

# Continental Access



## CONFIGURING NAPCO INTEGRATION

Revision B  
Date: 11/09/2010



## Important Information - MUST READ

**VERY IMPORTANT:** It is very important to have the Napco Alarm panel and the NLMOD programmed prior to integrating it with the CardAccess 3000. It is highly recommended to consult Napco Technical Support to properly configure the Napco Equipment (Refer to Appendix A). While working with Napco Technical Support, you must have the CA3000 shut down. Do not mention integration with CardAccess 3000. It is very important to get the Napco Equipment functioning properly over the customer's network, before integrating it with the CardAccess 3000.

### Notes:

- 1) Verify your security key or software license supports 1 napco server. You must purchase the Napco Integration feature to receive this license. The Napco Integration feature will not work without this license.
- 2) You **MUST** have FULL ADMINISTRATOR rights to run Napco Integration.
- 3) It is highly recommended to run the Napco Integration on a CardAccess 3000 workstation. This would require the security key to support 5 workstations.
- 4) Refer to Appendix B for recommended troubleshooting steps.

## Scope

This document contains information regarding the configuration of the CardAccess 3000 Napco Integration. As previously noted, it is very important to have the Napco equipment programmed prior to integrating it with the Continental software. Refer to Appendix A for instructions on configuring the Napco Alarm panel and the Napco NL-Mod. If you need assistance with the Napco equipment, contact Napco Technical support.

## Prerequisites

Prior to configuring the CA3000 with Napco Integration, the following are some things you will need:

- Napco Alarm Panel (3200, 9600, X255) with V60 firmware or later
- Napco Quickloader Software configured for TCP/IP
- NL-MOD (firmware version 1.6.76 or later)
- Napco NL-Mod configuration software (version 3.0.1.25 or later)
- Static IP, subnet mask and gateway (Contact the Network Administrator)
- Ethernet Patch cable
- Ethernet crossover cable for programming and troubleshooting
- Continental Security Key/Soft License for Napco Integration

# Configuring Napco Integration in the CardAccess 3000

**Reminder:** Before programming the CA3000, verify the Napco Alarm panel and the NL-MOD is programmed correctly. Refer to Appendix A.

1) Configure the Napco Panels screen as follows. Refer to figure 1.

- Click System/System Settings/Napco
- Click **Edit**.
- Select **Use NAPCO Panels**
- Select **Enforce NAPCO Permission settings**
- Click **Add NAPCO Server**
- Type in **UNC Name** of the Workstation (computer) the Napco Integration will be running on
- Click **Save and Close**

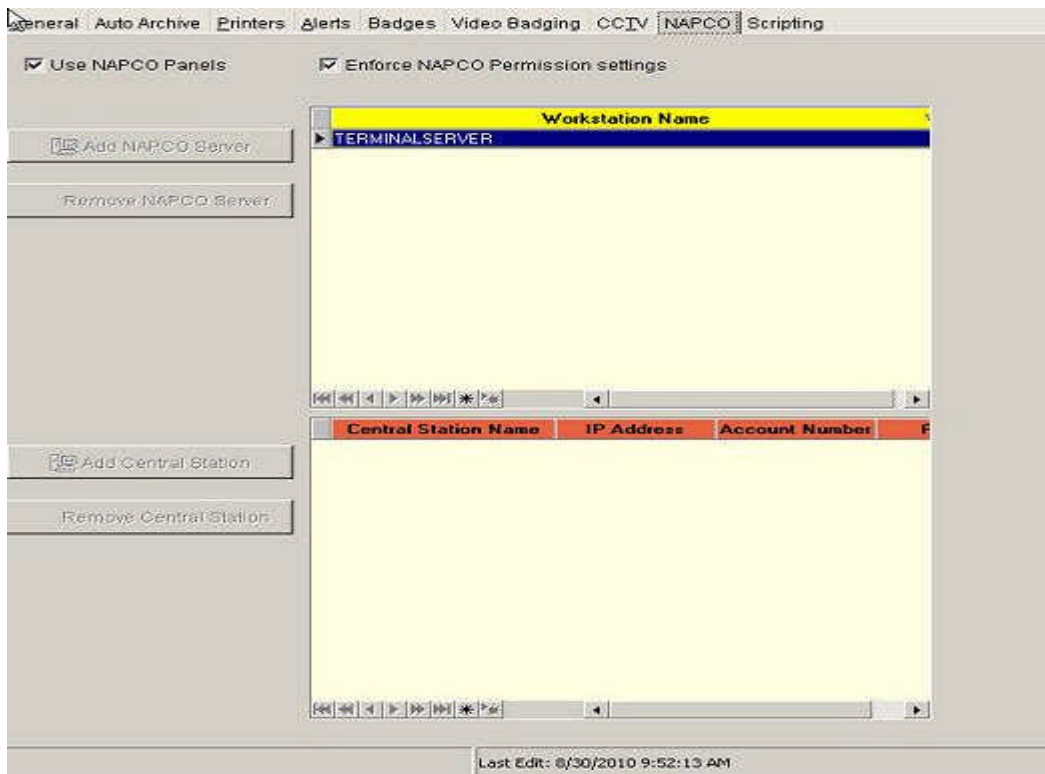


Figure 1.

2) Configure the **Napco Panel** screen (General tab) as follows. Refer to figure 2.

- Click **New**
  - Type in a Descriptive Napco **Panel Name**
  - Select the Napco **Panel Type** (ex. 3200, 9600, x255)
  - Select the **Enabled** checkbox
  - Enter the **Panel Security Code**. The Panel Security code can be found in the alarm panel. It is on the firmware chip and also on the metal can shielding the firmware chip
- Very Important:** If you are using CardAccess 3000 V2.6.19 or earlier, you must replace the zero(s) with "A"(s) in the master security code. Example: 907062 must be changed to 9A7A62
- Select None for **Group**
  - Select the **Napco Server name** for **Workstation**. This is the workstation name in figure 1
  - Select Net Link for **Connection type**
  - **Socket Number** = 10081
  - **PC Security Code** = Optional

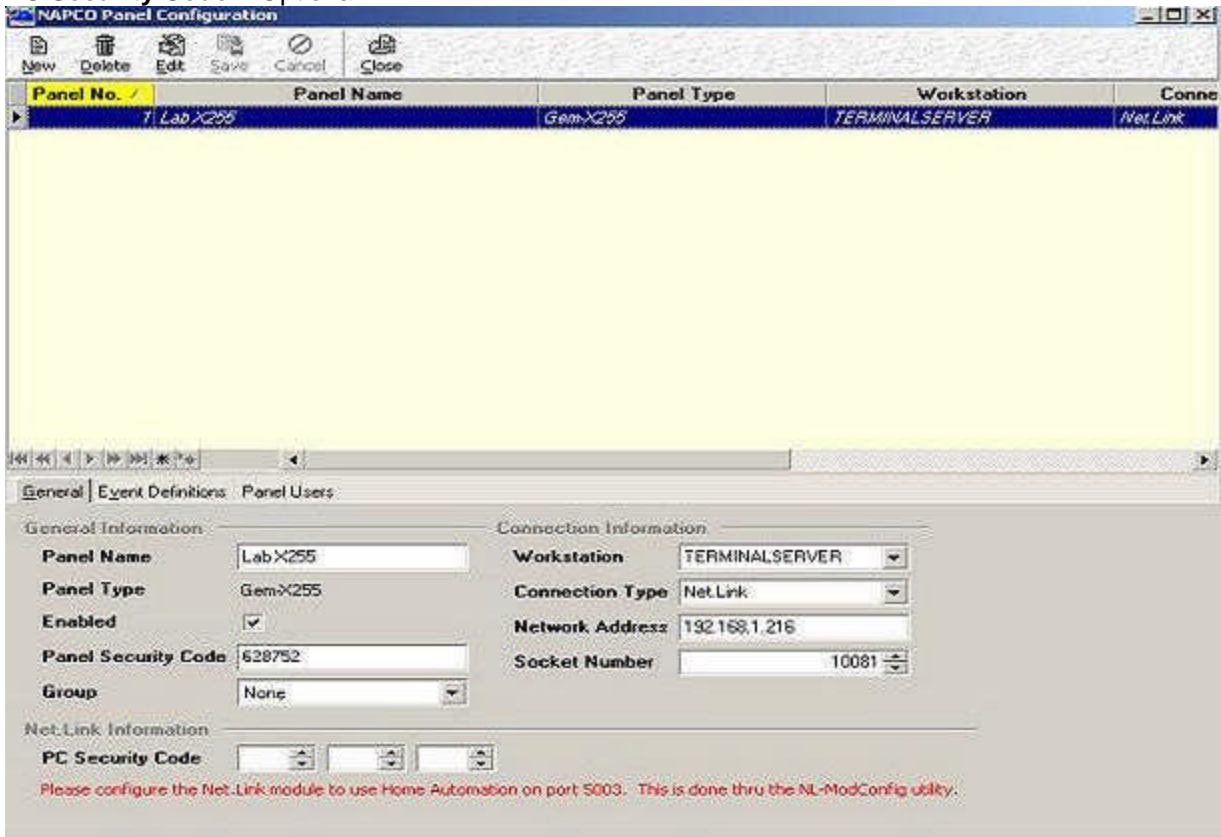


Figure 2.

