Honeywell

NetAXS-123

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.

April 2010

800-05168, Revision B

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

Chapter 3 Using WIN-PAK with NetAXS-123

Chapter 4 Monitoring NetAXS-123 Status

Chapter 5 File Management

Appendix A Upgrading NetAXS-123 Firmware

Appendix B NetAXS-123 DIP Switch Settings

FIGURES

TABLES

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 Supported Configurations, page 77.

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

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

- USB
- Ethernet through a web server hub connection
- Ethernet through a web server direct 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.

1.2.1 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.

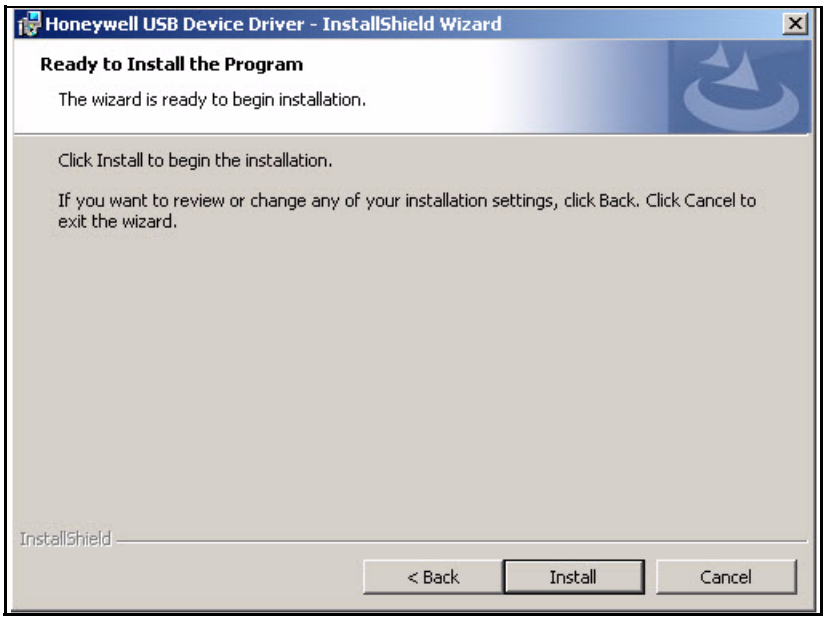
1. Insert the NetAXS-123 Product CD into your Windows-based computer. The NetAXS-123 product menu opens in the web browser.

   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.

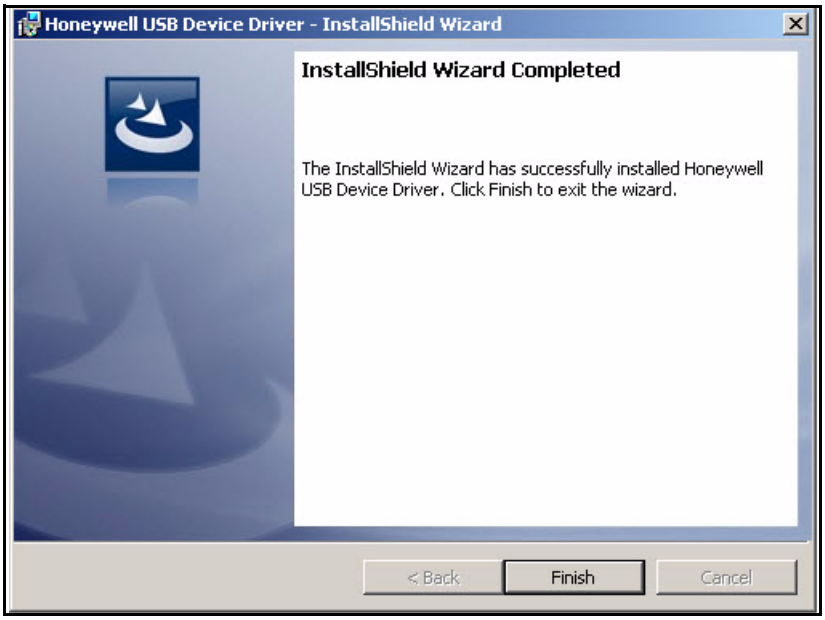
2. Click **Install USB Drivers** on the product menu to start the USB driver installation wizard.

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.

1.2.2 Setting up an Ethernet Port

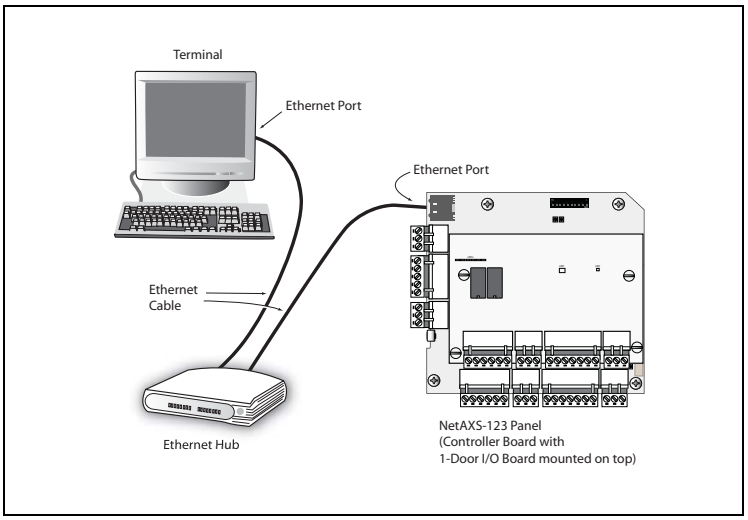
There are two options for connecting the panel to a PC via a web server:

- Using a hub connection
- Using a direct connection

Perform the following steps:

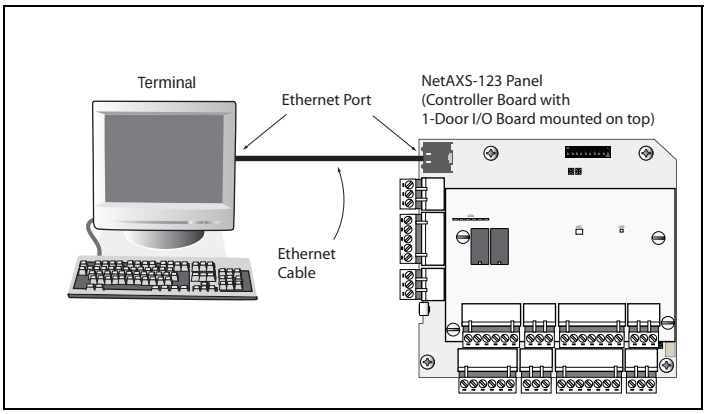
1. Connect your computer's Ethernet port to the panel's Ethernet Port using one of the two following methods:
    a. For an Ethernet Hub connection, connect both the computer’s Ethernet port and the panel's Ethernet port to an Ethernet hub with standard Ethernet patch cables.

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



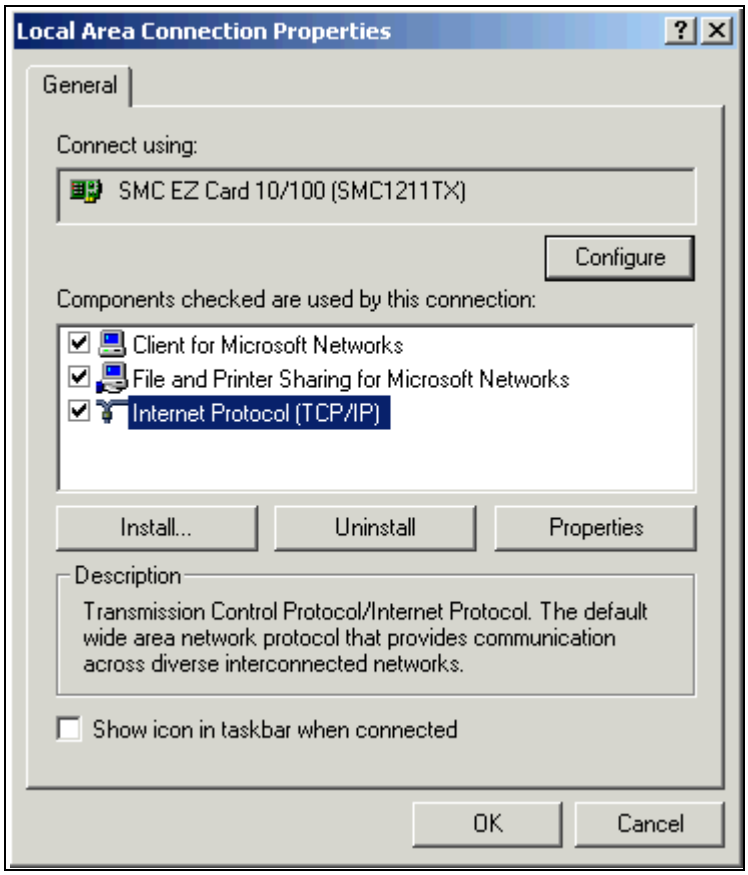
b. For a web server direct connection, connect the computer's Ethernet port directly to the panel's Ethernet port with either a crossover or an Ethernet cable.

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.

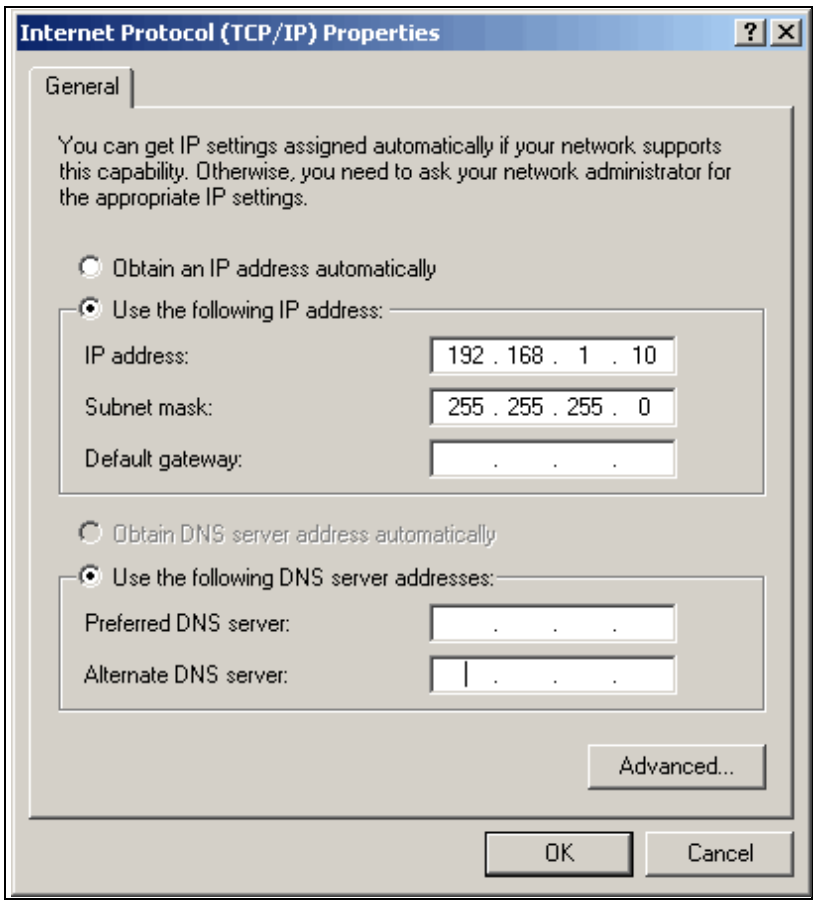
e. Click **Properties** to display your system's current Internet Protocol properties.

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."

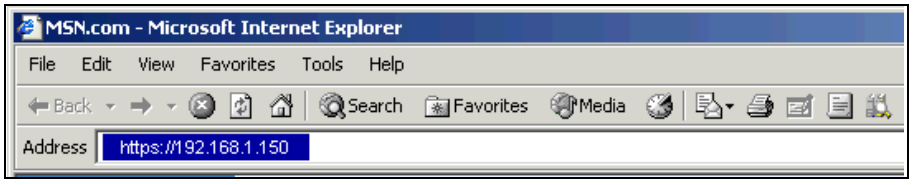
g. Enter "192.168.1.150" in the IP address field.

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



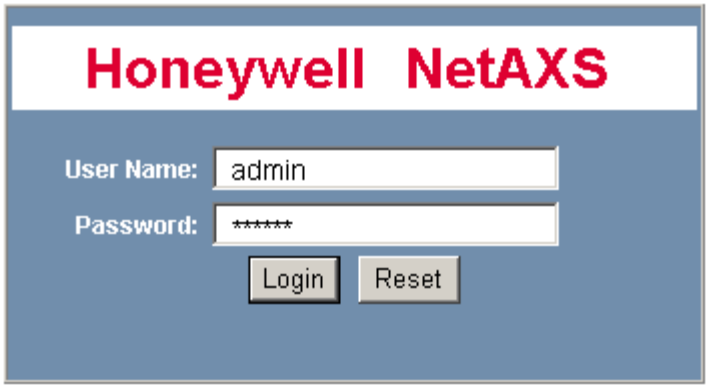
i. Click **OK** to accept the entries.

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.

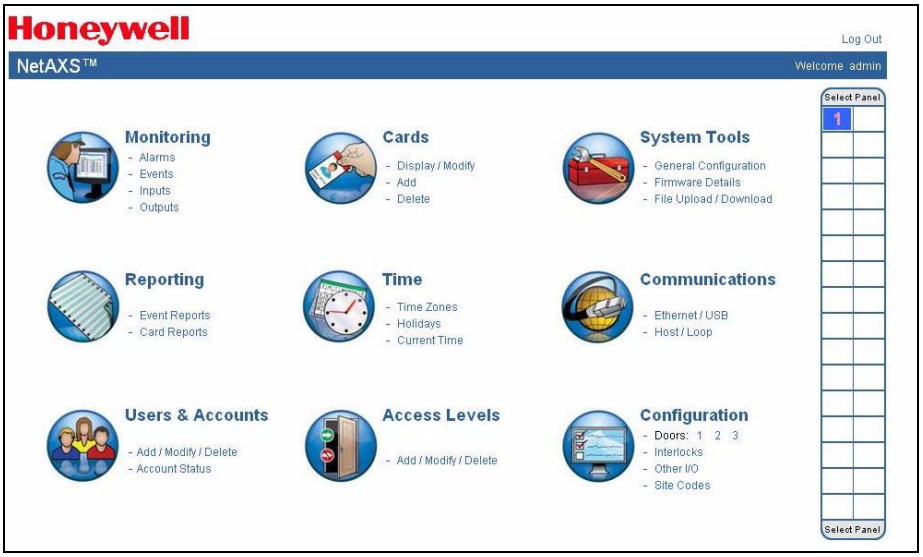
k. Enter the IP address again into the URL box. The login screen appears without the certificate error.

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 70.

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 Select Panel column on the right edge of the Main Window displays all panels available to the computer. This list displays the number of the gateway panel that you are connected to over Ethernet and any downstream panels connected via RS-485 to the Gateway panel.

1.3 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 117
	Generate event reports and card reports	Maintaining Cards, page 56 and Generating Reports, page 125
	Create, modify, and delete users, and checks account status	Configuring Users, page 70
	Manage cardholder cards	Maintaining Cards, page 56
	Configure time management	Time Zones Tab, page 31
	Manages access levels	Configuring Access Levels, page 54

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

Icon	Description	For more information, see..
	Provides file management functionality	Generating Reports, page 125
	Configure connectivity	Configuring the System, page 18
	Provides system configuration functionality[a]	Configuring the System, page 18

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. The Controller lists only the door, no numbers. A Controller with a 1-door I/O board will report Doors: 1 2.

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

1.4 Reading the Select Panel

The Select Panel is located at the right margin of the NetAXS-123 web server main screen. The presence of a number in one of the Select Panel cells indicates that its associated panel is online. For example, if you see a number 1 in a cell, this indicates that panel 1 is online. The combinations of size and color of the number and the color of the cell background indicate the panel's status, as shown in the following table.

Note: Holding the cursor over a cell also displays a popup message, which indicates whether the panel in that cell is online or selected.

The Select Panel refreshes automatically when the panel's status changes.

Table 1-2: *Reading the Select Panel*

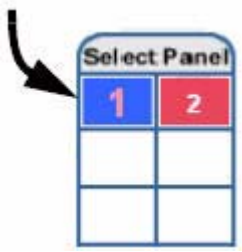
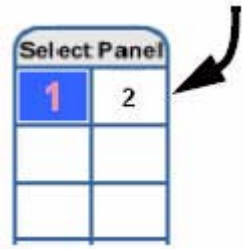
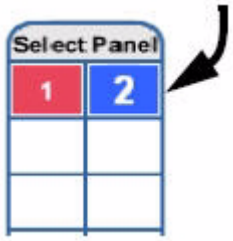
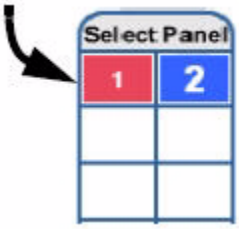
Cell Display	Status
Large red number on a blue background, such as "1" in the example below: 	Panel 1 is selected, and it has unacknowledged alarms.
Small black number on white background, such as "2" in the example below: 	Panel 2 is not selected and it has no unacknowledged alarms.

Table 1-2: *Reading the Select Panel* (continued)

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

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*

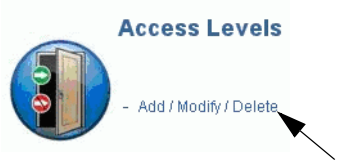
To perform this task...	Click this heading
1. Configure the panel: Host/Loop Communications Network General Site Codes	
2. Configure the time zones.	
3. Configure the doors: Readers Outputs Inputs	
4. Configure the access levels.	

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
- Site Codes
- 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 120 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:

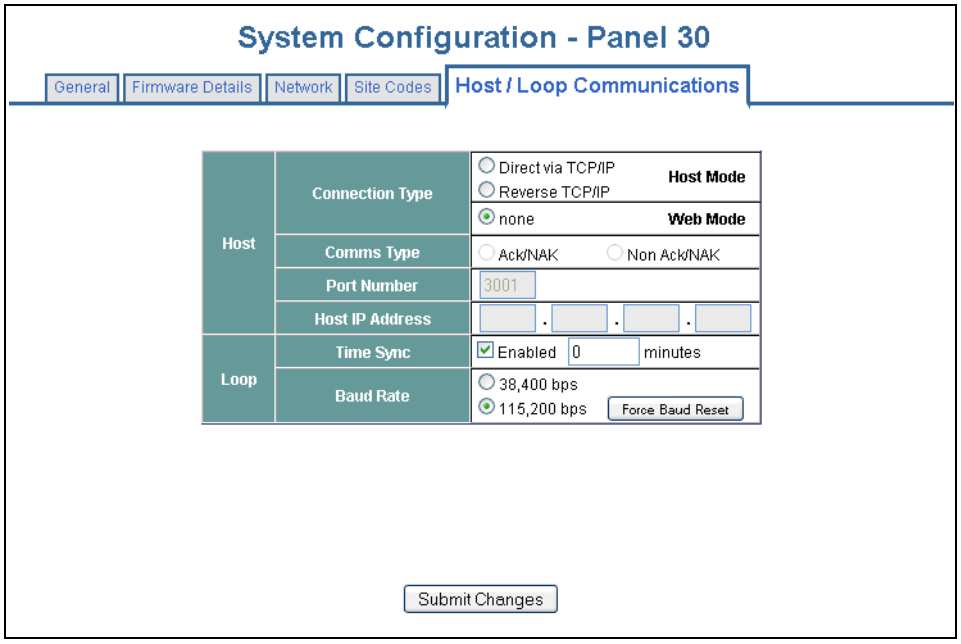
- Host mode (monitor only) – a host software system, such as WIN-PAK™, connects to the panel (through the gateway panel, which has an on-board PCI communications adapter). It enables you to monitor the status of the system.
- Web mode (configure and monitor) – the web server connects to the panel and 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 server)
  - Comms Type
  - Port Number
  - Host IP Address
- Configure the loop:
  - Time Sync (Enable—how often in minutes the gateway will broadcast its time to downstream panels)
  - Baud Rate (for communication among downstream panels)

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.
	Port Number	Specifies the port number for the Ethernet port (default is 3001). (Default for Reverse TCP/IP is 5001.)
	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.

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

Host/Loop	Setting	Description
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.

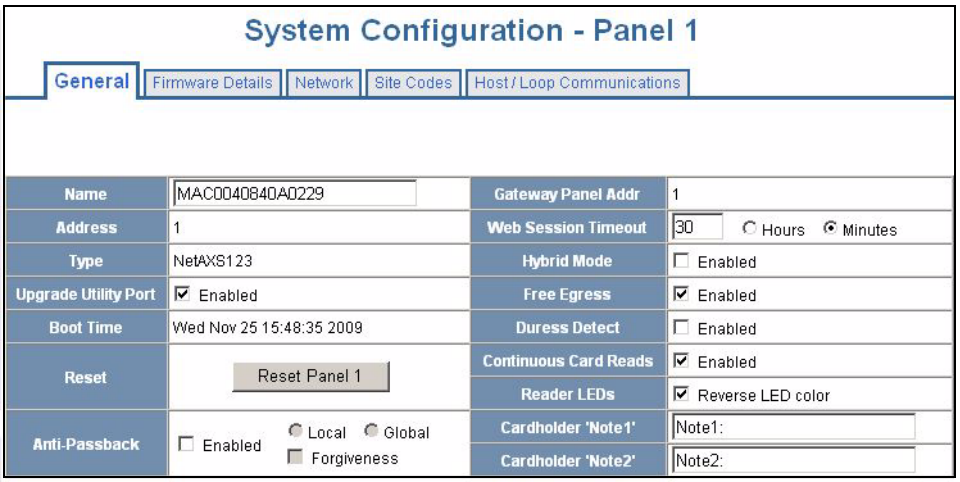
2.2.3 General Tab

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	Displays the address set by the panel's DIP (dual in-line package) switches. Note: DIP switches should be set as follows: For the 10-position DIP switch: Positions 1-5: ON position specify the RS-485 address. These settings require a reboot to take effect. Position 6: Gateway when ON, downstream when OFF. This setting requires a reboot to take effect. Position 7: When OFF, use user-provided IP address for Ethernet; when ON, use default IP address for Ethernet (192.168.1.150). When this switch changes state (OFF to ON, ON to OFF), the effect takes place immediately. No reboot is required. Positions 8 and 9: RS-485-1 line termination. Both ON: Terminated. Both OFF: Un-Terminated. Position 10: Reserved. For the 2-position DIP switch: Positions 1 and 2: RS-485 2-line termination. Both ON: Terminated. Both OFF: Un-Terminated. See NetAXS-123 DIP Switch Settings, page 153 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 www.honeywellaccess.com for details.
Boot Time	Displays the time that power was applied to the panel.
Reset	Reboots the panel. A reset does not change the current configuration in the database.

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

Parameter	Description
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).
Hybrid Mode	FUTURE FEATURE. LEAVE UNCHECKED.
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 36). 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 36) is also enabled. You then need to assign the selected output--a Pulse time in Configuration - Other I/O. (See Outputs Tab, page 48 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 36). 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 56.

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 56.

2.2.4 Firmware Details Tab

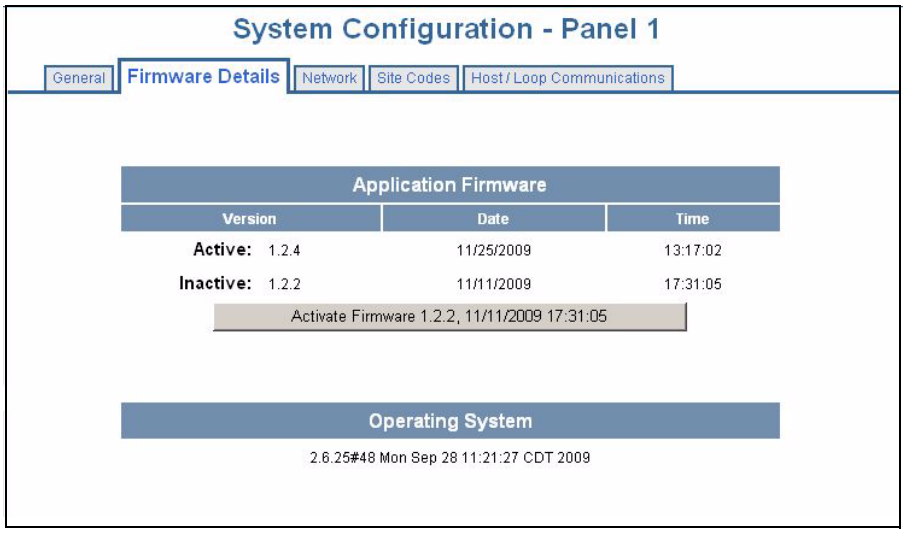
Firmware is software that is embedded in the NetAXS-123 boards. The firmware provides this web interface and all access control functionality. Periodically, the firmware is updated. The Firmware Details tab enables you to download new versions of the firmware, revert to a previous version of the firmware,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

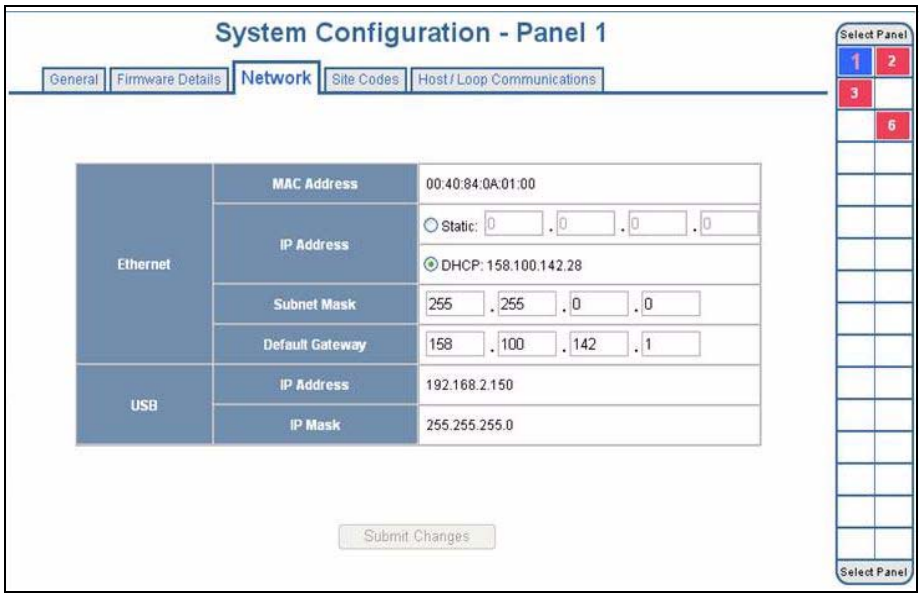
Your NetAXS-123 panel is physically configured in one of a number of possible network configurations. For the panel to function in any of these configurations, the other panels and devices in the network must know the panel's network addresses.

