# Operation/Reference Guide

# MVP-7500/8400

## 7.5" & 8.4" Modero® ViewPoint® Touch Panels

Touch Panels

Last Revised: 2/18/2013

# AMX Limited Warranty and Disclaimer

This Limited Warranty and Disclaimer extends only to products purchased directly from AMX or an AMX Authorized Partner which include AMX Dealers, Distributors, VIP's or other AMX authorized entity.

AMX warrants its products to be free of defects in material and workmanship under normal use for three (3) years from the date of purchase, with the following exceptions:

- Electroluminescent and LCD Control Panels are warranted for three (3) years, except for the display and touch overlay components are warranted for a period of one (1) year.
- Disk drive mechanisms, pan/tilt heads, power supplies, and MX Series products are warranted for a period of one (1) year.
- AMX lighting products are guaranteed to switch on and off any load that is properly connected to our lighting products, as long as the AMX lighting products are under warranty. AMX also guarantees the control of dimmable loads that are properly connected to our lighting products. The dimming performance or quality there of is not guaranteed, impart due to the random combinations of dimmers, lamps and ballasts or transformers.
- AMX software is warranted for a period of ninety (90) days.
- Batteries and incandescent lamps are not covered under the warranty.
- AMX AutoPatch Epica, Modula, Modula Series4, Modula CatPro Series and 8Y-3000 product models will be free of defects in materials and manufacture at the time of sale and will remain in good working order for a period of three (3) years following the date of the original sales invoice from AMX. The three-year warranty period will be extended to the life of the product (Limited Lifetime Warranty) if the warranty card is filled out by the dealer and/or end user and returned to AMX so that AMX receives it within thirty (30) days of the installation of equipment but no later than six (6) months from original AMX sales invoice date. The life of the product extends until five (5) years after AMX ceases manufacturing the product model. The Limited Lifetime Warranty applies to products in their original installation only. If a product is moved to a different installation, the Limited Lifetime Warranty will no longer apply, and the product warranty will instead be the three (3) year Limited Warranty.

All products returned to AMX require a Return Material Authorization (RMA) number. The RMA number is obtained from the AMX RMA Department. The RMA number must be clearly marked on the outside of each box. The RMA is valid for a 30-day period. After the 30-day period the RMA will be cancelled. Any shipments received not consistent with the RMA, or after the RMA is cancelled, will be refused. AMX is not responsible for products returned without a valid RMA number.

AMX is not liable for any damages caused by its products or for the failure of its products to perform. This includes any lost profits, lost savings, incidental damages, or consequential damages. AMX is not liable for any claim made by a third party or by an AMX Authorized Partner for a third party.

This Limited Warranty does not apply to (a) any AMX product that has been modified, altered or repaired by an unauthorized agent or improperly transported, stored, installed, used, or maintained; (b) damage caused by acts of nature, including flood, erosion, or earthquake; (c) damage caused by a sustained low or high voltage situation or by a low or high voltage disturbance, including brownouts, sags, spikes, or power outages; or (d) damage caused by war, vandalism, theft, depletion, or obsolescence.

This limitation of liability applies whether damages are sought, or a claim is made, under this warranty or as a tort claim (including negligence and strict product liability), a contract claim, or any other claim. This limitation of liability cannot be waived or amended by any person. This limitation of liability will be effective even if AMX or an authorized representative of AMX has been advised of the possibility of any such damages. This limitation of liability, however, will not apply to claims for personal injury.

Some states do not allow a limitation of how long an implied warranty last. Some states do not allow the limitation or exclusion of incidental or consequential damages for consumer products. In such states, the limitation or exclusion of the Limited Warranty may not apply. This Limited Warranty gives the owner specific legal rights. The owner may also have other rights that vary from state to state. The owner is advised to consult applicable state laws for full determination of rights.

EXCEPT AS EXPRESSLY SET FORTH IN THIS WARRANTY, AMX MAKES NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. AMX EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED TO THE TERMS OF THIS LIMITED WARRANTY. EXCEPT AS OTHERWISE LIMITED BY APPLICABLE LAW, AMX RESERVES THE RIGHT TO MODIFY OR DISCONTINUE DESIGNS, SPECIFICATIONS, WARRANTIES, PRICES, AND POLICIES WITHOUT NOTICE.

# AMX Software License and Warranty Agreement

- LICENSE GRANT. AMX grants to Licensee the non-exclusive right to use the AMX Software in the manner described in this License. The AMX Software is licensed, not sold. This license does not grant Licensee the right to create derivative works of the AMX Software. The AMX Software consists of generally available programming and development software, product documentation, sample applications, tools and utilities, and miscellaneous technical information. Please refer to the README.TXT file on the compact disc or download for further information regarding the components of the AMX Software. The AMX Software is subject to restrictions on distribution described in this License Agreement. AMX Dealer, Distributor, VIP or other AMX authorized entity shall not, and shall not permit any other person to, disclose, display, loan, publish, transfer (whether by sale, assignment, exchange, gift, operation of law or otherwise), license, sublicense, copy, or otherwise disseminate the AMX Software. Licensee may not reverse engineer, decompile, or disassemble the AMX Software.
- ACKNOWLEDGEMENT. You hereby acknowledge that you are an authorized AMX dealer, distributor, VIP or other AMX authorized entity in good standing and have the right to enter into and be bound by the terms of this Agreement.
- INTELLECTUAL PROPERTY. The AMX Software is owned by AMX and is protected by United States copyright laws, patent laws, international treaty provisions, and/or state of Texas trade secret laws. Licensee may make copies of the AMX Software solely for backup or archival purposes. Licensee may not copy the written materials accompanying the AMX Software.
- TERMINATION. AMX RESERVES THE RIGHT, IN ITS SOLE DISCRETION, TO TERMINATE THIS LICENSE FOR ANY REASON UPON WRITTEN NOTICE TO LICENSEE. In the event that AMX terminates this License, the Licensee shall return or destroy all originals and copies of the AMX Software to AMX and certify in writing that all originals and copies have been returned or destroyed.
- PRE-RELEASE CODE. Portions of the AMX Software may, from time to time, as identified in the AMX Software, include PRE-RELEASE CODE and such code may not be at the level of performance, compatibility and functionality of the GA code. The PRE-RELEASE CODE may not operate correctly and may be substantially modified prior to final release or certain features may not be generally released. AMX is not obligated to make or support any PRE-RELEASE CODE. ALL PRE-RELEASE CODE IS PROVIDED "AS IS" WITH NO WARRANTIES.
- LIMITED WARRANTY. AMX warrants that the AMX Software (other than pre-release code) will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt. AMX DISCLAIMS ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO THE AMX SOFTWARE. THIS LIMITED WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS. Any supplements or updates to the AMX SOFTWARE, including without limitation, any (if any) service packs or hot fixes provided to Licensee after the expiration of the ninety (90) day Limited Warranty period are not covered by any warranty or condition, express, implied or statutory.
- LICENSEE REMEDIES. AMX's entire liability and Licensee's exclusive remedy shall be repair or replacement of the AMX Software that does not meet AMX's Limited Warranty and which is returned to AMX in accordance with AMX's current return policy. This Limited Warranty is void if failure of the AMX Software has resulted from accident, abuse, or misapplication. Any replacement AMX Software will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside the United States, these remedies may not available. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL AMX BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THIS AMX SOFTWARE, EVEN IF AMX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO LICENSEE.
- U.S. GOVERNMENT RESTRICTED RIGHTS. The AMX Software is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph ©(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs ©(1) and (2) of the Commercial Computer Software Restricted Rights at 48 CFR 52.227-19, as applicable.
- SOFTWARE AND OTHER MATERIALS FROM AMX.COM MAY BE SUBJECT TO EXPORT CONTROL. The United States Export Control laws prohibit the export of certain technical data and software to certain territories. No software from this Site may be downloaded or exported (i) into (or to a national or resident of) Cuba, Iraq, Libya, North Korea, Iran, Syria, or any other country to which the United States has embargoed goods; or (ii) anyone on the United States Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders. AMX does not authorize the downloading or exporting of any software or technical data from this site to any jurisdiction prohibited by the United States Export Laws.

**This Agreement replaces and supersedes all previous AMX Software License Agreements and is governed by the laws of the State of Texas, and all disputes will be resolved in the courts in Collin County, Texas, USA. For any questions concerning this Agreement, or to contact AMX for any reason, please write: AMX License and Warranty Department, 3000 Research Drive, Richardson, TX 75082.**

# Table of Contents

# MVP Modero Viewpoint Wireless Touch Panels

## Overview

The MVP-7500 (7.5") and MVP-8400 (8.4") Modero Viewpoint Wireless Touch Panels (FIG. 1) are 802.11-based wireless handheld G4 touch panels, pre-installed with an 802.11 Wi-Fi Interface Card to communicate with a NetLinx Master via a standard 802.11b/g Wireless Access Point.


**FIG. 1** MVP-7500 and MVP-8400 Touch Panels

- Previous 802.11b versions of MVP panels are field upgradeable to 802.11g communication via the installation of the NXA-WC8011GCF Wi-Fi Card Kit (**FG2255-07**).
- MVP panels feature nine programmable external pushbuttons and two programmable LEDs, and support AMX G4 graphics technology, making them compatible with AMX's TPDesign4 Touch Panel Design program.
- MVP panels utilize two IR frequencies (38 KHz and 455 KHz) as well as 2 additional user-defined IR libraries, on 4 IR ports.
- MVP panels feature programmable firmware that can be upgraded via either the wireless interface card or the mini-USB port. MVP panels utilize unique firmware kit files: the MVP-7500 can be upgraded via the "5965-01.kit" file, while the MVP-8400 can be upgraded via the "5965-02.kit" file.
- MVP panels support *AMX Computer Control*, which enables remote viewing and control of any networked computer directly from the panel. This gives the user the ability to launch digital music from a PC, cruise the Internet, check and respond to E-mail, open software files, and launch applications.
- MVP panels come equipped with a battery and power supply (see specifications).

Optional AMX accessory solutions for the MVPs include

- MVP-TDS Table Top Docking Station (see the *MVP-TDS Table Top Docking Station Operation/Reference Guide* for details).
- MVP-WDS Wall/Flush Mount Docking Station-Black/Silver (see the *MVP-WDS Wall Docking Station Operation/Reference Guide* for details).
- MVP-KS Kickstand (see the *MVP-KS Kickstand Operation/Reference Guide* for details).

## MVP Specifications

- The MVP-7500 (FG5965-01) utilizes a 7.5" Color Passive LCD to display a 640 x 480 pixel image with 4096 colors.
- The MVP-8400 panel (FG5965-02) utilizes an 8.4" Color Active LCD to display an 800 x 600 pixel resolution using 256K colors.

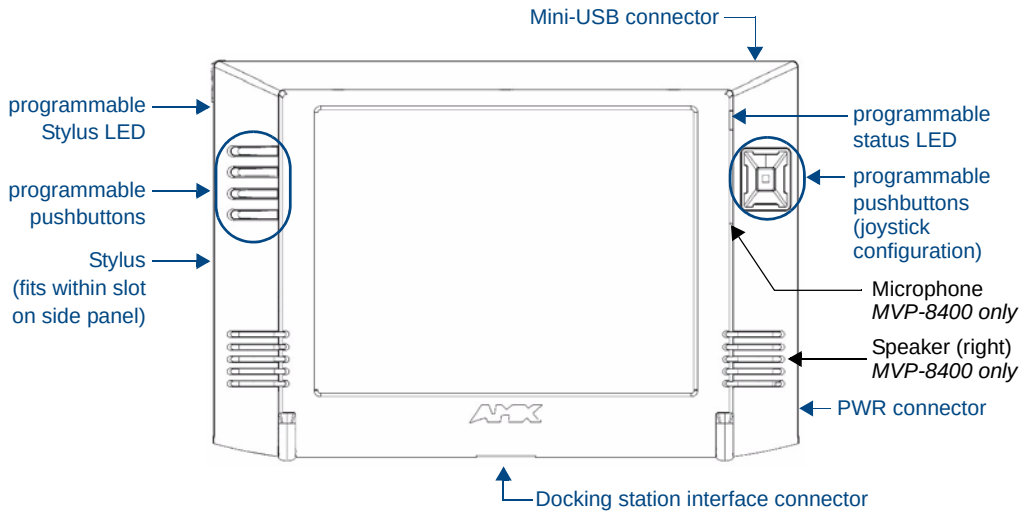



**FIG. 2** MVP Touch Panels

| MVP Specifications | |
|---|---|
| **Models:** | • MVP-7500<br>• MVP-8400 |
| **Dimensions (HWD):** | • 7.09" x 10.47" x 1.47" (18.00 cm x 26.60 cm x 3.73 cm) |
| **Power Requirements:** | **Without Charging:**<br>MVP-7500:<br>• Constant current draw: 1.0 A @ 12 VDC<br>• Startup current draw: 1.5 A @ 12 VDC<br>MVP-8400:<br>• Constant current draw: 1.2 A @ 12 VDC<br>• Startup current draw: 1.8 A @ 12 VDC |
| | **While Charging:**<br>MVP-7500:<br>• Constant current draw: 3.0 A @ 12 VDC<br>• Startup current draw: 3.6 A @ 12 VDC<br>MVP-8400:<br>• Constant current draw: 3.2 A @ 12 VDC<br>• Startup current draw: 3.8 A @ 12 VDC<br>• If MVP panel is mounted onto a TDS or WDS, add 0.1 A to the above figures. |
| **Power Modes:** | • ON: Panel is fully functional.<br>• STANDBY: Panel uses low power, the LCD/backlight is shutdown, LEDs still function. ***Panel resumes the ON mode in ~ 1 second.***<br>• OFF: On-board programs not running, touch screen still powered, LED not functional. ***Panel resumes the ON mode in ~ 30 seconds.*** |
| **Battery Duration: (per battery)** | • Four hours of normal use (25% On state, 25% Standby, and 50% Off).<br>• Two hours of continuous use. |
| **Memory (factory default):** | • 64 MB SDRAM<br>• 64 MB Compact Flash (upgradeable to 1 GB - factory programmed) |
| **Weight:** | 1.85 lbs (0.84 kg)<br>• with 1 battery: 2.25 lbs (1.02 kg)<br>• with 2 batteries: 2.65 lbs (1.20 kg) |

| MVP Specifications (Cont.) | |
|---|---|
| **MVP-7500 LCD Specifications:** | • Aspect ratio: 4 x 3<br>• Brightness (luminance): 120 cd/$m^2$<br>• Channel transparency: 8-bit Alpha blending<br>• Contrast ratio: 20:1<br>• Display colors: 4096 colors (12-bit color depth)<br>• Dot/pixel pitch: 0.23 mm<br>• Panel type: TFT Color Passive-Matrix<br>• Screen resolution: 640 x 480 pixels (HV) @ 60 Hz frame frequency<br>• Viewing angles (vertical): + 17° / - 17° (from center) |
| **MVP-8400 LCD Specifications:** | • Aspect ratio: 4 x 3<br>• Brightness (luminance): 180 cd/$m^2$<br>• Channel transparency: 8-bit Alpha blending<br>• Contrast ratio: 350:1<br>• Display colors: 256K colors (18-bit color depth)<br>• Dot/pixel pitch: 0.21 mm<br>• Panel type: TFT Color Active-Matrix<br>• Screen resolution: 800 x 600 pixels (HV) @ 60 Hz frame frequency<br>• Viewing angles (vertical): + 60° / - 40° (from center) |
| **Active Screen Area:** | • 6.71" x 5.03" (17.04cm x 12.78cm) |
| **External Components:** | |
| Docking station interface connector: | Metallic strip connector located on the bottom panel provides communication and power between the panel and the optional docking stations. |
| LEDs: | Two sets of NetLinx programmable LEDs (supporting On, Off, and Blink). Default blink patterns:<br>- Stylus LED: Blink = *Batteries charging*, On = *Batteries charged*.<br>- Front panel LED: Blink = *Panel booting,* On = *Panel operating properly*. |
| Mini-USB connector: | 5-pin mini-USB connector for programming, firmware update, and file transfer. |
| Power connector: | • 2.1mm barrel-style power jack, for use with the included PS4.4 power supply. |
| Stylus slot: | • Illuminated slot where the included stylus is stored, located on the left side of the MVP. |
| External Buttons: | • Nine programmable pushbuttons (four located on the left of the LCD and five located on the right in a joystick configuration). |
| **Internal Components:** | |
| Wireless Interface card: | Provides 802.11 (CF Type I) wireless connectivity between the panel and a Wireless Access Point (such as the NXA-WAP200G). |
| IR Emitters: | Transmit IR over 20 feet (6.10 m). |
| Internal buzzer: | Emits a Piezo electric tone (MVP-7500 only). |
| Internal speakers: | One speaker for stereo output (MVP-8400 only). |
| Internal microphone | For use with the intercom feature (MVP-8400 only). |
| Battery compartment: | Houses up to 2 MVP-BP Power Packs. |
| Button Assignments: | Button assignments can only be adjusted in TPD4 and not on the panels.<br>• Button channel range: 1 - 4000 button push and feedback (per address port)<br>• Button variable text range: 1 - 4000 (per address port)<br>• Button states range: 1 - 256 (General Button; 1 = Off State, 2 = On State)<br>• Level range: 1 - 600 (default level value 0-255, can be set up to 1-65535)<br>• Address port range: 1 - 100 |

| MVP Specifications (Cont.) | |
|---|---|
| Operating / Storage Environment: | • Operating Temperature: 0° C (32° F) to 40° C (104° F)<br>• Operating Humidity: 20% - 85% RH<br>• Storage Temperature: -20° C (-4° F) to 60° C (140° F)<br>• Storage Humidity: 5% - 85% RH |
| **Certifications:** | • FCC Part 15 Class B and CE |
| **Included Accessories:** | • MVP-BP Power Pack (**FG5965-20**): 1 with MVP-7500, 2 with MVP-8400<br>• 80211xCF Wireless Interface Compact Flash card (Type 1) - pre-installed<br>• PS4.4 Power Supply (**FG423-44**)<br>• Stylus |
| **Other AMX Equipment:** | • CB-MVPWDS Conduit Box (**FG037-10**)<br>• CC-USB (Type A) to Mini-B 5-Wire programming cable (**FG10-5965**)<br>• MVP-BP Power Pack (additional/spare) (**FG5965-20**)<br>• MVP-KS Kickstand (**FG5965-12**)<br>• MVP-STYLUS three pack (**FG5965-30**)<br>• MVP-TDS Table Top Docking Station (**FG5965-10**)<br>• MVP-WDS Wall/Flush Mount Docking Station: Black (**FG5965-11**) / Silver (**FG5965-21**)<br>• MVP-WDS-SK Silver Conversion Kit for MVP-WDS (**FG5965-22**)<br>• NXA-WC80211GCF 802.11g Wireless Compact Flash Card Upgrade Kit (**FG2255-07**)<br>• Upgrade Compact Flash (factory programmed with firmware):<br>MVP-7500:<br>NXA-75CF128M - 128 MB compact flash card (**FG2116-55**)<br>NXA-75CF256M - 256 MB compact flash card (**FG2116-56**)<br>NXA-75CF512M - 512 MB compact flash card (**FG2116-57**)<br>NXA-75CF1GB - 1 GB compact flash card (**FG2116-58**)<br>MVP-8400:<br>NXA-84CF128M - 128 MB compact flash card (**FG2116-50**)<br>NXA-84CF256M - 256 MB compact flash card (**FG2116-51**)<br>NXA-84CF512M - 512 MB compact flash card (**FG2116-52**)<br>NXA-84CF1GB - 1 GB compact flash card (**FG2116-53**) |

# MVP-BP Power Pack

## Overview

The MVP-BP Power Pack (**FG5965-20**) is a rechargeable Lithium-Ion battery used to provide power to the MVP touch panels.

- One MVP-BP is included with each MVP-7500 touch panel.
- Two MVP-BPs are included with each MVP-8400 touch panel.


**FIG. 3** MVP-BP Power Pack

MVP-BPs can be charged with either a Table Top Docking Station (MVP-TDS), Wall/Flush Mount Docking Station (MVP-WDS), or MVP panel itself. Extra MVP-BP Power Packs can be purchased separately.

### MVP-BP Specifications

| MVP-BP Specifications | |
|---|---|
| **Dimensions (HWD):** | 0.48" x 1.52" x 8.65" (1.23 cm x 3.86 cm x 21.97 cm) |
| **Power (Voltage):** | 7.2 Volts (nominal) |
| **Weight:** | 0.40 lbs (0.18 kg) |
| **Charge Capacity:** | 3600mAh |
| **Operating/Storage Environments:** | • Operating Temperature: 0° C (32° F) to 40° C (104° F)<br>• Operating Humidity: 20% - 85% RH<br>• Storage Temperature: -20° C (-4° F) to 60° C (140° F)<br>• Storage Humidity: 5% - 85% RH |

## Installing MVP-BP Batteries

1. Disconnect any cables, and place the MVP face down to expose the battery compartment.
2. Press down on the traction grooves to slide the battery compartment cover (away from the metal plate), to open the battery compartment.
3. Insert the MVP-BP(s) so that the connector makes contact with the battery pins at the end of the battery slot as shown in FIG. 4.

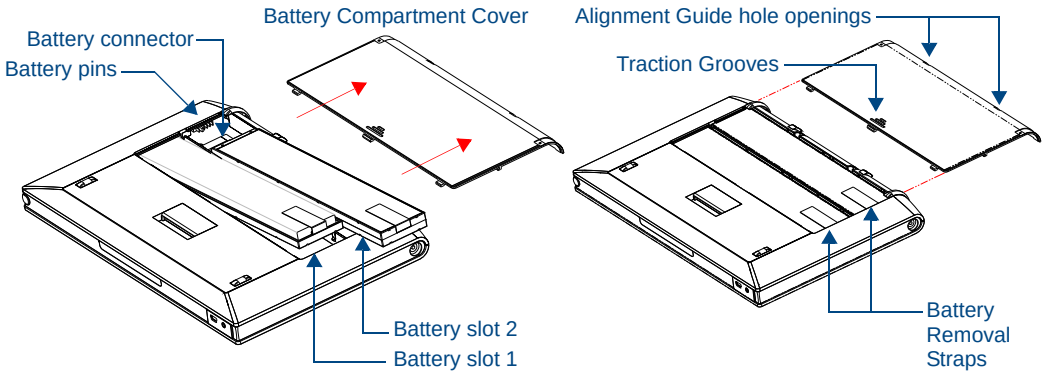



**FIG. 4** Installing MVP-BP batteries into the MVP battery slots

NOTE

*If you are only using one battery, use Battery Slot #1.*

**4.** To replace the battery compartment cover, use the alignment guide holes to align the cover with the edges of the battery compartment, and slide it back into place until it snaps shut.

# NXA-CFSP Compact Flash

## Overview

Every MVP panel is shipped with a 64 MB Compact Flash card.

## Compact Flash Card - Security

All security user names and passwords (for the docking station) are stored in the Compact Flash card. After installing the Compact Flash card upgrade, all security user names and passwords need to be re-entered to enable security. For this reason, it is recommended that you upgrade the card prior to setting up the security information for the docking station.

The NXA-CFSP Compact Flash card is factory programmed with panel firmware and can be upgraded up to 1GB:

| Optional Compact Flash Upgrades | |
|---|---|
| • NXA-CFSP128M - 128 MB Compact Flash card | (**FG2116-36**) |
| • NXA-CFSP256M - 256 MB Compact Flash card | (**FG2116-37**) |
| • NXA-CFSP512M - 512 MB Compact Flash card | (**FG2116-38**) |
| • NXA-CFSP1G - 1 GB Compact Flash card | (**FG2116-39**) |

## Installing the NXA-CFSP Compact Flash Card


*Batteries should be removed prior to upgrading the Compact Flash card.*

### Accessing the MVP's Internal Components

1. Remove all connectors, remove power and remove batteries.
2. Remove the two housing screws (FIG. 5).
3. Grasp the bottom rim of the rear housing just above the MVP interface connector, and carefully pull the bottom rim away from the IR Emitter and up, to expose the internal components.
4. Remove the trim from the top rim of the circuit board (FIG. 5).

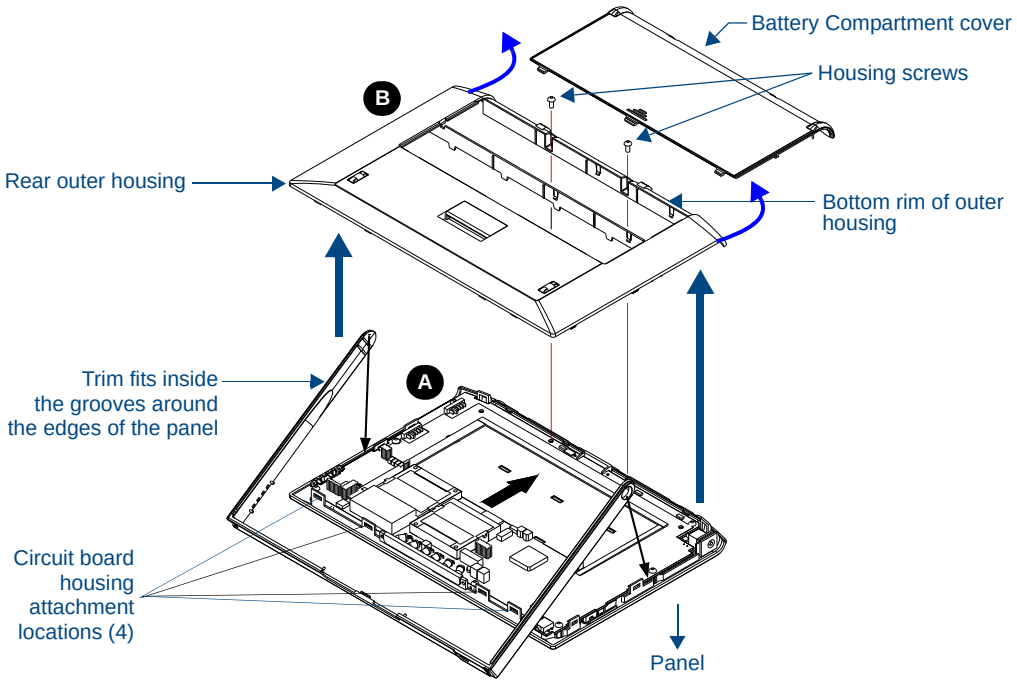



**FIG. 5** Removing the MVP enclosure (housing)

## Removing the Installed Card

1. Discharge any static electricity from your body by touching a grounded metal object and then locate the card slot on the main circuit board (FIG. 6).
2. Place the circuit board on a flat level surface so that the IR Emitters are pointing away from you (FIG. 6).
3. Insert the tip of a grounded flat-head screwdriver into one of the card removal grooves (located on either side of the existing card), and gently pry it out of the slot (FIG. 7). Repeat this process on the opposite card removal groove. *This alternating action causes the card to "wiggle" away from the on-board connector pins.*
4. Slip your finger into the gap between the card and the circuit board and firmly grab the card by its sides, then carefully pull it up and out of the slot. An angular removal of the card is required because one of the housing's latch attachments blocks the slot opening.

NOTE

*use care when pulling up on the card.*

## Installing the Compact Flash Upgrade Card

1. Discharge any static electricity from your body by touching a grounded metal object and then locate the memory card slot on the main board (**A** in FIG. 6).

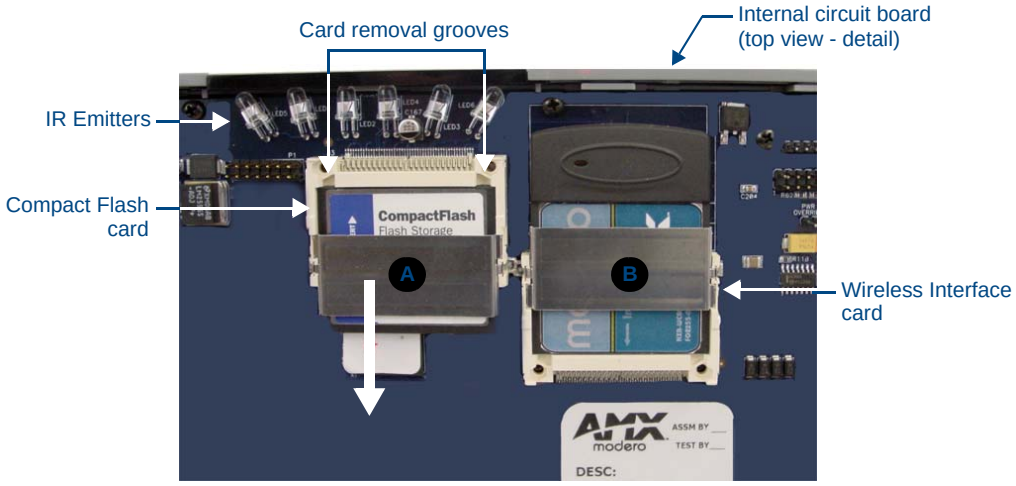



**FIG. 6** Location and orientation of the Compact Flash cards (both MVP panels)

2. Place the circuit board on a flat level surface so that the IR Emitters are pointing away from you (FIG. 6).
3. Insert the tip of a grounded flat-head screwdriver into one of the card removal grooves (located on either side of the existing Compact Flash card), and gently pry it out of the slot (FIG. 7). Repeat this process on the opposite card removal groove. *This alternating action causes the pre-existing card to "wiggle" away from the on-board connector pins.*
4. Slip your finger into the opening (between the connector pins and the card resulting from step 3) and push the card out.
5. Finish the process by firmly gripping the exposed sides of the card and pulling it out (FIG. 7). **USE CARE WHEN HANDLING THE CARD.**

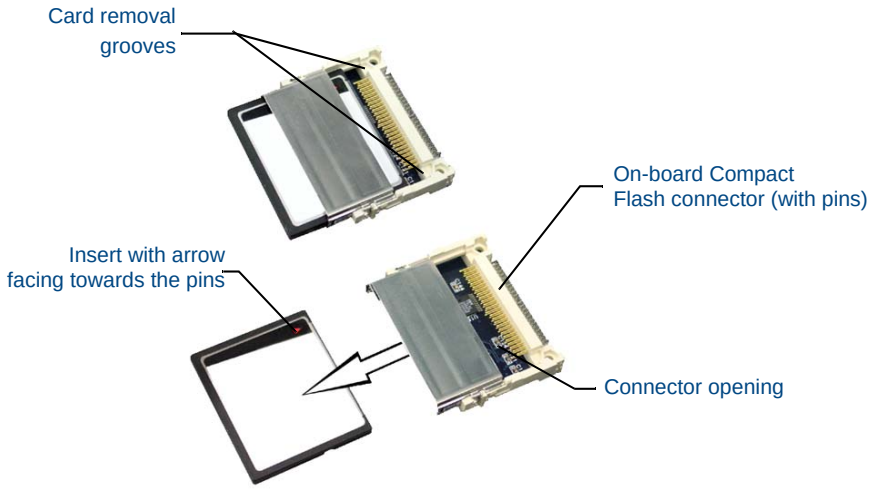



**FIG. 7** Removing/installing a Compact Flash Memory card

6. Insert the new card firmly into the slot opening connector (FIG. 7) until the contact pins are completely inside the card and securely attached to the pin sockets.

NOTE

*Any new Compact Flash card upgrade is detected by the panel only after the unit cycles power.*

# Wireless Interface Cards

## 802.11b Wireless Interface Card

MVP panels can connect to a wireless network using the 802.11b Wireless Interface Card (**70-5965-02**), pre-installed in MVP touch panel models. The 802.11b Wireless Interface Card is a 2.4 GHz Direct Sequence Spread Spectrum (DSSS) 802.11b 11M wireless PC card, with detachable antenna.

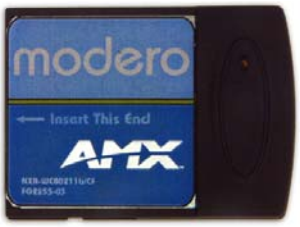



**FIG. 8** 802.11b Wireless Interface Card

The wireless interface card works with 802.11b/g Wireless Access Points, such as the NXA-WAP200G.

NOTE

*The NXA-WAP200G uses a default SSID of **AMX**.*

Follow your particular WAP's instruction manual for setup procedures.

### Specifications

| 802.11b Wireless Interface Card Specifications | |
|---|---|
| **Dimensions (HWD):** | • 2.07" x 1.68" x 0.21" (52.56 mm x 42.80 mm x 5.57 mm) |
| **Weight:** | • 13.61 grams (0.030 lbs) |
| **Features:** | • Wired Equivalent Privacy (WEP) 64-bit and 128-bit data encryption<br>• Diversity Antenna Connectors automatically select the best available signal<br>• Supports infrastructure (communications to wired networks via Access Points), and roaming (standard IEEE 802.11b compliant) |
| **Antenna:** | • 2, Ceramic (Diversity Supported) |
| **Host Interface:** | • Compact Flash Type I |
| **Interoperability:** | • Interoperable with Wi-Fi (WECA) certified products |
| **LED Indicators:** | • Power / Link activity |
| **Modulation:** | • DSSS, DBSK, DQSK, CCK |
| **Network Standard:** | • IEEE 802.11b |
| **Number of Channels:** | • 14 |
| **Operating Voltage:** | • 5 / 3.3 V |
| **Operating Channels:** | • 11 Channels (USA, Canada)<br>• 13 Channels (Europe)<br>• 14 Channels (Japan)<br>• 4 Channels (France) |
| **Operating Environment:** | • Temperature: 0°C ~ 70°C (non-operating) and -15 ~ 80°C (storage)<br>• Humidity (non-condensing): 5% ~ 95% RH |
| **Power Consumption:** | • TX power consumption: ≤ 265 mA<br>• RX power consumption: ≤ 165 mA<br>• Sleep Mode: 2 mA - 15 mA |
| **Radio Data Rate:** | • 1Mbps, 2Mbps, 5.5Mbps, 11Mbps, Auto Rate |

| 802.11b Wireless Interface Card Specifications (Cont.) | |
|---|---|
| **Receive Sensitivity:** | • @PER < 8%<br>11 Mbps: -83 dBm (max)<br>5.5 Mbps: -86 dBm (max)<br>2 Mbps: -89 dBm (max)<br>1 Mbps: -92 dBm (max) |
| **RF Output Power:** | • 15 dBm +/- 1 dBm<br>• Channels 1 - 11 (North America) |
| **Security:** | • WEP 64,128 bit, WPA/TKIP |
| **Wireless Restrictions:** | • In R&TTE countries, such as France, the 802.11g frequency band is restricted to 2454 - 2483.5 MHz (2.4 - 2.4835 GHz) and a max power output of 100 mW EIRP outdoor. |
| **Certifications:** | • FCC (United States)<br>• IC (Canada)<br>• CE (Europe)<br>• TELEC (Japan) |

NOTE

*The only time the wireless card should be removed is in case of failure or when upgrading to the 802.11g Wi-Fi card.*

## NXA-WC80211GCF 802.11g Wireless Interface Card

Optionally, MVP panels can be upgraded with the field-installable 802.11g Wi-Fi card (**FG2255-07**), purchased separately as a Wi-Fi Upgrade Kit.


**FIG. 9** NXA-WC80211GCF 802.11g wireless card

The NXA-WC80211GCF is a 2.4 GHz Wi-Fi LAN CF Card which upgrades a Modero panel's RF capabilities from 802.11b to 802.11g. This card provides enhanced range and throughput, wireless encryption and data security (WPA and WPA2 and WEP) in Compact Flash Type I form factor.

The NXA-WC80211GCF incorporates DSSS and OFDM radio technology and operates at ISM frequency bands of 2.4 GHz, while providing data transfer speeds of up to 54Mbps.

Other features include:

- Support for IEEE 802.11b and 802.11g
- Supports Advanced Encryption Standard (AES) at 128-bit.
- Supports authentication methods such as: EAP-FAST, EAP-LEAP, EAP-PEAP, EAP-TLS, and EAP-TTLS
- Supports Wired Equivalent Privacy (WEP) 64-bit and 128-bit data encryption (known to the on-board firmware as Static WEP)
- The NXA-WC80211GCF is backwards compatible with 802.11b networks.


*To fully utilize wireless security features, this card must be used in tandem with the latest Modero firmware upgrade available at www.amx.com.*

This upgrade kit requires that pre-existing panels first be removed from their current location (tabletop or wall docking station) before an installer can access the internal circuit boards and upgrade a pre-existing 802.11b wireless CF card.

MVP panels require the use of a cardboard cutout (Mounting Template) to properly position the metal antenna plate onto the inner surface of the unit's rear plastic housing. The procedures for upgrading a CF card on an MVP is identical for both MVP-7500 and MVP-8400 panels.

## Specifications

| NXA-WC80211GCF Specifications | |
|---|---|
| **Dimensions (HWD):** | • 0.22" x 1.68" x 2.40" (5.6 mm x 42.80 mm x 61.0 mm) |
| **Weight:** | • 19.50 grams (0.043 lbs) |
| **Description:** | • Wireless LAN Compact Flash Card with external PIFA antenna.<br>• Features enterprise-class security such as WPA and WPA2 security. |
| **Antenna Type:** | • External PIFA antenna (factory-installed) |
| **Bus Interface:** | • Compact Flash Type I |
| **Certifications:** | • FCC Part 15 Class B, CE, IC, TELEC, and Wi-Fi |
| **Media Access Control Techniques:** | • Using 802.11b DSSS communication:<br>DBPSK @ 1 Mbps<br>DQPSK @ 2 Mbps<br>CCK @ 5.5 Mbps<br>• Using 802.11g OFDM communication:<br>BPSK @ 6 and 9 Mbps<br>QPSK @ 12 and 18 Mbps<br>16-QAM @ 24 and 36 Mbps<br>64-QAM @ 48 and 54 Mbps |
| **Network Architecture:** | • Infrastructure mode (Client-to-Access Point) |
| **Operating Channels:** | • Using 802.11b & g communication:<br>- 04: (Ch 10 - 13) - France<br>- 11: (Ch 1 - 11) - North America<br>- 13: (Ch 1 - 13) - Europe ETSI<br>- 13: (Ch 1 - 13) - Japan (802.11g)<br>- 14: (Ch 1 - 14) - Japan (802.11b)<br>***Note**: To alter the card's default country code (North America), contact an AMX Technical Support representative for detailed procedures and information.* |
| **Operating Environment:** | • Temperature: 0°C ~ 45°C (32°F to 113°F) (operating) and -20°C ~ 70°C (-4°F to 158°F) (storage)<br>• Humidity: (non-condensing) 5% ~ 90% RH (operating) and (non-condensing) 5% ~ 95% RH (storage) |
| **Operating Voltage:** | • 3.3V + 5% I/O supply voltage |
| **Power Consumption:** | • @ 802.11b communication:<br>- RX: 270 mA<br>- TX: 435 mA<br>- Standby: 240 mA<br>• @ 802.11g communication:<br>- RX: 270 mA<br>- TX: 460 mA<br>- Standby: 240 mA |
| **Radio Data Rate:** | • 802.11g compliant: 1, 2, 5.5, 11 (DSSS/CCK); 6, 9, 12, 18, 24, 36, 48, and 54 (OFDM) Mbps data rates |

| NXA-WC80211GCF Specifications (Cont.) | |
|---|---|
| **Radio Technology:** | • Using 802.11b communication: DSSS (Direct Sequence Spread Spectrum)/ CCK (Complementary Code Keying)<br>• Using 802.11g communication: DSSS/CCK, OFDM (Orthogonal Frequency Division Multiplexing |
| **Receiver Sensitivity:** | • Using 802.11b communication @ FER<8%:<br>1 Mbps: -94 dBm (max)<br>2 Mbps: -93 dBm (max)<br>5.5 Mbps: -92 dBm (max)<br>11 Mbps: -90 dBm (max)<br>• Using 802.11g communication @ PER <10%:<br>6 Mbps: -87 dBm (max)<br>9 Mbps: -86 dBm (max)<br>12 Mbps: -86 dBm (max)<br>18 Mbps: -84 dBm (max)<br>24 Mbps: -82 dBm (max)<br>36 Mbps: -78 dBm (max)<br>48 Mbps: -74 dBm (max)<br>54 Mbps: -72 dBm (max) |
| **RF Frequency Ranges:** | • Using 802.11b & g communication:<br>Europe ETSI: 2.412 ~ 2.472 GHz<br>France: 2.457 ~ 2.472 GHz<br>Japan (802.11b): 2.412 ~ 2.484 GHz<br>Japan (802.11g): 2.412 ~ 2.472 GHz<br>North America: 2.412 ~ 2.462 GHz |
| **Standard Conformance:** | • IEEE 802.11b<br>• IEEE 802.11g<br>• IEEE 802.11e<br>• IEEE 802.11i<br>• Wi-Fi (WPA and WPA2) |
| **Transmit Output Power:** | • 802.11b communication: 12 +-1 dBm (1, 2, 5.5, 11 Mbps)<br>• 802.11g communication: 12 +-1 dBm (6, 9, 12, 18, 24, 36, 48, and 54 Mbps) |
| **Wireless LAN Security:** | • EAP-FAST<br>• EAP-LEAP<br>• EAP-PEAP<br>• EAP-TLS<br>• EAP-TTLS<br>• WEP 64 & 128<br>• WPA-PSK |
| **Touch Panel Compatibility:** | • MVP-7500 (**FG5965-01**)<br>• MVP-8400 (**FG5965-02**)<br>• NXD-CV10 (**FG2259-02**)<br>• NXT-CV10 (**FG2259-01/03**)<br>• NXD-CV7 (**FG2258-02**)<br>• NXT-CV7 (**FG2258-01**) |
| **Included Accessories:** | • Double-sided adhesive tape<br>• Mounting Template cutout (62-2255-04)<br>• NXA-WC80211GCF Quick Start Guide<br>• Two Alcohol cleaning pads<br>• Wireless CF card with wireless antenna |

# Installing the 802.11g Card and Antenna

Upgrading the cards on an MVP involves opening the panel enclosure, removing the existing card, replacing it with the upgrade, and then closing the panel enclosure, as described below.

## Firmware Requirements

The NXA-WC80211GCF requires panel firmware versions 5965-01(MVP-7500), and 5965-02 (MVP-8400). This firmware supports backwards compatibility with 802.11b cards, and security protocols for the NXA-WC80211GCF.

Before installing the NXA-WC80211GCF, upload the latest panel-specific kit file to your MVP *(5965-01.kit for the MVP-7500 and 5965-02.kit for the MVP-8400).*

## Access the MVP's Internal Components

Refer to the *Accessing the MVP's Internal Components* section on page 7 for details.

## Removing the Installed Card

Refer to the *Removing the Installed Card* section on page 8 for details.

## Preparing the MVP's Rear Housing

1. Flip over the MVP's rear housing so that the internal support structures are visible, and lay it directly in front of the circuit board such that the battery compartment is furthest away from you. This placement provides contact of both top rims (FIG. 10).
2. Use an alcohol pad (included) to clean both the rear housing's inner surface (bottom right corner) and the underside of the terminal antenna's metal plate (FIG. 9). These surfaces must be properly cleaned to provide good adhesion for the later installation of the antenna.
3. Place the included Mounting Template along the bottom right corner of the rear housing (FIG. 10). Use the housing's inner supports to position the template properly.

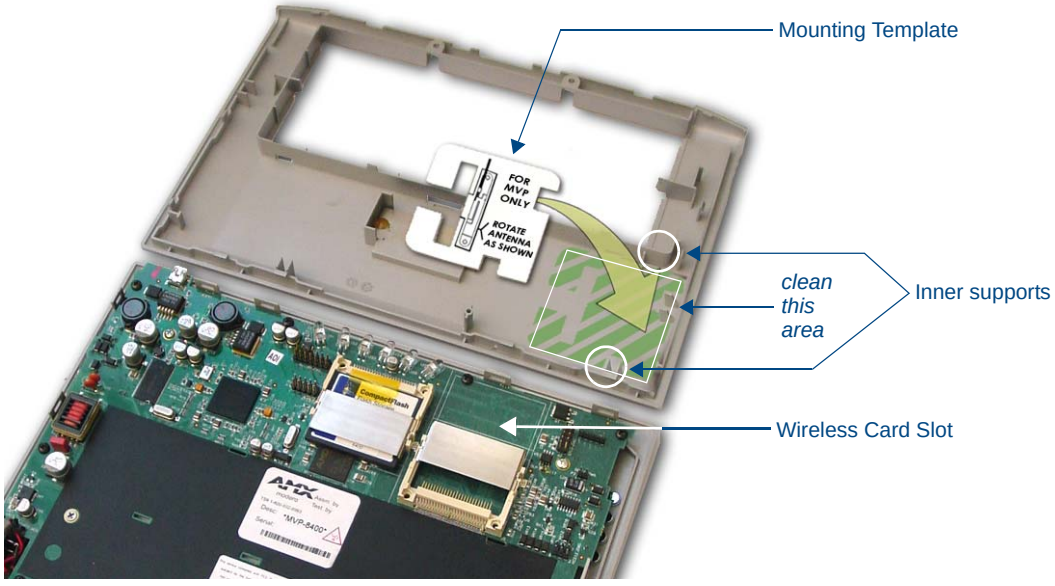



**FIG. 10** Installing the Mounting Template

## Installing the NXA-WC80211GCF

1. Grip the sides of the NXA-WC80211GCF and insert it into the slot opening at a downward angle until the contact pins are securely attached to the pin sockets.
2. Carefully peel off one side of the included double-sided tape and adhere the adhesive side to the surface of the antenna's metal plate.
3. Align the double-sided tape to the surface of the terminal antenna's metal plate, in order to later secure the antenna within the pre-defined installation area outlined by the included Mounting Template.
4. Locate the **T**-shaped opening on the left of the cutout and make sure the antenna wire is located along the left side of the cutout (FIG. 4).

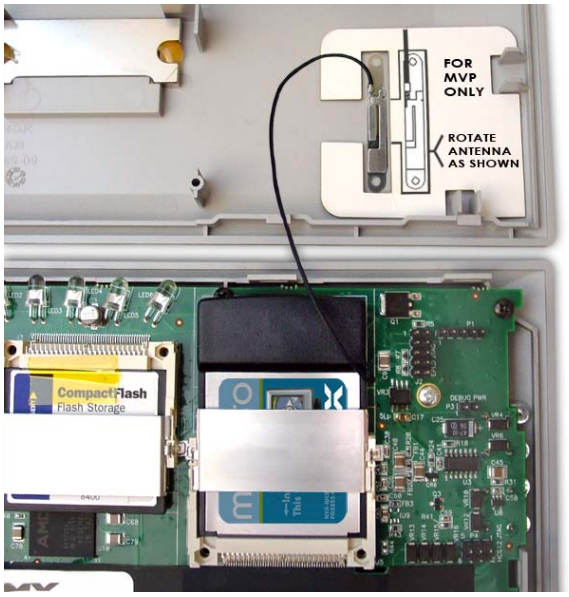



**FIG. 11** Adhering the antenna plate to the MVP outer housing

5. Grip the antenna by its sides and carefully peel-off the remaining protective film on the double-sided tape.
6. Align the antenna into the long vertical groove in the cutout and firmly adhere it to the inner surface of the housing. ***Make sure the wire is threaded along the left side of the cutout, this helps in the removal of the cutout.***
7. With the antenna now securely attached to the MVP's inner housing, remove the cutout by carefully pulling up on the cutout and threading the antenna wire through the **T**-shaped opening.

## Closing and Securing the MVP Enclosure

Once the card has been installed, close and re-secure the outer housing:

1. Reinstall the dark grey trim along the top rim of the board (**A** in FIG. 12).
2. While angling the top rim of the MVP's rear outer housing (**B** in FIG. 12) down toward the IR Emitters, insert the four outer housing latches into their corresponding attachment locations along the top rim of the MVP panel (two on either side of the IR Emitters).
3. While firmly holding the top rims together, gently press down on the bottom ridge of the outer housing (at the latch locations) and verify that each housing latch fits within its corresponding attachment location on the board. When done, complete the insertion of the remaining housing latches.
4. Verify that the notches along the bottom of the plastic battery slot separator strip also fit into the three provided alignment holes on the circuit board.
5. Firmly press down around the entire rim of the outer housing to snap the cover back into place.

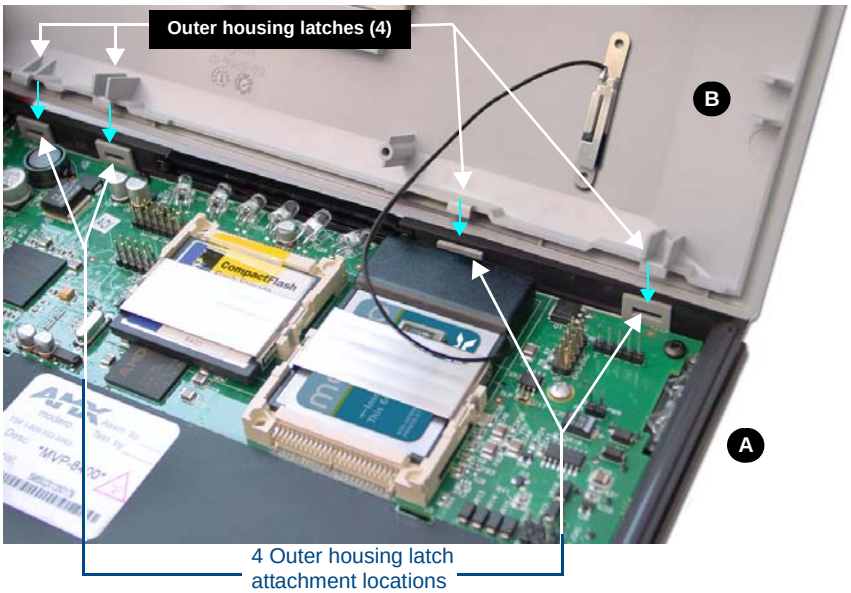



**FIG. 12** Outer housing latch attachment locations

NOTE

*Be careful not to pinch the antenna wire in the housing.*

6. Use a grounded Phillips-head screwdriver to insert and re-secure the two housing screws removed in Step 1.
7. Insert any available batteries back into the battery compartment.
8. Grab the battery cover and align it over the edges of the battery compartment. Apply downward pressure to the traction grooves on the Battery Compartment cover and slide it back towards the metal plate to reinstall the cover.

NOTE

*Once the wireless CF card has been installed, be careful not to disconnect or damage the antenna when subsequentally opening the MVP's housing.*

# Configuring Communications

Communication between the MVP and the Master consists of using either Wireless Ethernet (DHCP, Static IP) or USB. References to Ethernet in this manual focus on the use of Wireless Ethernet via the MVP's WiFi Card.

WARNING

*Before commencing, verify you are using the latest NetLinx Master and Modero panel-specific firmware. Verify you are using the latest versions of AMX's NetLinx Studio and TPDesign4 programs.*

NOTE

*USB input devices must be plugged into the USB connectors on the docking stations before the units are powered-up.*

## Modero Setup and System Settings

AMX Modero panels feature on-board Setup pages. Use the options in the Setup pages to access panel information and make various configuration changes.