Configure the **Napco Area** screen (General tab) as follows. Refer to figure 3.

- Click **Edit**
- Type in a Descriptive **Area Name**
- Select the **Configured** checkbox
- Select None for **Group**
- Select ALL for the **Manual Control Privilege**

Note: The next four items get configured only if you are using a Napco proxpoint cover with LEDs

- Select **Use Relay Control**
- Select **Use Access Control Panel**
- Select the **Panel** being used for the Prox Cover LED
- Select the **Relay** being used for the Prox Cover LED
- Click **Save**

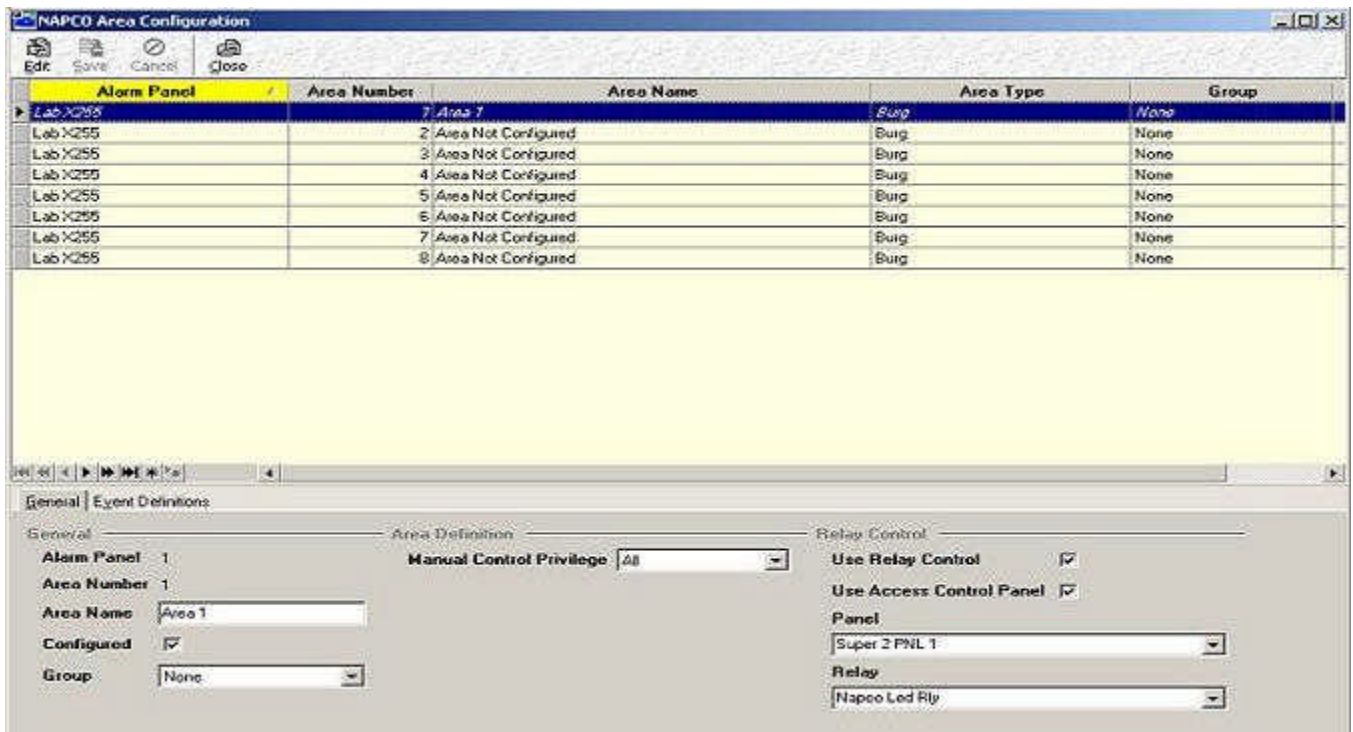


Figure 3.

Configure the **Zone** screen (General tab) as follows. Refer to figure 4.

- Click **Edit**
- Type in a Descriptive **Zone Name**
- Select the **Area**
- Select the **Zone Configured** checkbox
- Select None for **Group**
- Click **Save**

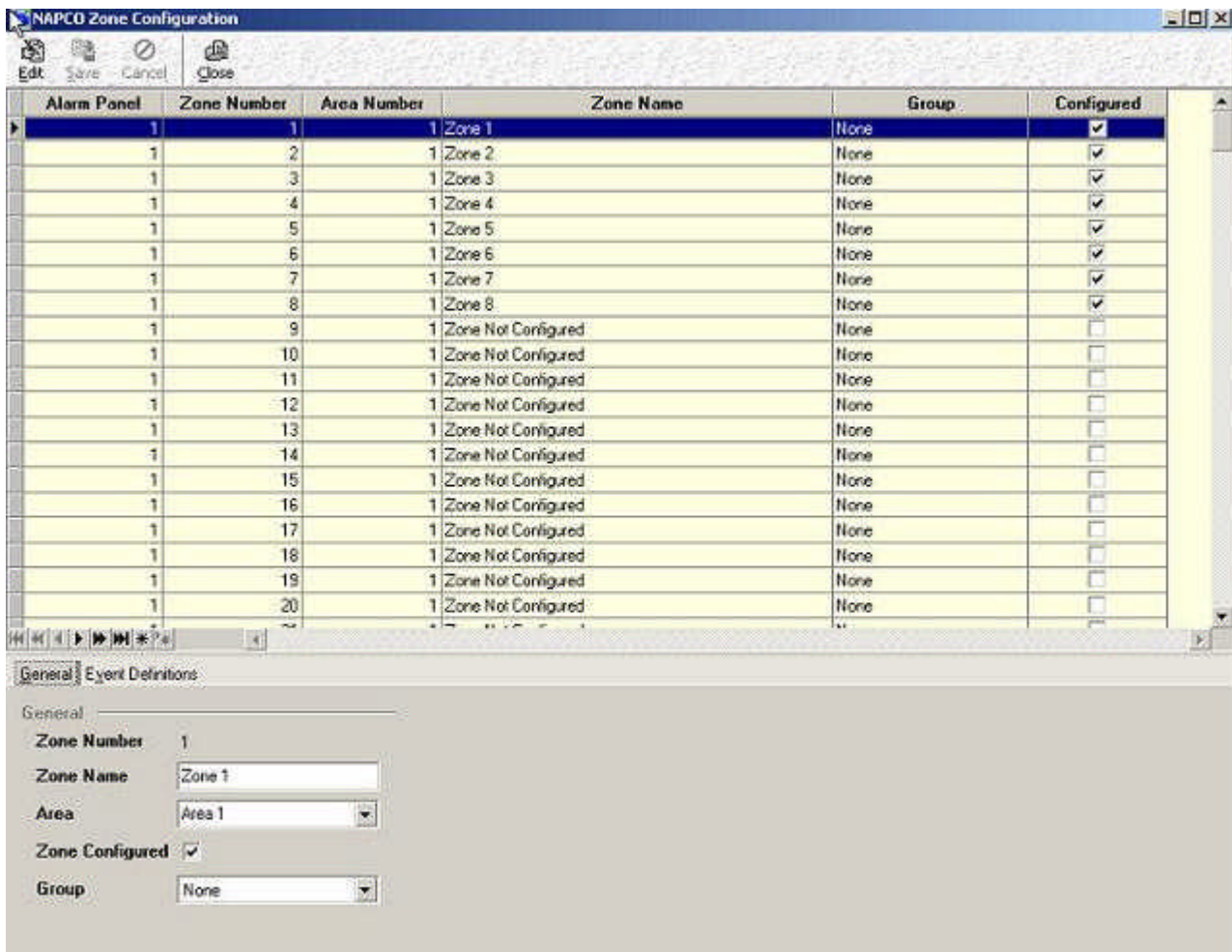


Figure 4.

Configure the **Napco Permissions** screen as follows. Refer to figure 5, 6 and 7.