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, set, 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*



2.2.6 Site Codes Tab

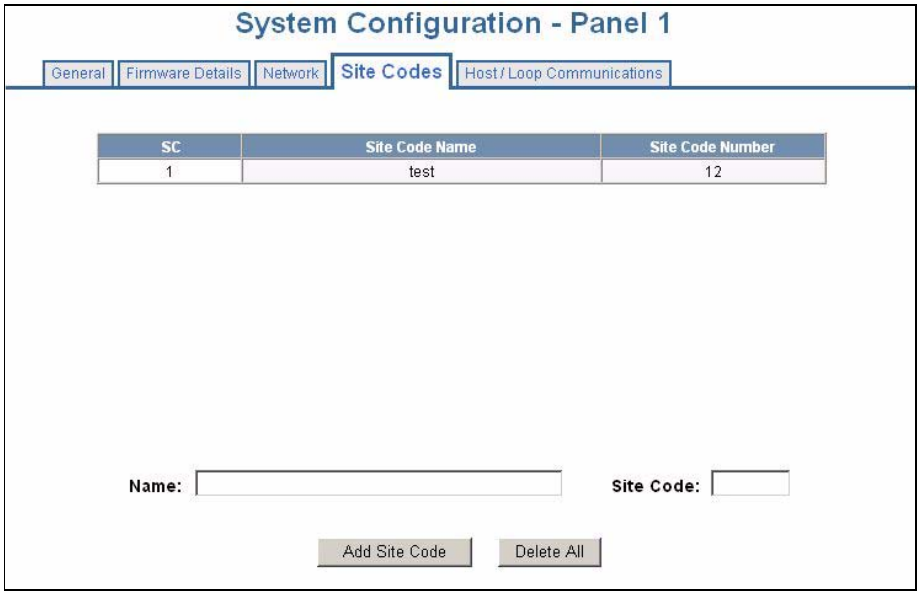
Site codes (also called facility codes) identify an enterprise's site with unique numbers for each site. You can create a maximum of eight site codes to serve as secondary IDs (in addition to the card number) on the card for additional validation.

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*

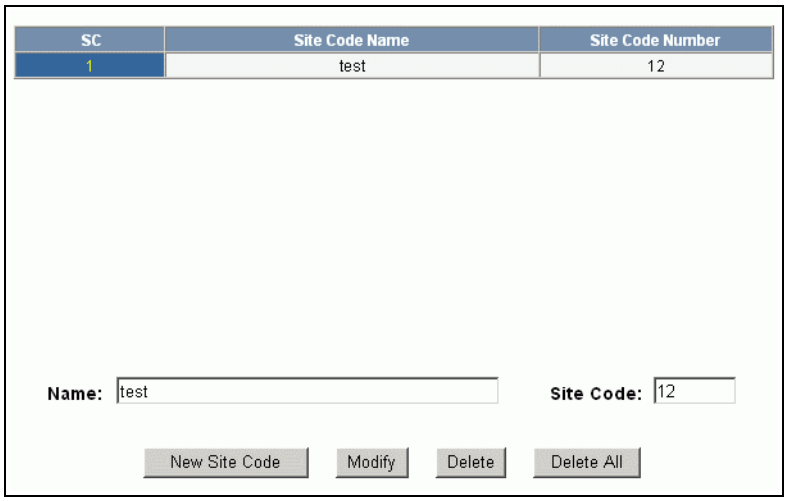


To create a site code:

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 Time Management

This set of time-related functions includes:

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

2.3.1 Current Time Tab

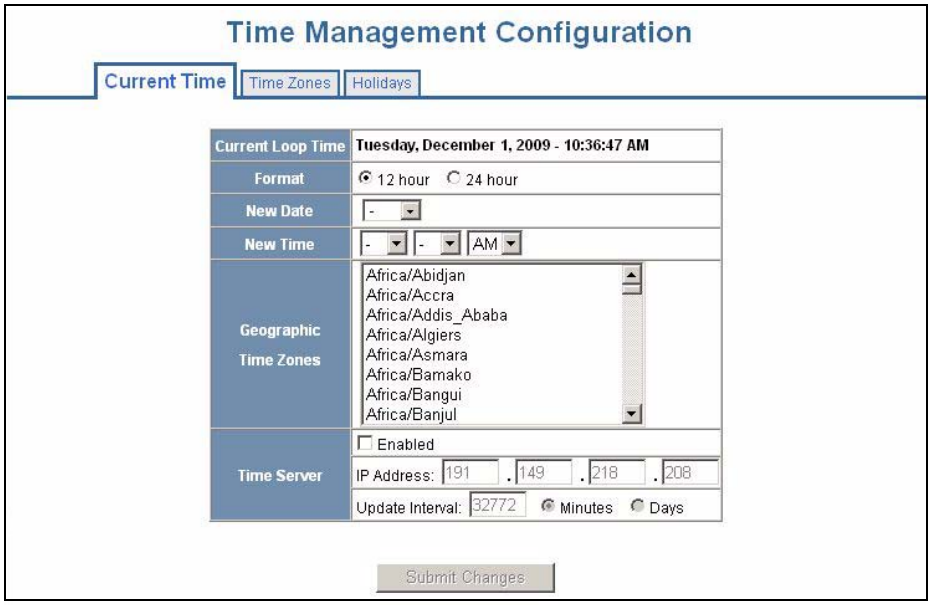
The Current Time tab displays time management configuration settings.

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



Steps: Use the descriptions in Table 2-4 to configure the time settings:

Table 2-4: *Time > Current Time > Current Time Tab Fields*

Setting	Description
Current Loop Time	Displays by default the current time setting in day/month/date/hour/minutes/seconds. For example: Fri Oct 30 07:16:27 2009.
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.
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.

2.3.2 Time Zones Tab

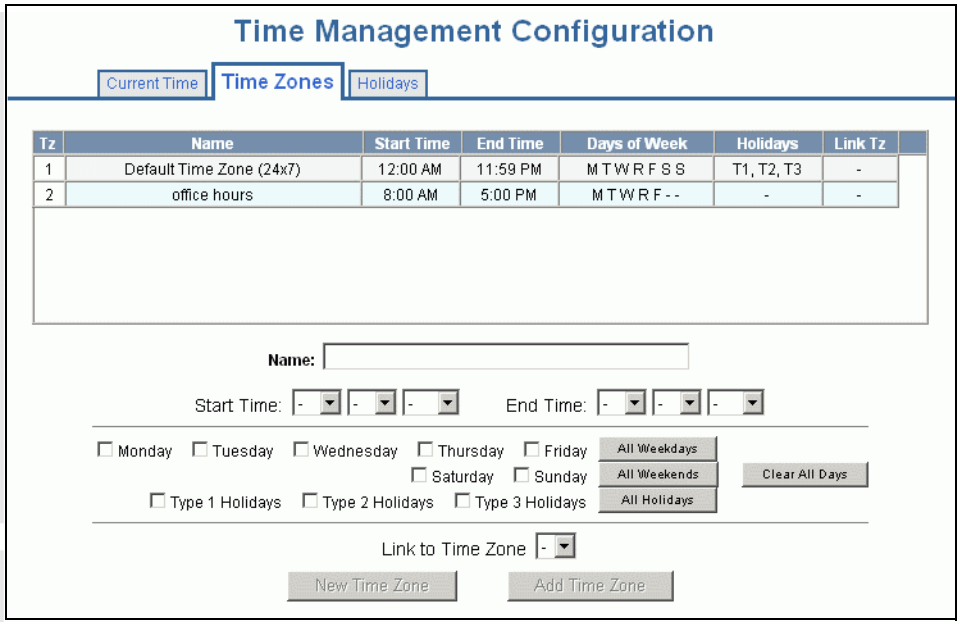
The NetAXS-123 panel controls access by using time zones, or time schedules. Inputs, outputs, readers, access levels, and cards through access levels are all configured with time zones by which they will be energized or de-energized, enabled or disabled. For example, you might assign a group of outputs 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 2-7: *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.

2.3.3 Holidays Tab

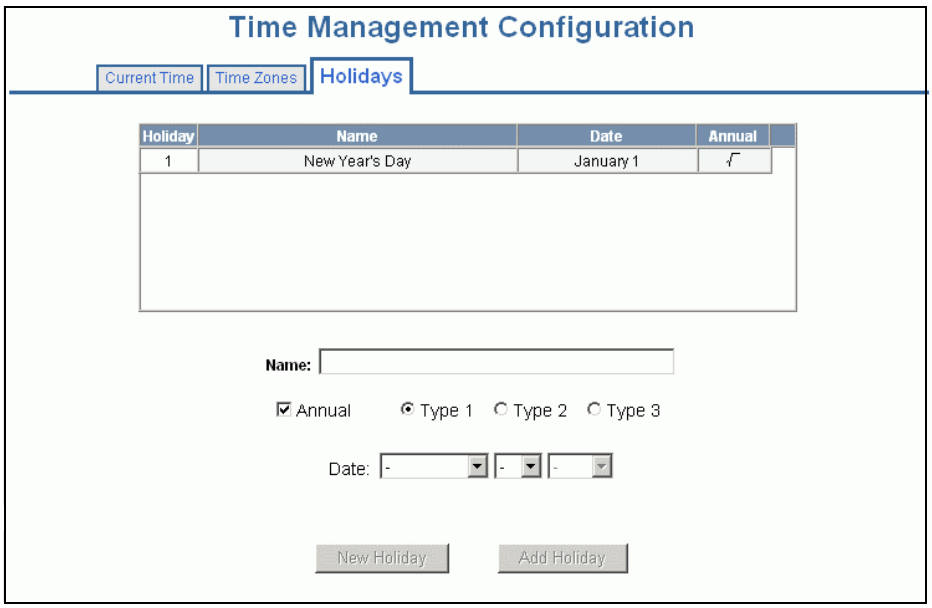
Holidays are considered special days of a week. They are similar, but of higher rank than the standard Monday-Sunday. If a day programmed as a Holiday should occur in the panel, the panel will treat that day as the Holiday type, regardless of the actual day of the week (Monday-Sunday). During this Holiday, 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 2-8: *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 31).
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:

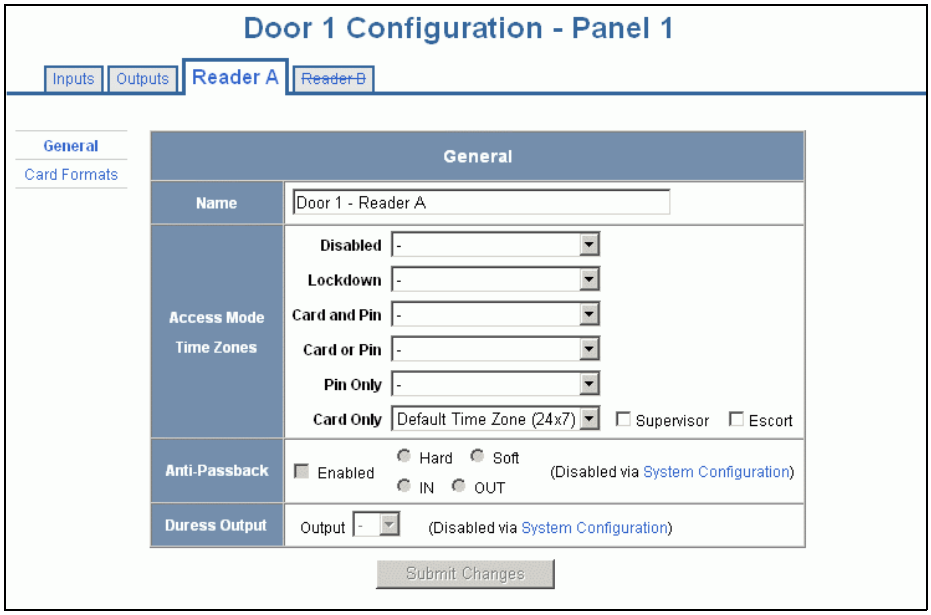
1. In the Holiday column, click the number of the holiday you want to delete.
2. Click **Delete**.
3. Click **OK** at the delete prompt.

2.4 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 2-9: *Configuration > Doors: > 1 > Reader A Tab*



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

2.4.1 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 2-9).

Steps:

1. Use the descriptions in Table 2-5 to configure the General reader settings.

Table 2-5: *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 2-5: *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.

Table 2-5: *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 21), 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.

Table 2-5: *Configuration > Doors > 1 > Reader A Tab Fields (continued)*

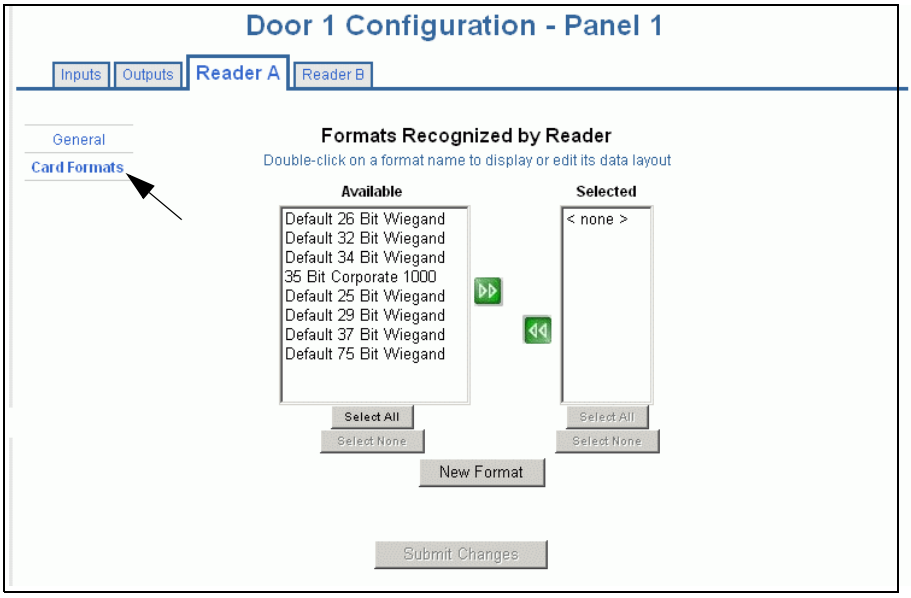
Setting	Description
Duress Output	Configures the output that will trip when a card holder enters a "duress PIN" at a keypad/card reader. A duress PIN is the PIN a user enters at a keypad when being forced (for example, during a robbery) to open a door. The card holder enters a PIN that is either one number higher or lower than the correct PIN. This PIN opens the door, but it also triggers the designated duress output and produces an alarm event. For example, if the PIN is 2222, the card holder would enter either 2221 or 2223. Even though the PIN is incorrect, the door will still open normally, but the duress output pulses and an alarm is generated. In this way, the card holder notifies others without detection by the unauthorized person. **Note**: A PIN ending in 0 (for example, 2320) will only trip a duress output when a 1 is used in place of the 0 (for example, 2321). The duress output feature requires the following: • "Duress" must be enabled on the Configuration > System > General tab. • A time zone must be selected for "Card and PIN" on the Configuration > Doors > Reader tab.

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

Note: The access mode defined here for the door can be overridden by a card assigned with a VIP card type. (See Adding New Cards, page 56 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 2-10: *Configuration > Doors: > 1 > Reader A Tab > Card Formats*



3. Use the descriptions in Table 2-6 to select card formats.

Table 2-6: *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.

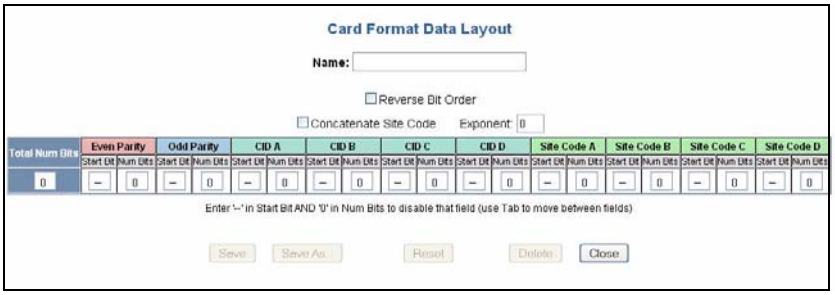
4. Click to highlight each desired card format listed in the Available box, and click the green right arrow button to move the format(s) into the Selected box.

Note: If you select no formats, the reader will use all available formats (up to 128) as described for the Available setting in Table 2-6. 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 2-6.

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 2-11: *Card Format Editing Screen*



7. Use the field descriptions in Table 2-7 to define the layout and click **Save**.

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

Table 2-7: *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.

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

Setting	Description
Total Num Bits	Lists the total number of bits on the card.
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 2-7: *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.

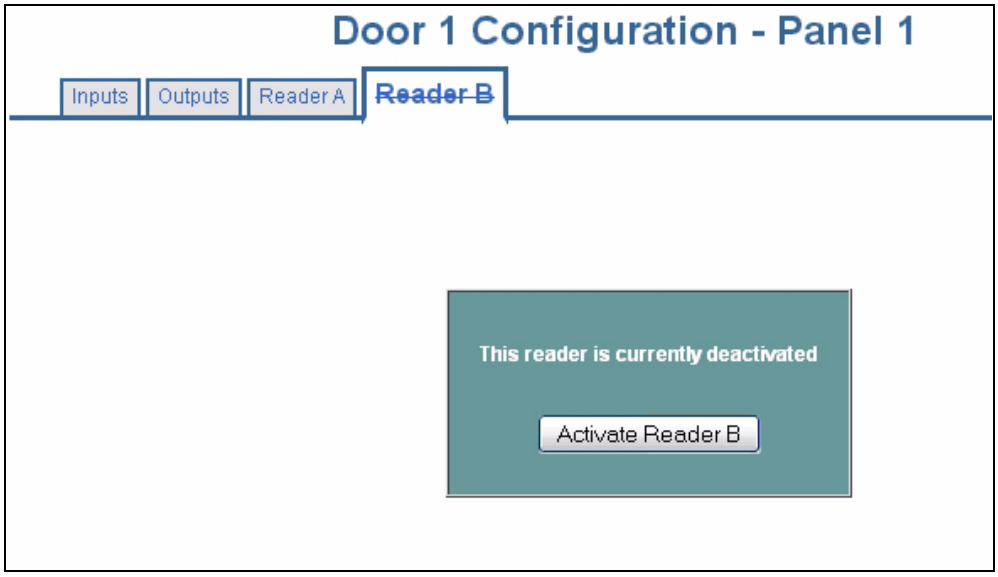
8. If you want to change an existing card format's data layout, double-click the format's name on the list of existing formats to display the Card Format Data Layout screen. Use the descriptions in the table above to edit the layout's fields. Then, click **Update** (to save in the format's current name)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

2.4.2 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.

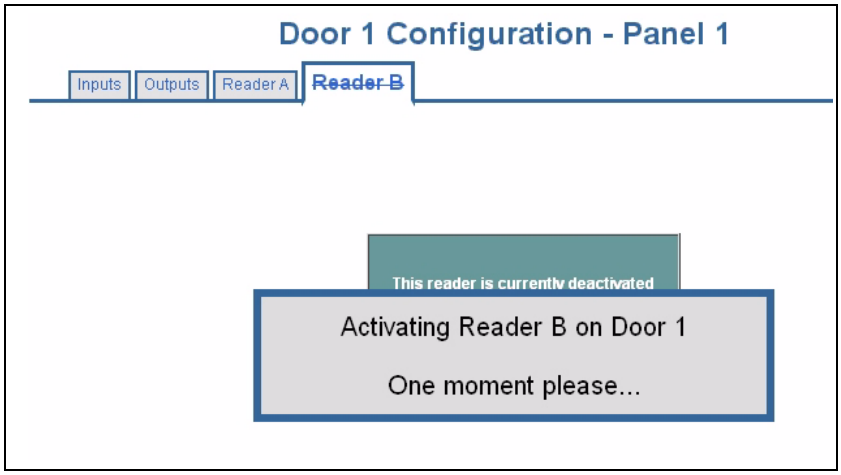
On the Reader A tab, click the **Reader B** tab to display the Reader B tab.

Figure 2-12: *Configuration > Doors: > 1 > Reader B Tab*



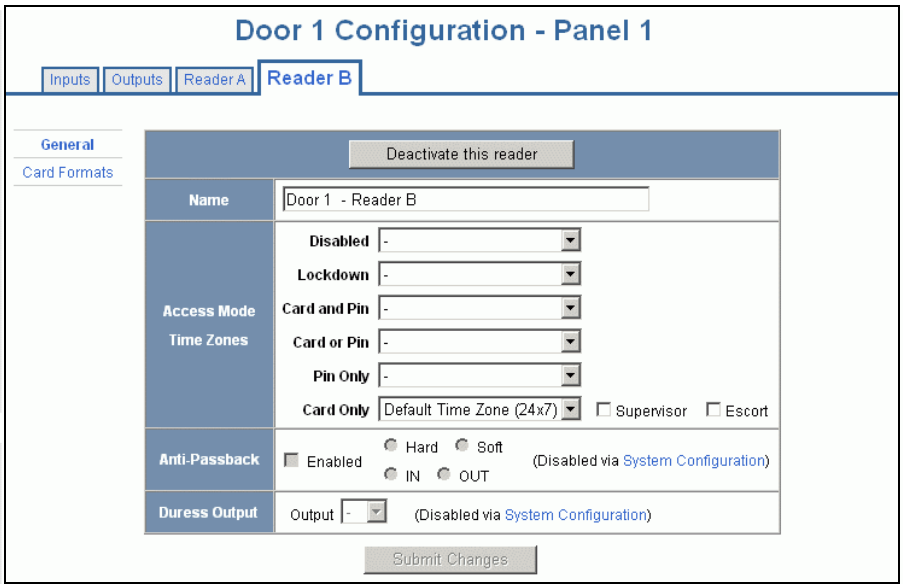
Click **Activate Reader B** to display the following "activation in-progress" screen:

Figure 2-13: *Reader B Activation In-Progress Message*



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

Figure 2-14: *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.