### Accessing the Setup and Protected Setup Pages

1. Press down and hold both the bottom, left pushbutton and down on the directional pad simultaneously for 3-5 seconds. This opens the Setup page.

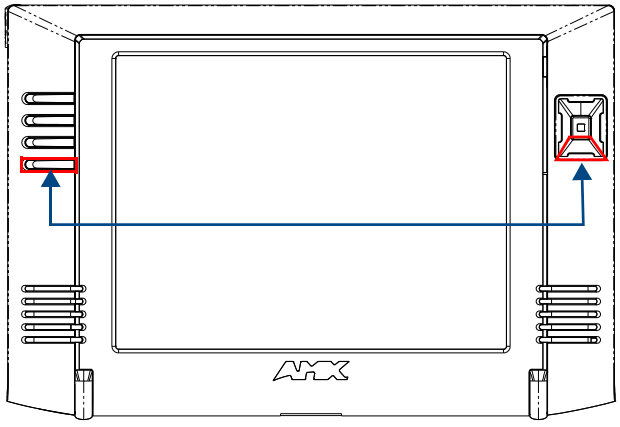



**FIG. 13** Setup Page Access buttons

2. Press the Protected Setup button. This invokes a keypad for entry of the password to allow access to the Protected Setup page. Enter **1988** (the default password), and press **Done** to proceed.

### Setting the Panel's Device Number

In the *Protected Setup* page:

1. Press the *Device Number* field to open the Device Number keypad (FIG. 14).

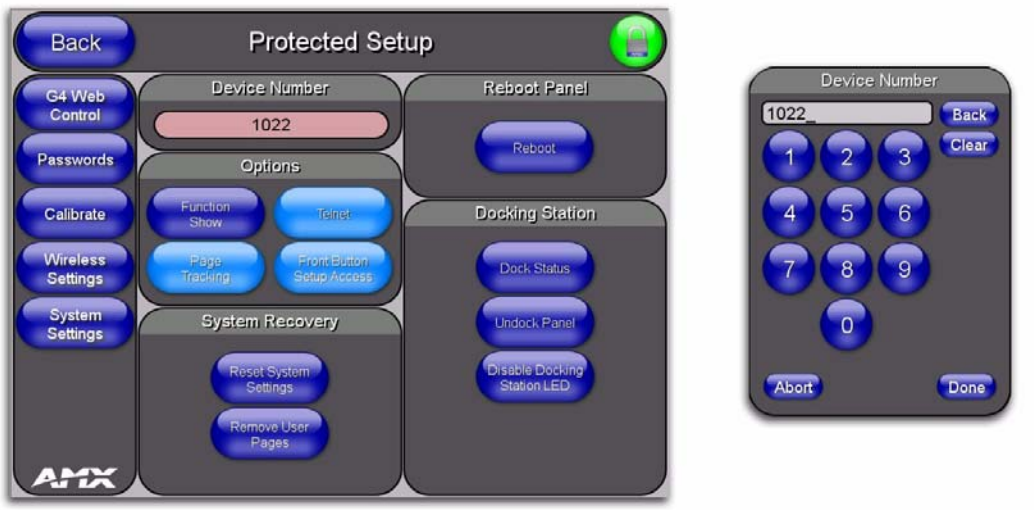



**FIG. 14** Protected Setup page

Enter a unique Device Number assignment for the panel, and press **Done** to return to the *Protected Setup* page. The Device Number range is 1 - 32000, the default is **10001**.

2. Press **Reboot** to reboot the panel, and apply the new Device Number.

## Wireless Settings Page - Wireless Access Overview

### Hot Swapping

Hot swapping is not an issue on these panels as the card is installed within the unit and cannot be removed without first removing the housing.

In the case of DHCP, there must be a DHCP server accessible before the fields are populated.

NOTE

*If the SSID (Network Name) and WEP fields have not previously been configured, the Wireless Settings page will not work until the panel is rebooted.*

Before selecting **Ethernet** as the Master Connection Type you must setup the parameters of the wireless card. **The Wireless Access Point communication parameters must match those of the pre-installed wireless CF card inside the MVP.**

The MVP touch panels allow users to connect to a wireless network through their use of the pre-installed AMX 802.11g wireless interface card to communicate with a Wireless Access Point (WAP) such as the NXA-WAP200G). The WAP communication parameters must match those of the pre-installed wireless interface card installed within the panel. This internal card transmits data wirelessly using the 802.11x signals at 2.4 GHz. For a more detailed explanation of the new security and encryption technology, refer to the section of the document entitled: *Appendix B - Wireless Technology* section on page 163.

For more information on utilizing the AMX Certificate Upload Utility in conjunction with the EAP security, refer to the section of the document entitled: *Appendix B - Wireless Technology* section on page 163.

## Configuring a Wireless Network Access

When working with a wireless card, the first step is to configure wireless communication parameters within the Wireless Settings page. This page only configures the card to communicate to a target WAP (such as the NXA-WAP200G), **it is still necessary to tell the panel which Master it should be communicating with**. This "pointing to a Master" is done via the System Settings page where you configure the IP Address, System Number and Username/Password information assigned to the target Master.

# Step 1: Configure the Panel's Wireless IP Settings

The first step to successfully setting up your internal wireless card is to configure the IP Settings section on the Wireless Settings page. The section configures the communication parameters from the MVP panel to the web.

## Wireless communication using a DHCP Address

In the *Protected Setup* page:

1. Select **Wireless Settings**. Wireless communication is set within the IP Settings section of this page (FIG. 15).
2. Toggle the *DHCP/Static* field (from the IP Settings section) until the choice cycles to *DHCP*. This action causes all fields in the IP Settings section (other than Host Name) to be greyed-out.

Do not alter any of these remaining greyed-out fields in the IP Settings section. Once the panel is rebooted, these values are obtained by the unit and displayed in the *DNS* fields after power-up.

NOTE

*DHCP will register the unique MAC Address (factory assigned) on the panel and once the communication setup process is complete, assign IP Address, Subnet Mask, and Gateway values from the DHCP Server.*

3. Press the optional *Host Name* field to open a Keyboard and enter the Host Name information.

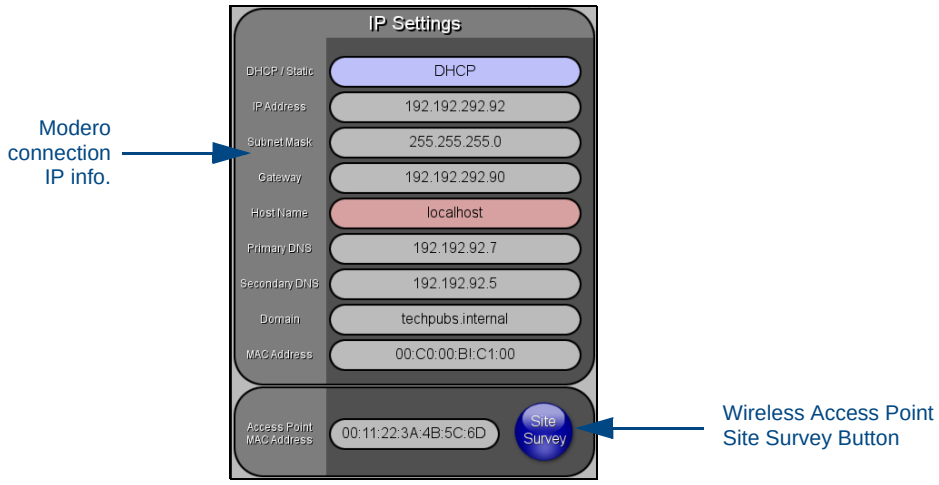



**FIG. 15** Wireless Settings page (IP Settings section)

4. Press **Done** after you are finished assigning the alpha-numeric string of the host name.
5. Do not alter any of these remaining greyed-out fields in the IP Settings section. Once the panel is rebooted, these values are obtained by the unit and displayed in the *DNS* fields after power-up.

NOTE

*This information can be found in either the Workspace - System name > Define Device section of your code (that defines the properties for your panel), or in the Device Addressing/Network Addresses section of the Tools > NetLinx Diagnostics dialog.*

6. Setup the security and communication parameters between the wireless card and the target WAP by configuring the Wireless Settings section on this page. Refer to *Step 2: Configure the Card's Wireless Security Settings* section on page 23 for detailed procedures to setup either a secure or unsecure connection.

## Wireless communication using a Static IP Address

In the *Protected Setup* page:

1. Press the **Wireless Settings** button (located on the lower-left) to open the Wireless Settings page. Wireless communication is set within the IP Settings section of this page (FIG. 15).

NOTE

*Check with your System Administrator for a pre-reserved Static IP Address assigned to the panel. This address must be obtained before Static assignment of the panel continues.*

2. Toggle the *DHCP/Static* field (***from the IP Settings section***) until the choice cycles to **Static**.
*The IP Address, Subnet Mask, and Gateway fields then become user-editable (red).*
3. Press the *IP Address* field to open a Keyboard and enter the Static IP Address (*provided by your System Administrator*).
4. Press **Done** after you are finished entering the IP information.
5. Repeat the same process for the *Subnet Mask* and *Gateway* fields.
6. Press the optional *Host Name* field to open the Keyboard and enter the Host Name information.
7. Press **Done** after you are finished assigning the alpha-numeric string of the host name.
8. Press the Primary DNS field to open a Keyboard, enter the Primary DNS Address (provided by your System Administrator) and press **Done** when compete. Repeat this process for the Secondary DNS field.
9. Press the Domain field to open a Keyboard, enter the resolvable domain Address (this is provided by your System Administrator and equates to a unique Internet name for the panel), and press **Done** when complete.
10. Setup the security and communication parameters between the wireless card and the target WAP by configuring the Wireless Settings section on this page. Refer to the following section for detailed procedures to setup either a secure or unsecure connection.

## Using the Site Survey tool

This tool allows a user to "sniff-out" all transmitting Wireless Access Points within the detection range of the internal NXA-WC80211GCF. Once pressed, the panel displays the Site Survey page which contains categories such as:

- **Network Name** (SSID) - Wireless Access Point names
- **Channel** (RF) - Channel currently being used by the WAP (*Wireless Access Point*)
- **Security Type** (if detectable - such as **WEP**, **OPEN** and **UNKNOWN**) - security protocol enabled on the WAP
- **Signal Strength** - None, Poor, Fair, Good, Very Good, and Excellent
- **MAC Address** - Unique identification of the transmitting Access Point

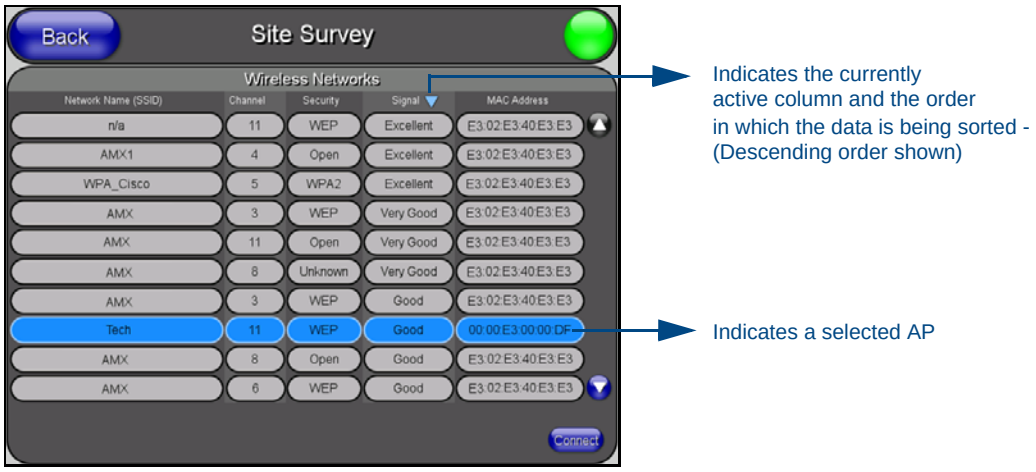



**FIG. 16** Site Survey page

In the *Protected Setup* page:

1. Press the **Wireless Settings** button (located on the lower-left) to open the Wireless Settings page.
2. Navigate to the Access Point MAC Address section of this page and press the on-screen **Site Survey** button. This action launches the Site Survey page which displays a listing of all detected WAPs in the communication range of the internal card.
   - The card scans its environment every four seconds and adds any new WAPs found to the list. Every scan cycle updates the signal strength field.
   - Access points are tracked by MAC Address.
     - If the WAP's SSID is set as a blank, then **N/A** is displayed within the *SSID* field.
     - If the WAP's SSID is hidden (*not broadcast*) it will not show up on the site survey screen but it can still be configured via the *SSID* field on the specified security mode screen.

- If a WAP is displayed in the list is not detected for 10 scans in a row it is then removed from the screen. In this way, a user can walk around a building and see access points come and go as they move in and out of range.

3. Sort the information provided on this page by pressing on a column name and toggling the direction of the adjacent arrow.
   - **Up arrow** - indicates that the information is being sorted in a Ascending order.
     - **SSID** (A to Z), **Channel** (1 to 14), **Security** (Unknown to WEP), **Signal** (None to Excellent). The firmware considers the following to be the security order from least secure to most secure: Open, WEP, WPA, WPA2, and Unknown.
   - **Down arrow** - indicates that the information is being sorted in a Descending order.
     - **SSID** (Z to A), **Channel** (11 to 6), **Security** (WEP to Unknown), **Signal** (Excellent to None)


*If the panel detects more than 10 WAPs, the Up/Down arrows at the far right side of the page become active (blue) and allow the user to scroll through the list of entries.*

4. Select a desired Access Point by touching the corresponding row. The up arrow and down arrow will be grayed out if there are ten or less access points detected. If there are more, then they will be enabled as appropriate so that the user can scroll through the list.
5. With the desired WAP selected and highlighted, click the **Connect** button to be directed to the selected security mode's Settings page with the *SSID* field filled in. You can then either **Cancel** the operation or fill in any necessary information fields and then click **Save**.
   *If you select an Open, WEP, and WPA-PSK Access Point and then click **Connect**, you will be flipped to the corresponding Settings page. For any other security mode, if you click **Connect** you will only return to the previous page without any information being pre-filled out for you.*
   - In an Open security mode, when a target WAP is selected and the connect to, the SSID name of the selected WAP is saved for the open security mode.
   - In a Static WEP security mode, when a WEP Access Point is selected and then connected to, the user is then redirected back to the Static WEP security screen where the *SSID* field is already filled out and the user is only required to enter in the remaining WEP key settings.
   - A similar process occurs for WPA-PSK access points. For any other case, the firmware switches back to the previous page and security and connection parameters must be entered in as normal.

## Step 2: Configure the Card's Wireless Security Settings

The second step to successfully setting up your wireless card is to configure the Wireless Settings section of the Wireless Settings page. This section configures both the communication and security parameters from the internal wireless card to the WAP. ***The procedures outlined within the following sections use an 802.11g card to configure a common security configuration to a target WAP.***

*Refer to either the G4 Web Control Settings/G4 Web Control Page* section on page 73 *or the Appendix B - Wireless Technology* section on page 163 *for more information on the other security methods.*

Once you have set up the wireless card parameters, you must configure the communication parameters for the target Master; see *Step 3: Choose a Master Connection Mode* section on page 29.

## Configuring the Modero's wireless card for unsecured access to a WAP200G

In the *Protected Setup* page:

1. Press the **Wireless Settings** button (located on the lower-left) to open the Wireless Settings page.

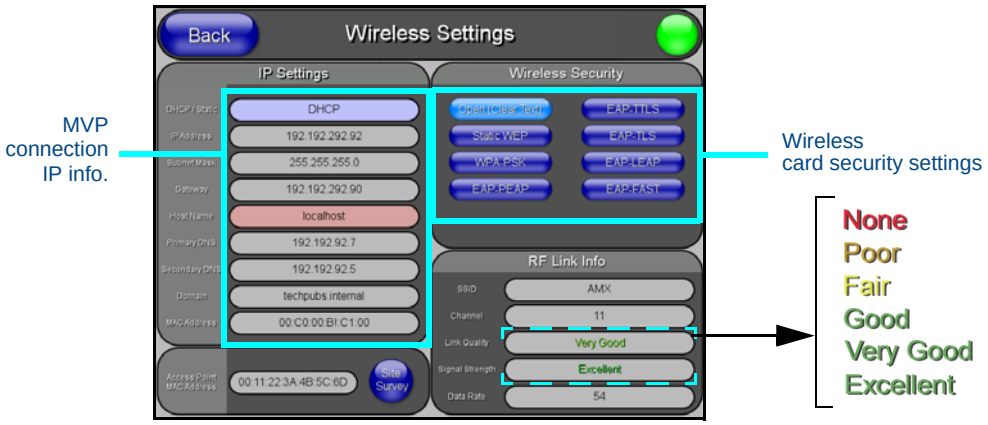



**FIG. 17** Wireless Settings page (showing a sample unsecured configuration)

2. Enter the SSID information by either:
   - *Automatically* having it filled in by pressing the Site Survey button and from the Site Survey page, choosing an ***Open*** WAP from within the Site Survey page and then pressing the **Connec**t button.

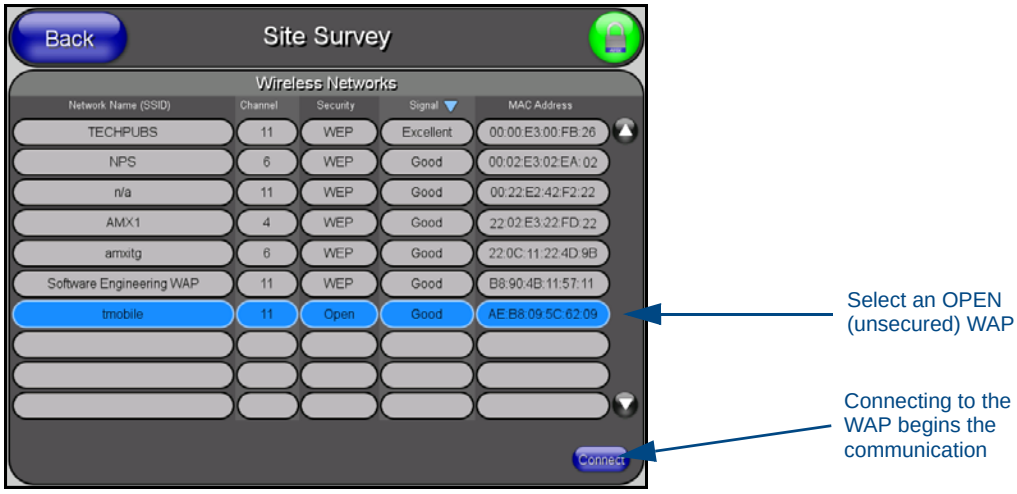



**FIG. 18** Site Survey of available WAPS (Unsecured WAP shown selected)

   - *Manually* entering the SSID information into their appropriate fields by following steps 7 thru 9.

3. From within the Wireless Security section, press the **Open (Clear Text)** button to open the Open (Clear Text) Settings dialog (FIG. 19). An Open security method does not utilize any encryption methodology but does require that an SSID (alpha-numeric) be entered. Using this method causes network packets to be sent out as unencrypted text.

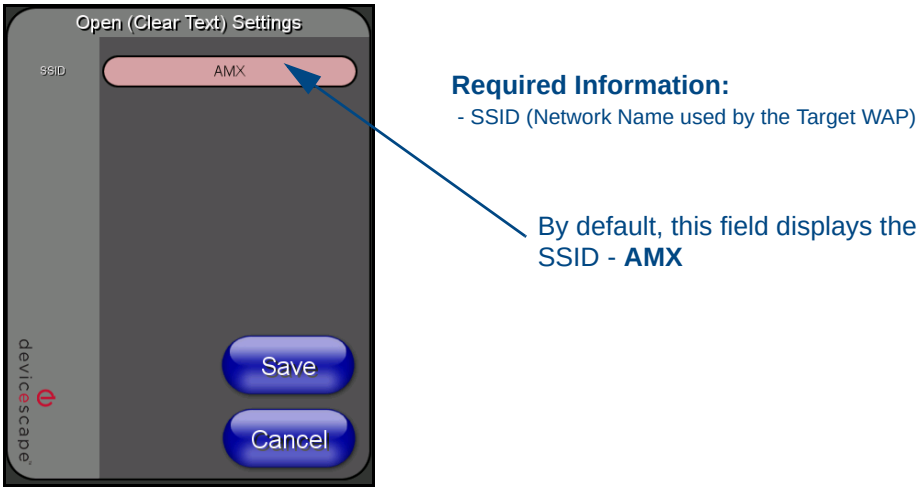



**FIG. 19** Wireless Settings page - Open (Clear Text) security method

4. Press the red *SSID* field (FIG. 19) to display an on-screen *Network Name (SSID)* keyboard.
5. In this keyboard, enter the SSID name used on your target Wireless Access Point (**case sensitive**).
   - The card should be given the SSID used by the target WAP. If this field is left blank, the unit will attempt to connect to the first available WAP. By default, all WAP200Gs use **AMX** as their assigned SSID value.
   - One of the most common problems associated with connection to a WAP arise because the SSID was not entered properly. You must maintain the same case when entering the SSID information. ABC is not the same as Abc.
6. Click **Done** when you've completed typing in the information.
7. From the Open (Clear Text) Settings page (FIG. 19), press the **Save** button to incorporate your new information into the panel and begin the communication process.
8. Verify the fields in the *IP Settings* section have been properly configured. Refer to *Step 1: Configure the Panel's Wireless IP Settings* section on page 21 for detailed information.
9. Press the **Back** button to return to the Protected Setup page and press the on-screen **Reboot** button to both save any changes and restart the panel. ***Remember that you will need to navigate to the System Settings page and configure the connection to a target Master.***
10. After the panel restarts, return to the Wireless Settings page's RF Link Info section and verify the Link Quality and Signal Strength:
    - The descriptions are: **None**, **Poor**, **Fair**, **Good**, **Very Good**, and **Excellent** (FIG. 17).

NOTE

*The signal strength field should provide some descriptive text regarding the strength of the connection to a Wireless Access Point. If there is no signal or no IP Address displayed; configuration of your network could be required.*

## Configuring the Modero's wireless card for secured access to a WAP200G

After logging into the WAP200G, the default Status page appears within the web browser. These read-only values are "pulled" from some of the other user-configurable Configuration Utility pages. By default, wireless Modero panels are configured for unsecured communication to a Wireless Access Point. To properly setup both the WAP200G and panel for secure communication, you must first prepare the Modero panel and then use the information given to fill out the fields within the WAP's browser-based Basic Wireless Configuration page.

Since the code key generator on Modero panels use the same key generation formula, all panels will generate identical keys for the same Passphrase. The generators used on WAPs will not produce the same key as the Modero generator even if you use the same Passphrase. **For this reason, we recommend FIRST creating the Current Key on the Modero and then entering that information into the appropriate NXA-WAP200G fields**.

## Automatically set SSID

In the *Protected Setup* page:

1. Select **Wireless Settings**.
2. Press the **Site Survey** button.
3. Select a **WEP** secured WAP from within the Site Survey page, and press the **Connect** button .

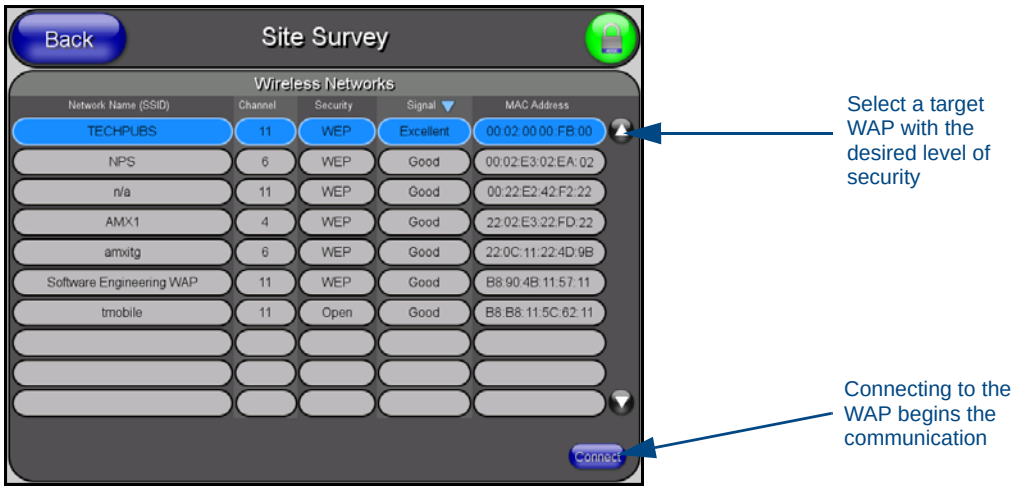



**FIG. 20** Site Survey of available WAPs (Secured WAP shown selected)

4. Write down the SSID name, Current Key string value, and panel MAC Address information so you can later enter it into the appropriate WAP dialog fields in order to "sync-up" the secure connection. These values must be identically reproduced on the target WAP.

## Manually set SSID

In the *Protected Setup* page:

1. Select **Wireless Settings**.
2. Locate the Wireless Security section (FIG. 21).

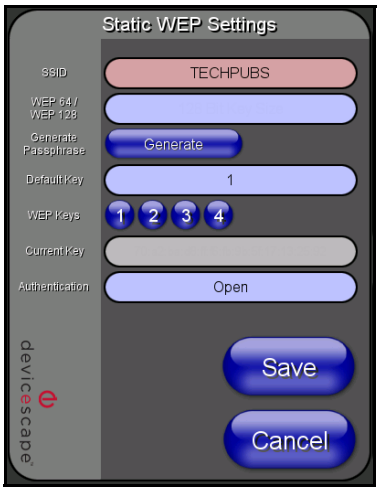

**802.11g wireless card**

**FIG. 21** Wireless Settings page

NOTE

*You must first take down the SSID name, Current Key string value, and panel MAC Address information so you can later enter it into the appropriate WAP dialog fields in order to "sync-up" the secure connection. These values must be identically reproduced on the target WAP.*

3. Press the **Static WEP** button to open the Static WEP Settings dialog (FIG. 22).




**Required Information:**
- SSID (Network Name used by the Target WAP)
- Encryption Method
- Passphrase
- WEP Key assignment
- Authentication Method

**FIG. 22** Wireless Settings page - Static WEP security method

4. Press the *SSID* field and from the *Network Name (SSID)* keyboard, enter the SSID name you are using on your target Wireless Access Point (**case sensitive**), and press **Done** when finished.
   - The card should be given the SSID used by the target WAP. If this field is left blank, the unit will attempt to connect to the first available WAP. By default, all WAP200Gs use **AMX** as their assigned SSID value.
   - One of the most common problems associated with connection to a WAP arise because the SSID was not entered properly. You must maintain the same case when entering this information. ***ABC is not the same as Abc***.
   - The alpha-numeric string is by default **AMX** but can later be changed to any 32-character entry. *This string must be duplicated within the Network Name (SSID) field on the WAP.*
   - As an example, if you use **TECHPUBS** as your SSID, you must **match this word and the case** within both the *Network Name (SSID)* field on the touch panel's *Network Name SSID* field and on the WAP's *Basic Wireless Configuration* page.
5. Toggle the *Encryption* field (FIG. 22) until it reads either: **64 Bit Key Size** or **128 Bit Key Size**.
   *The 64/128 selection reflects the bit-level of encryption security. This WEP encryption level must match the encryption level being used on the WAP.*

NOTE

*WEP will not work unless the same Default Key is set on both the panel and the Wireless Access Point.*
*For example: if you have your Wireless Access Point set to default key 4 (which was 01:02:03:04:05), you must set the panel's key 4 to 01:02:03:04:05.*

6. Toggle the *Default Key* field until the you've chosen a WEP Key value (**from 1- 4**) that matches what you'll be using on your target WAP200G. **This value MUST MATCH on both devices**.
   - **These WEP Key identifier values must match for both devices.**
7. With the proper WEP Key value displayed, press the **Generate** button to launch the WEP Passphrase keyboard. ***If you are wanting to have your target WAP (other than an NXA-WAP200G) generate the Current Key - Do not press the Generate button and continue with Step 13.***
   - This keyboard allows you to enter a Passphrase (such as *AMXPanel*) and then AUTOMATICALLY generate a WEP key which is compatible only among all Modero panels.

NOTE

*The code key generator on Modero panels use the same key generation formula. Therefore, this same Passphrase generates identical keys when done on any Modero because they all use the same Modero-specific generator. The Passphrase generator is case sensitive.*

8. Within this on-screen WEP Passphrase keyboard (FIG. 23), enter a character string or word (such as ***AMXPanel***) and press **Done** when you have finished.


**FIG. 23** WEP Passphrase Keyboard

- As an example, enter the word **AMXPanel** using a 128-bit hex digit encryption. After pressing **Done**, the on-screen Current Key field displays a long string of characters (separated by colons) which represents the encryption key equivalent to the word AMXPanel.
- **This series of hex digits (26 hex digits for a 128-bit encryption key) should be entered as the *Current Key* into both the WAP and onto other communicating Modero panels by using the WEP Key dialog (FIG. 24).**


**FIG. 24** WEP Key # Keyboard

9. Write down this Current Key string value for later entry into your WAP's *WEP Key* field (*typically entered without colons*) and into other communicating panel's *Current Key* field (FIG. 24).
10. **If you are entering a Current Key generated either by your target WAP or another Modero panel**, within the *WEP Keys* section, touch the **Key #** button to launch the *WEP Key #* keyboard (FIG. 24), enter the characters and press **Done** when finished.
    - This Key value corresponds to the Default WEP Key number used on the Wireless Access Point and selected in the Default Key field described in the previous step.

NOTE

*If your target Wireless Access Point does not support passphrase key generation and has previously been setup with a manually entered WEP KEY, you must manually enter that same WEP key on your panel.*

11. The remaining *Current Key* and *Authentication* fields are greyed-out and cannot be altered by the user.
12. Verify the fields within the IP Settings section have been properly configured. Refer to *Step 1: Configure the Panel's Wireless IP Settings* section on page 21 for detailed information.
13. Press the **Back** button to navigate to the Protected Setup page and press the on-screen **Reboot** button to both save any changes and restart the panel. ***Remember that you will need to navigate to the System Settings page and configure the connection to a target Master.***
14. After the panel restarts, return to the Wireless Settings page to verify the Link Quality and Signal Strength:
    - The descriptions are: **None**, **Poor**, **Fair**, **Good**, **Very Good**, and **Excellent**.

NOTE

*The signal strength field provides some descriptive text regarding the strength of the connection to a Wireless Access Point. If there is no signal or no IP Address displayed; configuration of your network could be required.*

Refer to the NXA-WAP200G Instruction Manual for more detailed setup and configuration procedures.

### Configuring multiple wireless Moderos to communicate to a target WAP200G

1. For each communicating touch panel, complete all of the steps outlined within the previous *Configuring the Modero's wireless card for secured access to a WAP200G* section on page 25.
2. Navigate back to the Wireless Settings page on each panel.
3. Verify that all communicating Modero panels are using the same **SSID**, **encryption level**, **Default Key #**, and an identical **Current Key value**.
   - As an example, all panels should be set to Default Key **#1** and be using **aa:bb:cc**..as the Current Key string value. This same Key value and Current Key string should be used on the target WAP.
4. Repeat steps 1 - 3 on each panel. **Using the same passphrase, generates the same key for all communicating Modero panels.**

## Step 3: Choose a Master Connection Mode

The panel requires you establish the type of connection you want made between it and your master.

In the *Protected Setup* page:

1. Select *System Settings*.
2. Select *Type* to toggle between the Master Connection Types *USB* and *Ethernet*.
   - A USB connection is a direct connection from the panel's mini-USB port to a corresponding USB port on the PC (acting as a Virtual Master).
   - A Wireless Ethernet connection involves indirect communication from the panel to a Master via a wireless connection to the network.

WARNING

*It is recommended that firmware KIT files only be transferred over a direct connection and only when the panel is connected to a power supply. If battery power or wireless connection fails during a firmware upgrade, the panel flash file system may become corrupted.*

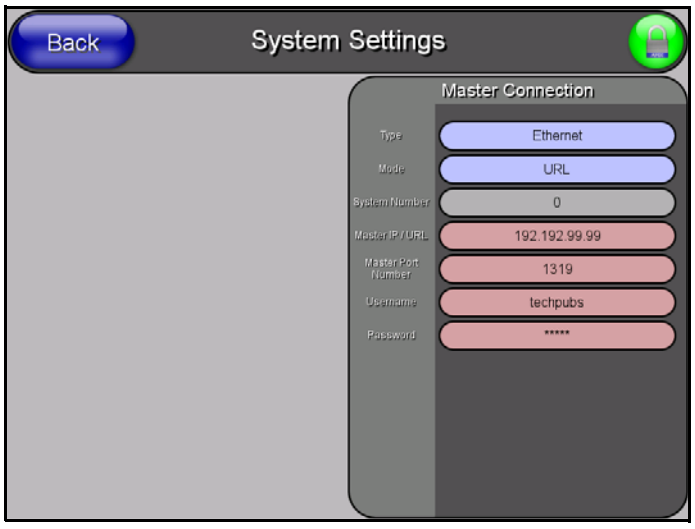



**FIG. 25** System Settings page

## USB

NetLinx Studio can be setup to run a Virtual Master where the PC acts as the Master by supplying its own IP Address for communication to the panel. For a PC to establish a USB connection with a Modero panel, it must have the AMX USBLAN driver installed.

NOTE

*The AMX USBLAN driver is included with both NetLinx Studio2 and TPDesign4, and can also be downloaded as a stand-alone application from www.amx.com.*

### Prepare your PC for USB communication with the panel

If you haven't already done so, download and install the latest versions of NetLinx Studio2 and TPDesign4 (from www.amx.com), and restart your PC.

### Configure the panel for USB communication

The first time the panel is connected to the PC it is detected as a new USB hardware device, and the correct (panel-specific) USBLAN driver must be associated to it manually. Each time thereafter, the panel is recognized as a unique USBLAN device, and the association to the driver is handled automatically.

1. Connect the PS4.4 power connector to the panel (or docking station if the panel is already installed) to supply power.
2. Press and hold the two lower external pushbuttons on either side of the panel simultaneously for 3 seconds to access the Setup page (see FIG. 13 on page 19).
3. In the Protected Settings page, select **System Settings** to open the System Settings page (FIG. 26).
4. Toggle the blue *Type* field (***from the Master Connection section***) until the choice cycles to **USB**.

   Refer to the *System Settings Page* section on page 54 for information about the fields on this page.

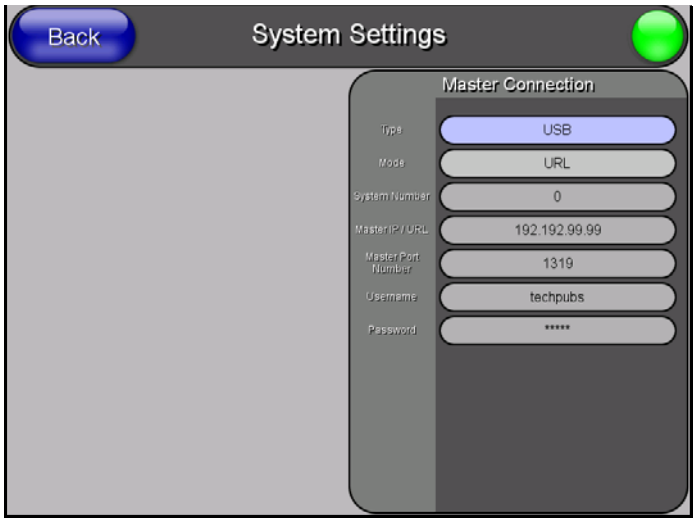



**FIG. 26** System Settings page - USB Connection

5. Press the **Back** button to return to the Protected Setup page.
6. Press **Reboot** to save changes and restart the panel.
7. When the panel powers up and displays the first panel page, insert the mini-USB connector into the Program Port on the panel.

   It may take a minute for the panel to detect the new connection and send a signal to the PC (*indicated by a green System Connection icon*).

The first time the panel is recognized by the PC as a new USB device, a USB driver installation popup window (FIG. 27) is displayed. This window notifies you that the panel has been detected as a USB device, and the appropriate USB driver is being installed to establish communication with the panel. It also indicates that the AMX USBLAN driver does not contain a Microsoft® digital signature.

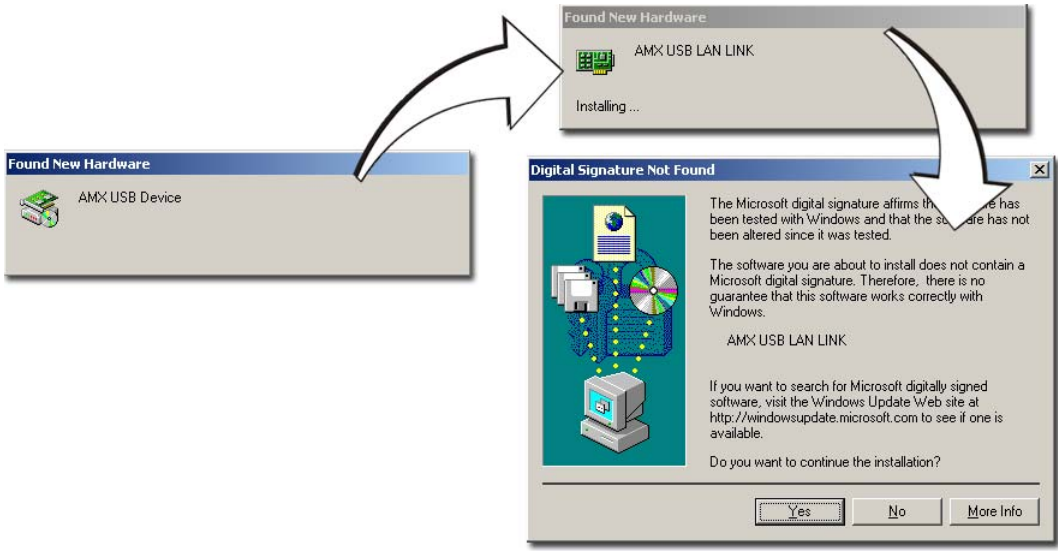



**FIG. 27** USB driver installation popup window

8. Click **Yes** to proceed with the driver installation.

   Once the installation is complete, the panel and PC are ready to communicate via USB.

9. Navigate back to the *System Settings* page.

## Configure a Virtual NetLinx Master using NetLinx Studio

A Virtual NetLinx Master (VNM) is used when the target panel is not connected to a physical NetLinx Master. In this situation, the PC takes on the functions of a Master via a Virtual NetLinx Master. This connection is made by either using the PC's Ethernet Address (via TCP/IP using a known PC's IP Address as the Master) or using a direct mini-USB connection to communicate directly to the panel.

Before beginning:

1. Verify the panel has been configured to communicate via USB within the System Settings page and that the USB driver has been properly configured. Refer to the previous section for more information.
2. In NetLinx Studio, select **Settings > Master Communication Settings**, from the Main menu to open the Master Communication Settings dialog (FIG. 28).

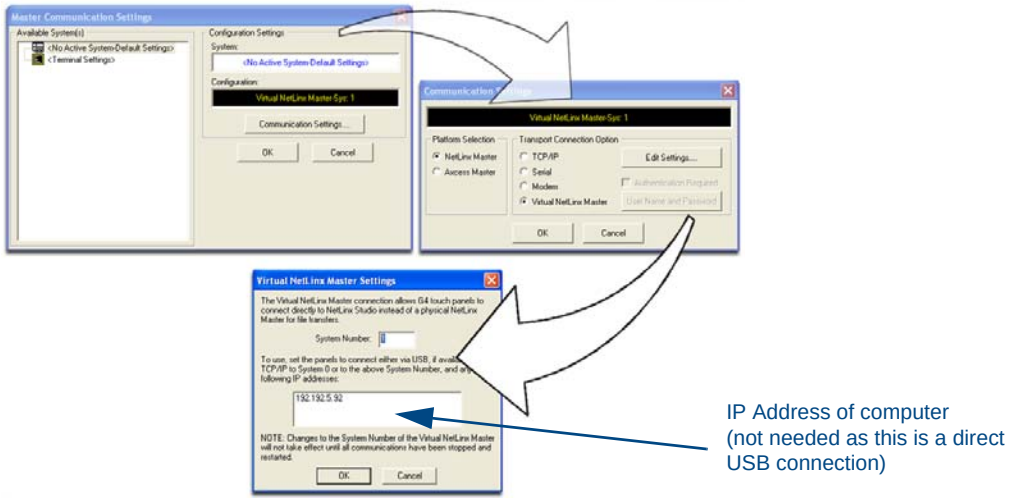



**FIG. 28** Assigning Communication Settings for a Virtual Master

3. Click the **Communications Settings** button to open the *Communications Settings* dialog.
4. Click the **NetLinx Master** radio button (*from the Platform Selection section*).
5. Click the **Virtual Master** radio button (*from the Transport Connection Option section*).
6. Click the **Edit Settings** button to open the *Virtual NetLinx Master Settings* dialog (FIG. 28).
7. Enter the System number (default is **1**).
8. Click **OK** to close all open dialogs and save your settings.
9. Click the **OnLine Tree** tab in the Workspace window to view the devices on the Virtual System.
10. Right-click on *Empty Device Tree/System* and select **Refresh System** to re-populate the list.
    ***The panel will not appear as a device below the virtual system number (in the Online Tree tab) until both the system number (default = 1) is entered into the Master Connection section of the System Settings page and the panel is restarted.***
    - The Connection status turns green after a few seconds to indicate an active USB connection to the PC (Virtual Master).
    - If the System Connection icon does not turn green, check the USP connection and communication settings and refresh the system.

### Ethernet

1. When using *Ethernet*, press the listed *Mode* to toggle through the available connection modes:

**Connection Modes**

| Mode | Description | Procedures |
|---|---|---|
| Auto | The device connects to the first master that responds. This setting requires you set the System Number. | Setting the System Number:<br>1. Select the *System Number* to open the keypad.<br>2. Set your System Number select **Done**. |
| URL | The device connects to the specific IP of a master via a TCP connection. This setting requires you set the Master's IP. | Setting the Master IP:<br>1. Select the *Master IP* number to the keyboard.<br>2. Set your Master IP and select **Done**. |
| Listen | The device "listens" for the master to initiate contact. This setting requires you provide the master with the device's IP. | Confirm device IP is on the Master URL list. You can set the Host Name on the device and use it to locate the device on the master. Host Name is particularly useful in the DHCP scenario where the IP address can change. |

2. Select the *Master Port Number* to open the keypad and change this value. The default setting for the port is *1319*.
3. Set your Master Port and select **Done**.

If you have enabled password security on your master you need to set the username and password within the device.

4. Select the blank field *Username* to open the keyboard.
5. Set your Username and select **Done**.
6. Select the blank field *Password* to open the keyboard.
7. Set your Password and select **Done**.
8. Press the **Back** button to return to the *Protected Setup* page.
9. Press the **Reboot** button to reboot device and confirm changes.

### Master Connection to a Virtual Master via Ethernet


*When configuring your panel to communicate with a Virtual Master (on your PC) via wireless Ethernet, the Master IP/URL field must be configured to match the IP Address of the PC and make sure to use the Virtual System value assigned to the Virtual Master within NetLinx Studio.*

Before beginning:

1. Verify the panel has been configured to communicate with the Wireless Access Point and verify the signal strength quality bargraph is On.

2. Launch NetLinx Studio 2.x (default location is **Start > Programs > AMX Control Disc > NetLinx Studio 2 > NetLinx Studio 2**).
3. Select **Settings > Master Communication Settings**, from the Main menu to open the Master Communication Settings dialog (FIG. 29).

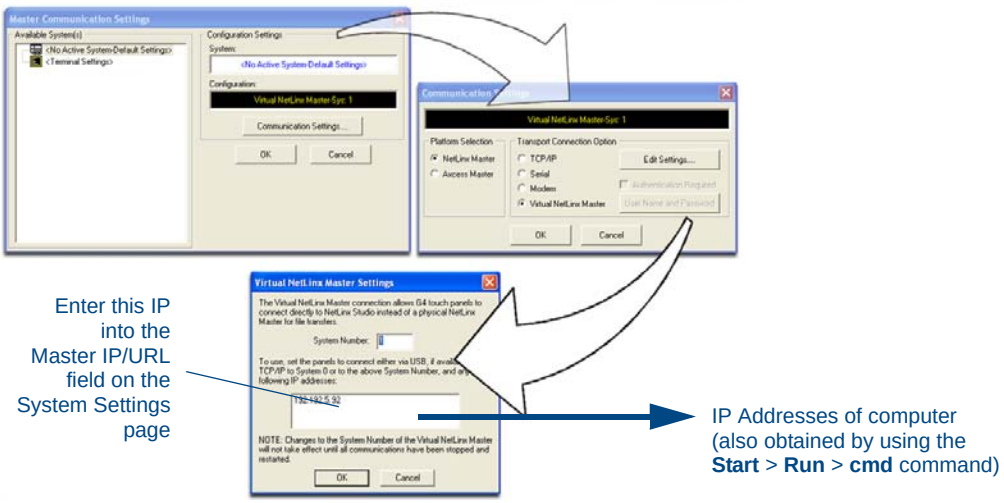



**FIG. 29** Assigning Communication Settings and TCP/IP Settings for a Virtual Master

4. Click the **Communications Settings** button to open the Communications Settings dialog.
5. Click on the **NetLinx Master** radio button (*from the Platform Selection section*) to indicate that you are working as a NetLinx Master.
6. Click on the **Virtual Master** radio box (*from the Transport Connection Option section*) to indicate you are wanting to configure the PC to communicate with a panel. Everything else such as the Authentication is greyed-out because you are not going through the Master's UI.
7. Click the **Edit Settings** button (*on the Communications Settings dialog*) to open the Virtual NetLinx Master Settings dialog (FIG. 29).
8. From within this dialog enter the System number (**default is 1**) and note the IP Address of the target PC being used as the Virtual Master. This IP Address can also be obtained by following these procedures:
   - On your PC, click **Start > Run** to open the Run dialog.
   - Enter **cmd** into the Open field and click **OK** to open the command DOS prompt.
   - From the **C:\>** command line, enter **ipconfig** to display the IP Address of the PC. This information is entered into the *Master IP/URL* field on the panel.
9. Click **OK** three times to close the open dialogs, save your settings, and return to the main NetLinx Studio application.
10. Click the **OnLine Tree** tab in the Workspace window to view the devices on the Virtual System. *The default System value is **one***.
11. Right-click on the *Empty Device Tree/System* entry and select **Refresh System** to re-populate the list.
12. Connect the terminal end of the PS4.4 power cable to the 12 VDC power connector on the side of the stand-alone touch panel.
    - If the MVP is installed onto a docking station, feed power to the docked panel by connecting the appropriate power supply to the docking station.
13. After the panel powers-up, press and hold the two lower buttons on both sides of the display (**for 3 seconds**) to continue with the setup process and proceed to the Setup page.

14. Select **Protected Setup > System Settings** (located on the lower-left) to open the System Settings page (FIG. 30).

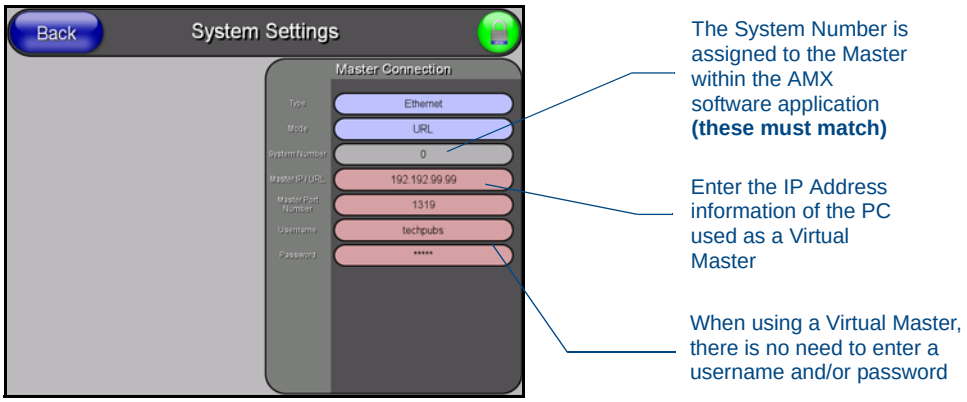



**FIG. 30** Sample System Settings page (for Virtual Master communication)

15. Press the blue *Type* field (***from the Master Connection section***) until the choice cycles to the word **Ethernet.**
16. Press the *Mode* field until the choice cycles to the word **URL**.
    - By selecting **URL**, the System Number field becomes read-only (grey) because the panel pulls this value directly from the communicating target Master (virtual or not). A Virtual Master system value can be set within the active AMX software applications such as: NetLinx Studio, TPD4, or IREdit.
17. Press the *Master IP/URL* field to open a Keyboard and enter the IP Address of the PC used as the Virtual Master.
18. Click **Done** to accept the new value and return to the System Settings page.
19. Do not alter the Master Port Number value (*this is the default value used by NetLinx*).
20. Press the **Back** button to open the Protected Setup page.
21. Press the on-screen **Reboot** button to both save any changes and restart the panel.

## Using G4 Web Control to Interact with a G4 Panel

The G4 Web Control feature allows you to use a PC to interact with a G4 enabled panel via the web. This feature works in tandem with the new browser-capable NetLinx Security firmware update (***build 300 or higher***). G4 Web Control is only available with the latest Modero panel firmware.

Refer to the *G4 Web Control Settings/G4 Web Control Page* section on page 73 for more detailed field information.

NOTE

*Verify your NetLinx Master (ME260/64 or NI-Series) has been installed with the latest firmware KIT file from **www.amx.com**. Refer to your NetLinx Master instruction manual for more detailed information on the use of the new web-based NetLinx Security.*

1. Press and hold the two lower buttons on both sides of the display for **3 seconds** to open the Setup page.
2. Press the **Protected Setup** button (located on the lower-left of the panel page) to open the Protected Setup page and display an on-screen keypad.
3. Enter ***1988*** into the Keypad's password field (***1988*** *is the default password*).

NOTE

*Clearing Password #5, from the initial Password Setup page, removes the need for you to enter the default password before accessing the Protected Setup page.*

4. Press **Done** when finished.
5. Press the **G4 WebControl** button to open the G4 Web Control page (FIG. 31).


**FIG. 31** G4 Web Control page

6. Press the **Enable/Enabled** button until it toggles to **Enabled** (*light blue color*).
7. The *Network Interface Select* field is read-only and displays the method of communication to the web.
   - **Wireless** is used when a wireless card is detected within the internal card slot. This method provides an indirect communication to the web via a pre-configured Wireless Access Point.

NOTE

*The Network Interface Select field is read-only and defaulted to **Wireless (since there is no Ethernet cable connection)**.*

8. Press the *Web Control Name* field to open the Web Name keyboard.
9. From the Web Name keyboard, enter a unique alpha-numeric string to identify this panel. This information is used by the NetLinx Security Web Server to display on-screen links to the panel. *The on-screen links use the IP Address of the panel and not the name for communication* (FIG. 32).
10. Press **Done** after you are finished assigning the alpha-numeric string for the Web Control name.
11. Press the *Web Control Password* field to open the Web Password keyboard.

