed databases.

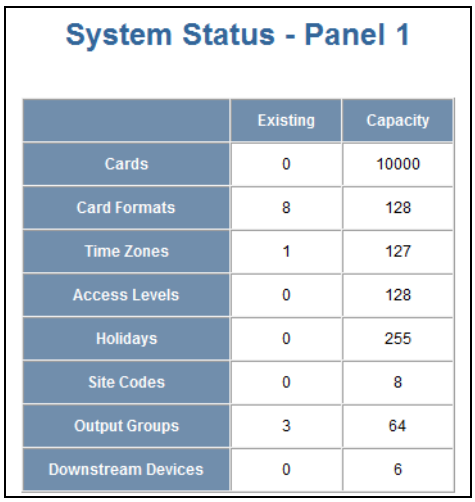
The System Status screen enables you to:

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

- Number of currently existing entries in the database.
- Maximum number of entries in the database.

Click **System Tools > General Configuration,** then in the navigation menu click **Status > System** to display the System Status screen:

Figure 4-12: *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	3	64
Downstream Devices	0	6

File Management

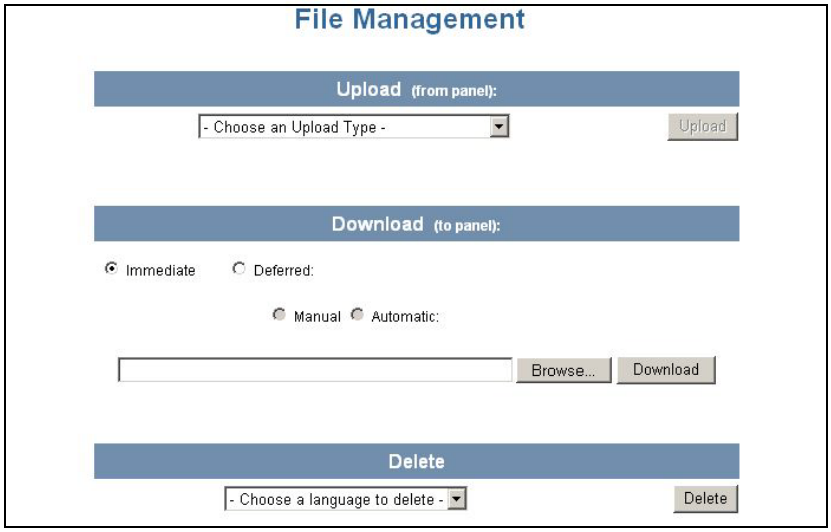
5

In this chapter...

5.1 Backing up and Restoring the NetAXS-123

Click **System Tools > File Upload/Download** to display the **File Management** screen:

Figure 5-1: *System Tools > File Upload/Download File Management Screen*



To back up (or upload) 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 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 configuration data—uploads both the card and panel configuration items in a proprietary internal format.
   - 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, Arabic, 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: Card report (short and long) data is stored in a 64-bit format. Microsoft Excel displays up to 32 characters. Therefore, you should save the report and then open the it in Notepad, instead of opening the report immediately in the default .CSV format in Excel.

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

To synchronize a new panel with information on an existing panel:

1. Upload the databases from an existing panel to a PC, as described above.
2. Remove the existing panel and insert a new panel.
3. Download the database backup to the new panel.

Important: Read Appendix A, Upgrading NetAXS-123 Firmware before downloading to the panel.

To restore (or download) firmware immediately:

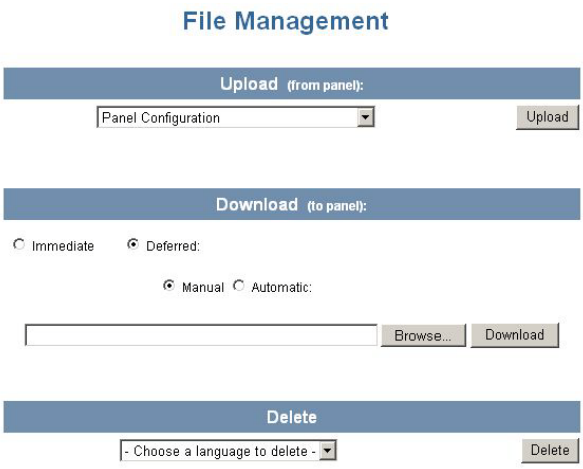
1. Click **Browse** to locate the firmware file.
2. Click **Immediate**.
3. Click **Download**.