2.4.3 Outputs Tab

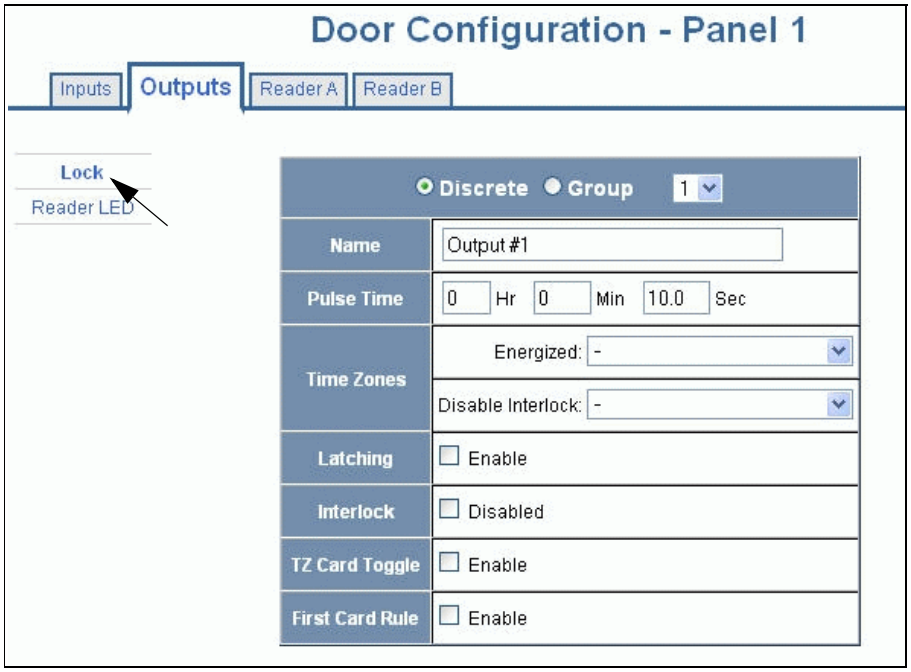
An output, or output relay, acts like a switch on the panel that either energizes or de-energizes or pulses an output device, such as a door lock or an LED. For example, a successful card read at a reader (input device) causes the output relay switch on the panel board to change the normal state of a 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

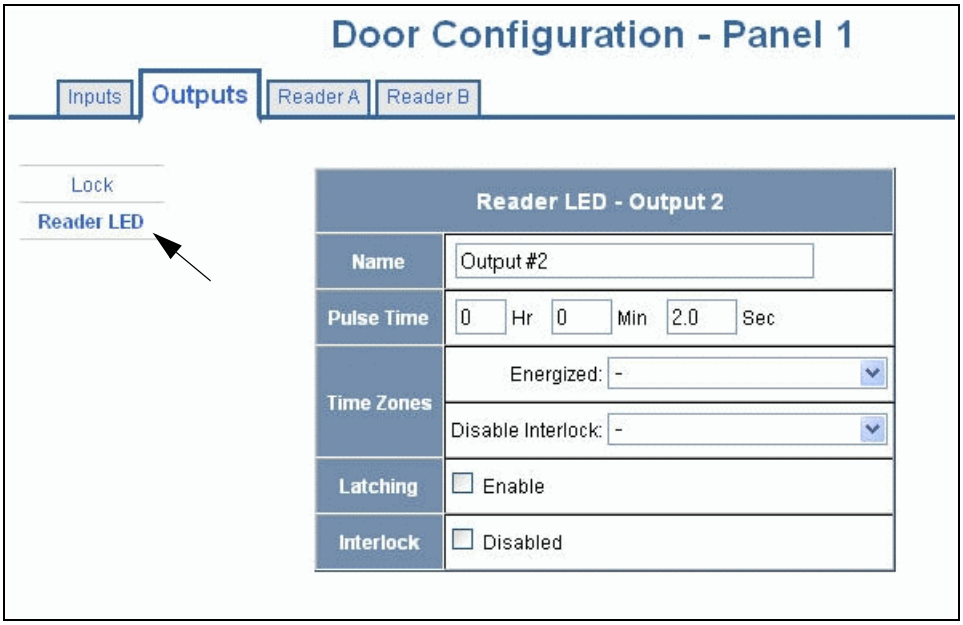
Click **Configuration > Doors: > 1 > Outputs** tab to display the Outputs tab. The **Lock > Discrete** tab appears, enabling you to configure an individual lock output. Select the output number in the drop-down list at the top of the screen. Note that lock and reader LED outputs are associated with each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

Figure 2-15: *Configuration > Doors: > 1 > Outputs > Lock Dialog Box*



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

Figure 2-16: *Configuration > Doors: > 1 > Outputs Tab > Reader LED Dialog Box*



Steps: Use the descriptions in Table 2-8 to configure each individual lock or Reader LED:

Table 2-8: *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 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. 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.

2.4.4 Inputs Tab

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

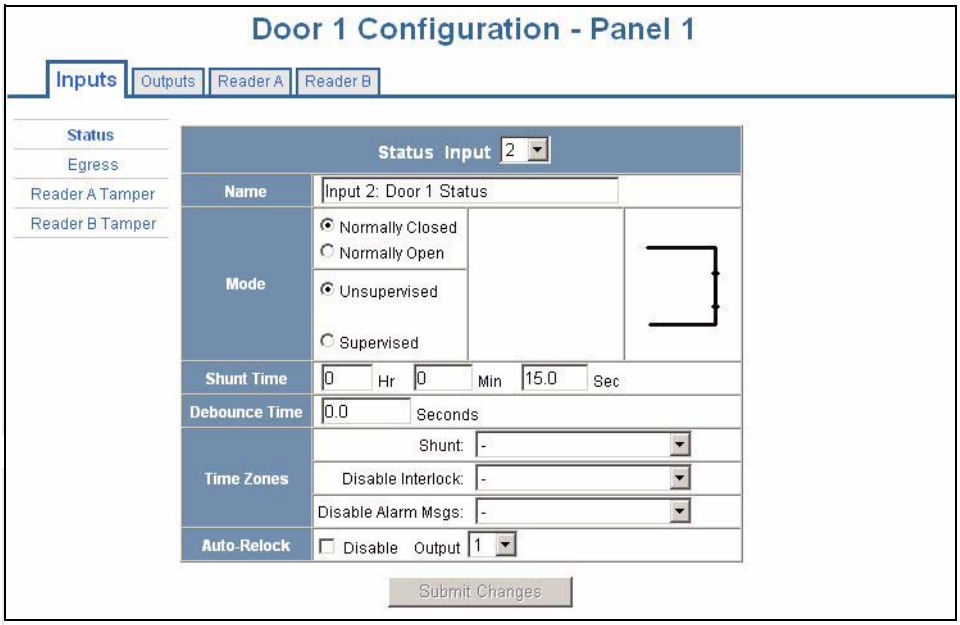
- Status – Provides door status information.
- Egress – Allows the door to open or close normally without generating an alarm.
- Tamper A – Reports abnormal handling of the reader device or wiring for Reader A.
- Tamper B – Reports abnormal handling of the reader device or wiring for Reader B.

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 2-17: *Configuration > Doors: > 1 > Inputs Tab > Status*



There are four possible Mode configurations. Figure 2-17 shows the Normally Closed/Unsupervised Mode. The following screens show the remaining modes:

Figure 2-18: *Input Status Mode - Normally Open - Unsupervised Mode*

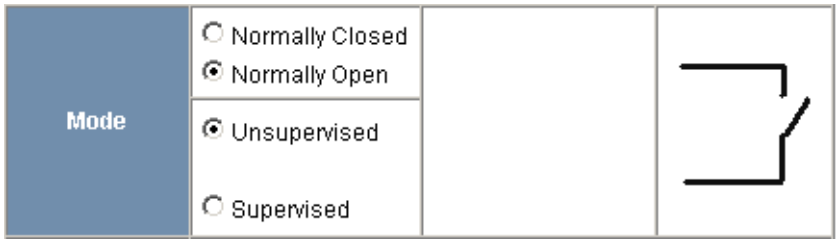


Figure 2-19: *Input Status Mode - Normally Closed - Supervised Mode*

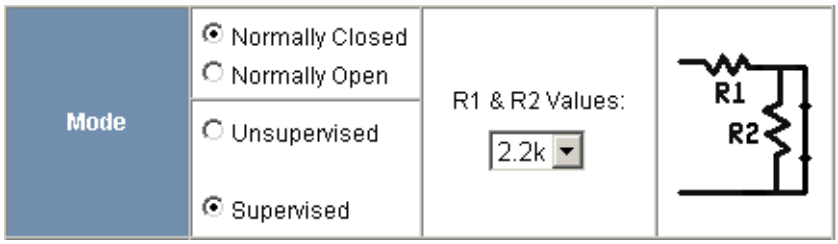
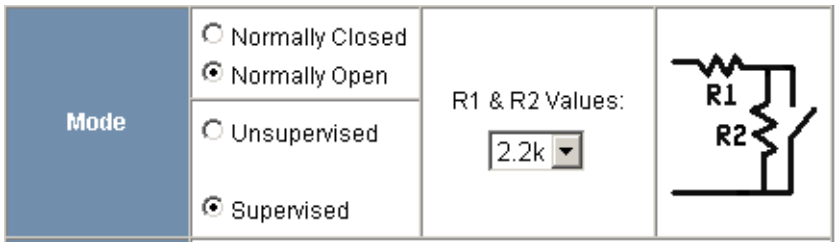


Figure 2-20: *Input Status Mode - Normally Open - Supervised Mode*



Steps: Use the descriptions in Table 2-9 to configure the Status, Egress, and Tamper inputs, then click **Submit Changes**:

Table 2-9: *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 2-9: *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.

2.5 Configuring Access Levels

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

The Access Levels screen enables you to:

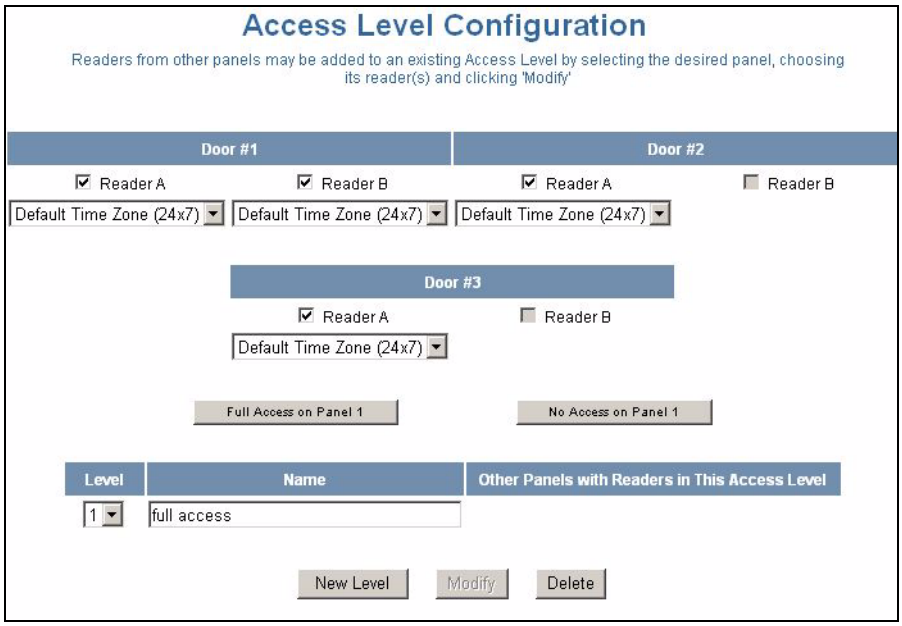
- Select Reader A and/or Reader B for each door. Note that if a reader is disabled, that reader's check box will also be disabled.
- Create an access level.
- Modify an access level.
- Delete an access level.
- Set a Time Zone for each door.
- View other panels with readers in this access level.

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 36) and the time zone (see Configuring Time Management, page 29) before configuring an access level.

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

Figure 2-21: *Access Levels > Add/Modify/Delete*



In this figure, Door 1 has Reader A and Reader B enabled. Reader 2 and Reader 3 only have Reader A enabled and Reader B is grayed out. Readers that are grayed out indicate to the user that they are deactivated.

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 **New 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.

2.6 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.

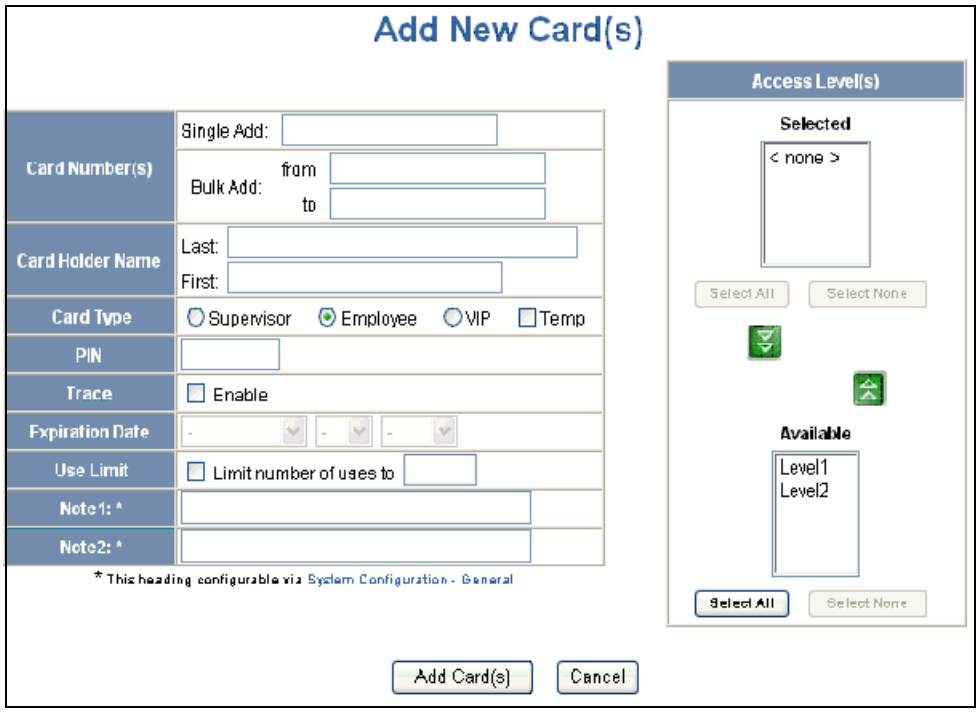
2.6.1 Adding New Cards

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 2-22: *Cards > Add*



Steps: Use the field descriptions in Table 2-10 to complete the card fields and click **Add Card(s)**:

Table 2-10: *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.
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 21). A card type is required.

Table 2-10: *Cards > Add Cards Fields*

Field	Description
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 36), 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 18 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 18 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.

2.6.2 Displaying and Modifying Cards

Use this function to display specified cards and modify them.

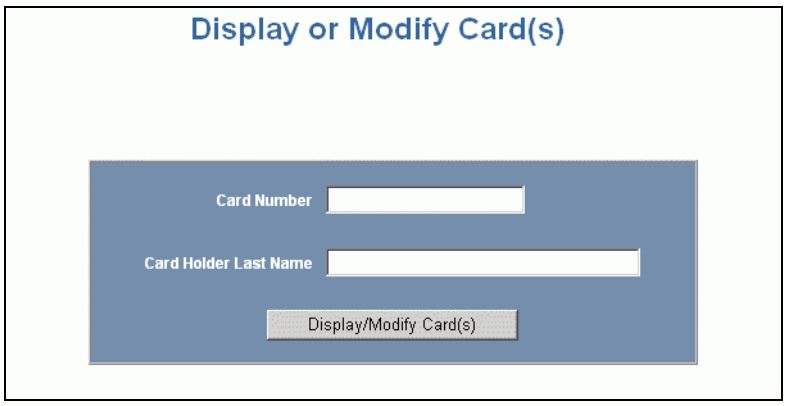
The Display or Modify Card(s) screen enables you to:

- 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 2-23: *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 2-10 on page 57 to complete the card fields and click **Submit Modification(s)**.

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

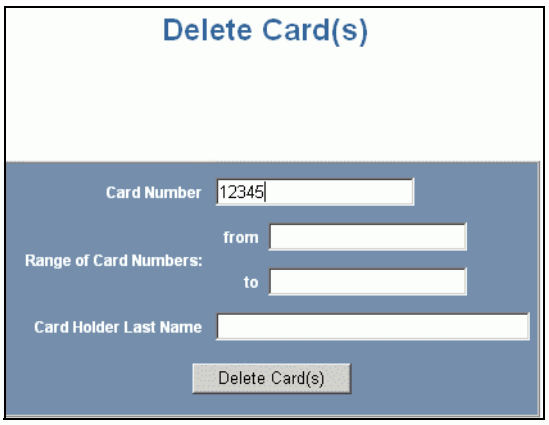
2.6.3 Deleting Cards

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 2-24: *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.

2.6.4 Displaying Reports

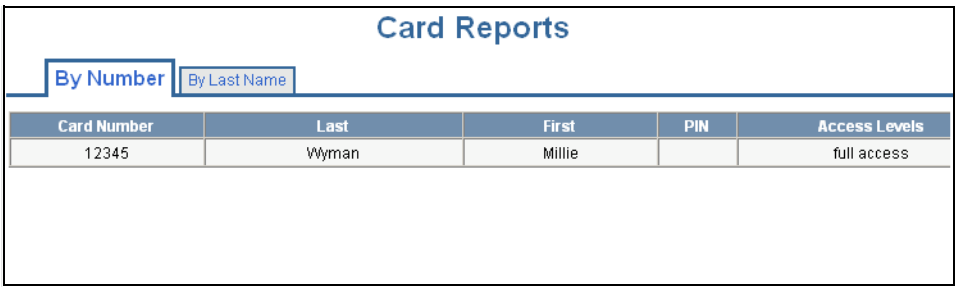
Use this function to display a report of all cards and card data. You can display the cards either by the card holder's last name or by the card number.

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 2-25: *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 2-25 shows only the leftmost side of the display. This screen is very wide, so use the scroll bar across the bottom to access the remaining columns on the right.

3. Use the descriptions in Table 2-11 to read the card records (see Adding New Cards, page 56 for more information about card data):

Table 2-11: *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 54 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.

2.7 Configuring Other I/O

This section explains how to configure “other” inputs and outputs on the NetAXS-123 panel. They are called “other” inputs and outputs because you can use them for things other than door lock/unlock functions. This section explains how to configure these other inputs and outputs.

2.7.1 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.

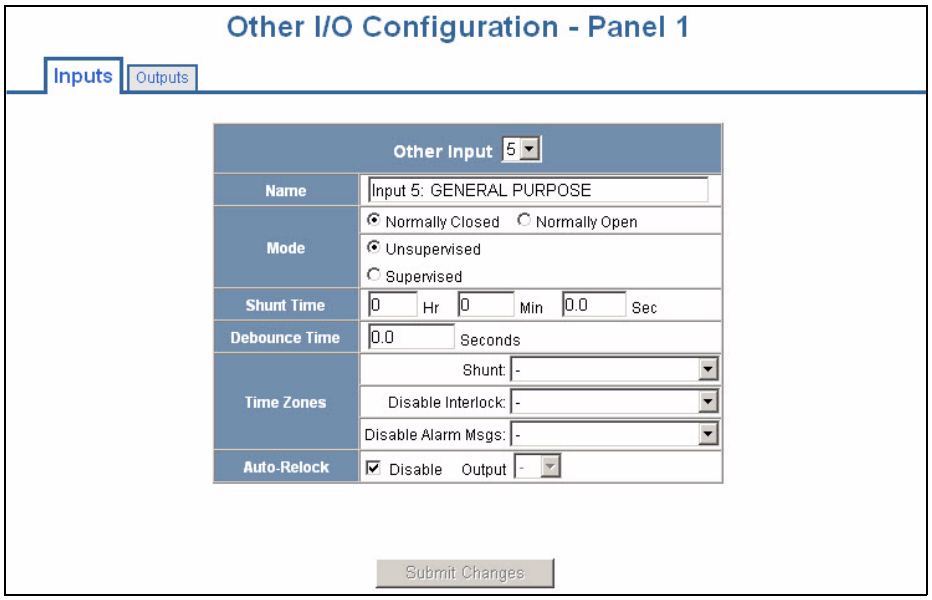
Note: You can also configure the Power Fail inputs for general use, if you choose not to wire them for power detection.

The Input tab enables you to:

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

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

Figure 2-26: *Configuration > Other I/O > Inputs Tab*



Steps: Use the descriptions in Table 2-12 to configure other panel inputs and downstream inputs.

Table 2-12: *Configuration > Other I/O > 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 shunted. **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 the input will generate no alarms.
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.

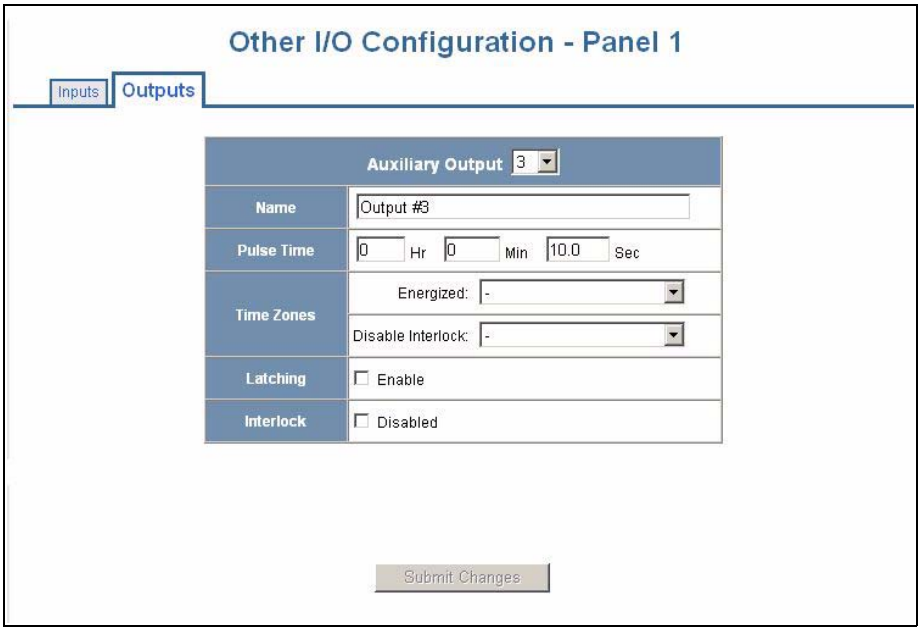
2.7.2 Outputs Tab

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

Figure 2-27: *Configuration > Other I/O > Outputs Tab*



Steps: Use the descriptions in Table 2-13 to configure each output device.

Table 2-13: *Configuration > Other I/O > 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 Configuring Interlocks

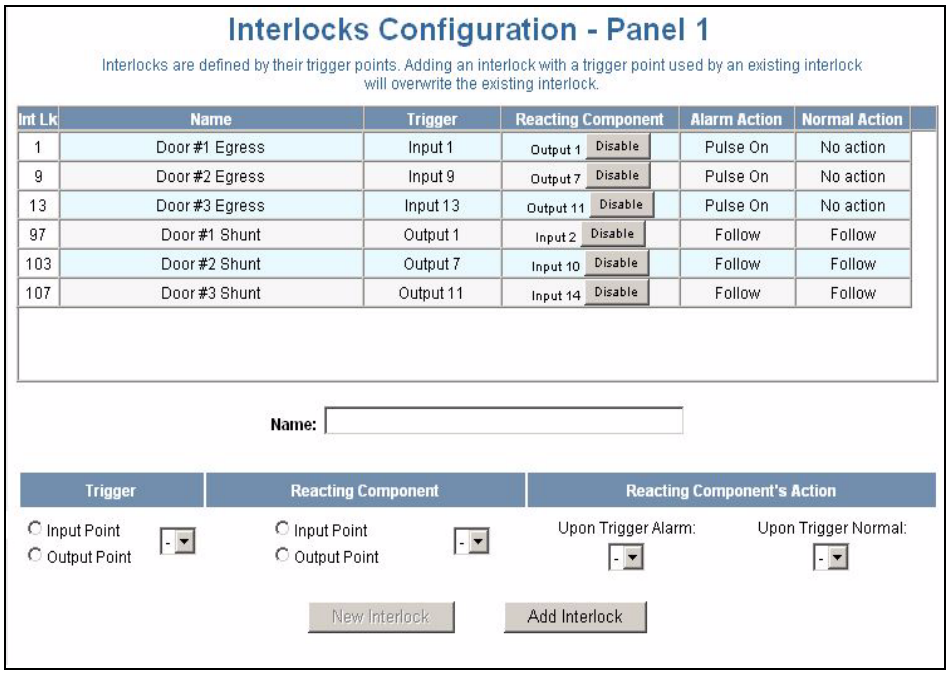
An interlock is a programmed connection between two points. The interlock causes an input point, output point, or group of output points to act in a specified manner when another input point, output point, or group of output points changes its state. An action on the trigger point causes a reaction on 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 2-28: *Configuration > Interlocks*



To create an interlock:

1. Click **New Interlock** to display the screen.
2. Use the descriptions in Table 2-14 to configure the interlock:

Table 2-14: *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 1-20 will have an interlock link (Int Lnk) number from 1-20. If Trigger = Outputs, then outputs 1-14 will have an interlock link (Int Lnk) number from 97-110. Use the drop-down list to specify the number of the input or output.
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, 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.

2.9 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.

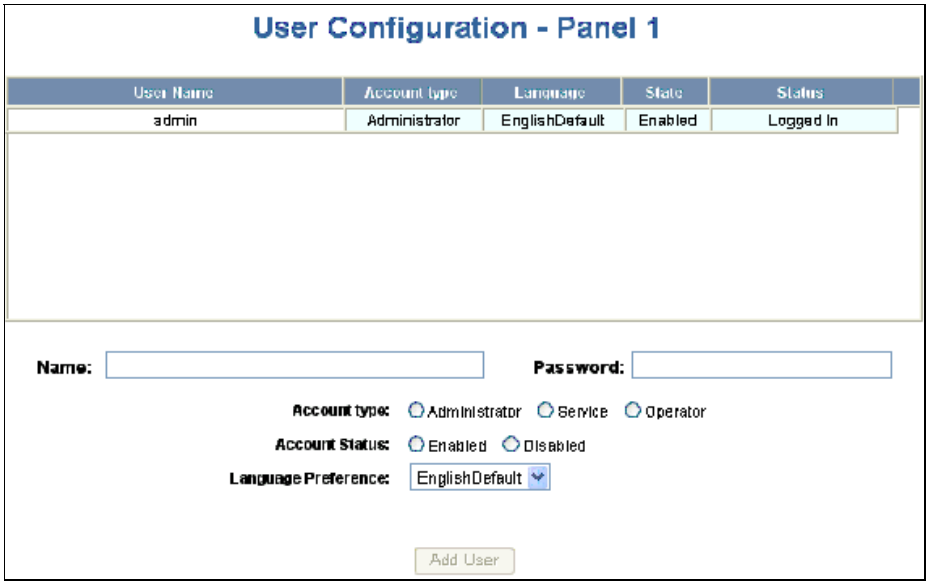
Table 2-15 lists the functions that each user type can perform.

Table 2-15: *User Functions*

Function	Operator	Service	Administrator
View alarms/events	X	X	X
Acknowledge alarms	X	X	X
View panel I/O status	X	X	X
Control I/O points	X	X	X
Generate reports	X	X	X
View card database	X	X	X
Create, modify, delete cards		X	X
View all configurations		X	X
Create, modify, delete configurations			X
Perform uploads/downloads			X
Manage own user account	X	X	X
Manage all user accounts			X

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

Figure 2-29: *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.

Using WIN-PAK with NetAXS-123 3

In this chapter...