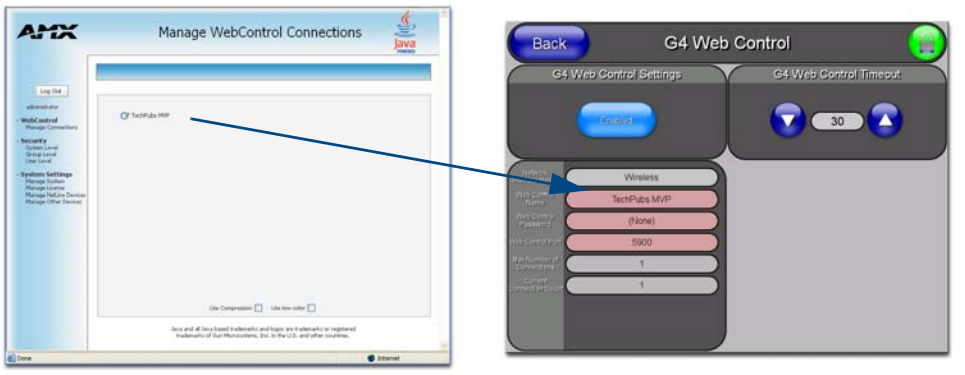



**FIG. 32** Sample relationship between G4 Web Control and Mange WebControl Connections window

12. From the Web Password keyboard, enter a unique alpha-numeric string to be assigned as the G4 Authentication session password associated with VNC web access of this panel.
13. Press **Done** after you are finished assigning the alpha-numeric string for the Web Control password.
14. Press the *Web Control Port* field to open the Web Port Number keypad.
15. Within the keypad, enter a unique numeric value to be assigned to the port the VNC Web Server is running on. The default value is ***5900***.
16. Press **Done** when you are finished entering the value. *The remaining fields within the G4 Web Control Settings section of this page are read-only and cannot be altered.*
17. Press the **Up/Down** arrows on either sides of the G4 Web Control *Timeout* field to increase or decrease the amount of time the panel can remain idle (***no cursor movements***) before the session is closed and the user is disconnected.
18. Press the **Back** button to open the Protected Setup page.
19. Press the on-screen **Reboot** button to save any changes and restart the panel.

NOTE

*Verify your NetLinx Master's IP Address and System Number have been properly entered into the Master Connection section of the System Settings page.*

## Using your NetLinx Master to control the G4 panel

Refer to your particular NetLinx Master's instruction manual for detailed information on how to download the latest firmware from **www.amx.com**. This firmware build enables SSL certificate identification and encryption, HTTPS communication, ICSP data encryption, and disables the ability to alter the Master security properties via a TELNET session.

NOTE

*In order to fully utilize the SSL encryption, your web browser should incorporate the an encryption feature. This encryption level is displayed as a Cipher strength.*

Once the Master's IP Address has been set through NetLinx Studio version 2.x or higher:

1. Launch your web browser.
2. Enter the IP Address of the target Master (***ex: http://198.198.99.99***) into the web browser's *Address* field.
3. Press the **Enter** key on your keyboard to begin the communication process between the target Master and your computer.
   - Initially, the Master Security option is disabled (from within the **System Security** page) and no username and password is required for access or configuration.
   - Both HTTP and HTTPS Ports are enabled by default (via the **Manage System > Server** page).
   - If the Master has been previously configured for secured communication, click **OK** to accept the AMX SSL certificate (*if SSL is enabled*) and then enter a valid username and password into the fields within the *Login* dialog.
4. Click **OK** to enter the information and proceed to the Master's Manage WebControl Connections window.
5. This Manage WebControl Connections page (FIG. 33) is accessed by clicking on the **Manage connections** link (*within the Web Control section within the Navigation frame*). Once activated, this page displays links to G4 panels running the latest G4 Web Control feature (*previously setup and activated on the panel*).

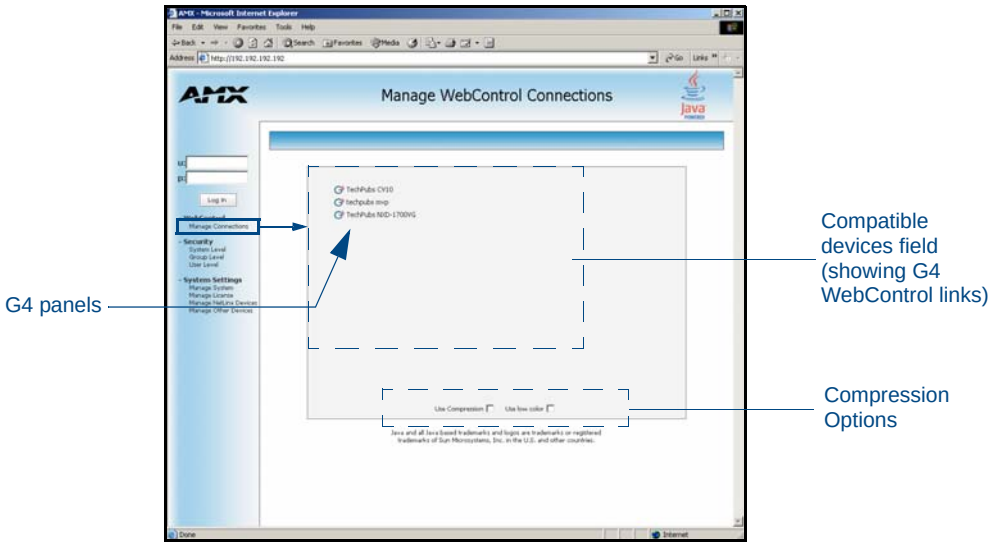



**FIG. 33** Manage WebControl Connections page (populated with compatible panels)

6. Click on the G4 panel name link associated with the target panel. A secondary web browser window appears on the screen (FIG. 34).
7. Click **Yes** from the Security Alert popup window to agree to the installation of the G4 WebControl application on your computer. This application contains the necessary Active X and VNC client applications necessary to properly view and control the panel pages from your computer.

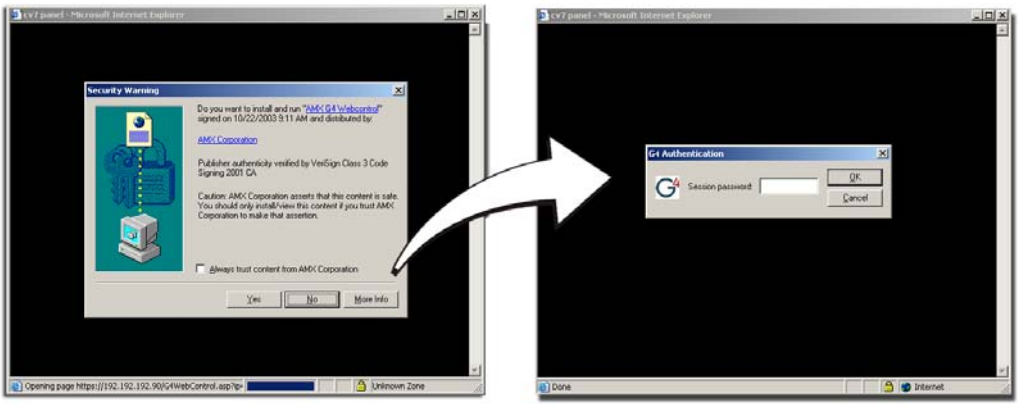



**FIG. 34** Web Control VNC installation and Password entry screens

NOTE

*The G4 Web Control application is sent by the panel to the computer that is used for communication. Once the application is installed, this popup will no longer appear. This popup will only appear if you are connecting to the target panel using a different computer.*

8. In some cases, you might get a *Connection Details* dialog (FIG. 35) requesting a VNC Server IP Address. This is the IP Address not the IP of the Master but of the target touch panel. Depending on which method of communication you are using, it can be found in either the:
   - **Wired Ethernet** - System Settings > IP Settings section within the *IP Address* field.
   - **Wireless** - Wireless Settings > IP Settings section within the *IP Address* field.
   - If you do not get this field continue to step 9.

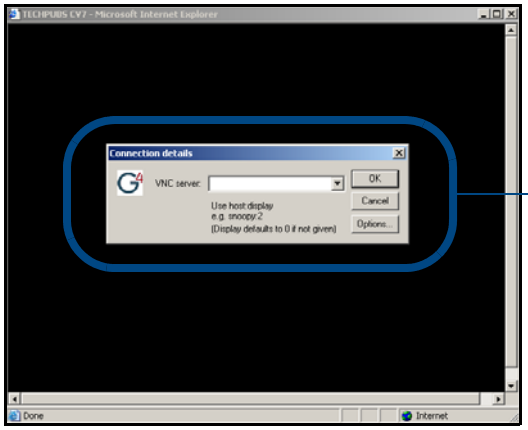



**FIG. 35** Connection Details dialog

9. If a WebControl password was setup on the G4 WebControl page, a G4 Authentication Session password dialog box appears on the screen within the secondary browser window.
10. Enter the Web Control session password into the *Session Password* field (FIG. 35). *This password was previously entered into the Web Control Password field within the G4 Web Control page on the panel.*
11. Click **OK** to send the password to the panel and begin the session. A confirmation message appears stating *"Please wait, Initial screen loading..".*

The secondary window then becomes populated with the same G4 page being displayed on the target G4 panel. A small circle appears within the on-screen G4 panel page and corresponds to the location of the mouse cursor. A left-mouse click on the computer-displayed panel page equates to an actual touch on the target G4 panel page.

# Upgrading MVP Firmware

Except for the MVP-KS (Kickstand for MVP Panels), all MVP panels and their accessories have on-board firmware which is upgradeable through the use of the latest NetLinx Studio. The MVP acts as a bridge between the NetLinx Studio program and the installed docking station. Studio can download firmware to the target docking station by using the connected MVP to pass-along the Kit file to the docking station. Refer to the *NetLinx Studio version 2.x or higher* Instruction Manual for more information on how to download firmware to both a panel and a docking station.


*The latest firmware 2.70.xx (or higher) kit file is panel-specific.*
*This new firmware also provides both backwards compatibility with the previous 802.11b cards and new security protocols for the new 802.11g wireless CF card.*

1. Upload the latest Kit file (**SW5965_xx version 2.70.xx or higher**) to your specific Modero touch panel and then confirm the firmware file update was successful. Refer to your panel's instruction manual for detailed communication and Kit file upload procedures.


*If you don't first update the firmware file on the panel, before proceeding with the card upgrade process, you will be required to configure NetLinx Studio to communicate with the target panel via a direct USB connection.*
*In this communication scenario, your PC acts as a Virtual NetLinx Master establishing a secure USB connection to the target panel and then uploading the new Kit file.*

Before beginning the Upgrade process:

- Setup and configure your NetLinx Master. Refer to the your particular NetLinx Master Instruction Manual for detailed setup procedures.
- Calibrate and prepare the communication pages on the Modero panel for use. Refer to the *Panel Calibration* section on page 155.
- Refer to the NetLinx Studio version 2.x or higher Help file for more information on uploading files via Ethernet.
- Configure your panel for either direct connect or wireless communication. Refer to the *Configuring Communications* section on page 19 for more detailed information about Ethernet or Wireless communication.


*It is recommended that firmware Kit files only be transferred over a direct connection and only when the panel is connected to a power supply.*
*If battery power or wireless connection fails during a firmware upgrade, the panel flash file system may become corrupted.*

The process of updating firmware involves the use of a communicating NetLinx Master. The required steps for updating firmware to a Modero panel are virtually identical to those necessary for updating Kit files to a NetLinx Master (*except the target device is a panel instead of a Master*). Refer to either your Master's literature or Studio 2.x Help file for those procedures.


*A touch panel which is not using a valid username and password will not be able to communicate with a secured Master. If you are updating the firmware on or through a panel which is not using a username or password field, you must first remove the Master Security feature to establish an unsecured connection.*

# Upgrading the Modero Firmware via the USB port

Before beginning with this section, verify your panel is powered and the Type-A USB connector is securely inserted into the PC's USB port. **The panel must be powered-on before connecting the mini-USB connector to the panel.**

WARNING

*Establishing a USB connection between the PC and the panel, prior to installing the USB Driver will cause a failure in the USB driver installation.*

## Step 1: Configure the panel for a USB Connection Type

1. After the installation of the USB driver has been completed, confirm the proper installation of the large Type-A USB connector to the PC's USB port, and restart your machine.
2. After the panel powers-up, press and hold the two lower buttons on both sides of the display for **3 seconds** to continue with the setup process and proceed to the Setup page.
3. Select **Protected Setup > System Settings** (located on the lower-left) to open the System Settings page.
4. Toggle the blue *Type* field (***from the Master Connection section***) until the choice cycles to **USB**.

NOTE

***ALL** fields are then greyed-out and read-only, but still display any previous network information.*

5. Press the **Back** button on the touch panel to return to the Protected Setup page.
6. Press the on-screen **Reboot** button to both save any changes and **restart the panel.** *Remember that the panel's connection type must be set to **USB** prior to rebooting the panel and prior to inserting the USB connector.*
7. **ONLY AFTER** the unit displays the first panel page, **THEN** insert the mini-USB connector into the Program Port on the panel. It may take a minute for the panel to detect the new connection and send a signal to the PC (*indicated by a green System Connection icon*).
   - If a few minutes have gone by and the System Connection icon still does not turn green, complete the procedures in the following section to setup the Virtual Master and refresh the System from the Online Tree. This action sends out a request to the panel to respond and completes the communication (turning the System Connection icon green).
8. Navigate back to the System Settings page.

## Step 2: Prepare Studio for communication via the USB port

1. Launch NetLinx Studio 2.x (default location is **Start > Programs > AMX Control Disc > NetLinx Studio 2 > NetLinx Studio 2**).
2. Select **Settings > Master Communication Settings**, from the Main menu to open the Master Communication Settings dialog (FIG. 36).

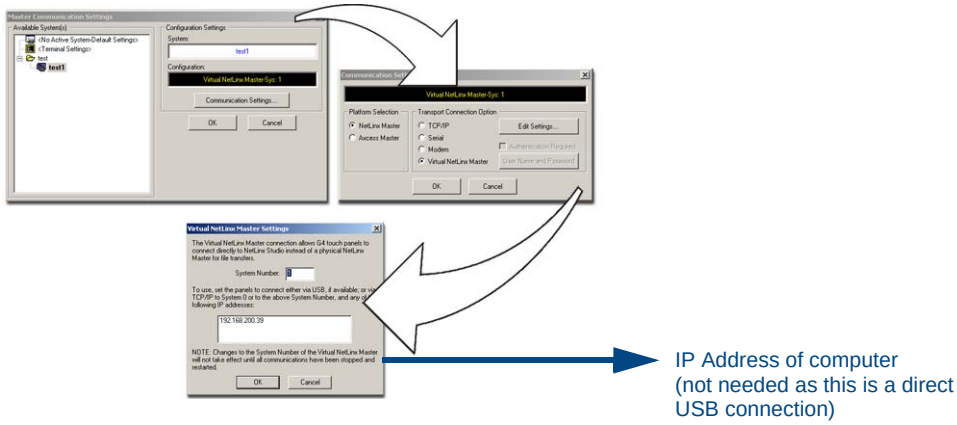



**FIG. 36** Assigning Communication Settings for a Virtual Master

3. Click the **Communications Settings** button to open the *Communications Settings* dialog.

4. Click on the **NetLinx Master** radio button (*from the Platform Selection section*) to indicate that you are working as a NetLinx Master.
5. Click on the **Virtual Master** radio box (*from the Transport Connection Option section*) to indicate you are wanting to configure the PC to communicate directly with a panel. Everything else such as the Authentication is greyed-out because you are not going through the Master's UI.
6. Click the **Edit Settings** button (*on the Communications Settings dialog*) to open the *Virtual NetLinx Master Settings* dialog (FIG. 36).
7. From within this dialog enter the System number (default is **1**).
8. Click **OK** three times to close the open dialogs, save your settings, and return to the main NetLinx Studio application.
9. Click the **OnLine Tree** tab in the Workspace window to view the devices on the Virtual System.
   *The default System value is one.*
10. Right-click on the *Empty Device Tree/System* entry and select **Refresh System** to re-populate the list.
    ***The panel will not appear as a device below the virtual system number (in the Online Tree tab) until both the system number used in step 7 for the VNM is entered into the Master Connection section of the System Settings page and the panel is restarted.***

## Step 3: Confirm and Upgrade the firmware via the USB port

Use the CC-USB Type-A to Mini-B 5-wire programming cable (**FG10-5965**) to provide communication between the mini-USB Program port on the touch panel and the PC. This method of communication is used to transfer firmware Kit files and TPD4 touch panel files.

NOTE

*A mini-USB connection is only detected after it is installed onto an active panel. Connection to a previously powered panel which then reboots, allows the PC to detect the panel and assign an appropriate USB driver.*

1. Verify this direct USB connection (Type-A on the panel to mini-USB on the panel) is configured properly using the steps outlined in the previous two sections.
2. With the panel already configured for USB communication and the Virtual Master setup within NetLinx Studio, its now time to verify the panel is ready to receive files.
3. After the Communication Verification dialog window verifies active communication between the Virtual Master and the panel, click the **OnLine Tree** tab in the Workspace window (FIG. 37) to view the devices on the Virtual System. *The default System value is **one**.*
4. Right-click on the System entry (FIG. 37) and select **Refresh System** to re-populate the list. Verify the panel appears in the **OnLine Tree** tab of the Workspace window.
   *The default Modero panel value is 10001.*

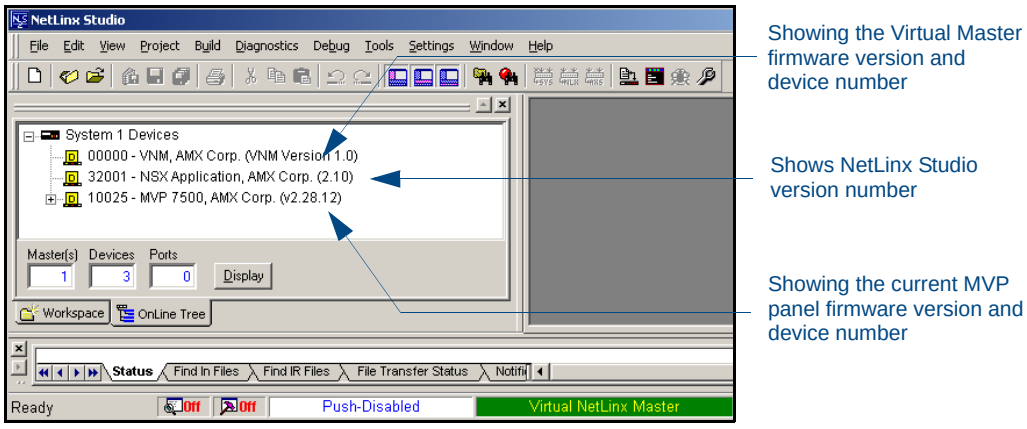



**FIG. 37** NetLinx Workspace window (showing panel connection via a Virtual NetLinx Master)

NOTE

*The panel-specific firmware is shown on the right of the listed panel. Download the latest firmware file from **www.amx.com** and then save the Kit file to your computer. Note that each kit file is intended for download to its corresponding panel.*

5. If the panel firmware version is not the latest available; locate the latest firmware file from the **www.amx.com > Tech Center > Downloadable Files > Firmware Files > Modero Panels** section of the website.
6. Click on the desired Kit file link and after you've accepted the Licensing Agreement, verify you have downloaded the Modero Kit file to a known location.
7. Select **Tools > Firmware Transfers > Send to NetLinx Device** from the Main menu to open the Send to NetLinx Device dialog (**B** in FIG. 38). Verify the panel's System and Device number values match those values listed within the System folder in the **OnLine Tree** tab of the Workspace window (**A** in FIG. 38).

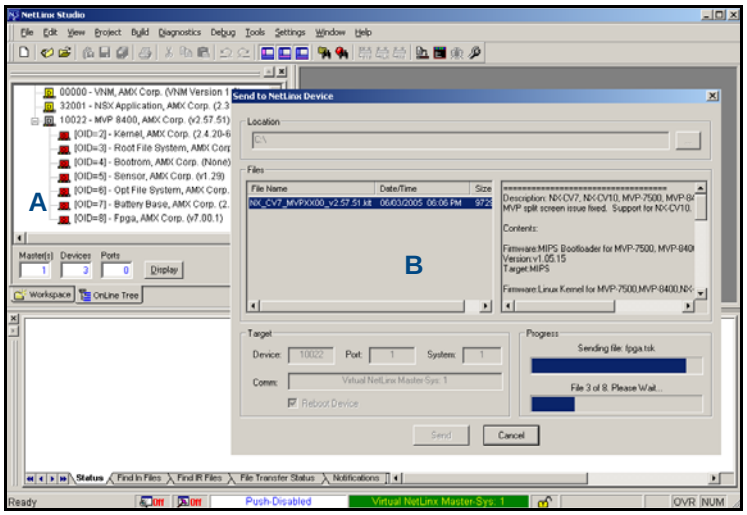



**FIG. 38** Using USB for a Virtual Master transfer

8. Select the panel's Kit file from the **Files** section.
9. Enter the **Device** value associated with the panel and the **System** number associated with the Master (*listed in the OnLine Tree tab of the Workspace window*). *The Port field is greyed-out.*
10. Click the **Reboot Device** checkbox. This causes the touch panel to reboot after the firmware update process is complete. *The reboot of the panel can take up 30 seconds after the firmware process has finished.*
11. Click **Send** to begin the transfer. The file transfer progress is indicated on the bottom-right of the dialog (**B** in FIG. 38).
12. As the panel is rebooting, temporarily unplug the USB connector on the panel until the panel has completely restarted.
13. Once the first panel page has been displayed, reconnect the USB connector to the panel.
14. Right-click the associated System number and select **Refresh System**. This causes a refresh of all project systems, establishes a new connection to the Master, and populates the System list with devices on your particular system.
15. Confirm the panel has been properly updated to the correct firmware version.

# Upgrading the Docking Station Firmware via USB

The following accessory devices are firmware upgradeable:

- MVP-TDS Table Top Docking Station (**FG5965-10**)
- MVP-WDS Wall/Flush Mount Docking Station - Black (**FG5965-11**)
- MVP-WDS Wall/Flush Mount Docking Station - Silver (**FG5965-21**)

This device is not given a unique device number which would ordinarily appear within the Online Tree tab of NetLinx Studio. It appears as a battery base below the target panel which it is a part of as seen below in FIG. 39.

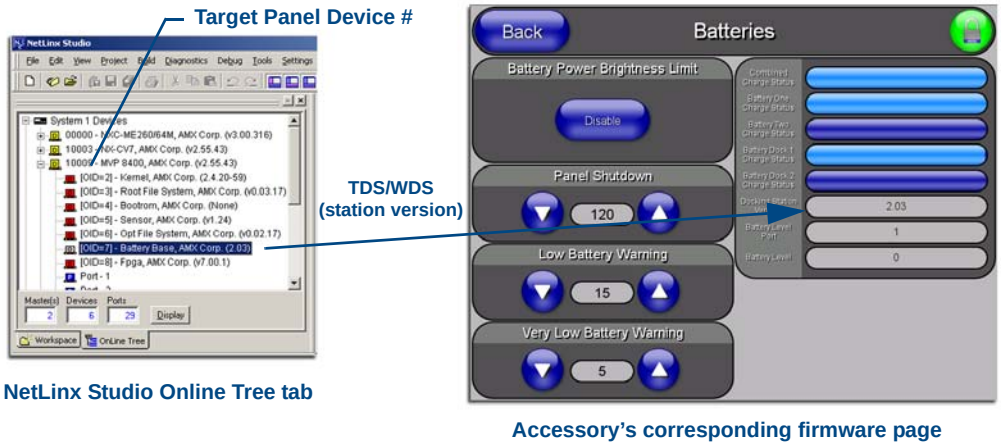



**FIG. 39** Location of Firmware version information within NetLinx Studio

The only way to upgrade the firmware of these accessory items is to send the accessory's firmware through a target panel. Its this panel's device number which is entered within the *Send to NetLinx Device transfer* dialog in Studio.

## Step 1: Prepare the Docking Station for firmware transfer via USB

Before beginning with this section:

- Verify the MVP is securely attached to the docking station and communicating properly.
- Verify that the panel is communicating from the mini-USB port to the Virtual NetLinx Master (VNM).

1. Complete the instructions for configuring the NetLinx Master for IP communication found in the *Upgrading the Modero Firmware via the USB port* section on page 40.
2. After the panel powers-up, press and hold the two lower buttons on both sides of the display for **3 seconds** to continue with the setup process and proceed to the Setup page.
3. Press the **Batteries** button to open the Batteries page (FIG. 40).

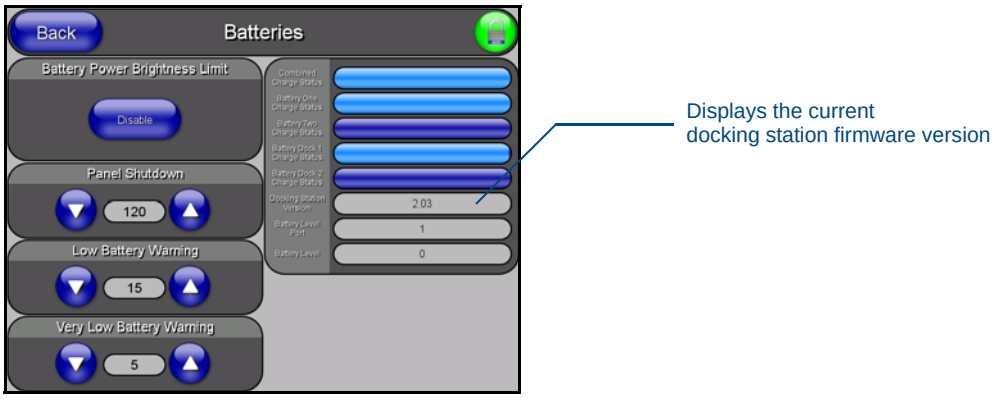



**FIG. 40** Batteries page

*The docking station firmware is shown on the right of the Batteries page. Verify you have downloaded the latest firmware file from **www.amx.com** and then save the Kit file to your computer.*

## Step 2: Upgrade the Docking Station firmware via USB

1. Complete the procedures outlined in the *Step 1: Configure the panel for a USB Connection Type* section on page 40.
2. Prepare NetLinx Studio for communication to the panel via a Virtual Master by following the procedures outlined in the *Step 2: Prepare Studio for communication via the USB port* section on page 40.
3. After the Communication Verification dialog window verifies active communication between the Virtual Master and the panel, click the **OnLine Tree** tab in the Workspace window to view the devices on the Virtual System. *The default System value is one*.
4. Right-click on the System entry and select **Refresh System** to re-populate the list. Verify the panel appears in the **OnLine Tree** tab of the Workspace window.
   *The default Modero panel value is 10001*.
5. Locate the latest firmware file from the **www.amx.com > Tech Center > Downloadable Files > Firmware Files > Modero Panels firmware (MVP Docking Stations: MVP-TDS/WDS)** section of the website.
6. Click on the desired Kit file link and after you've accepted the Licensing Agreement, verify you have downloaded the Docking Station Kit file to a known location.
7. Select **Tools > Firmware Transfers > Send to NetLinx Device** from the Main menu to open the Send to NetLinx Device dialog (FIG. 41). Verify the panel's System and Device number values match those values listed within the System folder in the **OnLine Tree** tab of the Workspace window.

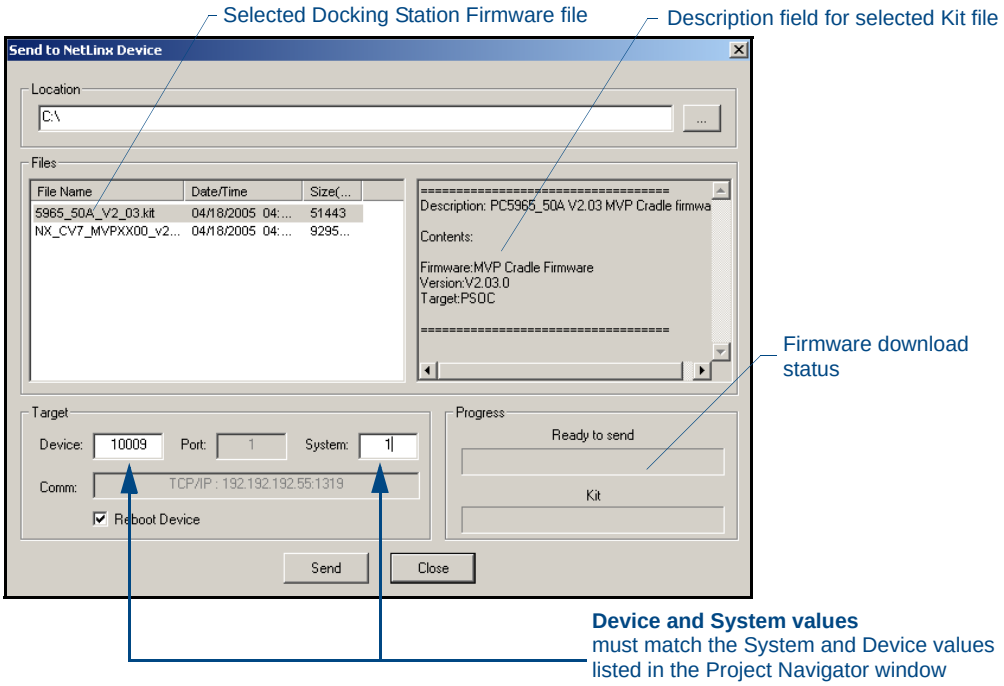



**FIG. 41** Send to NetLinx Device dialog (showing docking station firmware update via USB)

8. Select the docking station's Kit file (*ending in VXX.kit*) from the **Files** section (FIG. 41).
9. Enter the **Device** number associated with the panel and the **System** number associated with the Master (*listed in the OnLine Tree tab of the Workspace window*). *The Port field is greyed-out.*

*Firmware upgrades can not be done directly to the docking station but must be routed through the MVP panel.*

10. Click the **Reboot Device** checkbox. This causes the touch panel to reboot after the firmware update process is complete. *The reboot of the panel can take up 30 seconds after the firmware process has finished.*
11. Click **Send** to begin the transfer. The file transfer progress is indicated on the bottom-right of the dialog.
12. As the panel is rebooting, temporarily unplug the USB connector on the panel until the panel has completely restarted.
13. Once the first panel page has been displayed, reconnect the USB connector to the panel.
14. Right-click the associated System number and select **Refresh System**. This causes a refresh of all project systems, establishes a new connection to the Master, and populates the System list with devices on your particular system.
15. After the panel powers-up, press and hold the two lower buttons on both sides of the display for **3 seconds** to continue with the setup process and proceed to the Setup page.
16. Press the **Batteries** button (located on the lower-left) to open the Batteries page and confirm the new firmware does not read 0.00.

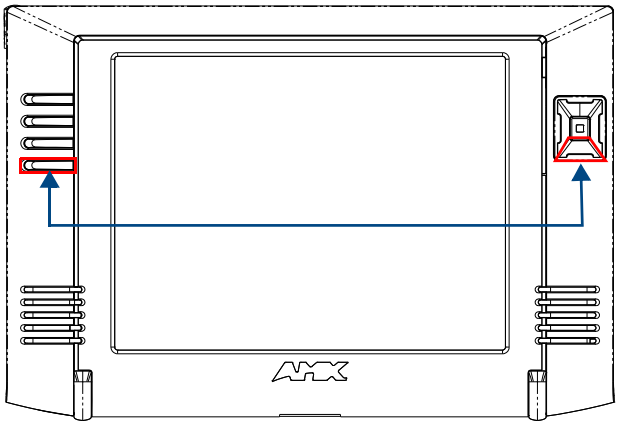

*If the Base Version field displays 0.00, this means there was an error in the firmware upload process. Re-install the base firmware and re-confirm that the new base version no longer reads 0.00.*


*Although firmware upgrades can be done over wireless Ethernet; it is recommended that firmware KIT files be transferred over a direct USB connection and only when the panel is connected to a power supply. If battery power or wireless connection fails during a firmware upgrade, the panel flash file system may become corrupted.*

# Setup Pages

AMX Modero panels feature on-board Setup pages. Use the options in the Setup pages to access panel information and make various configuration changes.

To access the Setup pages, press the two lower external pushbuttons on either side of the panel simultaneously and hold for 3 seconds (FIG. 42).



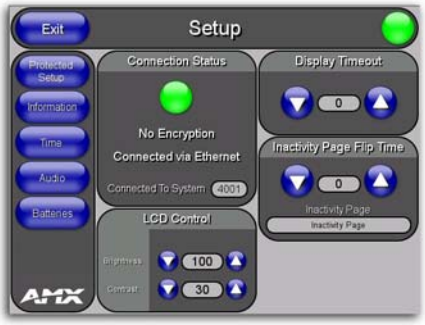
**Setup Page Access buttons**:
Press and hold simultaneously for 3 seconds to access the Setup pages

Press and hold for 6 seconds to access the Calibration page.

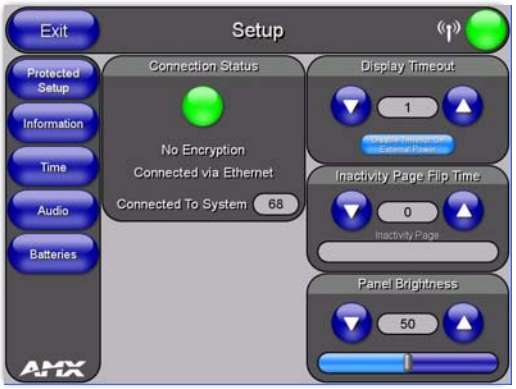
**FIG. 42** Setup Page Access buttons

## Setup Pages

The *Setup* page (FIG. 43) allows quick access to several basic panel properties:




MVP-7500




MVP-8400

**FIG. 43** MVP-7500 and MVP-8400 Setup pages

Features on this page include:

| Setup Page | |
|---|---|
| **Navigation Buttons:** | The buttons along on the left side of the page provide access to secondary Setup pages (see following sections). |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |

| Setup Page (Cont.) | |
|---|---|
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |
| **Connection Status:** | Displays whether the panel is communicating externally as well as the encryption status of the Master, the connection type (***Ethernet** or **USB***), and what System the panel is connected to.<br>• Until a connection is established, the message displayed is: "*Attempting via...*".<br>• When a connection is established, the message displayed is either: "*Connected via Ethernet* "or "*Connected via USB* ".<br>• The word "*Encrypted*" appears when an encrypted connection is established with a NetLinx Master.<br>***Note**: The panel must be rebooted before incorporating any panel communication changes and to detect Ethernet connections.* |
| **Display Timeout:** | Indicates the length of time that the panel can remain idle before activating Sleep mode (causing the LCD to power down).<br>• Press the UP/DN buttons to increase/decrease the Display Timeout setting. Range = 0 - 240 (minutes).<br>• Set the timeout value to zero to disable Sleep mode.<br>***Note**: Small timeout values maximize the life of the battery charge.* |
| **Display Timeout on Battery Power** *(MVP-8400 only)* | When enabled, this button allows the device to engage Display Timeout when the device has been removed from a charging station and is running solely on battery power. When disabled (the button goes dark), Display Timeout is not engaged, and the device will continue to run at full power until it is returned to a charging station or the device's battery is depleted. |
| **Inactivity Page Flip Timeout:** | Indicates the length of time that the panel can remain idle before automatically flipping to a pre-selected page.<br>• Press the UP/DN buttons to increase/decrease the Inactivity Page Flip Timeout setting. Range = 0 - 240 (minutes).<br>• Set the timeout value to zero to disable Inactivity Page Flip mode.<br>***Note**: The touch panel page used for the Inactivity page flip is shown within a small Inactivity Page field.* |
| **Panel Brightness:** *(MVP-8400 only)* | Sets the display brightness level of the panel.<br>• Press the UP/DN buttons to adjust the brightness level. Range = 0 - 100.<br>***Note**: The on-screen bargraph can be dragged to adjust the brightness level which is then reflected as a numeric value in the Panel Brightness field.* |
| **LCD Control:** *(MVP-7500 only)* | Sets the display brightness and contrast levels of the panel.<br>• Press the Brightness UP/DN buttons to adjust the brightness level. Range = 0 - 100.<br>• Press the Contrast UP/DN buttons to adjust the contrast level. Range = 0 - 100. |

## Navigation Buttons

The following Navigation buttons (FIG. 44 and FIG. 45) appear on the left side of the *Setup* page:

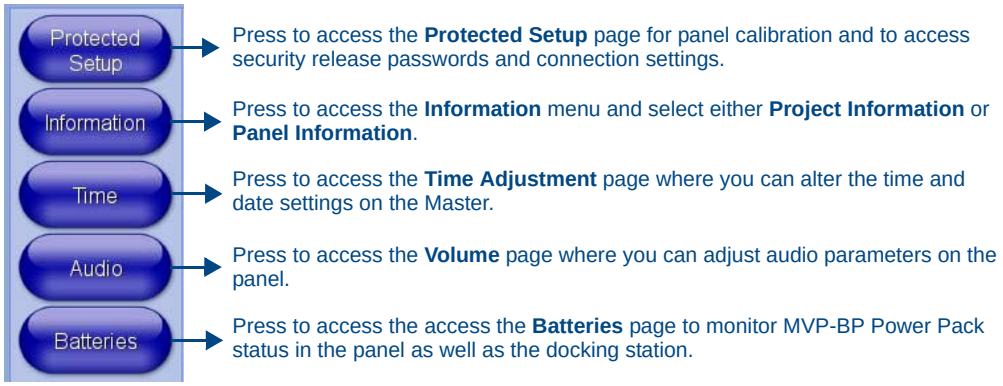



**FIG. 44** Setup Page Navigation Buttons (MVP-7500)

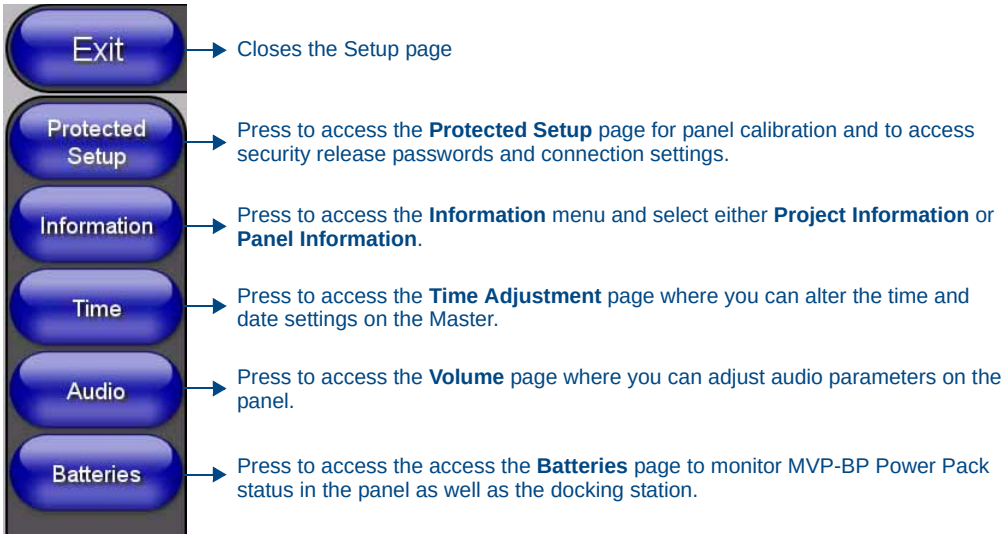



**FIG. 45** Setup Page Navigation Buttons (MVP-8400)

## Custom Logo

The custom logo feature allows a user to customize the boot splash screen with a JPEG image. The custom logo will be displayed a short time after the standard AMX logo appears and will be visible until the user pages are loaded. Adding a custom logo to a panel is done by importing an image into the resource manager of the user pages in TPDesign. Afterwards, transfer the user pages to the panel and reboot to see the new logo. The following guidelines must be followed:

- The custom logo image must be a JPEG
- Once the image is imported into the resource manager, it should be renamed to "custom_logo.jpg" (case sensitive)
- The image resolution should match the panel resolution
- The image should be saved with 2x2,1x1,1x1 sub-sampling. Different image editing tools implement this in different ways. If you are unsure how to set this with your application and you are having issues, try saving with a lower quality setting.

## Protected Setup Pages

The *Protected Setup* page (FIG. 46 and FIG. 47) provides secured access to advanced panel configuration options, including communication and security settings.

Enter the factory default password (***1988)*** into the password keypad to access this page.

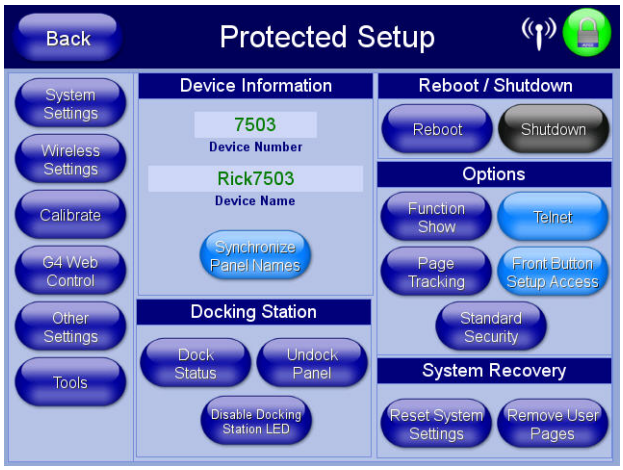



**FIG. 46** Protected Setup Page showing default values (MVP-7500)

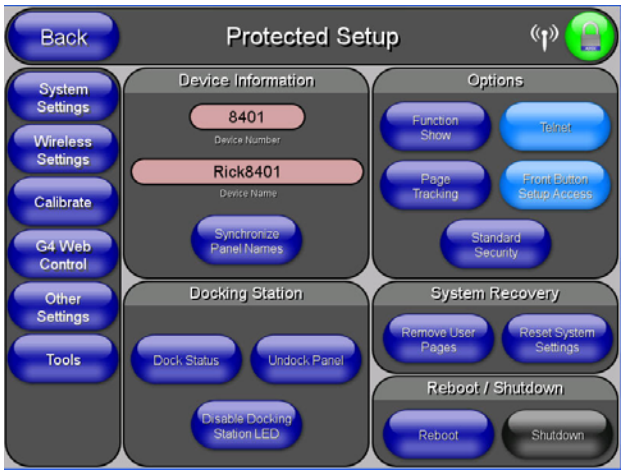



**FIG. 47** Protected Setup page showing default values (MVP-8400)

Features on the Protected Setup page include:

| Protected Setup Page | |
|---|---|
| **Navigation Buttons:** | The buttons along on the left side of the page provide access to secondary Protected Setup pages (see following sections). |
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |
| **Device Number:** | Opens a keypad used to view/set the device number of the panel. |
| **Options:** | • **Function Show** - toggles the display of the channel port, channel code, level port and level code on all touch panel buttons (see FIG. 48).<br>• **Page Tracking** - toggles the page tracking function. When enabled, the panel reports page data to the NetLinx Master.<br>• **Telnet** - enables/disables the panel's telnet server (to allow direct telnet communication to the panel).<br>• **Front Button Setup Access** - activates the two lower buttons on the front of the panel for accessing the Setup and Calibration pages (see FIG. 42 on page 47). The default setting is On.<br>- Press and hold these buttons for **3 seconds** to access the Setup page.<br>- Press and hold these buttons for **6 seconds** to access the Calibration page.<br>• Use the Security button to toggle between three security settings: Standard Security, Secure, and DoD. Refer to the Security Settings section on page 57 for very important information on using this feature. |
| **System Recovery:** | • **Reset System Settings** - deletes all of the current configuration parameters on the panel (including IP Addresses, Device Number assignments, Passwords, and other presets). This option invokes a Confirmation dialog, prompting you to confirm your selection before resetting the panel. |
| **System Recovery (Cont.):** | • **Remove User Pages** - allows you remove all TPD4 touch panel pages currently on the panel, including the pre-installed AMX Demo pages. This option invokes a Confirmation dialog, prompting you to confirm your selection before removing the panel pages.<br>Note that the **YES** button on the Confirmation dialog is disabled for 5 seconds as additional protection against accidentally resetting the panel or removing the panel pages. |
| **Reboot Panel:** | Pressing this button causes the panel to reboot after saving any changes. |
| **Docking Station:** | • **Dock Status** - illuminates when the MVP is docked and communicating with the Docking Station.<br>• **Undock Panel** - forces the docking station to release the MVP without requiring a User Access username or password.<br>• **Disable Docking Station LED** - disables the display of the LEDs on the docking station. |

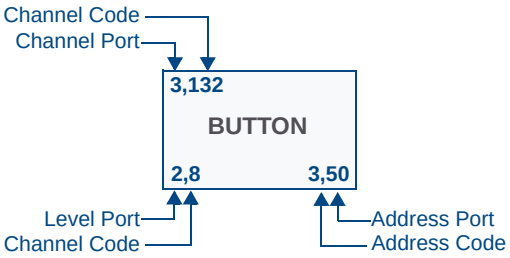



**FIG. 48** Function Show example

## Protected Setup Navigation Buttons

The Protected Setup Navigation Buttons (FIG. 49 and FIG. 50) appear on the left of the panel screen when the *Protected Setup* page is currently active.

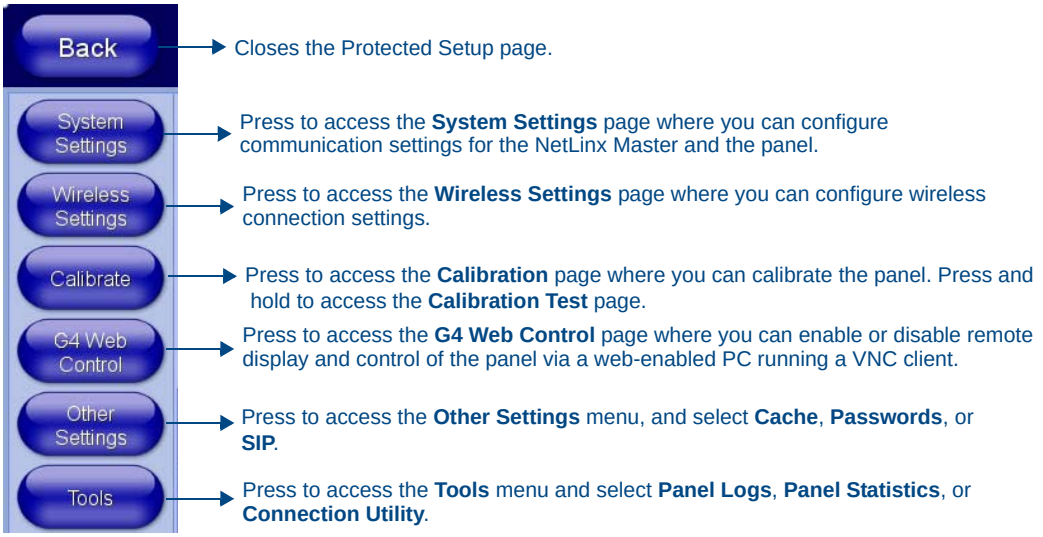



**FIG. 49** Protected Setup Navigation Buttons (MVP-7500)

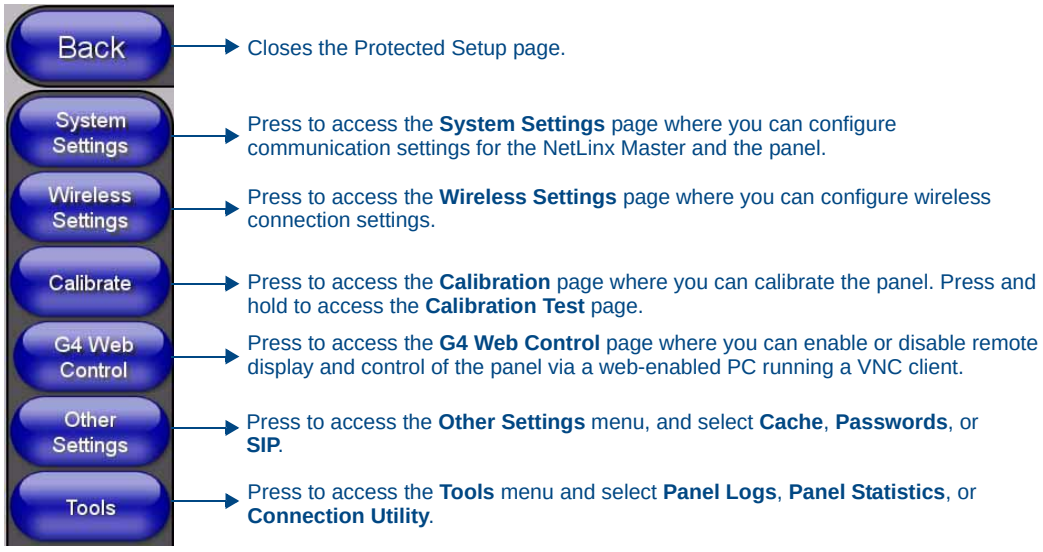



**FIG. 50** Protected Setup Navigation Buttons (MVP-8400)

## Security Settings

The **Security** button on the **Protected Setup** page has three settings: *Standard Security*, *Secure*, and *DoD*. Each setting has different features for touch panel security:

| Security Profile Features | |
|---|---|
| Standard Security: | • Factory default, shipped in this configuration.<br>• Default Protected Setup Password is "**1988**".<br>• Remote login uses Telnet. |
| Secure: | • Default Protected Setup Password is "**Amx1234!**".<br>• Minimum password requirement is 8 characters with at least one numeric character.<br>• Remote login uses SSH.<br>• Remote login user name is "**amx**".<br>• Login failure attempt pauses 4 seconds before another login attempt is allowed.<br>• After 3 consecutive unsuccessful SSH login attempts, login lockout is enabled for 15 minutes.<br>• Login and logout audit logging is enabled. |
| DOD: | • Default Protected Setup Password is "**Amx1234!**".<br>• Minimum password requirement is 8 characters with at least one numeric character, one uppercase character, one lower case character, and one special character, with no duplicate adjacent characters.<br>• Remote login uses SSH.<br>• Remote login user name is "**amx**".<br>• Login failure attempt pauses 4 seconds before another login attempt is allowed.<br>• After 3 consecutive unsuccessful SSH login attempts, login lockout is enabled for 15 minutes.<br>• Login and logout audit logging is enabled.<br>• DoD login banner is enabled. |

Toggling between these three immediately and automatically resets the existing password to the default password for that setting. With an unsecured panel using the *Standard Security* setting, the default password is **1988**. With panels using either the *Secure* or the *DoD* settings, the default password is **Amx1234!** (paying attention to the case of the letters). Entering the existing password will not work and the default will need to be entered at this point will allow access to the *Protected Settings* page and allow resetting of the password to a new one.