Note: Repeat the following steps 3 times for all three Napco **Permissions** as below (Full Control, Arm only and Disarm only)

- Click **New**
- Type in a Descriptive **Permission Name**
- Select None for **Group**
- Select Arm and Disarm accordingly as per the permission name:

Full Control = Arm and Disarm selected

Arm Only = Arm selected

Disarm = Disarm selected

- Click **Save**

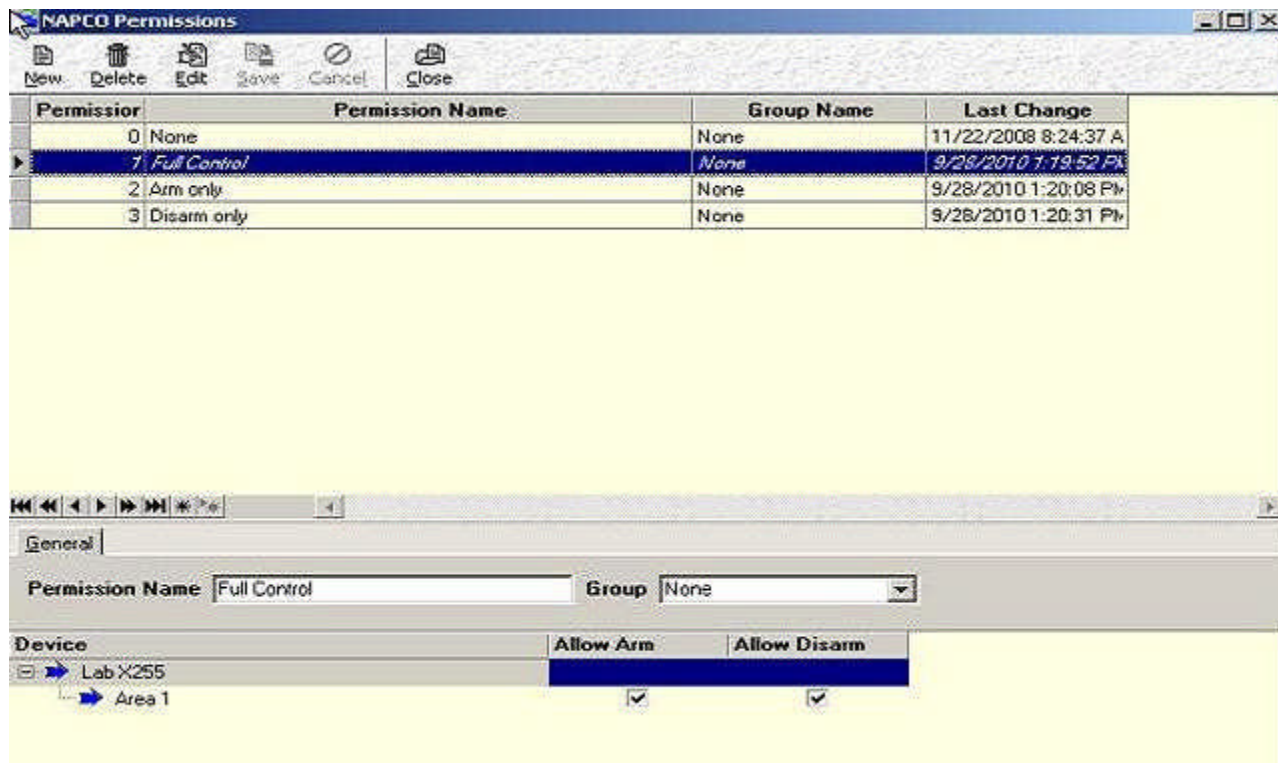


Figure 5.

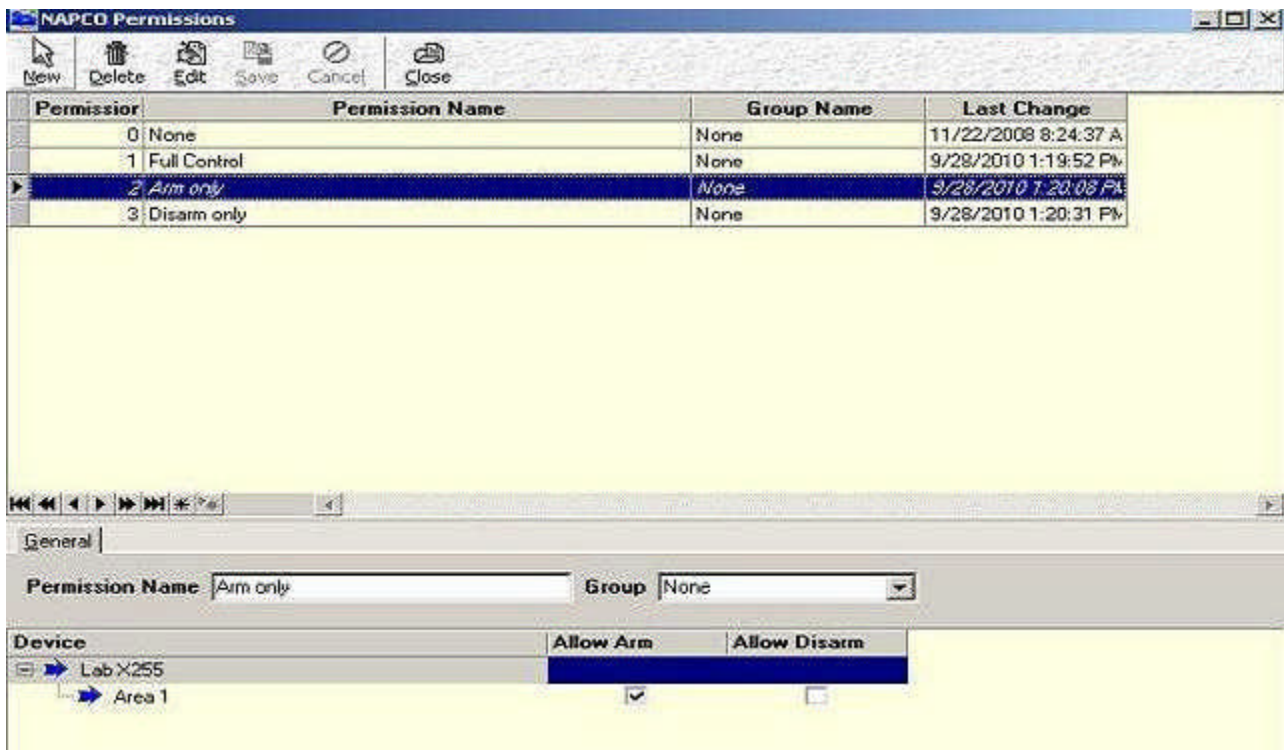


Figure 6.

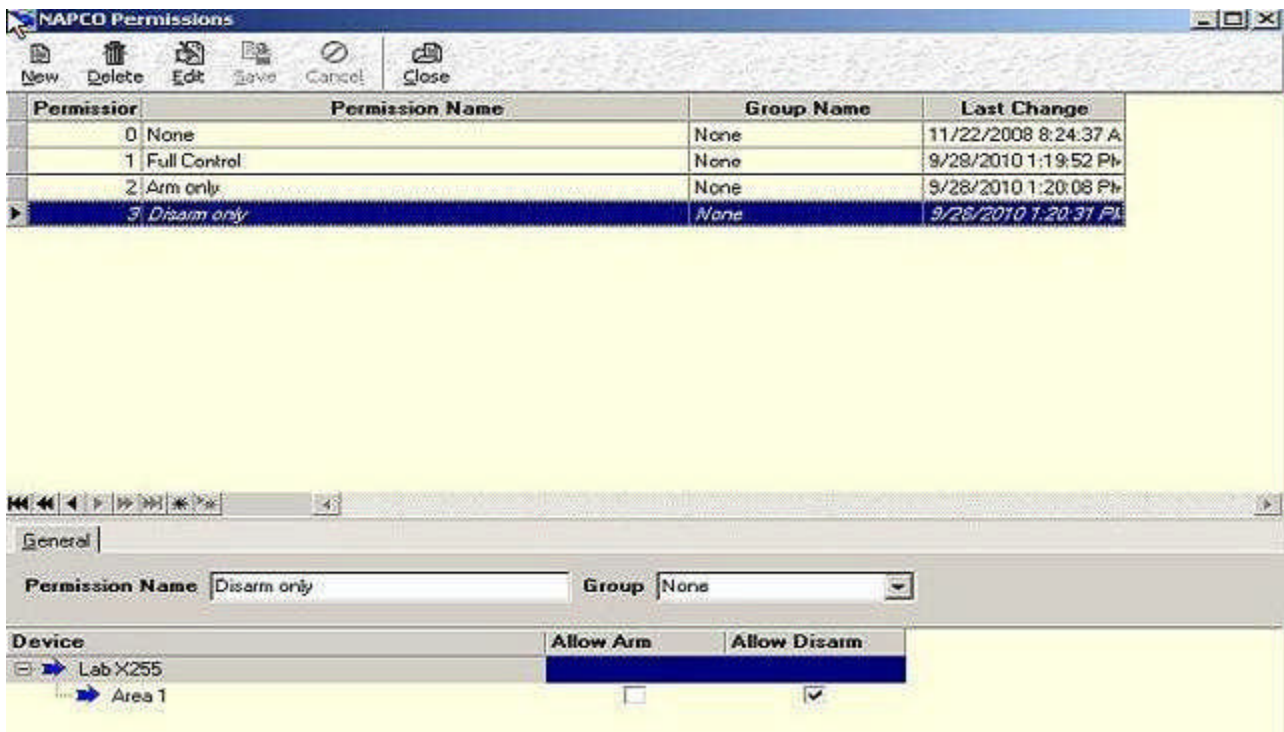


Figure 7.

Configure the **Panels Configuration** screen as follows. Refer to figure 8.