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

To restore (or download) firmware later, at a time to be determined later:

1. Click **Browse** to locate the firmware file.
2. Click **Deferred**.
3. Click **Manual**.

Figure 5-2: *File Management Manual Setting*

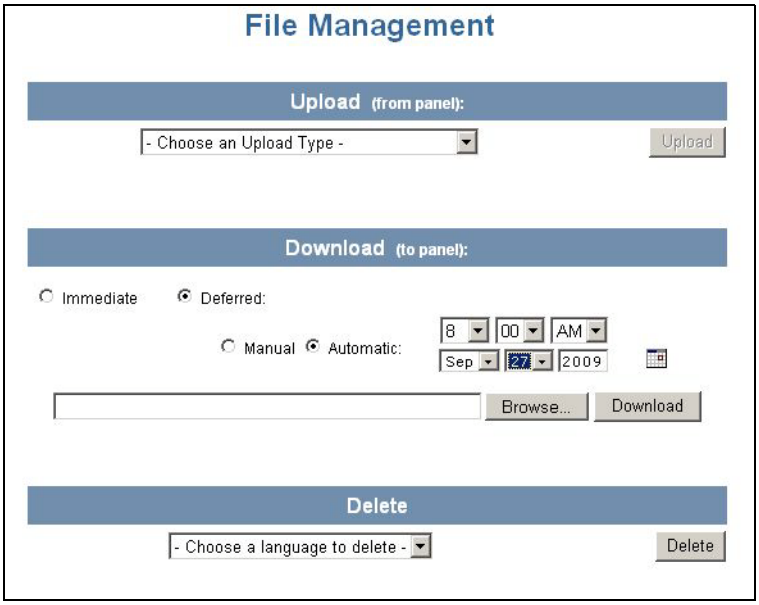


4. Click **Download**; the download status is shown as "Ready for activation".
5. Click **Ready for Activation** when you are ready to download your files.

To restore (or download) firmware automatically at a later date:

1. Click **Browse** to locate the firmware file.
2. Click **Deferred**.
3. Click **Automatic**. Time and date list boxes appear.

Figure 5-3: *File Management Automatic Setting*



4. Enter the specific date and time information.
5. Click **Download**. The download status is shown as "Activation scheduled for [month/day], [hr:min] [AM/PM]" .
6. Click **Activation Scheduled for <MONTH/TIME>** when you are ready to download your files.

Note: Every panel has its own database, and each panel's database must be backed up individually. For more information, see Upgrading NetAXS-123 Firmware, page 121.

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.

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.

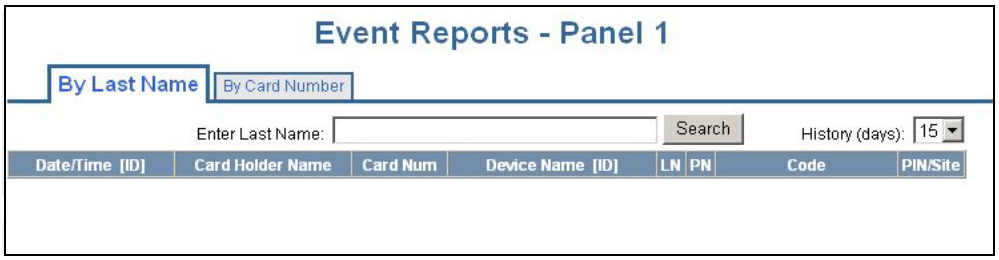
5.2 Generating Reports

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 5-4: *Reporting > Event Reports > By Last Name Tab*



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

3. Use the descriptions in Table 5-1 to read the event records.

Table 5-1: *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 either on a Controller or its attached 1- or 2-Door I/O board. There is one exception to this: Door Readers. For a list of common values, see Table 4-2.
PN	**Physical Device Number** - A number at the board level that is assigned to a specific alarm generating point. NetAXS-123 Controller starts at 1 and goes to 8, 1-Door I/O board as a new board goes from 1 to 4, and 2-door I/O board goes from 1 to 8. System alarms such as reset which are not board-specific will report a value of 0. There is one exception to this: Door Readers. For a list of common values, see Table 4-2.
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 5-5: *Event Reports By Card Number Example*

Upgrading NetAXS-123 Firmware

A

In this appendix...