*If the **Security** button setting is changed in any way, even if it is toggled back to its original setting, the password is automatically reset to the default for the chosen setting. You MUST use the new default of **1988** (Standard Security) or **Amx1234!** (Secure or DoD) to re-enter the* Protected Settings *page.*

For more information on configuring AMX devices for a secure environment, please refer to the guide *Security Profiles: Configuring AMX Devices For Installation Into a Secure Environment*, available at **www.amx.com**.

## System Settings Page

The *System Settings* page (FIG. 51 and FIG. 52) displays sets the NetLinx Master's communication settings.

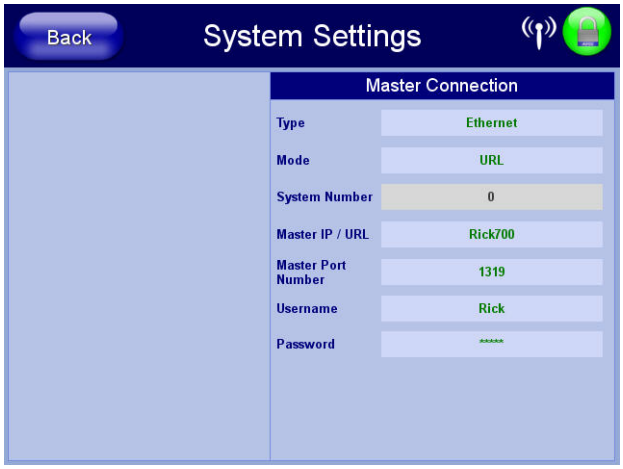



**FIG. 51** System Settings page (MVP-7500)

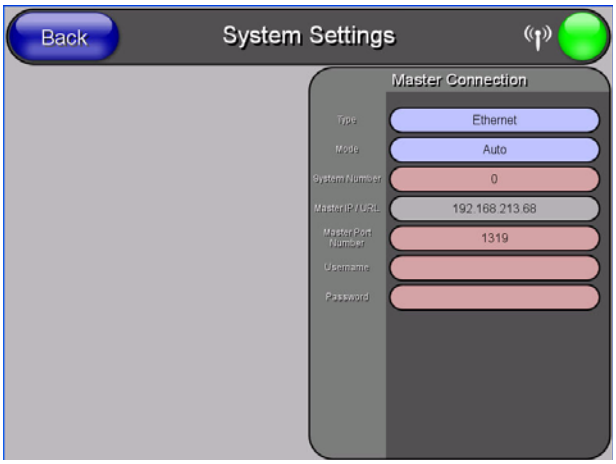



**FIG. 52** System Settings page (MVP-8400)

The elements of this page include:

| System Settings Page Elements | |
|---|---|
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |

| System Settings Page Elements (Cont.) | |
|---|---|
| **Master Connection:** | Sets the NetLinx Master communication values: |
| Type | Sets the NetLinx Master to communicate with the panel via either USB or Ethernet. This is based on the cable connection from the rear.<br>***Note**: ICSNet is not a supported option on this panel.*<br>• *Ethernet* is a CAT-5 cable (10/100Base T terminated in an RJ-45 connector) used to network computers together and is used in most LAN (local area networks). This description is also used to refer to both wired and wireless communication.<br>• *USB* option cannot be used on Modero panels which are not equipped with a rear USB port. |
| **Master Connection (Cont.):** | |
| Mode | Cycles between the connection modes: URL, Listen, and Auto.<br>*(Ethernet Only - disabled when USB is selected)*<br>• **URL** - In this mode, enter the IP/URL, Master Port Number, and username/password (if used) on the Master. The System Number field is read-only - the panel obtains this information from the Master.<br>• **Listen** - In this mode, add the panel address into the URL List in NetLinx Studio and set the connection mode to Listen. This mode allows the Modero touch panel to "listen" for the Master's communication signals. The System Number and Master IP/URL fields are read-only.<br>• **Auto** - In this mode, enter the System Number and a username/password (if applicable). Use this mode when both the panel and the NetLinx Master are on the same Subnet, and the Master has its UDP feature enabled. The Master IP/URL field is read-only. |
| System Number | Allows you to enter a system number. Default value is 0 (zero).<br>*(ETHERNET Only - disabled when USB is selected)* |
| Master IP/URL | Sets the Master IP or URL of the NetLinx Master.<br>*(ETHERNET Only - disabled when USB is selected)* |
| Master Port Number | Allows you to enter the port number used with the NetLinx Master.<br>• Default = 1319<br>*(ETHERNET Only - disabled when USB is selected)* |
| Username/Password | If the target Master has been previously secured, enter the alpha-numeric string (into each field) assigned to a pre-configured user profile on the Master. This profile should have the pre-defined level of access/configuration rights. |

Refer to the *Step 3: Choose a Master Connection Mode* section on page 29 for more detailed information on using the System Settings page.

## Wireless Settings Page

Use the options on the *Wireless Settings* page (FIG. 53 and FIG. 54) to configure communication settings for the wireless CF card (802.11b/g), and read the device number assigned to the panel.

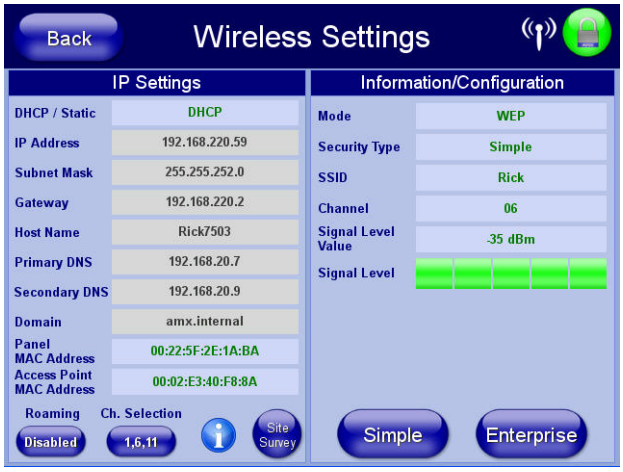



**FIG. 53** Wireless Settings Page (MVP-7500)


**FIG. 54** Wireless Settings Page (MVP-8400)

Features on this page include:

| Wireless Settings Page | |
|---|---|
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |

| Wireless Settings Page (Cont.) | |
|---|---|
| **IP Settings:** | Sets the IP communication values for the panel: |
| DHCP/STATIC | Sets the panel to either DHCP or Static communication modes.<br>• *DHCP* - a temporary IP Addresses is assigned to the panel by a DHCP server.<br>• *Static IP* is a permanent IP Address assigned to the panel. If Static IP is selected, the other *IP Settings* fields are enabled (below). |
| IP Address | Enter the secondary IP address for this panel. |
| Subnet Mask | Enter the subnetwork address for this panel. |
| Gateway | Enter the gateway address for this panel. |
| Host Name | Enter the host name for this panel. |
| Primary DNS | Enter the address of the primary DNS server used by this panel for host name lookups. |
| Secondary DNS | Enter the secondary DNS address for this panel. |
| Domain | Enter a unique name to the panel for DNS look-up. |
| MAC Address | This unique address identifies the wireless Ethernet card in the panel (read-only). |
| Active Roaming on Channels 1,6,11 | When enabled, the device is actively roaming on the channels 1, 6, and 11. By default, Active Roaming is disabled.<br>Of all the frequency channels that are assigned for wireless, only three are non-overlapping frequencies that do not interfere with each other. Non-overlapping channels avoid the interference that can affect the signal. |
| **Access Point MAC Address:** | This unique address identifies the Wireless Access Point (WAP) used by this panel for wireless communication (read-only).<br>• **Site Survey** button: Launches the Site Survey page. The options on this page allow you to detect ("sniff-out") all WAPs transmitting within range of the panel's *NXA-WC80211GCF* Wi-Fi card.<br>Data displayed on the *Site Survey* page is categorized by:<br>- **Network Name (SSID**) - WAP names<br>- **Channel (RF)** - channels currently being used by the WAP<br>- **Security Type** - security protocol enabled on the WAP, if detectable<br>- **Signal Strength** - None, Poor, Fair, Good, Very Good, and Excellent<br>- **MAC Address** - Unique identification of the transmitting Access Point<br>• Refer to the *Using the Site Survey tool* section on page 22 for more detailed information on the *SIte Survey* page.<br>• When communicating with a NXA- WAP200G, enter the MAC Address (**BSSID**) of the target WAP as the Access Point MAC Address. Refer to the ***WAP200G*** *Instruction Manual* for more information. |
| **Roaming:** | This button allows selection between three states: Disabled, Active, and Averaged:<br>• **Disabled** - No roaming: this setting will not scan for SSIDs until the panel loses its connection to the WAP. It will then roam to first matching SSID it finds on any channel.<br>• **Active** - Faster roaming. This setting actively scans channels 1, 6, and 11 for matching IDs<br>• **Averaged** - Slower roaming: designed for noisy wireless environments. This setting actively selects channels 1. 6, and 11 for matching SSIDs. When the site survey falls below -65dBm, the connection will roam to the nearest access point to a connection whose site survey is at least 10 dBm better than the previous one. |

| Wireless Settings Page (Cont.) | |
|---|---|
| **Channel Selection:** | Pressing this button presents a popup that gives the user the option, in high-interference areas, of excluding three channel groups in order to find the best possible connection.<br>• **Channel 1** includes channels 1, 2, and 3.<br>• **Channel 6** includes channels 4, 5, 6, 7, and 8.<br>• **Channel 11** includes channels 9, 10, 11, 12, and 13.<br>The default on the popup allows scanning on all three channel groups. Click the checkmark to exclude each channel group: any excluded channel group will be marked with a red "X". |
| **Information:** | Pressing this button opens a popup that explains the particular functions of the **Roaming** and **Channel Selection** buttons. |
| **Site Survey:** | Launches the *Site Survey* page. The options on this page allow you to detect ("sniff-out") all WAPs transmitting within range of the panel's *NXA-WC80211GCF* Wi-Fi card (this feature is not available with the 802.11b).<br>Data displayed on the **Site Survey** page is categorized by:<br>- **Network Name (SSID**) - WAP names<br>- **Channel (RF)** - channels currently being used by the WAP<br>- **Security Type** - security protocol enabled on the WAP, if detectable<br>- **Signal Strength** - None, Poor, Fair, Good, Very Good, and Excellent<br>- **MAC Address** - Unique identification of the transmitting Access Point<br>• Refer to the *Using the Site Survey tool* section on page 22 for more detailed information on the SIte Survey page.<br>When communicating with a NXA- WAP200G, enter the MAC Address (**BSSID**) of the target WAP as the Access Point MAC Address. Refer to the ***WAP200G*** *Instruction Manual* for more information. |
| **Information/Configuration:** | • **Mode -** Displays the current Security Type selected via either the Simple or Enterprise options.<br>• **Security Type -** Displays whether the currently used security type is *Simple* or *Enterprise*.<br>• **SSID -** Displays the currently used SSID of the target WAP.<br>• **Channel -** The RF channel being used for connection to the WAP (read-only).<br>• **Signal Level Value -** Displays the quality of the link from the wireless NIC to the Wireless Access Point (direct sequence spread spectrum) in real time (*None*, *Poor*, *Fair*, *Good*, *Very Good*, and *Excellent*).Even when link quality is at its lowest you still have a connection, and the ability to transmit and receive data, even if at lower speeds.<br>***Note:*** *"Signal Level Value" and "Signal Level" are applicable to RF connections only. It is possible to have an RF signal to a WAP, but be unable to communicate with it because of either incorrect IP or encryption settings.*<br>• **Signal Level -** This bar graph demonstrates the strength of the current signal. |
| **Simple/Enterprise:** | • Opens either the Wireless Security: Simple Mode or the Wireless Security: Enterprise Mode windows. |

Pressing the **Simple** or **Enterprise** buttons at the bottom of the *Information/Configuration* section open an appropriate Wireless Security window for Simple Mode (FIG. 55) or Enterprise Mode (FIG. 56). Simple Mode is best used for smaller installations that use a single Master, such as for residences or smaller office environments. Enterprise Mode is intended for installations that use multiple Masters, where a wireless device may need to switch between multiple wireless access points connected to different Masters in a network.


**FIG. 55** Wireless Security: Simple Mode

| Wireless Security: Simple Mode | |
|---|---|
| **Security Type:** | This field may be switched between WEP, WPA-PSK, and Open. If WEP is selected, the button to the right may be switched between *64* and *128*.<br>• **WEP** security requires that both a target WAP be identified and an encryption method be implemented prior to establishing communication. (Refer to the *WEP Settings* section on page 62 for further details.)<br>• **WPA-PSK** security is designed for environments where is it desirable to use WPA or WPA2, but an *802.1x authentication server is not available*. PSK connections are more secure than WEP and are simpler to configure since they implement dynamic keys but share a key between the WAP and the panel (client). (Refer to the *WPA-PSK Settings* section on page 63 for further details.)<br>• **Open** security does not utilize any encryption methodology, but requires an SSID (alpha-numeric) entry. This entry must match the Network Name (SSID) entry of the target WAP so the panel knows what device it is using to communicate with the network. (Refer to the following *Open Settings* section on page 61 for further details.) |
| **SSID:** | Press this field to enter a 32-character Network Name in the *Network Name* keypad. |
| **Password:** | This field is only enabled when *WPA-PSK* is selected as the Security Type. Clicking this field opens the *Password/Pass Phrase* keyboard |
| **WEP Keys:** | These buttons are only enabled when *WEP* is selected as the Security Type. Press each one to open a keyboard to enter a 10-digit WEP Key. |
| **Default Key:** | This field is only enabled when WEP is selected as the Security Type. Press the field to select which of the four WEP Keys is the default. |
| **Current Key:** | This field is only populated when WEP is selected as the Security Type. |
| **Authentication:** | This field is only enabled when WEP is selected as the Security Type. Press the field to select between *Shared* and *Open*. |
| **Cancel/Save:** | Press **Cancel** to return to the *Wireless Settings* page without saving any changes. Press **Save** to save all changes and return to the *Wireless Settings* page. |


**FIG. 56** Wireless Security: Enterprise Mode

| Wireless Security: Enterprise Mode | |
|---|---|
| **Security Type:** | Pressing this field changes the security type being used between EAP-PEAP, EAP-TTLS, EAP-TLS, EAP-LEAP, and EAP-FAST.<br>• **EAP-PEAP** security is designed for wireless environments where it is necessary to securely transmit data over a wireless network. (Refer to the *EAP-PEAP Settings* section on page 67 for details. For information on uploading a certificate file, refer to the *AMX Certificate Upload Utility* section on page 168.)<br>• **EAP-TTLS** security is designed for wireless environments where it is necessary to first have a Radius server directly validate the identity of the client (panel) before allowing it access to the network. (Refer to the *EAP-TTLS Settings* section on page 68 for details. For information on uploading a certificate file, refer to the *AMX Certificate Upload Utility* section on page 168.)<br>• **EAP-TLS** security is designed for wireless environments where it is necessary to securely transmit data over a wireless network by adding an additional level of security protocol via the use of a private key. (Refer to the *EAP-TLS Settings* section on page 70 for details. For information on uploading a certificate file, refer to the *AMX Certificate Upload Utility* section on page 168.)<br>• **EAP-LEAP** security is designed for wireless environments where it is not required to have both a client or server certificate validation scheme in place, yet necessary to securely transmit data over a wireless network. (Refer to the *EAP-LEAP Settings* section on page 64 for details.)<br>• **EAP-FAST** security is designed for wireless environments where security and ease of setup are equally desirable. (Refer to the *EAP-FAST Settings* section on page 65 for details.) |
| **SSID:** | Press this field to enter a 32-character Network Name in the *Network Name* keypad. |
| **Identity:** | Press this field to enter a Username in the *Identity (Username)* keypad. |
| **Anon. Identity:** | This field is only enabled when selecting EAP-TTLS and EAP-FAST as a Security Type. Press this field to enter another Username in the *Anonymous Identity* keypad. |
| **Password:** | Press this field to enter a password for wireless access in the *Password* keypad. (**NOTE:** this field is greyed out when selecting EAP-TLS as a Security Type.) |
| **Certificate Authority:** | Press this field to enter the file location for a Certificate Authority certificate in the *Certificate Authority (CA)* keypad. |
| **PEAP Version:** | This field is only enabled when selecting EAP-PEAP as a Security Type. Press this field to cycle between the available installed versions of PEAP. |

| Wireless Security: Enterprise Mode (Cont.) | |
|---|---|
| **Inner Auth. Type:** | This field is only enabled when selecting EAP-PEAP or EAP-TTLS as a Security Type. Press this field to cycle between MSCHAPv2, GTC, OTP, and MD5. |
| **Client Certificate:** | This field is only enabled when selecting EAP-TLS as a Security Type. Press this field to enter a file location in the Client Certificate File Location keypad. |
| **Private key:** | This field is only enabled when selecting EAP-TLS as a Security Type. Press this field to enter a file location in the *Client Private Key File Location* keypad. |
| **Private Key Password:** | This field is only enabled when selecting EAP-TLS as a Security Type. Press this field to enter the password for the private key in the *Private Key Password* keypad. |
| **Auto PAC Provisioning:** | This field is only enabled when selecting EAP-FAST as a Security Type. Press this field to enable or disable the use of PAC files. |
| **PAC File Location:** | This field is only enabled when selecting EAP-FAST as a Security Type, and only when Auto PAC Provisioning is Disabled. Press this field to enter a file location in the *PAC File Location* keypad. |
| **Auto Key Renewal:** | This field is blocked out, but will read "NEVER" when selecting EAP-FAST as a Security Type. |
| **Cancel/Save:** | Press the **Cancel** button to return to the *Wireless Settings* Page without saving any changes. Press the **Save** button to save all changes and return to the *Wireless Settings* Page. |

## Wireless Settings

The options on the *Wireless Security: Simple Mode* and *Wireless Security: Enterprise Mode* windows allow you to select from the wireless security methods supported by the NXA-WC80211GCF Wi-Fi card. These security methods incorporate *WPA*, *WPA2*, and *EAP* technology (some of which require the upload of unique certificate files to a target panel).

Refer to the *Appendix B - Wireless Technology* section on page 163 for more further information.

Some encryption and security features may/may not be supported depending on the type of wireless card being used:

| Wireless Security Support | |
|---|---|
| **802.11g Wi-Fi CF card:** | • Open (Clear Text)<br>• Static WEP (64-bit and 128-bit key lengths)<br>• WPA-PSK<br>• EAP security (with and without certificates)<br>• WAP SIte Survey |

Refer to the *Configuring a Wireless Network Access* section on page 20 for more information on configuring the panel for wireless network access using the various security options.

## Open Settings

Open security does not utilize any encryption methodology, but requires an SSID (alpha-numeric) entry. This entry must match the Network Name (SSID) entry of the target WAP so the panel knows what device it is using to communicate with the network.

| Open Settings | |
|---|---|
| **SSID (Service Set Identifier):** | Opens an on-screen keyboard to enter the SSID name used on the target WAP.<br>The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network.<br>• The SSID is case sensitive and must not exceed 32 characters.<br>• Make sure this setting is the same for all points in your wireless network.<br>• NXA-WAP200Gs use **AMX** as their default SSID.<br>• If this field is left blank, the panel will attempt to connect to the first available WAP. |

| Open Settings (Cont.) | |
|---|---|
| **Save/Cancel:** | • **Save** - store the new security information, apply changes, and return to the previous page.<br>• **Cancel** - discard changes and return to the previous page. |

- Refer to the *Configuring a Wireless Network Access* section on page 20 for further details on these security options.
- Refer to the *Using the Site Survey tool* section on page 22.

### WEP Settings

WEP security requires that both a target WAP be identified and an encryption method be implemented prior to establishing communication. In addition to providing both Open and Shared Authentication capabilities, this page also supports Hexadecimal and ASCII keys.

| WEP Settings | |
|---|---|
| **SSID (Service Set Identifier):** | Opens an on-screen keyboard to enter the SSID name used on the target WAP.<br>The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network.<br>• The SSID is case sensitive and must not exceed 32 characters.<br>• Make sure this setting is the same for all points in your wireless network.<br>• NXA-WAP200Gs use **AMX** as their default SSID.<br>• If this field is left blank, the panel will attempt to connect to the first available WAP. |
| **WEP 64 / WEP 128:** | Cycles through the available encryption options: *64 or 128 Bit Key Size*.<br>"WEP" (Wired Equivalent Privacy) is an 802.11 security protocol designed to provide wireless security equivalent to wired networks.<br>• **WEP64** enables WEP encryption using a 64 Bit Key Size. All packets are transmitted with their contents encrypted using the Default WEP Key.<br>• **WEP128** enables WEP encryption using a 128 Bit Key Size. All packets are transmitted with their contents encrypted using the Default WEP Key.<br>• If the key is not the correct size, the system will resize it to match the number of bits required for the WEP encryption mode selected. |
| **Generate (Passphrase):** | This button displays an on-screen keyboard which allows you to enter a passphrase. The panel then automatically generates four WEP keys (compatible only with Modero panels). Enter these WEP keys into the target WAP.<br>When working with multiple panels, WEP Keys must be entered into the WAP for each panel.<br>• All Modero panels use the same code key generator. Therefore, this Passphrase generates identical keys on any Modero panel.<br>• The Passphrase generator is case sensitive.<br>***Note**: This Key generator is unique to Modero panels and does not generate the same keys as non-AMX wireless devices. For example, a Current Key string generated anywhere else will not match those created on Modero panels.* |
| **Default Key:** | Cycles through the four available WEP key identifiers to select a WEP key to use. As the Default Key value is altered (through selection) the corresponding "Current Key" is displayed. Each Current Key corresponds to a WEP key.<br>This feature is useful for accessing different networks without having to reenter that networks' WEP key. It is also sometimes used to set up a rotating key schedule to provide an extra layer of security. |

| WEP Settings (Cont.) | |
|---|---|
| **WEP Keys:** | This feature provides another level of security by selecting up to four WEP Keys.<br>Push any of the four buttons to open an on-screen keyboard. Both ASCII and HEX keys are supported. Up to four keys can be configured for both.<br>• An ASCII key utilizes either 5 or 13 ASCII characters<br>• A HEX key utilizes either 10 or 26 Hexidecimal characters<br>Press **Done** to accept any changes and save the new value.<br>***Note**: A 64-bit key will be 10 characters in length while a 128-bit key will be 26 characters in length. The length of the key entered determines the level of WEP encryption employed (64 or 128-bit). 128-bit keys may be used if supported by the internal wireless card.* |
| **Current Key:** | Displays the current WEP key in use.<br>• When working with a single panel and a single WAP, it is recommended that you manually enter the *Current Key* from the WAP into the selected WEP Key.<br>• When working with a single WAP and multiple panels, it is recommended that you generate a Current Key using the same passphrase on all panels and then enter the panel-produced WEP key manually into the Wireless Access Point.<br>• Keys may also be examined by touching the key buttons and noting the keyboard initialization text.<br>• Use the on-screen keyboard's **Clear** button to erase stored key information. |
| **Authentication:** | Toggles between the two authentication modes: *Open + WEP* (broadcast publicly) or *Shared + WEP* (encrypted).<br>• An *Open + WEP* network allows connections from any client without authentication.<br>• A *Shared + WEP* network requires the client to submit a key which is shared by the network WAP before it is given permission to associate with the network. In this case the key is the same as the WEP encryption key.<br>In either case, if WEP encryption has been enabled, the client will still require the WEP key to encrypt and decrypt packets in order to communicate with the network. |
| **Save/Cancel:** | • **Save** - store the new security information, apply changes, and return to the previous page.<br>• **Cancel** - discard changes and return to the previous page. |

- Refer to the *Configuring a Wireless Network Access* section on page 20 for further details on these security options.
- Refer to the *Using the Site Survey tool* section on page 22 for more information on using this feature.

## WPA-PSK Settings

WPA-PSK security is designed for environments where is it desirable to use WPA or WPA2, but an 802.1x authentication server is not available. PSK connections are more secure than WEP and are simpler to configure since they implement dynamic keys but share a key between the WAP and the panel (client).

Using WPA-PSK, the encryption on the WAP could either be WPA or WPA2. The firmware in the panel will automatically connect to the WAP using the correct encryption. The WPA encryption type is configured on the WAP, not in the firmware.

WAPs do not display "WPA" or "WPA2" on their configuration screens:

- *WPA* is normally displayed as *TKIP*.
- *WPA2* is normally displayed as *AES CCMP*.

The following fields are required: *SSID* and *Password/Pass Phrase*.

- Enter the SSID of the WAP.
- Enter a pass phrase with a minimum of 8 characters and a maximum of 63.
- The exact same pass phrase (including capitalization) must be entered in the access point.
- Refer to the *Configuring a Wireless Network Access* section on page 20 for details on these security options.

| WPA-PSK Settings | |
|---|---|
| **SSID (Service Set Identifier):** | Opens an on-screen keyboard to enter the SSID name used on the target WAP.<br>The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network.<br>• The SSID is case sensitive and must not exceed 32 characters.<br>• Make sure this setting is the same for all points in your wireless network.<br>• NXA-WAP200Gs use **AMX** as their default SSID.<br>• If this field is left blank, the panel will attempt to connect to the first available WAP. |
| **Password:** | Opens an on-screen keyboard to enter a passphrase (password).<br>• This alpha-numeric string must use a minimum of 8 characters and a maximum of 63.<br>• The exact pass phrase string (including capitalization) must be entered on the target WAP. |
| **Save/Cancel:** | • **Save** - store the new security information, apply changes, and return to the previous page.<br>• **Cancel** - discard changes and return to the previous page. |

- Refer to the *Using the Site Survey tool* section on page 22 for more information on using this tool.

## EAP-LEAP Settings

EAP (Extensible Authentication Protocol) is an Enterprise authentication protocol that can be used in both wired and wireless network environments. EAP requires the use of an 802.1x Authentication Server, also known as a Radius server. The configuration fields described below take variable length strings as inputs. An on-screen keyboard is opened when these fields are selected.

LEAP (Lightweight Extensible Authentication Protocol) was developed to transmit authentication information securely in a wireless network environment.


*LEAP does not use client (panel) or server (RADIUS) certificates and is therefore one of the least secure EAP security methods but can be utilized successfully by implementing sufficiently complex passwords.*

EAP-LEAP security is designed for wireless environments where it is not required to have a client or server certificate validation scheme in place, yet necessary to transmit data securely over a wireless network.

| EAP-LEAP Settings | |
|---|---|
| **SSID (Service Set Identifier):** | Opens an on-screen keyboard to enter the SSID name used on the target WAP.<br>The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network.<br>• The SSID is case sensitive and must not exceed 32 characters.<br>• Make sure this setting is the same for all points in your wireless network.<br>• NXA-WAP200Gs use **AMX** as their default SSID.<br>• With EAP security, the SSID of the WAP *must* be entered. If it is left blank, the panel will try to connect to the first access point detected that supports EAP. However, a successful connection is not guaranteed because the detected WAP may be connected to a RADIUS server, which may not support this EAP type and/or have the proper user identities configured. |
| **Identity:** | Opens an on-screen keyboard. Enter an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server).<br>***Note**: This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Typically, this is in the form of a username such as: jdoe@amx.com.* |

| EAP-LEAP Settings (Cont.) | |
|---|---|
| **Password:** | Opens an on-screen keyboard. Enter the network password string specified for the user entered within the *Identity* field (used by the panel to identify itself to an Authentication (RADIUS) Server)<br>***Note**: This information is similar to the password entered to gain access to a secured workstation.* |
| **Save/Cancel:** | • **Save** - store the new security information, apply changes, and return to the previous page.<br>• **Cancel** - discard changes and return to the previous page. |

## EAP-FAST Settings

EAP-FAST (Flexible Authentication via Secure Tunneling) security was designed for wireless environments where security and ease of setup are equally desirable. EAP-FAST uses a certificate file, however it can be configured to download the certificate automatically the first time the panel attempts to authenticate itself. Automatic certificate downloading is convenient but slightly less secure, since its the certificate is transferred wirelessly and could theoretically be "sniffed-out".

| EAP-FAST Settings | |
|---|---|
| **SSID (Service Set Identifier):** | Opens an on-screen keyboard to enter the SSID name used on the target WAP.<br>The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network.<br>• The SSID is case sensitive and must not exceed 32 characters.<br>• Make sure this setting is the same for all points in your wireless network.<br>• NXA-WAP200Gs use **AMX** as their default SSID.<br>• With EAP security, the SSID of the WAP *must* be entered. If it is left blank, the panel will try to connect to the first access point detected that supports EAP. However, a successful connection is not guaranteed because the detected WAP may be connected to a RADIUS server, which may not support this EAP type and/or have the proper user identities configured. |
| **Identity:** | Opens an on-screen keyboard. Enter an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server).<br>***Note**: This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Typically, this is in the form of a username such as: jdoe@amx.com.* |
| **Anonymous Identity:** | Opens an on-screen keyboard. Enter an IT provided alpha-numeric string which (similar to the username) used as the identity, but that does not represent a real user.<br>This information is used as a fictitious name which might be seen by sniffer programs during the initial connection and setup process between the panel and the Radius server. In this way the real identity (username) is protected. Typically, this is in the form of a fictitious username such as: anonymous@amx.com |
| **Password:** | Opens an on-screen keyboard. Enter the network password string specified for the user entered within the *Identity* field (used by the panel to identify itself to an Authentication (RADIUS) Server)<br>***Note**: This information is similar to the password entered to gain access to a secured workstation.* |

| EAP-FAST Settings (Cont.) | |
|---|---|
| **Automatic PAC Provisioning:** | This selection toggles PAC (Protected Access Credential) Provisioning - **Enabled** *(automatic)* or **Disabled** *(manual)*.<br>• If **Enabled** is selected, the following *PAC File Location* field is disabled, because the search for the PAC file is done automatically.<br>• If **Disabled** is selected, the user is required to manually locate a file containing the PAC shared secret credentials for use in authentication. In this case, the IT department must create a PAC file and then transfer it into the panel using the *AMX Certificate Upload* application.<br>Note: Even when automatic provisioning is enabled, the PAC certificate is only downloaded the first time that the panel connects to the RADIUS server. This file is then saved into the panel's file system and is then reused from then on. It is possible for the user to change a setting (such as a new Identity) that would invalidate this certificate.<br>In that case, the panel must be forced to download a new PAC file.<br>To do this, set Automatic PAC Provisioning to *Disabled* and then back to *Enabled*. This forces the firmware to delete the old file and request a new one. |
| **PAC File Location:** | This field is used when the previous Automatic PAC Provisioning option has been **Disabled**.<br>• When pressed, the panel displays an on-screen PAC File Location keyboard which allows you to enter the name of the file containing the PAC shared secret credentials for use in authentication.<br>• This field is only valid when the automatic PAC provisioning feature has been enabled via the previous field. |
| **Save/Cancel:** | • **Save** - store the new security information, apply changes, and return to the previous page.<br>• **Cancel** - discard changes and return to the previous page. |

- Refer to the *EAP Authentication* section on page 166 for further details on these security options.
- Refer to the *Using the Site Survey tool* section on page 22 for more information on using this feature.

## EAP-PEAP Settings

PEAP (Protected Extensible Authentication Protocol) was developed as a way to securely transmit authentication information, such as passwords, over a wireless network environment. PEAP uses only server-side public key certificates and therefore does not need a client (panel) certificate which makes the configuration and setup easier.

There are two main versions of the PEAP protocol supported by panel's DeviceScape Wireless Client:

- PEAPv0
- PEAPv1

PEAP uses inner authentication mechanisms supported by the DeviceScape Wireless Client, the most common of which are:

- MSCHAPv2 with PEAPv0
- GTC with PEAPv1

EAP-PEAP security is designed for wireless environments where it is necessary to transmit data securely over a wireless network.

| EAP-PEAP Settings | |
|---|---|
| **SSID (Service Set Identifier):** | Opens an on-screen keyboard to enter the SSID name used on the target WAP. The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network.<br>• The SSID is case sensitive and must not exceed 32 characters.<br>• Make sure this setting is the same for all points in your wireless network.<br>• NXA-WAP200Gs use **AMX** as their default SSID.<br>• With EAP security, the SSID of the WAP *must* be entered. If it is left blank, the panel will try to connect to the first access point detected that supports EAP. However, a successful connection is not guaranteed because the detected WAP may be connected to a RADIUS server, which may not support this EAP type and/or have the proper user identities configured. |
| **Identity:** | Opens an on-screen keyboard. Enter an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server).<br>***Note**: This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Typically, this is in the form of a username such as: jdoe@amx.com.* |
| **Password:** | Opens an on-screen keyboard. Enter the network password string specified for the user entered within the *Identity* field (used by the panel to identify itself to an Authentication (RADIUS) Server)<br>***Note**: This information is similar to the password entered to gain access to a secured workstation.* |
| **Certificate Authority:** | When pressed, the panel displays an on-screen Certificate Authority (CA) File Location keyboard which allows you to enter the name of the certificate authority file which is used to validate the server certificate. This field is optional.<br>If a server certificate is used, it should first be downloaded into the panel and the *Certificate Authority* field should then be set to the name of that certificate file. No file path should be used for this setting as all certificates are stored in a specific directory that the user cannot control or change.<br>• Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information. |
| **PEAP Version:** | When pressed, this field cycles through the choices of available PEAP: **PEAPv0, PEAPv1,** or **PEAPv1 w/peaplabel=1**. |

| EAP-PEAP Settings (Cont.) | |
|---|---|
| **Inner Authentication Type:** | When pressed, this field cycles through the choices of available Inner Authentication mechanisms supported by the Devicescape Secure Wireless Client. The most commonly used are: **MSCHAPv2** and **GTC**.<br>• MSCHAPv2 (*used with PEAPv0*)<br>• TLS<br>• GTC (*used with PEAPv1*)<br>• OTP<br>• MD5-Challenge |
| **Save/Cancel:** | • **Save** - store the new security information, apply changes, and return to the previous page.<br>• **Cancel** - discard changes and return to the previous page. |

- Refer to the *EAP Authentication* section on page 166 for further details on these security options.
- Refer to the *Using the Site Survey tool* section on page 22 for more information on using this feature.

## EAP-TTLS Settings

TTLS (EAP Tunneled Transport Layer Security) is an authentication method that does not use a client certificate to authenticate the panel. However. this method is more secure than PEAP because it does not broadcast the identity of the user. Setup is similar to PEAP, but differs in the following areas:

- An anonymous identity must be specified until the secure tunnel between the panel and the Radius server is setup to transfer the real identity of the user.
- There is no end-user ability to select from the different types of PEAP.
- Additional Inner Authentication choices are available to the end-user.

EAP-TTLS security is designed for wireless environments where it is necessary to have the Radius server directly validate the identity of the client (panel) before allowing it access to the network. This validation is done by tunneling a connection through the WAP and directly between the panel and the Radius server. Once the client is identified and then validated, the Radius server disconnects the tunnel and allows the panel to access the network directly via the target WAP.

| EAP-TTLS Settings | |
|---|---|
| **SSID (Service Set Identifier):** | Opens an on-screen keyboard to enter the SSID name used on the target WAP.<br>The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network.<br>• The SSID is case sensitive and must not exceed 32 characters.<br>• Make sure this setting is the same for all points in your wireless network.<br>• NXA-WAP200Gs use **AMX** as their default SSID.<br>• With EAP security, the SSID of the WAP *must* be entered. If it is left blank, the panel will try to connect to the first access point detected that supports EAP. However, a successful connection is not guaranteed because the detected WAP may be connected to a RADIUS server, which may not support this EAP type and/or have the proper user identities configured. |
| **Identity:** | Opens an on-screen keyboard. Enter an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server).<br>***Note**: This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Typically, this is in the form of a username such as: jdoe@amx.com.* |
| **Anonymous Identity:** | Opens an on-screen keyboard. Enter an IT provided alpha-numeric string which (similar to the username) used as the identity, but that does not represent a real user.<br>This information is used as a fictitious name which might be seen by sniffer programs during the initial connection and setup process between the panel and the Radius server. In this way the real identity (username) is protected. Typically, this is in the form of a fictitious username such as: anonymous@amx.com |

| EAP-TTLS Settings (Cont.) | |
|---|---|
| **Password:** | Opens an on-screen keyboard. Enter the network password string specified for the user entered within the *Identity* field (used by the panel to identify itself to an Authentication (RADIUS) Server)<br>***Note**: This information is similar to the password entered to gain access to a secured workstation.* |
| **Certificate Authority:** | When pressed, the panel displays an on-screen Certificate Authority (CA) File Location keyboard which allows you to enter the name of the certificate authority file which is used to validate the server certificate.<br>This field is optional.<br>If a server certificate is used, it should first be downloaded into the panel and the *Certificate Authority* field should then be set to the name of that certificate file. No file path should be used for this setting as all certificates are stored in a specific directory that the user cannot control or change.<br>• Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information. |
| **Inner Authentication Type:** | When pressed, this field cycles through the choices of available Inner Authentication mechanism supported by the Devicescape Secure Wireless Client:<br>• MSCHAPv2 (*default because its the most common*)<br>• MSCHAP<br>• PAP<br>• CHAP<br>• EAP-MSCHAPv2<br>• EAP-GTC<br>• EAP-OTP<br>• EAP-MD5-Challenge |
| **Save/Cancel:** | • **Save** - store the new security information, apply changes, and return to the previous page.<br>• **Cancel** - discard changes and return to the previous page. |

- Refer to the *EAP Authentication* section on page 166 for further details on these security options.
- Refer to the *Using the Site Survey tool* section on page 22 for more information on using this feature.

## EAP-TLS Settings

TLS (Transport Layer Security) was the original standard wireless LAN EAP authentication protocol. TLS requires additional work during the deployment phase but provides additional security since even a compromised password is not enough to break into an EAP-TLS protected wireless network environment.

EAP-TLS security is designed for wireless environments where it is necessary to securely transmit data over a wireless network by adding an additional level of security protocol via the use of a private key.

| EAP-TLS Settings | |
|---|---|
| **SSID (Service Set Identifier):** | Opens an on-screen keyboard to enter the SSID name used on the target WAP.<br>The SSID is a unique name used by the WAP, and is assigned to all panels on that network. An SSID is required by the WAP before the panel is permitted to join the network.<br>• The SSID is case sensitive and must not exceed 32 characters.<br>• Make sure this setting is the same for all points in your wireless network.<br>• NXA-WAP200Gs use **AMX** as their default SSID.<br>• With EAP security, the SSID of the WAP *must* be entered. If it is left blank, the panel will try to connect to the first access point detected that supports EAP. However, a successful connection is not guaranteed because the detected WAP may be connected to a RADIUS server, which may not support this EAP type and/or have the proper user identities configured. |
| **Identity:** | Opens an on-screen keyboard. Enter an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server).<br>***Note**: This information is similar to a username used to login to a secured server or workstation. This works in tandem with the Password string which is similar to the password entered to gain access to a secured workstation. Typically, this is in the form of a username such as: jdoe@amx.com.* |
| **Certificate Authority:** | When pressed, the panel displays an on-screen Certificate Authority (CA) File Location keyboard which allows you to enter the name of the certificate authority file which is used to validate the server certificate.<br>This field is optional.<br>If a server certificate is used, it should first be downloaded into the panel and the *Certificate Authority* field should then be set to the name of that certificate file. No file path should be used for this setting as all certificates are stored in a specific directory that the user cannot control or change.<br>• Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information. |
| **Client Certificate:** | Opens an on-screen keyboard. Enter the name of the file containing the client (panel) certificate for use in certifying the identity of the client (panel).<br>• Refer to the *Client certificate configuration* section for information regarding Client Certificates and their parameters. |
| **Private Key:** | When pressed, the panel displays an on-screen Client Private Key File Location keyboard which allows you to enter the name of the file containing the private key.<br>• Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information. |
| **Private Key password:** | This field should only be used if the Private Key is protected with a password. If there is no password protection associated with the Private Key, then this field should be left ***blank***.<br>• When pressed, the panel displays an on-screen Private Key Password keyboard which allows you to enter an alpha-numeric password string.<br>• Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information. |
| **Save/Cancel:** | • **Save** - store the new security information, apply changes, and return to the previous page.<br>• **Cancel** - discard changes and return to the previous page. |

- Refer to the *EAP Authentication* section on page 166 for further details on these security options.

- Refer to the *Using the Site Survey tool* section on page 22 for more information on using this feature.

## Client certificate configuration

There are several ways in which a client certificate can be configured by an IT department. The client certificate and private key can both be incorporated into one file or split into two separate files. In addition, the file format used by these files could be PEM, DER, or PKCS12. These formats are described later in this section. The following table describes how to fill in the fields for each possible case.

**Client Certificate Configuration**

| Certificate Configuration | Client Certificate Field | Private Key Field |
|---|---|---|
| Single file contains both the client certificate and the private key. *Format is:* ***PEM*** *or* ***DER****.* | Enter the file name | Enter the same file name |
| First file contains the client certificate, second file contains the private key. *Format is:* ***PEM*** *or* ***DER****.* | Enter the first file name | Enter the second file name |
| Single file contains both the client certificate and the private key. *Format is:* ***PKCS12*** | Leave this field blank | Enter the file name |
| First file contains the client certificate, second file contains the private key. *Format is:* ***PKCS12*** | not supported | not supported |

AMX supports the following security certificates

- PEM (Privacy Enhanced Mail)
- DER (Distinguished Encoding Rules)
- PKCS12 (Public Key Cryptography Standard #12)


*PKCS12 files are frequently generated by Microsoft certificate applications. Otherwise, PEM is more common.*

Certificate files frequently use 5 file extensions. It can be confusing because there is not a one to one correspondence. The following table shows the possible file extension used for each certificate type:

**Certificates and their Extensions**

| Certificate Type | Possible File Extensions |
|---|---|
| PEM | .cer<br>.pem<br>.pvk |
| DER | .cer<br>.der |
| PKCS12 | .pfx |

It is important to note which certificate types are supported by the different certificate fields used on the configuration screens (PEAP, TTLS, and TLS). The following table outlines the firmware fields and their supported certificate types.

**Certificate Types Supported by the Modero Firmware**

| Configuration Field Name | Certificate File Type Supported |
|---|---|
| *Certificate Authority* field | PEM and DER |
| *Client Certificate* field | PEM and DER |
| *Private Key* field | .PEM, DER, and PKCS12 |

## Calibration Page

This page (FIG. 57) allows you to calibrate the touch panel for accurate button selection.

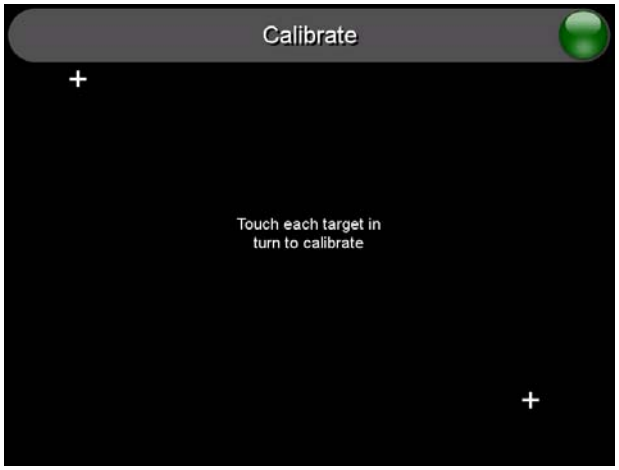



**FIG. 57** Calibration Page

- Press and hold the two lower button on both sides of the display for 6 seconds to access the Calibration page (see FIG. 88 on page 155).
- Press the crosshairs to calibrate the panel and return to the previous page.

Always calibrate the panel before its initial use, and after downloading new firmware.

NOTE

*In cases where the touch panel calibration is off to a degree that makes it difficult or impossible to navigate to this page, you can access it via G4 WebControl, so you can re-calibrate the panel.*

## G4 Web Control Settings/G4 Web Control Page

An on-board VNC (Virtual Network Computing) server allows the panel to connect to any remote PC running a VNC client. Once connected, the client can view and control the panel remotely. The options on the MVP-7500 G4 *Web Control Settings* page (FIG. 58) and the MVP-8400 Web Control page (FIG. 59) allow you to enable/disable G4 Web Control functionality.


**FIG. 58** G4 Web Control Settings Page (MVP-7500)


**FIG. 59** G4 Web Control Page (MVP-8400)

Features on this page include:

| G4 Web Control Page | |
|---|---|
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |

| G4 Web Control Page (Cont.) | |
|---|---|
| **G4 Web Control Settings:** | Sets the IP communication values for the touch panel: |
| Enable/Enabled | The Enable/Enabled button allows you to toggle between the two G4 activation settings:<br>• **Enable** - deactivates G4 Web Control on the panel.<br>• **Enabled** - activates G4 Web Control on the panel. |
| Network Interface Select | Displays **"Wireless"** when the panel is communicating via a Wireless Access Point (WAP). |
| Web Control Name | Use this field to enter a unique alpha-numeric string to be used as the panel's display name within the *Manage WebControl Connections* window of the NetLinx Security browser window. |
| Web Control Password | Use this field to enter the G4 Authentication session password required for VNC access to the panel. |
| Web Control Port | Enter the number of the port used by the VNC Web Server. Default = 5900. |
| Maximum Number of Connections | Displays the maximum number of users that can be simultaneously connected to this panel via VNC. Default = 1. |
| Current Connection Count | Displays the number of users currently connected to this panel via VNC. |
| **G4 Web Control Timeout:** | Sets the length of time (in minutes) that the panel can remain idle (no cursor movements) before the G4 Web Control session is terminated.<br>• Minimum value = 0 minutes (panel never times out)<br>• Maximum value = 240 minutes (panel times out after 240 minutes) |

NOTE

*Refer to the Using G4 Web Control to Interact with a G4 Panel* section on page 35 *for instructions on using the G4 Web Control page with the web-based NetLinx Security application.*

## Other Settings

The **Other Settings** button (FIG. 60 and FIG. 61) provides a menu to select the *Cache Settings/Cache Setup* page, *Password Setup* page, or *SIP Settings* page (MVP-8400 only). Select any option to access its page.


**FIG. 60** Other Settings Menu (MVP-7500)


**FIG. 61** Other Settings menu (MVP-8400)

## Cache Settings/Cache Setup Page

The *Cache Settings* page (MVP-7500, FIG. 62) and *Cache Setup* page (MVP-8400, FIG. 63) configures the allocation of memory for image caching. The G4 graphics engine caches images to decrease load time of previously viewed images. RAM caching is always enabled, and images (both static and dynamic) are stored in the RAM cache as they are viewed. The size of RAM cache is automatically configured to take into account available memory versus memory that may be needed by the panel later. As the RAM cache approaches its maximum size, the oldest items in the cache may be discarded to make room for newer items. If Flash caching is enabled, dynamic images that would have been discarded will be moved to Flash, since it is typically faster to retrieve images on Flash than across a network (although it is slower than RAM cache). Note that since static images are already stored on Flash, they are never moved to the Flash cache, so Flash caching applies only to dynamic images. Images in Flash cache are moved back to RAM cache the next time they are viewed. As the Flash cache approaches its maximum size, the least recently used items may be discarded to make room for new items.

Flash memory may be allocated for image caching, but RAM cache is always enabled. Flash memory is a secondary cache and is much slower than RAM cache, as it uses Compact Flash to store images. Flash memory should not be used frequently, but it may be appropriate to use Flash memory in some environments that are dynamic image intensive, at times when RAM cache is easily exhausted and the time taken to access Flash memory would be faster than network latency. For example, when large dynamic images are being used over slow wireless links, putting the images into Flash memory can help the situation, as the panel could spend more resources processing information rather than continuously waiting on images to arrive from a slow network.

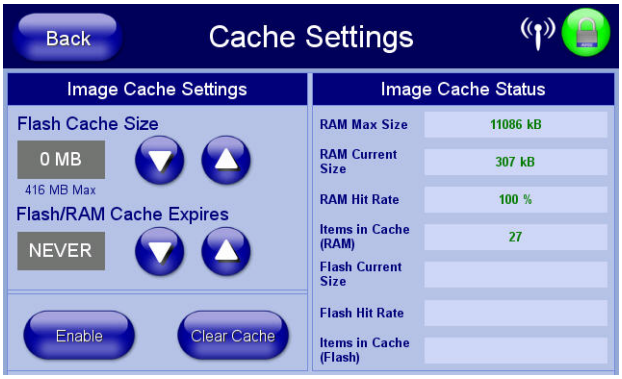



**FIG. 62** Cache Settings Page (MVP-7500)

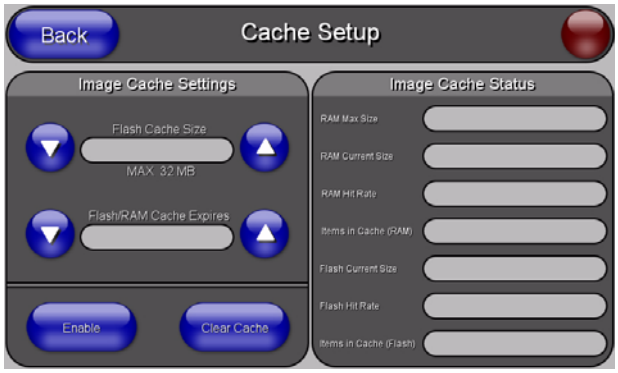



**FIG. 63** Cache Setup Page (MVP-8400)

The elements of this page include:

| Cache Settings/Cache Setup Page Elements | |
|---|---|
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |
| **Image Cache Settings:** | Allocates Flash memory for image caching. |
| Flash Cache Size | Press the Up and Down arrows to add and remove memory. Flash memory allocation cannot exceed the amount of Flash memory on the panel. |
| Flash/RAM Cache Expires | Press the Up and Down arrows to change the amount of time the images stay in cache memory. The options are:<br>• Never<br>• 2 Hours<br>• 8 Hours<br>• 1 Day<br>• 2 Days<br>• 5 Days |
| **Enable:** | Press this button to toggle the image Flash cache option On and Off. |
| **Clear Cache:** | Press this button to clear both the Flash and RAM cache of all stored images. |
| **Image Cache Status:** | The status of the memory available versus in use. |
| RAM Max Size | The maximum amount of memory available for all image caching. |
| RAM Current Size | The memory that is currently in use for caching static and dynamic images. |
| RAM Hit Rate | The percentage of image requests (static and dynamic) satisfied by accessing the cache.<br>100 * (# of cache hits) / (# of cache hits + # of cache misses)<br># of cache hits - the number of times an image was requested that the image was found in the cache. If your hit rate is low, you may want to consider enabling Flash cache.<br># of cache misses - the number of times an image was requested that the image could not be found in the cache, and the image had to either be loaded from flash or obtained via the network (for dynamic images). It is considered a RAM Cache Miss even if the image is subsequently found in flash cache. |
| Items in Cache (RAM) | The number of images that are currently stored in the RAM cache. |
| Flash Current Size | The maximum flash space allocated for image caching. Flash space is used for caching only when there is not enough available memory in the RAM cache for a newly requested image (it is used only for dynamic images). |
| Flash Hit Rate | The percentage of image requests (dynamic only) that are satisfied by accessing the flash cache.<br>100 * (# of flash cache hits) / (# of flash cache hits + # of flash cache misses)<br># of flash cache hits - # of times a dynamic image could not be found in RAM cache but was found in flash cache<br># of flash cache misses - # of times a dynamic image could not be found in either RAM or flash cache. RAM cache hits are not relevant in this calculation. |
| Items in Cache (Flash) | The number of images that are currently stored in the Flash cache. |

## Setting the image cache

In the *Protected Setup* page:

1. Press the **Cache** button in the *Protected Setup Navigation Buttons* section. This opens the *Cache Settings/Cache Setup* page.
2. Set the cache expiration in the field *Flash/RAM Cache Expires*. The Up and Down arrows increment through the available time frames.
3. Press the **Enable** button to turn on image caching. The button appears illuminated when enabled.