3.1 Overview

The NetAXS-123 is a modular 1-, 2-, or 3-Door System. It may be configured and managed from WIN-PAK Host Software. However, WIN-PAK does not currently provide native support for the NetAXS-123 controller, so a controller type of N-1000-IV-X is the recommended panel type for WIN-PAK. The following sections describe the factory default settings for NetAXS-123, and the recommended configuration steps in WIN-PAK.

3.2 Configuration Guidelines

3.2.1 NetAXS-123 Panel Default Settings

The following table lists the factory controller board I/O default settings for Door #1. These are the mappings for Readers, inputs and outputs on the controller board. Reader A and Reader B share many common connections as noted in Table 3-1.

Table 3-1: *Controller Board I/O Defaults for Door #1*

Purpose	Type	Reader A	Reader B[a]	Other
Egress	Input	Input 1	Input 1	
Door Status	Input	Input 2	Input 2	
Reader Tamper	Input	Input 3	Input 4	
General	Input			Input 5
Power/General	Input			Input 6
Panel Tamper	Input			Input 20
Lock Relay	Output	Output 1	Output 1	
Reader LED	Output	Output 2	Output 2	
Aux Relay	Output			Output 3
Reader Buzzer	Output	Output 4	Output 4	

a. Reader B is not available in WIN-PAK.

Notes:

The Controller Board includes Inputs 7 and 8 but they are reserved for system use.

The Controller Board also includes Output 5 and Output 6, which are reserved by the system to control the boards' RUN LEDs and thus are unavailable for user control.

Reader LED, while it is an output, should never be used to control anything other than its associated reader's LED.

Table 3-2 lists the factory I/O board default settings for Door #2. These mappings should be used for the readers, inputs, and outputs when either a 1- or 2-door I/O board is attached to the board-to-board connector on the controller board.

Table 3-2: *Factory Default Configuration Settings for Door 2*

Type	Purpose	Logical Number		Other
		Reader A	Reader B[a]	
Input	Egress	9	9	
	Status	10	10	
	Reader Tamper	11	12	
Output	Lock Relay	7	7	
	Reader LED	8	8	
	Aux Relay			9[b]
	Reader Buzzer	10[b]	10[b]	

a. Reader B is not available in WIN-PAK.
b. This output may not be controlled from WIN-PAK. However, you may configure custom commands to control it.

Table 3-3 lists the factory I/O board default settings for Door #3. These mappings should be used for the readers, inputs, and outputs when a 2-door I/O board is attached to the board-to-board connector on the controller board.

Table 3-3: *Factory Default Configuration Settings for Door 3*

Type	Purpose	Logical Number		Other
		Reader A	Reader B[a]	
Input	Egress	13	13	
	Status	14	14	
	Reader Tamper	15	16	
Output	Lock Relay	11	11	
	Reader LED	12	12	
	Aux Relay			13
	Reader Buzzer	14	14	

a. Reader B is not available in WIN-PAK.

Note: Reader LEDs, while they are outputs, should never be used to control anything other than their associated reader LEDs.

3.3 Supported Configurations

Table 3-4 lists the web server configurations supported by the NetAXS-123.

Table 3-4: *NetAXS-123/NS4 Interoperability Using a Web Server*

Gateway	Downstream	Web Server Support	Notes
NetAXS-123	NS4-R3 (4-Door)	Y	
NetAXS-123	NS4-R3 (2-Door)	N	NS4-R3 (2 Door) Panel may not be configured as downstream panel in any circumstance.
NetAXS-123	NetAXS-123	Y	
NS4-R3 (2- or 4-Door)	NetAXS-123	N	The NS4-R3 may be used as a PCI by WIN-PAK, but the Web Server will not support configuration of NetAXS-123™ Panels. The NetAXS-123™ will reject any Binary Commands requested from an NS4-R3.
NetAXS-123	Mixed loop of NetAXS-123 & NS4-R3	Y	
PCI2/PCI3	Mixed loop of NetAXS-123 & NS4-R3 & N-1000 & NS2	N	

Table 3-5 lists the WIN-PAK configurations supported by the NetAXS-123.

Table 3-5: *NetAXS-123/NS4 Interoperability using WIN-PAK*

Gateway	Downstream	WIN-PAK Support	Notes
NetAXS-123	NS4-R3 (4-Door)	Y	
NetAXS-123	NS4-R3 (2-Door)	N	NS4-R3 (2 Door) Panel may not be configured as downstream panel in any circumstance.
NetAXS-123	NetAXS-123	Y	
NS4-R3 (2- or 4-Door)	NetAXS-123	Y	The NS4-R3 may be used as a PCI by WIN-PAK, but the Web Server will not support configuration of NetAXS-123™ Panels. The NetAXS-123™ will reject any Binary Commands requested from an NS4-R3.
NetAXS-123	Mixed loop of NetAXS-123 & NS4-R3	Y	
PCI2/PCI3	Mixed loop of NetAXS-123 & NS4-R3 & N-1000 & NS2	Y	

Additional notes with respect to WIN-PAK compatibility:

- WIN-PAK will not be aware of NetAXS-123 specific controller type at NetAXS-123 release.
- WIN-PAK configuration of NetAXS-123 3-door system will be supported as an N-1000-4/PW-2000-4X, but reader 4 will be inoperative.
- WIN-PAK configuration of NetAXS-123 2-door will be supported as an N-1000-4/PW-2000-4X, but readers 3 and 4 will be inoperative.
- WIN-PAK configuration of NetAXS-123 1-door controller will be supported as an N-1000-4/PW-2000-4X, but readers 2, 3, 4 will be inoperative.
- WIN-PAK factory defaults will not work with the NetAXS-123. I/O and interlock assignments must be made for WIN-PAK to work with an NetAXS-123, as described in earlier sections.

- WIN-PAK configuration does not support two readers per door. Reader B is unusable. The NetAXS-123 controller and I/O board allow two readers (sharing a hold line) to control a single door. However, the current version of WIN-PAK does not support the 2 readers per door using hold lines.
- WIN-PAK direct Ethernet to NetAXS-123 is supported; serial Host and Dial-Up Connections are not available on the NetAXS-123.

3.4 Setting up WIN-PAK

3.4.1 Summary of WIN-PAK I/O Settings for NetAXS-123

The NetAXS-123 controller and I/O board allow two readers (sharing a hold line) to control a single door. However, the current version of WIN-PAK does not provide for this 2-door Reader control using hold lines. WIN-PAK will only support readers using Reader A for doors 1-3. Reader B is not recognized by WIN-PAK but inputs (4, 12, and 16) may be used as general purpose inputs.

Table 3-6: *NetAXS-123 to WIN-PAK Mapping*

I/O Name	Type	Reader 1	Reader 2	Reader 3
Egress	Input	Input 1	Input 9	Input 13
Status	Input	Input 2	Input 10	Input 14
Reader Tamper	Input	Input 3	Input 11	Input 15
Lock Relay	Output	Output 1	Output 7	Output 11
Reader LED	Output	Output 2	Output 8	Output 12

Table 3-7: *NetAXS-123 Panel Interlock Configuration*

Reader 1			
Type	Point to Point	On Action	Off Action
Egress	Input 1 to Output 1	Pulse	No Action
Door	Output 1 to Input 2	Follow	No Action
Reader 2			
Type	Point to Point	On Action	Off Action
Egress	Input 9 to Output 7	Pulse	No Action
Door	Output 7 to Input 10	Follow	No Action
Reader 3			
Type	Point to Point	On Action	Off Action
Egress	Input 13 to Output 11	Pulse	No Action
Door	Output 11 to Input 14	Follow	No Action

3.4.2 General Setup

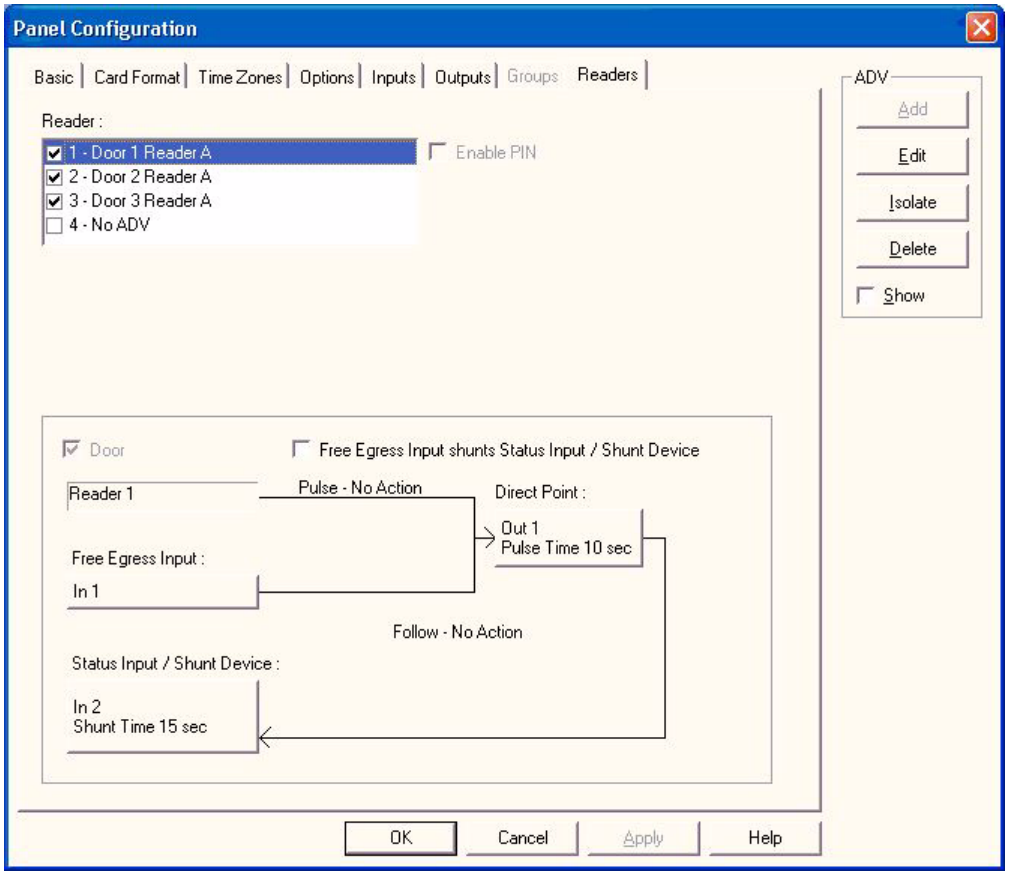
To set up WIN-PAK to control a NetAXS-123 panel, first configure Loop and Panel objects. See Configuring the System, page 18 for detailed procedures. Once you have performed these steps, you may configure the NetAXS-123 Doors as described below.

3.5 WIN-PAK Screen Shots for Door 1

The following screen shots illustrate setting up Reader, Egress Input, Status Input, Lock Output and LED Output for Door 1.

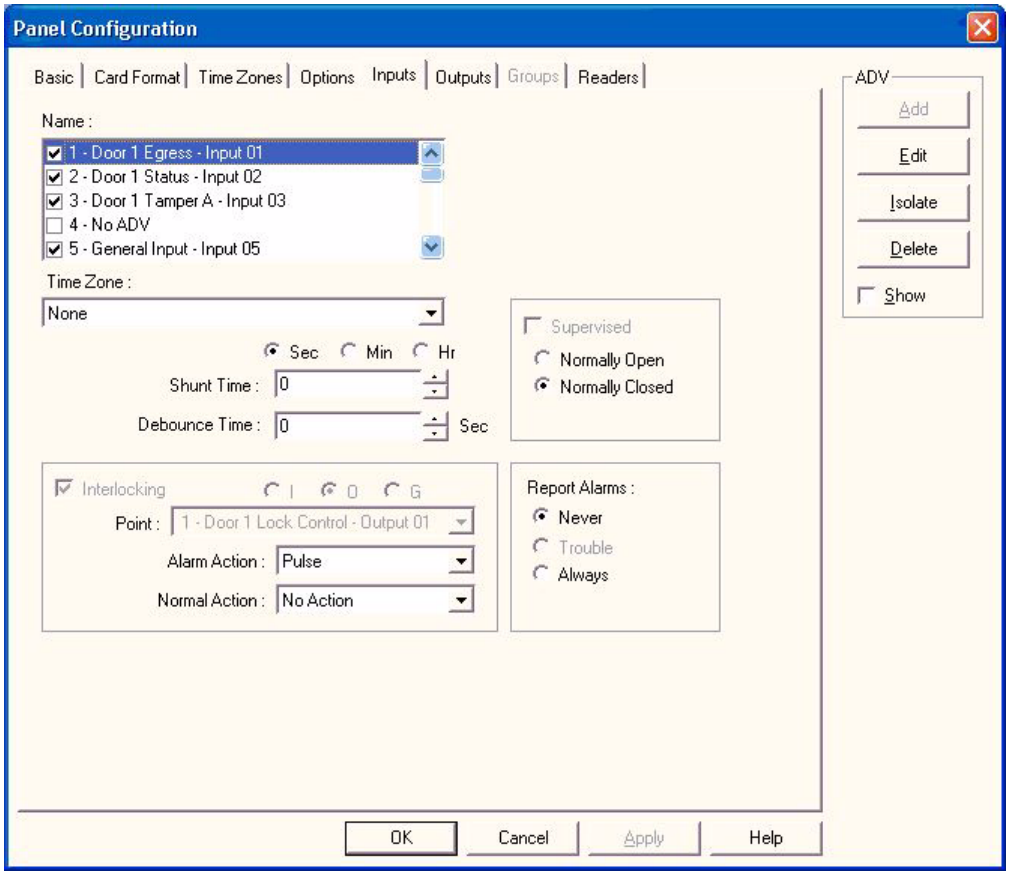
Click the Readers tab to configure the reader setup parameters.

Figure 3-1: *Reader Setup for Door 1*



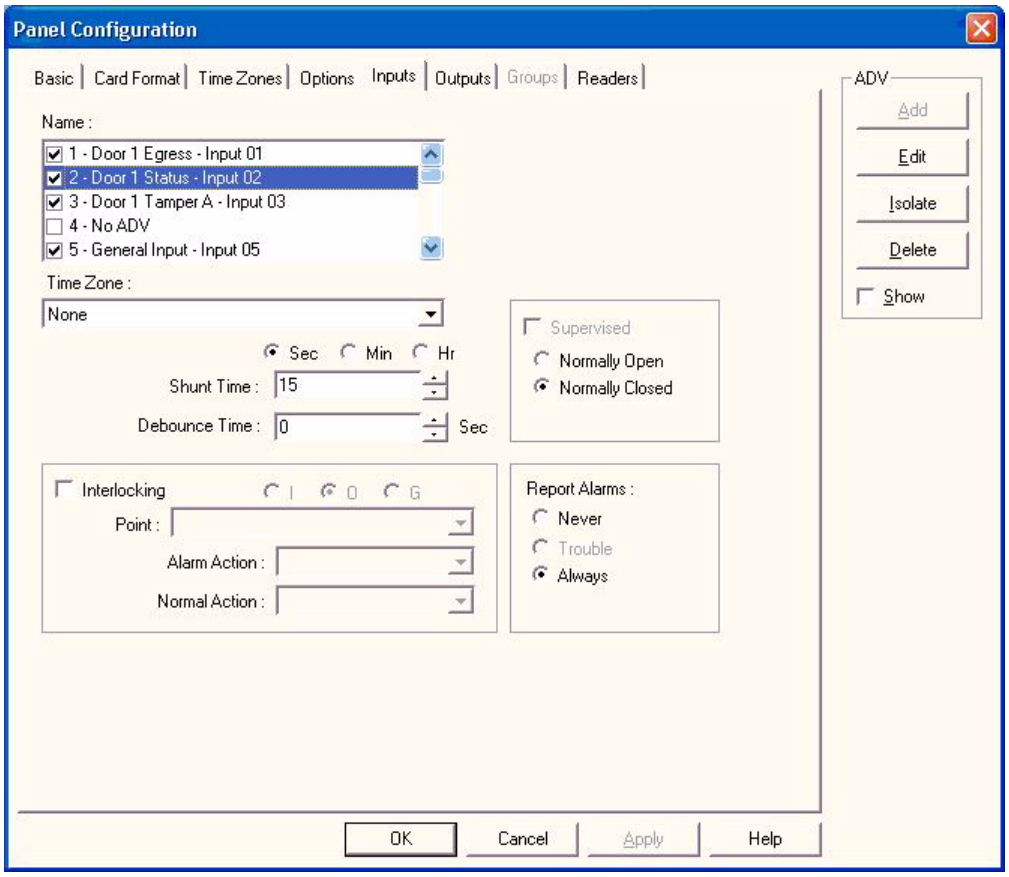
Click the Inputs tab to configure the Egress parameters.

Figure 3-2: *Egress Setup for Door 1*



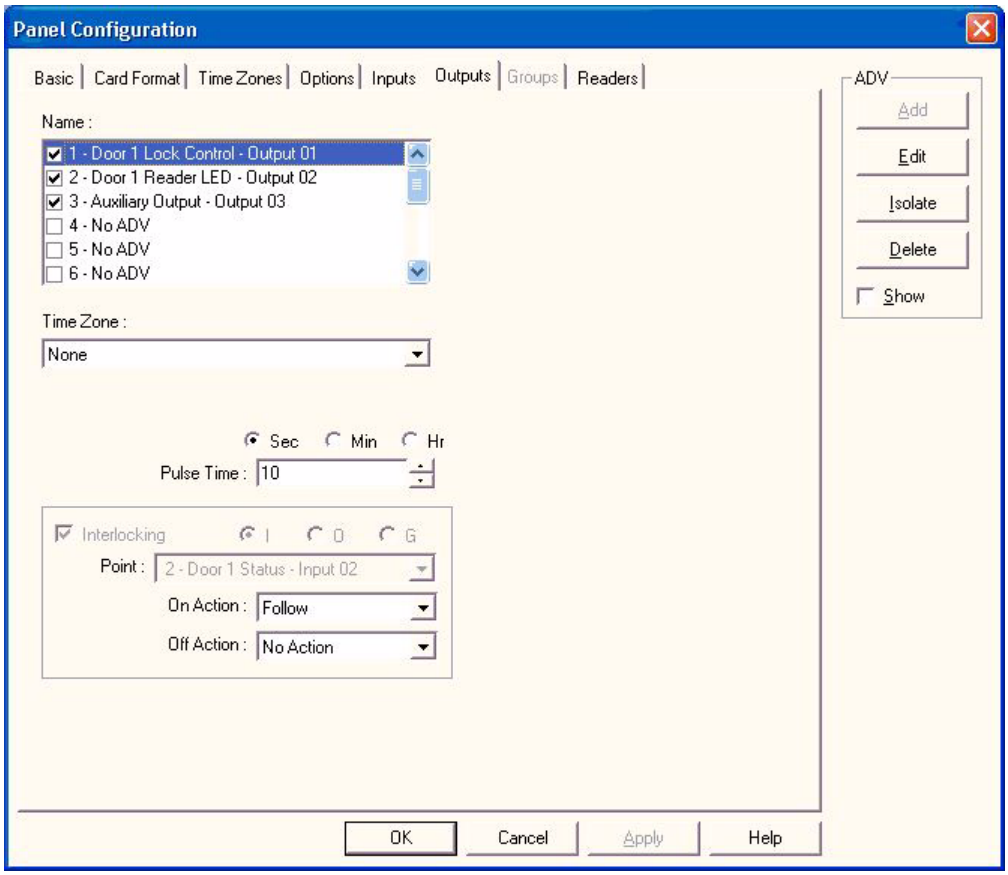
Click the Inputs tab to configure the status setup parameters.

Figure 3-3: *Status Setup for Door 1*



Click the Outputs tab to configure the lock setup parameters.

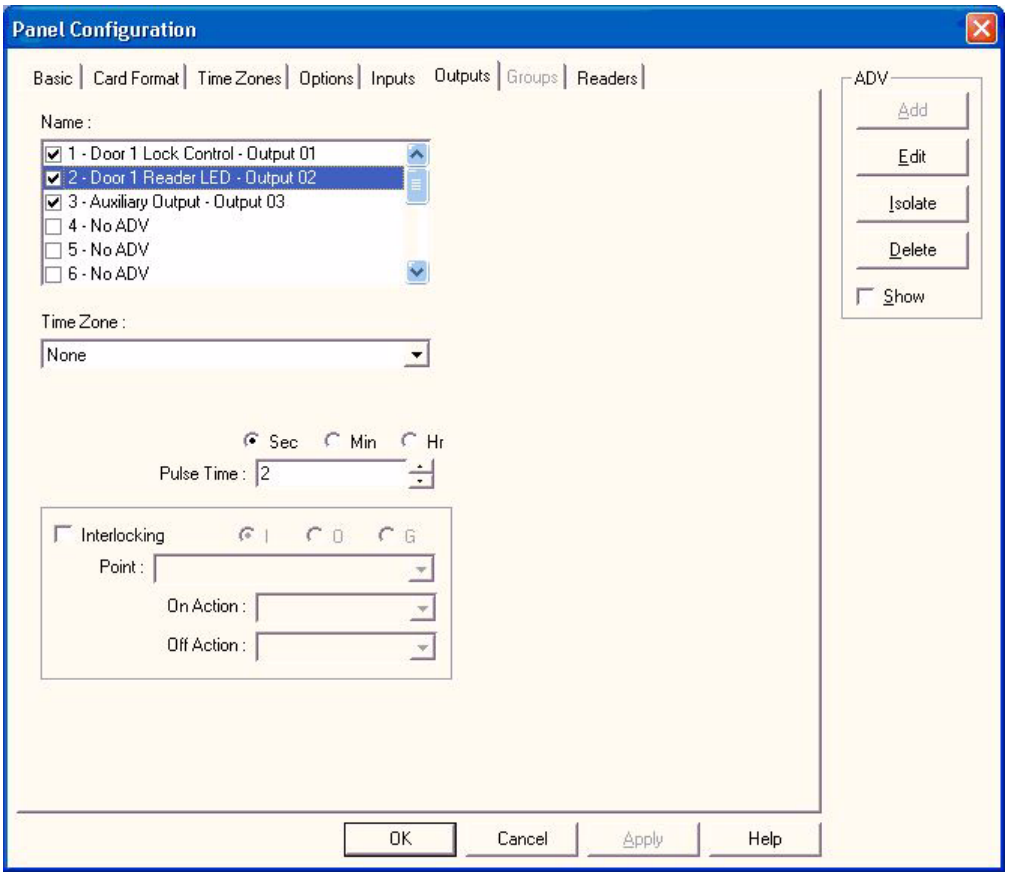
Figure 3-4: *Lock Setup for Door 1*



Note: Outputs 5 and 6 are system outputs. WIN-PAK cannot control these outputs and you cannot customize them.

Click the Outputs tab to configure the Reader LED setup parameters.

Figure 3-5: *Reader LED Setup for Door 1*



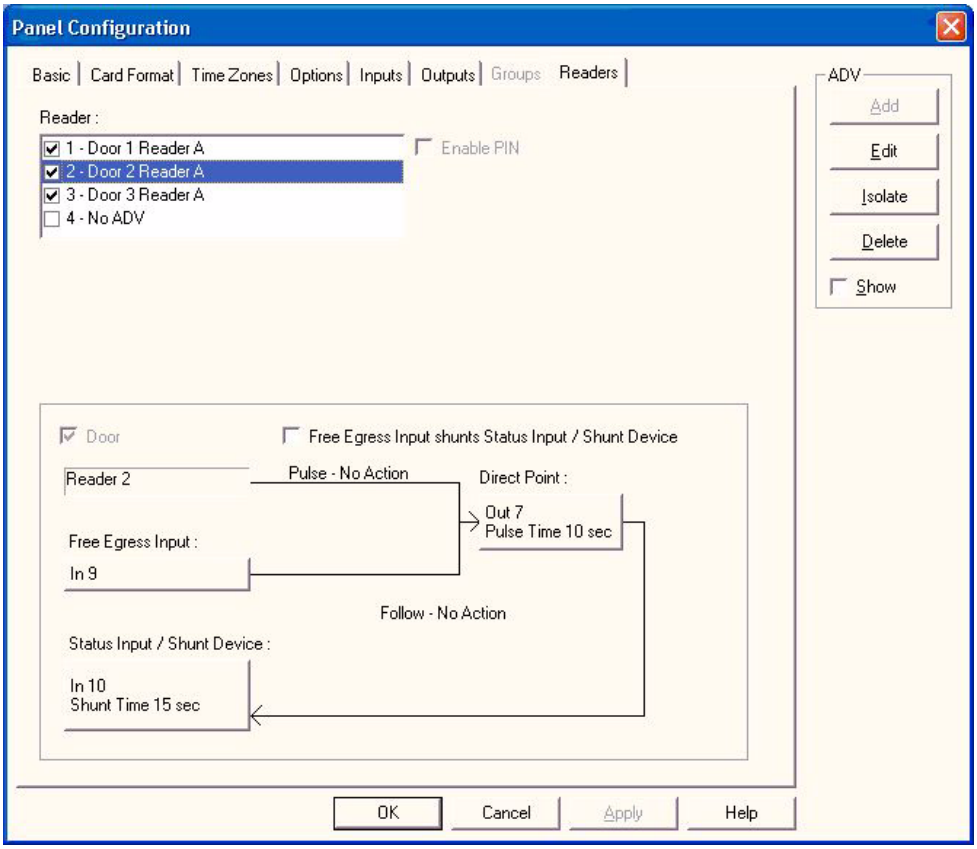
Note: Outputs 5 and 6 are system outputs. WIN-PAK cannot control these outputs and you cannot customize them.

3.6 WIN-PAK Screen Shots for Door 2

The following screen shots illustrate setting up Reader, Egress Input, Status Input, LED Output and Lock Output for Door 2.