Caution: Make sure to back up the panel database prior to upgrading the panel firmware.

Overview

The following procedures provide step-by-step instructions for upgrading NetAXS-123 controllers to version 5.0 software. The v5.0 software upgrade consists of an application firmware update (performed first) and a Linux OS kernel update (performed after the application firmware update).

The following procedures are provided:

- Backing up the database from each panel
- Updating the panel (Using NetAXS Update Utility)
- Updating the panel (Using Web Interface)

Important Notes

1. NetAXS-123 firmware must be at level **3.3.6** or higher before upgrading to the current R5.0 release.
2. **WARNING**: the application file must be downloaded **BEFORE** the **OS** file.
3. **WIN-PAK: WIN-PAK XE/SE/PE** Build Number **670.21(v3.3)** will work with **NetAXS-123 v5.0**. **WIN-PAK CS v4.2** (upcoming release) will also work with **NetAXS-123 v5.0**.

Upgrade Planning

You should plan for approximately 12 minutes to upgrade 1 panel (switched to gateway mode). Depending upon your configuration, to save time, you may be able to start multiple panel upgrades on your loop at the same time. Given the time needed to upgrade your loop, please plan the upgrade so it has the least impact on the access control of the building.

The new application firmware and Linux kernel can be downloaded from the Honeywell Download Center at the following site: http://www.honeywellsystems.com/support/download-center/index.html.

Download the following version numbers:

Application firmware version: 5.0.16 (file name 1-NetAXS-123_Upgrade_apps05.00.16.bin)
Linux OS (kernel update) version: 2.6.25#107 (file name 2-NetAXS-123_Upgrade_OS107.bin)

Systems with Both NetAXS-4 and NetAXS-123 Panels Looped

Upgrade your system commencing with the gateway panel first. There are two requirements for mixing the two types of panels:

1. NetAXS-123 must be the gateway. This is due to the new web screens that a NetAXS-4 as a gateway will not understand.
2. NetAXS-4 panels are required to be at Release 3 (v3.1.8) or higher before being added to the loop. For optimum performance the NetAXS-4 panels should be upgraded to Release 3.4 (v3.4.3) with OS #368.

Note: The v5.0 firmware upgrade is only for NetAXS-123 panels. V5.0 does not operate in NetAXS-4 panels.

Preliminary Step for Web-Based Panels: Backup the Databases

Note: The upgrade scripts bring all your panel data forward into the new version without the need for user intervention. However, it is always recommended **that the user have a backup database from EACH of the panels**. The upgrade task provides an opportunity to keep your backups current. The procedure below can be used to backup each of your panel's databases. The backup features are **per panel**, so the user will have to first select the desired panel to backup.

Backing Up Database from Each Panel

1. Select the panel to backup from the Select Panel section in the Web Server.
2. Navigate to System Tools > File Upload/Download from the Home page.
3. Under Upload (from panel), select each of the following three upload options (one at a time) from the drop-down menu:
    a. Cards, Common, and Panel Configuration (then go to step 4),
    b. Cards and Common Configuration (then go to step 4),
    c. Panel Configuration (then go to step 4).
4. Click Upload to upload (backup) the data from the panel to the host PC or laptop. Return to step 3 until all 3 database files have been saved to the PC.

    Give the backup file a useful name for easy recognition when restoring.

Note: Ensure you repeat the process to get a copy of each of the three menu options listed in step 3. The user should start with the Cards, Common, and Panel Configuration option as that is the entire database.

Method A: Update NetAXS-123 Panel Using NetAXS Upgrade Utility

Installing the NetAXS Upgrade Utility

The current version of NetAXS Upgrade Utility is v01.01.12.

