Operation/Reference Guide

MVP-5200i

Modero® Viewpoint Widescreen Touch Panel

Mio Modero Touch Panels

Initial Release: 4/28/2008

Download from Www.Somanuals.com. All Manuals Search And Download.

AMX Limited Warranty and Disclaimer

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.

Warranty Repair Policy

- AMX will repair any defect due to material or workmanship issues during the applicable warranty period at no cost to the AMX Authorized Partner., provided that the AMX Authorized Partner is responsible for in-bound freight and AMX is responsible for out-bound ground freight expenses.
- The AMX Authorized Partner must contact AMX Technical Support to validate the failure before pursuing this service.
- AMX will complete the repair and ship the product within five (5) business days after receipt of the product by AMX. The AMX Authorized Partner will be notified if repair cannot be completed within five (5) business days.
- Products repaired will carry a ninety (90) day warranty or the balance of the remaining warranty, whichever is greater.
- Products that are returned and exhibit signs of damage or unauthorized use will be processed under the Non-Warranty Repair Policy.
- AMX will continue to provide Warranty Repair Services for products discontinued or replaced by a Product Discontinuance Notice.

Non-Warranty Repair Policy

- Products that do not qualify to be repaired under the Warranty Repair Policy due to age of the product or Condition of the product may be repaired utilizing this service.
- The AMX Authorized Partner must contact AMX Technical Support to validate the failure before pursuing this service.
- Non-warranty repair is a billable service.
- Products repaired under this policy will carry a ninety (90) day warranty on material and labor.
- AMX will notify the AMX Authorized Partner with the cost of repair, if cost is greater than the Standard Repair Fee, within five (5) days of receipt.
- The AMX Authorized Partner must provide a Purchase Order or credit card number within five (5) days of notification, or the product will be returned to the AMX Authorized Partner.
- The AMX Authorized Partner will be responsible for in-bound and out-bound freight expenses.
- Products will be repaired within ten (10) business days after AMX Authorized Partner approval is obtained.
- Non-repairable products will be returned to the AMX Authorized Partner with an explanation.
- See AMX Non-Warranty Repair Price List for minimum and Standard Repair Fees and policies.

Download from Www.Somanuals.com. All Manuals Search And Download.

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

Table of Contents

Introduction 1
Memory 4
Connector Locations 5
Navigation Wheel 5
Basic Operation 6
Intercom Microphone 6
Stylus 6
Kick Stand 6
"Find Me" Capability 6
Audio/Video Capabilities 6
Power Management 6
Cleaning the Touch Overlay and Navigation Wheel 7
Accessories 9
Table Charging Station 9
Wall Charging Station 10
Recharging 11
Security Release 11
Installing the MVP-5200i Touch Panel 13
Installing the panel on a NetLinx system 13
Establishing a wireless connection with AMX WAP 13
Configuring the device 13
Locating the device in NetLinx Studio 13
Verifying and upgrading the firmware 13
Downloading custom touch panel pages 13
Power Management 14
Wireless Interface Cards 15
802.11b Wireless Interface Card 15
Specifications 15
NXA-WC80211GCF 802.11g Wireless Interface Card 16
Specifications 17
Installing the 802.11g Card and Antenna 19
Firmware Requirements 19
Preparing the MVP's Rear Housing 19
Installing the NXA-WC80211GCF 20
Closing and Securing the MVP Enclosure 21

Download from Www.Somanuals.com. All Manuals Search And Download.

Configuring Communication 23
IR Communication 25
"Find Me" Function 25
Modero Setup and System Settings 26
Accessing the Setup and Protected Setup Pages 26
Setting the Panel's Device Number 26
Wireless Settings - Wireless Access Overview 27
Hot Swapping 27
DHCP 27
Configuring a Wireless Network Access 28
Step 1: Configure the Panel's Wireless IP Settings 28
Wireless communication using a DHCP Address 28
Wireless communication using a Static IP Address 29
Using the Site Survey tool 29
Step 2: Configure the Card's Wireless Security Settings 31
Configuring the Modero's wireless card for unsecured access to a WAP200G 31
Configuring the Modero's wireless card for secured access to a WAP200G 33
Automatically set SSID 34
Manually set SSID 34
Configuring multiple wireless Moderos to communicate to a target WAP200G 37
Step 3: Choose a Master Connection Mode 38
Ethernet over USB 38
Touch panel setup 39
Setting up a device IP address 41
Configure a Virtual NetLinx Master using NetLinx Studio 42
Ethernet 44
Master Connection to a Virtual Master via Ethernet 45
Using G4 Web Control to Interact with a G4 Panel 47
Using your NetLinx Master to control the G4 panel 48
Upgrading Firmware 53
Scale Images For Setup Pages 53
Upgrading the Modero Firmware via the USB port 53
Step 1: Configure the panel for a USB Connection Type 53
Step 2: Prepare Studio for communication via the USB port 54
Step 3: Confirm and Upgrade the firmware via the USB port 55
Setup Pages 59
Setup Pages 59
Navigation Buttons 61
Project Information Page 61

Download from Www.Somanuals.com. All Manuals Search And Download.

Panel Information Page 63
Time & Date Setup Page 64
Audio Adjustments/Volume Page 65
WAV files - Supported sample rates 66
Batteries Page 66
Protected Setup Pages 67
Protected Setup Navigation Buttons 69
G4 Web Control Page 70
Password Setup Page 71
Calibration Page 72
Wireless Settings Page 73
Wireless Security Page 76
Open (Clear Text) Settings 77
Static WEP Settings 78
WPA-PSK Settings 80
EAP-LEAP Settings 81
EAP-FAST Settings 84
EAP-PEAP Settings 86
EAP-TTLS Settings 88
EAP-TLS Settings 90
Client certificate configuration 91
System Settings Page 93
EAP Security & Server Certificates - Overview 95
Programming 97
Overview 97
Navigation Wheel Programming 97
Page Commands 97
Programming Numbers 104
RGB triplets and names for basic 88 colors 104
Font styles and ID numbers 106
Border styles and Programming numbers 107
"^" Button Commands 110
Miscellaneous MVP Strings back to the Master 129
MVP Panel Lock Passcode commands 129
Text Effects Names 130
Button Query Commands 131
Panel Runtime Operations 140
Input Commands 144
Embedded codes 145

Download from Www.Somanuals.com. All Manuals Search And Download.

Panel Setup Commands 146
Dynamic Image Commands 147
Browser-Based User Pages 151
Battery Life and Replacement 153
Overview 153
Battery Replacement 153
Appendix A: Text Formatting 155
Text Formatting Codes for Bargraphs/Joysticks 155
Text Area Input Masking 156
Input mask character types 156
Input mask ranges 157
Input mask next field characters 157
Input mask operations 157
Input mask literals 157
Input mask output examples 158
URL Resources 159
Special escape sequences 159
Appendix B: Wireless Technology 160
Overview of Wireless Technology 160
Terminology 161
EAP Authentication 164
EAP characteristics 164
EAP communication overview 165
AMX Certificate Upload Utility 166
Configuring your MVP-5200i for USB Communication 166
Step 1: Setup the Panel and PC for USB Communication 166
Step 2: Confirm the Installation of the USB Driver on the PC 167
How to Upload a Certificate File 168
Appendix C: Troubleshooting 169
Panel Doesn't Respond To Touches 169
Battery Will Not Hold Or Take A Charge 169
MVP-5200i Isn't Appearing In The Online Tree Tab 170
MVP Can't Obtain a DHCP Address 170
My WEP Doesn't Seem To Be Working 170
NetLinx Studio Only Detects One Of My Connected Masters 170
Can't Connect To a NetLinx Master 170
Only One Modero Panel In My System Shows Up 171
Panel Behaves Strangely After Downloading A Panel File Or Firmware 171

Download from Www.Somanuals.com. All Manuals Search And Download.

Introduction

The MVP-5200i Modero® Viewpoint® Widescreen Touch Panel is AMX's smallest and most powerful wireless handheld panel, available in black (**FG5966-01**) (FIG. 1) and white (**FG5966-02**). The MVP-5200i is a wireless-only ergonomic device capable of Voice Over Internet Protocol (VoIP) communication, with all control established through a NetLinx Master. Besides offering the same functionality as the rest of AMX's line of G4 touch panels, the MVP-5200i touch panel offers full duplex VoIP communication, quick wakeup and connection time, and an extended battery life for longer operation between charges. The MVP-5200i device utilizes a 5.2" Color Active LCD to display a 800 x 480 pixel image with 262,144 colors.

FIG. 1 MVP-5200i-GB touch panel

Download from Www.Somanuals.com. All Manuals Search And Download.

The MVP-5200i comes with an integrated rear "kickstand", allowing it to be used and displayed away from a Charging Station if necessary (FIG. 2). It also comes with a pre-installed 802.11g WPA/WPA2 SDIO wireless card.

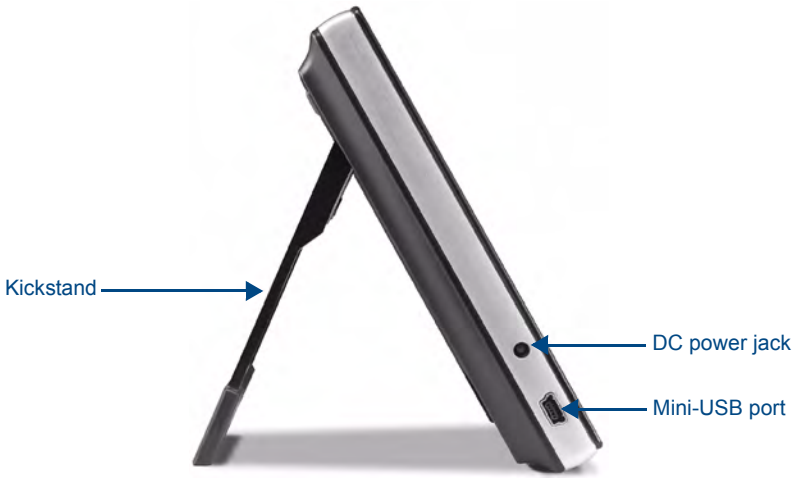


FIG. 2 MVP-5200i side view (with kickstand)

MVP-5200i Specifications (FG5966-01, FG5966-02)	
Dimensions:	4 3/4" x 7 9/16" x 13/16" (120.7 mm x 191.8 mm x 20.3 mm)
Weight:	• Panel: 1.4 lbs (0.64 kg)
Enclosure:	*MVP-5200i-GB*: High-gloss black plastic with brushed metal retaining ring. *MVP-5200i-GW*: High-gloss white plastic with brushed metal retaining ring.
Power Requirements (Without Charging):	Panel with battery fully charged: • Constant current draw: 0.3 A @ 12 VDC • Startup current draw: 0.4 A @ 12 VDC
Power Requirements (While Charging):	Panel while charging battery: • Constant current draw: 1.1 A @ 12 VDC • Startup current draw: 1.3 A @ 12 VDC
Minimum Power Supply Required:	• PS3.0 Power Supply (**FG423-30**) - both 120 VAC and 240 VAC models are shipped with this power supply
Power Modes:	• *AWAKE:* All necessary modules are powered up and device remains online with the Netlinx Master. • *ASLEEP:* Only the backlight will be turned off after the user selectable time of inactivity has elapsed. Panel resumes the ON mode in ~ 1 second. • *PROCESSOR SHUTDOWN:* Power to all peripherals and components is turned off. The system remains in this mode until either it is rebooted or the battery is completely drained.
Certifications:	• FCC Part 15 Class B and CE • CE • IEC60950 • RoHS • TELEC • Lithium polymer microbattery: UN/IATA
Battery Duration:	• Four days of *normal* use (25% Awake state, 25% Asleep, and 50% Processor Shutdown). • Eight hours of *continuous* use (continuous Awake state).

Download from Www.Somanuals.com. All Manuals Search And Download.

MVP-5200i Specifications (FG5966-01, FG5966-02) (Cont.)	
Memory:	• 128 MB Mobile DDRAM (upgrade not available) • 256 MB NAND Flash (upgrade not available)
Panel LCD Parameters:	• Size: 5.2" (13.21 cm) • Type: WVGA • Aspect ratio: 16 x 9 • Brightness (luminance): 300 cd/m^2 • Channel transparency: 8-bit Alpha blending • Contrast ratio: 20:1 • Display colors: 262,144 colors (18-bit color depth) • Dot/pixel pitch: 0.23 mm • Panel type: TFT Color Active-Matrix • Screen resolution: 800 x 480 pixels (HV) @ 60 Hz frame frequency • Viewing angles: Vertical: + 40° (up from center) and - 80° (down from center) Horizontal: + 60° (left from center) and - 60° (right from center)
External Components	
Connector:	5-pin Mini-USB connector used for audio output to USB headphones, programming, firmware updates, and touch panel file transfer between the PC and the target panel. **Note:** When connecting the panel to PC using a CC-USB (or compatible) cable, be sure to power the panel On **before** attempting to connect the USB cable from the PC to the mini-USB port on the panel.
DC power port:	2.5 mm port to power the panel away from a Charging Station.
Stylus Slot:	Slot where the included stylus is stored, located on the right side of the device.
Microphone:	For use with the intercom feature. • Frequency: 20 to 160,000 Hz • S/N Ratio: More than 58 dB
Speaker:	• 4Ohm • 2 Watts 300Hz cutoff frequency
Audio Standards:	• G.711 sound standard • 75dB SPL@1m
IR Emitters:	Transmit IR over 20 feet (6.10 m) from the panel. • IR emitters on G4 panels share the device address number of the panel. • Transmits AMX fixed frequencies at 38KHz and 455KHz and user programmable frequencies from 20KHz to 1.5MHz
Operating/Storage Environment	• Operating Temperature: 0° C (32° F) to 40° C (104° F) • Operating Humidity: 20% - 85% RH • Storage Temperature: -20° C (-4° F) to 60° C (140° F) • Storage Humidity: 5% - 85% RH
Included Accessories:	• MVP-5200i Installation Guide (**93-5966-01**) • PS3.0 Power Supply (**FG423-30**) • MVP-STYLUS-52 (pre-installed onto the right side of the unit) (**FG5966-10xx**)

Download from Www.Somanuals.com. All Manuals Search And Download.