- Click **Edit**
- In the Panel Configuration screen, select the **NAPCO Panel Link**. The Continental panel to be edited is the panel the arming/disarming reader is attached to.
- Click **Save**

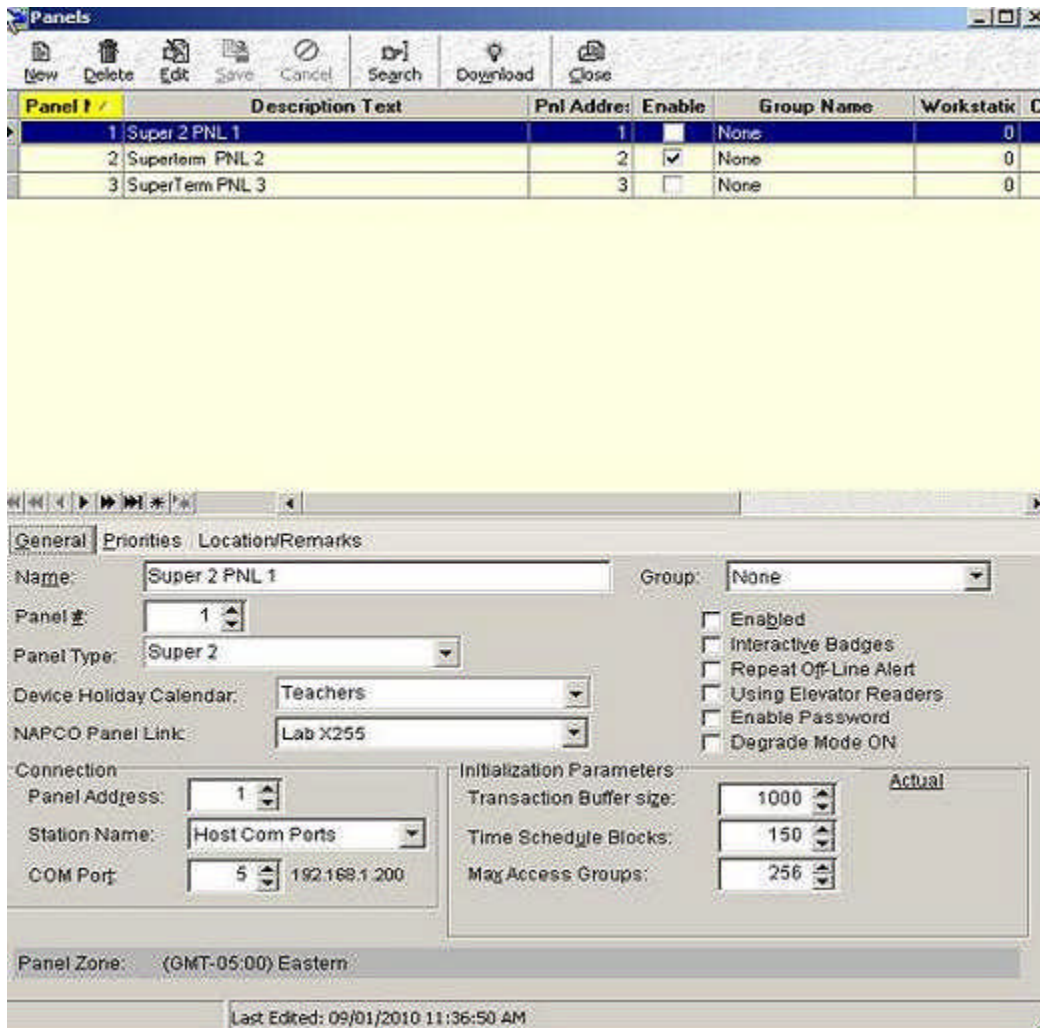


Figure 8.

Configure the **Readers Configuration** screen as follows. Refer to figure 9.

- Click **Edit**
- Select **Remote Control** tab
- In the Reader Configuration screen, select the Area to control in the **NAPCO Alarm Panel Areas** (this is the area this reader will arm/disarm)
- Click **Save**

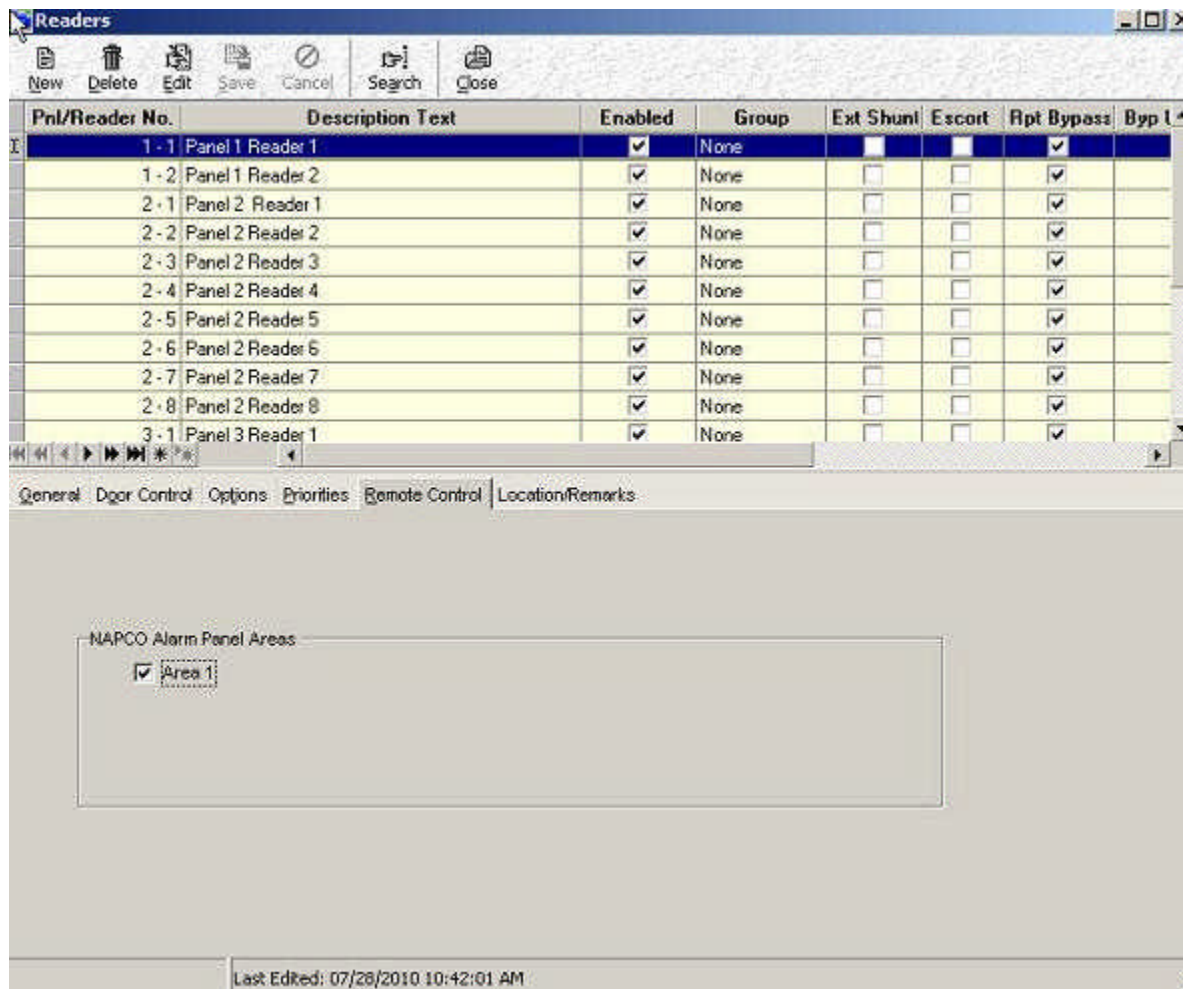


Figure 9.

Configure the **Personnel** screen for the correct **NAPCO Permission**. Refer to figure 10.

- Click **Edit**
- Select the badge being used for Napco arming and disarming
- Click **Control** tab
- Select the **NAPCO Permission** to be assigned to the badge
- Click **Save**