1. Locate and download the Update Utility from the Honeywell Download Center at the following site: http://www.honeywellsystems.com/support/download-center/index.html. The file name is **NetAXS Upgrade Setup.exe**.
2. Double-click on the file to open the NetAXS Upgrade Setup window.
3. Click **Install**.

4. A screen with a progress bar will appear, then the NetAXS Upgrade Setup Wizard will launch.
5. Click **Next**, then follow the prompts.
6. The final screen will display Installation Complete. Click **Close**.
7. You should now have the NetAXS Upgrade icon on your desktop.

Running the NetAXS Upgrade Utility

1. Launch the NetAXS Upgrade Utility.
2. On the menu bar go to Tool > IP Configuration.
3. Enter in the panel's IP address and click **Confirm**. The default Ethernet IP address is 192.168.1.150.
4. Go to Connection Type on the menu bar and select Ethernet.
5. In the utility click **Get Panel Info** to ensure it is the correct panel.
6. Click **Browse for Upgrade Files** and locate the following files:

   1-NetAXS-123_Upgrade_apps05.00.16.bin and **2-NetAXS-123_Upgrade_OS107.bin**
7. Use the arrows on the right side to arrange the order of installation.
8. Make sure the 1-NetAXS-123_Upgrade_apps05.00.16.bin file is the first on the list.
9. Click **Start Upgrade**. The process takes about 6-7 minutes for each file.
10. The new version information will display in the top section of the utility when done.

Note: If the correct version does not display, repeat the upgrade one file at a time.

Note: To upgrade using the NetAXS Upgrade Utility via USB connection, follow the steps above, except at step 3 enter the default USB IP address 192.168.2.150 and at step 4 select USB instead of Ethernet.

Warning: Do NOT connect the USB cable to the panel until AFTER the drivers are installed. See Installing the NetAXS-123 USB Driver, page 138, for the procedure to install the USB drivers.

Note: The USB port will work without the panel being a GATEWAY panel for the purpose of using the NetAXS Upgrade Utility.

Note: If the OS or the firmware versions are already the latest, you may select only the file necessary.

Method B (Alternative): Update NetAXS-123 Panel Using Web Interface

Note: To use this method the panel must be set as a Gateway and also be in WEB mode.

1. Connect to your Gateway panel using the instructions from Connecting to the Web Server, page 3.
2. If you are unsure if the panel requires a firmware update, from the Landing Page go to System Tools > Firmware Details. Under Application Firmware you will see the Active Version of the firmware. For panels that have already had the firmware updated to v5.0, their Active Version will be displayed as **5.0.16**.
3. Once logged into your Gateway panel, go to the System Tools > General Configuration > Host/Loop Communications tab, and select **none** next to Web Mode. Click **Submit Changes**.

Warning: The application file must be downloaded as in step 1 below **BEFORE** downloading the OS file.

Step 1: Install the new App file 1-NetAXS-123_Upgrade_apps05.00.16.bin

1. Navigate back to the web server Landing page > System Tools > File Upload/Download.
2. Under Download click **Browse** to locate the **1-NetAXS-123_Upgrade_apps05.00.16.bin** file.
3. Select the file and click **Download**. Click **OK** to continue. Once the *Download to gateway panel complete; now processing the image* message pops up, click **OK** again.
4. You will see the *Download to gateway panel complete; now processing the image* message once again. Click **OK**. This time a reboot will be triggered and you will see the message: *The Panel is now rebooting*. Wait 4-5 minutes, then click **Refresh** and log back in.

Step 2: Install the new OS file 2-NetAXS-123_Upgrade_OS107.bin

Note: This procedure may not be needed, panels may already be at the latest OS.

1. Navigate back to the web server Landing page > System Tools > File Upload/Download.
2. Under Download click **Browse** to locate the **2-NetAXS123_Upgrade_OS107.bin** file.
3. Select the file and click **Download**. Click **OK** to continue. Once the *Download to gateway panel complete; now processing the image* message pops up, click **OK** again.
4. You will see the *Download to gateway panel complete; now processing the image* message once again. Click **OK** to continue. This time a reboot will be triggered. It will take approximately 2 minutes for the reboot to complete.
5. **Clear Cache and Cookies:** This time, before logging back in, use the browser-dependent steps found in Clearing Cache and Certificate Errors, page

127, to clear your browser cache and cookies. You can navigate away from the current web screen, clear the files, and then navigate back.