MVP-5200i Specifications (FG5966-01, FG5966-02) (Cont.)	
Other AMX Equipment:	• MVP-TCS-52: Table Charging Station (**FG5966-1X**) • MVP-WCS-52: Wall Charging Station (**FG5966-1X**) • MVP-BP-52: Battery Replacement Kit (**FG5966-20**) • MVP-STYLUS-52: Replacement Stylus, Pack of 3 (**FG5966-30-xx**) • CC-USB: USB Programming Cable (**FG10-5965**) • MVP-HP USB 1/8" Adapter (**FG5966-23**)

1.2.

NOTE

This device complies with FCC Part 15 and Industry Canada RSS 210 subject to the following conditions:
1. This device must not cause harmful interference and
2. This device must accept all interference, including interference that interferes with the operation of this device.

Memory

The MVP-5200i comes with 128MB of Mobile DDRAM memory and 256 MB NAND Flash memory. Neither may be upgraded.

Table Charging Station Connector Locations

With the unit facing you, the mini-USB port (for programming and downloading firmware as well as connecting USB headphones using the AMX-provided adaptor cable) and the DC power port are located on the lower left side of the device (FIG. 3). The connector for the Table Charging Station (please refer to the *Table Charging Station* section on page 7) is located on the bottom of the device.

FIG. 3 MVP-5200i side view with programming port

WARNING

Although firmware upgrades can be conducted over a wireless Ethernet connection, transferring firmware KIT files over a direct USB connection is recommended, 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.

In addition to its speaker, the MVP-5200i also utilizes its mini-USB port as a connector for standard headphones or headsets. These headphones must use a mini-USB plug or adaptor in order to utilize this feature.

NOTE

While standard input/output headsets may be used in lieu of headphones, the headset may only be used for output. While you may receive sound from the headset, its microphone will not function. Always use the MVP-5200i's microphone for receiving sound.

Download from Www.Somanuals.com. All Manuals Search And Download.

Basic Operation

The MVP-5200i is operated using both its integral touchscreen and the navigation wheel on the right side of the device. If the device has gone into its Standby Mode, a touch of the touchscreen or of the button wheel will reactivate it.

The MVP-5200i device's power use allows up to 96 continuous hours of use between rechargings of its internal battery, but its battery charge lasts up to 120 hours if the device goes into Standby Mode during that time. The device may be placed in its charging cradle at any time and operated within its cradle.

The device will automatically go into Sleep Mode after fifteen minutes of inactivity, and this limit may be changed at any time. Any wireless Internet connection intended for the device will be reconnected within approximately twenty seconds after the device is placed in its charging cradle. Depending upon preselected settings, the device may be set to go into Active Mode as soon as it is placed in the cradle.

Navigation Wheel

The MVP-5200i device uses a unique button wheel for all commands not directly involving the touchscreen. This wheel, known as a navigation wheel, is located in the upper right corner of the device (FIG. 4). Used with the touchscreen, the navigation wheel allows scrolling and adjusting by turning the wheel with a thumb or finger and then pressing down on one of the wheel's compass points for up, down, left, and right. The wheel is sensitive enough to adjust levels with one-third of a rotation. The center of the navigation wheel also acts as a button in its own right: press down directly upon the wheel center for the equivalent of an "Enter" keystroke

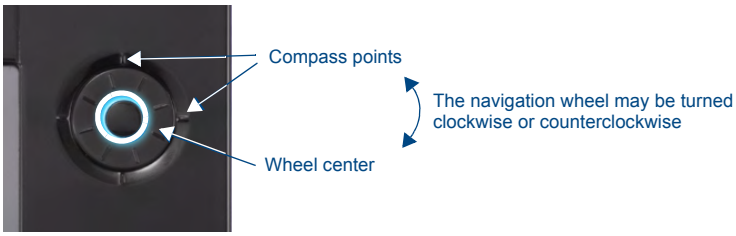


FIG. 4 Navigation wheel detail

Press and hold the wheel center for three seconds to access the *Setup* pages (for more information, please see the *Setup Pages* section on page 47). Continue to hold the wheel center for another three seconds to access the *Calibration* page (page 84).

If the MVP-5200i needs to be shut down or reset for any reason, press and hold down the wheel center button until the popup stating "panel shutting down" appears or the screen goes dark. To turn it back on, press any of the wheel's compass points and hold until the AMX splash screen appears on the touchscreen.

NOTE

Shut down the panel by holding the wheel center button only if the Setup pages are otherwise inaccessible. Regularly shutting down the device by this method can corrupt the Flash memory.

The navigation wheel may also be programmed to initiate specific commands. For more information, please see the *Programming* section on page 101.

Intercom Microphone

The MVP-5200i contains a built-in microphone above the upper lefthand corner of the touch screen for video and audio conferencing capabilities. This microphone is concealed by the casing.

Download from Www.Somanuals.com. All Manuals Search And Download.

Stylus

The MVP-5200i comes with a unique touchscreen stylus that slides into a storage groove on the right side of the device when not in use. Replacement styluses may be ordered in a 3-pack (**FG5966-30-xx**) from **www.amx.com**.

Kick Stand

Since the MVP-5200i device is designed to be a unit used away from its charging station, it has an extendable "kickstand" on the back of the unit (FIG. 2). This may be opened by physically lifting the free end of the kick stand away from the device. The device may then be propped up on a flat surface and accessed in a normal fashion.

Audio/Video Capabilities

The MVP-5200i has the capability of displaying multiple JPEG and PNG files at one time. The device also supports streaming motion JPEG video (of the sort used by many IP and Web cameras), as well as MP3 and WAV audio files.

Power Management

The MVP-5200i utilizes a dual voltage external power supply. It may be recharged through the supplied PS3.0 Power Supply (**FG423-30**), as well as through the MVP-TCS-52 Table Charging Station (**FG5966-1X**) or the MVP-WCS-52 Wall Charging Station (**FG5966-1X**). For more information, see the *Accessories* section on page 7 for details.

Although the MVP-5200i unit is equipped with a mini-USB port, the device cannot be powered through the USB port. The port is only used for uploading firmware.

When not in active use, the MVP-5200i conserves battery life between chargings. In its Sleep Mode, the device's entire system is shut down, with only wakeup systems powered to detect incoming commands or touch panel contact. Pressing any of the compass points on the navigation wheel will return the device to its Active Mode,

For more information on the battery, see the *Battery Life and Replacement* section on page 153.

Cleaning the Touch Overlay, Case, and Navigation Wheel

You should clean the touch screen overlay after each day's use to maintain the appearance of the device. Always use a clean cotton cloth and a spray bottle containing water or a vinegar-based cleaner, as alcohol-based cleaners can damage the device's touch screen overlay. **Do not directly spray the device**: instead, spray the cloth to clean the touch screen overlay and navigation wheel. Do NOT use an abrasive of any type to clean the MVP-5200i, as this may permanently damage or remove the device's finish.

Download from Www.Somanuals.com. All Manuals Search And Download.

Accessories

Table Charging Station

The MVP-5200i device comes with the MVP-TCS-52 Table Charging Station (**FG5966-1X**) (FIG. 5), which acts both as a charging station and a direct power connection. The charging station is available in either white (**FG5966-10**) or black (**FG5966-11**).

FIG. 5 MVP-TCS-52-GB Table Charging Station - Front

MVP-TCS-52 Specifications	
Dimensions (HWD):	• 8.0” x 4.75” x 3.5” (20.32cm x 12.07cm x 8.89cm)
Weight:	• .65 lbs (.29 kg)
Rear Connector:	• 5-pin charging connector on bottom of charging cradle.
Operating/ Storage Environments:	• Operating Temperature: 0° C (32° F) to 40° C (104° F) • Operating Humidity: 20% - 85% RH • Storage Temperature: -20° C (-4° F) to 60° C (140° F) • Storage Humidity: 5% - 85% RH
Included Accessories	• MVP-TCS-52 Table Charging Station Quick Start Guide (**93-5966-02**) • PS3.0 Power Supply (**FG423-44**)
Other AMX Equipment:	• MVP-5200i Modero Viewpoint Widescreen Touch Panel -Gloss Black (**FG5966-01**) • MVP-5200i Modero Viewpoint Widescreen Touch Panel - Gloss White (**FG5966-02**) • MVP-WCS-52: Wall Charging Station (**FG5966-1X**)

Powering the MVP-TCS-52

The MVP-TCS-52 uses a PS3.0 power supply (included with the MVP-5200i touch panel or available separately from **www.amx.com**) to provide direct power for the MVP panel both for standard functions and for charging its internal battery.

1. Connect the terminal end of the PS3.0 power supply to the PWR connector on the bottom of the MVP-TCS-52.
2. To prevent wear on the power supply cord and assure that the device’s base is in full contact with the table surface, press the cord into the locking groove running across the bottom of the device.
3. Provide power to the MVP-TCS by connecting the PS3.0 cord to an external power source.

Download from Www.Somanuals.com. All Manuals Search And Download.

4. Place the touch panel in the Charging Station cradle (FIG. 6), guiding it into place with the locking grooves on each side of the cradle (FIG. 7). When fully seated, the touch panel's charging station connector should be in contact with the Charging Station's charger pins.

FIG. 6 MVP-5200i in MVP-TCS-52-GB Table Charging Station

Connections and Wiring

The PS3.0 is used to supply power to the MVP-5200i by routing incoming power through the connector pins and charge the device's internal battery

Recharging

To recharge the MVP-5200i, slide the device into the Table Charging Station cradle bottom-first and make sure the device is fully seated in the Charging Station. The charger pins in the bottom of the cradle (FIG. 7) must be in contact with the connector on the bottom of the MVP-5200i for it to start recharging. The MVP panel will stop recharging automatically once the battery has achieved its maximum charge.

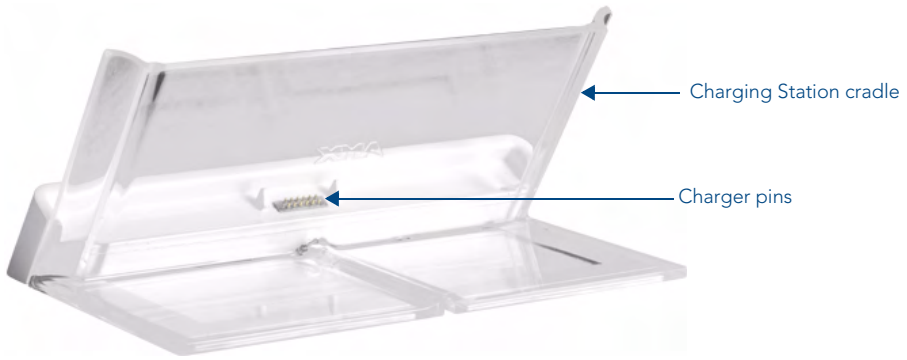


FIG. 7 MVP-TCS-52-GW Table Charging Station - Rear

Cleaning the MVP-TCS-52

You should clean the Table Charging Station after each day's use to maintain the device's appearance. Always use a clean cotton cloth and a spray bottle containing water or a vinegar-based cleaner, as alcohol-based cleaners can damage the device. Do not directly spray the device: instead, spray the cloth to prevent moisture from collecting on the charger pins. Do NOT use an abrasive of any type to clean the Table Charging Station, as this may permanently damage or remove the device's finish.

Download from Www.Somanuals.com. All Manuals Search And Download.

Wall Charging Station

The optional MVP-WCS-52 Wall Charging Station (**FG5966-1X**) offers the same recharging and connection features as the Table Charging Station, with the advantage of being placed within accessible locations where the table station is either inconvenient or impractical (FIG. 8). The Wall Charging Station is available in either white (**FG5966-13**) or black (**FG5966-12**).

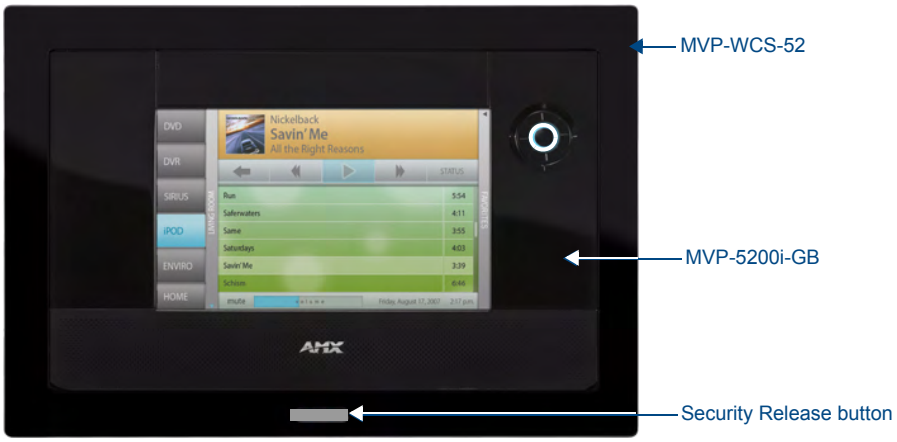


FIG. 8 MVP-WCS-52-GB Wall Charging Station - Front

The features of the MVP-WCS-52 include:

- Full charging of a docked MVP-5200i in approximately 4.5 hours
- Touch panel code lock for security
- Integrated docking alignment guides for easy docking
- Panel eject design with mechanical or electronically controlled capabilities.

.

MVP-WCS-52 Specifications	
Dimensions (HWD):	• 8.375" x 6.09" x 2.19" (21.27 cm x 15.46 cm x 5.56 cm) ***Note**: Always use the cutout/installation dimensions for the MVP-WCS-52 when installing this unit into various surfaces. This SP engineering drawing is available online at **www.amx.com**.*
Power Requirements:	• 3 A @ 12 VDC (Class II listed power supplemented)
Startup Power Requirements	• Total: 1.7A • Charging: 1.1A • Ejection: 0.6A
Weight:	• Without conduit box: 0.85 lbs (0.39 kg) • With conduit box: 1.30 lbs (0.59 kg)
Available Colors:	• MVP-WCS-52-GW (White) - **FG5966-13** • MVP-WCS-52-GB (Black) - **FG5966-12**

Download from Www.Somanuals.com. All Manuals Search And Download.