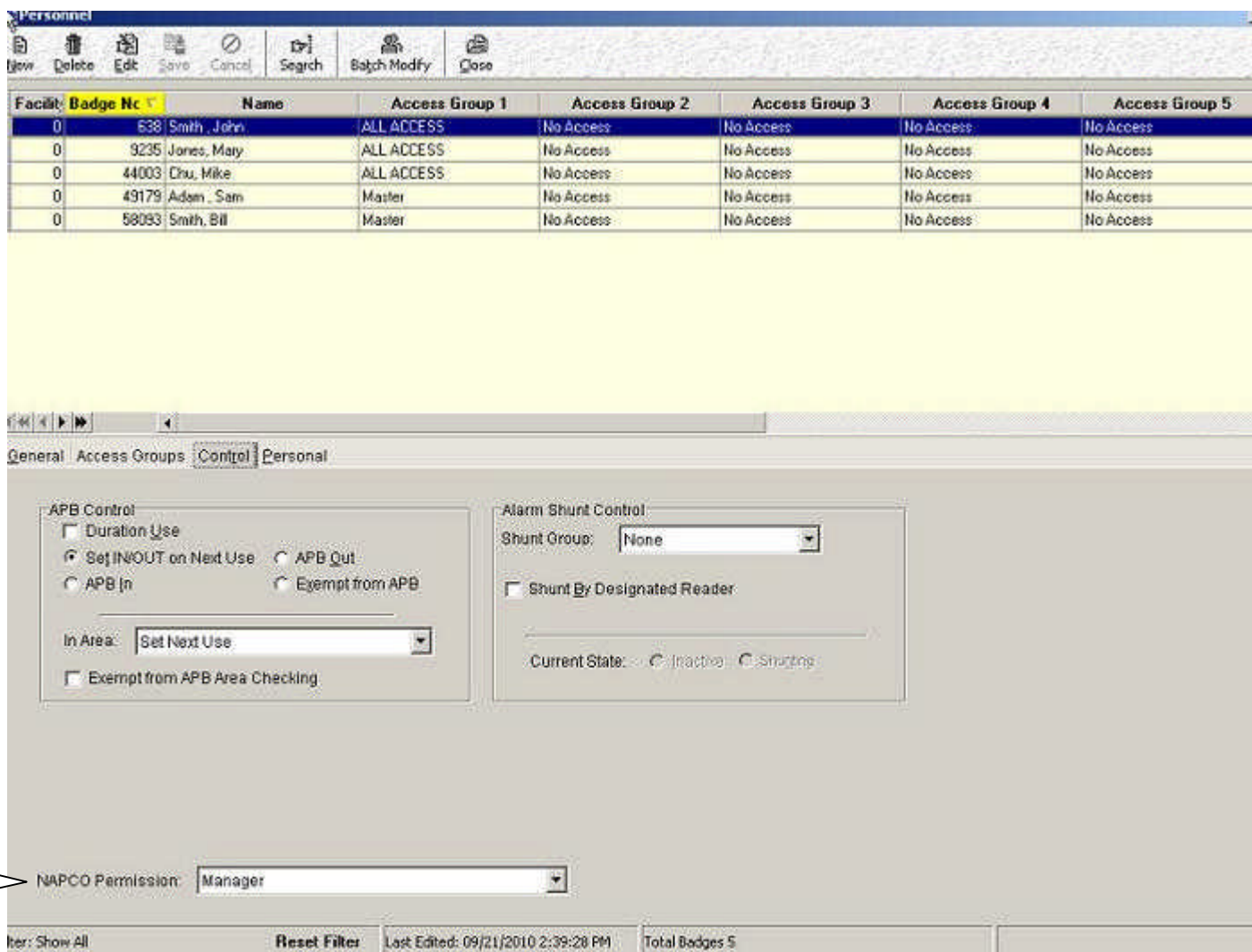


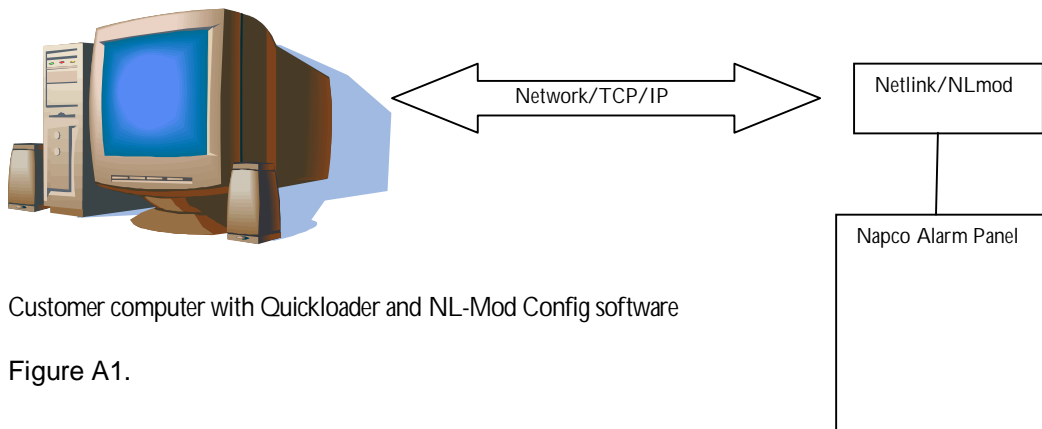
Figure 10.

## APPENDIX A

### Programming the Napco Alarm Panel and NL-Mod utilizing the Napco Quickloader and Napco NL-Mod configuration software

**VERY IMPORTANT: If you are not familiar with the following steps, it is highly recommended to contact Napco Technical Support. They will assist with programming the Napco Alarm Panel and the NL-MOD via TCPIP.**

Note: If possible, it is highly recommended programming the NL-Mod and the Napco Alarm panel using the customer's network configuration. Refer to figure A1.



Customer computer with Quickloader and NL-Mod Config software

Figure A1.

## Programming the NLMOD

- 1) You **MUST** have a STATIC IP address (not DHCP) programmed into the NL-Mod.
- 2) Verify the NL-Mod is powered up and connected to the Ethernet.
- 3) Click **Search** button. Refer to figure A2.

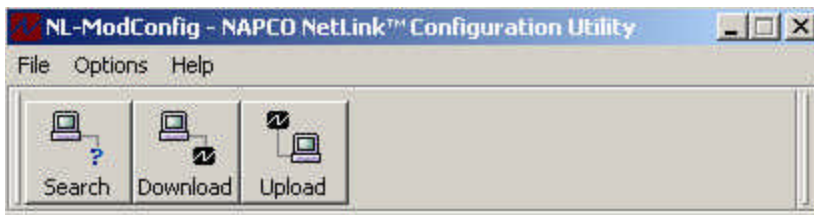


Figure A2.

- 4) The **Search Results** window will display (refer to figure A3). Your NL-Mod should display in this window. If you have multiple unsecured (not programmed) devices on the network, they will also be on the list.

NOTE: If the Search Results does not display your NL-Mod, you might have to do one or more of the following:

- If the NL-Mod has a static IP programmed into it, you must **click “Find Static IP NL-Mod” button** on the Search Results window
- Try **selecting a different network card** if there are multiple cards in the PC
- A proxy or firewall might be prevented the NL-Mod from displaying. You **MUST DISABLE** them
- **RESET NL-Mod** to factory defaults (Remove power, remove jumper JP2, power-up, upon continuous LED flashing (about 1 min), insert jumper JP2 back on

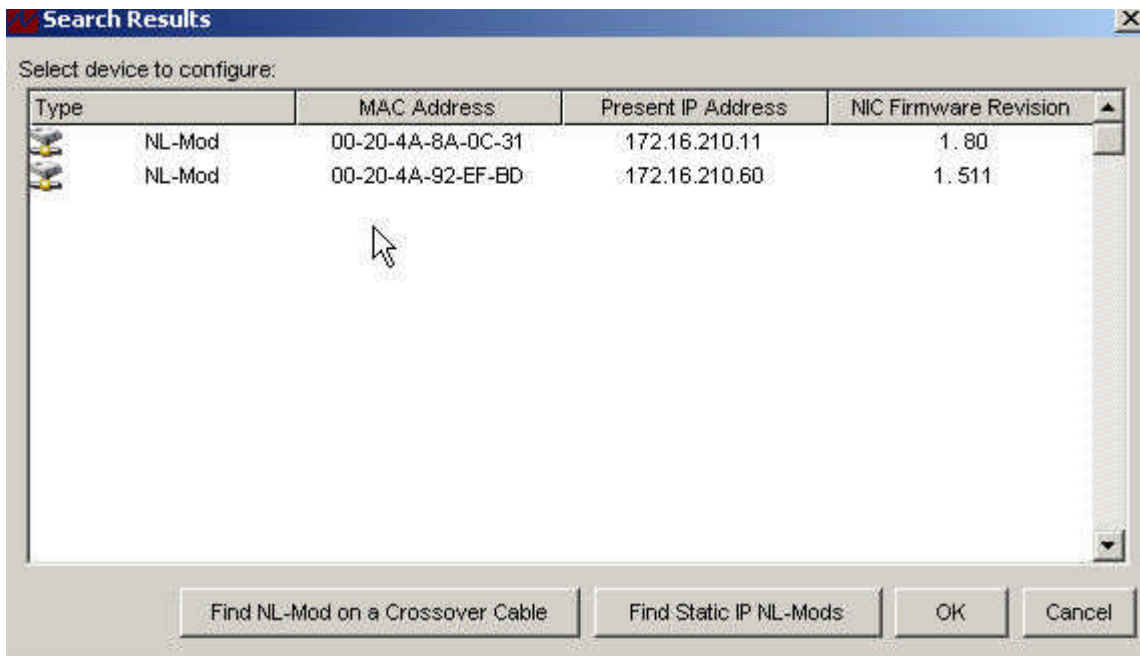


Figure A3.

5) Using the MAC Address as reference, locate your NL-Mod device on the list. **Double-Click** on you NL-Mod. The temporary account will display. The default PC Security Code is 0.0.0, which represents No Code. Refer to figure A4.