Select the Up and Down arrows for the field *Flash Cache Size* to increase or reduce the amount of Flash memory used; the maximum amount of flash that can be allocated for caching is 75% of available flash.

## Clearing the image cache

In the *Protected Setup* page:

1. Press the **Cache** button in the *Protected Setup Navigation Buttons* section. This opens the *Cache Settings/Cache Setup* page.
2. Press **Clear Cache**. This clears all image cache currently stored on the panel (both Flash and RAM).

## Checking image cache status

In the *Protected Setup* page:

Press the **Cache** button in the *Protected Setup Navigation Buttons* section. This opens the *Cache Settings/Cache Setup* page. All status information is located in the *Image Cache Status* section of the page.

## Password Setup Page

The options on the Password Setup page enable you to assign the passwords required for users to access the Protected Setup page, and to release the MVP from a MVP-TDS or MVP-WDS docking station (FIG. 64).

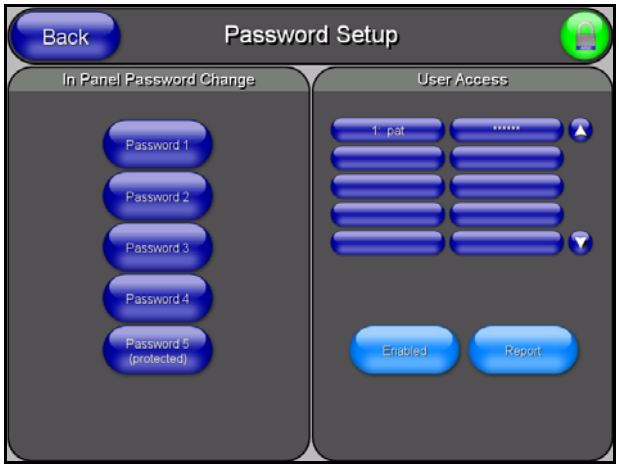



**FIG. 64** Password Setup page (MVP-8400)

Features on this page include:

| Password Setup Page | |
|---|---|
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **In Panel Password Change:** | Accesses the alphanumeric values associated to particular password sets.<br>• The PASSWORD 1, 2, 3, 4, and 5 (protected) buttons open a keyboard to enter alphanumeric values associated to the selected password group.<br>***Note**: Clearing Password #5 removes the need to enter a password before accessing the Protected Setup page.* |

| Password Setup Page (Cont.) | |
|---|---|
| **User Access:** | Use these buttons to access and modify the user name/password combinations required for removing the panel from a docking station. The number of user access passwords on the panel is limited only by the amount of storage memory available.<br>Use the UP/DN buttons to scroll through the list of saved User Access user names and passwords.<br>The Enable/Enabled button allows you to toggle between activating or deactivating the MVP panel requirement of a user to enter a pre-defined password before removing the panel from a connected docking station:<br>• **Enable** - does not prompt the user for a password, the docking station just releases the panel when the security release pushbutton is pressed.<br>• **Enabled** - requires that a valid password from the User Access list be entered before removing a panel from a docking station.<br>• The **Report** button enables/disables reporting the panel's docking status to the Master. |

## SIP Settings Page (MVP-8400 only)

The options on the SIP Settings page for the MVP-8400 (FIG. 65) enable you to establish network settings for using your touch panel as an IP phone. With a CSG SIP Communications Gateway (**FG2182-01, -02, -03**), you can use your touch panel to make and receive local, long distance, and international phone calls, and have access to phone features like call waiting, caller ID, call forwarding, call queuing, and voice mail. Setting up your touch panel as a telephone requires that you set it up as one in the CSG SIP Communications Gateway. Refer to the *CSG SIP Communications Gateway Operation/Reference Guide* for information on setting up your touch panel to work as a telephone.

You may need to load a Duet module to enable the touch panel to receive SIP calls. The Duet module translates between the standard interface and the device protocol. It parses the buffer for responses from the device, sends strings to control the device, and receives commands from the UI module or telnet sessions. Refer to the documentation supplied with the Duet Module for more details.

NOTE

*A sample UI module is provided in the module package. It is not intended to cover every possible application, but can be expanded as needed by a dealer to meet the requirements of a particular installation.*

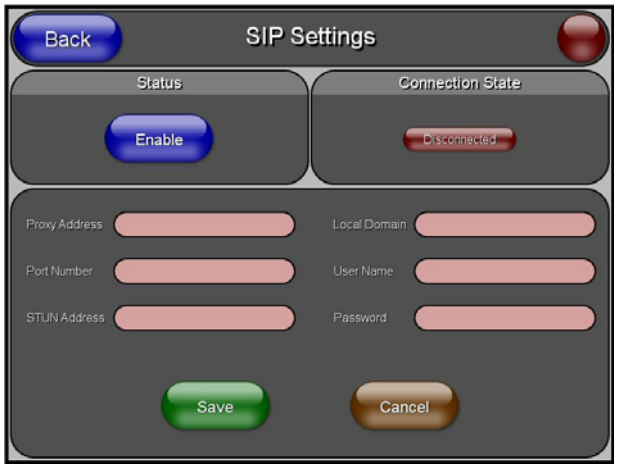



**FIG. 65** SIP Settings Page (MVP-8400 only)

Features on this page include:

| SIP Settings Page | |
|---|---|
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |
| **Status:** | This option enables the SIP Stack on startup. If you disable this option, the panel will not attempt to read the rest of the configuration and will not register with a proxy server. However, point-to-point SIP will still be enabled allowing for existing intercom functionality. |
| **Connection State:** | This option displays whether you are connected to the proxy server. |
| **Proxy Address:** | This option enables you to enter the IP address or DNS name of the proxy server that you want to use to register. |
| **Port Number:** | The option displays the port you use to connect to the proxy server. The standard SIP port is 5060, but some providers use different ports. |
| **STUN Address:** | This option enables you to enter the IP address or DNS name of the Simple Traversal of UDP through NATs (STUN) server. This field is optional. |
| **Local Domain:** | This is the realm used for authentication. This field is optional. |
| **User Name:** | This option enables you to enter the user name used for authentication to the proxy server. The user name must match an extension defined in the SIP Gateway to "register" the panel so it can receive calls. Normally, the user name is the same as the phone number assigned to the extension you are using. This field is required. |
| **Password:** | This option enables you to enter the password for the user at the proxy server. This field is optional. |

## Tools

The **Tools** button(FIG. 66 and FIG. 67) provides a menu to select either the *Panel Connection Logs/Panel Logs Page* section on page 80, the *Panel Statistics Page* section on page 81, or the *Connection Utility Page* section on page 83. Select any of the options to access that page.


**FIG. 66** Tools menu (MVP-7500)


**FIG. 67** Tools menu (MVP-8400)

## Panel Connection Logs/Panel Logs Page

The options on the *Panel Connection Logs* page (FIG. 68) and the *Panel Logs* page (FIG. 69) allow you to view and track the connection history of the panel.

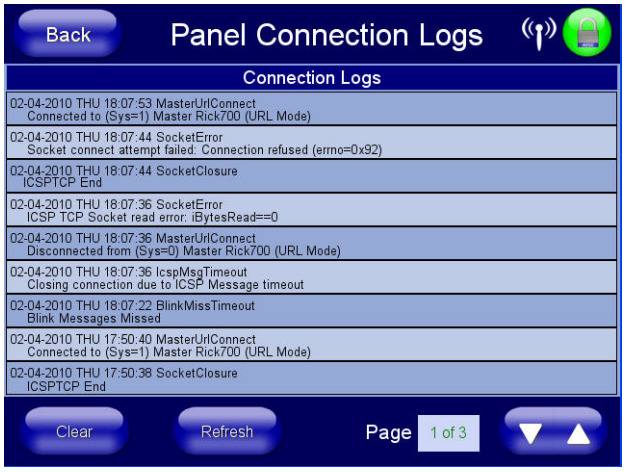



**FIG. 68** Panel Connection Logs (MVP-7500)

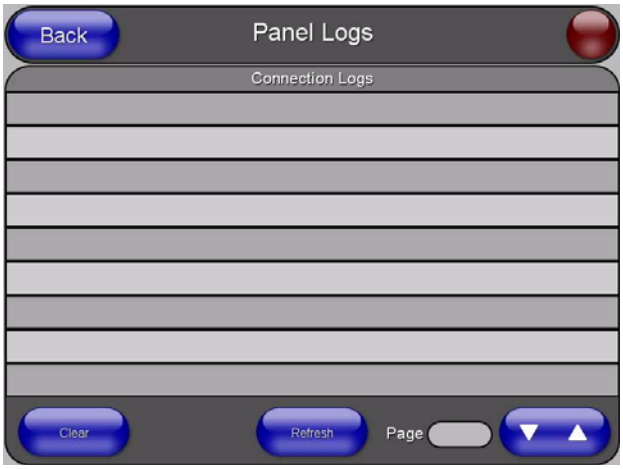



**FIG. 69** Panel Logs page (MVP-8400)

Features on this page include:

| Panel Logs Page | |
|---|---|
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |
| **Connection Logs** | A history of all connections, attempts, and failures for the panel. |
| **Clear** | Clears the Connection Logs history. |

| Panel Logs Page (Cont.) | |
|---|---|
| **Refresh** | Refreshes the Connection Logs history. |
| **Page** | Indicates the current page of the Connection Logs.<br>Use the Up and Down arrows to move from one page to the next. |

## Checking the Panel Connection Logs

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Panel Logs** button. All connection data is contained in the section *Connection Logs*.

## Refreshing the Panel Connections Log

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Panel Logs** button.
3. Push the **Refresh** button.

## Clearing the Panel Connections Log

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Panel Logs** button.
3. Push the **Clear** button.
4. Confirm your selection.

## Panel Statistics Page

The options on the *Panel Statistics* page (FIG. 70 and FIG. 71) allow you to track the connection status for the panel. The *Panel Statistics* page tracks ICSP messages, Blink messages, Ethernet connection statistics, and Wireless connection statistics.

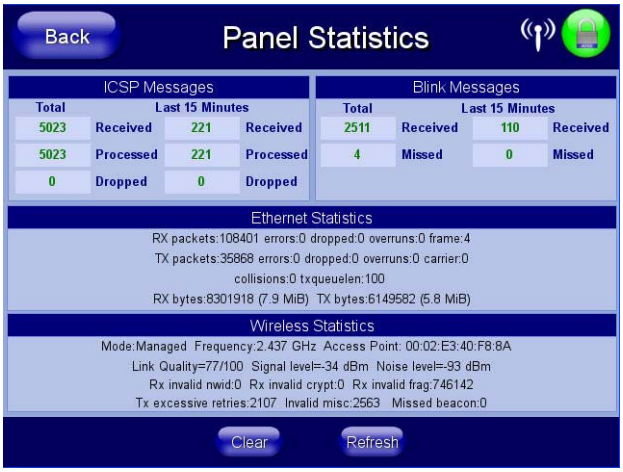



**FIG. 70** Panel Statistics Page (MVP-7500)

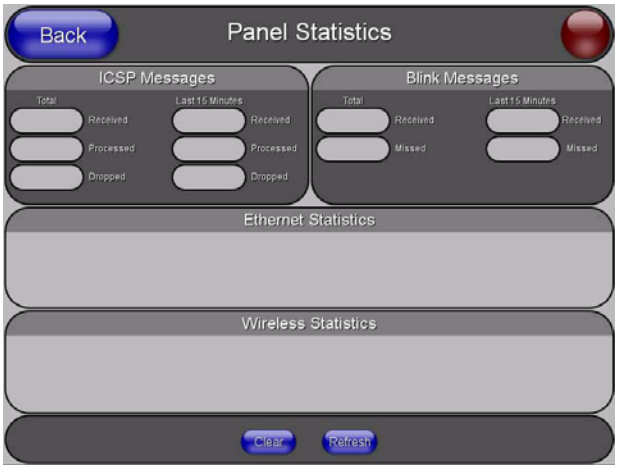



**FIG. 71** Panel Statistics page (MVP-8400)

Features on this page include:

| Panel Statistics Page | |
|---|---|
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |
| **ICSP Messages** | Messages sent between the master and the touch panel; it is the protocol they use to communicate to each other. |
| **Total** | • Received - The total ICSP messages received by the panel.<br>• Processed - The total ICSP messages processed by the panel.<br>• Dropped - The total ICSP messages dropped by the panel. |
| **Last 15 Minutes** | • Received - The total ICSP messages received by the panel in the last 15 minutes.<br>• Processed - The total ICSP messages processed by the panel in the last 15 minutes.<br>• Dropped - The total ICSP messages dropped by the panel in the last 15 minutes. |
| **Blink Messages** | The master sends this message once every 5 seconds to all connected devices. |
| **Total** | • Received - The total Blink messages received by the panel.<br>• Missed - The total Blink messages missed by the panel. |
| **Last 15 Minutes** | • Received - The total Blink messages received by the panel in the last 15 minutes.<br>• Missed - The total Blink messages missed by the panel in the last 15 minutes. |
| **Ethernet Statistics** | The Ethernet connection statistics for the panel. |
| **Wireless Statistics** | The Wireless connection statistics for the panel. |
| **Clear** | Clears all panel connection statistics. |
| **Refresh** | Refreshes all panel connection statistics. |

## Checking the Panel Statistics

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Panel Statistics** button. All connection statistics are contained on this page, e.g., *Received, Processed, and Dropped ICSP Messages*.

## Refreshing the Panel Statistics

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Panel Statistics** button.
3. Push the **Refresh** button.

## Clearing the Panel Statistics

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Panel Statistics** button.
3. Push the **Clear** button.
4. Confirm your selection.

## Connection Utility Page

The options on the *Connection Utility* page (FIG. 72 and FIG. 73) allow you to utilize your panel as a site survey tool. While in this page, move around your wireless network coverage area and see if there are any weak points within the spaces between your WAPs

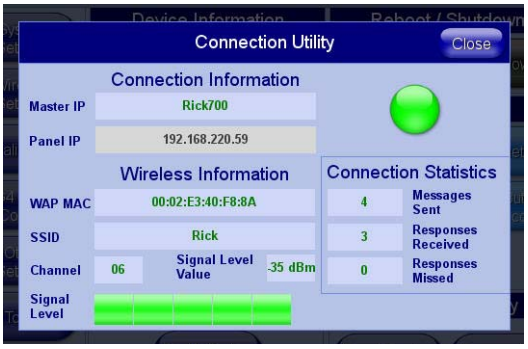



**FIG. 72** Connection Utility Page (MVP-7500)

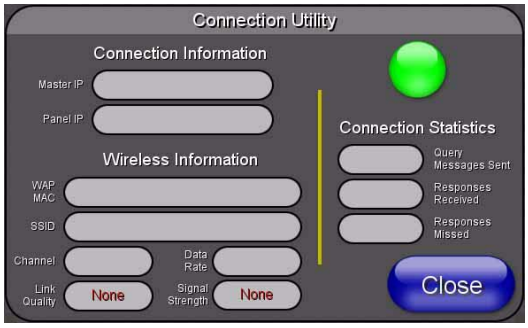



**FIG. 73** Connection Utility Page (MVP-8400)

Features on this page include:

| Connection Utility Page | |
|---|---|
| **Close:** | Closes the *Connection Utility* popup. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |

| Connection Utility Page (Cont.) | |
|---|---|
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |
| **Connection Information** | |
| **Master IP** | The IP Address for the connected master. |
| **Panel IP** | The IP Address for the panel. |
| **Wireless Information** | |
| **WAP MAC** | The MAC Address for the WAP currently in use.<br>If the MAC Address changes, it means the panel has switched/roamed to a different access point. This can be used to determine coverage for each access point and help isolate "brown" areas where coverage is minimal or non-existent, and thus require another access installed. |
| **SSID** | Displays the currently used SSID of the target WAP. |
| **Channel** | The RF channel being used for connection to the WAP (*read -only*). |
| **Signal Level Value (MVP-7500)** | The value of the outgoing signal in dBm. |
| **Data Rate (MVP-8400)** | The data rate (in Mbps) at which the panel is currently communicating with the target WAP.<br>***Note**: Data rates for 802.11b communication are: 1, 2, 5.5, and 11 Mbps.* |
| **Signal Level (MVP-7500)** | A bar display showing the current signal strength. |
| **Link Quality (MVP-8400)** | Displays the quality of the link from the wireless NIC to the Wireless Access Point (direct sequence spread spectrum) in real time (*None*, *Poor*, *Fair*, *Good*, *Very Good*, and *Excellent*).<br>• Even when link quality is at its lowest you still have a connection, and the ability to transmit and receive data, even if at lower speeds.<br>**Note:** “Link Quality” and “Signal Strength” are applicable to RF connections only. It is possible to have an RF signal to a WAP, but be unable to communicate with it because of either incorrect IP or encryption settings. |
| **Signal Strength (MVP-8400)** | This indicator displays a description of the signal strength from the Wireless Access Point connection in real time (*None*, *Poor*, *Fair*, *Good*, *Very Good*, and *Excellent*).<br>SNR (Signal Noise Ratio) is a measure of the relative strength of a wireless RF connection. Given this value and the link quality above, you can determine the noise level component of the SNR. For example, if signal strength is high but the link quality is low, then the cause of the link degradation is noise. However, if signal strength is low and link quality is low the cause would simply be signal strength. |
| **Connection Statistics** | |
| **Query Messages Sent** | The number of messages sent from the panel to the master. |
| **Responses Received** | The number of responses the panel has received from the master. |
| **Responses Missed** | The number of expected responses from the master to the panel missed. |

### Using the Connection Utility

1. Press the **Tools** button in the *Protected Setup Navigation Buttons* section. This opens the *Tools* menu.
2. Within the *Tools* menu, press the **Connection Utility** button. This launches the *Connection Utility* popup.
3. Move the panel throughout your wireless network, and changes within the utility. The *Connection Information* notes the IP of the connected master and the IP of your panel. The *Wireless Information* indicates the current wireless connection method for the panel, e.g., the MAC Address for the WAP currently in use. The *Connection Statistics* show the current quality of the panel connection.
4. Push **Close** when you are done using the site survey tool.

## Information

The **Information** button (FIG. 74 and FIG. 75) provides a menu to select either the *Project Information Page* section on page 85 or the *Panel Information Page* section on page 87. Select either option to access that page.


**FIG. 74** Information Menu (MVP-7500)


**FIG. 75** Information Menu (MVP-8400)

### Project Information Page

The *Project Information* page (FIG. 76 and FIG. 77) displays the project properties of the TPDesign4 project file currently loaded on the panel.

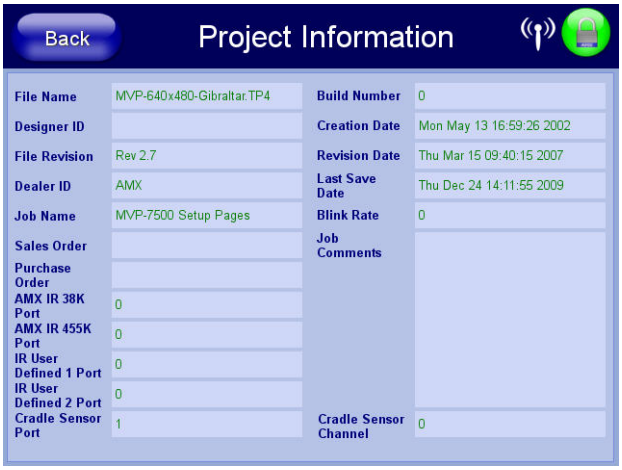



**FIG. 76** Project Information Page (MVP-7500)

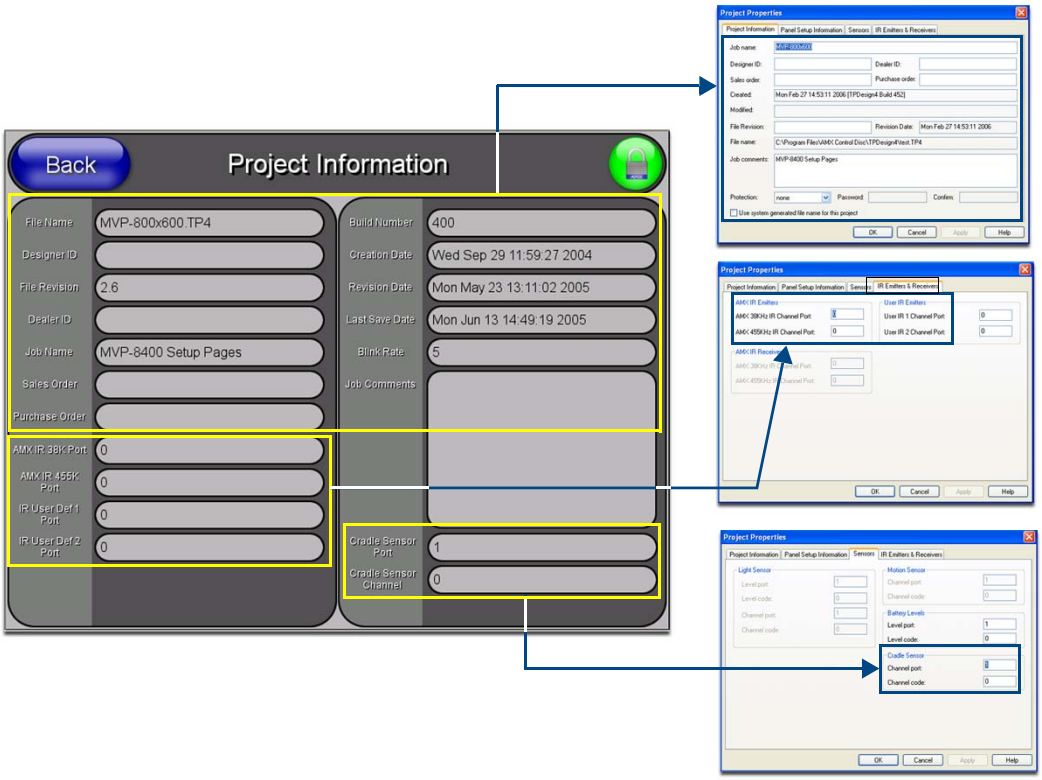



**FIG. 77** Project Information page (MVP-8400) and corresponding TPD4 project properties tabs

Features on this page include:

| Project Information Page | |
|---|---|
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |
| **File Name:** | Displays the name of the TPDesign4 project file downloaded to the panel. |
| **Designer ID:** | Displays the designer information. |
| **File Revision:** | Displays the revision number of the file. |
| **Dealer ID:** | Displays the dealer ID number (*unique to every dealer and entered in TPD4*). |
| **Job Name:** | Displays the job name. |
| **Sales Order:** | Displays the sales order information. |
| **Purchase Order:** | Displays the purchase order information. |

| Project Information Page (Cont.) | |
|---|---|
| **AMX IR 38K Port:** | Displays the AMX 38 kHz IR channel port used by the IR Emitter on the panel.<br>• This information is specified in TPD4 (Project Properties > IR Emitters & Receivers tab).<br>• For example if you set the AMX IR 38K Port to *7* and then put a button on the panel with a channel code of *5* and a port of *7*, it will trigger the IR code in slot 5 of the AMX IR 38K Port. |
| **AMX IR 455K Port:** | Displays the AMX 455 kHz IR channel port used by the IR Emitter on the panel. |
| **IR User Def 1 Port:** | Displays the User Defined IR channel port used by the IR Emitter on the panel.<br>• ***Note**: User Defined ports can be downloaded by the user and are customizable, whereas the AMX ones are fixed.* |
| **IR User Def 2 Port:** | Displays the User Defined IR channel port used by the IR Emitter on the panel. |
| **Build Number:** | Displays the build number information of the TPD4 software used to create the project file. |
| **Creation Date:** | Displays the project creation date. |
| **Revision Date:** | Displays the last revision date for the project. |
| **Last Save Date:** | Displays the last date the project was saved. |
| **Blink Rate:** | Displays the feedback blink rate, in .10 second increments. |
| **Job Comments:** | Displays any comments associated to the job (from the TPD4 project file). |
| **Cradle Sensor Port:** | Displays the port assignment being used to report Cradle Sensor information. |
| **Cradle Sensor Channel:** | Displays the channel assignment being used to report Cradle Sensor information. The channel is turned on when the panel is docked (in either the TDS or WDS docking stations. |

NOTE

*IR receivers and transmitters on G4 panels share the device address number of the panel.*

## Panel Information Page

The *Panel Information* page (FIG. 78 and FIG. 79) provides detailed panel information.

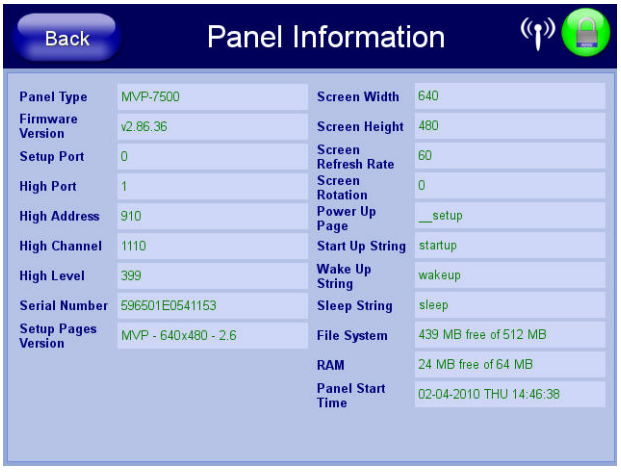



**FIG. 78** Panel Information Page (MVP-7500)

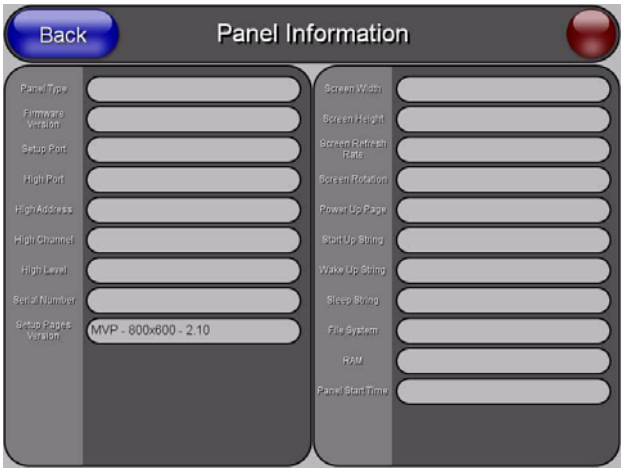



**FIG. 79** Panel Information Page (MVP-8400)

Features on this page include:

| Panel Information Page | |
|---|---|
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |
| **Panel Type:** | Displays the model of the panel being used. |
| **Firmware Version:** | Displays the version number of the G4 firmware loaded on the panel. |
| **Setup Port:** | Displays the setup port information (value) being used by the panel. |
| **High Port:** | Displays the high port (port count) value for the panel. |
| **High Address:** | Displays the high address (address count) value for the panel. |
| **High Channel:** | Displays the high channel (channel count) value for the panel. |
| **High Level:** | Displays the high level (level count) value being used by the panel. |
| **Serial Number:** | Displays the specific serial number value assigned to the panel. |
| **Setup Pages Version:** | Displays the type and version of the Setup pages being used by the panel. |
| **Screen Width:** | Displays the screen width (in pixels).<br>• MVP-8400 = 800 |
| **Screen Height:** | Displays the screen height (in pixels).<br>• MVP-8400 = 600 pixels. |
| **Screen Refresh Rate:** | Displays the video refresh rate applied to the incoming video signal from the panel. |
| **Screen Rotation:** | Displays the degree of rotation applied to the on-screen image. |
| **Power Up Pages:** | Displays the page assigned to display after the panel is powered-up. |
| **Start Up String:** | Displays the start-up string. |
| **Wake Up String:** | Displays the wake up string used after an activation from a timeout. |

| Panel Information Page (Cont.) | |
|---|---|
| **Sleep String:** | Displays the sleep string used during a panel's sleep mode. |
| **File System:** | Displays the amount of Compact Flash memory available on the panel. |
| **RAM:** | Displays the available RAM (or Extended Memory module) on the panel. |
| **Panel Start Time:** | Displays the last time the panel booted. |

## Time & Date Setup

The options on the Time & Date Setup page (FIG. 80 and FIG. 81) allow you to set and adjust time and date information on the NetLinx Master. If the time and/or date on the Master is modified, all connected devices will be updated to reflect the new information.

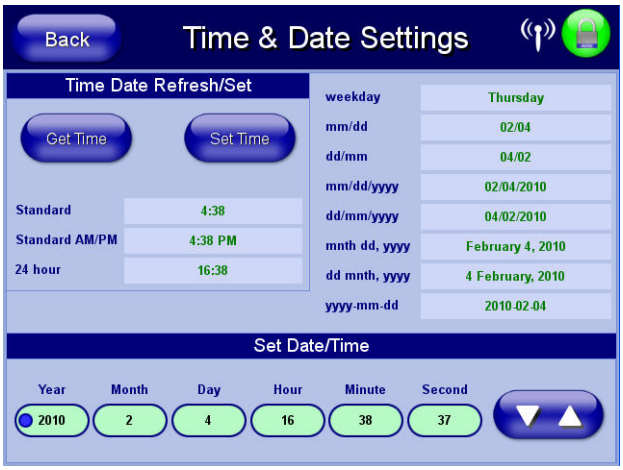



**FIG. 80** Time & Date Settings Page (MVP-7500)

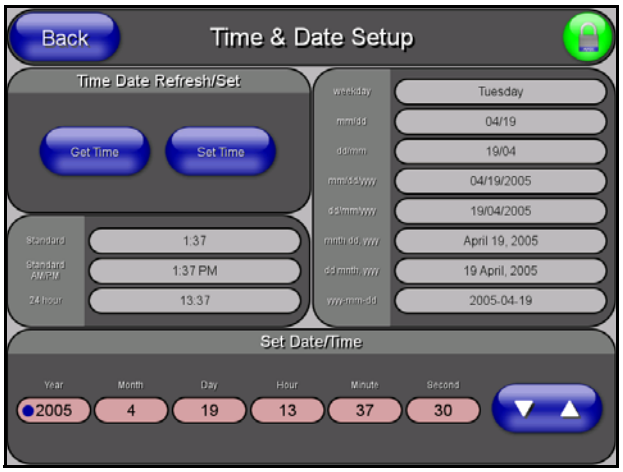



**FIG. 81** Time and Date Setup Page (MVP-8400)

NOTE

*MVP touch panels do not have an on-board clock; the only way to modify a panel's time without altering the Master is via NetLinx Code.*

Features on this page include:

| Time & Date Setup Page | |
|---|---|
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |
| **Time Date Refresh/Set:** | This section provides two options:<br>• The **Get Time/Date** button retrieves Time and Date information from the Master.<br>• The **Set Time/Date** button sets the Master to retain and save any time/date modifications made on the panel. |
| **Time Display fields:** | • These fields display the time in three formats: STANDARD, STANDARD AM/PM, and 24 HOUR. |
| **Date Display fields:** | • These fields display the calendar date information in several different formats. |
| **Set Date/Time:** | Use the UP/DN arrow buttons to adjust the Master's calendar date and time. The blue icon indicates which field is currently selected (see FIG. 81).<br>• **Year** range = 2000 - 2037<br>• **Month** range = 1 - 12<br>• **Day** range = 1 - 31<br>• **Hour** = 24-hour military<br>• **Minute** range = 0 - 59<br>• **Second** range = 0 - 59 |

## Audio Settings

The MVP-8400 provides an *Audio Settings* page (FIG. 82 and FIG. 83) with options that allow you to adjust volume levels, set intercom sound and microphone levels, and set panel sounds.

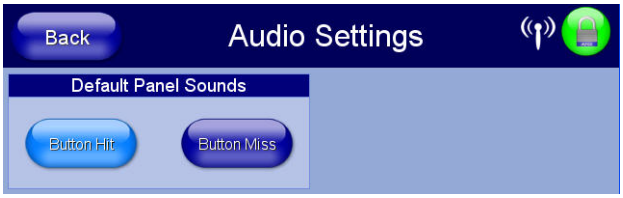



**FIG. 82** Audio Settings Page (MVP-7500)

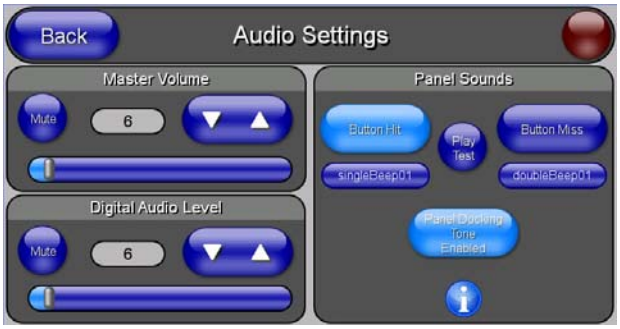



**FIG. 83** Audio Settings Page (MVP-8400)

Features on these pages include:

| Volume Page | |
|---|---|
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |
| **Master Volume:** | This section allows you to alter the current master volume level:<br>• Use the UP/DN buttons to adjust the volume level (range = 0 - 100).<br>• The Master Volume bargraph indicates the current volume level.<br>• The **Mute** button toggles the Mute feature.<br>Default = 50 |
| **Digital Audio Level:** | Adjusts the volume level on the panel's internal speaker:<br>• Use the UP/DN buttons to adjust the volume (range = 0 - 100)<br>• The *Internal Sound Level* bargraph indicates the current sound level<br>• The **Mute** button mutes the internal speaker volume<br>Default = 50 |

| Volume Page (Cont.) | |
|---|---|
| **Panel Sounds:** | • Activating the **Button Hit** button plays a default sound when you touch an active button.<br>• Activating the **Button Miss** button plays a default sound when you touch a non-active button or any area outside of the active button<br>• The **Play Test Sound** button plays a test WAV/MP3 file over the panel's internal speakers.<br>• The **singlebeep01** button plays the default single-beep file.<br>• The **doublebeep03** button plays the default double-beep file.<br>• The **Panel Docking Tone Enabled** button enables or disables sound when the panel is in a docking station or cradle.<br>• The **Information** button opens a popup explaining procedures for using the **Button Hit**, **Button Miss**, and **Panel Docking Tone Enabled** buttons. |

Environmental acoustics, personal voice level and ambient noise are all deciding factors when setting your mic and panel sound levels. Consider your environment when adjusting sound levels and use caution so as not to damage the speaker.

### WAV files - Supported sample rates

The following sample rates for WAV files are supported by MVP-8400 panels:

| Supported WAV Sample Rates | |
|---|---|
| • 48000 Hz | • 16000 Hz |
| • 44100 Hz | • 12000 Hz |
| • 32000 Hz | • 11025 Hz |
| • 24000 Hz | • 8000 Hz |
| • 22050 Hz | |

### Custom Sounds

The custom button hit/miss sound feature allows a user to add one custom button hit and one custom button miss sound to any user page project. Once the user page is downloaded into the panel, the user can select the custom sounds from the Audio Setup page.

To add custom sounds to a TPDesign project, import a WAV file into the resource manager. Rename the resource to "customSingle.wav" for a custom button hit sound or "customDouble.wav" for a custom button miss sound.

## Battery Settings/Batteries

The options on the MVP-7500 Battery Settings page (FIG. 84) and the MVP-8400 Batteries page (FIG. 85) allow you to set power warning preferences, monitor battery status information, and adjust the display times for battery warnings. This page is populated with information from MVP-BP batteries in the panel, as well as batteries in a connected MVP-TDS/WDS docking station.

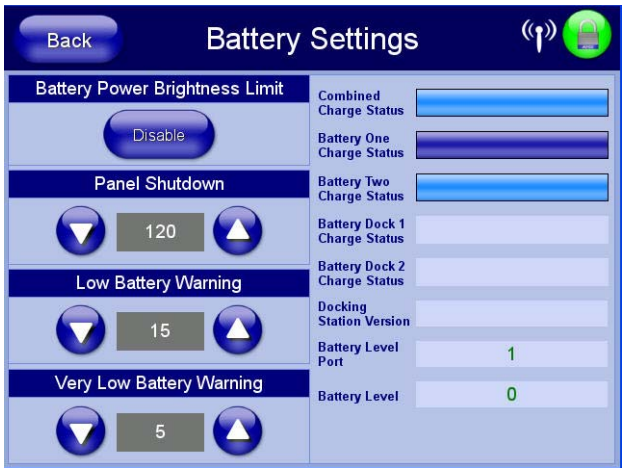



**FIG. 84** Battery Settings Page (MVP-7500)

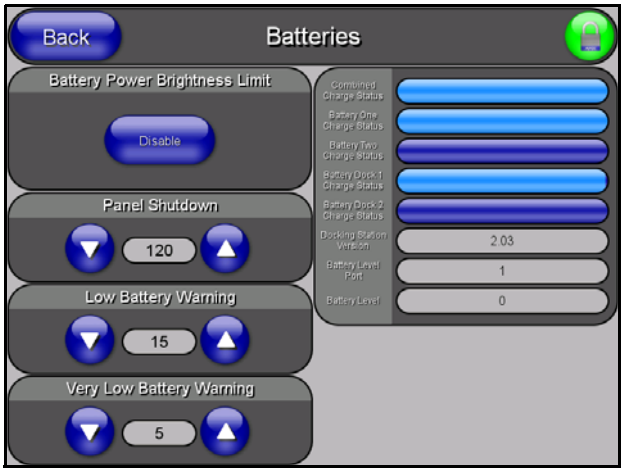



**FIG. 85** Batteries Page (MVP-8400)

Features on this page include:

| Batteries Page | |
|---|---|
| **Back:** | Saves all changes and returns to the previous page. |
| **WiFi/Wired icon:** | The icon to the left of the Connection Status Icon displays whether the current connection to the Master is *Wireless* (image of a radio antenna) or *Wired* (image of three networked computers). |
| **Connection Status icon:** | The icon in the upper-right corner of each Setup page shows online/offline state of the panel to the master.<br>• Bright red - disconnected<br>• Bright green - connected. Blinks when a blink message is received to dark green every 5 seconds for half a second then go back to bright green.<br>• Bright yellow - panel missed a blink message from the master. It will remain yellow for 3 missed blink messages and then turn red. It will return to green when a blink message is received.<br>***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.* |
| **Battery Power Brightness Limit:** | The DISABLE/DISABLED button acts as a power save feature with two options:<br>• **Disable** - activates the brightness limit set on the panel (conserves battery power). Activating this feature causes the panel to function at 80% of full brightness and overrides the Panel Brightness value set on the Setup page.<br>• **Disabled** - deactivates this power save feature. The panel will use the Panel Brightness level.<br>***Note**: This field applies to MVP-BP batteries installed in the panel.* |
| **Panel Shutdown:** | This value determines the number of minutes that would need to pass before the panel automatically shuts-down. Once shutdown, the unit would have to be restarted. The UP/DN buttons alter the timeout value (in minutes). A value of 0 disables this feature.<br>Range = 0 - 240, default = 1200 min.<br>***Note**: This field applies to MVP-BP batteries installed in the panel.* |
| **Low Battery Warning:** | The UP/DN buttons adjust the time value (in minutes) available on the battery (for use) before the panel displays a low battery warning.<br>Range - 10 - 45, default = 15 min.<br>***Note**: This field applies to MVP-BP batteries installed in the panel.* |

| Batteries Page (Cont.) | |
|---|---|
| **Very Low Battery Warning:** | The UP/DN buttons adjust the time value (in minutes) available on the battery before the panel displays a very low battery warning (indicating near-term panel shutdown).<br>• Range = 3 - 15, default = 5 min.<br>• This value cannot exceed the Low Battery Warning value.<br>***Note**: This field applies to MVP-BP batteries installed in the panel.* |
| **Battery Status:** | • The **Combined Charge Status** bargraph indicates the combined power charge available from batteries installed in the panel.<br>• The **Battery One Charge Status** bargraph indicates the power charge available on the Slot 1 battery (in the panel).<br>• The **Battery Two Charge Status** bargraph indicates the power charge available on the Slot 2 battery (in the panel).<br>• The **Battery Dock 1 Charge Status** bargraph indicates the power charge available on the docking station's battery #1.<br>• The **Battery Dock 2 Charge Status** bargraph indicates the power charge available on the docking station's battery #2.<br>***Note**: If no batteries are being charged within the docking station's battery compartments, or the MVP is not connected to a docking station; both Battery Dock Charge Status fields are left blank.*<br>• The **Docking Station Version** field indicates the firmware version currently installed on the docking station.<br>• The **Battery Level Port** field indicates the port being used to report charge status levels back to the NetLinx Master (set in TPDesign4).<br>• The **Battery Level** field indicates the level being used to report status levels back to the NetLinx Master (set in TPDesign4). |

## EAP Security & Server Certificates - Overview

The following EAP types all support a server certificate:

- EAP-PEAP
- EAP-TTLS
- EAP-TLS

All three of these certificate-using security methods are documented in the following sections. EAP Authentication goes a step beyond just encrypting data transfers, but also requires that a set of credentials be validated before the client (panel) is allowed to connect to the rest of the network (FIG. 86). Below is a description of this process. It is important to note that there is no user intervention necessary during this process. It proceeds automatically based on the configuration parameters entered into the panel.

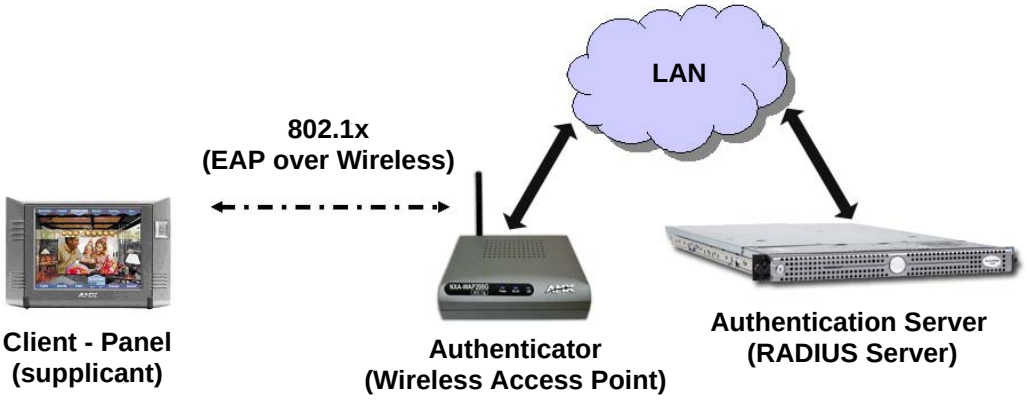



**FIG. 86** EAP security method in process

A server certificate file uses a certificate that is installed in a panel so that the RADIUS server can be validated before the panel tries to connect to it. The field name associated with this file is *Certificate Authority.*

If a server certificate is used, it should first be downloaded into the panel and the *Certificate Authority* field should then be set to the name of that certificate file. No file path should be used for this setting as all certificates are stored in a specific directory that the user cannot control or change. The most secure connection method uses a server certificate.

If no server certificate will be used then, this field should be left blank. If the field contains a file name, then a valid certificate file with the same file name must be previously installed on the panel. Otherwise the authentication process will fail.

# Programming

## Overview

You can program this touch panel, using the commands in this section, to perform a wide variety of operations using Send_Commands and variable text commands.

**A device must first be defined in the NetLinx programming language with values for the Device: Port: System** (in all programming examples - ***Panel*** is used in place of these values and represents all Modero panels).


*Verify you are using the latest NetLinx Master and Modero firmware.*
*Verify you are using the latest version of NetLinx Studio and TPD4.*

## Button Assignments

- Button Channel Range: 1 - 4000 Button push and Feedback (per address port)
- Button Variable Text range: 1 - 4000 (per address port)
- Button States Range: 1 - 256 (0 = All states, for General buttons 1 = Off state and 2 = On state).
- Level Range: 1 - 600 (Default level value 0 - 255, can be set up to 1 - 65535)
- Address port Range: 1 - 100


*These button assignments can only be adjusted in TPD4 and not on the panels themselves.*

## Page Commands

These Page Commands are used in NetLinx Programming Language and are case insensitive.

| Page Commands | |
|---|---|
| **@APG**<br>Add a specific popup page to a specified popup group. | Add the popup page to a group if it does not already exist. If the new popup is added to a group which has a popup displayed on the current page along with the new pop-up, the displayed popup will be hidden and the new popup will be displayed.<br>Syntax:<br>`"'@APG-<popup page name>;<popup group name>'"`<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the popup page.<br>popup group name = 1 - 50 ASCII characters. Name of the popup group.<br>Example:<br>`SEND_COMMAND Panel,"'@APG-Popup1;Group1'"`<br>Adds the popup page 'Popup1' to the popup group 'Group1'. |
| **@CPG**<br>Clear all popup pages from specified popup group. | Syntax:<br>`"'@CPG-<popup group name>'"`<br>Variable:<br>popup group name = 1 - 50 ASCII characters. Name of the popup group.<br>Example:<br>`SEND_COMMAND Panel,"'@CPG-Group1'"`<br>Clears all popup pages from the popup group 'Group1'. |

| Page Commands (Cont.) | |
|---|---|
| **@DPG**<br>Delete a specific popup page from specified popup group if it exists. | Syntax:<br>"'@DPG-<popup page name>;<popup group name>'"<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the popup page.<br>popup group name = 1 - 50 ASCII characters. Name of the popup group.<br>Example:<br>SEND_COMMAND Panel,"'@DPG-Popup1;Group1'"<br>Deletes the popup page 'Popup1' from the popup group 'Group1'. |
| **@PDR**<br>Set the popup location reset flag. | If the flag is set, the popup will return to its default location on show instead of its last drag location.<br>Syntax:<br>"'@PDR-<popup page name>;<reset flag>'"<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>reset flag = 1 = Enable reset flag<br>0 = Disable reset flag<br>Example:<br>SEND_COMMAND Panel,"'@PDR-Popup1;1'"<br>Popup1 will return to its default location when turned On. |
| **@PHE**<br>Set the hide effect for the specified popup page to the named hide effect. | Syntax:<br>"'@PHE-<popup page name>;<hide effect name>'"<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>hide effect name = Refers to the popup effect names being used.<br>Example:<br>SEND_COMMAND Panel,"'@PHE-Popup1;Slide to Left'"<br>Sets the Popup1 hide effect name to 'Slide to Left'. |
| **@PHP**<br>Set the hide effect position. | Only 1 coordinate is ever needed for an effect; however, the command will specify both. This command sets the location at which the effect will end at.<br>Syntax:<br>"'@PHP-<popup page name>;<x coordinate>,<y coordinate>'"<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>Example:<br>SEND_COMMAND Panel,"'@PHP-Popup1;75,0'"<br>Sets the Popup1 hide effect x-coordinate value to 75 and the y-coordinate value to 0. |
| **@PHT**<br>Set the hide effect time for the specified popup page. | Syntax:<br>"'@PHT-<popup page name>;<hide effect time>'"<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>hide effect time = Given in 1/10ths of a second.<br>Example:<br>SEND_COMMAND Panel,"'@PHT-Popup1;50'"<br>Sets the Popup1 hide effect time to 5 seconds. |

| Page Commands (Cont.) | |
|---|---|
| **@PPA**<br>Close all popups on a specified page. | *If the page name is empty, the current page is used.* Same as the 'Clear Page' command in TPDesign4.<br>Syntax:<br>`"'@PPA-<page name>'"`<br>Variable:<br>page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>Example:<br>`SEND_COMMAND Panel,"'@PPA-Page1'"`<br>Close all popups on Page1. |
| **@PPF**<br>Deactivate a specific popup page on either a specified page or the current page. | *If the page name is empty, the current page is used (see example 2).* If the popup page is part of a group, the whole group is deactivated. This command works in the same way as the 'Hide Popup' command in TPDesign4.<br>Syntax:<br>`"'@PPF-<popup page name>;<page name>'"`<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the popup page.<br>page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>Example:<br>`SEND_COMMAND Panel,"'@PPF-Popup1;Main'"`<br>Example 2:<br>`SEND_COMMAND Panel,"'@PPF-Popup1'"`<br>Deactivates the popup page 'Popup1' on the current page. |
| **@PPG**<br>Toggle a specific popup page on either a specified page or the current page. | *If the page name is empty, the current page is used (see example 2).* Toggling refers to the activating/deactivating (On/Off) of a popup page. This command works in the same way as the 'Toggle Popup' command in TPDesign4.<br>Syntax:<br>`"'@PPG-<popup page name>;<page name>'"`<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the popup page.<br>page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>Example:<br>`SEND_COMMAND Panel,"'@PPG-Popup1;Main'"`<br>Toggles the popup page 'Popup1' on the 'Main' page from one state to another (On/Off).<br>Example 2:<br>`SEND_COMMAND Panel,"'@PPG-Popup1'"`<br>Toggles the popup page 'Popup1' on the current page from one state to another (On/Off). |
| **@PPK**<br>Kill a specific popup page from all pages. | Kill refers to the deactivating (Off) of a popup window from all pages. If the pop-up page is part of a group, the whole group is deactivated. This command works in the same way as the 'Clear Group' command in TPDesign 4.<br>Syntax:<br>`"'@PPK-<popup page name>'"`<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the popup page.<br>Example:<br>`SEND_COMMAND Panel,"'@PPK-Popup1'"`<br>Kills the popup page 'Popup1' on all pages. |

| Page Commands (Cont.) | |
|---|---|
| **@PPM**<br>Set the modality of a specific popup page to Modal or NonModal. | A Modal popup page, when active, only allows you to use the buttons and features on that popup page. All other buttons on the panel page are inactivated.<br>Syntax:<br>`"'@PPM-<popup page name>;<mode>'"`<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the popup page.<br>mode = NONMODAL converts a previously Modal popup page to a NonModal.<br>MODAL converts a previously NonModal popup page to Modal.<br>***modal = 1 and non-modal = 0***<br>Example:<br>`SEND_COMMAND Panel,"'@PPM-Popup1;Modal'"`<br>Sets the popup page 'Popup1' to Modal.<br>`SEND_COMMAND Panel,"'@PPM-Popup1;1'"`<br>Sets the popup page 'Popup1' to Modal. |
| **@PPN**<br>Activate a specific popup page to launch on either a specified page or the current page. | *If the page name is empty, the current page is used (see example 2).* If the popup page is already on, do not re-draw it. This command works in the same way as the 'Show Popup' command in TPDesign4.<br>Syntax:<br>`"'@PPN-<popup page name>;<page name>'"`<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the popup page.<br>page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>Example:<br>`SEND_COMMAND Panel,"'@PPN-Popup1;Main'"`<br>Activates 'Popup1' on the 'Main' page.<br>Example 2:<br>`SEND_COMMAND Panel,"'@PPN-Popup1'"`<br>Activates the popup page 'Popup1' on the current page. |
| **@PPT**<br>Set a specific popup page to timeout within a specified time. | If timeout is empty, popup page will clear the timeout.<br>Syntax:<br>`"'@PPT-<popup page name>;<timeout>'"`<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the popup page.<br>timeout = Timeout duration in 1/10ths of a second.<br>Example:<br>`SEND_COMMAND Panel,"'@PPT-Popup1;30'"`<br>Sets the popup page 'Popup1' to timeout within 3 seconds. |
| **@PPX**<br>Close all popups on all pages. | This command works in the same way as the 'Clear All' command in TPDesign 4.<br>Syntax:<br>`"'@PPX'"`<br>Example:<br>`SEND_COMMAND Panel,"'@PPX'"`<br>Close all popups on all pages. |
| **@PSE**<br>Set the show effect for the specified popup page to the named show effect. | Syntax:<br>`"'@PSE-<popup page name>;<show effect name>'"`<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>show effect name = Refers to the popup effect name being used.<br>Example:<br>`SEND_COMMAND Panel,"'@PSE-Popup1;Slide from Left'"`<br>Sets the Popup1 show effect name to 'Slide from Left'. |

| Page Commands (Cont.) | |
|---|---|
| **@PSP**<br>Set the show effect position. | Only 1 coordinate is ever needed for an effect; however, the command will specify both. This command sets the location at which the effect will begin at.<br>Syntax:<br>`"'@PSP-<popup page name>;<x coordinate>,<y coordinate>'"`<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>Example:<br>`SEND_COMMAND Panel,"'@PSP-Popup1;100,0'"`<br>Sets the Popup1 show effect x-coordinate value to 100 and the y-coordinate value to 0. |
| **@PST**<br>Set the show effect time for the specified popup page. | Syntax:<br>`"'@PST-<popup page name>;<show effect time>'"`<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>show effect time = Given in 1/10ths of a second.<br>Example:<br>`SEND_COMMAND Panel,"'@PST-Popup1;50'"`<br>Sets the Popup1 show effect time to 5 seconds. |
| **PAGE**<br>Flip to a specified page. | Flips to a page with a specified page name. If the page is currently active, it will not redraw the page.<br>Syntax:<br>`"'PAGE-<page name>'"`<br>Variable:<br>page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>Example:<br>`SEND_COMMAND Panel,"'PAGE-Page1'"`<br>Flips to page1. |
| **PPOF**<br>Deactivate a specific popup page on either a specified page or the current page. | *If the page name is empty, the current page is used (see example 2).* If the popup page is part of a group, the whole group is deactivated. This command works in the same way as the 'Hide Popup' command in TPDesign4.<br>Syntax:<br>`"'PPOF-<popup page name>;<page name>'"`<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the popup page.<br>page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>Example:<br>`SEND_COMMAND Panel,"'PPOF-Popup1;Main'"`<br>Deactivates the popup page 'Popup1' on the Main page.<br>Example 2:<br>`SEND_COMMAND Panel,"'PPOF-Popup1'"`<br>Deactivates the popup page 'Popup1' on the current page. |

| Page Commands (Cont.) | |
|---|---|
| **PPOG**<br>Toggle a specific popup page on either a specified page or the current page. | *If the page name is empty, the current page is used (see example 2).* Toggling refers to the activating/deactivating (On/Off) of a popup page. This command works in the same way as the 'Toggle Popup' command in TPDesign4.<br>Syntax:<br>`"'PPOG-<popup page name>;<page name>'"`<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the popup page.<br>page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>Example:<br>`SEND_COMMAND Panel,"'PPOG-Popup1;Main'"`<br>Toggles the popup page 'Popup1' on the Main page from one state to another (On/Off).<br>Example 2:<br>`SEND_COMMAND Panel,"'PPOG-Popup1'"`<br>Toggles the popup page 'Popup1' on the current page from one state to another (On/Off). |
| **PPON**<br>Activate a specific popup page to launch on either a specified page or the current page. | *If the page name is empty, the current page is used (see example 2).* If the popup page is already On, do not re-draw it. This command works in the same way as the 'Show Popup' command in TPDesign4.<br>Syntax:<br>`"'PPON-<popup page name>;<page name>'"`<br>Variable:<br>popup page name = 1 - 50 ASCII characters. Name of the popup page.<br>page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.<br>Example:<br>`SEND_COMMAND Panel,"'PPON-Popup1; Main'"`<br>Activates the popup page 'Popup1' on the Main page.<br>Example 2:<br>`SEND_COMMAND Panel,"'PPON-Popup1'"`<br>Activates the popup page 'Popup1' on the current page. |

# Programming Numbers

The following information provides the programming numbers for colors, fonts, and borders.