MVP-WCS-52 Specifications	
Front Panel Components:	• Securing Magnets: Prevent MVP touch panel from falling free during ejection. • Security Latch: Adds the primary layer of security when mounting an MVP touch panel. When the device is inserted, this latch grabs onto the rear of the touch panel and secures it to prevent it from being removed. • Interface Connector Pins: A set of retractable pins (male) that connect to the underside MVP connector strip. This connection provides both communication and power between the touch panel and the MVP-WCS-52. • Support Cradle: This retractable mechanism supports a resting MVP panel and allows a user to either insert or remove a connected MVP panel. • Security Release pushbutton: Located on the front of the unit, this pushbutton toggles an on-screen security keypad (if security is enabled). *- Entering the correct release code allows the MVP-WCS-52 to release the touch panel from the security latch.*
Operating/Storage Environments:	• Operating Temperature: 0° C (32° F) to 40° C (104° F) • Operating Humidity: 20% - 85% RH • Storage Temperature: -20° C (-4° F) to 60° C (140° F) • Storage Humidity: 5% - 85% RH
Included Accessories	• MVP-WCS-52 Wall Charging Station Quick Start Guide (**93-5966-12**) • Wallmount plastic conduit box (**62-5966-12**) • MVP-WCS-52 Installation Kit - Black (**KA 5966-01bl**) • MVP-WCS-52 Installation Kit - White (**KA 5966-01wh**)
Other AMX Equipment:	• MVP-TCS-52: Table Charging Station (**FG5966-1X**) • Wallmount Metal Conduit Box (**FG037-11**) • MVP-5200i Modero Viewpoint Widescreen Touch Panel -Gloss Black (**FG5966-01**) • MVP-5200i Modero Viewpoint Widescreen Touch Panel - Gloss White (**FG5966-02**) • PS3.0 Power Supply (**FG423-30**)

The MVP-5200i touch panel remains locked in the MVP-WCS-52 until unlocked by the user. This may be done by entering an appropriate password (please refer to the *Password Settings Page* section on page 88 for more information), or by pressing the Security Release button on the front of the device in emergencies. The station ejects the device top first (FIG. 9). The device uses two neodymium rare-earth magnets to keep the MVP-5200i from falling out of its cradle when the touch panel is angled forward..

FIG. 9 MVP-WCS-52-GW Wall Charging Station - Side view

Download from Www.Somanuals.com. All Manuals Search And Download.

Unlocking the touch panel

Once placed within the Wall Charging Station, the MVP-5200i remains secured until the user unlocks it. To release the touch panel from the Wall Charging Station:

1. Press the Security Release button.
2. A password keypad will pop up on the MVP-5200i screen. Enter a password in the password keypad and press **Enter**.
3. Wait for the Wall Charging Station to pivot the touch panel away from the wall.
4. The device will remain in the ejected position until the MVP-5200i is removed. Wait until the device's ejection door has completely withdrawn before re-installing the MVP-5200i.

Unique passwords may be entered for up to four unique users as well as the administrator. For more information on setting passwords, please refer to the Password Settings Page section on page 88.

Recharging

To recharge the MVP-5200i:

1. Slide the device into the Wall Charging Station cradle bottom-first and make sure the device is fully seated in the Charging Station.
2. Press the top of the MVP-5200i back until it clicks. The touch panel is now locked into the Charging Station, and the station will automatically charge the device's battery. (Please refer to the *Battery Settings Page* section on page 56 to check on the battery charge status.)
3. To release the touch panel, unlock the touch panel and wait for the Wall Charging Station to pivot the touch panel away from the wall.

Download from Www.Somanuals.com. All Manuals Search And Download.

Installing the MVP-WCS-52

Since the Wall Charging Station is intended to be affixed to a wall or other permanent structure, care must be taken to ensure its proper installation to prevent potential damage to the MVP-5200i placed within.

NOTE

Other than wall installation tools, the only tool required for this installation is a #1 Phillips screwdriver.

Installing the Plastic Conduit Box

The plastic conduit box has two knockouts at the top of the box and four (4) lockdown wings attached to the box with Phillips-head screws. For ease of installation, the interior of the box contains an "UP" arrow pointing to the knockouts. The metal conduit box does not have to be installed beforehand, but it offers an extra level of support.

To install the plastic conduit box:

1. Cut a hole into the wall or surface intended to hold the conduit box. The conduit box is sized 8.375 inches (21.27cm) long and 5.75 inches (14.60cm) high (FIG. 10), so the hole should be at least 1/4" (0.64cm) smaller in each dimension.

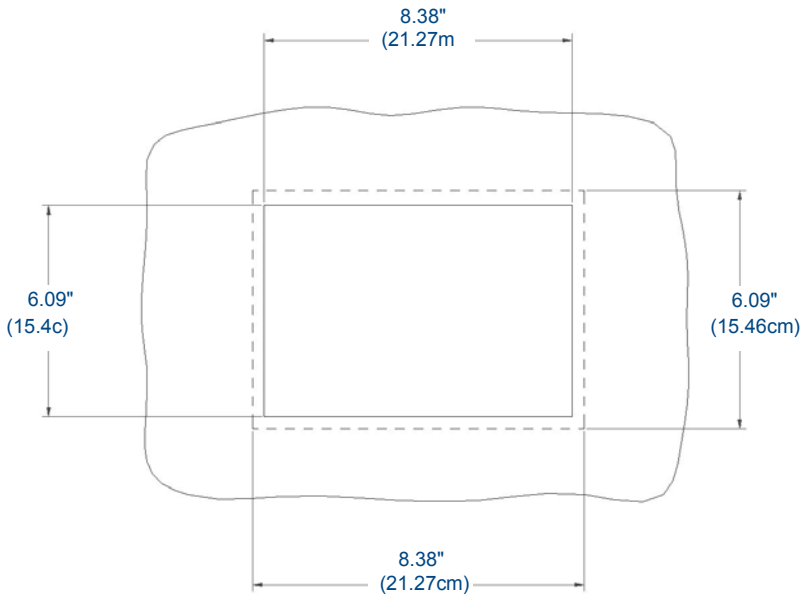


FIG. 10 Recommended cutout for plastic conduit box

WARNING

Make sure to measure the size of the intended hole before starting to cut it.

2. Select the knockout to be removed from the top of the conduit box. The box has two knockouts, at the top left and the top right.

Download from Www.Somanuals.com. All Manuals Search And Download.

NOTE

To assist with wiring, and to avoid mechanical stresses on the wire and the mechanism of the Wall-Mounted Charging Station, the top right knockout is preferred for use.

3. Run the power cable through the knockout into the conduit box. Pull out about six inches (15.25cm) of cable into the conduit box to facilitate installation of the MVP-WCS-52.
4. Slide the plastic conduit box into the hole, being careful not to twist or pinch the cable, and set it flush with the wall (FIG. 11). Make sure that all of the lockdown wings are folded into their slots before attempting to insert the box. For ease of installation, the inside of the box has the direction "UP" labeled for reference.

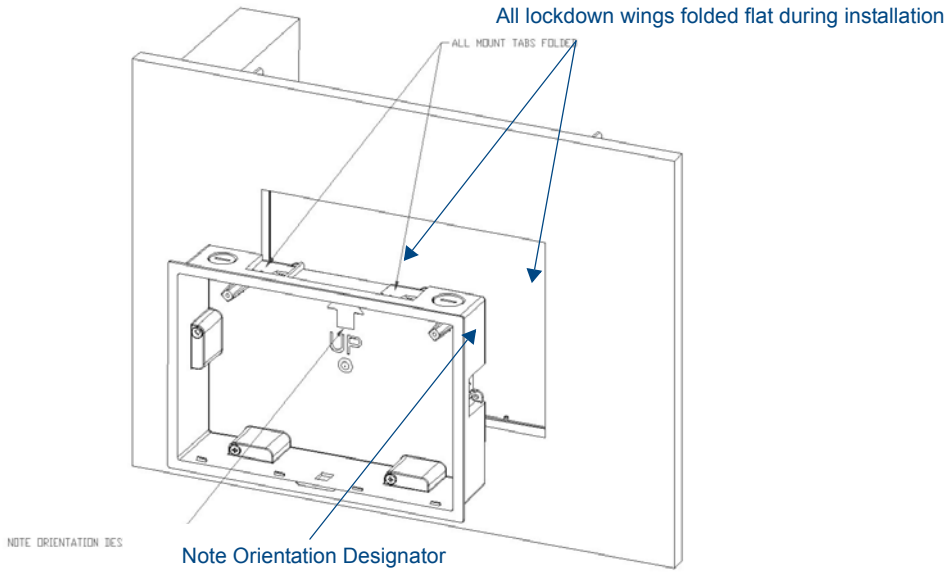


FIG. 11 Installation of plastic conduit box

5. Extend the wings on the sides of the conduit box by tightening the screws inside the box. Not all of the wings must be extended to lock the conduit box in place, but extending a minimum of the top and bottom wings is highly recommended. Apply enough pressure to the screw head to keep the box flush with the wall: this ensures that the wing will tighten up against the inside of the wall.

WARNING

Make absolutely certain that the conduit box is in its intended position. Once the conduit box lockdown wings are extended within the box's hole within the wall, removing the conduit box will be extremely difficult without damaging the wall in the process.

6. Prepare the captive wires for the 2-pin 3.55 mm mini-captive wire connector used for the MVP-WCS-52's power supply:

NOTE

Preparing and connecting the captive wires requires the use of a wire stripper and flat-blade screwdriver.

- Strip 0.25 inch (6.35 mm) of wire insulation off all wires.
- Insert each wire into the appropriate opening on the connector.
- Turn the screws clockwise to secure the wires in the connector. Do not over-torque the screws; doing so can bend the seating pins and damage the connector.

Download from Www.Somanuals.com. All Manuals Search And Download.

7. Secure the power cable to the device, using either of the two tie-wrap anchors included in the Installation Kit at the top rear of the device (FIG. 12). Point the head of each tie wrap toward the center of the device.

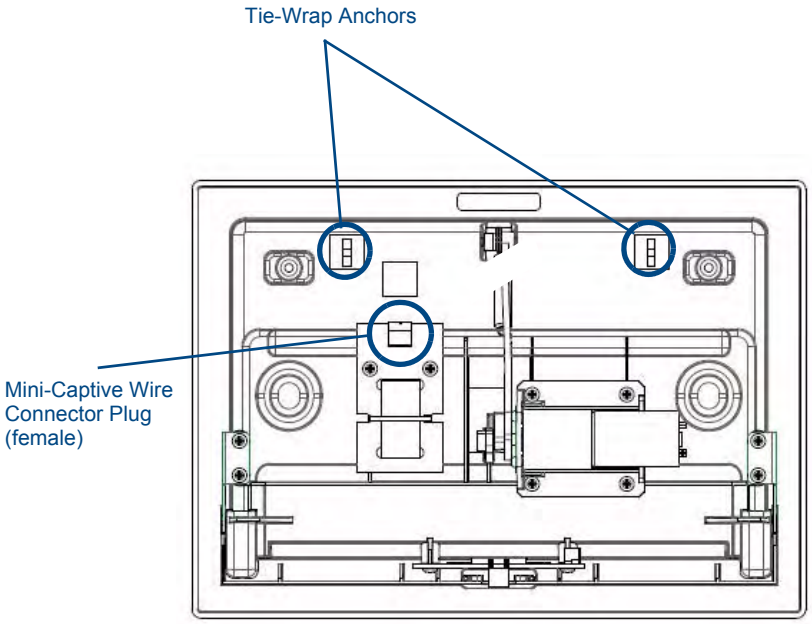


FIG. 12 MVP- WCS-52 - Rear

8. Firmly seat the mini-captive wire connector to the power connector on the device.
9. Firmly seat the device against the conduit box. Make sure that the tab connector at the top of the device is locked into the conduit box.
10. Insert the two installation screws from the MVP-WCS-52 Installation Kit into the screw holes in the interior compartment of the device and tighten them to anchor the device to the conduit box.

Download from Www.Somanuals.com. All Manuals Search And Download.

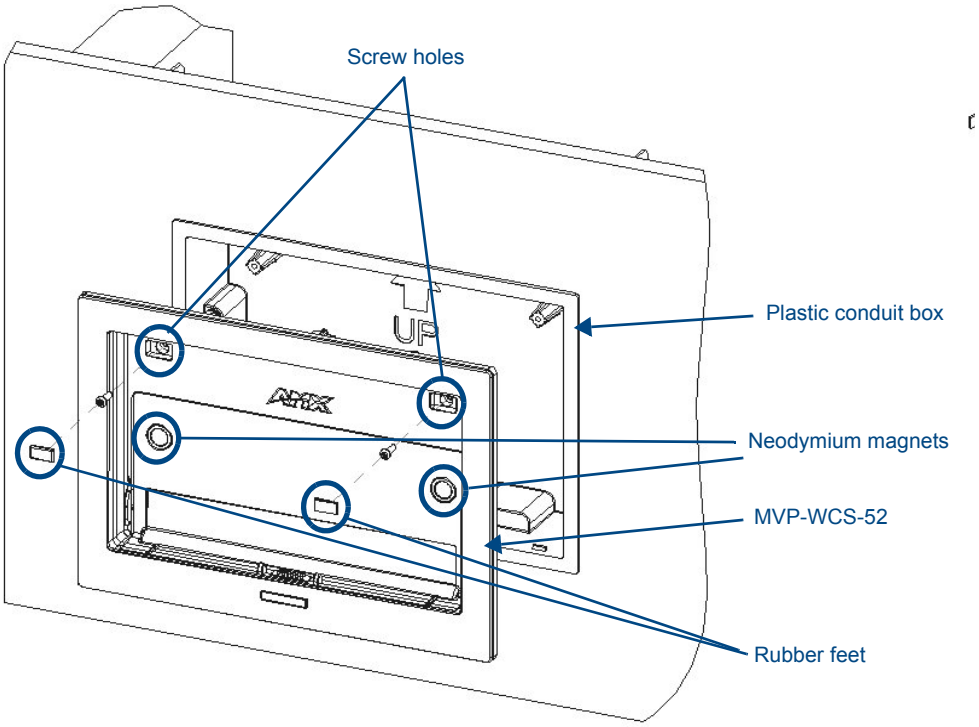


FIG. 13 Installation of MVP-WCS-52

NOTE

For ease of installation, put each screw on a neodymium magnet in the device's interior compartment to keep them on hand until they are needed.

11. After fully seating the screws, wipe down the area around the screw holes with the alcohol prep pad from the Installation Kit. Take a rubber foot and remove its adhesive backing. Put the foot, adhesive-side down, in the slot surrounding the screw hole in the Wall Charging Station. Press down firmly to remove any air bubbles from underneath the foot.
12. Install an MVP-5200i device by placing it into the interior compartment bottom-first. Press the top of the touch panel until it is flush with the Wall Charging Station. The neodymium magnets will hold it in place.
13. To remove the MVP-5200i, unlock the touch panel (see the *Unlocking the touch panel* section on page 11 for more information) and wait for the touch panel to pull away from the Wall Charging Station. Once it has been released, grip it by the top of the device, and pull it free from the Charging Station.