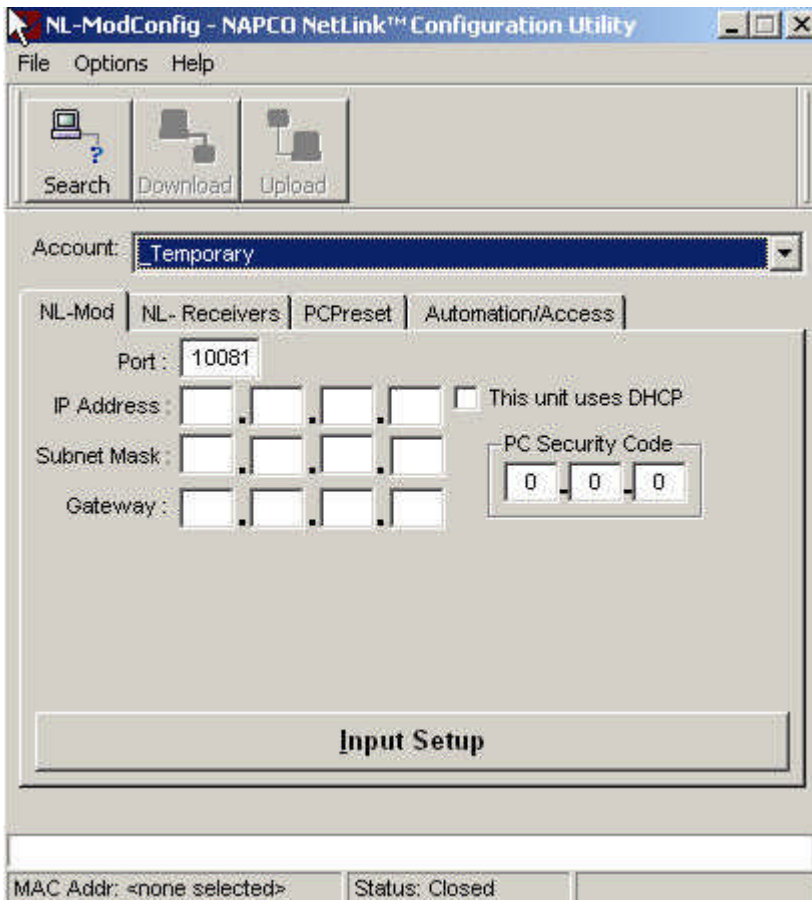


Figure A4.

6) Configure the **Network settings** for the **NLMOD**. Refer to figure A5.

- Click on the **NL-Mod** tab. Refer to figure A5.
- Verify **Port number** is preset at 10081
- If the “This unit uses **DHCP**” is checked, **DESELECT** it
- Enter the **static IP address** to be assigned to the NL-Mod (In this example, we will be using 172.16.210.12)
- Enter the **subnet mask** to be assigned to the NL-Mod (In this example we will be using 255.255.255.0.)
- Enter the **Gateway** to be assigned to the NL-Mod. In this example we will be using 172.16.210.1.
- Assigning a **PC Security Code** is optional. For this example, we will not use one. If it's mandatory you use one, you must also configure in the CA3000 Napco Panels screen (refer to figure 2).  
  
(A **PC Security code** is three – 3 digit numbers ex. 123.0.255)

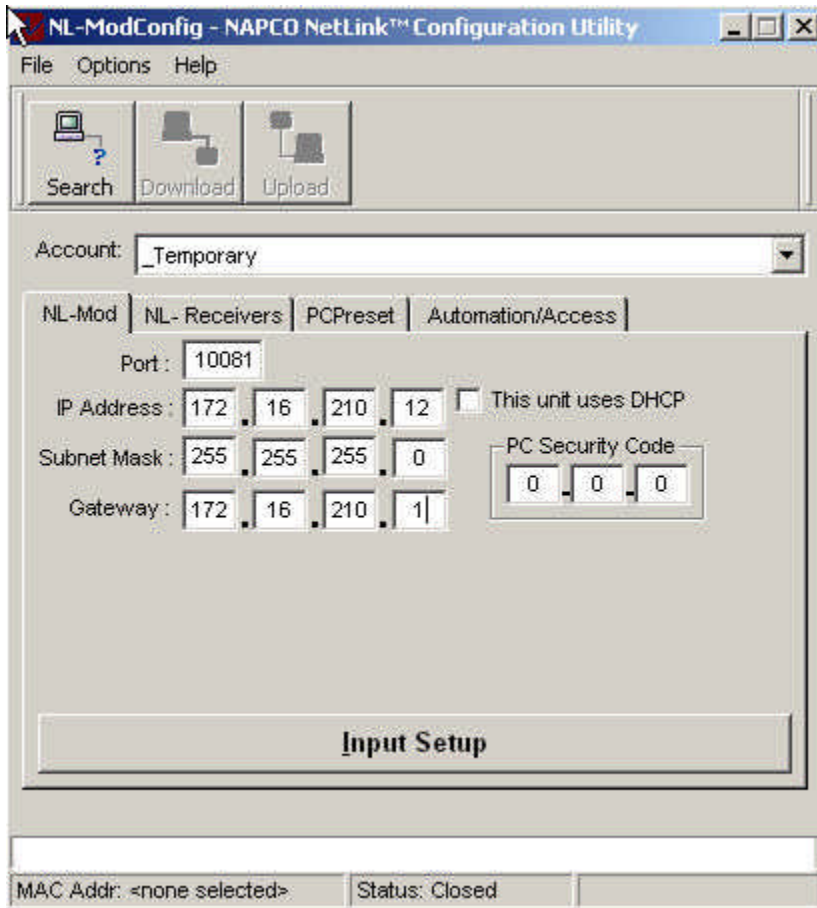


Figure A5.

7) Click on the **Automation/Access** tab. Refer to figure A6.

- Verify **Port number** is preset at 5003
- Enter the **IP address** assigned to the computer that the CA3000 will eventually be installed on.

Note: If this address is not configured for the IP address of the CA3000 host, no Napco Integration events will be received in from the Napco Panel and NL-Mod when integrating with CA3000.

- Select **Enable Real Time Messages to Automatic/Access System**
- Select **Enable Keypad Messages to Automatic/Access System**
- Select **Enable Network ID to Messages to Automatic/Access System**

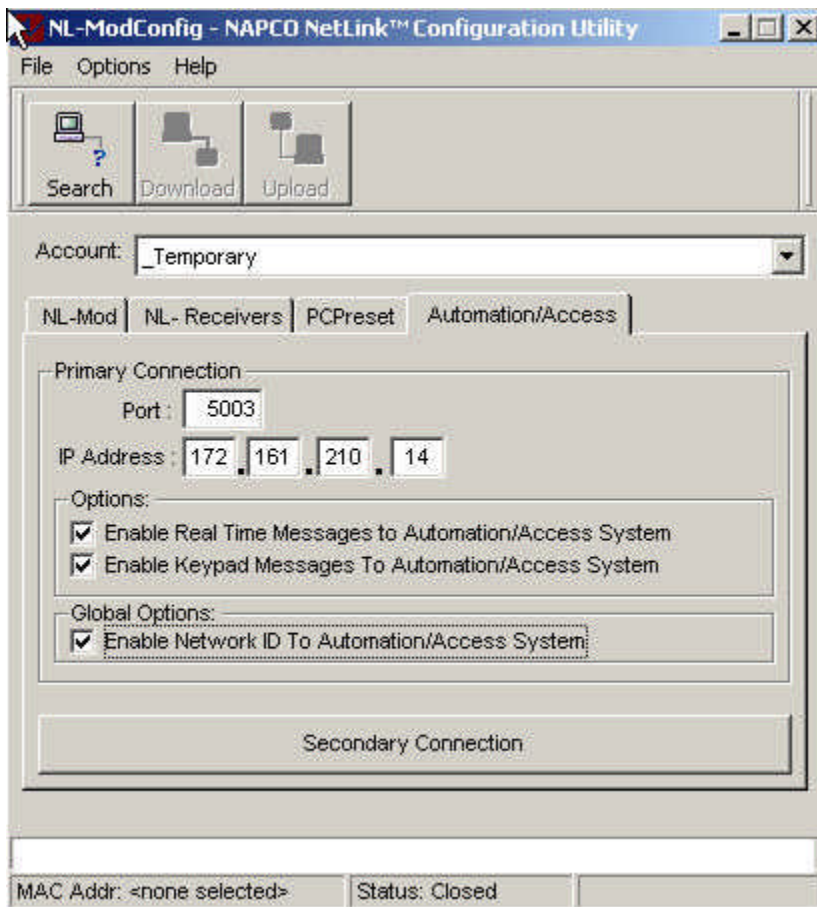


Figure A6.

18) Click **File/Save As**. Refer to figure A7.

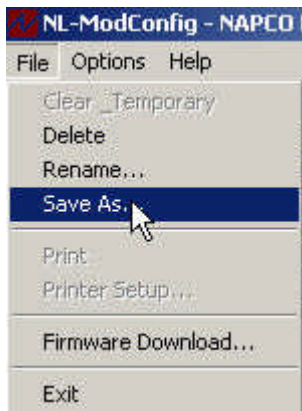


Figure A7.

19) You will be prompted to enter a **New Account Name**. In this example we use “123456” as the new account name. Refer to figure A8.