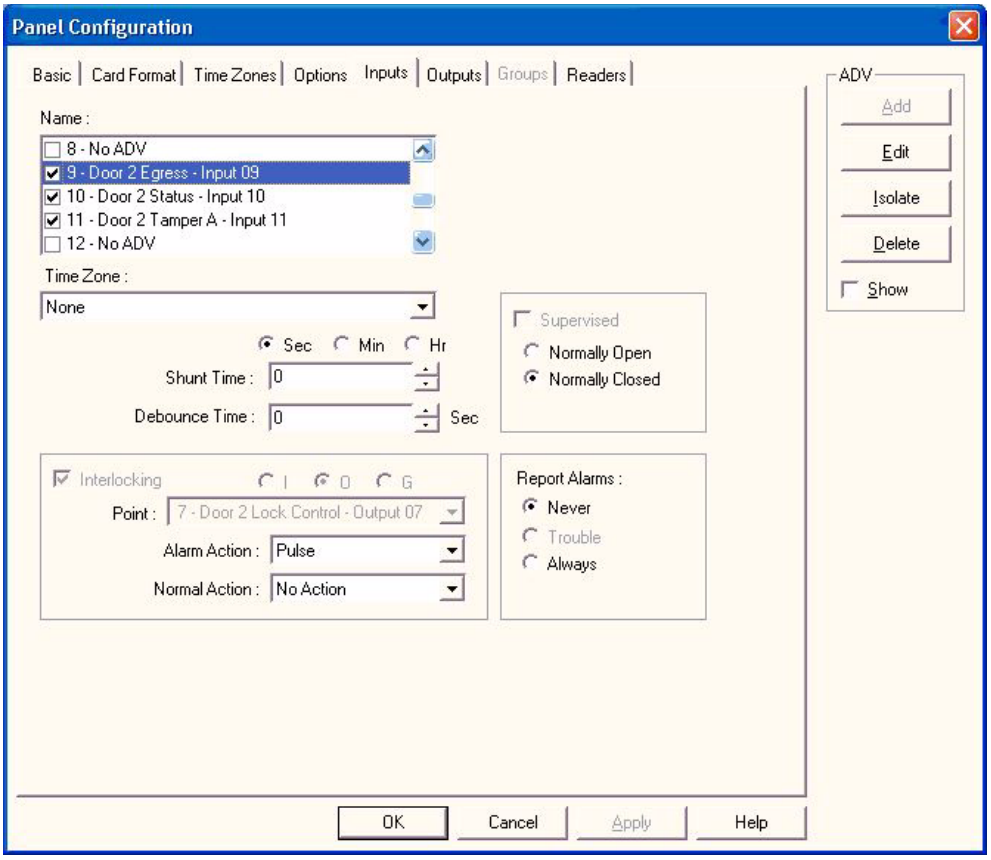
Click the Readers tab to configure the reader setup parameters.

Figure 3-6: *Reader Setup for Door 2*



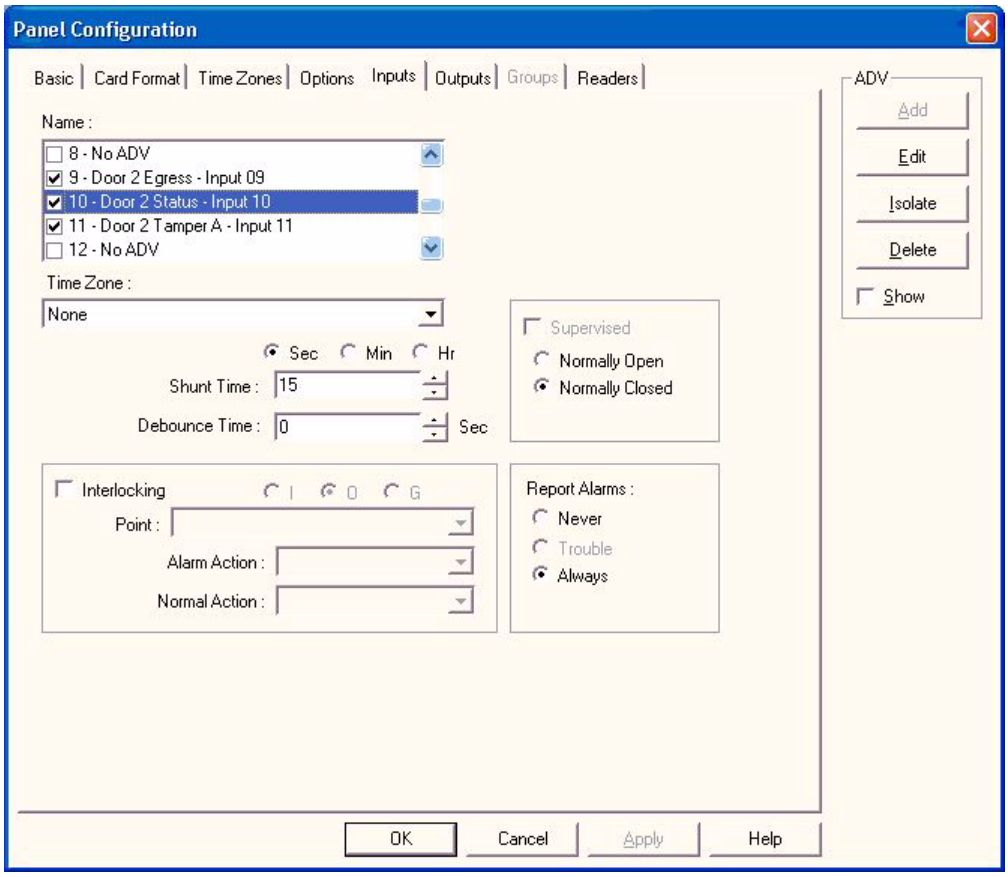
Click the Inputs tab to configure the egress setup parameters.

Figure 3-7: *Egress Setup for Door 2*



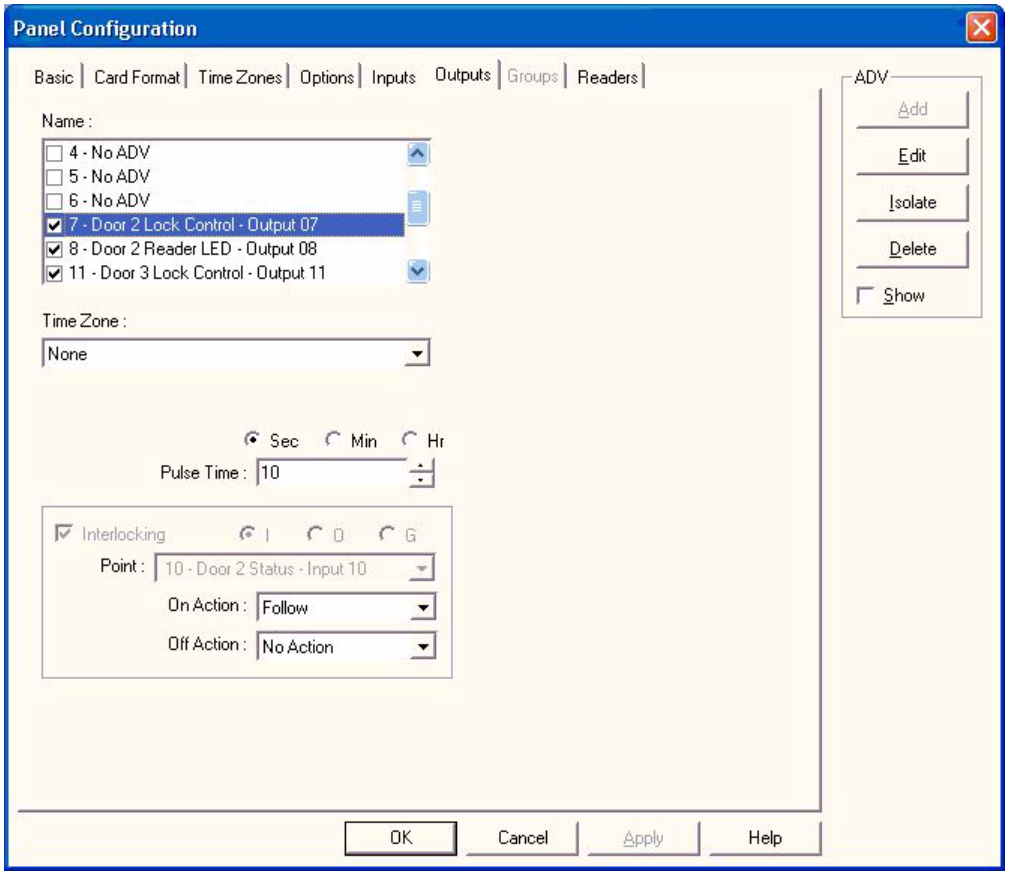
Click the Inputs tab to configure the status setup parameters.

Figure 3-8: *Status Setup for Door 2*



Click the Outputs tab to configure the lock setup parameters.

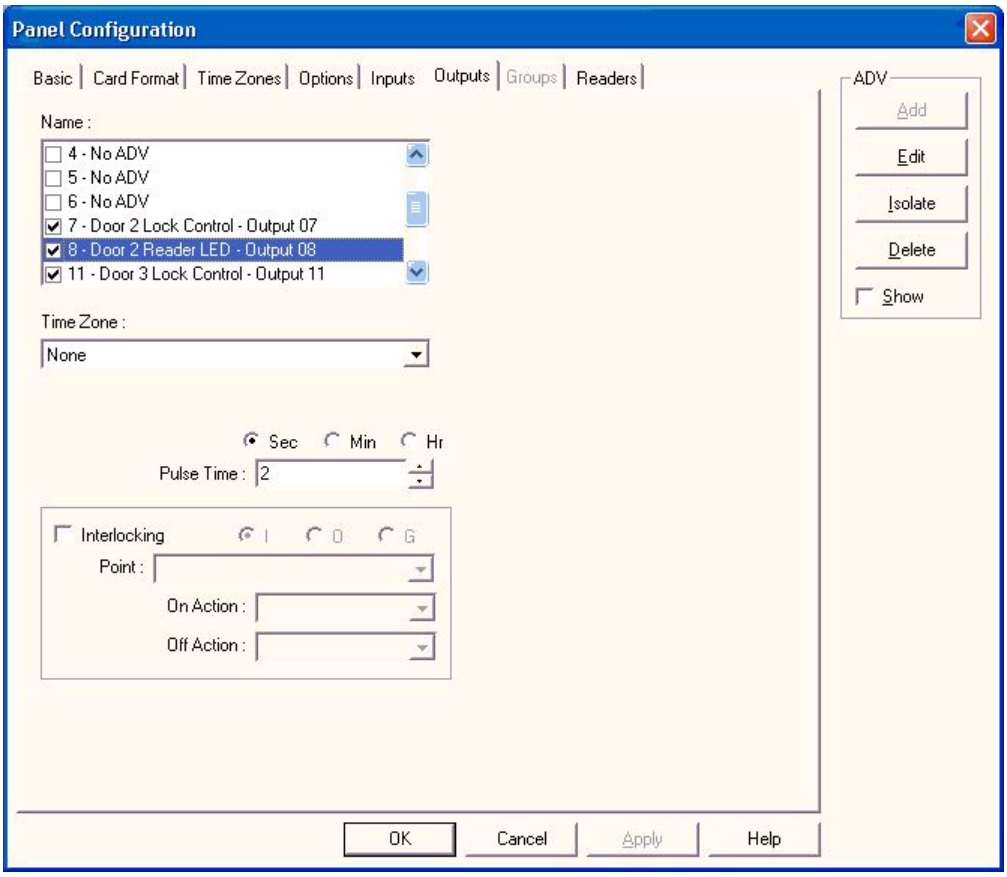
Figure 3-9: *Lock Setup for Door 2*



Note: Outputs 5 and 6 are system outputs. WIN-PAK cannot control these outputs and you cannot customize them.

Click the Outputs tab to configure the Reader LED setup parameters.

Figure 3-10: *Reader LED Setup for Door 2*



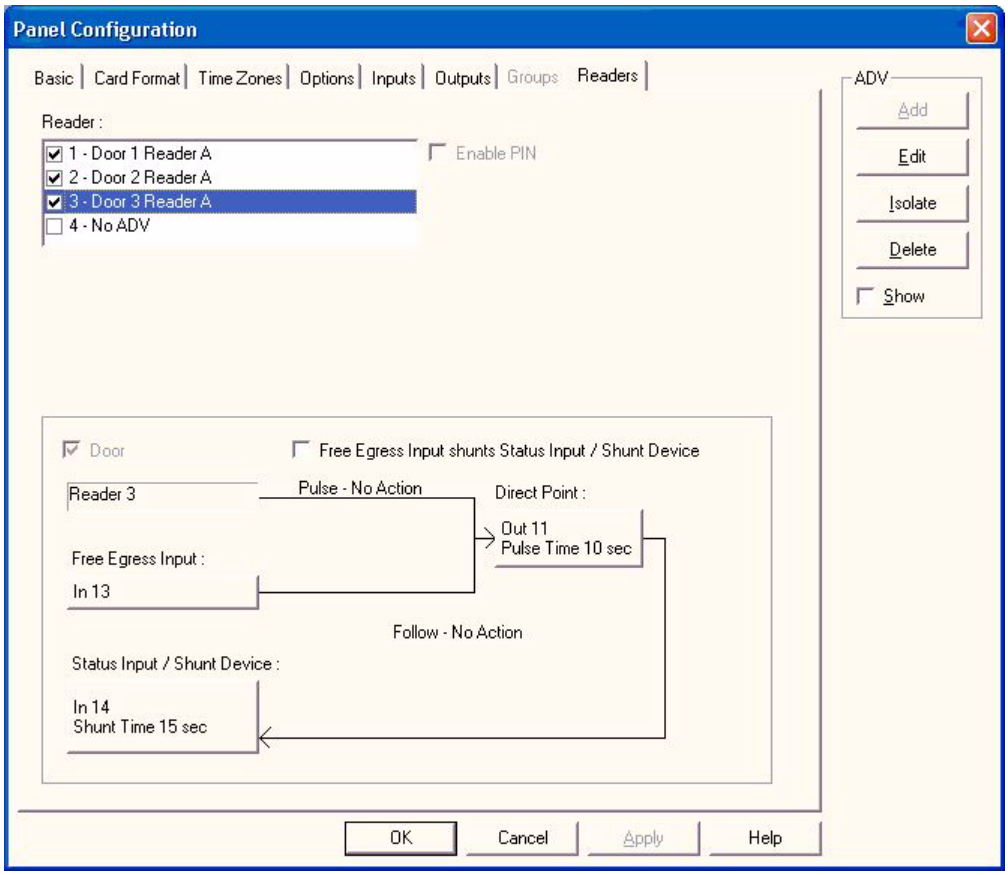
Note: Outputs 5 and 6 are system outputs. WIN-PAK cannot control these outputs and you cannot customize them.

3.7 WIN-PAK Screen Shots for Door 3

The following screen shots illustrate setting up Reader, Egress Input, Status Input, LED Output and Lock Output for Door 3.

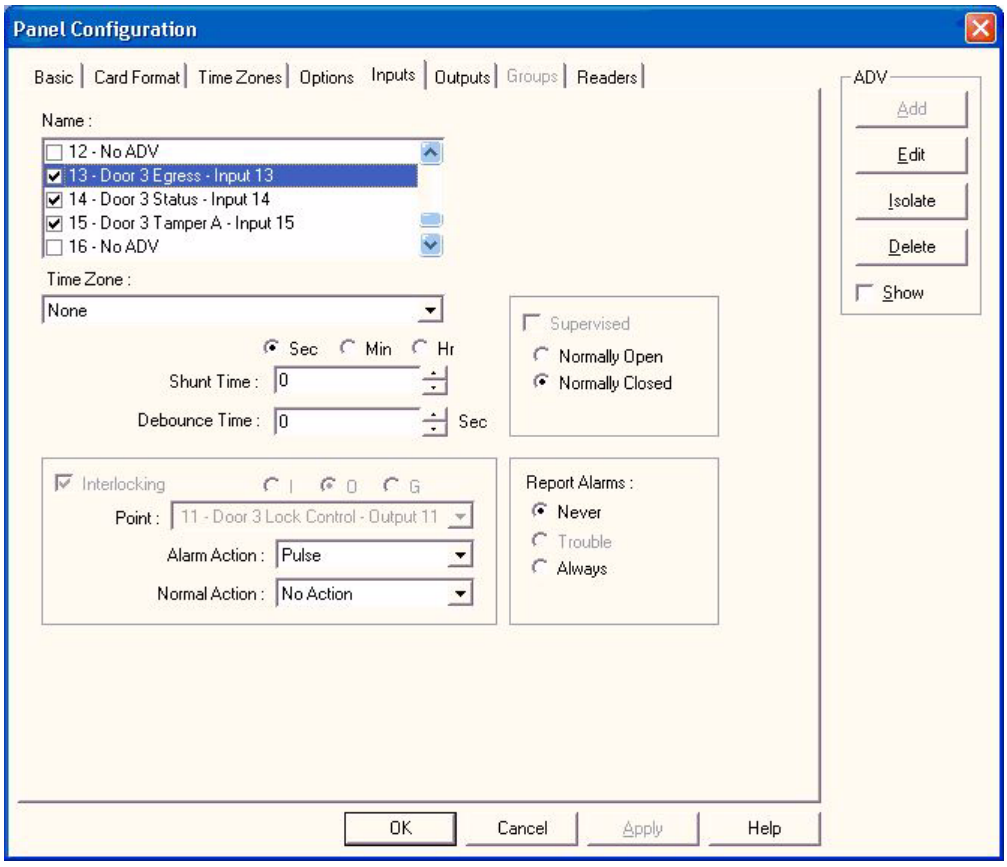
Click the Readers tab to configure the reader setup parameters.

Figure 3-11: *Reader Setup for Door 3*



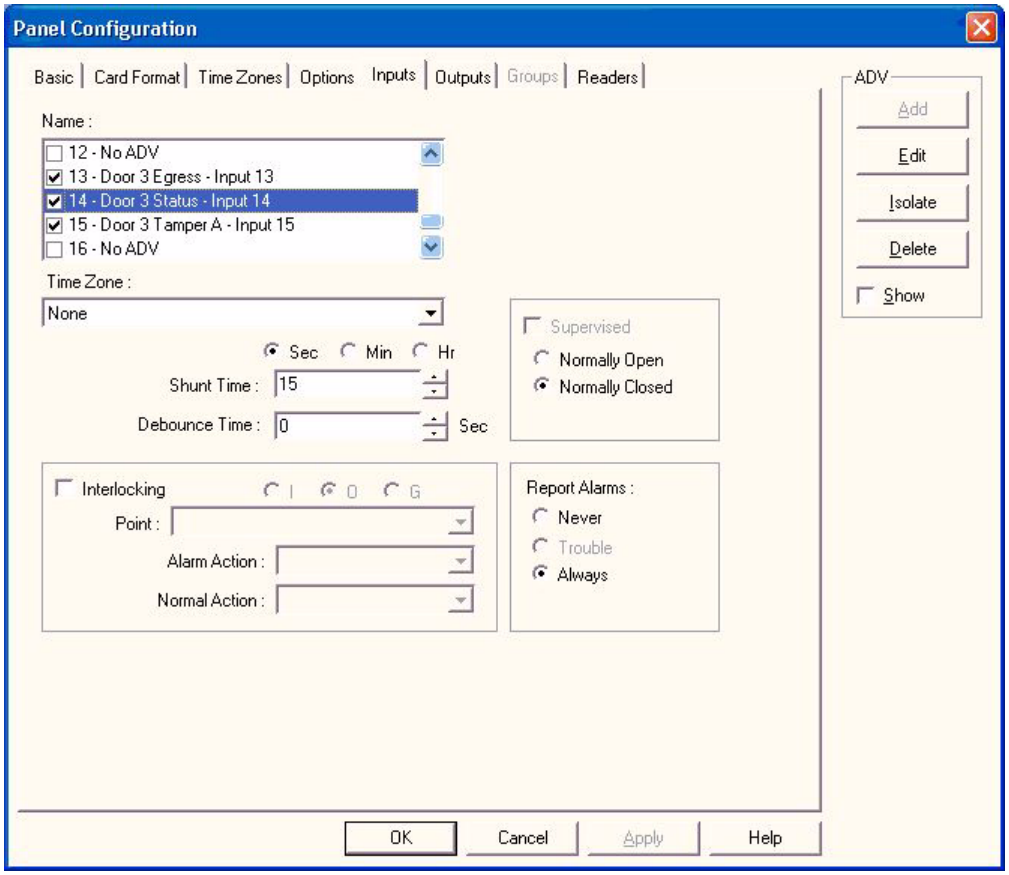
Click the Inputs tab to configure the egress setup parameters.

Figure 3-12: *Egress Setup for Door 3*



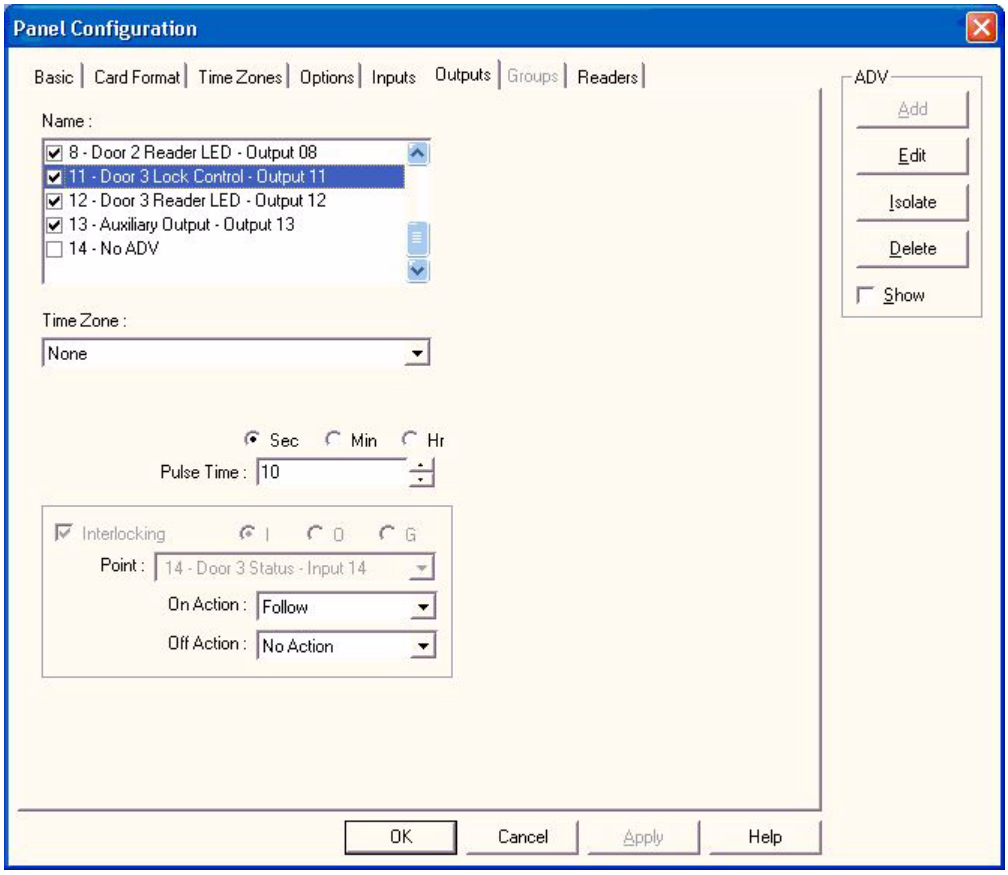
Click the Inputs tab to configure the status setup parameters.

Figure 3-13: *Status Setup for Door 3*



Click the Outputs tab to configure the lock setup parameters.

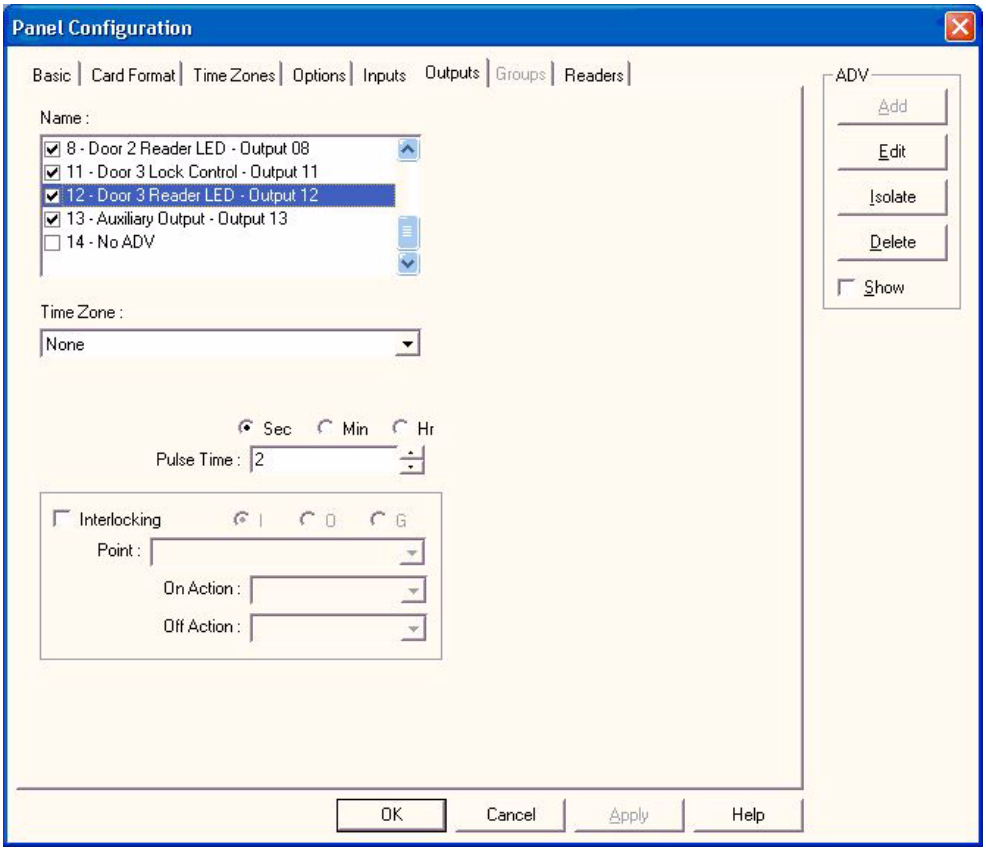
Figure 3-14: *Lock Setup for Door 3*



Note: Outputs 5 and 6 are system outputs. WIN-PAK cannot control these outputs and you cannot customize them.