Download from Www.Somanuals.com. All Manuals Search And Download.

Installing the Optional Metal Conduit Box

The optional metal conduit box (FIG. 14) is 10 inches wide at its widest dimension, and is intended to be used in conjunction with the plastic conduit box in circumstances where additional support is needed for the Wall Charging Station. The box requires an appropriate spacer if used within a standard 16" stud space. Without the Metal Conduit Box, the supported minimum wall thickness is 1/2" (1.27cm), and the maximum is 7/8" (2.22cm). With the Metal Conduit Box, the minimum supported wall thickness is 3/8" (0.95cm), and the maximum is 3/4" (1.91cm).

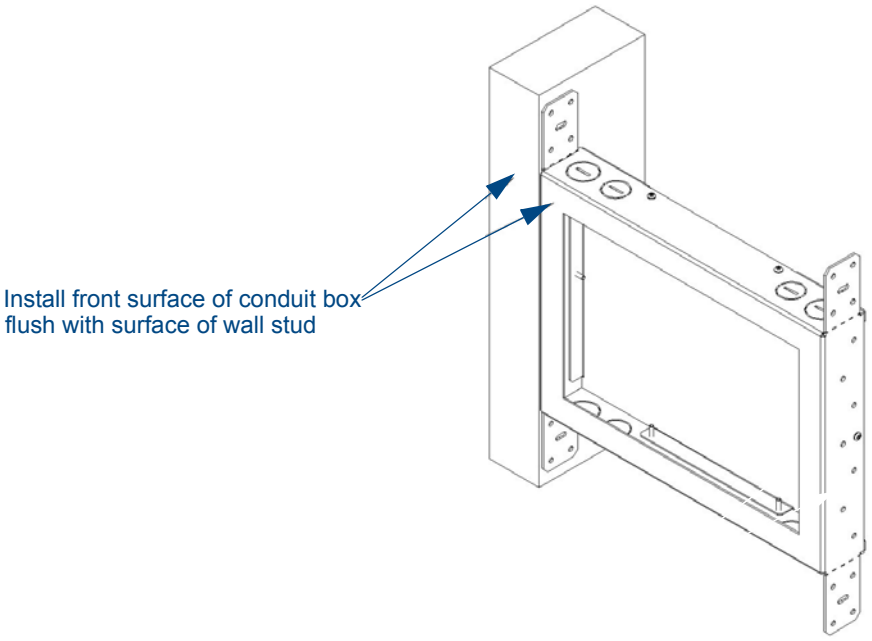


FIG. 14 Typical Metal Conduit Box Installation

The metal conduit box bears a wing on each corner which is intended to bridge gaps between studs and/or spacers. These wings may be bent carefully in order to fit a particular gap, but may not be so bent as to allow the conduit box to hang in a vertical position. Once placed in the desired position, put at least one screw through each wing into the adjoining stud or spacer to secure it.

The interior of the conduit box contains a set of holes on either side, as well as top and bottom, for standard 1/4-inch screws. Use these holes to anchor the conduit box to its adjoining studs or spacers.

WARNING

Ensure that the metal conduit box is flush with the 2x4 studs. Any overhang will affect the installation of the covering sheetrock, as well as affect the placement of the plastic conduit box.

The conduit box has two sets of knockouts in the top and bottom, one of the set for US wiring and one for international wiring.

NOTE

Make sure that the power cable has been pulled through the metal conduit box by the resident electrician before continuing the installation.

After completing the installation of the metal conduit box, install sheet rock or other wall material over the box, cut a hole matching the size of the inside diameter in the sheet rock, and clean out all dust before proceeding with the installation of the plastic conduit box.

Download from Www.Somanuals.com. All Manuals Search And Download.

Configuring Communication

All control for a MVP-5200i touch panel is established through a NetLinx Master. 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.

In the example below (FIG. 15), three MVP-5200i devices are shown at varying distances from the two WAP gateways. As with any other WAP network, the gateways are spaced so as to allow a maximum wireless coverage for the three devices.

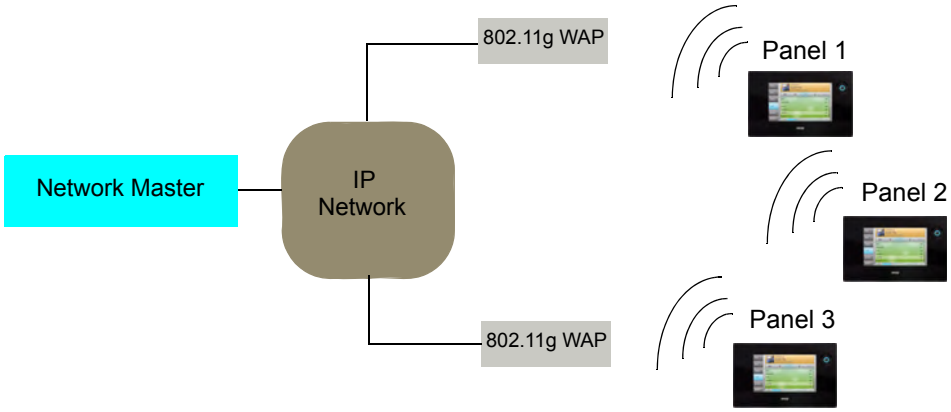


FIG. 15 System Deployment Diagram

When initially installing the MVP-5200i, some basic configuration items, including network settings and NetLinx settings, will need to be set. For more information, refer to the *Protected Setup Pages* section on page 59.

NOTE

The MVP-5200i defaults to Ethernet and Auto mode for its Master connection.

Download from Www.Somanuals.com. All Manuals Search And Download.

IR Communication

In certain situations, the MVP-5200i may be used as an infrared remote device for other AMX controllers. The device can transmit IR over 20 feet (6.10 m) from the panel at frequencies of 38KHz, 455KHz, and 1.2MHz. IR receivers and transmitters on G4 panels share the device address number of the panel.

The MVP-5200i includes an IR transmitter for communication between the device and the NetLinx Master and between separate devices. The transmitter is located behind the IR Emitter Panel on the rear of the device (FIG. 16).

FIG. 16 IR transmitter window on the MVP-5200i-GW

Download from Www.Somanuals.com. All Manuals Search And Download.

Modero Setup and System Settings

All AMX Modero panels, including the MVP-5200i, 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. At any time, press down and hold the center button of the navigation wheel for 3-5 seconds. This opens a release notice to release the button immediately to open the *Setup* page (FIG. 17).

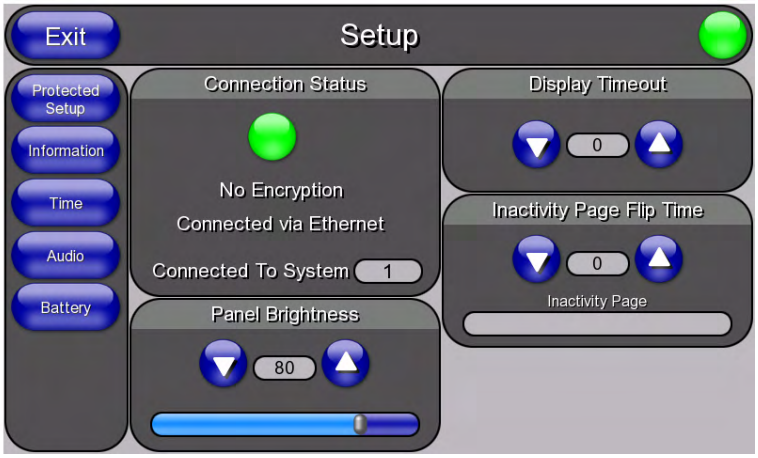


FIG. 17 Setup page

2. Press the **Protected Setup** button. This opens a keypad for entry of the password to allow access to the *Protected Setup* page (FIG. 18). Enter the device's password and press **Done** to proceed.

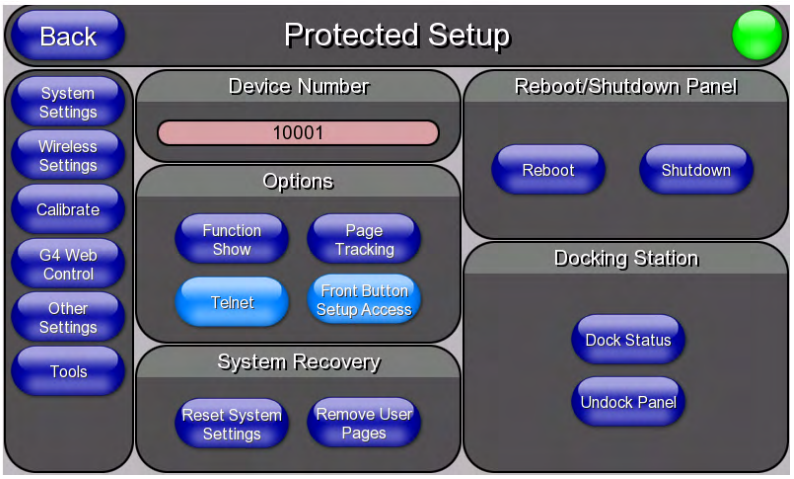


FIG. 18 Protected Setup page

NOTE

*The default password for the Protected Setup page is **1988**, but this may be changed at any time.*

For more information on the *Setup* and *Protected Setup* pages, refer to the *Setup Pages* section on page 47 and the *Protected Setup Pages* section on page 59.

Download from Www.Somanuals.com. All Manuals Search And Download.

Setting the Panel's Device Number

In the *Protected Setup* page:

1. Press the *Device Number* field in the *Device ID* section to open the *Device Number* keypad.
2. Enter a unique Device Number assignment for the device**,** and press **Done** to return to the *Protected Setup* page. The Device Number range is 1 - 32000, and the default is **10001**.
3. Press **Reboot** to reboot the device and apply the new Device Number.

Wireless Settings - Wireless Access Overview

DHCP

When choosing DHCP, a DHCP server must be accessible before the fields are populated.

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.

The parameters of the wireless card must be set before selecting **Ethernet** as the Master Connection Type. **The Wireless Access Point communication parameters must match those of the pre-installed wireless CF card inside the device.**

MVP touch panels connect to a wireless network through their use of the pre-installed AMX 802.11g wireless interface card. This allows users to communicate with a Wireless Access Point (WAP). The WAP communication parameters must match those of the pre-installed wireless interface card installed within the panel. This internal card transmits data using 802.11x signals at 2.4 GHz. For a more detailed explanation of the new security and encryption technology, refer to the *Appendix B: Wireless Technology* section on page 162.

For more information on utilizing the AMX Certificate Upload Utility in conjunction with the EAP security, refer to the *AMX Certificate Upload Utility* section on page 168.

Download from Www.Somanuals.com. All Manuals Search And Download.

Configuring Wireless Network Access

The first step in connecting the MVP-5200i to a wireless network is to configure the wireless communication parameters within the device's *Wireless Settings* page. This page only configures the card to communicate to a target WAP: **the device must still be directed to communicate with the correct Master**. This "pointing to a Master" is done via the *System Settings* page, which allows configuration of the IP Address, System Number and Username/Password information assigned to the target Master.

Step 1: Configure the Device's Wireless IP Settings

The first step to a successful setup of the internal wireless card is to configure the *IP Settings* section on the *Wireless Settings* page. This 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. 19).

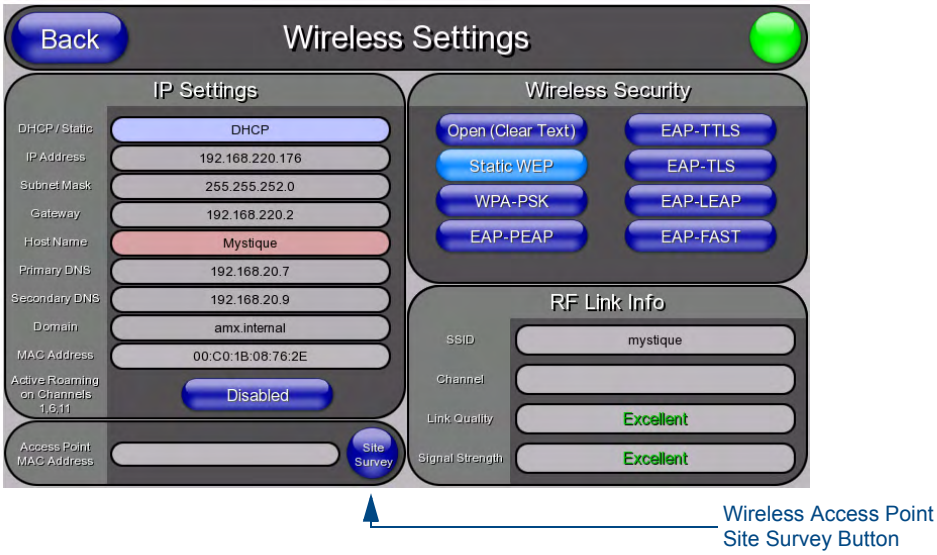


FIG. 19 Wireless Settings page (IP Settings section)

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.

NOTE

DHCP will register the unique factory-assigned MAC Address 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 the *Host Name* keyboard and enter the host name information.
4. Press **Done** after assigning the alpha-numeric string of the host name.
5. The remaining greyed-out fields in the *IP Settings* section cannot be altered. Once the panel is rebooted, these values are obtained by the unit and displayed in the *DNS* fields after power-up.

Download from Www.Somanuals.com. All Manuals Search And Download.

NOTE

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

6. Set up 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 25 for detailed procedures to setup either a secure or insecure connection.

Wireless communication using a Static IP Address

1. From the *Protected Setup* page, press the **Wireless Settings** button to open the *Wireless Settings* page. Wireless communication is set within the IP Settings section of this page (FIG. 19).

NOTE

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

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 turn red, noting that they are now user-editable.
3. Press the *IP Address* field to open a keyboard and enter the Static IP Address provided by the System Administrator. Press **Done** after entering the IP address information and repeat the same process for the *Subnet Mask* and *Gateway* fields.
4. Press the optional *Host Name* field to open the keyboard and enter the Host Name information. Press **Done** after assigning the alpha-numeric string of the host name.
5. Press the **Primary DNS** field to open a Keyboard, enter the Primary DNS Address (provided by the System Administrator) and press **Done** when compete. Repeat this process for the Secondary DNS field.
6. Press the **Domain** field to open a Keyboard, enter the resolvable domain Address (this is provided by the System Administrator and equates to a unique Internet name for the panel), and press **Done** when complete.
7. Set up 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 set up either a secure or unsecure connection.