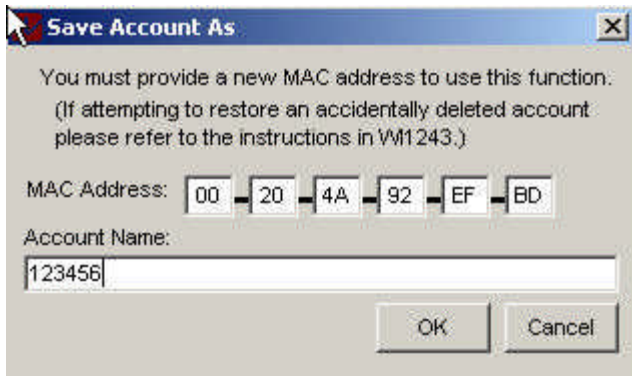


Figure A8.

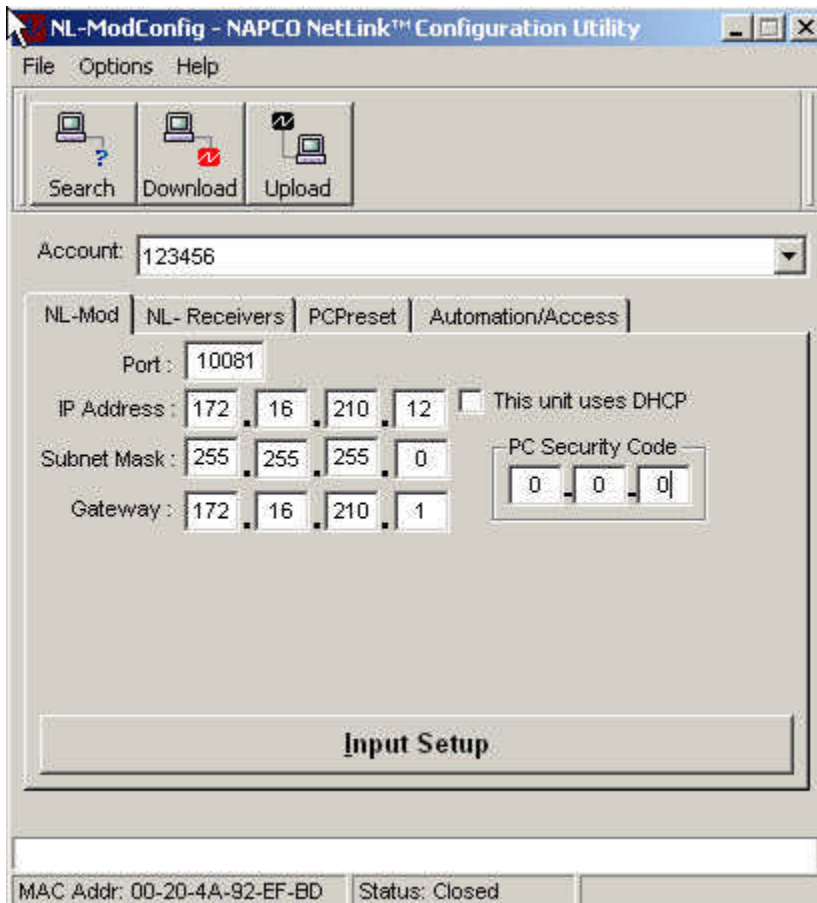


Figure A9.

20) After the new account is saved, verify the NL-Mod tab information is correct. Refer to figure A9.

21) After the new account is saved, you must **download** the information to the NL-Mod. Click **Download**.

## Programming the Quickloader

Note: As previously mentioned, contact Napco Technical Support for assistance with the following steps.

- 1) Program the Napco Alarm Panel through the NL-Mod as per Figure A1. The Napco panel must be programmed for TCP/IP communications. This can be done through the keypad or the Quickloader software.
- 2) After completing the programming of the Quickloader, verify you have a fully functional alarm system. Verify the keypads, areas and zones are all operating properly.

## **APPENDIX B**

### **RECOMMENDED TROUBLESHOOTING STEPS FOR NAPCO INTEGRATION PROBLEMS**

VERY IMPORTANT: You must follow these steps in the following order to isolate the problem. These steps must be performed on the customer's network where the Napco Integration is experiencing problems.

Warning: Window permissions, firewalls and network limitations can cause many hours of wasted troubleshooting time. It is very important to eliminate these items as the problem.

## **Verify the ability to Arm and Disarm a Napco Area through the Napco Keypad**

### **DIAGNOSTIC TEST**

- Arm and Disarm the Alarm panel using the Napco keypad.

### **SYMPTOM**

- The Napco Alarm panel is not arming or disarming through the Napco Keypad.

### **RESOLUTION**

- Verify the programming in the alarm panel is correct using the Napco Quickloader.
- Verify there are no alarms while trying to arm the system with the keypad. If there are any alarms, clear them. Get all zones to the normal condition.

## Verify the Napco Quickloader and the NL-Mod configuration software communicate over the customer network and all programming is correct

Note: Configure as per figure B1.

### DIAGNOSTIC TEST

- Using the Napco Quickloader and Napco NL-Mod configuration software, verify all programming is correct as per the beginning of this document.

### SYMPTOM

- Unable to communicate with the NL-Mod or the Alarm panel over the customer network.

### RESOLUTION

- Verify the CA3000 software is not started while performing these steps.
- Use a network crossover cable to eliminate any routers, switches or firewalls. After switching to a crossover cable, repeat this step. If this corrects the problem, contact the Network Administrator to determine which network component is causing the problem.

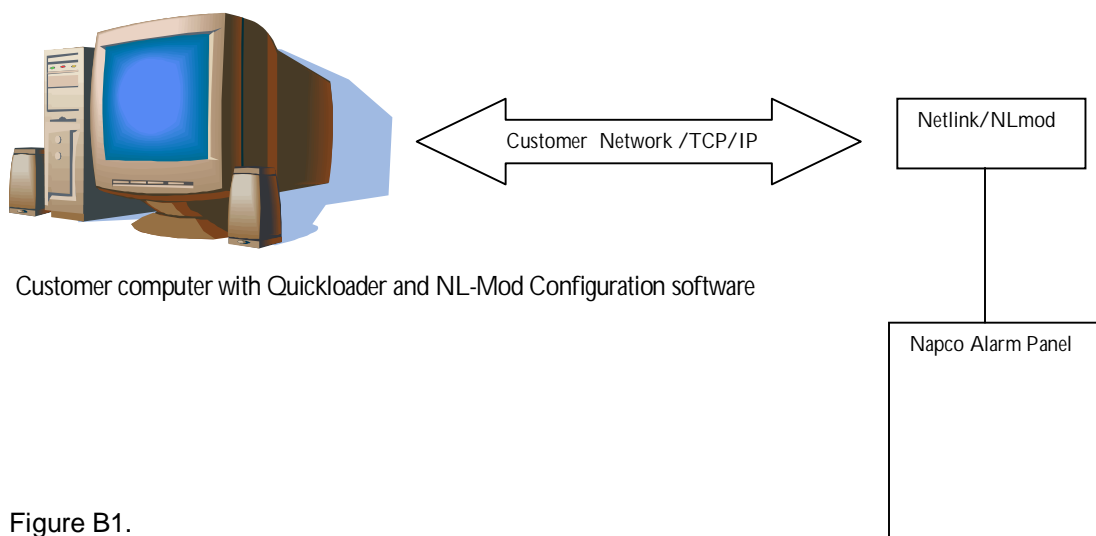


Figure B1.

## Verify the ability to ping the NL-Mod from the CA3000 host

### DIAGNOSTIC TEST

Note: Configure as per figure B2.

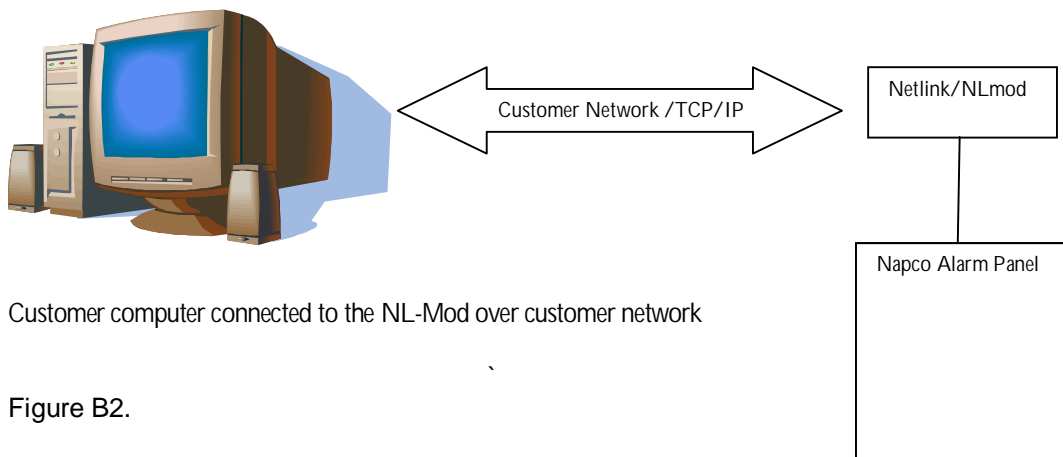
- Ping the static IP address programmed into the NL-Mod from the CardAccess 3000 computer.