Step 3: Check that the Installed Versions are Correct

1. Navigate back to the web server Landing page > System Tools, and select **Firmware Details**.
2. In the Application Firmware section, you should see the new Active application versions listed as **5.0.16**. In the Operating System section, you should see the OS version as **2.6.25#107**.
3. For WIN-PAK based loops, it is recommended that you run a full download to all the panels once the new version is installed.
4. If you notice any communication issues, and the upgrades are complete, typically this means there is more than one panel set up as a gateway on the active loop. You should disconnect each panel from the 485 loop (C-TB9), and cycle power on all the panels on the loop. Once all panels are powered up, reconnect the 485 loop to clear the issue.

Note: It is recommended to save a current backup of the database after upgrading the panel.

After upgrading a NetAXS-123 panel to Rel 5.0, you must clear your browser's cache. See Clearing the COokies and Cache, page 138 for details.

Clearing Cache and Certificate Errors

B

In this appendix...

Clearing the Cache and Cookies in the Internet Browsers Used by the NetAXS-123 Web Server

The NetAXS-123 R5 supports Internet Explorer 8 (IE8), Internet Explorer 9 (IE9), and Mozilla Firefox 19-21. It is recommended that the cache be cleared following a successful upgrade.

Note: After upgrading a NetAXS-123 panel to Rel 5.0, you must clear your browser's cache.

1. To clear the cache in either Firefox or Internet Explorer, press these 3 keys simultaneously: ***Ctrl* + *Shift* + *Del***.
2. Then, ensure that the selections pictured in the following screens (see Figure 1 for Firefox and Figure 2 for Internet Explorer) are chosen and click **Clear Now** (for Firefox) or **Delete** (for Internet Explorer).

Figure B-1: *Clearing Cache with Mozilla Firefox*

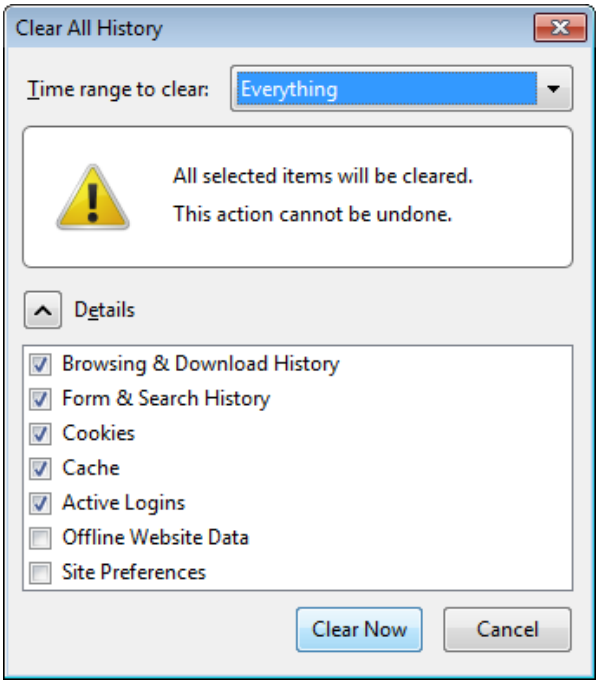
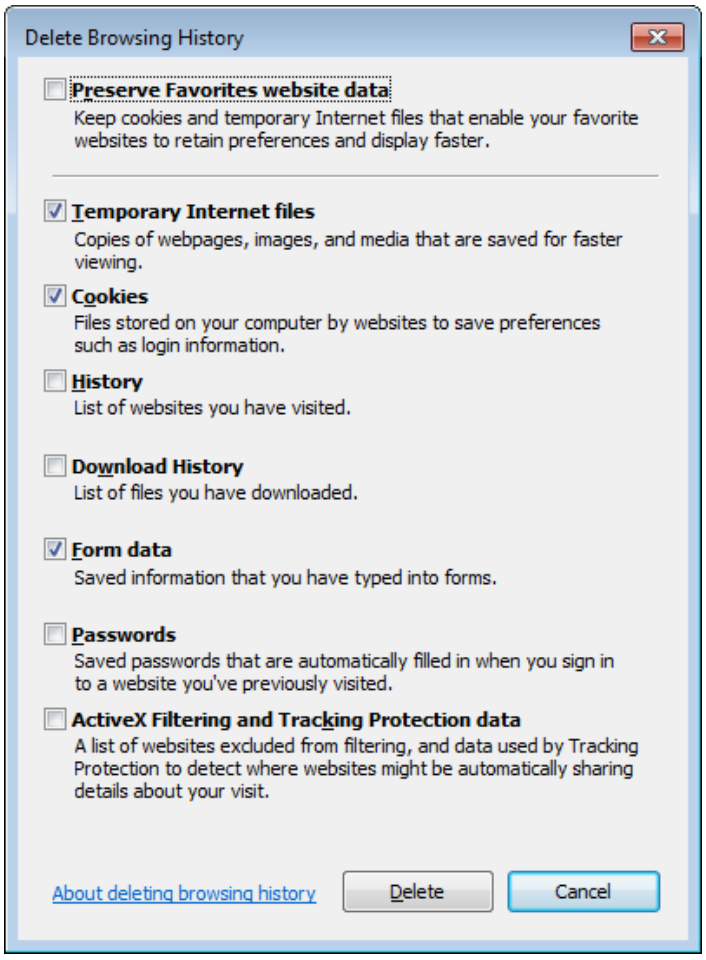