Download from Www.Somanuals.com. All Manuals Search And Download.

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 wireless card (FIG. 20). Once the **Site Survey** button is pressed, the device displays the *Site Survey* page, which contains the following categories:

- **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** - displaying None, Poor, Fair, Good, Very Good, and Excellent
- **MAC Address** - Unique identification of the transmitting Access Point

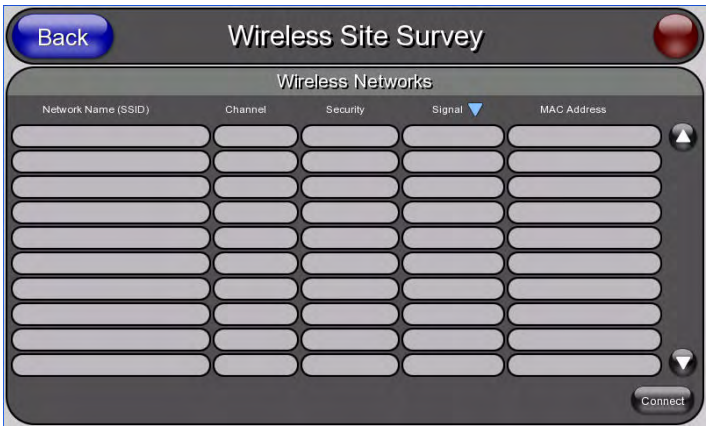


FIG. 20 Site Survey page

To access the Site Survey Tool:

1. From the *Protected Setup* page, press the **Wireless Settings** button to open the *Wireless Settings* page.
2. Press the **Site Survey** button. This action launches the *Wireless 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 fields.
   - 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 not broadcast, it will not show up on the *Wireless Networks* 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 track access points as they move in and out of range.
3. Sort the information provided on this page by pressing on a column name. This moves the sorting arrow to that column, where it may be toggled up or down.
   - **Up arrow** - indicates that the information is being sorted in an ascending order.
   - **Down arrow** - indicates that the information is being sorted in a descending order.

Download from Www.Somanuals.com. All Manuals Search And Download.

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 ten or fewer access points are detected. If more are detected, 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. From there, either **Cancel** the operation or fill in any necessary information fields and then click **Save**.
   Selecting an Open, WEP, and WPA-PSK Access Point and then clicking **Connect** will open the corresponding Settings page. For any other security mode, clicking **Connect** will only return to the previous page without any information being entered.
   - In an *Open* security mode, after selection and connection to a target WAP, the SSID name of the selected WAP is saved for the open security mode.
   - In a *Static WEP* security mode, after selection and connection to a WEP Access Point, the user is then redirected back to the *Static WEP* security screen, where the *SSID* field is already filled out. 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 situation, the security mode switches back to the previous page and security and connection parameters must be entered in as usual.

Download from Www.Somanuals.com. All Manuals Search And Download.

Step 2: Configure the Card's Wireless Security Settings

The second step in setting up the 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 for an 802.11g card facilitate a common security configuration to a target WAP.***

Refer to the Appendix B: Wireless Technology section on page 162 *for more information on other security methods.*

After setting up the wireless card parameters, configure the communication parameters for the target Master; see *Step 3: Choose a Master Connection Mode* section on page 31.

Configuring the device's wireless card for unsecured access to a WEP

In the *Protected Setup* page:

1. Press the **Wireless Settings** button (located on the lower-left) to open the *Wireless Settings* page (FIG. 21).

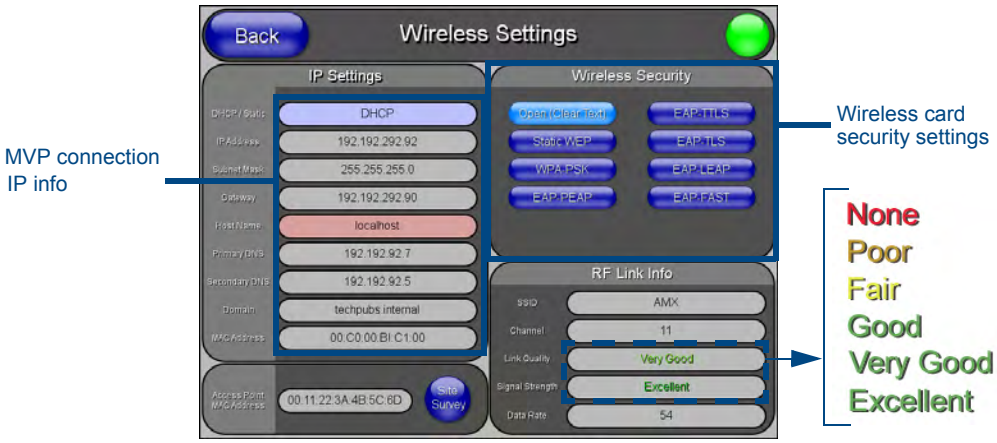


FIG. 21 Wireless Settings page (showing a sample unsecured configuration)

2. Enter the SSID information by:

   - Automatically filling it by pressing the **Site Survey** button. From the *Site Survey* page, choosing an ***Open*** WAP from within the *Site Survey* page and then pressing the **Connec**t button at the bottom of the page (FIG. 22).

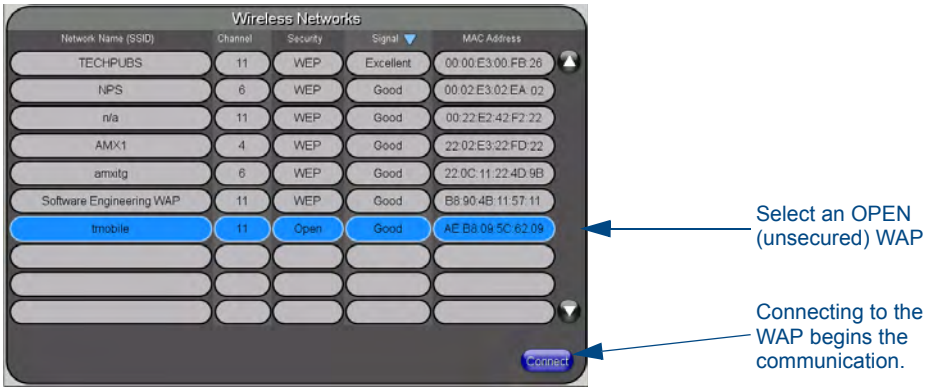


FIG. 22 Site Survey of available WAPS (Unsecured WAP shown selected)

   - Manually entering the SSID information into the appropriate fields by following steps 7 through 9.

Download from Www.Somanuals.com. All Manuals Search And Download.

3. From within the *Wireless Security* section, press the **Open (Clear Text)** button to open the *Open (Clear Text) Settings* dialog (FIG. 23). An Open security method does not utilize any encryption methodology, but does require that an alpha-numeric SSID be entered. This method sends out network packets as unencrypted text.

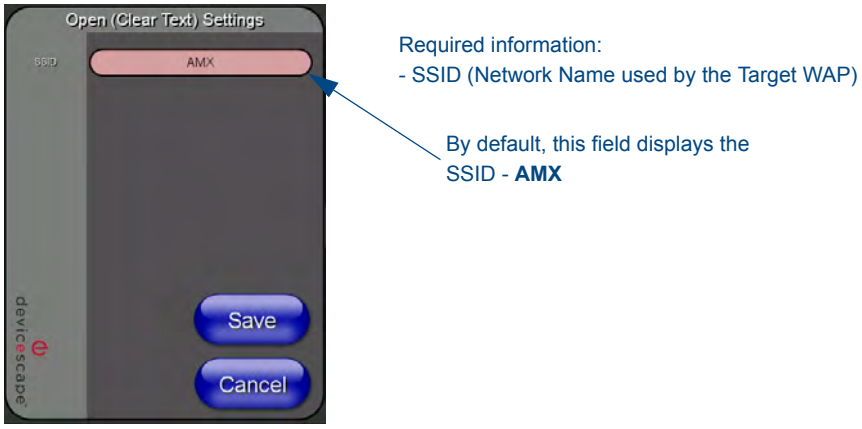


FIG. 23 Wireless Settings page - Open (Clear Text) security method

4. Press the red *SSID* field to display an on-screen *Network Name (SSID)* keyboard.
5. In this keyboard, enter the SSID name used on the 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 involves an incorrect SSID. Make sure to maintain the same case when entering the SSID information. ***ABC is not the same as Abc***.
6. Click **Done** when complete.
7. From the *Open (Clear Text) Settings* page (FIG. 23), press the **Save** button to incorporate the new information into the device and begin the communication process.
8. Verify the proper configuration in the fields in the *IP Settings* section. Refer to *Step 1: Configure the Device'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 save any changes and restart the device. ***Remember that the connection must be configured to a target Master from the System Settings page.***
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. 21).

NOTE

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Automatically setting SSID

In the *Protected Setup* page:

1. Select **Wireless Settings**.
2. Press the **Site Survey** button at the bottom of the page.
3. Select a **WEP** secured WAP from within the *Site Survey* page, and press the **Connect** button (FIG. 24). .

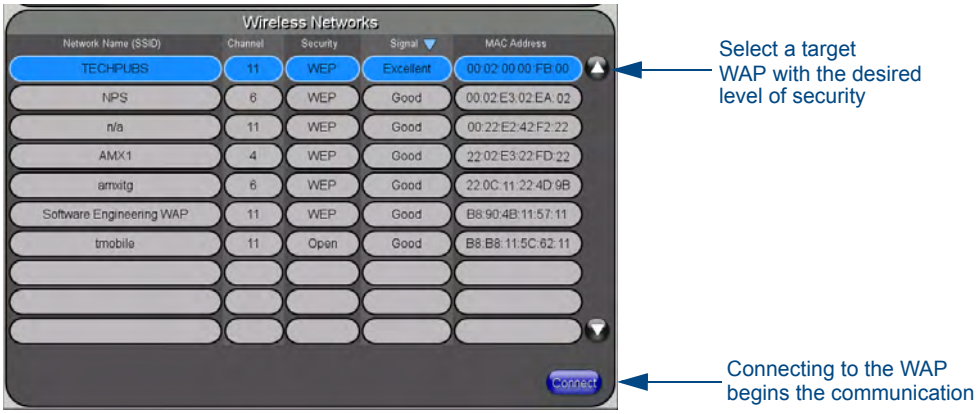


FIG. 24 Site Survey of available WAPs (Secured WAP shown selected)

4. If the security is not handled automatically, the information must be entered manually from the *Wireless Security* menu.

Manually setting SSID

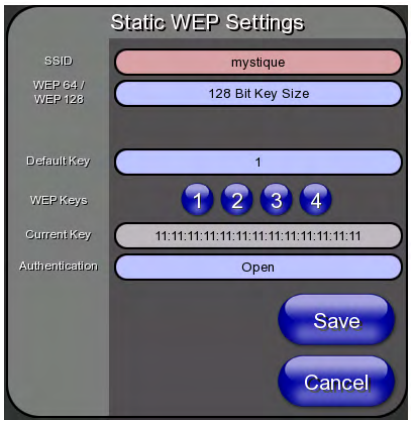
From the *Protected Setup* page:

1. Select **Wireless Settings**.
2. Locate the *Wireless Security* menu (FIG. 25).

FIG. 25 Wireless Security page

Download from Www.Somanuals.com. All Manuals Search And Download.

3. Press the **Static WEP** button to open the *Static WEP Settings* dialog (FIG. 26).



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

FIG. 26 Wireless Settings page - Static WEP security method

4. Press the *SSID* field. From the *Network Name (SSID)* keyboard, enter the SSID name used by the 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 device will attempt to connect to the first available WAP.
   - One of the most common problems associated with connection to a WAP arises because of an improperly entered SSID. The same case must be maintained when entering this information. ***ABC is not the same as Abc***.
   - The alpha-numeric string is **AMX** by default, 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 the SSID is **TECHPUBS**, **this word and the case** within must match 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. 26) 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 the Wireless Access Point has been set to default key 4 (which was 01:02:03:04:05), the panel's key 4 must be set to 01:02:03:04:05.

6. Toggle the *Default Key* field to choose a WEP Key value (**from 1- 4**) that matches what will be used on the target. **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 the target WAP is to generate the Current Key, do not press the Generate button. Instead, continue with Step 13.

Download from Www.Somanuals.com. All Manuals Search And Download.

8. Within the WEP Passphrase keyboard (FIG. 27), enter a character string or word (such as ***AMXPanel***) and press **Done** when finished.

FIG. 27 WEP Passphrase Keyboard

- For 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. 28).

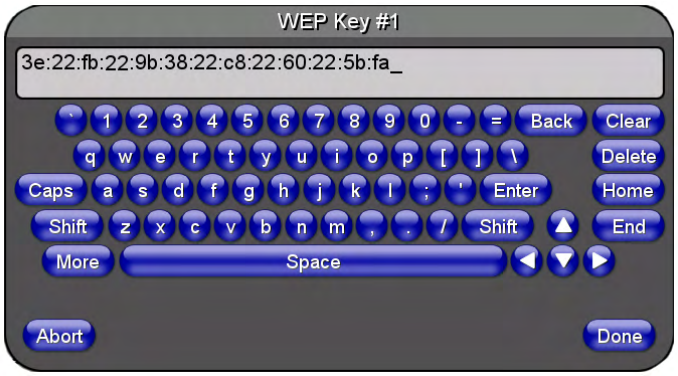


FIG. 28 WEP Key # Keyboard

9. Write down this Current Key string value for later entry into the WAP's *WEP Key* field (*typically entered without colons*) and into other communicating panel's *Current Key* field.
10. **If entering a Current Key generated either by the target WAP or another Modero panel**, within the *WEP Keys* section, touch the **Key #** button to launch the *WEP Key #* keyboard, enter the characters and press **Don**e 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.

NOTE

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

11. The remaining *Current Key* and *Authentication* fields are greyed-out and cannot be altered by the user.

Download from Www.Somanuals.com. All Manuals Search And Download.

12. Verify that the fields within the *IP Settings* section have been properly configured. Refer to *Step 1: Configure the Device'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 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**.

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

Configuring multiple wireless touch panels to communicate to a target WEP

1. For each communicating touch panel, complete all of the steps outlined within the previous section on page 26.
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.**

Download from Www.Somanuals.com. All Manuals Search And Download.

Step 3: Choose a Master Connection Mode

The MVP-5200i requires a decision on the type of connection to be made between it and the Master.