Click the Outputs tab to configure the Reader LED setup parameters.

Figure 3-15: *Reader LED Setup for Door 3*



Note: Outputs 5 and 6 are system outputs. WIN-PAK cannot control these outputs and you cannot customize them.

3.8 Standalone Commands

Note: Standalone commands are not supported in web mode. They are only available for use when you configure your NetAXS-123 system using WIN-PAK's command files. These standalone commands can also be applied from a "terminal mode" method of programming.

Caution: Use the following commands, in the order they are listed, to configure the NetAXS-123 panel:

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

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

3.8.1 T (Time) Command

_T=pn_hh:mm<CR>

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

Example #1:

_T=1_08:30<CR>

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

Example #2:

_T=6_18:15<CR>

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

3.8.2 D (Date) Command

_D=pn_mm/dd/yyyy_day<CR>

Variables:

pn = panel number (1-31)
mm = month number (1-12)
dd = day number (1-31)
yyyy = year number (ex 2007, 1999, etc.)
date = day of week (1-7):
1 = Monday
2 = Tuesday
3 = Wednesday
4 = Thursday
5 = Friday
6 = Saturday
7 = Sunday

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

Example #1:

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

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

Example #2:

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

This command would set panel 25 to a date of 12/14/2009 and to Sunday as the day of the week.

3.8.3 L (Time Zone) Command

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

Variables:

pn = panel number (1-31)
tz = time zone number (1-63 (127))
h1 = start time zone: hours (00-23) (Military time)
m1 = start time zone: minutes (00-59)
h2 = end time zone: hours (00-23) (Military time)
m2 = end time zone: minutes (00-59)
days = days of week, valid values as listed below:
1 = Monday
2 = Tuesday
3 = Wednesday
4 = Thursday
5 = Friday
6 = Saturday
7 = Sunday
0 = Holiday 1
8 = Holiday 2
9 = Holiday 3

Notes:

WIN-PAK only supports 0-63 natively, with 1-63 being definable.

The earliest time possible is 00:00; the latest time possible is 23:59. A single time zone cannot be made to span midnight; this can be simulated through extended commands. For more information, contact Technical Support.

Holiday 2 and Holiday 3 are not supported by current WIN-PAK.

Example #1:

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

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

Example #2:

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

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

3.8.4 C (Card Add) Command

_C=pn_code_time zone_dev<CR>

Variables:

pn = panel number (1-31)
code = card number (range depends on card format)
time zone = time zone number the card will follow (1-255)
dev = device numbers card will work with, as follows:
1 = card reader #1
2 = card reader #2
3 = card reader #3

Example #1:

_C=6_12345_10_1_2_3<CR>

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

Example #2:

_C=18_52989_120_1_3<CR>

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

3.8.5 C (Card Delete) Command

_C=pn_code<CR>

Variables:

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

Example #1:

_C=6_12345<CR>

This command would remove card 12345 from panel 6.

Example #2:

_C=18_52989<CR>

This command would remove card 52989 from panel 18.

3.8.6 W (Input) Command

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

Variables:

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

Example:

_W=1_9_SO<CR>

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

3.8.7 P (Interlock) Command

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

Parameters:

number: for an input number, the range is 1-16; for output, 1-14
D: De-energize
E: Energize
F: Follow
N: No action
P: Pulse

Example:

_P=1_I_5_O_3_E_D<CR>

When Input 5 is triggered, Output 3 energizes.

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

3.8.8 H (Holiday) Command

Function:

Set holiday dates.

_H=pn_sn_mm/dd[_type]

Type = 0, 8, 9:

0 = Holiday 1

8 = Holiday 2

9 = Holiday 3

Note: No type is automatically selected as Holiday 1.

Example:

_H=0_1_12/25

December 25 is set as a type 1 holiday in all panels.

Deleting Holidays:

To delete an existing holiday database entry, enter the H command for the desired holiday number WITHOUT the month (mm) and day (dd) parameters.

Example:

_H=0_1

Holiday 1 is removed from all panels.

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.
- 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.

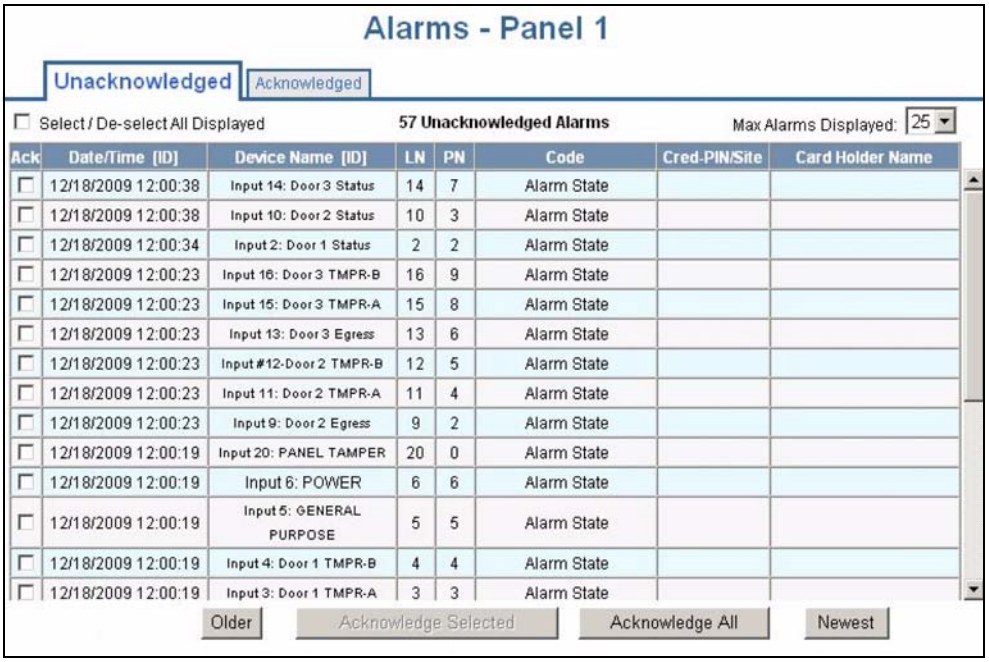
4.2 Monitoring Alarms

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

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

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

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



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*

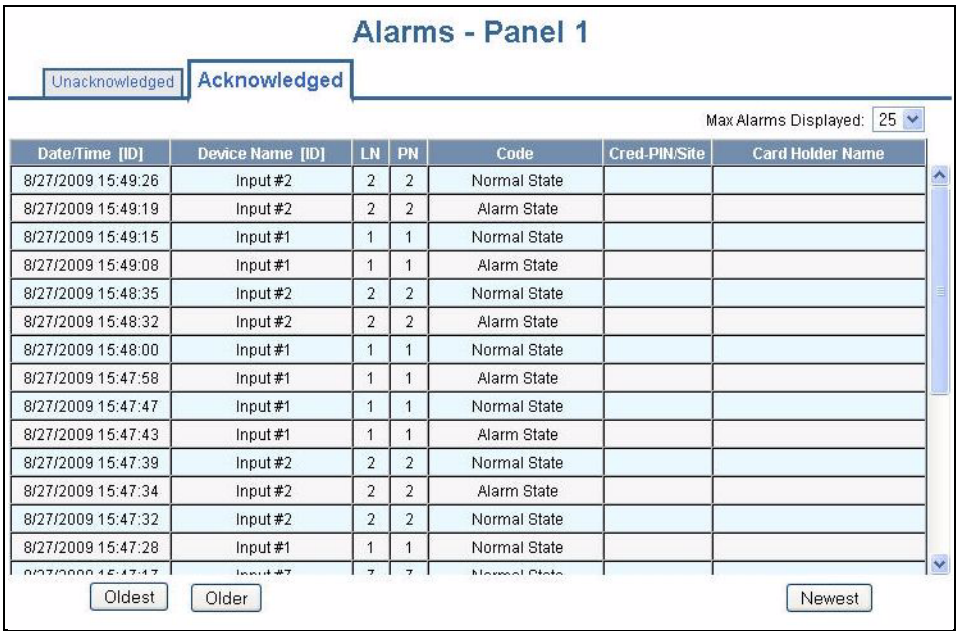


Table 4-1 describes the information displayed on both the Unacknowledged alarms tab and Acknowledged alarms tab:

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

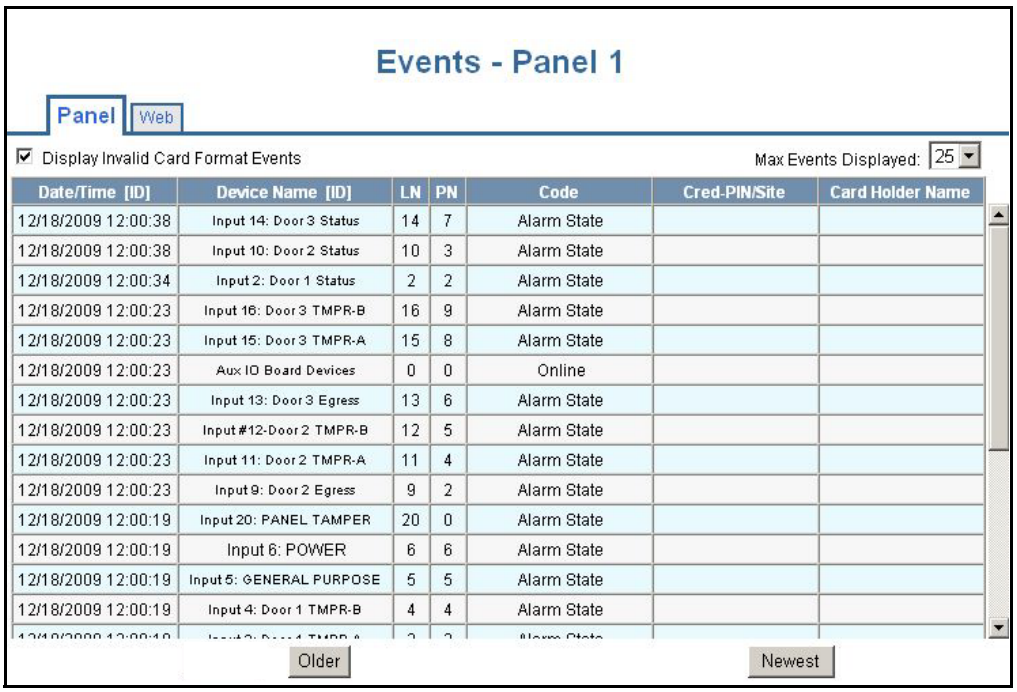
Note: The values listed in this table are based on defaults. For information on other values, contact Technical Support.

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*



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*

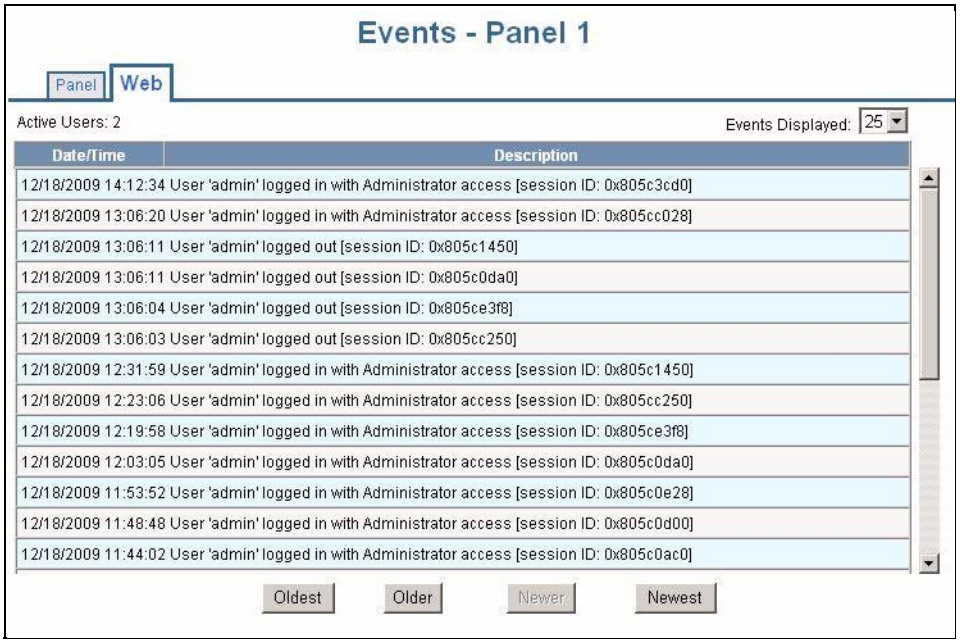
Column Head	Description
Date/Time [ID]	Provides the date and exact time the event was generated, according to the panel's time.
Device Name [ID]	Identifies the device that generated the event.
LN	**Logical device number** – A unique number starting at 1 that is assigned to an alarm generating point. 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 Inputs

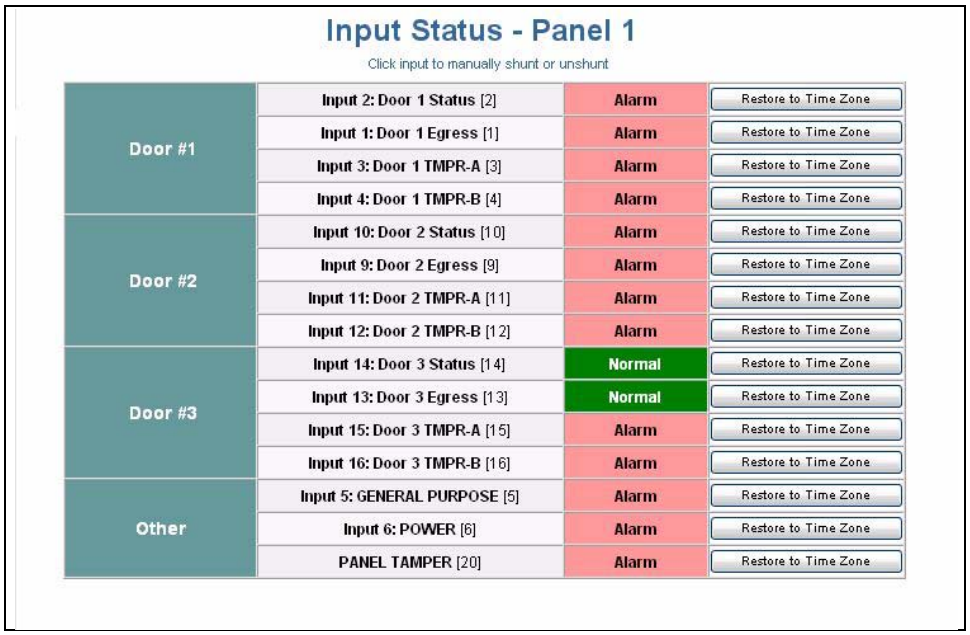
The panel supports door, panel, and auxiliary inputs. The door inputs provide egress, status, and tamper monitoring. The panel inputs provide power fail and tamper status. The auxiliary inputs support any monitoring devices connected.

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 29).

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

Figure 4-5: *Monitoring > 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 4-6: *Toggle Shunt State Dialog Box*

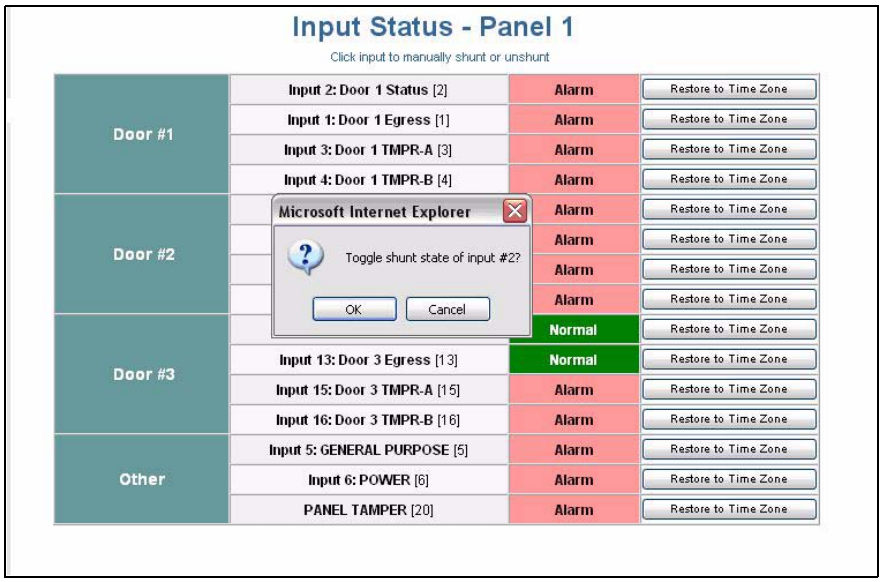
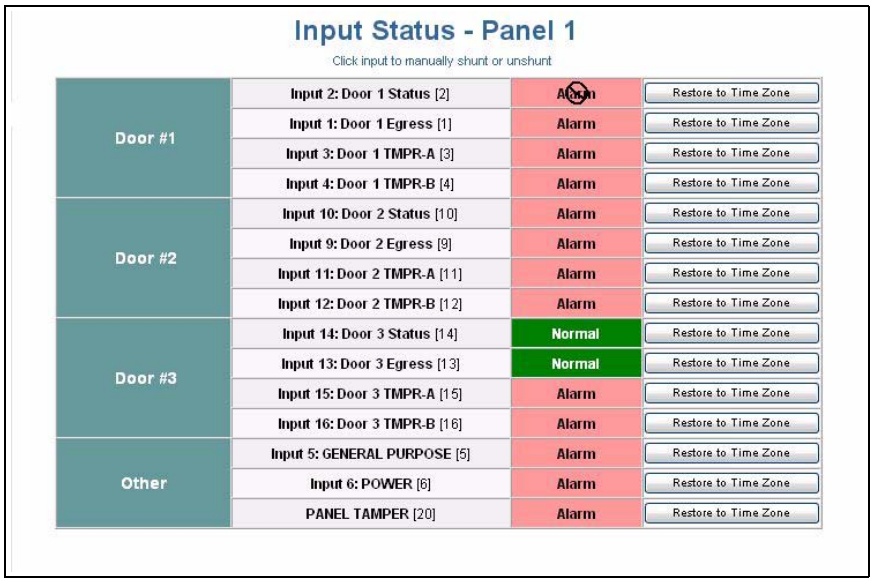


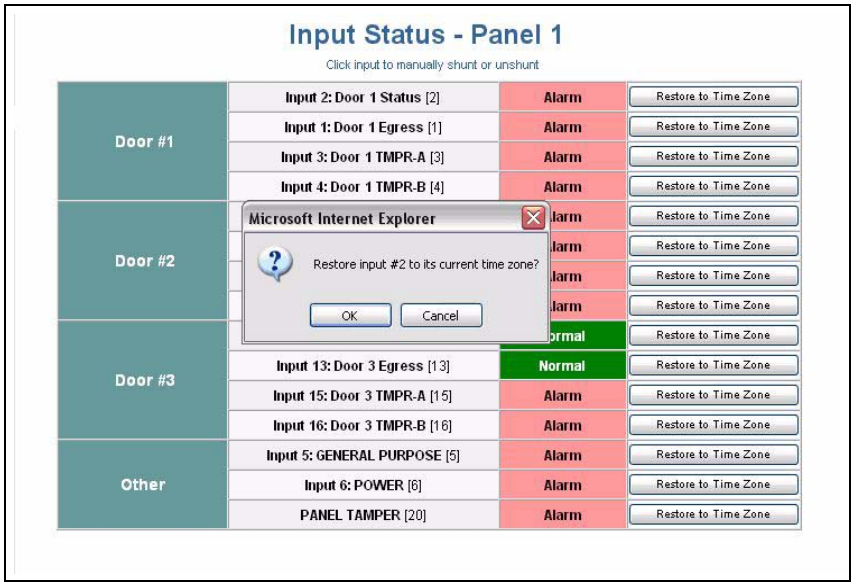
Figure 4-7 displays an example of a shunted input status.

Figure 4-7: *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 4-8: *Time Zone Restore Dialog Box*



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

4.5 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 48 and Outputs Tab, page 66) or collectively as a group of outputs.

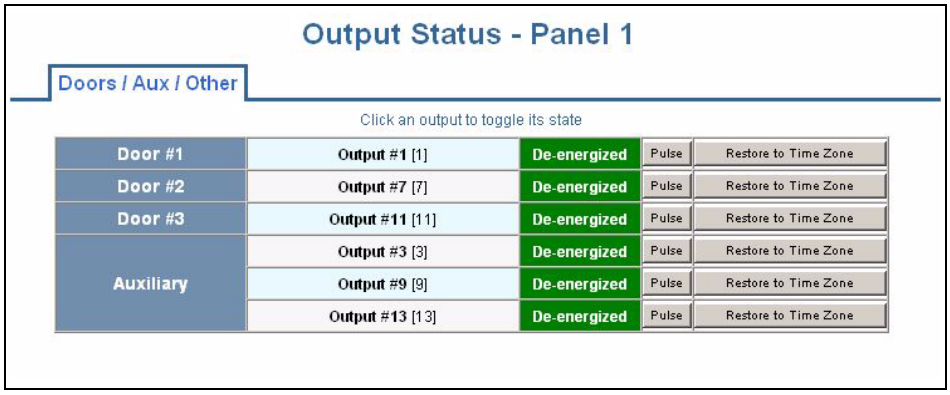
Note: The Pulse and Restore to Time Zone buttons will only function when an output or a group has a valid pulse time or a time zone assigned.

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 48).
- 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 29).

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

Figure 4-9: *Monitoring > Outputs > Doors/Aux/Other 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.

4.6 Monitoring System Status

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

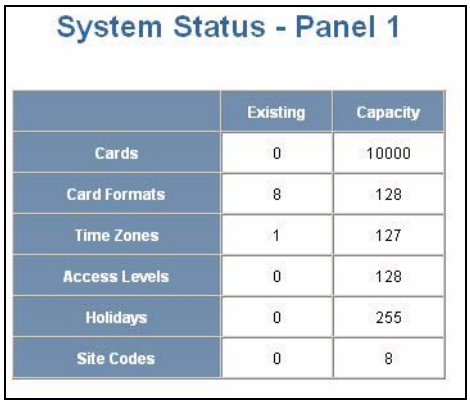
The System Status screen enables you to:

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 4-10: *Status > System*



File Management

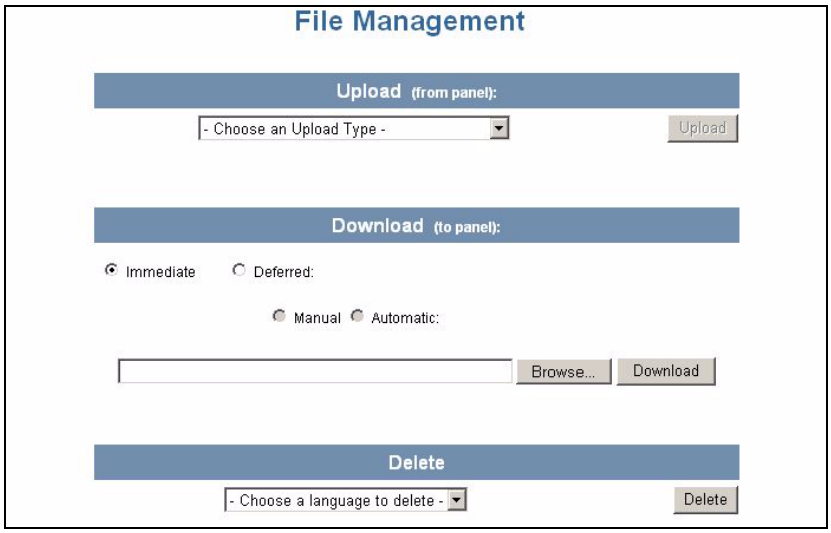
5

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.

- Alarms and events report—uploads the Date, Time, Event Type, Acknowledged Date, Acknowledged Time, and Message of Alarms/Events for alarms and events in a .CSV file.
- Language: English default, Spanish, French, Italian, Dutch, Czech, and simplified Chinese. 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.

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.