Colors can be used to set the colors on buttons, sliders, and pages. The lowest color number represents the lightest color-specific display; the highest number represents the darkest display. For example, 0 represents light red, and 5 is dark red.

## RGB triplets and names for basic 88 colors

| RGB Values for all 88 Basic Colors | | | | |
|---|---|---|---|---|
| Index No. | Name | Red | Green | Blue |
| 00 | Very Light Red | 255 | 0 | 0 |
| 01 | Light Red | 223 | 0 | 0 |
| 02 | Red | 191 | 0 | 0 |
| 03 | Medium Red | 159 | 0 | 0 |
| 04 | Dark Red | 127 | 0 | 0 |
| 05 | Very Dark Red | 95 | 0 | 0 |
| 06 | Very Light Orange | 255 | 128 | 0 |
| 07 | Light Orange | 223 | 112 | 0 |
| 08 | Orange | 191 | 96 | 0 |
| 09 | Medium Orange | 159 | 80 | 0 |
| 10 | Dark Orange | 127 | 64 | 0 |
| 11 | Very Dark Orange | 95 | 48 | 0 |
| 12 | Very Light Yellow | 255 | 255 | 0 |

| RGB Values for all 88 Basic Colors (Cont.) | | | | |
|---|---|---|---|---|
| Index No. | Name | Red | Green | Blue |
| 13 | Light Yellow | 223 | 223 | 0 |
| 14 | Yellow | 191 | 191 | 0 |
| 15 | Medium Yellow | 159 | 159 | 0 |
| 16 | Dark Yellow | 127 | 127 | 0 |
| 17 | Very Dark Yellow | 95 | 95 | 0 |
| 18 | Very Light Lime | 128 | 255 | 0 |
| 19 | Light Lime | 112 | 223 | 0 |
| 20 | Lime | 96 | 191 | 0 |
| 21 | Medium Lime | 80 | 159 | 0 |
| 22 | Dark Lime | 64 | 127 | 0 |
| 23 | Very Dark Lime | 48 | 95 | 0 |
| 24 | Very Light Green | 0 | 255 | 0 |
| 25 | Light Green | 0 | 223 | 0 |
| 26 | Green | 0 | 191 | 0 |
| 27 | Medium Green | 0 | 159 | 0 |
| 28 | Dark Green | 0 | 127 | 0 |
| 29 | Very Dark Green | 0 | 95 | 0 |
| 30 | Very Light Mint | 0 | 255 | 128 |
| 31 | Light Mint | 0 | 223 | 112 |
| 32 | Mint | 0 | 191 | 96 |
| 33 | Medium Mint | 0 | 159 | 80 |
| 34 | Dark Mint | 0 | 127 | 64 |
| 35 | Very Dark Mint | 0 | 95 | 48 |
| 36 | Very Light Cyan | 0 | 255 | 255 |
| 37 | Light Cyan | 0 | 223 | 223 |
| 38 | Cyan | 0 | 191 | 191 |
| 39 | Medium Cyan | 0 | 159 | 159 |
| 40 | Dark Cyan | 0 | 127 | 127 |
| 41 | Very Dark Cyan | 0 | 95 | 95 |
| 42 | Very Light Aqua | 0 | 128 | 255 |
| 43 | Light Aqua | 0 | 112 | 223 |
| 44 | Aqua | 0 | 96 | 191 |
| 45 | Medium Aqua | 0 | 80 | 159 |
| 46 | Dark Aqua | 0 | 64 | 127 |
| 47 | Very Dark Aqua | 0 | 48 | 95 |
| 48 | Very Light Blue | 0 | 0 | 255 |
| 49 | Light Blue | 0 | 0 | 223 |
| 50 | Blue | 0 | 0 | 191 |
| 51 | Medium Blue | 0 | 0 | 159 |
| 52 | Dark Blue | 0 | 0 | 127 |
| 53 | Very Dark Blue | 0 | 0 | 95 |
| 54 | Very Light Purple | 128 | 0 | 255 |
| 55 | Light Purple | 112 | 0 | 223 |
| 56 | Purple | 96 | 0 | 191 |

| RGB Values for all 88 Basic Colors (Cont.) | | | | |
|---|---|---|---|---|
| Index No. | Name | Red | Green | Blue |
| 57 | Medium Purple | 80 | 0 | 159 |
| 58 | Dark Purple | 64 | 0 | 127 |
| 59 | Very Dark Purple | 48 | 0 | 95 |
| 60 | Very Light Magenta | 255 | 0 | 255 |
| 61 | Light Magenta | 223 | 0 | 223 |
| 62 | Magenta | 191 | 0 | 191 |
| 63 | Medium Magenta | 159 | 0 | 159 |
| 64 | Dark Magenta | 127 | 0 | 127 |
| 65 | Very Dark Magenta | 95 | 0 | 95 |
| 66 | Very Light Pink | 255 | 0 | 128 |
| 67 | Light Pink | 223 | 0 | 112 |
| 68 | Pink | 191 | 0 | 96 |
| 69 | Medium Pink | 159 | 0 | 80 |
| 70 | Dark Pink | 127 | 0 | 64 |
| 71 | Very Dark Pink | 95 | 0 | 48 |
| 72 | White | 255 | 255 | 255 |
| 73 | Grey1 | 238 | 238 | 238 |
| 74 | Grey3 | 204 | 204 | 204 |
| 75 | Grey5 | 170 | 170 | 170 |
| 76 | Grey7 | 136 | 136 | 136 |
| 77 | Grey9 | 102 | 102 | 102 |
| 78 | Grey4 | 187 | 187 | 187 |
| 79 | Grey6 | 153 | 153 | 153 |
| 80 | Grey8 | 119 | 119 | 119 |
| 81 | Grey10 | 85 | 85 | 85 |
| 82 | Grey12 | 51 | 51 | 51 |
| 83 | Grey13 | 34 | 34 | 34 |
| 84 | Grey2 | 221 | 221 | 221 |
| 85 | Grey11 | 68 | 68 | 68 |
| 86 | Grey14 | 17 | 17 | 17 |
| 87 | Black | 0 | 0 | 0 |
| 255 | TRANSPARENT | 99 | 53 | 99 |

## Font styles and ID numbers

Font styles can be used to program the text fonts on buttons, sliders, and pages. The following chart shows the default font type and their respective ID numbers generated by TPDesign4.

**Default Font Styles and ID Numbers**

| Font ID # | Font type | Size | Font ID # | Font type | Size |
|---|---|---|---|---|---|
| 1 | Courier New | 9 | 19 | Arial | 9 |
| 2 | Courier New | 12 | 20 | Arial | 10 |
| 3 | Courier New | 18 | 21 | Arial | 12 |
| 4 | Courier New | 26 | 22 | Arial | 14 |
| 5 | Courier New | 32 | 23 | Arial | 16 |
| 6 | Courier New | 18 | 24 | Arial | 18 |
| 7 | Courier New | 26 | 25 | Arial | 20 |
| 8 | Courier New | 34 | 26 | Arial | 24 |
| 9 | AMX Bold | 14 | 27 | Arial | 36 |
| 10 | AMX Bold | 20 | 28 | Arial Bold | 10 |
| 11 | AMX Bold | 36 | 29 | Arial Bold | 8 |
| | | | 32 - Variable Fonts start at 32. | | |


*You must import fonts into a TPDesign4 project file. The font ID numbers are assigned by TPDesign4. These values are also listed in the* ***Generate Programmer's Report****.*

## Border styles and Programming numbers

Border styles can be used to program borders on buttons, sliders, and popup pages.

**Border Styles and Programming Numbers**

| No. | Border styles | No. | Border styles |
|---|---|---|---|
| 0-1 | No border | 10-11 | Picture frame |
| 2 | Single line | 12 | Double line |
| 3 | Double line | 20 | Bevel-S |
| 4 | Quad line | 21 | Bevel-M |
| 5-6 | Circle 15 | 22-23 | Circle 15 |
| 7 | Single line | 24-27 | Neon inactive-S |
| 8 | Double line | 40-41 | Diamond 55 |
| 9 | Quad line | | |

The TPDesign4 Touch Panel Design program has pre-set border styles that are user selectable.

You cannot use the following number values for programming purposes when changing border styles. TPD4 border styles can ONLY be changed by using the name.

**TPD4 Border Styles by Name**

| No. | Border styles | No. | Border styles |
|---|---|---|---|
| 1 | None | 6 | Bevel -M |
| 2 | AMX Elite -L | 7 | Bevel -S |
| 3 | AMX Elite -M | 8 | Circle 15 |
| 4 | AMX Elite -S | 9 | Circle 25 |
| 5 | Bevel -L | 10 | Circle 35 |

| TPD4 Border Styles by Name (Cont.) | | | |
|---|---|---|---|
| No. | Border styles | No. | Border styles |
| 11 | Circle 45 | 55 | Double Bevel -L |
| 12 | Circle 55 | 56 | Double Bevel -M |
| 13 | Circle 65 | 57 | Double Bevel -S |
| 14 | Circle 75 | 58 | Double Line |
| 15 | Circle 85 | 59 | Fuzzy |
| 16 | Circle 95 | 60 | Glow-L |
| 17 | Circle 105 | 61 | Glow-S |
| 18 | Circle 115 | 62 | Help Down |
| 19 | Circle 125 | 63 | Neon Active -L |
| 20 | Circle 135 | 64 | Neon Active -S |
| 21 | Circle 145 | 65 | Neon Inactive -L |
| 22 | Circle 155 | 66 | Neon Inactive -S |
| 23 | Circle 165 | 67 | Oval H 60x30 |
| 24 | Circle 175 | 68 | Oval H 100x50 |
| 25 | Circle 185 | 69 | Oval H 150x75 |
| 26 | Circle 195 | 70 | Oval H 200x100 |
| 27 | Cursor Bottom | 71 | Oval V 30x60 |
| 28 | Cursor Bottom with Hole | 72 | Oval V 50x100 |
| 29 | Cursor Top | 73 | Oval V 75x150 |
| 30 | Cursor Top with Hole | 74 | Oval V 100x200 |
| 31 | Cursor Left | 75 | Picture Frame |
| 32 | Cursor Left with Hole | 76 | Quad Line |
| 33 | Cursor Right | 77 | Single Line |
| 34 | Cursor Right with Hole | 78 | Windows Style Popup |
| 35 | Custom Frame | 79 | Windows Style Popup (Status Bar) |
| 36 | Diamond 15 | 80 | Menu Bottom Rounded 15 |
| 37 | Diamond 25 | 81 | Menu Bottom Rounded 25 |
| 38 | Diamond 35 | 82 | Menu Bottom Rounded 35 |
| 39 | Diamond 45 | 83 | Menu Bottom Rounded 45 |
| 40 | Diamond 55 | 84 | Menu Bottom Rounded 55 |
| 41 | Diamond 65 | 85 | Menu Bottom Rounded 65 |
| 42 | Diamond 75 | 86 | Menu Bottom Rounded 75 |
| 43 | Diamond 85 | 87 | Menu Bottom Rounded 85 |
| 44 | Diamond 95 | 88 | Menu Bottom Rounded 95 |
| 45 | Diamond 105 | 89 | Menu Bottom Rounded 105 |
| 46 | Diamond 115 | 90 | Menu Bottom Rounded 115 |
| 47 | Diamond 125 | 91 | Menu Bottom Rounded 125 |
| 48 | Diamond 135 | 92 | Menu Bottom Rounded 135 |
| 49 | Diamond 145 | 93 | Menu Bottom Rounded 145 |
| 50 | Diamond 155 | 94 | Menu Bottom Rounded 155 |
| 51 | Diamond 165 | 95 | Menu Bottom Rounded 165 |
| 52 | Diamond 175 | 96 | Menu Bottom Rounded 175 |
| 53 | Diamond 185 | 97 | Menu Bottom Rounded 185 |
| 54 | Diamond 195 | 98 | Menu Bottom Rounded 195 |

| TPD4 Border Styles by Name (Cont.) | | | |
|---|---|---|---|
| 99 | Menu Top Rounded 15 | 128 | Menu Right Rounded 115 |
| 100 | Menu Top Rounded 25 | 129 | Menu Right Rounded 125 |
| 101 | Menu Top Rounded 35 | 130 | Menu Right Rounded 135 |
| 102 | Menu Top Rounded 45 | 131 | Menu Right Rounded 145 |
| 103 | Menu Top Rounded 55 | 132 | Menu Right Rounded 155 |
| 104 | Menu Top Rounded 65 | 133 | Menu Right Rounded 165 |
| 105 | Menu Top Rounded 75 | 134 | Menu Right Rounded 175 |
| 106 | Menu Top Rounded 85 | 135 | Menu Right Rounded 185 |
| 107 | Menu Top Rounded 95 | 136 | Menu Right Rounded 195 |
| 108 | Menu Top Rounded 105 | 137 | Menu Left Rounded 15 |
| 109 | Menu Top Rounded 115 | 138 | Menu Left Rounded 25 |
| 110 | Menu Top Rounded 125 | 139 | Menu Left Rounded 35 |
| 111 | Menu Top Rounded 135 | 140 | Menu Left Rounded 45 |
| 112 | Menu Top Rounded 145 | 141 | Menu Left Rounded 55 |
| 113 | Menu Top Rounded 155 | 142 | Menu Left Rounded 65 |
| 114 | Menu Top Rounded 165 | 143 | Menu Left Rounded 75 |
| 115 | Menu Top Rounded 175 | 144 | Menu Left Rounded 85 |
| 116 | Menu Top Rounded 185 | 145 | Menu Left Rounded 95 |
| 117 | Menu Top Rounded 195 | 146 | Menu Left Rounded 105 |
| 118 | Menu Right Rounded 15 | 147 | Menu Left Rounded 115 |
| 119 | Menu Right Rounded 25 | 148 | Menu Left Rounded 125 |
| 120 | Menu Right Rounded 35 | 149 | Menu Left Rounded 135 |
| 121 | Menu Right Rounded 45 | 150 | Menu Left Rounded 145 |
| 122 | Menu Right Rounded 55 | 151 | Menu Left Rounded 155 |
| 123 | Menu Right Rounded 65 | 152 | Menu Left Rounded 165 |
| 124 | Menu Right Rounded 75 | 153 | Menu Left Rounded 175 |
| 125 | Menu Right Rounded 85 | 154 | Menu Left Rounded 185 |
| 126 | Menu Right Rounded 95 | 155 | Menu Left Rounded 195 |
| 127 | Menu Right Rounded 105 | | |

## "^" Button Commands

These Button Commands are used in NetLinx Studio and are case insensitive.

All commands that begin with "^" have the capability of assigning a variable text address range and button state range. **A device must first be defined in the NetLinx programming language with values for the Device: Port : System** (in all programming examples - ***Panel*** is used in place of these values).

- **Variable text ranges** allow you to target 1 or more variable text channels in a single command.
- **Button State ranges** allow you to target 1 or more states of a variable text button with a single command.
- **"."** Character is used for the 'through' notation, also the "**&**" character is used for the 'And' notation.

| "^" Button Commands | |
|---|---|
| **^ANI**<br>Run a button animation (in 1/10 second). | Syntax:<br>`"'^ANI-<vt addr range>,<start state>,<end state>,<time>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>start state = Beginning of button state (0= current state).<br>end state = End of button state.<br>time = In 1/10 second intervals.<br>Example:<br>`SEND_COMMAND Panel,"'^ANI-500,1,25,100'"`<br>Runs a button animation at text range 500 from state 1 to state 25 for 10 second. |
| **^APF**<br>Add page flip action to a button if it does not already exist. | Syntax:<br>`"'^APF-<vt addr range>,<page flip action>,<page name>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>page flip action = **Stan**[dardPage] - Flip to standard page<br>**Prev**[iousPage] - Flip to previous page<br>**Show**[Popup] - Show Popup page<br>**Hide**[Popup] - Hide Popup page<br>**Togg**[lePopup] - Toggle popup state<br>**ClearG**[roup] - Clear popup page group from all pages<br>**ClearP**[age] - Clear all popup pages from a page with the specified page name<br>**ClearA**[ll] - Clear all popup pages from all pages<br>page name = 1 - 50 ASCII characters.<br>Example:<br>`SEND COMMAND Panel,"'^APF-400,Stan,Main Page'"`<br>Assigns a button to a standard page flip with page name 'Main Page'. |
| **^BAT**<br>Append non-unicode text. | Syntax:<br>`"'^BAT-<vt addr range>,<button states range>,<new text>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>new text = 1 - 50 ASCII characters.<br>Example:<br>`SEND_COMMAND Panel,"'^BAT-520,1,Enter City'"`<br>Appends the text 'Enter City' to the button's OFF state. |

| "^" Button Commands (Cont.) | |
|---|---|
| **^BAU**<br>Append unicode text. | Same format as ^UNI.<br>Syntax:<br>`"'^BAU-<vt addr range>,<button states range>,<unicode text>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>unicode text = 1 - 50 ASCII characters. Unicode characters must be entered in Hex format.<br>Example:<br>`SEND_COMMAND Panel,"'^BAU-520,1,00770062'"`<br>Appends Unicode text '00770062' to the button's OFF state. |
| **^BCB**<br>Set the border color to the specified color. | **Only if** the specified border color is not the same as the current color.<br>**Note**: Color can be assigned by color name (without spaces), number or R,G,B value (RRGGBB or RRGGBBAA).<br>Syntax:<br>`"'^BCB-<vt addr range>,<button states range>,<color value>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>color value = Refer to theRGB Values for all 88 Basic Colors table on page 102 for more information.<br>Example:<br>`SEND_COMMAND Panel,"'^BCB-500.504&510,1,12'"`<br>Sets the Off state border color to 12 (Yellow). Colors can be set by Color Numbers, Color name, R,G,B,alpha colors (RRGGBBAA) and R, G & B colors values (RRGGBB). Refer to theRGB Values for all 88 Basic Colors table on page 102. |
| **^BCF**<br>Set the fill color to the specified color. | **Only if** the specified fill color is not the same as the current color.<br>**Note**: Color can be assigned by color name (without spaces), number or R,G,B value (RRGGBB or RRGGBBAA).<br>Syntax:<br>`"'^BCF-<vt addr range>,<button states range>,<color value>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>color value = Refer to theRGB Values for all 88 Basic Colors table on page 102 for more information.<br>Example:<br>`SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,12'"`<br>`SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,Yellow'"`<br>`SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,#F4EC0A63''"`<br>`SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,#F4EC0A'"`<br>Sets the Off state fill color by color number. Colors can be set by Color Numbers, Color name, R,G,B,alpha colors (RRGGBBAA) and R, G & B colors values (RRGGBB). |

| "^" Button Commands (Cont.) | |
|---|---|
| **^BCT**<br>Set the text color to the specified color. | **Only if** the specified text color is not the same as the current color.<br>***Note**: Color can be assigned by color name (without spaces), number or R,G,B value (RRGGBB or RRGGBBAA).*<br>Syntax:<br>`"'^BCT-<vt addr range>,<button states range>,<color value>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>color value = Refer to theRGB Values for all 88 Basic Colors table on page 102 for more information.<br>Example:<br>`SEND_COMMAND Panel,"'^BCT-500.504&510,1,12'"`<br>Sets the Off state border color to 12 (Yellow). Colors can be set by Color Numbers, Color name, R,G,B,alpha colors (RRGGBBAA) and R, G & B colors values (RRGGBB). |
| **^BDO**<br>Set the button draw order. | Determines what order each layer of the button is drawn.<br>Syntax:<br>`"'^BDO-<vt addr range>,<button states range>,<1-5><1-5><1-5><1-5><1-5>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>layer assignments = Fill Layer = 1<br>Image Layer = 2<br>Icon Layer = 3<br>Text Layer = 4<br>Border Layer = 5<br>***Note**: The layer assignments are from bottom to top. The default draw order is* **12345**.<br>Example:<br>`SEND_COMMAND Panel,"'^BDO-530,1&2,51432'"`<br>Sets the button's variable text 530 ON/OFF state draw order (from bottom to top) to Border, Fill, Text, Icon, and Image.<br>Example 2:<br>`SEND_COMMAND Panel,"'^BDO-1,0,12345'"`<br>Sets all states of a button back to its default drawing order. |
| **^BFB**<br>Set the feedback type of the button. | **ONLY works** on General-type buttons.<br>Syntax:<br>`"'^BFB-<vt addr range>,<feedback type>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>feedback type = (None, Channel, Invert, On (Always on), Momentary, and Blink).<br>Example:<br>`SEND_COMMAND Panel,"'^BFB-500,Momentary'"`<br>Sets the Feedback type of the button to 'Momentary'. |

| "^" Button Commands (Cont.) | |
|---|---|
| **^BIM**<br>Set the input mask for the specified address. | Syntax:<br>`"'^BIM-<vt addr range>,<input mask>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>input mask = Refer to the *Text Area Input Masking* section on page 158 for character types.<br>Example:<br>`SEND_COMMAND Panel,"'^BIM-500,AAAAAAAAAA'"`<br>Sets the input mask to ten 'A' characters, that are required, to either a letter or digit **(entry is required).** |
| **^BLN**<br>Set the number of lines removed equally from the top and bottom of a composite video signal. | The maximum number of lines to remove is 240. A value of 0 will display the incoming video signal unaffected. This command is used to scale non 4x3 video images into non 4x3 video buttons.<br>Syntax:<br>`"'^BLN-<vt addr range>,<button states range>,<number of lines>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>number of lines = 0 - 240.<br>Example:<br>`SEND_COMMAND Panel,"'^BLN-500,55'"`<br>Equally removes 55 lines from the top and 55 lines from the bottom of the video button. |

| "^" Button Commands (Cont.) | |
|---|---|
| **^BMC**<br>Button copy command. Copy attributes of the source button to all the destination buttons. | Note that the source is a single button state. Each state must be copied as a separate command. The <codes> section represents what attributes will be copied. All codes are 2 char pairs that can be separated by comma, space, percent or just ran together.<br>Syntax:<br>`"'^BMC-<vt addr range>,<button states range>,<source port>,<source address>,<source state>,<codes>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>• source port = 1 - 100.<br>• source address = 1 - 4000.<br>• source state = 1 - 256.<br>codes:<br>BM - Picture/Bitmap<br>BR - Border<br>CB - Border Color<br>CF - Fill Color<br>CT - Text Color<br>EC - Text effect color<br>EF - Text effect<br>FT - Font<br>IC - Icon<br>JB - Bitmap alignment<br>JI - Icon alignment<br>JT - Text alignment<br>LN - Lines of video removed<br>OP - Opacity<br>SO - Button Sound<br>TX - Text<br>VI - Video slot ID<br>WW - Word wrap on/off<br>Example:<br>`SEND_COMMAND Panel,"'^BMC-425,1,1,500,1,BR'"`<br>or<br>`SEND_COMMAND Panel,"'^BMC-425,1,1,500,1,%BR'"`<br>Copies the OFF state border of button with a variable text address of 500 onto the OFF state border of button with a variable text address of 425.<br>Example 2:<br>`SEND_COMMAND Panel,"'^BMC-150,1,1,315,1,%BR%FT%TX%BM%IC%CF%CT'"`<br>Copies the OFF state border, font, Text, bitmap, icon, fill color and text color of the button with a variable text address of 315 onto the OFF state border, font, Text, bitmap, icon, fill color and text color of the button with a variable text address of 150. |

## "^" Button Commands (Cont.)

**^BMF**

Set any/all button parameters by sending embedded codes and data.

Syntax:

```
"'^BMF-<vt addr range>,<button states range>,<data>'"
```

Variables:

variable text address char array = 1 - 4000.

button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).

level range = 1 - 600 (level value is 1 - 65535).

data:

'%R<left>, <top>, <right>, <bottom>' = Set rectangle.

'%B<border style>' = Set the border style name. See theBorder Styles and Programming Numbers table on page 105.

'%B',<border 0-27,40,41> = Set the borer style number. See theBorder Styles and Programming Numbers table on page 105.

'%DO<1-5><1-5><1-5><1-5><1-5> = Set the draw order. Listed from bottom to top. Refer to the ^BDO command on page 110 for more information.

'%F',<font 1-8,10,11,20-29,32-xx> = Set the font. See theDefault Font Styles and ID Numbers table on page 105.

'%F<font 01-08,10,11,20-29,32-xx>' = Set the font. See theDefault Font Styles and ID Numbers table on page 105.

'%MI<mask image>' = Set the mask image. Refer to the ^BMI command on page 115 for more information.

'%T<text >' = Set the text using ASCII characters (empty is clear).

'%P<bitmap>' = Set the picture/bitmap filename (empty is clear).

'%I',<icon 01-9900, 0-clear>' = Set the icon using values of 01 - 9900 (icon numbers are assigned in the TPDesign4 Resource Manager tab - Slots section).

'%I<icon 01-9900, 0-clear>' = Set the icon using values of 01 - 9900 (icon numbers are assigned in the TPDesign4 Resource Manager tab - Slots section).

'%J',<alignment of text 1-9> = As shown the following telephone keypad alignment chart:

0

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |

Zero can be used for an absolute position

'%JT<alignment of text 0-9>' = As shown the above telephone keypad alignment chart, **BUT** the 0 (zero) is absolute and followed by **',<left>,<top>'**

'%JB<alignment of bitmap/picture 0-9>' = As shown the above telephone keypad alignment chart BUT the 0 (zero) is absolute and followed by **',<left>,<top>'**

'%JI<alignment of icon 0-9>' = As shown the above telephone keypad alignment chart, **BUT** the 0 (zero) is absolute and followed by **',<left>,<top>'**

*For some of these commands and values, refer to* theRGB Values for all 88 Basic Colors table on page 102.

'%CF<on fill color>' = Set Fill Color.

'%CB<on border color>' = Set Border Color.

'%CT<on text color>' = Set Text Color.

'%SW<1 or 0>' = Show/hide a button.

'%SO<sound>' = Set the button sound.

'%EN<1 or 0>' = Enable/disable a button.

'%WW<1 or 0>' = Word wrap ON/OFF.

'%GH<bargraph hi>' = Set the bargraph upper limit.

'%GL<bargraph low>' = Set the bargraph lower limit.

'%GN<bargraph slider name>' = Set the bargraph slider name/Joystick cursor name.

'%GC<bargraph slider color>' = Set the bargraph slider color/Joystick cursor color.

'%GI<bargraph invert>' = Set the bargraph invert/noninvert or joystick coordinate (0,1,2,3). *^GIV* section on page 121 more information.

| "^" Button Commands (Cont.) | |
|---|---|
| **^BMF (Cont.)** | '%GU<bargraph ramp up>' = Set the bargraph ramp up time in intervals of 1/10 second.<br>'%GD<bargraph ramp down>' = Set the bargraph ramp down time in 1/10 second.<br>'%GG<bargraph drag increment> = Set the bargraph drag increment. Refer to the ^GDI command on page 121 for more information.<br>'%VI<video ON/OFF>' = Set the Video either ON (value=1) or OFF (value=0).<br>'%OT<feedback type>' = Set the Feedback (Output) Type to one of the following: None, Channel,Invert, ON (Always ON), Momentary, or Blink.<br>'%SM' = Submit a text for text area button.<br>'%SF<1 or 0>' = Set the focus for text area button.<br>'%OP<0-255>' = Set the button opacity to either Invisible (value=0) or Opaque (value=255).<br>'%OP#<00-FF>' = Set the button opacity to either Invisible (value=00) or Opaque (value=FF).<br>'%UN<Unicode text>' = Set the Unicode text. See the^*UNI* section on page 126 for the text format.<br>'%LN<0-240>' = Set the lines of video being removed. ^*BLN* section on page 111 for more information.<br>'%EF<text effect name>' = Set the text effect.<br>'%EC<text effect color>' = Set the text effect color.<br>'%ML<max length>' = Set the maximum length of a text area.<br>'%MK<input mask>' = Set the input mask of a text area.<br>'%VL<0-1>' = Log-On/Log-Off the computer control connection<br>'%VN<network name>' = Set network connection name.<br>'%VP<password>' = Set the network connection password.<br>Example:<br>`SEND_COMMAND Panel,"'^BMF-500,1,%B10%CFRed%CB Blue %CTBlack%Ptest.png'"`<br>Sets the button OFF state as well as the Border, Fill Color, Border Color, Text Color, and Bitmap. |

| "^" Button Commands (Cont.) | |
|---|---|
| **^BMI**<br>Set the button mask image. | Mask image is used to crop a borderless button to a non-square shape. This is typically used with a bitmap.<br>Syntax:<br>`"'^BMI-<vt addr range>,<button states range>,<mask image>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>mask image = Graphic file used.<br>Example:<br>`SEND_COMMAND Panel,"'^BMI-530,1&2,newMac.png'"`<br>Sets the button with variable text 530 ON/OFF state mask image to 'newmac.png'.<br><br>`'"^BMI-<variable text address range>,<button states range>,<mask image>"'`<br>Set the Chameleon Image button property. See Working With Chameleon Images in TPD4 Help.<br>**Note:** If the Border Style properties is set to something other than 'None', no visible change will occur. Setting the Border Style to 'None' via ^BOR or ^BMF..%B will reveal the Chameleon image.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'^BMI-<vt addr range>,<button states range>,<mask image>'"`<br>Variables:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons<br>(0 = All states, for General buttons 1 = Off state and 2 = On state).<br>mask image = Chameleon used.<br>Example:<br>`SEND_COMMAND Panel,"'^BMI-530,1&2,newMac.png'"`<br>Sets the button with variable text 530 ON/OFF state mask image to 'newmac.png'. |
| **^BML**<br>Set the maximum length of the text area button. | If this value is set to zero (0) there is no max length. The maximum length available is 2000. This is only for a Text area input button and not for a Text area input masking button.<br>Syntax:<br>`"'^BML-<vt addr range>,<max length>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>max length = 2000 (0=no max length).<br>Example:<br>`SEND_COMMAND Panel,"'^BML-500,20'"`<br>Sets the maximum length of the text area input button to 20 characters. |
| **^BMP**<br>Assign a picture to those buttons with a defined address range. | Syntax:<br>`"'^BMP-<vt addr range>,<button states range>,<name of bitmap/picture>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>name of bitmap/picture = 1 - 50 ASCII characters.<br>Example:<br>`SEND_COMMAND Panel,"'^BMP-500.504&510.515,1,bitmap.png'"`<br>Sets the OFF state picture for the buttons with variable text ranges of 500-504 & 510-515. |

| "^" Button Commands (Cont.) | |
|---|---|
| **^BNC**<br>Clear current TakeNote annotations. | Syntax:<br>"'^BNC-<vt addr range>,<command value>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>command value = (0= clear, 1= clear all).<br>Example:<br>SEND_COMMAND Panel,"'^BNC-973,0'"<br>Clears the annotation of the TakeNote button with variable text 973. |
| **^BNN**<br>Set the TakeNote network name for the specified Addresses. | Syntax:<br>"'^BNN-<vt addr range>,<network name>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>network name = Use a valid IP Address.<br>Example:<br>SEND_COMMAND Panel,"'^BNN-973,192.168.169.99'"<br>Sets the TakeNote button network name to 192.168.169.99. |
| **^BNT**<br>Set the TakeNote network port for the specified Addresses. | Syntax:<br>"'^BNT-<vt addr range>,<network port>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>network port = 1 - 65535.<br>Example:<br>SEND_COMMAND Panel,"'^BNT-973,5000'"<br>Sets the TakeNote button network port to 5000. |
| **^BOP**<br>Set the button opacity. | The button opacity can be specified as a decimal between 0 - 255, where zero (0) is invisible and 255 is opaque, or as a HEX code, as used in the color commands by preceding the HEX code with the # sign. In this case, #00 becomes invisible and #FF becomes opaque. If the opacity is set to zero (0), this does not make the button inactive, only invisible.<br>Syntax:<br>"'^BOP-<vt addr range>,<button states range>,<button opacity>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>button opacity = 0 (invisible) - 255 (opaque).<br>Example:<br>SEND_COMMAND Panel,"'^BOP-500.504&510.515,1,200'"<br>Example 2:<br>SEND_COMMAND Panel,"'^BOP-500.504&510.515,1,#C8'"<br>Both examples set the opacity of the buttons with the variable text range of 500-504 and 510-515 to 200. |

| "^" Button Commands (Cont.) | |
|---|---|
| **^BOR**<br>Set a border to a specific border style associated with a border value for those buttons with a defined address range. | Refer to theBorder Styles and Programming Numbers table on page 105 for more information.<br>Syntax:<br>`"'^BOR-<vt addr range>,<border style name or border value>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>border style name = Refer to theBorder Styles and Programming Numbers table on page 105.<br>border value = 0 - 41.<br>Examples:<br>`SEND_COMMAND Panel,"'^BOR-500.504&510.515,10'"`<br>Sets the border by number (#10) to those buttons with the variable text range of 500-504 & 510-515.<br>`SEND_COMMAND Panel,"'^BOR-500.504&510,AMX Elite -M'"`<br>Sets the border by name (AMX Elite) to those buttons with the variable text range of 500-504 & 510-515.<br>The border style is available through the TPDesign4 border-style drop-down list. Refer to theTPD4 Border Styles by Name table on page 105 for more information. |
| **^BOS**<br>Set the button to display either a Video or Non-Video window. | Syntax:<br>`"'^BOS-<vt addr range>,<button states range>,<video state>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>video state = Video Off = 0 and Video On = 1.<br>Example:<br>`SEND_COMMAND Panel,"'^BOS-500,1,1'"`<br>Sets the button to display video. |
| **^BPP**<br>Set or clear the protected page flip flag of a button. | Zero clears the flag.<br>Syntax:<br>`"'^BPP-<vt addr range>,<protected page flip flag value>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>protected page flip flag value range = 0 - 4 (**0 clears the flag**).<br>Example:<br>`SEND_COMMAND Panel,"'^BPP-500,1'"`<br>Sets the button to protected page flip flag 1 (sets it to password 1). |
| **^BRD**<br>Set the border of a button state/ states. | **Only if** the specified border is not the same as the current border. The border names are available through the TPDesign4 border-name drop-down list.<br>Syntax:<br>`"'^BRD-<vt addr range>,<button states range>,<border name>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>border name = Refer toBorder Styles and Programming Numbers table on page 105.<br>Example:<br>`SEND_COMMAND Panel,"'^BRD-500.504&510.515,1&2,Quad Line'"`<br>Sets the border by name (Quad Line) to those buttons with the variable text range of 500-504 & 510-515.<br>Refer to theTPD4 Border Styles by Name table on page 105. |

| "^" Button Commands (Cont.) | |
|---|---|
| **^BSF**<br>Set the focus to the text area. | **Note**: Select one button at a time (single variable text address). Do not assign a variable text address range to set focus to multiple buttons. Only one variable text address can be in focus at a time.<br>Syntax:<br>`"'^BSF-<vt addr range>,<selection value>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>selection value = Unselect = 0 and select = 1.<br>Example:<br>`SEND_COMMAND Panel,"'^BSF-500,1'"`<br>Sets the focus to the text area of the button. |
| **^BSM**<br>Submit text for text area buttons. | This command causes the text areas to send their text as strings to the NetLinx Master.<br>Syntax:<br>`"'^BSM-<vt addr range>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>Example:<br>`SEND_COMMAND Panel,"'^BSM-500'"`<br>Submits the text of the text area button. |
| **^BSO**<br>Set the sound played when a button is pressed. | If the sound name is blank the sound is then cleared. If the sound name is not matched, the button sound is not changed.<br>Syntax:<br>`"'^BSO-<vt addr range>,<button states range>,<sound name>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>sound name = (**blank** - sound cleared, **not matched** - button sound not changed).<br>Example:<br>`SEND_COMMAND Panel,"'^BSO-500,1&2,music.wav'"`<br>Assigns the sound 'music.wav' to the button Off/On states. |
| **^BVL**<br>Log-On/Log-Off the computer control connection. | Syntax:<br>`"'^BVL-<vt addr range>,<connection>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>connection = 0 (Log-Off connection) and 1 (Log-On connection).<br>Example:<br>`SEND_COMMAND Panel,"'^BVL-500,0'"`<br>Logs-off the computer control connection of the button. |
| **^BVN**<br>Set the computer control remote host for the specified address. | Syntax:<br>`SEND_COMMAND <DEV>,"'^BVN-<vt addr range>,<remote host>'"`<br>Variables:<br>variable text address range = 1 - 4000.<br>remote host = 1 - 50 ASCII characters.<br>Example:<br>`SEND_COMMAND Panel,"'^BVN-500,191.191.191.191'"`<br>Sets the remote host to '191.191.191.191' for the specific computer control button. |

| "^" Button Commands (Cont.) | |
|---|---|
| **^BVP**<br>Set the network password for the specified address. | Syntax:<br>"'^BVP-<vt addr range>,<network password>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>network password = 1 - 50 ASCII characters.<br>Example:<br>SEND_COMMAND Panel,"'^BVP-500,PCLOCK'"<br>Sets the password to PCLOCK for the specific PC control button. |
| **^BVT**<br>Set the computer control network port for the specified address. | Syntax:<br>"'^BVT-<vt addr range>,<network port>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>network port = 1 - 65535.<br>Example:<br>SEND_COMMAND Panel,"'^BVT-500,5000'"<br>Sets the network port to 5000. |
| **^BWW**<br>Set the button word wrap feature to those buttons with a defined address range. | By default, word-wrap is Off.<br>Syntax:<br>"'^BWW-<vt addr range>,<button states range>,<word wrap>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>word wrap = (0=Off and 1=On). Default is Off.<br>Example:<br>SEND_COMMAND Panel,"'^BWW-500,1,1'"<br>Sets the word wrap on for the button's Off state. |
| **^CPF**<br>Clear all page flips from a button. | Syntax:<br>"'^CPF-<vt addr range>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>Example:<br>SEND_COMMAND Panel,"'^CPF-500'"<br>Clears all page flips from the button. |
| **^DLD**<br>Set the disable cradle LED flag. | Syntax:<br>"'^DLD-<status>'"<br>Variable:<br>status = (**0**= cradle operates normally, **1**= forces the cradle LEDs to always be dim).<br>Example:<br>SEND_COMMAND Panel,"'^DLD-1'"<br>Disables the cradle LEDs. |

| "^" Button Commands (Cont.) | |
|---|---|
| **^DPF**<br>Delete page flips from button if it already exists. | Syntax:<br>"'^DFP-<vt addr range>,<actions>,<page name>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>actions = **Stan**[dardPage] - Flip to standard page<br>**Prev**[iousPage] - Flip to previous page<br>**Show**[Popup] - Show Popup page<br>**Hide**[Popup] - Hide Popup page<br>**Togg**[lePopup] - Toggle popup state<br>**ClearG**[roup] - Clear popup page group from all pages<br>**ClearP**[age] - Clear all popup pages from a page with the specified page name<br>**ClearA**[ll] - Clear all popup pages from all pages<br>page name = 1 - 50 ASCII characters.<br>Example:<br>SEND COMMAND Panel,"'^DPF-409,Prev'"<br>Deletes the assignment of a button from flipping to a previous page. |
| **^ENA**<br>Enable or disable buttons with a set variable text range. | Syntax:<br>"'^ENA-<vt addr range>,<command value>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>command value = (0= disable, 1= enable)<br>Example:<br>SEND_COMMAND Panel,"'^ENA-500.504&510.515,0'"<br>Disables button pushes on buttons with variable text range 500-504 & 510-515. |
| **^FON**<br>Set a font to a specific Font ID value for those buttons with a defined address range. | Font ID numbers are generated by the TPDesign4 programmers report.<br>Syntax:<br>"'^FON-<vt addr range>,<button states range>,<font value>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>font value = range = 1 - XXX. Refer to theDefault Font Styles and ID Numbers table on page 105.<br>Example:<br>SEND_COMMAND Panel,"'^FON-500.504&510.515,1&2,4'"<br>Sets the font size to font ID #4 for the On and Off states of buttons with the variable text range of 500-504 & 510-515. |


*The Font ID is generated by TPD4 and is located in TPD4 through the Main menu.*
***Panel > Generate Programmer's Report >Text Only Format >Readme.txt.***

| "^" Button Commands (Cont.) | |
|---|---|
| **^GDI**<br>Change the bargraph drag increment. | Syntax:<br>`"'^GDI-<vt addr range>,<bargraph drag increment>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>bargraph drag increment = The default drag increment is 256.<br>Example:<br>`SEND_COMMAND Panel,"'^GDI-7,128'"`<br>Sets the bargraph with variable text 7 to a drag increment of 128. |
| **^GIV**<br>Invert the joystick axis to move the origin to another corner. | Parameters 1,2, and 3 will cause a bargraph or slider to be inverted regardless of orientation. Their effect will be as described for joysticks.<br>Syntax:<br>`"'^GIV-<vt addr range>,<joystick axis to invert>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>joystick axis to invert = 0 - 3.<br>0 1<br>2 3<br>0 = Normal<br>1 = Invert horizontal axis<br>2 = Invert vertical axis<br>3 = Invert both axis locations<br>For a bargraph 1 = Invert , 0 = Non Invert<br>Example:<br>`SEND_COMMAND Panel,"'^GIV-500,3'"`<br>Inverts the joystick axis origin to the bottom right corner. |
| **^GLH**<br>Change the bargraph upper limit. | Syntax:<br>`"'^GLH-<vt addr range>,<bargraph hi>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>bargraph limit range = 1 - 65535 (*bargraph upper limit range*).<br>Example:<br>`SEND_COMMAND Panel,"'^GLH-500,1000'"`<br>Changes the bargraph upper limit to 1000. |
| **^GLL**<br>Change the bargraph lower limit. | Syntax:<br>`"'^GLL-<vt addr range>,<bargraph low>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>bargraph limit range = 1 - 65535 (*bargraph lower limit range*).<br>Example:<br>`SEND_COMMAND Panel,"'^GLL-500,150'"`<br>Changes the bargraph lower limit to 150. |
| **^GRD**<br>Change the bargraph ramp-down time in 1/10th of a second. | Syntax:<br>`"'^GRD-<vt addr range>,<bargraph ramp down time>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>bargraph ramp down time = In 1/10th of a second intervals.<br>Example:<br>`SEND_COMMAND Panel,"'^GRD-500,200'"`<br>Changes the bargraph ramp down time to 20 seconds. |

<table>
<tr><th colspan="2">"^" Button Commands (Cont.)</th></tr>
<tr><td>^GRU<br>Change the bargraph ramp-up time in 1/10th of a second.</td><td>Syntax:<br>"'^GRU-<vt addr range>,<bargraph ramp up time>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>bargraph ramp up time = In 1/10th of a second intervals.<br>Example:<br>SEND_COMMAND Panel,"'^GRU-500,100'"<br>Changes the bargraph ramp up time to 10 seconds.</td></tr>
<tr><td>^GSC<br>Change the bargraph slider color or joystick cursor color.</td><td>A user can also assign the color by Name and R,G,B value (RRGGBB or RRGGBBAA).<br>Syntax:<br>"'^GSC-<vt addr range>,<color value>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>color value = Refer to theRGB Values for all 88 Basic Colors table on page 102.<br>Example:<br>SEND_COMMAND Panel,"'^GSC-500,12'"<br>Changes the bargraph or joystick slider color to Yellow.</td></tr>
<tr><td>^GSN<br>Change the bargraph slider name or joystick cursor name.</td><td>Slider names and cursor names can be found in the TPDesign4 slider name and cursor drop-down list.<br>Syntax:<br>"'^GSN-<vt addr range>,<bargraph slider name>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>bargraph slider name = See table below.<br><table><tr><td colspan="3">Bargraph Slider Names:</td></tr><tr><td>None</td><td>Ball</td><td>Circle -L</td></tr><tr><td>Circle -M</td><td>Circle -S</td><td>Precision</td></tr><tr><td>Rectangle -L</td><td>Rectangle -M</td><td>Rectangle -S</td></tr><tr><td>Windows</td><td>Windows Active</td><td></td></tr><tr><td colspan="3">Joystick Cursor Names:</td></tr><tr><td>None</td><td>Arrow</td><td>Ball</td></tr><tr><td>Circle</td><td>Crosshairs</td><td>Gunsight</td></tr><tr><td>Hand</td><td>Metal</td><td>Spiral</td></tr><tr><td>Target</td><td>View Finder</td><td></td></tr></table><br>Example:<br>SEND_COMMAND Panel,"'^GSN-500,Ball'"<br>Changes the bargraph slider name or the Joystick cursor name to 'Ball'.</td></tr>
<tr><td>^ICO<br>Set the icon to a button.</td><td>Syntax:<br>"'^ICO-<vt addr range>,<button states range>,<icon index>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>icon index range = 0 - 9900 (a value of 0 is clear).<br>Example:<br>SEND_COMMAND Panel,"'^ICO-500.504&510.515,1&2,1'"<br>Sets the icon for On and Off states for buttons with variable text ranges of 500-504 & 510-515.</td></tr>
</table>