To establish a Master connection:

1. From the *Protected Setup* page, select **System Settings**.
2. Select *Type* to toggle between the Master Connection Types *USB* and *Ethernet* (FIG. 29).
   - 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

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

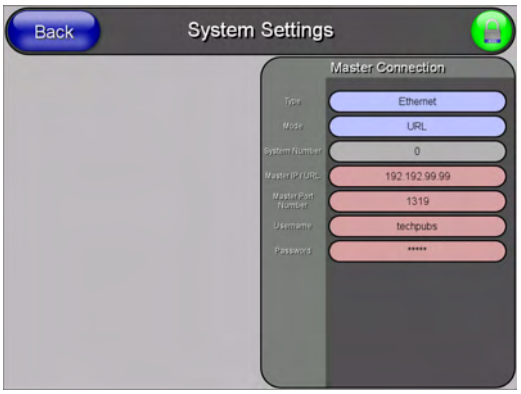


FIG. 29 System Settings page

Ethernet over USB

The MVP-5200i device is the first G4 device to support a new Ethernet over USB driver for panel downloads and firmware updates. This means that the device can connect to a host computer for updates through its Mini USB port instead of through a standard Ethernet port (FIG. 30).

FIG. 30 USB Port on the MVP-5200i

Because of its Ethernet over USB capabilities, the MVP-5200i also follows a different procedure for downloading firmware than with other G4 devices. Firmware downloads require use of the USB Programming Cable (**FG10-5965**) and a computer running Windows XP.

Download from Www.Somanuals.com. All Manuals Search And Download.

Touch panel setup

To prepare the MVP-5200i for Ethernet for USB communication:

1. Turn on the MVP-5200i and wait for the device to finish booting up.
2. Insert the mini-USB end of the USB Programming Cable into the mini-USB port on the device. Insert the other end into the appropriate USB port on the computer containing the files to be downloaded.
3. If the connection goes well, the Windows XP machine will detect the device as an unsupported USB device. It then presents a dialogue box that prompts the user for a suitable driver (FIG. 31):

FIG. 31 Found New Hardware Wizard dialogue box

4. Select *Yes, this time only* and click on **Next**.
5. In the next box (FIG. 32), select *Install from a list or specific location (Advanced)* and click on **Next**.

FIG. 32 Found New Hardware Wizard software search box

Download from Www.Somanuals.com. All Manuals Search And Download.

6. In the next box (FIG. 33), make sure to:
   - Select *Search for the best driver in these locations*
   - Select *Include this location in the search*
   - Click on **Browse**
   - Select the folder that contains the 'linux.inf' file

FIG. 33 Found New Hardware Wizard Installation Options dialogue box

7. Click on **Next**.
8. The Windows XP machine now searches for the suitable driver (FIG. 34).

FIG. 34 Found New Hardware Wizard while searching for the driver

Download from Www.Somanuals.com. All Manuals Search And Download.

9. Once the system finds the driver, it displays its choice (FIG. 35). Click **Finish** to complete the driver installation.

FIG. 35 Completing the Found New Hardware Wizard

When an IP address is assigned to the usb0 interface on the device, Windows XP will make an attempt to assign an IP address to the corresponding interface on the Windows side. Usually, this IP address is a random value and in a totally different subnet. The user may set the Windows network properties for the Ethernet over USB interface to have a specific address whenever the Windows XP system detects an MVP-5200i with an assigned IP address.

In Windows XP:

1. From the Windows XP desktop, click on **Start > Settings > Network Connections**. This opens a window listing the currently active network connections.
2. Select the connection that is specific to *AMX USB Device Link*.
3. Right click and select **Properties**.
4. In the Local Area Connection 3 Properties window (FIG. 36) under the **General** tab, select *Internet Protocol (TCP/IP)* and click on **Properties**.

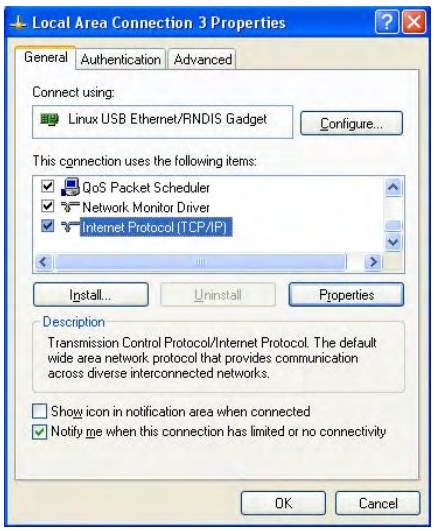


FIG. 36 Local Area Connection 3 Properties

Download from Www.Somanuals.com. All Manuals Search And Download.

5. In the new window:
   - Select *Use the following IP Address*.
   - Under *IP address*, provide an IP address (ensure that it is in the same subnet as the IP address given to the usb0 interface on the MVP-5200i).
   - Under *Subnet mask*, set the suitable subnet mask.
   - Click on **OK**'
6. In the *Local Area Connection 3 Properties* window, click on **OK**.

The user should now be able to run any TCP/IP application between the two systems.

Configure a Virtual NetLinx Master using NetLinx Studio

A Virtual NetLinx Master (VNM) is used when the target panel is not actually 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. If using the mini-USB connection, verify the panel has been configured to communicate via USB within the *System Settings* page and that the USB driver has been properly configured. Changing the Master Connection type requires a reboot before the change takes effect.
2. In NetLinx Studio, select **Settings > Master Communication Settings**, from the Main menu to open the *Master Communication Settings* dialog (FIG. 37).

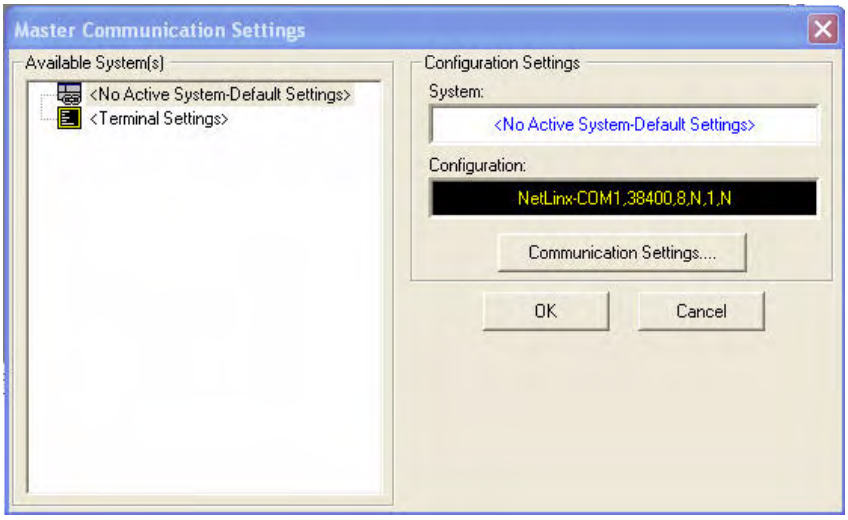


FIG. 37 Master Communications Settings dialog box

Download from Www.Somanuals.com. All Manuals Search And Download.

3. Click the **Communications Settings** button to open the *Communications Settings* dialog (FIG. 38).

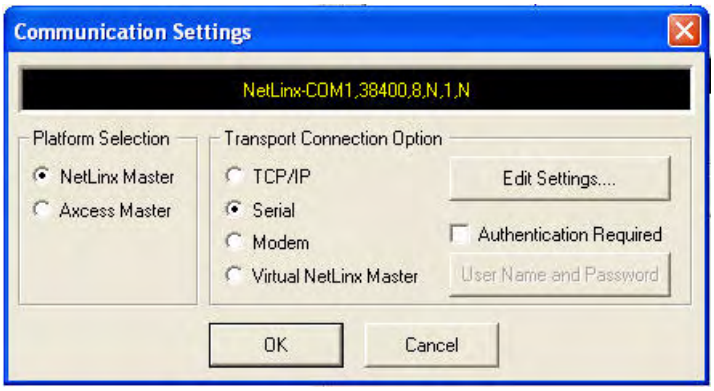


FIG. 38 Communications Settings dialog box

4. Click the **NetLinx Master** radio button in the *Platform Selection* section.
5. Click the **Virtual NetLinx Master** radio button in the *Transport Connection Option* section.
6. Click the **Edit Settings** button to open the *Virtual NetLinx Master Settings* dialog (FIG. 39).

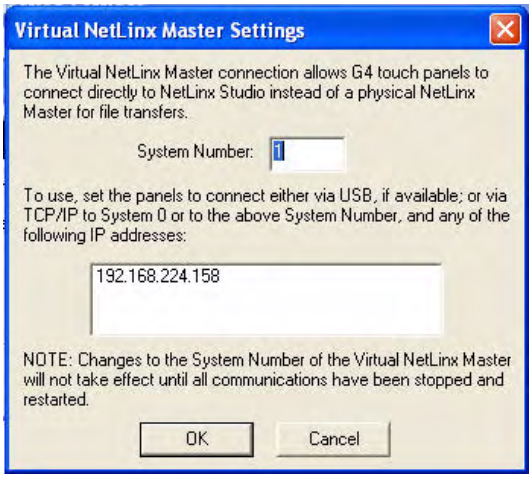


FIG. 39 Virtual NetLinx Master Settings dialog box

7. Enter the System number; the default is **1**.
8. Click **OK** on all open dialogs to 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 **System Connection** status button turns green after a few seconds to indicate an active USB connection to the PC via the Virtual Master.
    - If the *System Connection* icon does not turn green, check the USB connection and communication settings and refresh the system.

Download from Www.Somanuals.com. All Manuals Search And Download.

Ethernet

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

Connection Modes		
Mode	**Description**	**Procedures**
None	No connection	None
Auto	The device connects to the first master that responds. This setting requires setting the System Number.	Setting the System Number: 1. Select the *System Number* to open the keypad. 2. Set your System Number and select **Done**.
URL	The device connects to the specific IP of a Master via a TCP connection. This setting requires setting the Master's IP.	Setting the Master IP: 1. Select the *Master IP* number to the keyboard. 2. Set the Master IP and select **Done**.
Listen	The device "listens" for the Master to initiate contact. This setting requires providing the Master with the device's IP.	Confirm that the device IP is on the Master URL list. 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 the Master Port and select **Done**.
4. If you enabled password security on your Master, set the username and password within the device.
5. Select the blank field *Username* to open the keyboard.
6. Set the Username and select **Done**.
7. Select the blank field *Password* to open the keyboard.
8. Set the Password and select **Done**.
9. Press the **Back** button to return to the *Protected Setup* page.
10. Press the **Reboot** button to reboot the device and confirm changes.

Download from Www.Somanuals.com. All Manuals Search And Download.

Master Connection to a Virtual Master via Ethernet

NOTE

When configuring the 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. Make sure to use the Virtual System value assigned to the Virtual Master within NetLinx Studio.

Before beginning:

1. Verify that the panel has been configured to communicate with the Wireless Access Point and confirm that the signal strength quality bargraph is *On*.
2. In NetLinx Studio, select **Settings > Master Communication Settings** from the *Main* menu to open the *Master Communication Settings* dialog (FIG. 40).

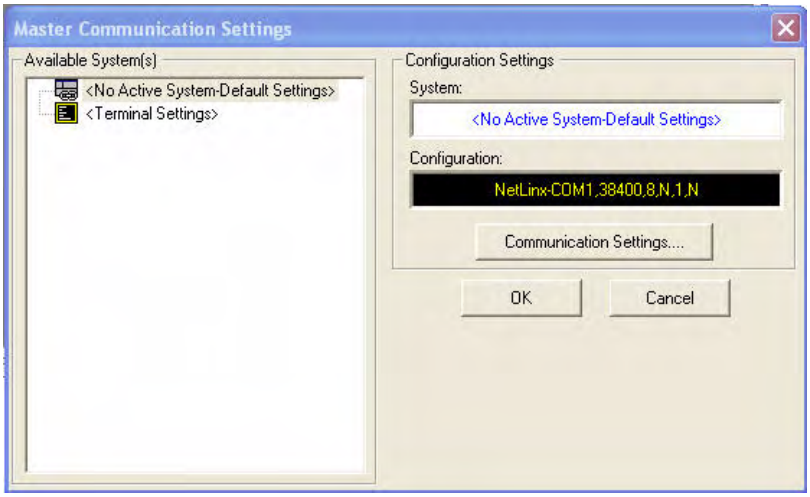


FIG. 40 Master Communications Settings dialog box

3. Click the **Communications Settings** button to open the *Communications Settings* dialog (FIG. 41).

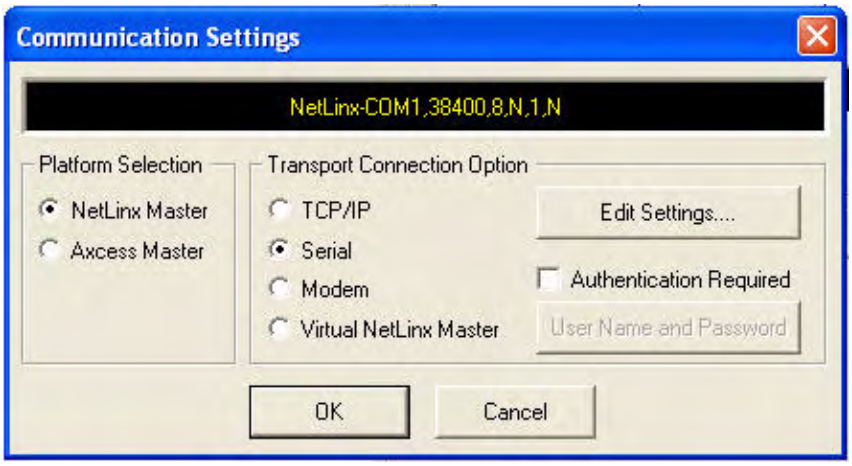


FIG. 41 Communications Settings dialog box

4. Click on the **Virtual NetLinx Master** radio button (*from the Platform Selection section*) to indicate that you are working as a NetLinx Master.

Download from Www.Somanuals.com. All Manuals Search And Download.

5. Click on the **Virtual NetLinx Master** radio box from the *Transport Connection Option* section to indicate wanting to configure the PC to communicate with a panel. Everything else, such as the Authentication, is greyed out because the procedure is not being made through the Master's UI.
6. Click the **Edit Settings** button in the *Communications Settings* dialog to open the *Virtual NetLinx Master Settings* dialog (FIG. 42).