To restore (or download) firmware immediately:

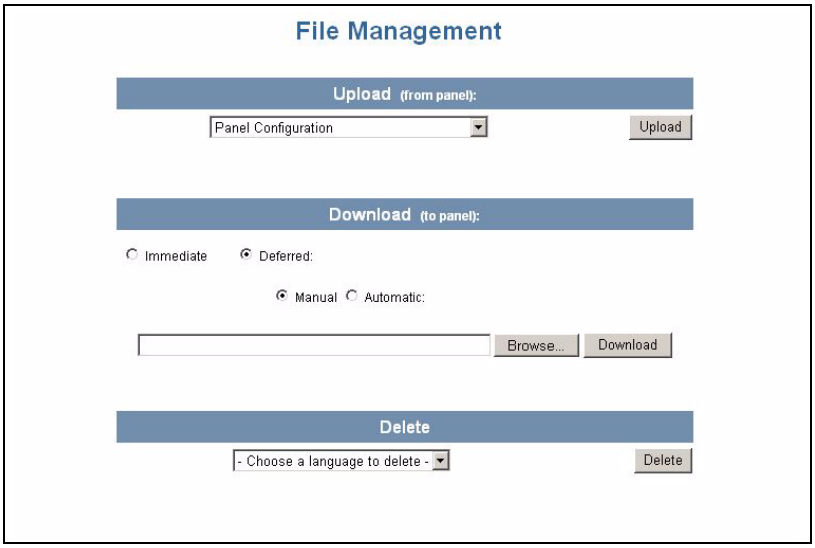
1. Click **Browse** to locate the firmware file.
2. Click **Immediate**.
3. Click **Download**.

   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 Time Setting*

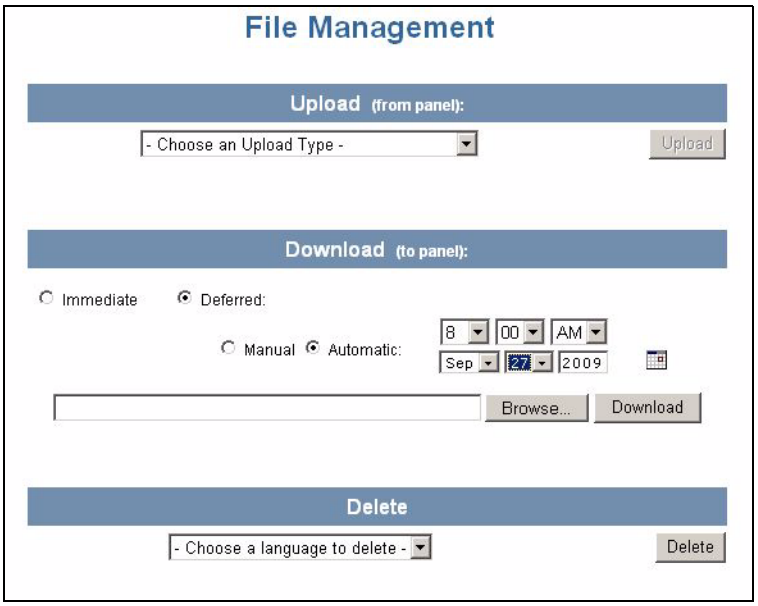


4. Click **Download**; the download status is shown as "Ready for activation".
5. Click **Ready for Activation** when you are ready to download your files.

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 Time 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 129.

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

1. Click **Browse** to locate the .CSV file.
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.

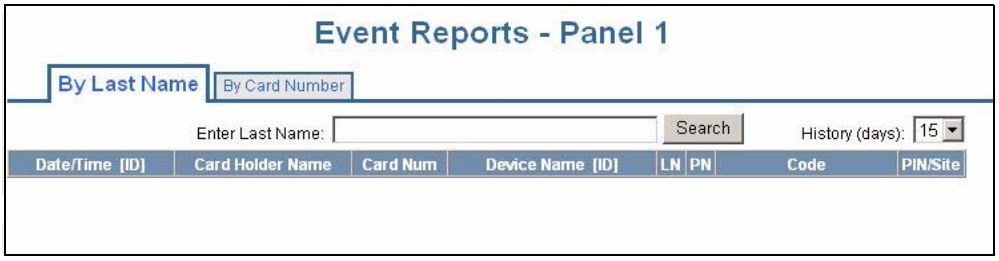
5.2 Generating Reports

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.

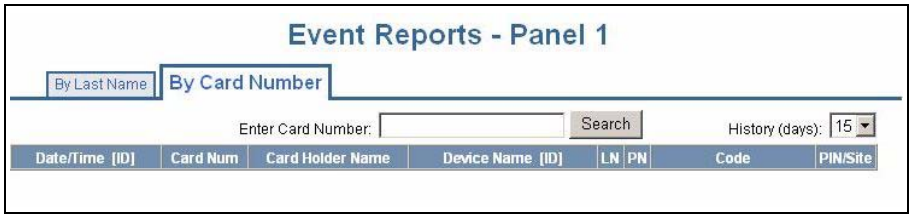
Table 5-1: *Status > Report Fields*

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...

Note: Make sure to back up the panel database prior to upgrading the panel firmware. See Backing up and Restoring the NetAXS-123, page 120 for instructions.

A.1 Planning the Upgrade

Because upgrading a loop takes some time, you will want to plan the upgrade to minimize its impact on the access control of your building. You should allow for approximately 20 minutes to upgrade one gateway panel, and 25 minutes for one downstream panel (switched to gateway mode). Depending upon your configuration, you may be able save time by starting multiple panel upgrades on your loop simultaneously.

With respect to the timing of the upgrade, you may:

- download data to a selected panel immediately
- download data to all panels later--for activation either manually or automatically
- cancel an automatically deferred download
- cancel a deferred download altogether

These options are described in Uploading Data from the Panel, page 131.

Note: Make sure to back up the panel database prior to upgrading the panel firmware. See Backing up and Restoring the NetAXS-123, page 120 for instructions.

A.2 Mixed Revision Loops

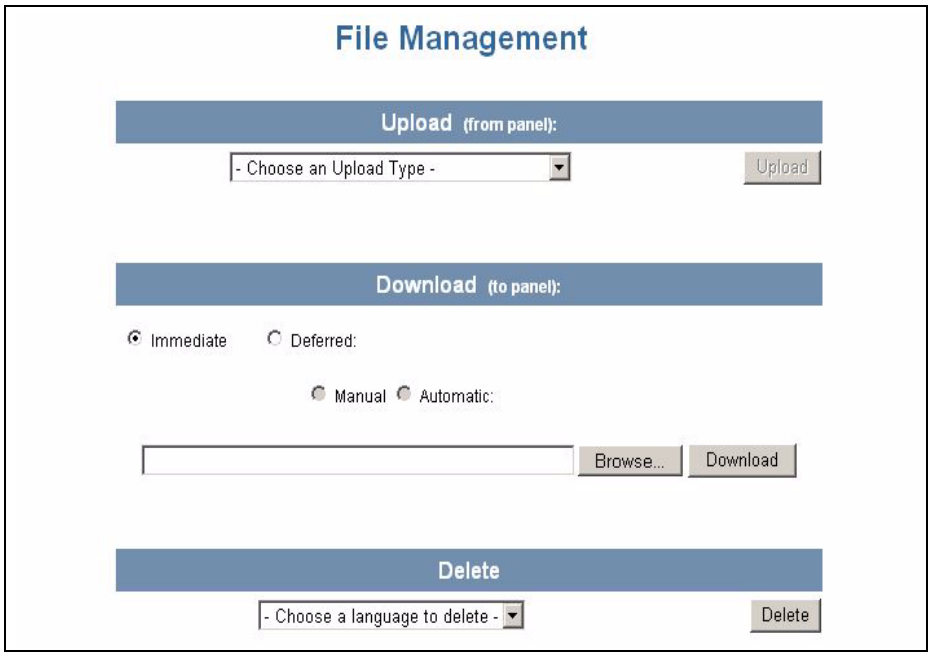
In a loop configuration, upgrade the gateway panel first.

A.3 Uploading Data from the Panel

Note: Before you upgrade a web-based panel, we recommend that you back up your databases. The upgrade scripts bring all your panel data forward into the new version without the need for user intervention. Therefore, it is always recommended to have backup copies of your panel's databases, and an upgrade provides an opportunity to keep your backups current. Use following procedure to backup each of your panel's databases. The backup features are **per panel**, so you need to select the panel to backup.

1. In the web server, select **System Tools > File Upload/Download** to display the File Management screen:

Figure A-1: *File Management Screen*



2. In the **Upload** section, select the Card, Common, and Panel Configuration upload option from the drop-down list.
3. Click **Upload** to upload the data to the host PC or laptop.
4. Follow the instructions to save a backup file on your PC. Give the backup file a useful name for easy restoring.

A.4 Downloading Data to the Panel

This section describes how to:

- download data to a selected panel immediately
- download data to all panels later--for activation either manually or automatically
- cancel an automatically deferred download
- cancel a deferred download altogether

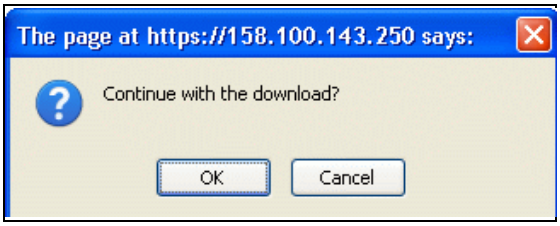
A.4.1 Downloading Data Immediately

You may download data immediately only on a per-panel basis.

To download data immediately:

1. In the web server, select **System Tools > File Upload/Download** to display the File Management screen (see Figure A-1).
2. Select the panel you wish to download the data to.
3. In the **Download** section, click **Browse** to locate the file you want to download.
4. When a file is selected, click **Immediate,** then click **Download**. A confirmation prompt appears:

Figure A-2: *Immediate Download Confirmation*



5. After confirmation, the file transfer to the gateway panel starts immediately and takes only a few seconds. The following popup then appears:

6. Click **OK**. If the receiving panel is a gateway panel, it will reboot almost immediately (since no further file transfer is necessary). If, however, the receiving panel is a downstream panel, the file transfer will take approximately two hours.

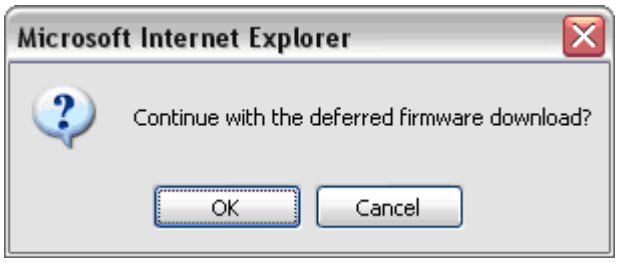
When the download/file transfer is complete, the panel reboots and the screen displays the following message: “This panel is now rebooting. Please wait at least 2 minutes for the reboot to complete.”

A.4.2 Downloading Data Later

Deferred downloads automatically transfer files to all panels in the loop. For deferred downloads, you can choose to activate the new firmware manually or have all panels in the loop activate the new firmware automatically (reboot) at a specified time in the future.

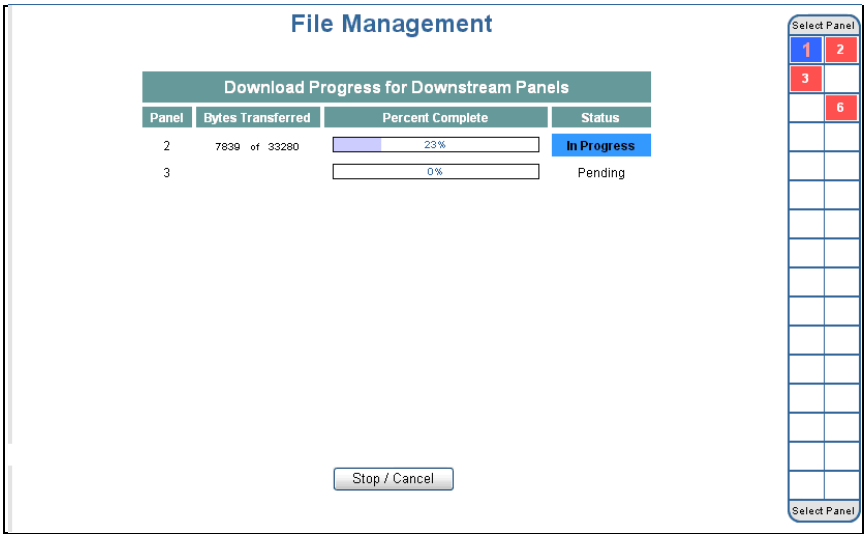
To set up a *manually deferred* download:

1. In the web server, select **System Tools > File Upload/Download** to display the File Management screen (see Figure A-1).
2. In the **Download** section, click **Browse** to locate the file you want to download.
3. When a file is selected, click **Deferred**, then click **Manual**, then click **Download**. A confirmation prompt appears:



4. Click **OK**. The download will complete to the gateway panel. If there are no downstream panels on your loop, the gateway will then reboot. If, however, there are one or more downstream panels, the following screen appears (showing two downstream panels):

Figure A-3: *Deferred Manual Download Confirmation*

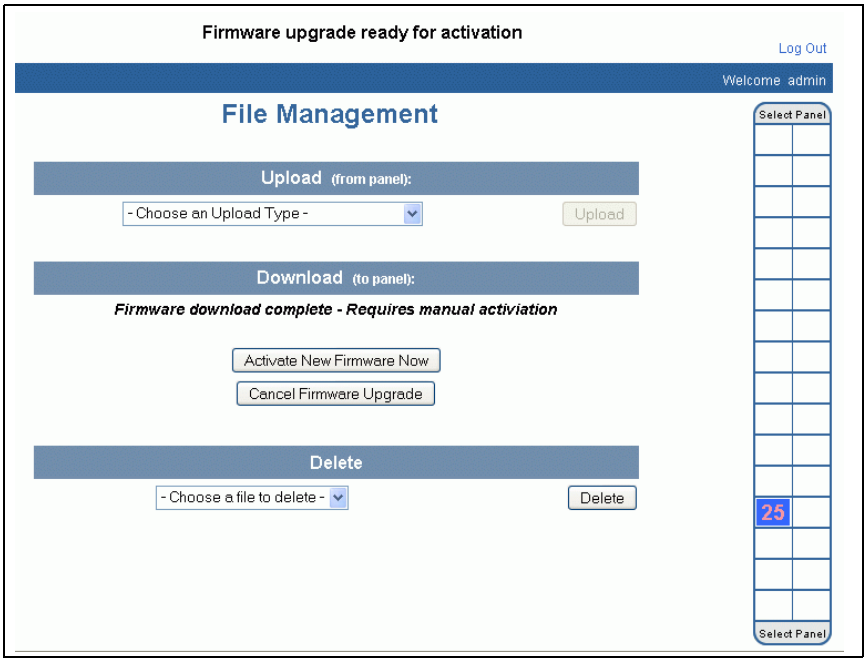


This screen shows the real-time progress of the file transfer for each NetAXS-123 panel on your loop.

In the example above, Panel #1 is the gateway and is not listed in the display area because it already has the firmware. Panel #2 and Panel #3 are NetAXS-123 panels either being downloaded to or waiting for the download. Panel #6 is not listed in the display area because it is an NX4 panel and cannot currently use NetAXS-123 firmware.

As the transfer completes to each NetAXS-123 panel on the loop, the file is moved into flash memory so that it remains on the panel even if the panel is rebooted (in which case it will still not be activated until you activate it manually). When the file transfer to all NetAXS-123 panels on the loop is complete, the following screen appears:

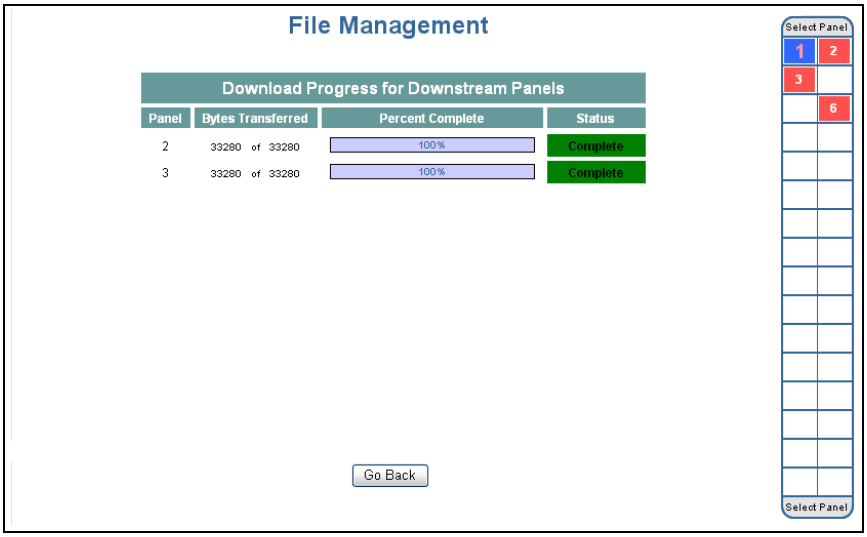
Figure A-4: *Firmware Upgrade Ready for Activation*



A status message at the top of the screen indicates that the upgrade is ready for activation.

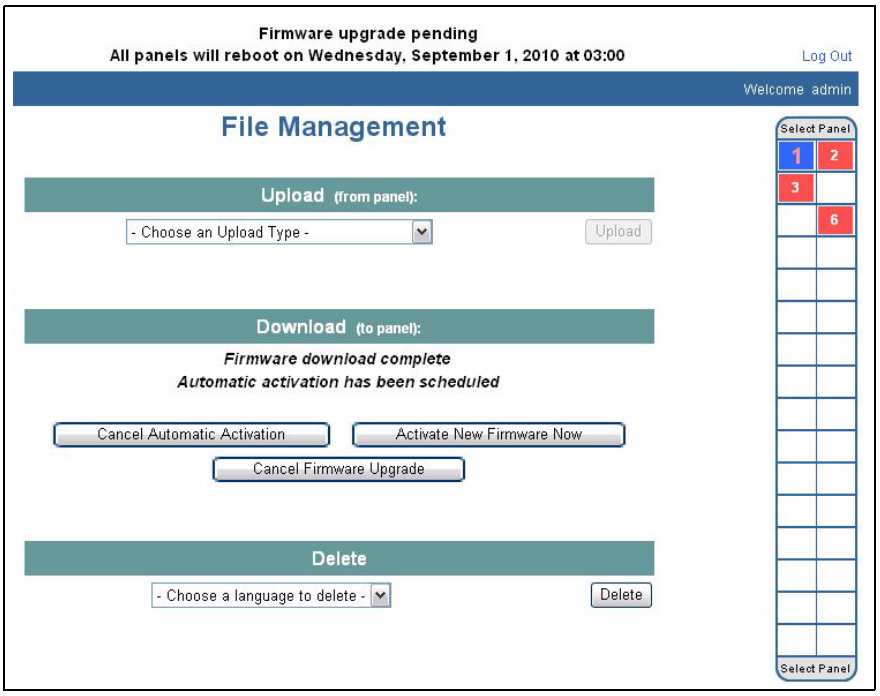
5. Set a date and time for the download and click **Download**. When the file transfers to all NetAXS-123 panels on the loop have completed, the following screen appears:

Figure A-5: *Download Progress Complete*



6. Click **Go Back** to display the following screen:

Figure A-6: *Firmware Upgrade Pending*



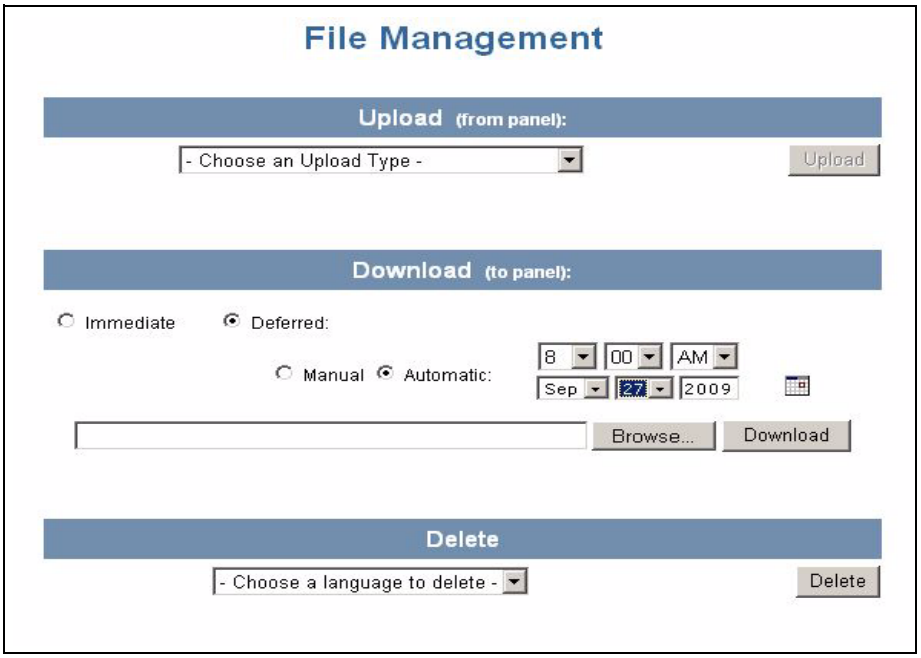
You now have the option of activating the new firmware immediately, cancelling automatic activation of the firmware (requiring manual activation), or cancelling the firmware upgrade entirely, which removes the newly downloaded firmware from all NetAXS-123 panels on the loop.

To set up an *automatically deferred* download:

1. In the web server, select **System Tools > File Upload/Download** to display the File Management screen (see Figure A-1).
2. In the Download section, click **Browse** to locate the file you want to download.

3. When a file is selected, click **Deferred**, then click **Automatic**. Date and time pull-down menus appear on the screen.

Figure A-7: *Deferred Automatic Download Configuration*



4. Set a date and time for the download and click **Download**. The following message appears under the Download header: "Activation scheduled for [month/day] [hr:min] [AM/PM].

A.4.3 Cancelling a Download

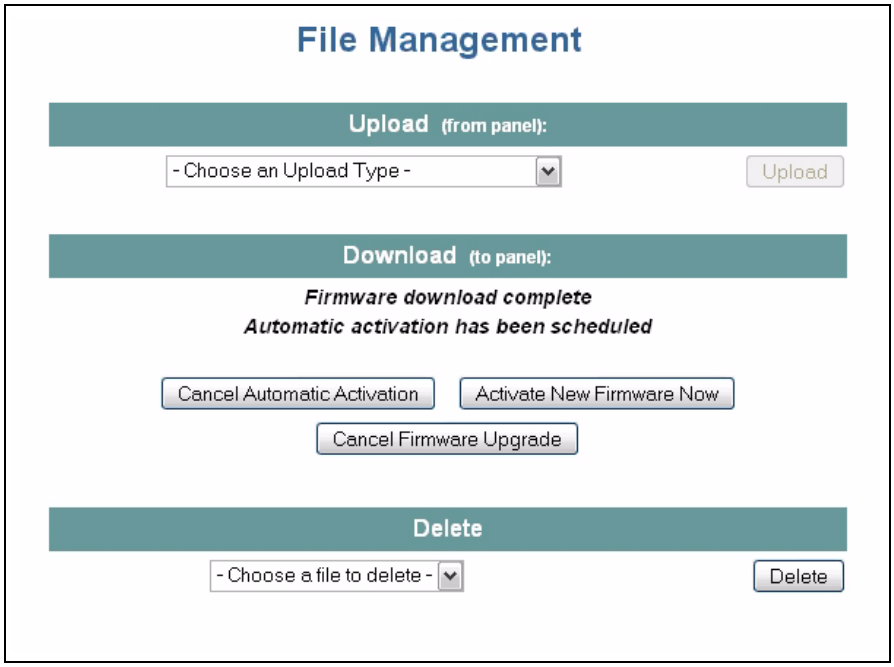
You may return to the firmware download page at any time and cancel all downloads that are pending or in progress.

For deferred downloads, the panels waiting to begin are removed from the download queue and the download is cancelled.

For manually deferred downloads that are awaiting activation, the cancellation removes the downloaded firmware entirely from the waiting area.

1. Click **Download** to complete the deferred download setup and display the following acknowledgment screen:

Figure A-8: *Automatic Download Configuration Acknowledgment*



2. To cancel the automatic activation, click **Cancel Automatic Activation** which displays the following message box:

3. Click **OK** to complete the cancellation.
4. The File Management screen will acknowledge cancellation of the automatic upgrade and the need for manual activation (Figure A-4).

5. Click **Activate New Firmware Now** to activate the new firmware. The system displays the following message box:

6. Click **OK** to activate the new firmware.

A.5 Upgrades to Gateway vs. Multi-drop Panels

You can upgrade multi-drop panels in the same way you upgrade the gateway panels via the web screen.

1. Set DIP switch 6 to “ON.”
2. Connect directly to each panel via a Local Area Network or a direct-connect Ethernet connection.
3. Return the configuration back to a downstream panel once the upgrade has been successfully completed.

Caution: You cannot have more than one gateway on a loop, so it is critical that you disconnect the 485 cables on the panel you are upgrading.

To perform the upgrade:

1. Before starting, make sure your panels are not buffered. If you have not logged in to the web pages lately, or WIN-PAK has not been connected recently, you should login and make sure you have current events coming in. This will ensure that the panels are not buffered, and you will not have to wait for the un-buffer to complete before starting. If you try to login and get “time-outs,” your panels are probably buffered and you should wait for them to complete their un-buffer before starting the upgrade.

Note: For WIN-PAK systems, we recommend that you stop the “communications server service” while upgrading, and then restart the service after your panels are upgraded.

2. Connect to your gateway panel using the instructions in Connecting to the Web Server, page 3.

Caution: You cannot have more than one gateway on a loop, so it is critical that you disconnect the 485 cables on the panel you are upgrading.