<table>
<tr><th colspan="2">"^" Button Commands (Cont.)</th></tr>
<tr><td>^IRM<br>Set the IR channel.</td><td>Pulse the given IR channel for onTime in tenths of seconds. Delay offTime in tenths of a second before the next IR pulse is allowed. ^IRM allows the command itself to specify the port number. ^IRM is needed because commands programmed on the panel itself can only be sent to a single port number. (currently this is defined as 1 only).<br>Note: The port number of the IR will be the port number assigned in TPD4.<br>Syntax:<br><code>"'^IRM-<port>,<channel>,<onTime>,<offTime>'"</code><br>Variable:<br>port = User-defined port on the device (panel).<br>channel = 1 - 255 (channel to pulse).<br>onTime = 1/10th of a second.<br>offTime = 1/10th of a second.<br>Example:<br><code>SEND_COMMAND Panel,"'^IRM-10,5, 20, 10'"</code><br>Sets the port 10 IR channel 5 on time to 1 second and off time to 2 seconds.</td></tr>
<tr><td>^JSB<br>Set bitmap/ picture alignment using a numeric keypad layout for those buttons with a defined address range.</td><td>The alignment of 0 is followed by ',<left>,<top>'. The left and top coordinates are relative to the upper left corner of the button.<br>Syntax:<br><code>"'^JSB-<vt addr range>,<button states range>,<new text alignment>'"</code><br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>new text alignment = Value of 1- 9 corresponds to the following locations:<br>0<br>1 2 3<br>4 5 6<br>7 8 9<br>Zero can be used for an absolute position<br>Example:<br><code>SEND_COMMAND Panel,"'^JSB-500.504&510.515,1&2,1'"</code><br>Sets the off/on state picture alignment to upper left corner for those buttons with variable text ranges of 500-504 & 510-515.</td></tr>
<tr><td>^JSI<br>Set icon alignment using a numeric keypad layout for those buttons with a defined address range.</td><td>The alignment of 0 is followed by ',<left>,<top>'. The left and top coordinates are relative to the upper left corner of the button.<br>Syntax:<br><code>"'^JSI-<vt addr range>,<button states range>,<new icon alignment>'"</code><br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>new icon alignment = Value of 1 - 9 corresponds to the following locations:<br>0<br>1 2 3<br>4 5 6<br>7 8 9<br>Zero can be used for an absolute position<br>Example:<br><code>SEND_COMMAND Panel,"'^JSI-500.504&510.515,1&2,1'"</code><br>Sets the Off/On state icon alignment to upper left corner for those buttons with variable text range of 500-504 & 510-515.</td></tr>
</table>

| "^" Button Commands (Cont.) | |
|---|---|
| **^JST**<br>Set text alignment using a numeric keypad layout for those buttons with a defined address range. | The alignment of 0 is followed by ',<left>,<top>'. The left and top coordinates are relative to the upper left corner of the button.<br>Syntax:<br>`"'^JST-<vt addr range>,<button states range>,<new text alignment>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>new text alignment = Value of 1 - 9 corresponds to the following locations:<br>0<br>1 2 3<br>4 5 6<br>7 8 9<br>Zero can be used for an absolute position<br>Example:<br>`SEND_COMMAND Panel,"'^JST-500.504&510.515,1&2,1'"`<br>Sets the text alignment to the upper left corner for those buttons with variable text ranges of 500-504 & 510-515. |
| **^MBT**<br>Set the Mouse Button mode On for the virtual PC. | Syntax:<br>`"'^MBT-<pass data>'"`<br>Variable:<br>**pass data**:<br>0 = None<br>1 = Left<br>2 = Right<br>3 = Middle<br>Example:<br>`SEND COMMAND Panel,"'^MBT-1'"`<br>Sets the mouse button mode to 'Left Mouse Click'. |
| **^MDC**<br>Turn On the 'Mouse double-click' feature for the virtual PC. | Syntax:<br>`"'^MDC'"`<br>Example:<br>`SEND COMMAND Panel,"'^MDC'"`<br>Sets the mouse double-click for use with the virtual PC. |
| **^SAV**<br>Save the configuration values. | Syntax:<br>`"'^SAV'"` |
| **^SHO**<br>Show or hide a button with a set variable text range. | Syntax:<br>`"'^SHO-<vt addr range>,<command value>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>command value = (0= hide, 1= show).<br>Example:<br>`SEND_COMMAND Panel,"'^SHO-500.504&510.515,0'"`<br>Hides buttons with variable text address range 500-504 & 510-515. |

| "^" Button Commands (Cont.) | |
|---|---|
| **^SKT**<br>Receive touch information on specified socket. | Syntax:<br>`'^SKT-<0=disable socket, greater than 1023=enable socket on specified port>`<br>Only socket values equal to or greater than 1024 are valid. The panel will open up a TCP listening socket on the port specified. User or 3rd party program can connect to the panel using this port/socket number and receive touch/release/move strings. By default, the panel disables touch notifications on startup. Format of the output is:<br><Press/Release/Move>,<x-coordinate>,<y-coordinate><br>Example:<br>`send_command TP, '^SKT-7425' (enables touch notifications on socket 7425) send_command TP, '^SKT-0' (disable touch notification)` |
| **^STO**<br>Set the shutdown timeout value. | Returned in Custom event.<br>Value1=shutdown timeout value (in minutes) |
| **^TEC**<br>Set the text effect color for the specified addresses/states to the specified color. | The Text Effect is specified by name and can be found in TPD4. You can also assign the color by name or RGB value (RRGGBB or RRGGBBAA).<br>Syntax:<br>`"'^TEC-<vt addr range>,<button states range>,<color value>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>color value = Refer to theRGB Values for all 88 Basic Colors table on page 102.<br>Example:<br>`SEND_COMMAND Panel,"'^TEC-500.504&510.515,1&2,12'"`<br>Sets the text effect color to Very Light Yellow on buttons with variable text 500-504 and 510-515. |
| **^TEF**<br>Set the text effect. | The Text Effect is specified by name and can be found in TPD4.<br>Syntax:<br>`"'^TEF-<vt addr range>,<button states range>,<text effect name>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>text effect name = **Refer to theText Effects table on page 128 for a listing of text effect names**.<br>Example:<br>`SEND_COMMAND Panel,"'^TEF-500.504&510.515,1&2,Soft Drop Shadow 3'"`<br>Sets the text effect to Soft Drop Shadow 3 for the button with variable text range 500-504 and 510-515. |
| **^TOP**<br>Enable/disable SEND strings sent to the master. | Syntax:<br>`^TOP-<0=disable output,1=enable output>`<br>Enable/disable send strings sent to master when PRESS/RELEASE happens:<br>`Press,564,219`<br>or<br>`Release,445,224` |

| "^" Button Commands (Cont.) | |
|---|---|
| **^TXT**<br>Assign a text string to those buttons with a defined address range. | Sets Non-Unicode text.<br>Syntax:<br>`"'^TXT-<vt addr range>,<button states range>,<new text>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>new text = 1 - 50 ASCII characters.<br>Example:<br>`SEND_COMMAND Panel,"'^TXT-500.504&510.515,1&2,Test Only'"`<br>Sets the On and Off state text for buttons with the variable text ranges of 500-504 & 510-515. |
| **^UNI**<br>Set Unicode text. | For the ^UNI command (%UN and ^BMF command), the Unicode text is sent as ASCII-HEX nibbles.<br>Syntax:<br>`"'^UNI-<vt addr range>,<button states range>,<unicode text>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>unicode text = Unicode HEX value.<br>Example:<br>`SEND_COMMAND Panel,"'^UNI-500,1,0041'"`<br>Sets the button's unicode character to 'A'.<br>***Note: To send the variable text 'A' in unicode to all states of the variable text button 1, (for which the character code is 0041 Hex), send the following command:***<br>`SEND_COMMAND TP,"'^UNI-1,0,0041'"`<br>Note: Unicode is always represented in a HEX value. TPD4 generates (through the Text Enter Box dialog) unicode HEX values. Refer to the TPDesign4 Instruction Manual for more information. |
| **^VTP**<br>Simulates a touch/release/ pulse at the given coordinate. | Syntax:<br>`^VTP-<0=Release, 1=Press, 2=Pulse>,<x>,<y>` |

## Miscellaneous MVP Strings back to the Master

The following two strings are sent by the MVP panel back to the communicating Master:

| MVP Strings to Master | |
|---|---|
| **undock <master>** | This is sent to the target Master when the MVP is undocked.<br>• If the panel has no information within the User Access Passwords list, 'none' is sent as a user.<br>• If the undock button on the Protected Setup page is used, 'setup' is sent as a user.<br>• This string can be disabled from within the firmware setup pages. |
| **dock** | This is sent to the target Master when the MVP is docked.<br>• This string can be disabled from within the firmware setup pages. |

## MVP Panel Lock Passcode commands

These commands are used to maintain a passcode list. From certain panels a password must be entered to remove the panel from its cradle. Only the passcode is entered. The user is just for identifying the passcodes.

| MVP Panel Lock Passcode Commands | |
|---|---|
| **^LPC**<br>Clear all users from the User Access Passwords list on the Password Setup page. | Syntax:<br>`"'^LPC'"`<br>Example:<br>`SEND_COMMAND Panel,"'^LPC'"`<br>Clear all users from the User Access Password list on the Password Setup page. Refer to the *Password Setup Page* section on page 77 for more information. |
| **^LPR**<br>Remove a given user from the User Access Passwords list on the Password Setup page. | Syntax:<br>`"'^LPR-<user>'"`<br>Variable:<br>user = 1 - 50 ASCII characters.<br>Example:<br>`SEND_COMMAND Panel,"'^LPR-Robert'"`<br>Remove user named 'Robert' from the User Access Password list on the Password Setup page. Refer to the*Password Setup Page* section on page 77 for more information. |
| **^LPS**<br>Set the user name and password. | This command allows you to:<br>1. Add a new user name and password OR<br>2. Set the password for a given user.<br>The user name and password combo is added to the User Access and/or Password list in the Password Setup page. The user name must be alphanumeric.<br>Syntax:<br>`"'^LPS-<user>,<passcode>'"`<br>Variable:<br>user = 1 - 50 ASCII characters.<br>passcode = 1 - 50 ASCII characters.<br>Example:<br>`SEND_COMMAND Panel,"'^LPS-Manager,undock'"`<br>Sets a new user name as "Manager" and the password to "undock".<br>Example 2:<br>`SEND_COMMAND Panel,"'^LPS-Manager,test'"`<br>Changes the given user name password to "test".<br>Refer to the*Password Setup Page* section on page 77 for more information. |

## Text Effects Names

The following is a listing of text effects names (associated with the **^TEF** command on page 125).

| Text Effects | | |
|---|---|---|
| • Glow -S | • Medium Drop Shadow 1 | • Hard Drop Shadow 1 |
| • Glow -M | • Medium Drop Shadow 2 | • Hard Drop Shadow 2 |
| • Glow -L | • Medium Drop Shadow 3 | • Hard Drop Shadow 3 |
| • Glow -X | • Medium Drop Shadow 4 | • Hard Drop Shadow 4 |
| • Outline -S | • Medium Drop Shadow 5 | • Hard Drop Shadow 5 |
| • Outline -M | • Medium Drop Shadow 6 | • Hard Drop Shadow 6 |
| • Outline -L | • Medium Drop Shadow 7 | • Hard Drop Shadow 7 |
| • Outline -X | • Medium Drop Shadow 8 | • Hard Drop Shadow 8 |
| • Soft Drop Shadow 1 | • Medium Drop Shadow 1 with outline | • Hard Drop Shadow 1 with outline |
| • Soft Drop Shadow 2 | • Medium Drop Shadow 2 with outline | • Hard Drop Shadow 2 with outline |
| • Soft Drop Shadow 3 | • Medium Drop Shadow 3 with outline | • Hard Drop Shadow 3 with outline |
| • Soft Drop Shadow 4 | • Medium Drop Shadow 4 with outline | • Hard Drop Shadow 4 with outline |
| • Soft Drop Shadow 5 | • Medium Drop Shadow 5 with outline | • Hard Drop Shadow 5 with outline |
| • Soft Drop Shadow 6 | • Medium Drop Shadow 6 with outline | • Hard Drop Shadow 6 with outline |
| • Soft Drop Shadow 7 | • Medium Drop Shadow 7 with outline | • Hard Drop Shadow 7 with outline |
| • Soft Drop Shadow 8 | • Medium Drop Shadow 8 with outline | • Hard Drop Shadow 8 with outline |
| • Soft Drop Shadow 1 with outline | | |
| • Soft Drop Shadow 2 with outline | | |
| • Soft Drop Shadow 3 with outline | | |
| • Soft Drop Shadow 4 with outline | | |
| • Soft Drop Shadow 5 with outline | | |
| • Soft Drop Shadow 6 with outline | | |
| • Soft Drop Shadow 7 with outline | | |
| • Soft Drop Shadow 8 with outline | | |

## Button Query Commands

Button Query commands reply back with a custom event. There will be one custom event for each button/state combination. Each query is assigned a unique custom event type. **The following example is for debug purposes only:**

```
NetLinx Example: CUSTOM_EVENT[device, Address, Custom event type]

DEFINE_EVENT
CUSTOM_EVENT[TP,529,1001]      // Text
CUSTOM_EVENT[TP,529,1002]      // Bitmap
CUSTOM_EVENT[TP,529,1003]      // Icon
CUSTOM_EVENT[TP,529,1004]      // Text Justification
CUSTOM_EVENT[TP,529,1005]      // Bitmap Justification
CUSTOM_EVENT[TP,529,1006]      // Icon Justification
CUSTOM_EVENT[TP,529,1007]      // Font
CUSTOM_EVENT[TP,529,1008]      // Text Effect Name
CUSTOM_EVENT[TP,529,1009]      // Text Effect Color
CUSTOM_EVENT[TP,529,1010]      // Word Wrap
CUSTOM_EVENT[TP,529,1011]      // ON state Border Color
CUSTOM_EVENT[TP,529,1012]      // ON state Fill Color
CUSTOM_EVENT[TP,529,1013]      // ON state Text Color
CUSTOM_EVENT[TP,529,1014]      // Border Name
CUSTOM_EVENT[TP,529,1015]      // Opacity

{
   Send_String 0,"'ButtonGet Id=',ITOA(CUSTOM.ID),' Type=',ITOA(CUSTOM.TYPE)"
   Send_String 0,"'Flag   =',ITOA(CUSTOM.FLAG)"
   Send_String 0,"'VALUE1 =',ITOA(CUSTOM.VALUE1)"
   Send_String 0,"'VALUE2 =',ITOA(CUSTOM.VALUE2)"
   Send_String 0,"'VALUE3 =',ITOA(CUSTOM.VALUE3)"
   Send_String 0,"'TEXT   =',CUSTOM.TEXT"
   Send_String 0,"'TEXT LENGTH =',ITOA(LENGTH_STRING(CUSTOM.TEXT))"
}
```

All custom events have the following 6 fields:

**Custom Event Fields**

| Field | Description |
|---|---|
| Uint Flag | 0 means text is a standard string, 1 means Unicode encoded string |
| slong value1 | button state number |
| slong value2 | actual length of string (this is not encoded size) |
| slong value3 | index of first character (usually 1 or same as optional index |
| string text | the text from the button |
| text length (string encode) | button text length |

These fields are populated differently for each query command. The text length (String Encode) field is not used in any command.

| Button Query Commands | |
|---|---|
| **?BCB**<br>Get the current border color. | Syntax:<br>`"'?BCB-<vt addr range>,<button states range>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1011:**<br>Flag - zero<br>Value1 - Button state number<br>Value2 - Actual length of string (should be 9)<br>Value3 - Zero<br>Text - Hex encoded color value (ex: #000000FF)<br>Text length - Color name length (should be 9)<br>Example:<br>`SEND COMMAND Panel,"'?BCB-529,1'"`<br>Gets the button 'OFF state' border color. information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1011<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 9<br>VALUE3 = 0<br>TEXT = #222222FF<br>TEXT LENGTH = 9 |
| **?BCF**<br>Get the current fill color. | Syntax:<br>`"'?BCF-<vt addr range>,<button states range>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1012:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - Actual length of string (should be 9)<br>Value3 - Zero<br>Text - Hex encoded color value (ex: #000000FF)<br>Text length - Color name length (should be 9)<br>Example:<br>`SEND COMMAND Panel,"'?BCF-529,1'"`<br>Gets the button 'OFF state' fill color information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1012<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 9<br>VALUE3 = 0<br>TEXT = #FF8000FF<br>TEXT LENGTH = 9 |

| Button Query Commands (Cont.) | |
|---|---|
| **?BCT**<br>Get the current text color. | Syntax:<br>`"'?BCT-<vt addr range>,<button states range>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1013:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - Actual length of string (should be 9)<br>Value3 - Zero<br>Text - Hex encoded color value (ex: #000000FF)<br>Text length - Color name length (should be 9)<br>Example:<br>`SEND COMMAND Panel,"'?BCT-529,1'"`<br>Gets the button 'OFF state' text color information.<br>The result sent to Master would be:<br>ButtonGet Id = 529 Type = 1013<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 9<br>VALUE3 = 0<br>TEXT = #FFFFFEFF<br>TEXT LENGTH = 9 |
| **?BMP**<br>Get the current bitmap name. | Syntax:<br>`"'?BMP-<vt addr range>,<button states range>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1002:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - Actual length of string<br>Value3 - Zero<br>Text - String that represents the bitmap name<br>Text length - Bitmap name text length (should be 9)<br>Example:<br>`SEND COMMAND Panel,"'?BMP-529,1'"`<br>Gets the button 'OFF state' bitmap information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1002<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 9<br>VALUE3 = 0<br>TEXT = Buggs.png<br>TEXT LENGTH = 9 |

| Button Query Commands (Cont.) | |
|---|---|
| **?BOP**<br>Get the overall button opacity. | Syntax:<br>"'?BOP-<vt addr range>,<button states range>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1015:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - Opacity<br>Value3 - Zero<br>Text - Blank<br>Text length - Zero<br>Example:<br>SEND COMMAND Panel,"'?BOP-529,1'"<br>Gets the button 'OFF state' opacity information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1015<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 200<br>VALUE3 = 0<br>TEXT =<br>TEXT LENGTH = 0 |
| **?BRD**<br>Get the current border name. | Syntax:<br>"'?BRD-<vt addr range>,<button states range>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1014:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - Actual length of string<br>Value3 - Zero<br>Text - String that represents border name<br>Text length - Border name length<br>Example:<br>SEND COMMAND Panel,"'?BRD-529,1'"<br>Gets the button 'OFF state' border information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1014<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 22<br>VALUE3 = 0<br>TEXT = Double Bevel Raised -L<br>TEXT LENGTH = 22 |
| **?BRT**<br>Get the current panel brightness. | Returned in Custom event.<br>Value1=panel brightness value |

| Button Query Commands (Cont.) | |
|---|---|
| **?BWW**<br>Get the current word wrap flag status. | Syntax:<br>"'?BWW-<vt addr range>,<button states range>'"<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1010:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - 0 = no word wrap, 1 = word wrap<br>Value3 - Zero<br>Text - Blank<br>Text length - Zero<br>Example:<br>SEND COMMAND Panel,"'?BWW-529,1'"<br>Gets the button 'OFF state' word wrap flag status information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1010<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 1<br>VALUE3 = 0<br>TEXT =<br>TEXT LENGTH = 0 |
| **?CHR**<br>Get the charging status. | Returned in Custom event.<br>Value1=status(0=not charging,1=charging)<br>Value2=current (combined) battery level |
| **?FBC**<br>Get the frame buffer CRC. | Returned in Custom event.<br>Value1=CRC32 calculated on the panel's frame buffer |

| Button Query Commands (Cont.) | |
|---|---|
| **?FON**<br>Get the current font index. | Syntax:<br>`"'?FON-<vt addr range>,<button states range>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1007:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - Font index<br>Value3 - Zero<br>Text - Blank<br>Text length - Zero<br>Example:<br>`SEND COMMAND Panel,"'?FON-529,1'"`<br>Gets the button 'OFF state' font type index information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1007<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 72<br>VALUE3 = 0<br>TEXT =<br>TEXT LENGTH = 0 |
| **?ICO**<br>Get the current icon index. | Syntax:<br>`"'?ICO-<vt addr range>,<button states range>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1003:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - Icon Index<br>Value3 - Zero<br>Text - Blank<br>Text length - Zero<br>Example:<br>`SEND COMMAND Panel,"'?ICO-529,1&2'"`<br>Gets the button 'OFF state' icon index information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1003<br>Flag = 0<br>VALUE1 = 2<br>VALUE2 = 12<br>VALUE3 = 0<br>TEXT =<br>TEXT LENGTH = 0 |

| Button Query Commands (Cont.) | |
|---|---|
| **?JSB**<br>Get the current bitmap justification. | Syntax:<br>`"'?JSB-<vt addr range>,<button states range>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1005:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - 1 - 9 justify<br>Value3 - Zero<br>Text - Blank<br>Text length - Zero<br>Example:<br>`SEND COMMAND Panel,"'?JSB-529,1'"`<br>Gets the button 'OFF state' bitmap justification information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1005<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 5<br>VALUE3 = 0<br>TEXT =<br>TEXT LENGTH = 0 |
| **?JSI**<br>Get the current icon justification. | Syntax:<br>`"'?JSI-<vt addr range>,<button states range>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1006:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - 1 - 9 justify<br>Value3 - Zero<br>Text - Blank<br>Text length - Zero<br>Example:<br>`SEND COMMAND Panel,"'?JSI-529,1'"`<br>Gets the button 'OFF state' icon justification information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1006<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 6<br>VALUE3 = 0<br>TEXT =<br>TEXT LENGTH = 0 |

| Button Query Commands (Cont.) | |
|---|---|
| **?JST**<br>Get the current text justification. | Syntax:<br>`"'?JST-<vt addr range>,<button states range>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1004:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - 1 - 9 justify<br>Value3 - Zero<br>Text - Blank<br>Text length - Zero<br>Example:<br>`SEND COMMAND Panel,"'?JST-529,1'"`<br>Gets the button 'OFF state' text justification information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1004<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 1<br>VALUE3 = 0<br>TEXT =<br>TEXT LENGTH = 0 |
| **?LOG**<br>Get the XML panel logs. | Returned in MULTIPLE Custom events (size of strings are limited per message). Values in Custom event displays the number of messages and how many total bytes of xml data.<br>`Value 1 = 1 (which one of multiple events is this (1 based))`<br>`Value 2 = 5 (total number of events required to send this string)`<br>`Value 3 = total size in bytes of string`<br>`Text = XML output (1 of 5)`<br>total XML output resembles:<br>`<?xml version="1.0" ?>`<br>`<PanelLogs>`<br>`<Log>`<br>`<Date>09-04-2008 THU 11:24:07</Date>`<br>`<Name>MasterUrlConnect</Name>`<br>`<Message>Connected to (Sys=303) Master cjc-master (URL Mode)</Message>`<br>`</Log>`<br>`</PanelLogs>` |
| **?MCO**<br>Get the microphone output level. | Returned in Custom event.<br>Value1=mic out level |
| **?MUT**<br>Get the mute value. | Returned in Custom event<br>Value1=button state(0=off, 1=on) |
| **?PIF**<br>Get the panel file system, RAM, and panel start time information. | Returned in Custom event.<br>Text=<Filesystem Info>,<RAM Info>,<Panel Start Time> |

| Button Query Commands (Cont.) | |
|---|---|
| **?STA**<br>Get the XML panel statistics. | Returned in MULTIPLE Custom events (size of strings are limited per message). Values in the Custom event displays the number of messages and how many total bytes of xml data.<br>`Value 1 = 1 (which one of multiple events is this (1 based))`<br>`Value 2 = 5 (total number of events required to send this string)`<br>`Value 3 = total size in bytes of string`<br>`Text = XML output (1 of 5)`<br>total XML output looks like:<br>`<?xml version="1.0" ?>`<br>`<PanelStats>`<br>`<Icsp>`<br>`<Total><Rx>11</Rx><Proc>11</Proc><Drop>0</Drop></Total>`<br>`<Rolling><Rx>11</Rx><Proc>11</Proc><Drop>0</Drop></Rolling>`<br>`</Icsp>`<br>`<Blink>`<br>`<Total><Rx>3</Rx><Miss>0</Miss></Total>`<br>`<Rolling><Rx>3</Rx><Miss>0</Miss></Rolling>`<br>`</Blink>`<br>`<Ethernet>`<br>`<RxPackets>53063571</RxPackets><RxErrors>0</RxErrors>`<br>`<RxDrops>0</RxDrops><RxOverRuns>0</RxOverRuns><RxFrames>63</RxFrames>`<br>`<TxPackets>17842136</TxPackets><TxErrors>0</TxErrors><TxDrops>0</TxDrops>`<br>`<TxOverRuns>0</TxOverRuns><TxCarriers>0</TxCarriers>`<br>`<Collisions>0</Collisions><TxQueueLen>100</TxQueueLen>`<br>`<RxBytes>292901735</RxBytes><TxBytes>1182103211</TxBytes>`<br>`</Ethernet>`<br>`<Wireless>`<br>`<Mode>Managed</Mode><Frequenc` |
| **?STO**<br>Get the shutdown timeout value. | Returned in Custom event.<br>Value1=shutdown timeout value (in minutes) |
| **?TEC**<br>Get the current text effect color. | Syntax:<br>`"'?TEC-<vt addr range>,<button states range>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1009:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - Actual length of string (should be 9)<br>Value3 - Zero<br>Text - Hex encoded color value (ex: #000000FF)<br>Text length - Color name length (should be 9)<br>Example:<br>`SEND COMMAND Panel,"'?TEC-529,1'"`<br>Gets the button 'OFF state' text effect color information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1009<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 9<br>VALUE3 = 0<br>TEXT = #5088F2AE<br>TEXT LENGTH = 9 |

| Button Query Commands (Cont.) | |
|---|---|
| **?TEF**<br>Get the current text effect name. | Syntax:<br>`"'?TEF-<vt addr range>,<button states range>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>custom event type **1008:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - Actual length of string<br>Value3 - Zero<br>Text - String that represents the text effect name<br>Text length - Text effect name length<br>Example:<br>`SEND COMMAND Panel,"'?TEF-529,1'"`<br>Gets the button 'OFF state' text effect name information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1008<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 18<br>VALUE3 = 0<br>TEXT = Hard Drop Shadow 3<br>TEXT LENGTH = 18 |
| **?TXT**<br>Get the current text information. | Syntax:<br>`"'?TXT-<vt addr range>,<button states range>,<optional index>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>optional index = This is used if a string was too long to get back in one command. The reply will start at this index.<br>custom event type **1001:**<br>Flag - Zero<br>Value1 - Button state number<br>Value2 - Actual length of string<br>Value3 - Index<br>Text - Text from the button<br>Text length - Button text length<br>Example:<br>`SEND COMMAND Panel,"'?TXT-529,1'"`<br>Gets the button 'OFF state' text information.<br>The result sent to the Master would be:<br>ButtonGet Id = 529 Type = 1001<br>Flag = 0<br>VALUE1 = 1<br>VALUE2 = 14<br>VALUE3 = 1<br>TEXT = This is a test<br>TEXT LENGTH = 14 |

| Button Query Commands (Cont.) | |
|---|---|
| **?WIF**<br>Get the wireless network information. | Returned in Custom event.<br>Text=<WAP MAC address>,<SSID>,<Channel #>,<Signal Level Value> |

## Panel Runtime Operations

Serial Commands are used in the AxcessX Terminal Emulator mode. These commands are case insensitive.

| Panel Runtime Operation Commands | |
|---|---|
| **ABEEP**<br>Output a single beep even if beep is Off. | Syntax:<br>`"'ABEEP'"`<br>Example:<br>`SEND COMMAND Panel,"'ABEEP'"`<br>Outputs a beep of duration 1 beep even if beep is Off. |
| **ADBEEP**<br>Output a double beep even if beep is Off. | Syntax:<br>`"'ADBEEP'"`<br>Example:<br>`SEND COMMAND Panel,"'ADBEEP'"`<br>Outputs a double beep even if beep is Off. |
| **@AKB**<br>Pop up the keyboard icon and initialize the text string to that specified. | Keyboard string is set to null on power up and is stored until power is lost. The Prompt Text is optional.<br>Syntax:<br>`"'@AKB-<initial text>;<prompt text>'"`<br>Variables:<br>`initial text = 1 - 50 ASCII characters.`<br>`prompt text = 1 - 50 ASCII characters.`<br>Example:<br>`SEND COMMAND Panel,"'@AKB-Texas;Enter State'"`<br>Pops up the Keyboard and initializes the text string 'Texas' with prompt text 'Enter State'. |
| **AKEYB**<br>Pop up the keyboard icon and initialize the text string to that specified. | Keyboard string is set to null on power up and is stored until power is lost.<br>Syntax:<br>`"'AKEYB-<initial text>'"`<br>Variables:<br>`initial text = 1 - 50 ASCII characters.`<br>Example:<br>`SEND COMMAND Panel,"'AKEYB-This is a Test'"`<br>Pops up the Keyboard and initializes the text string 'This is a Test'. |
| **AKEYP**<br>Pop up the keypad icon and initialize the text string to that specified. | The keypad string is set to null on power up and is stored until power is lost.<br>Syntax:<br>`"'AKEYP-<number string>'"`<br>Variables:<br>`number string = 0 - 9999.`<br>Example:<br>`SEND COMMAND Panel,"'AKEP-12345'"`<br>Pops up the Keypad and initializes the text string '12345'. |
| **AKEYR**<br>Remove the Keyboard/ Keypad. | Remove keyboard or keypad that was displayed using 'AKEYB', 'AKEYP', 'PKEYP', @AKB, @AKP, @PKP, @EKP, or @TKP commands.<br>Syntax:<br>`"'AKEYR'"`<br>Example:<br>`SEND COMMAND Panel,"'AKEYR'"`<br>Removes the Keyboard/Keypad. |

| Panel Runtime Operation Commands (Cont.) | |
|---|---|
| **@AKP**<br>Pop up the keypad icon and initialize the text string to that specified. | Keypad string is set to null on power up and is stored until power is lost. The Prompt Text is optional.<br>Syntax:<br>`"'@AKP-<initial text>;<prompt text>'"`<br>Variables:<br>`initial text = 1 - 50 ASCII characters.`<br>`prompt text = 1 - 50 ASCII characters.`<br>Example:<br>`SEND COMMAND Panel,"'@AKP-12345678;ENTER PASSWORD'"`<br>Pops up the Keypad and initializes the text string '12345678' with prompt text 'ENTER PASSWORD'. |
| **@AKR**<br>Remove the Keyboard/ Keypad. | Remove keyboard or keypad that was displayed using 'AKEYB', 'AKEYP', 'PKEYP', @AKB, @AKP, @PKP, @EKP, or @TKP commands.<br>Syntax:<br>`"'@AKR'"`<br>Example:<br>`SEND COMMAND Panel,"'@AKR'"`<br>Removes the Keyboard/Keypad. |
| **BEEP**<br>Output a beep. | Syntax:<br>`"'BEEP'"`<br>Example:<br>`SEND COMMAND Panel,"'BEEP'"`<br>Outputs a beep. |
| **BRIT**<br>Set the panel brightness. | Syntax:<br>`"'BRIT-<brightness level>'"`<br>Variable:<br>brightness level = 0 - 100.<br>Example:<br>`SEND COMMAND Panel,"'BRIT-50'"`<br>Sets the brightness level to 50. |
| **@BRT**<br>Set the panel brightness. | Syntax:<br>`"'@BRT-<brightness level>'"`<br>Variable:<br>brightness level = 0 - 100.<br>Example:<br>`SEND COMMAND Panel,"'@BRT-70'"`<br>Sets the brightness level to 70. |
| **DBEEP**<br>Output a double beep. | Syntax:<br>`"'DBEEP'"`<br>Example:<br>`SEND COMMAND Panel,"'DBEEP'"`<br>Outputs a double beep. |
| **@EKP**<br>Extend the Keypad. | Pops up the keypad icon and initializes the text string to that specified. The Prompt Text is optional.<br>Syntax:<br>`"'@EKP-<initial text>;<prompt text>'"`<br>Variables:<br>`initial text = 1 - 50 ASCII characters.`<br>`prompt text = 1 - 50 ASCII characters.`<br>Example:<br>`SEND COMMAND Panel,"'@EKP-33333333;Enter Password'"`<br>Pops up the Keypad and initializes the text string '33333333' with prompt text 'Enter Password'. |

| Panel Runtime Operation Commands (Cont.) | |
|---|---|
| **PKEYP**<br>Present a private keypad. | Pops up the keypad icon and initializes the text string to that specified. Keypad displays a '*' instead of the numbers typed. The Prompt Text is optional.<br>Syntax:<br>`"'PKEYP-<initial text>'"`<br>Variables:<br>`initial text = 1 - 50 ASCII characters.`<br>Example:<br>`SEND COMMAND Panel,"'PKEYP-123456789'"`<br>Pops up the Keypad and initializes the text string '123456789' in '*'. |
| **@PKP**<br>Present a private keypad. | Pops up the keypad icon and initializes the text string to that specified. Keypad displays a '*' instead of the numbers typed. The Prompt Text is optional.<br>Syntax:<br>`"'@PKP-<initial text>;<prompt text>'"`<br>Variables:<br>`initial text = 1 - 50 ASCII characters.`<br>`prompt text = 1 - 50 ASCII characters.`<br>Example:<br>`SEND COMMAND Panel,"'@PKP-1234567;ENTER PASSWORD'"`<br>Pops up the Keypad and initializes the text string 'ENTER PASSWORD' in '*'. |
| **SETUP**<br>Send panel to SETUP page. | Syntax:<br>`"'SETUP'"`<br>Example:<br>`SEND COMMAND Panel,"'SETUP'"`<br>Sends the panel to the Setup Page. |
| **SHUTDOWN**<br>Shut down the batteries providing power to the panel. | Syntax:<br>`"'SHUTDOWN'"`<br>Example:<br>`SEND COMMAND Panel,"'SHUTDOWN'"`<br>Shuts-down the batteries feeding power to the panel. This function saves the battery from discharging. |
| **SLEEP**<br>Force the panel into screen saver mode. | Syntax:<br>`"'SLEEP'"`<br>Example:<br>`SEND COMMAND Panel,"'SLEEP'"`<br>Forces the panel into screen saver mode. |
| **@SOU**<br>Play a sound file. | Syntax:<br>`"'@SOU-<sound name>'"`<br>Variables:<br>`sound name = Name of the sound file. Supported sound file formats are: WAV & MP3.`<br>Example:<br>`SEND COMMAND Panel,"'@SOU-Music.wav'"`<br>Plays the 'Music.wav' file. |

| Panel Runtime Operation Commands (Cont.) | |
|---|---|
| **@TKP**<br>Present a telephone keypad. | Pops up the keypad icon and initializes the text string to that specified. The Prompt Text is optional.<br>Syntax:<br>`"'@TKP-<initial text>;<prompt text>'"`<br>Variables:<br>`initial text = 1 - 50 ASCII characters.`<br>`prompt text = 1 - 50 ASCII characters.`<br>Example:<br>`SEND COMMAND Panel,"'@TKP-999.222.1211;Enter Phone Number'"`<br>Pops-up the Keypad and initializes the text string '999.222.1211' with prompt text 'Enter Phone Number'. |
| **TPAGEON**<br>Turn On page tracking. | This command turns On page tracking, whereby when the page or popups change, a string is sent to the Master. This string may be captured with a CREATE_BUFFER command for one panel and sent directly to another panel.<br>Syntax:<br>`"'TPAGEON'"`<br>Example:<br>`SEND COMMAND Panel,"'TPAGEON'"`<br>Turns On page tracking. |
| **TPAGEOFF**<br>Turn Off page tracking. | Syntax:<br>`"'TPAGEOFF'"`<br>Example:<br>`SEND COMMAND Panel,"'TPAGEOFF'"`<br>Turns Off page tracking. |
| **@VKB**<br>Popup the virtual keyboard. | Syntax:<br>`"'@VKB'"`<br>Example:<br>`SEND COMMAND Panel,"'@VKB'"`<br>Pops-up the virtual keyboard. |
| **WAKE**<br>Force the panel out of screen saver mode. | Syntax:<br>`"'WAKE'"`<br>Example:<br>`SEND COMMAND Panel,"'WAKE'"`<br>Forces the panel out of the screen saver mode. |

# Input Commands

These Send Commands are case insensitive.

| Input Commands | |
|---|---|
| **^CAL**<br>Put panel in calibration mode. | Syntax:<br>`"'^CAL'"`<br>Example:<br>`SEND COMMAND Panel,"'^CAL'"`<br>Puts the panel in calibration mode. |
| **^KPS**<br>Set the keyboard passthru. | Syntax:<br>`"'^KPS-<pass data>'"`<br>Variable:<br>**pass data**:<br><blank/empty> = Disables the keyboard.<br>0 = Pass data to G4 application (default). This can be used with VPC or text areas.<br>1 - 4 = Not used.<br>5 = Sends out data to the Master.<br>Example:<br>`SEND COMMAND Panel,"'^KPS-5'"`<br>Sets the keyboard passthru to the Master. Option 5 sends keystrokes directly to the Master via the Send Output String mechanism. This process sends a virtual keystroke command (^VKS) to the Master.<br>Example 2:<br>`SEND COMMAND Panel,"'^KPS-0'"`<br>Disables the keyboard passthru to the Master.<br>The following point defines how the parameters within this command work:<br>• Accepts keystrokes from any of these sources: attached USB keyboard or Virtual keyboard. |
| **^VKS**<br>Send one or more virtual key strokes to the G4 application. | Key presses and key releases are not distinguished except in the case of CTRL, ALT, and SHIFT.<br>**Refer to theEmbedded Codes table on page 144** that define special characters which can be included with the string but may not be represented by the ASCII character set.<br>Syntax:<br>`"'^VKS-<string>'"`<br>Variable:<br>string = Only 1 string per command/only one stroke per command.<br>Example:<br>`SEND COMMAND Panel,"'^VKS-'8"`<br>Sends out the keystroke 'backspace' to the G4 application. |

## Embedded codes

The following is a list of G4 compatible embedded codes:

| Embedded Codes | | |
|---|---|---|
| Decimal numbers | Hexidecimal values | Virtual keystroke |
| 8 | ($08) | Backspace |
| 13 | ($0D) | Enter |
| 27 | ($1B) | ESC |
| 128 | ($80) | CTRL key down |
| 129 | ($81) | ALT key down |
| 130 | ($82) | Shift key down |
| 131 | ($83) | F1 |
| 132 | ($84) | F2 |
| 133 | ($85) | F3 |
| 134 | ($86) | F4 |
| 135 | ($87) | F5 |
| 136 | ($88) | F6 |
| 137 | ($89) | F7 |
| 138 | ($8A) | F8 |
| 139 | ($8B) | F9 |
| 140 | ($8C) | F10 |
| 141 | ($8D) | F11 |
| 142 | ($8E) | F12 |
| 143 | ($8F) | Num Lock |
| 144 | ($90) | Caps Lock |
| 145 | ($91) | Insert |
| 146 | ($92) | Delete |
| 147 | ($93) | Home |
| 148 | ($94) | End |
| 149 | ($95) | Page Up |
| 150 | ($96) | Page Down |
| 151 | ($97) | Scroll Lock |
| 152 | ($98) | Pause |
| 153 | ($99) | Break |
| 154 | ($9A) | Print Screen |
| 155 | ($9B) | SYSRQ |
| 156 | ($9C) | Tab |
| 157 | ($9D) | Windows |
| 158 | ($9E) | Menu |
| 159 | ($9F) | Up Arrow |
| 160 | ($A0) | Down Arrow |
| 161 | ($A1) | Left Arrow |
| 162 | ($A2) | Right Arrow |
| 192 | ($C0) | CTRL key up |
| 193 | ($C1) | ALT key up |
| 194 | ($C2) | Shift key up |

## Panel Setup Commands

These commands are case insensitive.

| Panel Setup Commands | |
|---|---|
| **^MUT**<br>Set the panel mute state. | Syntax:<br>`"'^MUT-<mute state>'"`<br>Variable:<br>mute state= 0 = Mute Off and 1 = Mute On.<br>Example:<br>`SEND_COMMAND Panel,"'^MUT-1'"`<br>Sets the panel's master volume to mute. |
| **@PWD**<br>Set the page flip password. | @PWD sets the level 1 password only.<br>Syntax:<br>`"'@PWD-<page flip password>'"`<br>Variables:<br>`page flip password = 1 - 50 ASCII characters.`<br>Example:<br>`SEND COMMAND Panel,"'@PWD-Main'"`<br>Sets the page flip password to 'Main'. |
| **^PWD**<br>Set the page flip password. | Password level is required and must be 1 - 4.<br>Syntax:<br>`"'^PWD-<password level>,<page flip password>'"`<br>Variables:<br>`password level = 1 - 4.`<br>page flip password = 1 - 50 ASCII characters.<br>Example:<br>`SEND COMMAND Panel,"'^PWD-1,Main'"`<br>Sets the page flip password on Password Level 1 to 'Main'. |
| **^VOL**<br>Set the panel volume. | Syntax:<br>`"'^VOL-<volume level>'"`<br>Variable:<br>volume level = 0 - 100. ***100 is maximum volume setting.***<br>Example:<br>`SEND_COMMAND Panel,"'^VOL-50'"`<br>Set the panel volume to 50. |

## Dynamic Image Commands

The following table describes Dynamic Image Commands.

| Dynamic Image Commands | |
|---|---|
| **^BBR**<br>Set the bitmap of a button to use a particular resource. | Syntax:<br>`"'^BBR-<vt addr range>,<button states range>,<resource name>'"`<br>Variable:<br>variable text address range = 1 - 4000.<br>button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).<br>resource name = 1 - 50 ASCII characters.<br>Example:<br>`SEND_COMMAND Panel,"'^BBR-700,1,Sports_Image'"`<br>Sets the resource name of the button to 'Sports_Image'. |
| **^RAF**<br>Add new resources. | Adds any and all resource parameters by sending embedded codes and data.<br>Since the embedded codes are preceded by a '%' character, any '%' character contained in the URL must be escaped with a second '%' character (see example).<br>The file name field (indicated by a **%F** embedded code) may contain special escape sequences as shown in the *^RAF, ^RMF - Embedded Codes* table below.<br>Syntax:<br>`"'^RAF-<resource name>,<data>'"`<br>Variables:<br>• resource name = 1 - 50 ASCII characters.<br>• data = Refers to the embedded codes, see the *^RAF, ^RMF - Embedded Codes* section on page 147.<br>Example:<br>`SEND_COMMAND Panel,"'^RAF-New Image,%P0%HAMX.COM%ALab/Test%%5Ffile%Ftest.jpg'"`<br>Adds a new resource.<br>• The resource name is 'New Image'<br>• %P (protocol) is an HTTP<br>• %H (host name) is ***AMX.COM***<br>• %A (file path) is ***Lab/Test_file***<br>• %F (file name) is ***test.jpg***.<br>Note that the **%%5F** in the file path is actually encoded as **%5F**. |
| **^RFR**<br>Force a refresh for a given resource. | Syntax:<br>`"'^RFR-<resource name>'"`<br>Variable:<br>resource name = 1 - 50 ASCII characters.<br>Example:<br>`SEND_COMMAND Panel,"'^RFR-Sports_Image'"`<br>Forces a refresh on 'Sports_Image'. |

| Dynamic Image Commands (Cont.) | |
|---|---|
| **^RMF**<br>Modify an existing resource. | Modifies any and all resource parameters by sending embedded codes and data.<br>Since the embedded codes are preceded by a '%' character, any '%' character contained in the URL must be escaped with a second '%' character (see example).<br>The file name field (indicated by a **%F** embedded code) may contain special escape sequences as shown in the *^RAF, ^RMF - Embedded Codes* section on page 147.<br>Syntax:<br>`"'^RMF-<resource name>,<data>'"`<br>Variables:<br>• resource name = 1 - 50 ASCII characters<br>• data = Refers to the embedded codes, see the *^RAF, ^RMF - Embedded Codes* section on page 147.<br>Example:<br>`SEND_COMMAND Panel,"'^RMF-Sports_Image,%ALab%%5FTest/Images%Ftest.jpg'"`<br>Changes the resource 'Sports_Image' file name to 'test.jpg' and the path to 'Lab_Test/Images'.<br>Note that the **%%5F** in the file path is actually encoded as **%5F**. |
| **^RSR**<br>Change the refresh rate for a given resource. | Syntax:<br>`"'^RSR-<resource name>,<refresh rate>'"`<br>Variable:<br>resource name = 1 - 50 ASCII characters.<br>refresh rate = Measured in seconds.<br>Example:<br>`SEND_COMMAND Panel,"'^RSR-Sports_Image,5'"`<br>Sets the refresh rate to 5 seconds for the given resource ('Sports_Image'). |

## ^RAF, ^RMF - Embedded Codes

The ^RAF and ^RMF commands add and modify any and all resource parameters by sending embedded codes and data:

```
"'^RAF-<resource name>,<data>'"
"'^RMF-<resource name>,<data>'"
```

The <data> variable uses the embedded codes described in the following table:

| ^RAF, ^RMF - Embedded Codes | | |
|---|---|---|
| Parameter | Embedded Code | Description |
| protocol | '%P <0-1>' | Set protocol. HTTP (0) or FTP (1). |
| user | '%U <user>' | Set Username for authentication. |
| password | '%S <password>' | Set Password for authentication. |
| host | '%H <host>' | Set Host Name (fully qualified DNS or IP Address). |
| file | '%F <file>' | Full path to the location of the file or program that will return the resource. The path must be a valid HTTP URL minus the protocol and host.<br>The only exception to this is the inclusion of special escape sequences and in the case of FTP protocol, regular expressions. |
| path | '%A <path>' | Set Directory path. The path must be a valid HTTP URL minus the protocol, host and filename.<br>The only exception to this is the inclusion of special escape sequences and in the case of FTP protocol, regular expressions. |
| refresh | '%R <refresh 1-65535>' | The number of seconds between refreshes in which the resource is downloaded again. Refreshing a resource causes the button displaying that resource to refresh also.<br>The default value is 0 (only download the resource once). |

| ^RAF, ^RMF - Embedded Codes (Cont.) | | |
|---|---|---|
| Parameter | Embedded Code | Description |
| newest | '%N <0-1>' | Set the newest file. A value of 1 means that only the most recent file matching the pattern is downloaded.<br>***Note**: The 'newest file' option only applies to FTP Dynamic Images, and only those that have pattern matching as part of their filename. Neither 'newest file' nor pattern matching apply to HTTP Dynamic Images.*<br>*When set, the panel will first pull a list of files matching the given pattern from the specified FTP server and path. The timestamps of the items in the list will be compared, with the newest one being displayed on the panel. This is useful for source devices that place a uniquely named still image in a folder at constant intervals, allowing the panel always to display the most recent one.* |
| preserve | '%V <0-1>' | Set the value of the preserve flag.<br>Default is 0. Currently preserve has no function. |

## Escape Sequences

The ^RAF and ^RMF commands support the replacement of any special escape sequences in the filename (specified by the **%F** embedded code) with the corresponding data obtained from the system as outlined in the table below:

| Escape Sequences | |
|---|---|
| Sequence | Panel Information |
| **$DV** | Device Number |
| **$SY** | System Number |
| **$IP** | IP Address |
| **$HN** | Host Name |
| **$MC** | Mac Address |
| **$ID** | Neuron ID (*Only supported on panels that use ICSNet; ignored on all other panels*) |
| **$PX** | X resolution of current panel mode/file |
| **$PY** | Y resolution of current panel mode/file |
| **$ST** | Current state |
| **$AC** | Address code |
| **$AP** | Address port |
| **$CC** | Channel code |
| **$CP** | Channel port |
| **$LC** | Level code |
| **$LP** | Level port |
| **$BX** | X Resolution of Current button |
| **$BY** | Y Resolution of Current button |
| **$BN** | Name of Button |

For instance, **http://www.amx.com/img.asp?device=$DV**

would become

http://www.amx.com/img.asp?device=10001.