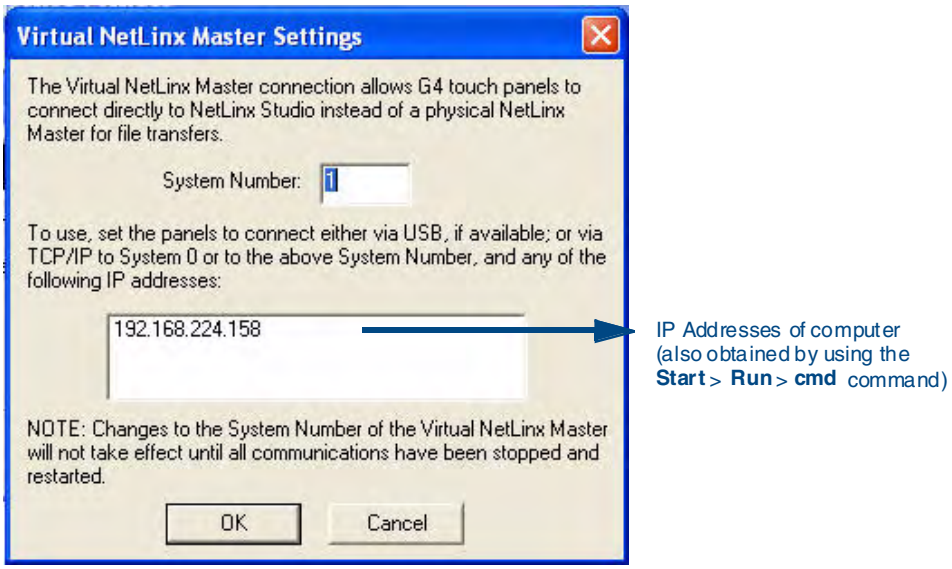


FIG. 42 Virtual NetLinx Master Settings dialog box

7. 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 the 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.
8. Click **OK** to close the open dialogs, save the 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.
11. Place the panel in the Table Charging Station or in the Wall Charging Station and turn the panel *On*.
12. After the panel powers up, press and hold down the navigation wheel center button **for 3 seconds** to continue with the setup process and proceed to the *Setup* page.

Download from Www.Somanuals.com. All Manuals Search And Download.

13. Select **Protected Setup > System Settings** (located on the lower-left) to open the *System Settings* page (FIG. 43).

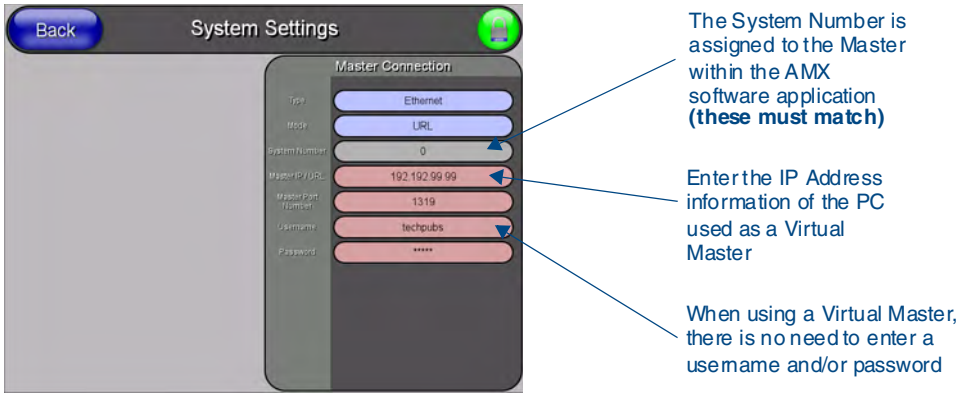


FIG. 43 Sample System Settings page (for Virtual Master communication)

14. Press the blue *Type* field (***from the Master Connection section***) until the choice cycles to the word **Ethernet.**
15. 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.
16. Press the *Master IP/URL* field to open a Keyboard and enter the IP Address of the PC used as the Virtual Master.
17. Click **Done** to accept the new value and return to the *System Settings* page.
18. Do not alter the *Master Port Number* value, as this is the default value used by NetLinx.
19. Press the **Back** button to open the *Protected Setup* page.
20. Press the on-screen **Reboot** button to save any changes and restart the panel.

Download from Www.Somanuals.com. All Manuals Search And Download.

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 Page* section on page 85 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 the 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 the appropriate password into the Keypad's password field (***1988** is the default password with a new unit*) and press **Done**.
4. Press the **G4 WebControl** button to open the *G4 Web Control* page (FIG. 44).

FIG. 44 G4 Web Control page

5. Press the **Enable/Enabled** button until it toggles to **Enabled** and turns light blue.
6. 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 the device has no Ethernet cable connection.

7. Press the *Web Control Name* field to open the *Web Name* keyboard.

Download from Www.Somanuals.com. All Manuals Search And Download.

8. 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. 45).

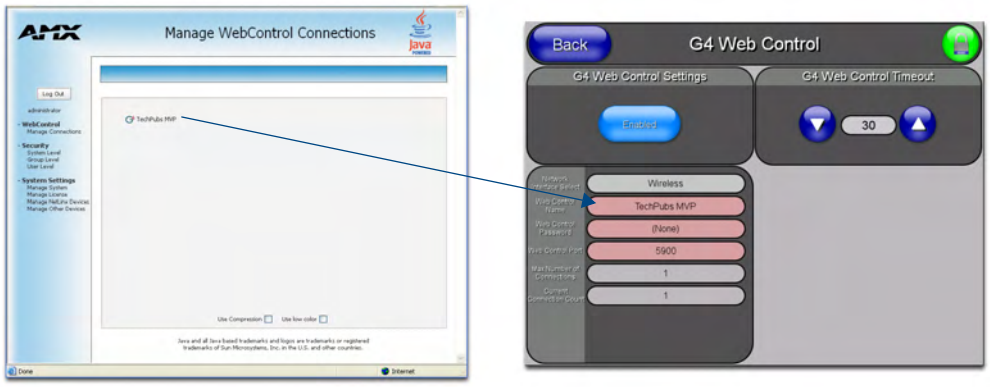


FIG. 45 Sample relationship between G4 Web Control and Mange WebControl Connections window

9. Assign the alpha-numeric string for the Web Control name and then press **Done**.
10. Press the *Web Control Password* field to open the *Web Password* keyboard.
11. 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.
12. Press **Done** after assigning the alpha-numeric string for the Web Control password.
13. Press the *Web Control Port* field to open the *Web Port Number* keypad.
14. Within the keypad, enter a unique numeric value to be assigned to the port on which the VNC Web Server is running. The default value is ***5900***. Press **Done** after entering the value. The remaining fields within the *G4 Web Control Settings* section of this page are read-only and cannot be altered.
15. Press the **Up/Down** arrows on either sides of the G4 Web Control *Timeout* field to increase or decrease the amount of time the device can remain idle *with no cursor movements* before the session is closed and the user is disconnected.
16. Press the **Back** button to open the *Protected Setup* page.
17. Press the on-screen **Reboot** button to save any changes and restart the device.

NOTE

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Using the NetLinx Master to control the G4 panel

Refer to the 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 make full use of the SSL encryption, the web browser used should incorporate 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 (***example: 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. This page (FIG. 46) 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 that were previously set up and activated on the device.

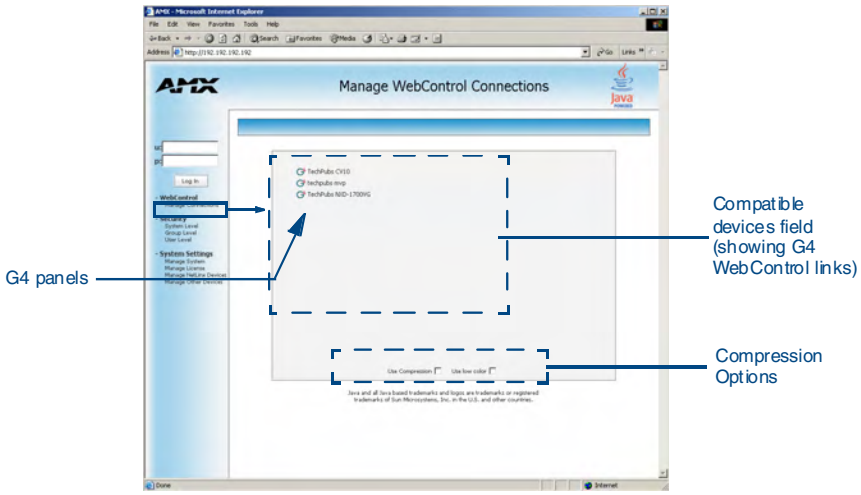


FIG. 46 Manage WebControl Connections page (populated with compatible panels)

Download from Www.Somanuals.com. All Manuals Search And Download.

5. Click on the G4 panel name link associated with the target panel. A secondary web browser window appears on the screen (FIG. 47).

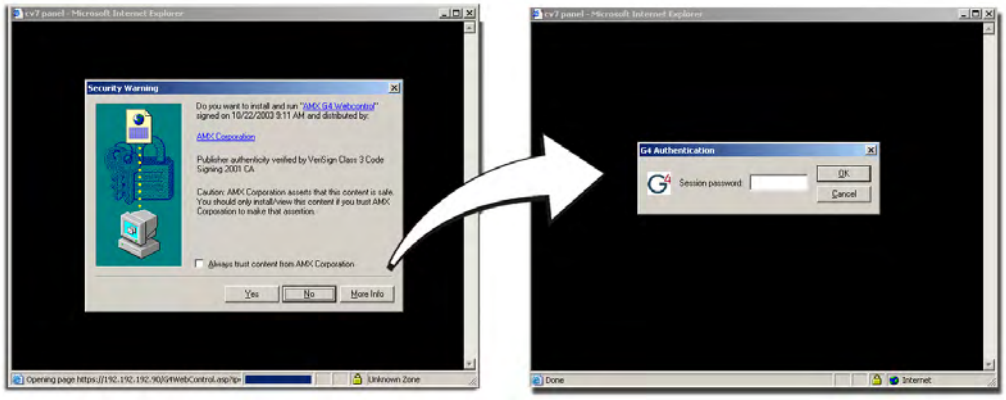


FIG. 47 Web Control VNC installation and Password entry screens

6. 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.

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.

7. Some situations might display a *Connection Details* dialog (FIG. 48) requesting a VNC Server IP Address. This is the IP Address not of the Master but of the target touch panel. Depending on which method of communication is being used, it can be found in either:

   - **Wired Ethernet** - System Settings > IP Settings section within the *IP Address* field.
   - **Wireless** - Wireless Settings > IP Settings section within the *IP Address* field.

   If this field does not appear, continue to step 9.

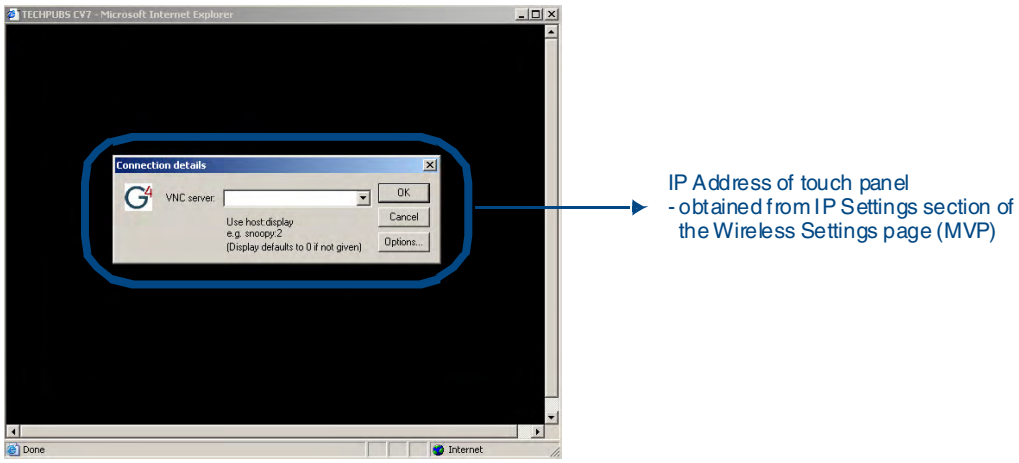


FIG. 48 Connection Details dialog

8. If a WebControl password was set up on the *G4 WebControl* page, a *G4 Authentication Session* password dialog box appears on the screen within the secondary browser window.

Download from Www.Somanuals.com. All Manuals Search And Download.

9. Enter the Web Control session password into the *Session Password* field (FIG. 48). *This password was previously entered into the Web Control Password field within the G4 Web Control page on the panel.*
10. 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 is then 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.

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

Setup Pages

The MVP-5200i features 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 center button of the navigation wheel and hold for 3 to 5 seconds (FIG. 49).

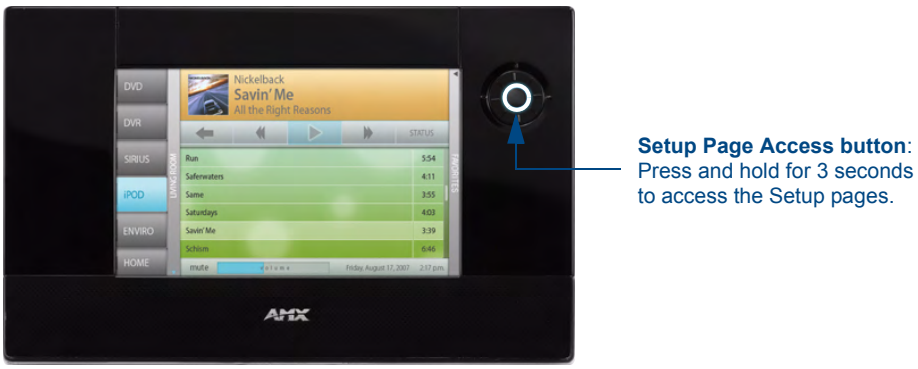


FIG. 49 Setup Page Access buttons

Setup Pages

The *Setup* page (FIG. 50) allows quick access to several essential panel properties:

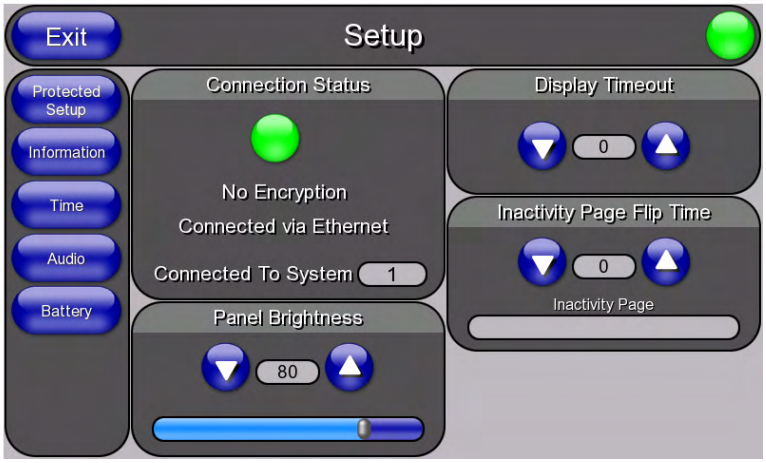


FIG. 50 MVP-5200i main Setup page

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).
Connection Status icon:	The icon in the upper-right corner of each Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*

Download from Www.Somanuals.com. All Manuals Search And Download.