### SYMPTOM

- Unable to ping the NL-Mod from the CardAccess 3000 computer.

### RESOLUTION

- Verify all firewalls are disabled.
- Use a network crossover cable as a test from the CA3000 computer to the NL-Mod. This will eliminate any routers, switches and firewalls. If this corrects the problem, contact the Network Administrator to determine which network component is causing the problem.
- Verify the static IP address in the NL-Mod is correct.



Customer computer connected to the NL-Mod over customer network

Figure B2.

## Verify the Napco server is started and the Napco Integration icon is displaying

### DIAGNOSTIC TEST

Note: Configure as per figure B4.

- After the CardAccess 3000 is started, verify the Napco Integration icon displays in the system tray near the computer clock. Refer to figure B3.



Figure B3,

### SYMPTOM

- Napco Integration icon is not displaying in the system tray near the clock.

### RESOLUTION

- Reboot computer and restart the CA3000.
- You **MUST** have **FULL ADMINISTRATOR** rights. If you are logged on to a domain, log off the domain and log on as the Local Administrator. After making changes, restart CardAccess 3000 and verify if the Napco icon displays.
- Verify that the correct Napco Server name is configured. Refer to (pg. 4).
- Verify the Napco Quickloader and the NL-Mod Configuration software is shut down while running CardAccess 3000.

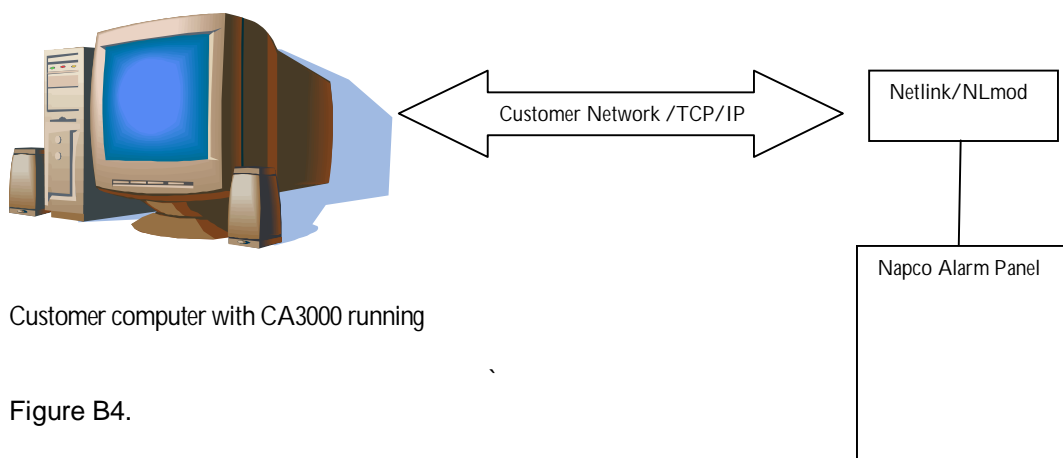


Figure B4.

## Verify Alarm Panel events display on the CardAccess 3000 event grid while arming and disarming using the Napco Keypad

Note: Configure as per figure B5.

### DIAGNOSTIC TEST

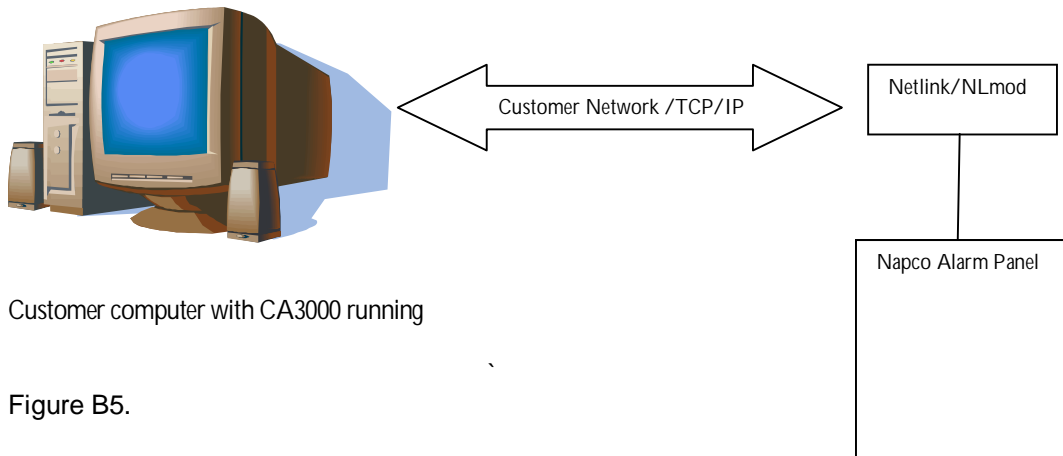
- Generate ALARM PANEL EVENTS by Arming and Disarming the Alarm panel using the Napco keypad. Verify these events display in the CardAccess 3000.

### SYMPTOM

- No ALARM PANEL EVENTS are being received from the NL-Mod and the Napco panel.

### RESOLUTION

- Verify the **Home Automation/Access IP Address** in the NL-Mod points to the computer running CardAccess 3000. Refer to page 18.
- Verify all firewalls are disabled.



## Verify the ability to Manual Arm and Disarm a Napco Area through the CardAccess 3000 manual Napco control icon

Note: This must function properly, before arming and disarming with badges.

### DIAGNOSTIC TEST

- Arm and Disarm an AREA using the Napco manual control icon.

### SYMPTOM

- The Napco Alarm panel is not arming or disarming through the Napco manual control icon.

### RESOLUTION

- Verify the NL-Mod is configured properly and the IP address, subnet mask and gateway are correct. Refer to page 17.
- Verify the **Panel Security Code** is correct. Refer to page 5.
- Verify the **PC Security code** is correct if you are using one. Refer to page 5.
- Verify the panel is configured for the correct Napco Panel Link. Refer to page 10.
- Verify all firewalls are disabled.

## Verify Home Automation alarm panel events display at the CardAccess 3000 after performing a manual Napco control icon

### DIAGNOSTIC TEST

- Generate HOME AUTOMATION ALARM PANEL EVENTS by performing a Napco manual control arm and disarm (as per previous test).

### SYMPTOM

- Alarm panel is arming and disarming fine, but No HOME AUTOMATION ALARM PANEL EVENTS are being received from the NL-Mod and the Napco panel.

### RESOLUTION

- Verify the **Home Automation/Access IP Address** in the NL-Mod points to the computer running CardAccess 3000. Refer to page 18.
- Verify all firewalls are disabled.

## **Verify the ability to ARM Napco panel with a double swipe of a badge**

### **DIAGNOSTIC TEST**

- Arm a Napco panel area with a double swipe of a badge at the reader.

### **SYMPTOM**

- The Napco Alarm panel is not arming after performing a double swipe at the reader.

### **RESOLUTION**

- Verify the panel is configured for the correct Napco Panel Link. Refer to page 10.
- Verify the reader the badge is being swiped at is configured to control the Napco area. Refer to page 11.
- Verify the badge being swiped has the correct Napco permission selected in personnel. The Napco permission must have ARM permissions. Refer to page 12.
- Verify all firewalls are disabled.
- Handshaking between the Continental panel, CardAccess 3000 host and the alarm panel takes seconds. Be very careful to allow enough time for communications to complete after double swiping a badge to arm.

## **Verify the ability to DISARM Napco panel with a single swipe of a badge**

### **DIAGNOSTIC TEST**

- Disarm a Napco panel area with a single swipe of a badge at the reader.

### **SYMPTOM**

- The Napco Alarm panel is not disarming after performing a single swipe at the reader.

### **RESOLUTION**

- Verify the panel is configured for the correct Napco Panel Link. Refer to page 10.
- Verify the reader the badge is being swiped at is configured to control the Napco area. Refer to page 11.
- Verify the badge being swiped has the correct Napco permission selected in personnel. The Napco permission must have DISARM permissions. Refer to page 12.
- Verify all firewalls are disabled.
- Handshaking between the Continental panel, CardAccess 3000 host and the alarm panel takes seconds. Be very careful to allow enough time for communications to complete after single swiping a badge to disarm.

**Perform the following if all the above tests fail to correct the problem.**

- **RESET NL-Mod** to factory defaults (Remove power, remove jumper JP2, power-up, upon continuous LED flashing (about 1 min), insert jumper JP2 back on. Consult Napco Technical support on this.
- **RESET ALARM PANEL** and reload program back in using Quickloader. Consult Napco Technical support on this.
- Completely **remove the NL-Mod Configuration software** and reinstall it. After doing so, you must reconfigure all the settings as per Appendix A.
- Create a new CardAccess 3000 database and reconfigure all Napco Integration programming. Verify if the Napco Integration works correctly with a new database. If it does, this will confirm the problem is definitely in the database.