## Intercom Commands

The following is a list of Intercom Commands:

| Intercom Commands | |
|---|---|
| **^MODEL?**<br>Sets model name. | Panel model name. If the panel supports intercom hardware it will respond with its model name as shown in the response below. Older hardware or newer hardware that has intercom support disabled with not respond to this command.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'^MODEL?'"`<br>Variables:<br>None.<br>Example:<br>`SEND_COMMAND TP1,"'^MODEL?'"`<br>Panel response string if intercom enabled:<br>`^MODEL-MVP-8400i` |
| **^ICS-**<br>Intercom start. | ^ICS-<IP>,<TX UDP port>,<RX UDP port>,<initial mode>'"<br>Intercom start. Starts a call to the specified IP address and ports, where initial mode is either 1 (talk) or 0 (listen) or 2 (both). If no mode is specified 0 (listen) is assumed. Please note, however, that no data packets will actually flow until the intercom modify command is sent to the panel.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'^ICS-<IP>,<TX UDP port>,<RX UDP port>,<initial mode>'"`<br>Variables:<br>IP = IP Address of panel to connect with on an Intercom call.<br>TX UDP port = UDP port to transmit to.<br>RX UDP port = UDP port to receive from.<br>initial mode = 0 (listen) or 1 (talk) or 2 (handsfree). 0 is the default.<br>Examples:<br>Example of setting up a handsfree unicast call between two panels:<br>`send_command TP1, "^ICS-192.168.0.3,9000,9002,2"`<br>`send_command TP2, "^ICS-192.168.0.4,9002,9000,2"`<br>Example of setting up a multicast call where the first panel is paging two other panels:<br>`send_command TP1, "^ICS-239.252.1.1,9002,9000,1"`<br>`send_command TP2, "^ICS-239.252.1.1,9002,9000,0"`<br>`send_command TP3, "^ICS-239.252.1.1,9002,9000,0"`<br>Example of setting up a baby monitor call where the first panel is listening to the microphone audio coming from the second panel:<br>`send_command TP1, "^ICS-192.168.0.3,9000,9002,0"`<br>`send_command TP2, "^ICS-192.168.0.4,9002,9000,1"` |
| **^ICE'**<br>Intercom end. | Intercom end. This terminates an intercom call/connection.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'^ICE'"`<br>Variables:<br>None<br>Example:<br>`SEND_COMMAND TP1,"'^ICE'"`<br>`SEND_COMMAND TP2,"'^ICE'"`<br>Terminates an intercom call between two panels. |

| Intercom Commands (Cont.) | |
|---|---|
| **^ICM-TALK**<br>**^ICM-LISTEN**<br>Intercom modify command. | Intercom modify command. For backwards compatibility both versions are supported.<br>In this release, however, the TALK and LISTEN subcommands are ignored. The microphone and/or speaker are activated based on the initial mode value of the intercom start command and the audio data packet flow is started upon receipt of this command by the panel.<br>Syntax:<br>SEND_COMMAND <DEV>,'"^ICM-TALK"'<br>Variables:<br>None.<br>Example:<br>SEND_COMMAND TP1,'"^ICM-TALK"' |
| **^ICM-MUTEMIC**<br>Set the state of the microphone on a panel to muted (1) or unmuted (0). At the start of each call the microphone starts out unmuted. | Syntax:<br>`"'^ICM-MUTEMIC,<state>'"`<br>Variables:<br>0 - unmuted<br>1 - muted<br>Example:<br>`SEND_COMMAND Panel, "^ICM-MUTEMIC,1"`<br>Sets the microphone to muted. |

## SIP Commands

The following table lists and describes SIP commands that are generated from the touch panel.

| SIP Commands | |
|---|---|
| **^PHN-AUTOANSWER**<br>Provides the state of the auto-answer feature. | Syntax:<br>`"'^PHN-AUTOANSWER, <state>'"`<br>Variable:<br>state = 0 or 1 (off or on)<br>Example:<br>`SEND_COMMAND Panel,"'^PHN-AUTOANSWER, 1'"` |
| **^PHN-CALL**<br>Provides call progress notification for a call. | Syntax:<br>`"'^PHN-CALL, <status>, <connection id>'"`<br>Variable:<br>status = CONNECTED, DISCONNECTED, TRYING, RINGING, or HOLD.<br>connection id = The identifying number of the connection.<br>Example:<br>`SEND_COMMAND Panel"'^PHN-CALL, CONNECTED, 1'"`<br>Notifies that the call is connected. |
| **^PHN-INCOMING**<br>Provides incoming call notification. | Provides incoming call notification and the connection id used for all future commands related to this call. The connection id will be 0 or 1.<br>Syntax:<br>`"'^PHN-INCOMING, <caller number>, <caller name>, <connection id>, <timestamp>, '"`<br>Variable:<br>caller number = The phone number of the incoming call.<br>caller name = The name associated with the caller number.<br>connection id = The identifying number of the connection.<br>timestamp = The current time in MM/DD/YY HH:MM:SS format.<br>Example:<br>`SEND_COMMAND Panel,"'^PHN-INCOMING, 2125551000, AMX, 07/22/08 12:00:00, 1'"` |

| SIP Commands (Cont.) | |
|---|---|
| **^PHN-LINESTATE**<br>Indicates the current state of each of the available connections used to manage calls. | Syntax:<br>"'^PHN-LINESTATE, <connection id>, <state>, <connection id>, <state>,...'"<br>Variable:<br>connection id = The identifying number of the connection.<br>state = IDLE, HOLD, or CONNECTED<br>extn = The local extension of this panel (see Example)<br>Example:<br>SEND_COMMAND Panel,"'^PHN-LINESTATE, 1, IDLE, 2, CONNECTED, SIP, <extn>'" |
| **^PHN-MSGWAITING**<br>Indicates the number of messages waiting the user's voice mail box. | Syntax:<br>"'^PHN-MSGWAITING, <messages>, <new message count>, <old message count>, <new urgent message count>, <old urgent message count>'"<br>Variable:<br>messages = 0 or 1 (1 indicates new messages)<br>new message count = The number of new messages.<br>old message count = The number of old messages.<br>new urgent message count = The number of new messages marked urgent.<br>old urgent message count = The number of old messages marked urgent.<br>Example:<br>SEND_COMMAND Panel,"'^PHN-MSGWAITING, 1, 1, 2, 1, 0’" |
| **^PHN-PRIVACY**<br>Indicates the state of the privacy feature. | Syntax:<br>"'^PHN-PRIVACY, <state>'"<br>Variable:<br>state = 0 (Disable) or 1 (Enable)<br>new message count = The number of new messages.<br>old message count = The number of old messages.<br>new urgent message count = The number of new messages marked urgent.<br>old urgent message count = The number of old messages marked urgent.<br>Example:<br>SEND_COMMAND Panel,"'^PHN-PRIVACY, 0’" |
| **^PHN-REDIAL**<br>Indicates the panel is redialing the number. | Syntax:<br>"'^PHN-REDIAL, <number>'"<br>Variable:<br>number = The phone number to dial.<br>Example:<br>SEND_COMMAND Panel,"'^PHN-REDIAL, 2125551000’" |
| **^PHN-TRANSFERRED**<br>Indicates a call has been transferred. | Syntax:<br>"'^PHN-TRANSFERRED'"<br>Example:<br>SEND_COMMAND Panel,"'^PHN-TRANSFERRED’" |

The following table lists and describes SIP commands that are sent to the touch panel to manage calls.

| SIP Commands | |
|---|---|
| **^PHN-ANSWER**<br>Answers the call. | Syntax:<br>"'^PHN-ANSWER, <connection id>'"<br>Variable:<br>connection id = The identifying number of the connection<br>Example:<br>SEND_COMMAND Panel,"'^PHN-ANSWER, 1'" |

| SIP Commands (Cont.) | |
|---|---|
| **^PHN-AUTOANSWER**<br>Enables or disables the auto-answer feature of the phone. | Enables (1) or disables (0) the auto-answer feature on the phone.<br>Syntax:<br>`"'^PHN-AUTOANSWER, <state>'"`<br>Variable:<br>state = 0 (Disable) or 1 (Enable)<br>Example:<br>`SEND_COMMAND Panel,"'^PHN-AUTOANSWER, 1'"`<br>Enables the auto-answer feature. |
| **?PHN-AUTOANSWER**<br>Queries the state of the auto-answer feature. | The panel responds with the ^PHN-AUTOANSWER, <state> message.<br>Syntax:<br>`"'?PHN-AUTOANSWER'"`<br>Example:<br>`SEND_COMMAND Panel,"'?PHN-AUTOANSWER'"` |
| **^PHN-CALL**<br>Calls the provided number. | Syntax:<br>`"'^PHN-CALL, <number>'"`<br>Variable:<br>number = The provided phone number<br>Example:<br>`SEND_COMMAND Panel,"'^PHN-CALL, 2125551000'"` |
| **^PHN-DTMF**<br>Sends DTMF codes. | Syntax:<br>`"'^PHN-DTMF, <DTMF code>'"`<br>Variable:<br>DTMF code = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, POUND, or ASTERISK.<br>Example:<br>`SEND_COMMAND Panel,"'^PHN-DTMF, 1234567879ASTERISK'"` |
| **^PHN-HANGUP**<br>Hangs up the call. | Syntax:<br>`"'^PHN-HANGUP, <connection id>'"`<br>Variable:<br>connection id = The identifying number of the connection<br>Example:<br>`SEND_COMMAND Panel,"'^PHN-HANGUP, 1'"` |
| **^PHN-HOLD**<br>Places the call on hold. | Syntax:<br>`"'^PHN-HOLD, <connection id>'"`<br>Variable:<br>connection id = The identifying number of the connection<br>Example:<br>`SEND_COMMAND Panel,"'^PHN-HOLD, 1'"` |
| **?PHN-LINESTATE**<br>Queries the state of each of the connections used by the SIP device. | The panel responds with the ^PHN-LINESTATE message.<br>Syntax:<br>`"'?PHN-LINESTATE'"`<br>Example:<br>`SEND_COMMAND Panel,"'?PHN-LINESTATE'"` |
| **^PHN-PRIVACY**<br>Enables or disables the privacy feature of the phone. | Enables or disables the privacy feature on the phone (do not disturb).<br>Syntax:<br>`"'^PHN-PRIVACY, <state>'"`<br>Variable:<br>state = 0 (Disable) or 1 (Enable)<br>Example:<br>`SEND_COMMAND Panel,"'^PHN-PRIVACY, 1'"`<br>Enables the privacy feature. |

| SIP Commands (Cont.) | |
|---|---|
| **?PHN-PRIVACY**<br>Queries the state of the privacy feature. | The panel responds with the ^PHN-PRIVACY, <state> message.<br>Syntax:<br>"'?PHN-PRIVACY'"<br>Example:<br>SEND_COMMAND Panel,"'?PHN-PRIVACY'" |
| **^PHN-REDIAL**<br>Redials the last number. | Syntax:<br>"'^PHN-REDIAL'"<br>Example:<br>SEND_COMMAND Panel,"'^PHN-REDIAL'" |
| **^PHN-TRANSFER**<br>Transfers the call to the provided number. | Syntax:<br>"'^PHN-TRANSFER, <connection id>, <number>'"<br>Variable:<br>connection id = The identifying number of the connection<br>number = The number to which you want to transfer the call.<br>Example:<br>SEND_COMMAND Panel,"'^PHN-TRANSFER, 1, 2125551000'" |

The following table lists and describes SIP setup commands. Using any of these commands causes the current user to go offline.

| SIP Setup Commands | |
|---|---|
| **^PHN-SETUP-DOMAIN**<br>Sets the realm for authentication. | Syntax:<br>"'^PHN-SETUP-DOMAIN, <domain>'"<br>Variable:<br>domain = The realm used for authentication<br>Example:<br>SEND_COMMAND Panel,"'^PHN-SETUP-DOMAIN, asterisk'" |
| **^PHN-SETUP-ENABLE**<br>Registers a new user | Once the configuration has been updated, the ENABLE command should be run to re-register the new user.<br>Syntax:<br>"'^PHN-SETUP-ENABLE'" |
| **^PHN-SETUP-PASSWORD**<br>Sets the user password for the proxy server. | Syntax:<br>"'^PHN-SETUP-PASSWORD, <password>'"<br>Variable:<br>password = The password for the user name<br>Example:<br>SEND_COMMAND Panel,"'^PHN-SETUP-PASSWORD, 6003'" |
| **^PHN-SETUP-PORT**<br>Sets the port number for the proxy server. | Syntax:<br>"'^PHN-SETUP-PORT, <port>'"<br>Variable:<br>port = The port for the proxy server<br>Example:<br>SEND_COMMAND Panel,"'^PHN-SETUP-PORT, 5060'" |
| **^PHN-SETUP-PROXYADDR**<br>Sets the IP address for the proxy server. | Syntax:<br>"'^PHN-SETUP-PROXYADDR, <IP>'"<br>Variable:<br>IP = The IP address for the proxy server<br>Example:<br>SEND_COMMAND Panel,"'^PHN-SETUP-PROXYADDR, 192.168.223.111'" |

| SIP Commands (Cont.) | |
|---|---|
| **^PHN-SETUP-STUNADDR**<br>Sets the IP address for the STUN server. | Syntax:<br>"'^PHN-SETUP-STUNADDR, <IP>'"<br>Variable:<br>IP = The IP address for the STUN server<br>Example:<br>SEND_COMMAND Panel,"'^PHN-SETUP-STUNADDR, 192.168.223.111'" |
| **^PHN-SETUP-USERNAME**<br>Sets the user name for authentication with the proxy server. | Syntax:<br>"'^PHN-SETUP-USERNAME, <username>'"<br>Variable:<br>username = The user name (usually the phone extension)<br>Example:<br>SEND_COMMAND Panel,"'^PHN-SETUP-USERNAME, 6003'" |

# Panel Calibration

This section outlines the steps for calibrating the touch panel. *It is recommended that you calibrate the panel both before its initial use and after completing a firmware download.*

Modero panels are factory setup with specific demo touch panel pages. The first splash screen that appears indicates the panel is receiving power, beginning to load firmware, and preparing to display the default touch panel pages. When the panel is ready, the AMX Splash Screen is replaced by the Initial Panel Page (FIG. 87).


**FIG. 87** AMX splash screen and initial Panel Page

## Calibrating the MVP Panels

1. Press and hold the two lower external pushbuttons on both sides of the MVP (FIG. 88) for **6 seconds** to pass-over the Setup page and access the Calibration setup page (FIG. 89).

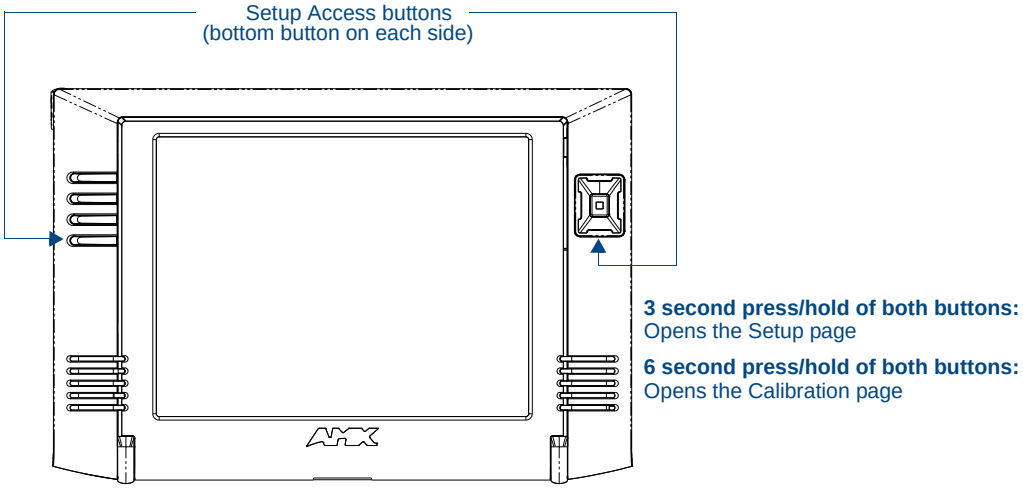



**FIG. 88** Location of Setup Access buttons

2. Using the included stylus, press the crosshairs (on the Calibration page) to set the calibration points on the LCD (FIG. 89).
3. After the "***Calibration Successful.***" message appears, press anywhere on the screen to continue and return to the Setup page.

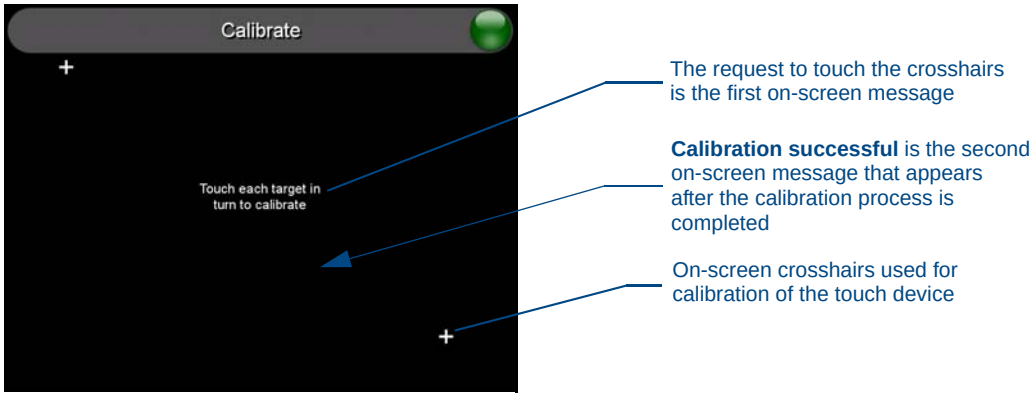



**FIG. 89** Touch Panel Calibration Screens

NOTE

***If the calibration was improperly set and you cannot return to the Calibration page (through the panel's firmware);*** *you can then access this firmware page via G4 WebControl where you can navigate to the Protected Setup page and press the Calibrate button through your VNC window.*
*This action causes the panel to go to the Calibration page seen above, where you can physically recalibrate the actual touch panel again using the above procedures.*

## Testing your Calibration

1. Press and hold down the on-screen **Calibration** button for 6 seconds to enter the Calibration Test page (FIG. 90).

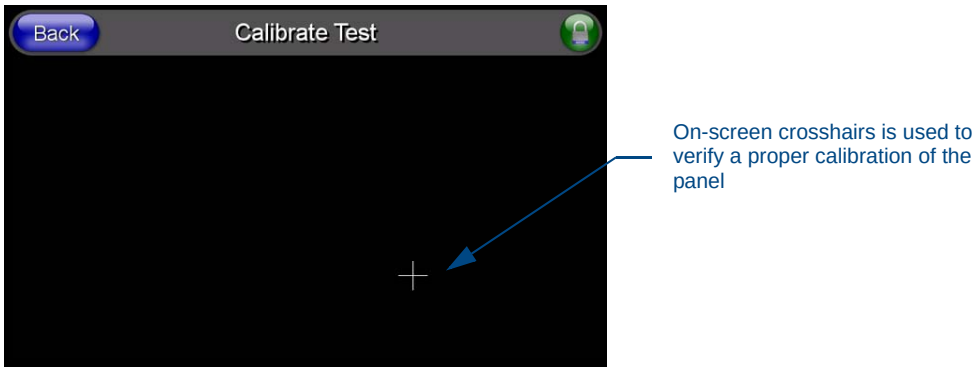



**FIG. 90** Calibration Test page

2. Press anywhere on this page to confirm the on-screen crosshairs match your touch points.
3. If the crosshairs do not appear directly below your LCD touch points, press the **Back** button and recalibrate the panel using the above steps.

Peel the protective plastic film from the LCD.

NOTE

*If the protective plastic film on the LCD is not removed, the panel may not respond properly to touch points on the LCD nor allow proper screen calibration.*

4. Exit this Calibration Test page by pressing the **Back** button to return to the *Protected Setup* page.

## If Calibration Is Not Working

Cycling power to the panel should provide a baseline calibration for the particular touch panel. Re-calibrate the panel.

# Appendix A: Text Formatting

## Text Formatting Codes for Bargraphs/Joysticks

Text formatting codes for bargraphs provide a mechanism to allow a portion of a bargraphs text to be dynamically provided information about the current status of the level (multistate and traditional). These codes are entered into the text field along with any other text.

The following is a code list used for bargraphs:

| Bargraph Text Code Inputs | | |
|---|---|---|
| Code | Bargraph | Multi-State Bargraph |
| $P | Display the current percentage of the bargraph (derived from the Adjusted Level Value as it falls between the Range Values) | Display the current percentage of the bargraph (derived from the Adjusted Level Value as it falls between the Range Values) |
| $V | Raw Level Value | Raw Level Value |
| $L | Range Low Value | Range Low Value |
| $H | Range High Value | Range High Value |
| $S | N/A | Current State |
| $A | Adjusted Level Value (Range Low Value subtracted from the Raw Level Value) | Adjusted Level Value (Range Low Value subtracted from the Raw Level Value) |
| $R | Low Range subtracted from the High Range | Low Range subtracted from the High Range |
| $$ | Dollar sign | Dollar sign |

By changing the text on a button (via a VT command), you can modify the codes on a button. When one of the Text Formatting Codes is encountered by the firmware, it is replaced with the correct value. These values are derived from the following operations:

| Formatting Code Operations | |
|---|---|
| Code | Operation |
| $P | (Current Value - Range Low Value / Range High Value - Range Low Value) x 100 |
| $V | Current Level Value |
| $L | Range Low Value |
| $H | Range High Value |
| $S | Current State (if regular bargraph then resolves to nothing) |
| $A | Current Value - Range Low Value |
| $R | Range High Value - Range Low Value |

Given a current raw level value of 532, a range low value of 500, and a high range value of 600, the following text formatting codes would yield the following strings as shown in the table below:

| Example | |
|---|---|
| Format | Display |
| $P% | 32% |
| $A out of $R | 32 out of 100 |
| $A of 0 - $R | 32 of 0 - 100 |
| $V of $L - $H | 532 of 500 - 600 |

# Text Area Input Masking

Text Area Input Masking may be used to limit the allowed/correct characters that are entered into a text area. For example, in working with a zip code, a user could limit the entry to a max length of only 5 characters; with input masking, this limit could be changed to 5 mandatory numerical digits and 4 optional numerical digits. A possible use for this feature is to enter information into form fields. The purpose of this feature is to:

- Force the use of correct type of characters (i.e. numbers vs. characters)
- Limit the number of characters in a text area
- Suggest proper format with fixed characters
- Right to Left
- Required or Optional
- Change/Force a Case
- Create multiple logical fields
- Specify range of characters/number for each field

With this feature, it is not necessary to:

- Limit the user to a choice of selections
- Handle complex input tasks such as names, days of the week, or month by name
- Perform complex validation such as Subnet Mask validation

## Input mask character types

These character types define what information is allowed to be entered in any specific instance. The following table lists what characters in an input mask will define what characters are allowed in any given position.

**Character Types**

| Character | Masking Rule |
|---|---|
| 0 | Digit (0 to 9, entry required, plus [+] and minus [-] signs not allowed) |
| 9 | Digit or space (entry not required, plus and minus signs not allowed) |
| # | Digit or space (entry not required; plus and minus signs allowed) |
| L | Letter (A to Z, entry required) |
| ? | Letter (A to Z, entry optional) |
| A | Letter or digit (entry required) |
| a | Letter or digit (entry optional) |
| & | Any character or a space (entry required) |
| C | Any character or a space (entry optional) |


*The number of the above characters used determines the length of the input masking box. Example: 0000 requires an entry, requires digits to be used, and allows only 4 characters to be entered/used.*

Refer to the following SEND_COMMANDs for more detailed information:

- `^BIM` - Sets the input mask for the specified addresses. (see the *^BIM* section on page 111).
- `^BMF` subcommand **`%MK`** - sets the input mask of a text area (see the *^BMF* section on page 113).

## Input Mask Ranges

These ranges allow a user to specify the minimum and maximum numeric value for a field. ***Only one range is allowed per field. Using a range implies a numeric entry ONLY.***

| Input Mask Ranges | |
|---|---|
| Character | Meaning |
| [ | Start range |
| ] | End range |
| \| | Range Separator |

An example from the above table:

**[0|255]** This allows a user to enter a value from 0 to 255.

## Input mask next field characters

These characters allow you to specify a list of characters that cause the keyboard to move the focus to the next field when pressed, instead of inserting the text into the text area.

| Input Mask Next Field Char | |
|---|---|
| Character | Meaning |
| { | Start Next Field List |
| } | End Next Field List |

An example from the above table:

**{.} or {:} or {.:}** Proceed to the next text area input box after a user hits any of these keys.

## Input mask operations

Input Mask Operators change the behavior of the field in the following way:

| Input Mask Operators | |
|---|---|
| Character | Meaning |
| < | Forces all characters to be converted to lowercase |
| > | Forces all characters to be converted to uppercase |
| ^ | Sets the overflow flag for this field |

## Input mask literals

To define a literal character, enter any character, other than those shown in the above table *(including spaces, and symbols)*. A back-slash ('\') causes the character that follows it to be displayed as the literal character. For example, **\A** is displayed just as the letter **A**. To define one of the following characters as a literal character, precede that character with a back-slash. Text entry operation using Input Masks.

A keyboard entry using normal text entry is straightforward. However, once an input mask is applied, the behavior of the keyboard needs to change to accommodate the input mask's requirement. When working with masks, any literal characters in the mask will be "skipped" by any cursor movement, including cursor, backspace, and delete keys.

When operating with a mask, the mask should be displayed with placeholders. The "-" character should display where you should enter a character. The arrow keys will move between the "-" characters and allow you to replace them. The text entry code operates as if it is in the overwrite mode. If the cursor is positioned on a character already entered and you type in a new (and valid) character, the new character replaces the old character. There is no shifting of characters.

When working with ranges specified by the [] mask, the keyboard allows you to enter a number between the values listed in the ranges. If a user enters a value that is larger than the maximum, the maximum number of right-most characters is used to create a new, acceptable value.

- **Example 1**: If you type "125" into a field accepting 0-100, then the values displayed will be "1", "12", "25".
- **Example 2**: If the max for the field was 20, then the values displayed will be "1", "12", "5".

When data overflows from a numerical field, the overflow value is added to the previous field on the chain if the overflow character was specified. In the above example, if the overflow flag was set, the first example will place the "1" into the previous logical field and the second example will place "12" in the previous logical field. If the overflow field already contains a value, the new value will be inserted to the right of the current characters and the overflow field will be

evaluated. Overflow continues to work until a field with no overflow value is set or no more fields remain (i.e. reached first field).

If a character is typed and that character appears in the Next Field list, the keyboard should move the focus to the next field. For example, when entering time, a **":"** is used as a next field character. If you enter "1:2", the 1 is entered in the current field (hours) and then the focus is moved to the next field and 2 is entered in that field.

When entering time in a 12-hour format, entry of AM and PM is required. Instead of adding AM/PM to the input mask specification, the AM/PM should be handled within the NetLinx code. This allows a programmer to show/hide and provide discrete feedback for AM and PM.

### Input mask output examples

The following are some common input masking examples:

| Output Examples | | |
|---|---|---|
| Common Name | Input Mask | Input |
| IP Address Quad | [0\|255]{.} | Any value from 0 to 255 |
| Hour | [1\|12]{:} | Any value from 1 to 12 |
| Minute/Second | [0\|59]{:} | Any value from 0 to 59 |
| Frames | [0\|29]{:} | Any value from 0 to 29 |
| Phone Numbers | (999) 000-0000 | (555) 555-5555 |
| Zip Code | 00000-9999 | 75082-4567 |

## URL Resources

A URL can be broken into several parts. For example, with the URL *http://www.amx.com/company-info-home.asp*, this URL indicates that the protocol in use is **http** (HyperText Transport Protocol) and that the information resides on a host machine named **www.amx.com**. The image on that host machine is given an assignment (*by the program*) name of **company-info-home.asp** *(Active Server Page)*.

The exact meaning of this name on the host machine is both protocol dependent and host dependent. The information normally resides in a file, but it could be generated dynamically. This component of the URL is called the file component, even though the information is not necessarily in a file.

A URL can optionally specify a port, which is the port number to which the TCP/IP connection is made on the remote host machine. If the port is not specified, the default port for the protocol is used instead. For example, the default port for http is *80*. An alternative port could be specified as: *http://www.amx.com:8080/company-info-home.asp*.


*Any legal HTTP syntax can be used.*

### Special Escape Sequences

The system has only a limited knowledge of URL formats, as it transparently passes the URL information onto the server for translation. A user can then pass any parameters to the server side programs such as CGI scripts or active server pages.

However; the system will parse the URL looking for special escape codes. When it finds an escape code, it replaces that code with a particular piece of panel, button, or state information.

For example, "http://www.amx.com/img.asp?device=$DV" would become *http://www.amx.com/img.asp?device=10001*.

Other used escape sequences include:

| Escape Sequences | |
|---|---|
| Sequence | Panel Information |
| $DV | Device Number |
| $SY | System Number |
| $IP | IP Address |
| $HN | Host Name |
| $MC | Mac Address |
| $ID | Neuron ID |
| $PX | X Resolution of current panel mode/file |
| $PY | Y Resolution of current panel mode/file |
| $BX | X Resolution of current button |
| $BY | Y Resolution of current button |
| $BN | Name of button |
| $ST | Current state |
| $AC | Address Code |
| $AP | Address Port |
| $CC | Channel Code |
| $CP | Channel Port |
| $LC | Level Code |
| $LP | Level Port |

# Appendix B - Wireless Technology

## Overview of Wireless Technology

- **802.11b/2.4 GHz and 802.11a/5 GHz** are the two major WLAN standards and both operate using radio frequency (RF) technology. Together the two standards are together called Wi-Fi and operate in frequency bands of 2.4 GHz and 5 GHz respectively.
  The ***802.11b*** specification was the first to be finalized and reach the marketplace. The actual throughput obtained from an 802.11b network will typically be between 4 and 5 Mbps.
  Because of the higher frequency (and thus shorter wavelength) that they use, ***802.11a*** signals have a much tougher time penetrating solid objects like walls, floors, and ceilings. As a result, the price for 802.11a's higher speed is not only a shorter range but also a weaker and less consistent signal.
  ***802.11g*** provides increased bandwidth at 54 Mbps. As part of the IEEE 802.11g specification, when throughput cannot be maintained, this card will automatically switch algorithms in order to maintain the highest spread possible at a given distance. In addition, 802.11g can also step down to utilize 802.11b algorithms and also maintain a connection at longer distances.
- **IP Routing** is a behavior of the wireless routing is largely dependent on the wired network interface. Although the panel can be connected to two networks simultaneously, it may only have one gateway. If the wired network was successfully set up and a gateway was obtained; then the default route for all network traffic will be via the wired network. In the event that the wired network was not configured, then the default route for all network traffic will be via the wireless network. The wired network connection always takes priority.

  *Example*: Imagine a panel connected to the two networks A & B. A is the wired network and B is the wireless network. If the Master controller is on either of these networks, then it will be reached. However if the Master controller is on a different network, C, then the gateway determines which network interface (wired or wireless) will be used.
- **Wireless Access Points (WAPs)** are the cornerstone of any wireless network. A WAP acts as a bridge between a wired and wireless network. It aggregates the traffic from all wireless clients and forwards it down the network to the switch or router. One WAP may be all that is necessary for a standard installation. However, more WAPs may be needed, depending on the size of the installation, its layout, and its construction.
- **Wireless Equivalent Privacy** (**WEP**) Security is a method by which WLANs protect wireless data streams. A data stream encrypted with WEP can still be intercepted or eavesdropped upon, but the encryption makes the data unintelligible to the interloper. The strength of WEP is measured by the length of the key used to encrypt the data. The longer the key, the harder it is to crack.
  802.11b implementations provided 64-bit and 128-bit WEP keys. This is known respectively as 64-bit and 128-bit WEP encryption. 64-bit is generally not regarded as adequate security protection. Both key lengths are supported by the Modero product line.
  Whichever level of WEP used, ***using identical settings is crucial (CASE SENSITIVE)***--the key length, and the key itself-- on all devices. Only devices with common WEP settings will be able to communicate. Similarly,

  If one device has WEP enabled and another does no, they will not be able to talk to each other.
  Although the calculations required to encrypt data with WEP can impact the performance of your wireless network, this impact is generally only seen when running benchmarks, and is not large enough to be noticeable in the course of normal network usage.

# Terminology

## 802.1x

IEEE 802.1x is an IEEE standard that is built on the Internet standard EAP (Extensible Authentication Protocol). 802.1x is a standard for passing EAP messages over either a wired or wireless LAN. Additionally, 802.1x is also responsible for communicating the method with which WAPs and wireless users can share and change encryption keys. This continuous key change helps resolve any major security vulnerabilities native to WEP.

## AES

Short for Advanced Encryption Standard, is a cipher currently approved by the NSA to protect US Government documents classified as Top Secret. The AES cipher is the first cipher protecting Top Secret information available to the general public.

## CERTIFICATES (CA)

A certificate can have many forms, but at the most basic level, a certificate is an identity combined with a public key, and then signed by a certification authority. The certificate authority (CA) is a trusted external third party which "signs" or validates the certificate. When a certificate has been signed, it gains some cryptographic properties. AMX supports the following security certificates within three different formats:

- **PEM** (Privacy Enhanced Mail)
- **DER** (Distinguished Encoding Rules)
- **PKCS12** (Public Key Cryptography Standard #12)

Typical certificate information can include the following items:

- Certificate Issue Date
- Extensions
- Issuer
- Public Key
- Serial Number
- Signature Algorithm
- User
- Version

## MIC

Short for Message Integrity Check, this prevents forged packets from being sent. Through WEP, it was possible to alter a packet whose content was known even if it had not been decrypted.

TKIP

Short for Temporal Key Integration, this is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP provides a per-packet key mixing, message integrity check and re-keying mechanism, thus ensuring that every data packet is sent with its own unique encryption key. Key mixing increases the complexity of decoding the keys by giving the hacker much less data that has been encrypted using any one key.

## WEP

Short for Wired Equivalent Privacy, WEP is a scheme used to secure wireless networks (Wi-Fi). A wireless network broadcasts messages using radio which are particularly susceptible to hacker attacks. WEP was intended to provide the confidentiality and security comparable to that of a traditional wired network. As a result of identified weaknesses in this scheme, WEP was superseded by Wi-Fi Protected Access (WPA), and then by the full IEEE 802.11i standard (also known as WPA2).

## WPA

Wi-Fi Protected Access (WPA and WPA2) is a class of system used to secure wireless (Wi-Fi) computer networks. It was created in response to several serious weaknesses researchers had found in the previous WEP system. WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared (WPA2).

WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points.

To resolve problems with WEP, the Wi-Fi Alliance released WPA (FIG. 91), which integrated **802.1x**, **TKIP** and **MIC**. Within the WPA specifications, the RC4 cipher engine was maintained from WEP. RC4 is widely used in SSL (Secure Socket Layer) to protect internet traffic.

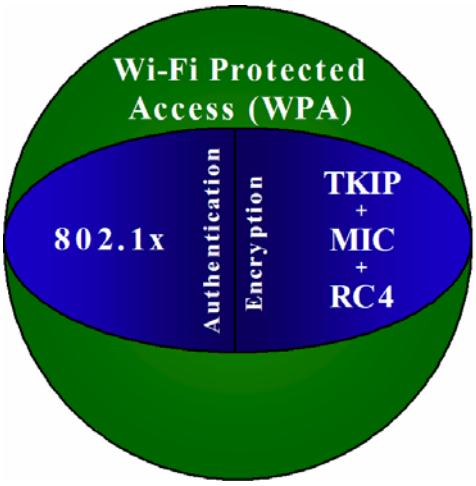



**FIG. 91** WPA Overview

## WPA2

Also know as IEEE 802.11i, this is an amendment to the 802.11 standard specifying security mechanisms for wireless networks. The 802.11i scheme makes use of the Advanced Encryption Standard (AES) block cipher; WEP and WPA use the RC4 stream cipher.

The 802.11i architecture contains the following components: 802.1X for authentication (entailing the use of EAP and an authentication server), RSN for keeping track of associations, and AES-based CCMP to provide confidentiality, integrity and origin authentication.

WPA2 implements the full standard, but will not work with some older network cards. Both provide good security, with two significant issues:

- either WPA or WPA2 must be enabled and chosen in preference to WEP.
- WEP is usually presented as the first security choice in most installation instructions.
- in the "Personal" mode, the most likely choice for homes and small offices, a passphrase is required that, for full security, must be longer than the typical 6 to 8 character passwords users are taught to employ.

With the RC4 released to the general public, the IEEE implemented the Advanced Encryption Standard (AES) as the cipher engine for 802.11i, which the Wi-Fi Alliance has branded as WPA2 (FIG. 92).

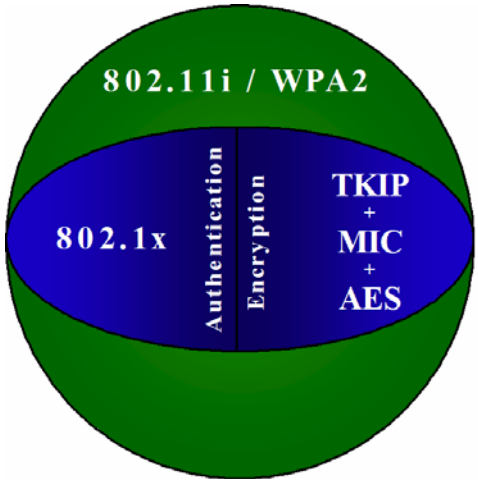



**FIG. 92** WPA2 Overview

# EAP Authentication

**EAP** (Extensible Authentication Protocol) is an Enterprise authentication protocol that can be used in both a wired and wireless network environment. EAP requires the use of an 802.1x Authentication Server, also known as a RADIUS server. Although over 40 different EAP methods are currently defined, the current internal Modero 802.11g wireless card and accompanying firmware only support the following EAP methods (***listed from simplest to most complex***):

- EAP-LEAP (Cisco Light EAP)
- EAP-FAST (Cisco Flexible Authentication via Secure Tunneling, a.k.a. LEAPv2)

The following use certificates:

- EAP-PEAP (Protected EAP)
- EAP-TTLS (Tunneled Transport Layer Security)
- **EAP-TLS** (Transport Layer Security)

EAP requires the use of an 802.1x authentication server (also known as a RADIUS server). Sophisticated Access Points (such as Cisco) can use a built-in RADIUS server. The most common RADIUS servers used in wireless networks today are:

- Microsoft Sever 2003
- Juniper Odyssey (once called Funk Odyssey)
- Meetinghouse AEGIS Server
- DeviceScape RADIUS Server
- Cisco Secure ACS

## EAP Characteristics

The following table outlines the differences among the various EAP Methods from most secure (at the top of the list) to the least secure (at the bottom of the list):

**EAP Method Characteristics**

| Method: | Credential Type: | Authentication: | Pros: | Cons: |
|---|---|---|---|---|
| EAP-TLS | • Certificates | • Certificate is based on a two-way authentication | • Highest Security | • Difficult to deploy |
| EAP-TTLS | • Certificates<br>• Fixed Passwords<br>• One-time passwords (tokens) | • Client authentication is done via password and certificates<br>• Server authentication is done via certificates | • High Security | • Moderately difficult to deploy |
| EAP-PEAP | • Certificates<br>• Fixed Passwords<br>• One-time passwords (tokens) | • Client authentication is done via password and certificates<br>• Server authentication is done via certificates | • High Security | • Moderately difficult to deploy |
| EAP-LEAP | • Certificates<br>• Fixed Passwords<br>• One-time passwords (tokens) | • Authentication is based on MS-CHAP and MS-CHAPv2 authentication protocols | • Easy deployment | • Susceptible to dictionary attacks |
| EAP-FAST | • Certificates<br>• Fixed Passwords<br>• One-time passwords (tokens) | • N/A | • N/A | • N/A |

### EAP Communication Overview

EAP Authentication goes a step beyond just encrypting data transfers, but also requires that a set of credentials be validated before the client (panel) is allowed to connect to the rest of the network (FIG. 93). Below is a description of this process. It is important to note that no user intervention is necessary during this process. It proceeds automatically based on the configuration parameters entered into the panel.

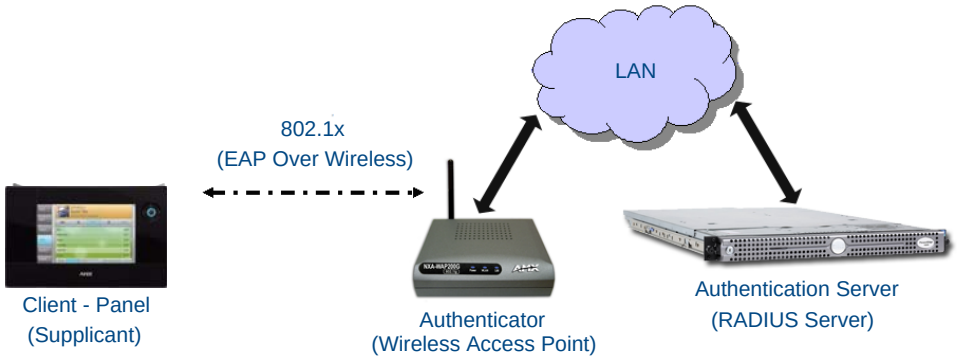



**FIG. 93** EAP security method in process

1. The client (panel) establishes a wireless connection with the WAP specified by the SSID.
2. The WAP opens up a tunnel between itself and the RADIUS server configured via the access point. This tunnel means that packets can flow between the panel and the RADIUS server but nowhere else. ***The network is protected until authentication of the client (panel) is complete and the ID of the client is verified.***
3. The WAP (Authenticator) sends an "EAP-Request/Identity" message to the panel as soon as the wireless connection becomes active.
4. The panel then sends a "EAP-Response/Identity" message through the WAP to the RADIUS server providing its identity and specifying which EAP type it wants to use. If the server does not support the EAP type, then it sends a failure message back to the WAP which will then disconnect the panel. As an example, EAP-FAST is only supported by the Cisco server.
5. If the EAP type is supported, the server then sends a message back to the client (panel) indicating what information it needs. This can be as simple as a username (*Identity*) and password or as complex as multiple CA certificates.
6. The panel then responds with the requested information. If everything matches, and the panel provides the proper credentials, the RADIUS server then sends a success message to the access point instructing it to allow the panel to communicate with other devices on the network. At this point, the WAP completes the process for allowing LAN Access to the panel (possibly a restricted access based on attributes that came back from the RADIUS server).

   As an example, the WAP might switch the panel to a particular VLAN or install a set of farewell rules.

## Configuring Modero Firmware via the USB Port

The MVP-5200i needs to be configured to connect with a PC to transfer firmware via the mini-USB port. To configure the touch panel:

### Step 1: Configure The Panel For a USB Connection Type

1. After completing the installation of the USB driver (for more information, refer to the *Upgrading the Modero Firmware via the USB port* section on page 40), confirm the proper installation of the large Type-A USB connector to the PC's USB port, and restart your computer.
2. After the panel powers up, hold the reset button to display the *Setup* Page (for more information, refer to the *Accessing the Setup and Protected Setup Pages* section on page 19 ) and open the *Protected Setup* page.
3. Press **System Settings** to open the *System Settings* page.
4. Toggle the blue *Type* field in the *Master Connection* section until the choice cycles to **USB**.

NOTE

***ALL** fields are then greyed out and read-only. However, they still display any previous network information.*

5. Press the **Back** button on the touch panel to return to the *Protected Setup* page.

6. Press the **Reboot** button both to save any changes and to **restart the panel.** *Remember that the panel's connection type must be set to **USB** prior to rebooting the panel and prior to inserting the USB connector.*
7. **ONLY AFTER** the unit displays the first panel page should you **THEN** insert the mini-USB connector into the Mini-USB Port on the panel. It may take a minute for the panel to detect the new connection and send a signal to the PC, *indicated by a green System Connection icon*.
   - If a few minutes have gone by and the *System Connection* icon still does not turn green, complete the procedures in the following section to set up the Virtual Master and refresh the System from the Online Tree. This action sends out a request to the panel to respond and completes the communication, turning the *System Connection* icon green.
8. Repeat steps 2 and 3 to return to the *System Settings* page

### Step 2: Prepare NetLinx Studio For Communication Via the USB Port

1. From the **Start** menu in Windows XP, open the *Network Connections* dialog (**Start > Settings > Network Connections > Local Area Connection**).
2. Look for the Local Area Connection reading *Local Area Connection, AMX USB Device Link* and double-click on it to open the Local Status.
3. Press the **Properties** tab to open the *Local Area Connection Properties* section.
4. Press the **Properties** button to open the *TCP/IP Properties* dialog box.
5. Set the IP address to an address within the same subnet as the panel IP address specified within the USB IP settings of the panel. For instance, if the default IP address on the device is **12.0.0.2**, set the IP address to **12.0.0.1**.
6. Set the Subnet Mask to **255.255.255.0**.
7. In the *TCP/IP Properties* dialog box, click **OK**.
8. In the *Local Area Connection Properties*, section, click **Close**.

## AMX Certificate Upload Utility

The Certificate Upload utility gives you the ability to compile a list of target touch panels, select a pre-obtained certificate (uniquely identifying the panel), and then upload that file to the selected panel.


*This application must be run from a local machine and should not be used from a remote network location.*

This application ensures that a unique certificate is securely uploaded to a specific touch panel. Currently, the target panels must be capable of supporting the WPA-PSK and EAP-XXX wireless security formats.

The Certificate Upload utility supports the following capabilities:

- Ability to browse both a local and network drive to find a desired certificate file.
- Ability to create a list of target AMX G4 touch panels based on IP Addresses.
- Ability to display the IP Address of the local computer hosting the application.
- Ability to load a previously created list of target touch panels.
- Ability to save the current list of target Modero panel as a file.
- Ability to track the progress of the certificate upload by noting the current data size being transmitted and any associated error messages (if any).

The Certificate Upload Utility recognizes the following certificate file types:

- **CER** (Certificate File)
- **DER** (Distinguished Encoding Rules)
- **PEM** (Privacy Enhanced Mail)
- **PFX** (Normal Windows generated certificate)
- **PVK** (Private Key file)

## Uploading a Certificate File

1. Install the latest AMX USB LAN LINK driver onto your computer by installing the latest versions of either TPDesign4 or NetLinx Studio2. This USB driver prepares your computer for proper communication with the panel.
   Refer to Step 1 from within the *Upgrading the Docking Station Firmware via USB* section on page 43.
2. Access the target panel's Protected Setup firmware page and configure the USB communication parameters.
3. With the panel successfully communicating with the target computer, launch the Certificate Upload Utility.
   Familiarize yourself with the Certificate Utility User Interface options.
4. Locate your certificate file by using the **Browse** button and navigating to the desired file type.
5. Use the drop-down arrow in the *Local Address* field to select direct communication through the USB port.
6. **S**elect the ***10.XX.XX.1*** IP Address that corresponds to the virtual IP Address assigned to the USB connection port on the computer.
7. **N**avigate to the *Add IP Address* field at the bottom-right of the interface and enter a value of **1** greater than the virtual USB IP Address.
   For example: If the virtual USB IP Address is **10.0.0.1**, then add an address for the directly connected panel of **10.0.0.2**. This is one greater than the USB address value detected by the utility.
   - A certificate may be sent to ONLY ONE directly connected panel via USB.
   - Use the Ethernet port's IP Address to send a server certificate to multiple panel targets.
8. **S**elect the IP Address which corresponds to the local computer's Ethernet address.
9. Navigate to the *Add IP Address* field (bottom-right of the interface) and enter the IP Addresses of the various target touch panels.
10. Click the **Add** button to complete the entry and add the new IP Address to the listing of available device IP Addresses. Repeat this process for all subsequent device IP Addresses.
11. Once the list is complete, click on the **File** drop-down menu and select the **Save** option. This launches a *Save* dialog to assign a name to the current list of addresses and then save the information as a TXT (text) file to a known location.


*This application must be run from a local machine and should not be used from a remote network location.*

12. Select the target devices to be uploaded with the selected certificate. These may be:
    - individually selected by toggling the box next to the *Send* entry (with the Type column).
    - selected as a group by clicking on the *Check All* radio box located at the top of the device IP Address listing.
13. When ready to send the certificate file to the selected panels, click the **Send** button to initiate the upload.

Once the *Status* field for each entry reads **Done**, the upload was successfully completed.

# Appendix C: Troubleshooting

## Overview

This section describes the solutions to possible hardware/firmware issues that could arise during the common operation of a Modero touch panel.

### Panel Doesn't Respond To Touches

***Symptom:*** *The device either does not respond to touches on the touch screen or does not register the touch as being in the correct area of the screen.*

If the screen is off:

- The device may be in Standby Mode. Press and hold the navigation wheel to wake up the panel.
- The device may be in Shutdown Mode. Press and hold the center button on the navigation wheel until the device turns on.
- The device battery may be drained. Place the device into a Table Charging Station or a Wall Charging Station, or connect it to its included power source to recharge the battery.

If the screen is on:

- The protective laminate coating may still be on the LCD. Verify that the coating on the LCD is removed before beginning any calibration process. The protective cover makes calibration difficult because the device cannot calibrate on specific crosshairs when the sheet is pressing on the whole LCD.
- The previous calibration may be off. Reset the device calibration, as explained in the *Calibration Page* section on page 72.

### Battery Will Not Hold Or Take A Charge

***Symptom:*** *The battery will not hold or take a charge and shows no indication of charging, either on the bargraphs or in the Battery Setup page.*

To keep the battery from being damaged from operating at too low a level, the firmware places it into a protected state.

The panel must have the latest firmware. If it doesn't, the firmware can be found at **www.amx.com** *Dealers/Tech Center > Firmware Files.> Modero*.

1. Load the firmware into the panel, using NetLinx Studio.
2. After loading the firmware, power cycle the MVP (this is a complete power cycle, not a Reboot). The panel will now show the current firmware version within the Setup > Panel Information page.
3. Connect the power supply to the panel. You will see 2 warning messages on the display.
   - The first one warns that the battery is low and must be charged.
   - The second warning tells you that the battery is in a protected mode.
4. Wait a few minutes and then check the *Battery Settings* page on the device to see any charging activity on the bar graphs. (For more information, refer to the *Battery Settings/Batteries* section on page 92).

   The "Sensor" device in the Online Tree tab below the MVP panel should show v1.24 or higher after the upgrade, as shown in FIG. 94:

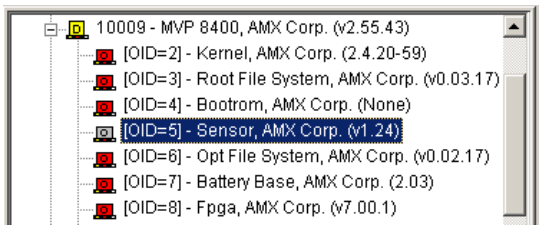



**FIG. 94** "Sensor" device in the Online Tree tab

### Panel Isn't Appearing In The Online Tree Tab

1. Verify that the System number is the same on both the NetLinx Project Navigator window and the System Settings page on the device.

2. Verify the proper NetLinx Master IP and connection methods entered into the Master Connection section of the *System Settings* page.

### MVP Can't Obtain a DHCP Address

In requesting a DHCP Address, the DHCP Server can take up to a few minutes to provide the address.

1. Verify that the WAP is configured to match the MVP panel Network Name (SSID) field, Encryption, Default Key, and Current Key string.


*Remember that the Passphrase generator on the panel does not produce the same Current Key if using the same passphrase on the WAP.*

2. In NetLinx Studio, select *Diagnostics* > *Network Address* and verify the System number.
3. If the *IP Address* field is still empty, give the device a few minutes to negotiate a DHCP Address and try again.

### My WEP Doesn't Seem To Be Working

WEP will not work unless the same default key is set on both the panel and the Wireless Access Point (WAP).

For example, if the access point was set to default WEP key 4 (which was 01:02:03:04:05), the Modero's Default WEP key 4 must be set to 01:02:03:04:05.

### NetLinx Studio Only Detects One Of My Connected Masters

Each Master is given a Device Address of **00000**.

Only one Master can be assigned to a particular System number. If you want to work with multiple Masters, open different instances of NetLinx Studio and assign each Master its own System value.

Example: A site has an NXC-ME260/64 and an NI-4000. In order to work with both units. The ME260 can be assigned System #1 and the NI-4000 can then be assigned System #2 using two open sessions of NetLinx Studio v 2.x.

### Can't Connect To a NetLinx Master

***Symptom:*** *I can't seem to connect to a NetLinx Master using NetLinx Studio 2.*

Select *Settings* > *Master Comm Settings* > *Communication Settings* > *Settings (for TCP/IP)*, and uncheck the "Automatically Ping the Master Controller to ensure availability".

The pinging is to determine if the Master is available and to reply with a connection failure instantly if it is not. Without using the ping feature, a connection may still be attempted, but a failure will take longer to be recognized.


*If you are trying to connect to a Master controller that is behind a firewall, you may have to uncheck this option. Most firewalls will not allow ping requests to pass through for security reasons.*

When connecting to a NetLinx Master controller via TCP/IP, the program will first try to ping the controller before attempting a connection. Pinging a device is relatively fast and will determine if the device is off-line, or if the TCP/IP address that was entered was incorrect.

If you decide not to ping for availability and the controller is off-line, or you have an incorrect TCP/IP address, the program will try for 30-45 seconds to establish a connection.

### Only One Modero Panel In My System Shows Up

***Symptom:*** *I have more than one Modero panel connected to my System Master and only one shows up.*

Multiple NetLinx Compatible devices, such as MVP panels, can be associated for use with a single Master. Each panel comes with a defaulted Device Number value of 10001. When using multiple panels, different Device Number values have to be assigned to each panel.

1. Press and hold the two lower buttons on both sides of the display for 3 seconds to open the *Setup* page.
2. Press the Protected Setup button (located on the lower-left of the panel page), enter **1988** into the on-screen Keypad's password field, and press **Done** when finished.
3. Enter a Device Number value for the panel into the Device Number Keypad. The default is 10001 and the range is from 1 - 32000.

### Panel Behaves Strangely After Downloading A Panel File Or Firmware

***Symptom:*** *After downloading a panel file or firmware to a G4 device, the panel behaves strangely.*

If the panel already contains a large enough file, subsequent downloads will take up more space than is available and could often corrupt the Compact Flash. The demo file that typically ships with G4 panels is one such file.

Symptoms include:

- Having to repeat the download.
- Inability to make further downloads to the panel. May get "directory" errors, "graphics hierarchy" errors, etc., indicating problems with the Compact Flash.
- Panel will not boot, or gets stuck on "AMX" splash screen.

Other problems also started after downloading to a new panel or a panel with a TPD4 file that takes up a considerable amount of the available Compact Flash.

1. DO NOT download TPD4 files (of large size) over the demo pages, or any other large TPD4 file.
2. First download a small blank one page file to the G4 panel using the Normal Transfer option to send/download the page.
3. Reboot the device.
4. Do your regular file or firmware download.

It's Your World - Take Control™

3000 RESEARCH DRIVE, RICHARDSON, TX 75082 USA • 800.222.0193 • 469.624.8000 • 469-624-7153 fax • 800.932.6993 technical support • www.amx.com