3. Log in to your gateway.

4. Click **Communications > Host/Loop** and set the panel to web mode, if it is not already set. In the Connection Type box, select **none** and click **Submit Changes**. Wait one to one-and-a-half minutes. You can click **Refresh** on your browser after one minute and navigate to the General tab to see if the buttons are present.
5. After the screen is refreshed, and you are in the General tab, click **Reset Panel**, and then click **OK** to continue. This step prepares the panel to accept the new application and operating system files that you will be downloading. The reset usually takes between two and two-and-a-half minutes. After two-and-a-half minutes (or after you hear the relays "click"), click **Refresh** on your browser and log back in. Both sets will appear correctly after the upgrade is complete.
6. Install the new application file, 3-NetAXSimagexx.xx.xx.bin. To do this:
    a. Click **System Tools > File Upload/Download** tab.
    b. In the Download box, click **Browse** to locate the file, 3-NetAXSimagexx.xx.xx.bin.
    c. Select the file and click **Download**. Click **OK** to continue. After the "Download complete" message appears, click **OK** again. The "Download image" message appears and tells you to wait five minutes while NetAXS-123 reboots.
    d. Clear the cache. Before logging back in to NetAXS-123, use the browser-dependent steps to clear your browser cache (Clearing the Cache, page 151).
    e. Wait either for the relays to click or five minutes, and log back in to the NetAXS-123 web server.
7. Check to be sure the new versions are installed. To do this:
    a. Select the **System Tools > File Upload/Download** tab.
    b. In the Version Information section, the new OS and application versions should appear. Verify that the correct versions of the OS and firmware are listed.
    c. For WIN-PAK-based loops, we recommend that you run a full download to all panels after the new version is installed.

A.6 Upgrade Notes

1. If you notice any communication issues, and the upgrades are complete, you probably had more than one panel configured as a gateway. In this case, you should reset the panels to clear the issue.
2. If you are using Microsoft Internet Explorer 7—According to Microsoft, if you are running IE7 version 7.0.5730.11, you should upgrade to version 7.0.5730.13 or newer. NetAXS™ is not compatible with IE7 version 7.0.5730.11. You should either use a newer version, IE 6, or another browser.

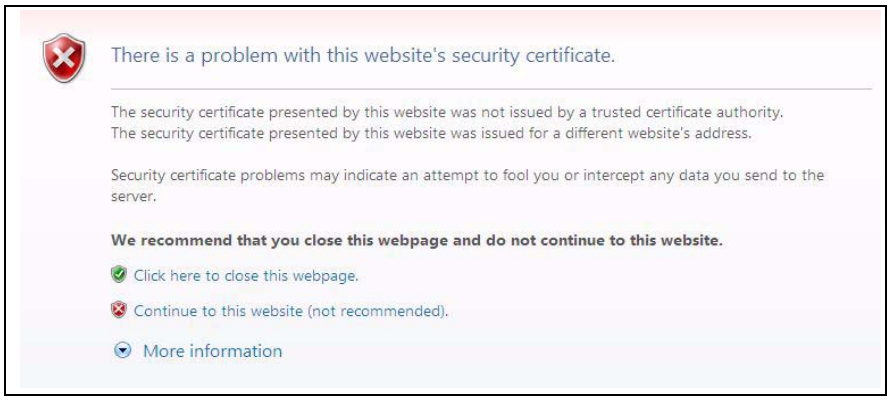
A.6.1 Microsoft Internet Explorer 7 Security Certificate Failure

Note: The IP address shown in the following screens is for illustration purposes only. For these procedures use the default IP address that is provided to you.

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

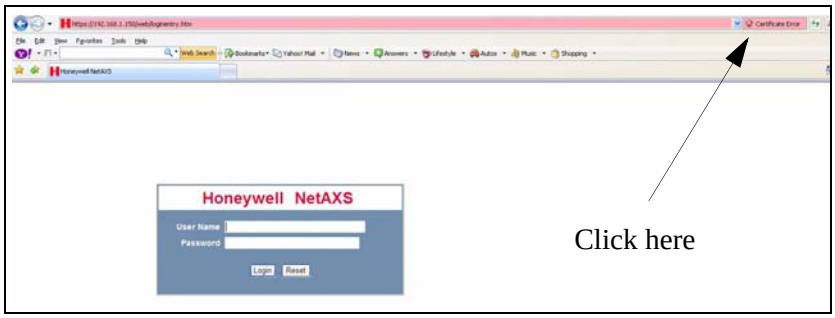
1. Enter the IP address of the panel into the URL box. The following message appears:

Figure A-9: *Security Certificate Failure Screen*



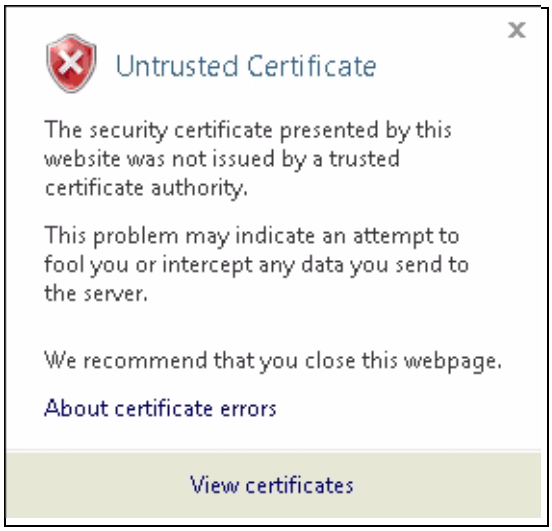
2. Click **Continue to this website (not recommended)** to display the login screen.

Figure A-10: *Security Certificate Failure Correction Login*



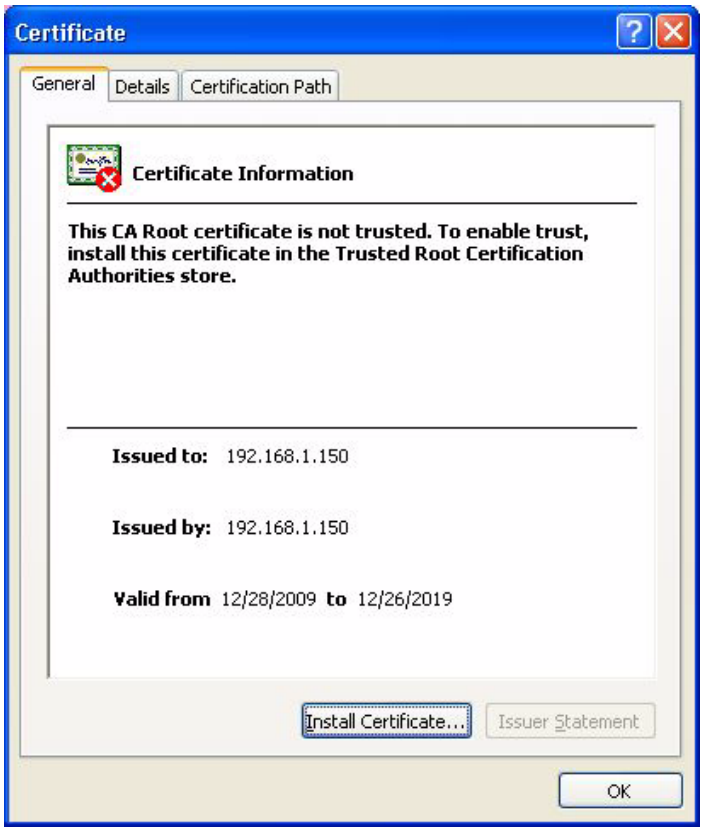
3. Click **Certificate Error** at the top-right of the IP address. The Untrusted Certificate screen appears.

Figure A-11: *Untrusted Certificate Message*



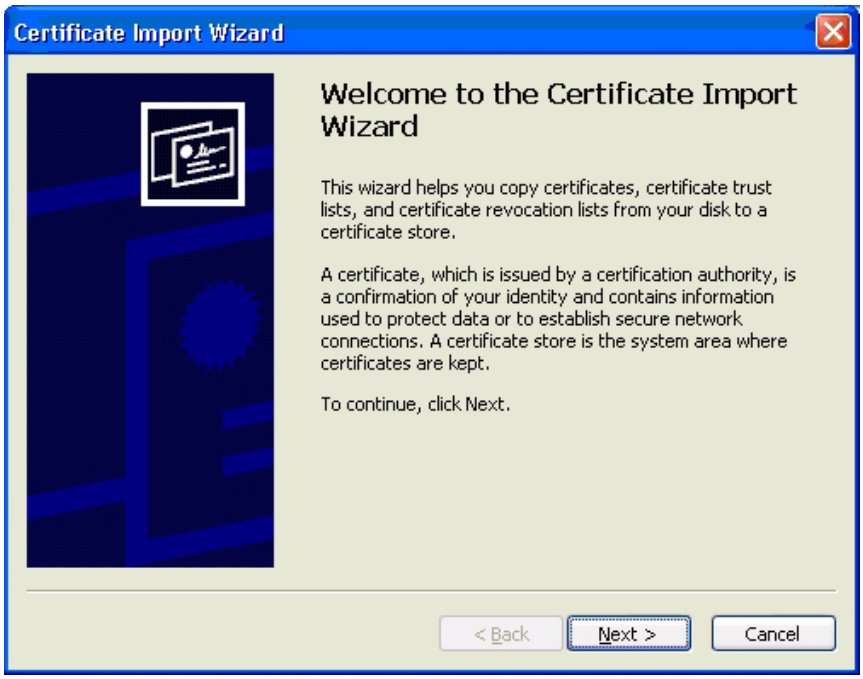
4. Click the **View Certificates** bar. The Certificate Information screen appears.

Figure A-12: *Certificate Information Screen*



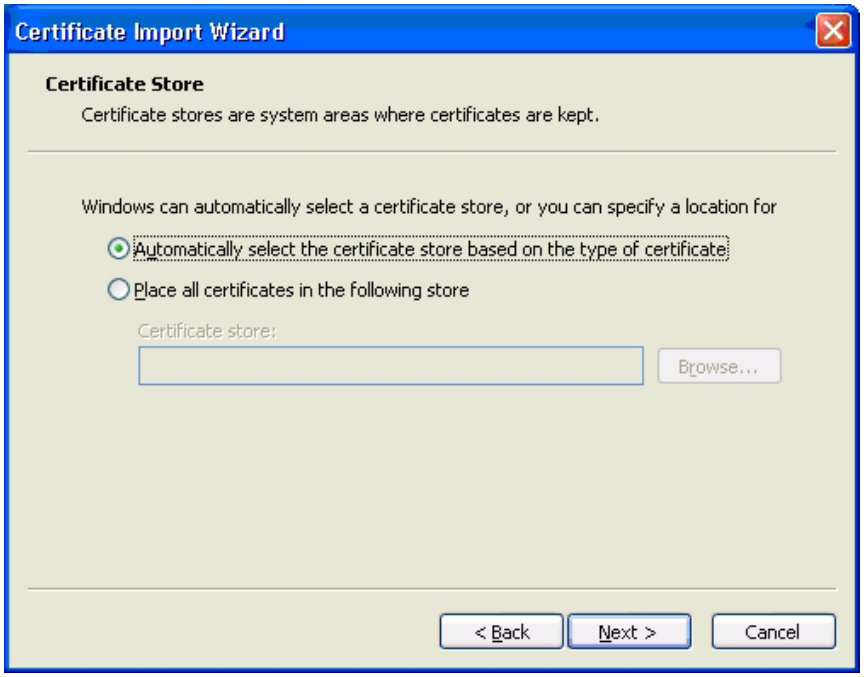
5. Click **Install Certificate.** The Certificate Import Wizard screen appears.

Figure A-13: *Certificate Import Wizard Welcome Screen*



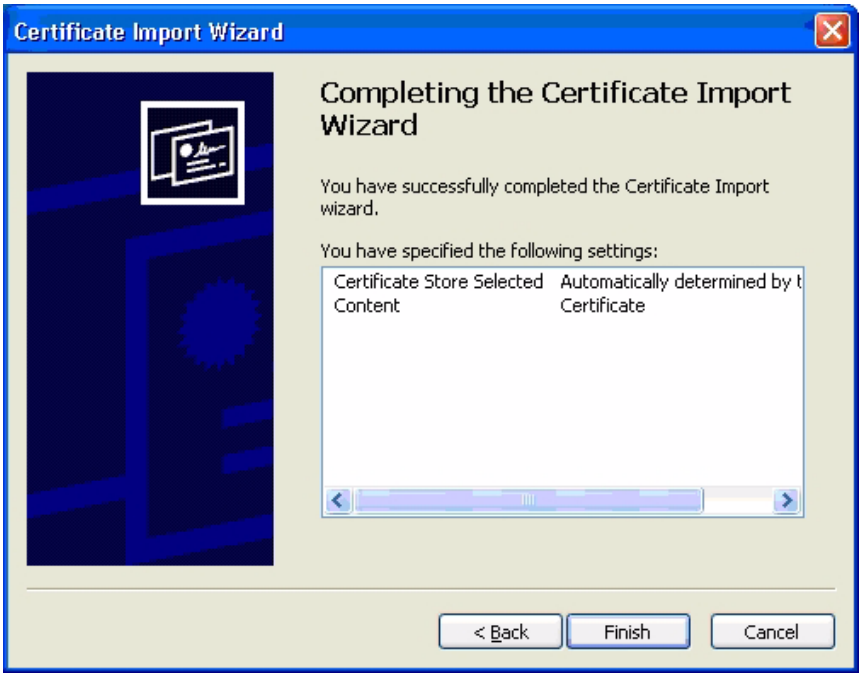
6. Click **Next** to view the Certificate Store screen.

Figure A-14: *Certificate Store Screen*



7. Accept the default value and click **Next** to display the Certificate Import Wizard completion screen.

Figure A-15: *Certificate Import Wizard Completion Screen*



8. Click **Finish**. The following warning appears:

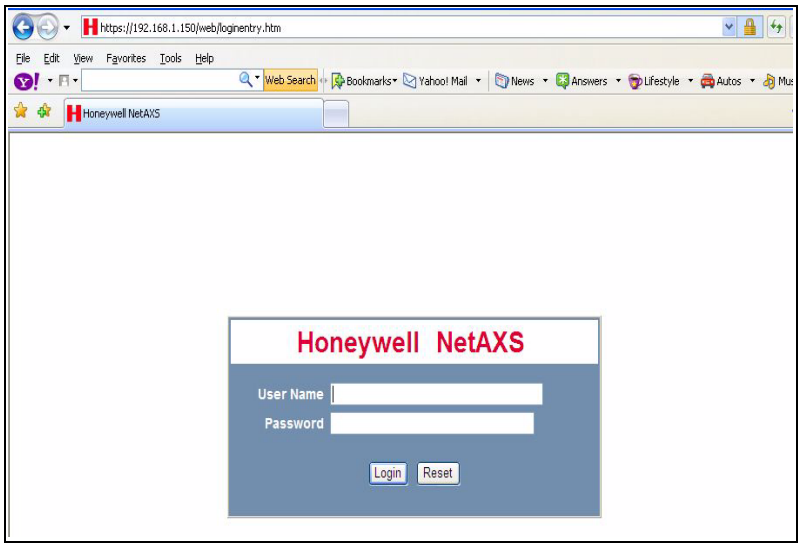
Figure A-16: *Security Warning Screen*

9. Click **Yes** to view the following popup.

Figure A-17: *Successful Import Message*

10. Click **OK** to return to the Certificate Information screen (Figure A-12 on page 144).
11. Click **OK**.
12. Close the web browser and re-open it.
13. Enter the IP address again into the URL box. The login screen appears without Certificate Error.

Figure A-18: *Security Certificate Login*

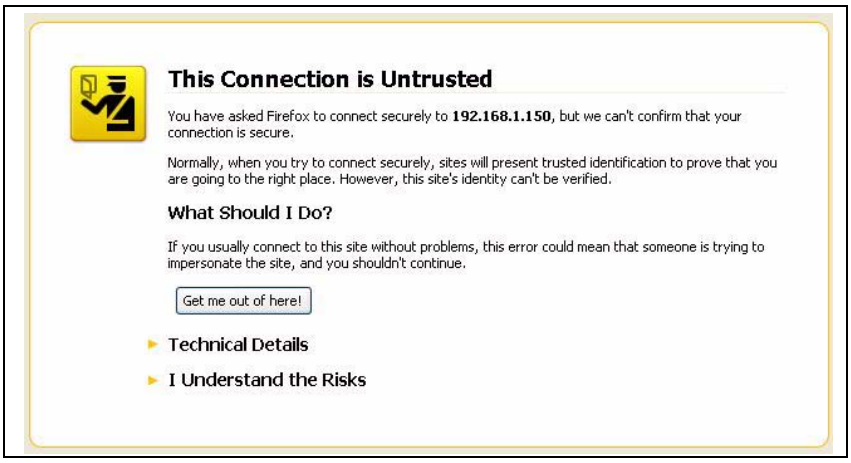


A.6.2 Firefox 3 Security Certificate Failure

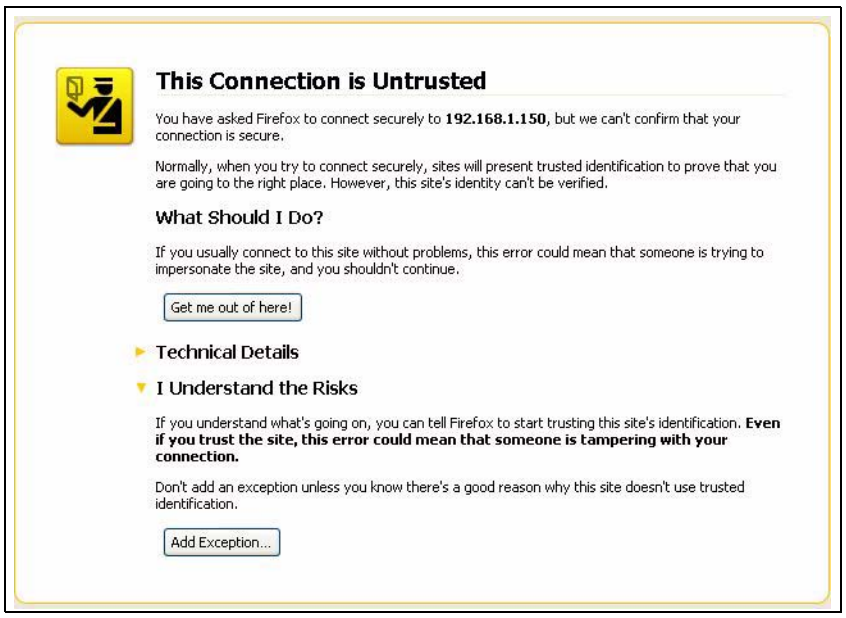
If you are using Firefox 3, and you receive a certificate error message, follow these steps to clear it:

1. Enter the IP address of the panel into the URL box. The following message appears:

Figure A-19: *Secure Connection Failed Message*

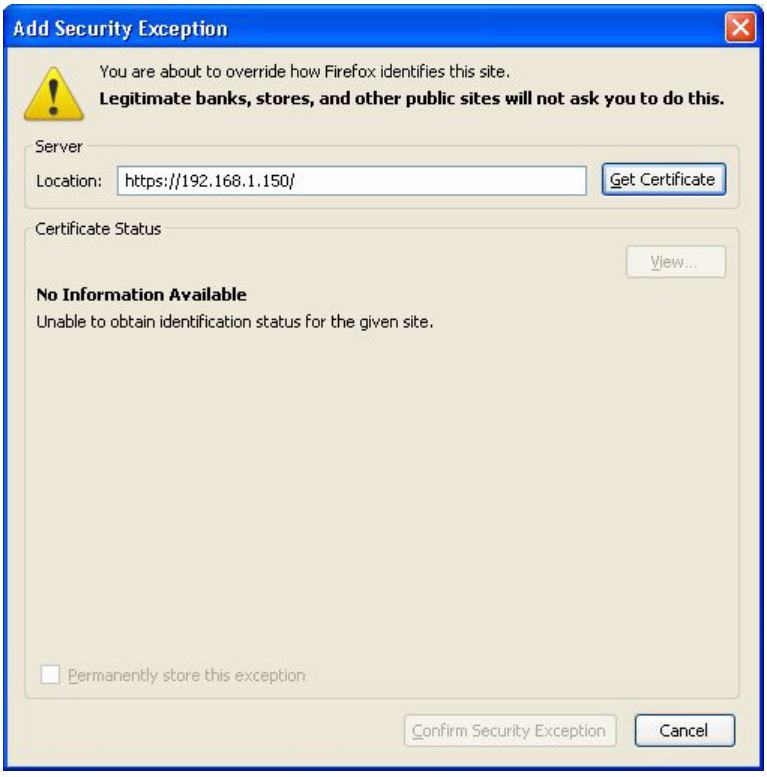


2. Click on “I Understand the Risks” to expand the screen:



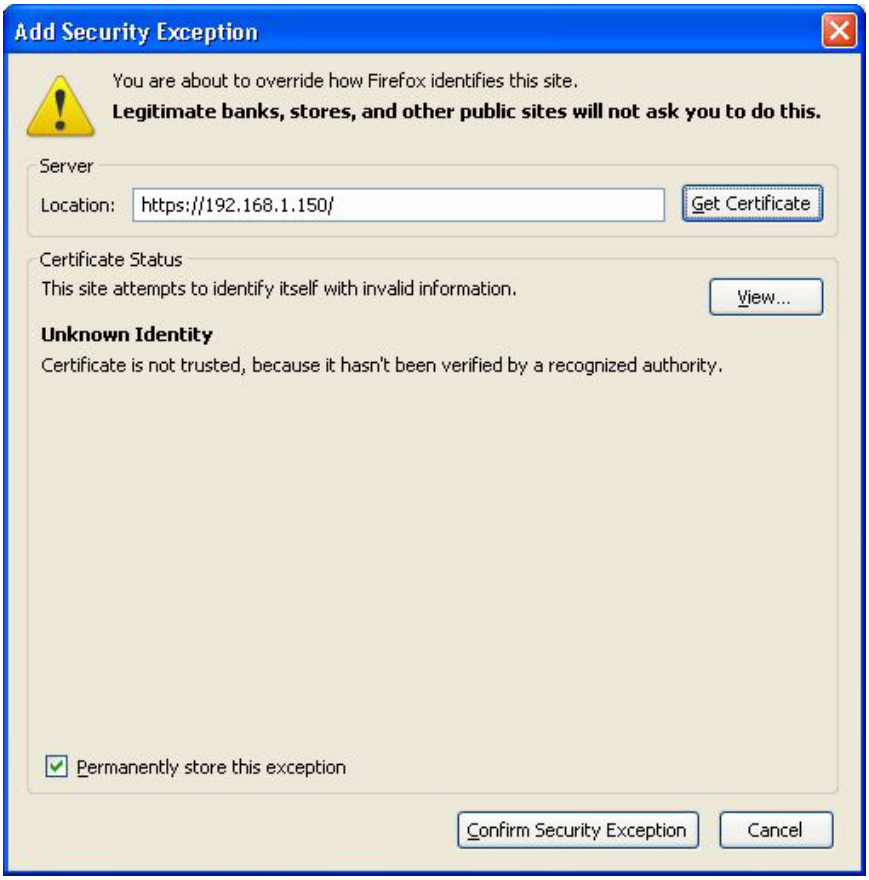
3. Click **Add Exception** to display the Add Security Exception screen:

Figure A-20: *Add Security Exception Screen*



4. Click **Get Certificate**. The following Unknown Identity message appears:

Figure A-21: *Unknown Identity Message Screen*



5. Ensure the “Permanently store this exception” check box is checked. (This is the default.)
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 screen next displays the NetAXS-123 Login screen (8-10 seconds later).
8. Continue with the login.

A.7 Clearing the Cache

The NetAXS-123 panel supports Internet Explorer (IE8), Internet Explorer 7 (IE7), Internet Explorer 6 (IE6), Firefox 2, and Firefox 3. For all browsers, we recommend that you clear the cache after a successful upgrade.

A.7.1 Using Internet Explorer Versions IE7 and IE8

To clear the cache using IE7 and IE8:

1. Select **Tools > Delete Browsing History.** A "Delete Browsing History" popup appears, showing the following defaults:
   - Preserve Favorite Website Date
   - Temporary Internet files
   - Cookies
   - History

   Leave these selections alone.
2. Click **Delete**. The "Delete Browsing History" popup closes.

A.7.2 Using Internet Explorer 6 (IE6)

To clear the cache using IE6:

1. Select **Tools > Internet Options > General**.
2. Click **Delete Cookies**. A Delete Cookies popup prompts, "Delete all cookies in the Temporary Internet Files folder?"
3. Click **OK**.
4. With the Internet Options screen open, click **Delete Files**. A Delete Files message prompts, "Delete all files in the Temporary Internet Files. You can also delete all your offline content stored locally."
5. Click **OK**.
6. Click **OK** on the Internet Options screen to close it.

A.7.3 Using Firefox 2 or Firefox 3

To clear the cache using Firefox 2 or Firefox 3:

1. Select **Tools > Clear Private Data.** The Clear Private Data screen appears.
2. Ensure that the Cache and the Cookies check boxes are enabled.
3. Click **Clear Private Data Now.** The Clear Private Data screen automatically closes.

NetAXS-123 DIP Switch Settings

B

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

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

S1	S2	S3	S4	S5	S6	S7[a]	S8[b]	S9[b]	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 B-1: *NetAXS-123 SW1 DIP Switch Settings (continued)*

S1	S2	S3	S4	S5	S6	S7[a]	S8[b]	S9[b]	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	OFF	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

a. DIP Switch 7 does NOT require a panel reboot to take effect. This does not affect the USB IP address.

b. Both DIP Switch 8 and DIP Switch 9 need to be either ON or OFF to be properly configured.

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

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

a. 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.
7. The RUN LED should flash normal.

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

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 800-05168, Revision B