Figure B-2: *Clearing Cache with Internet Explorer (IE9 shown)*



Certificate Error with IE8 on Windows XP

If you receive a Certificate Error when using IE8 on Windows XP, follow these steps to add the certificate:

1. Enter the IP Address of the panel into the URL box.
2. Click on **Continue to the website (not recommended)** to get the login screen.
3. Click **Certificate Error** to the top-right of the IP Address.
4. The Untrusted Certificate popup will open, click on the **View certificates** bar.
5. The Certificate Information screen will appear, click **Install Certificate**.
6. The Certificate Import Wizard will open.
7. Click **Next** and follow the prompts, leaving all of the settings at default.
8. A Security Warning asking if you want to install the certificate will open. Click **Yes**.

9. The Certificate Import Wizard popup that reads The import was successful will open. Click **OK**.
10. The Certification Information popup will appear again. Click **OK**.
11. ***Close the web browser and re-open it***.
12. Enter the IP Address into the URL box again. The login screen without the Certificate Error will appear.

Certificate Error with IE8/IE9 on Windows 7

If you receive a Certificate Error when using IE8 or IE9 on Windows 7, follow these steps to add the certificate:

1. Enter the IP Address of the panel into the URL box.
2. Click on **Continue to the website (not recommended)** to get the login screen.
3. Click **Certificate Error** to the top-right of the IP Address.
4. The Untrusted Certificate popup will open, click on the **View certificates** bar.
5. The Certificate screen will appear defaulted to the **General** tab. Click **Install Certificate**.
6. The Certificate Import Wizard will open.
7. Click **Next**. The Certificate Store page will open.
8. Select the **Place all certificates in the following store** radio button.
9. Click **Browse**. The Select Certificate Store window will open.
10. Select **Trusted Root Certification Authorities** and click **OK**.
11. Click **Next** on the wizard then click **Finish**.
12. You may get a Security Warning, asking if you want to install the certificate. Click **Yes**.
13. The **Certificate Import Wizard** popup that reads The import was successful will open. Click **OK**.
14. The Certificate screen is still open. Click **OK** to close it.
15. ***Close the web browser and re-open it.***

Certificate Error with Firefox 19-21

If you receive a Certificate Error when using Firefox v19 through 21, follow these steps to add the certificate:

1. Enter the IP Address of the panel into the URL box.
2. Click on **I Understand the Risks** to expand the screen.
3. Click **Add Exception** to display the Add Security Exception screen.

4. Click **Get Certificate**. An Unknown Identity message will appear in the middle of the screen.
5. Ensure that the **Permanently store this exception** checkbox is enabled. (This is the default setting.)
6. Click **Confirm Security Exception**. The screen returns to the Security Connection Failed screen with a progress bar in the lower right corner.
7. The next screen displays the NetAXS-123 Login screen.
8. Continue with the login.

NetAXS-123 DIP Switch Settings C

This appendix provides a table listing DIP switch settings for the NetAXS-123 panel.

Table C-1: *NetAXS-123 SW1 DIP Switch Settings*

S1	S2	S3	S4	S5	S6	S7[1]	S8[2]	S9[2]	S10	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

Table C-1: *NetAXS-123 SW1 DIP Switch Settings* (continued)

S1	S2	S3	S4	S5	S6	S7[1]	S8[2]	S9[2]	S10	Selection
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					Downstream Panel
					ON					Gateway Panel (Default)
						OFF				Uses the User Provided Ethernet IP address (Default)
						ON				Uses the Default Ethernet IP Address (192.168.1.150)
							OFF	OFF		RS-485_1 termination (EOL) DISABLED (Default)
							ON	ON		RS-485_1 termination (EOL) ENABLED
									OFF	Future Use (Default)
									ON	Future Use

1. DIP Switch 7 does NOT require a panel reboot to take effect. This does not affect the USB IP address.
2. Both DIP Switch 8 and DIP Switch 9 need to be either ON or OFF to be properly configured.

Table C-2: *NetAXS-123 SW2 DIP Switch Settings*

S1[1]	S2[1]	Selection
OFF	OFF	RS-485_2 termination (EOL) DISABLED (Default)
ON	ON	RS-485_2 termination (EOL) ENABLED (FUTURE)

1. Both DIP Switch 1 and DIP Switch 2 need to be either ON or OFF to be properly configured.

Note: When you use the DIP switches to reset a panel to the original factory default values, the Event History is lost and any customized databases are removed, so the panel is reset with the original factory default database. This does not affect the Ethernet IP address.

You can also use the ASCII command _I=pn_R to reset a panel to the original factory default values, but this command only removes the customized databases and restores the original factory default database. The Event History is retained.

To reset the panel to the factory default values:

1. Make a note of the existing settings on SW1 DIP switches.
2. While the panel is powered up, turn all of the DIP switches to the OFF position.
3. Power down; then power the panel back up.
4. Wait for the panel to come up. The RUN LED should flicker fast.
5. Set the DIP switches back to their original positions.
6. Power down; then power the panel back up. The RUN LED should flash normal.

The panel is now reset to the original factory default values.

USB Driver

D

In this appendix...

Installing the NetAXS-123 USB Driver

You will need to install a USB driver to support the connection with your laptop or PC. The following procedure will take you through the steps to do so.

Warning: Do NOT connect the USB cable to the panel until AFTER the drivers are installed.

1. Insert the NetAXS-123 Product CD into your Windows-based computer. Select your preferred language when the NetAXS-123 product menu opens.

Note: If the NetAXS-123 product menu does not open automatically, right click on the **Start** button and select **Explore**. In the folder tree, find and click the CD drive that is reading the NetAXS-123 Product CD and double-click **CD_Start.exe**.

2. Click **Install USB Drivers** on the product menu to start the USB driver installation wizard.
3. Click **Next** to display the Ready to Install the Program screen.

Note: If confirmation dialog boxes pop up before or during the installation procedure, click the appropriate boxes to allow or approve the installation.

4. Click **Install** to initiate the installation.
5. When the installation is complete, the closing screen appears.
6. Click **Finish**.
7. Connect the computer to the NetAXS-123 controller with a USB-A to Micro USB-B cable.
8. Turn on the power to the NetAXS-123 controller.
9. To log-in to the NetAXS-123 panel using the USB, enter **https://192.168.2.150** into the browser.

Index

E

F

G

H

I

L

M

N

O

P

R

S

T

U

W

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 800-05168V2 - Rev A

Honeywell