Setup Page (Cont.)	
Connection Status:	Displays whether the panel is has external communication, as well as the encryption status of the Master, the connection type (***Ethernet*** *or* ***USB***), and to which System the panel is connected. • Until a connection is established, the message displayed is: "*Attempting via Ethernet*" or "*Attempting via USB*". • When a connection is established, the message displayed is either: "*Connected via Ethernet* "or "*Connected via USB* ". • The word "*Encrypted*" appears when an encrypted connection is established with a NetLinx Master. ***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 device to power down. • Press the Up/Down buttons to increase/decrease the Display Timeout setting in 5-second increments. Range = 0 - 30 (seconds). • Set the timeout value to 0 to disable Sleep mode. ***Note****: Small timeout values maximize the life of the battery charge.*
Inactivity Page Flip Timeout:	Indicates the length of time that the panel can remain idle before automatically flipping to a pre-selected page. • Press the Up/Down buttons to increase/decrease the Inactivity Page Flip Timeout setting. Range = 0 - 240 (minutes). • Set the timeout value to 0 to disable Inactivity Page Flip mode. ***Note****: The touch panel page used for the Inactivity page flip is named within a small Inactivity Page field below the buttons.*
Panel Brightness:	Sets the display brightness and contrast levels of the panel. • Press the Brightness Up/Down buttons to adjust the brightness level. Range = 0 - 100. **NOTE:** Be careful not to turn down the brightness too low to be able to see the Setup page.

Download from Www.Somanuals.com. All Manuals Search And Download.

Navigation Buttons

The following Navigation buttons (FIG. 51) appear on the left side of the Setup page:

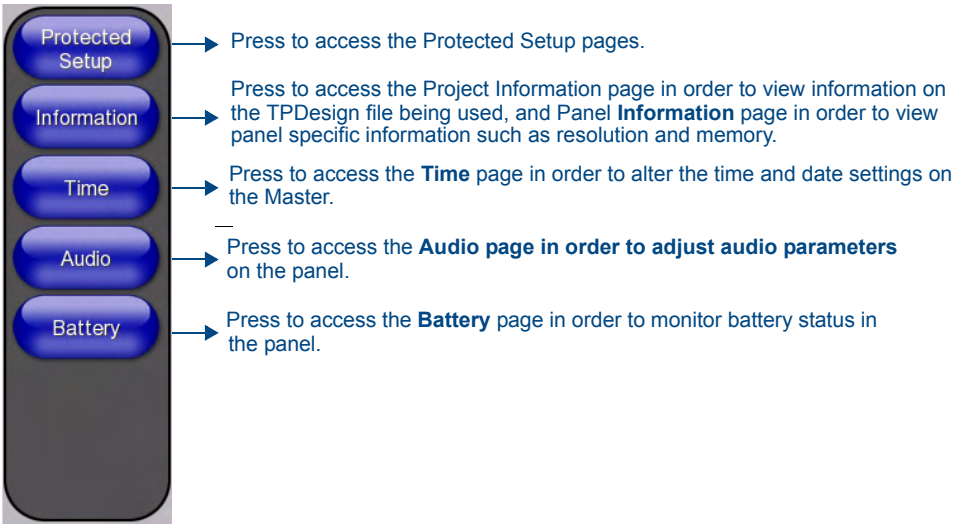


FIG. 51 Setup Page Navigation Buttons

Protected Setup Pages

Information on the *Protected Setup* pages is available on page 59.

Download from Www.Somanuals.com. All Manuals Search And Download.

Information Button

The **Information** button allows access of both the *Project Information* page, which contains data on the TPDesign4 file being used with the MVP-5200i, and the *Panel Information* page, which contains detailed information on the panel itself. To access these pages:

1. Press and hold the **Information** button until the **Project Information** button and the **Panel Information** button slide from the left.

NOTE

*The **Project Information** and the **Panel Information** buttons will be displayed for three seconds before they slide back behind the **Information** button, whether or not the **Information** button is still being pressed.*

2. Press the appropriate button for the information required.
3. To return to the *Setup* page, press the **Back** button.

Project Information Page

The Project Information page displays the project properties of the TPDesign4 project file currently loaded on the panel (FIG. 52).

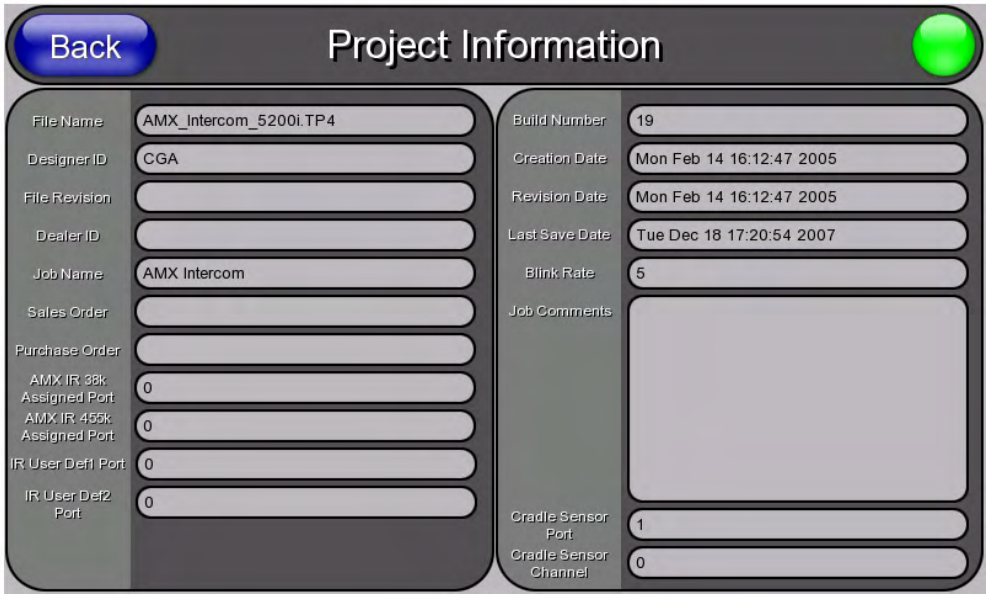


FIG. 52 Project Information page

Features on this page include:

Project Information Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Setup page provides a constant visual indication of current connection status. ***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.

Download from Www.Somanuals.com. All Manuals Search And Download.

Project Information Page (Cont.)	
Sales Order:	Displays the sales order information.
Purchase Order:	Displays the purchase order information.
AMX IR 38K Assigned Port:	Displays the AMX 38 kHz IR channel port used by the IR Emitter on the panel. • This information is specified in TPD4 (Project Properties > IR Emitters & Receivers tab). • 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 Assigned Port:	Displays the AMX 455 kHz IR channel port used by the IR Emitter on the panel.
IR User Def1 Port:	Displays the primary channel port used by the IR receiver on the panel.
IR User Def2 Port:	Displays the secondary channel port used by the IR receiver 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 used by the charging cradle sensor.
Cradle Sensor Channel:	Displays the channel used to broadcast the charging cradle sensor status.

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Panel Information Page

The Panel Information page provides detailed panel information (FIG. 53).

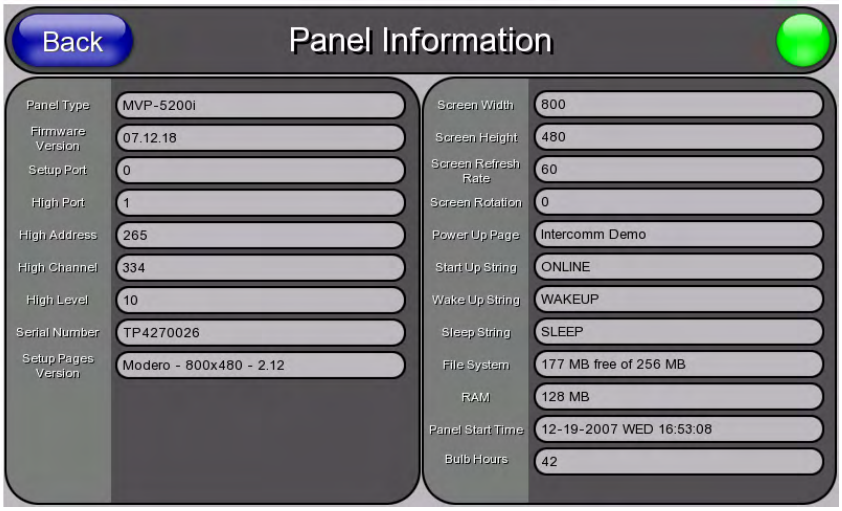


FIG. 53 Panel Information page

Features on this page include:

Panel Information Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Setup page provides a constant visual indication of current connection status. ***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). MVP-5200i = 640 pixels.
Screen Height:	Displays the screen height (in pixels). MVP-5200i = 480 pixels.
Screen Refresh Rate:	Displays the video refresh rate applied to the incoming video signal.
Screen Rotation:	Displays the degree of rotation applied to the on-screen image.
Power Up Page:	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.
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 time taken by the panel to wake up from sleep mode.
Bulb Hours:	Displays the number of hours elapsed with the display on full power.

Download from Www.Somanuals.com. All Manuals Search And Download.

Time & Date Settings Page

The options on the Time & Date Settings page (FIG. 54) allows setting and adjusting of 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.

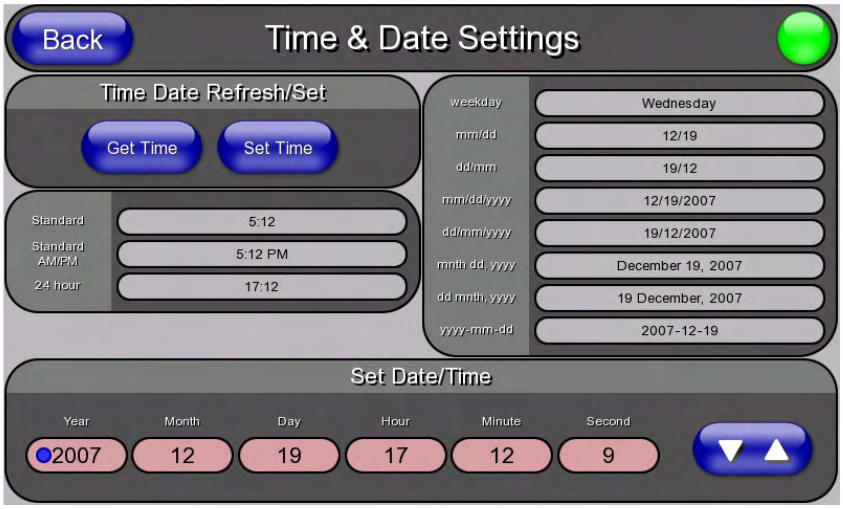


FIG. 54 Time and Date Setup page

NOTE

The MVP-5200i does not have an on-board clock, so 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.
Connection Status icon:	The icon in the upper-right corner of each Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*
Time Date Refresh/Set:	• The **Get Time** button retrieves Time and Date information from the Master. • The **Set Time** button retains and saves 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/Down arrow buttons to adjust the Master's calendar date and time. The blue icon indicates which field is currently selected. • **Year** range = 2000 - 2199 • **Month** range = 1 - 12 • **Day** range = 1 - 31 • **Hour** = 24-hour military • **Minute** range = 0 - 59 • **Second** range = 0 - 59

Download from Www.Somanuals.com. All Manuals Search And Download.

Audio Settings Page

The *Audio Settings* page allows adjustment of volume levels and panel sounds settings (FIG. 55).

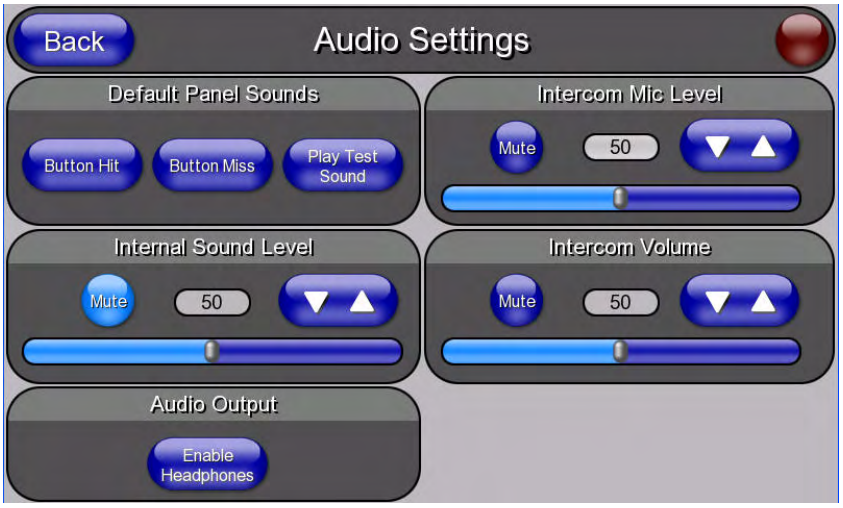


FIG. 55 Audio Settings pages

Features on these pages include:

Audio Settings Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Setup page provides a constant visual indication of current connection status. ***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: • Use the Up/Down buttons to adjust the volume level in 25-percent increments (range = 0 - 100). • The Master Volume bargraph indicates the current volume level. Press the bargraph to the left or right of the graph marker to adjust the volume level in one-percent increments (range = 0 - 100), or press the bargraph and hold to move the graph marker to the desired level. • The **Mute** button toggles the Mute feature.
Default Panel Sounds:	• Activating the **Button Hit** button plays a default sound when you touch an active button. • Activating the **Button Miss** button plays a default sound when you touch a non-active button or any area outside of the active button • The **Play Test Sound** button plays a test WAV/MP3 file over the panel's internal speakers.
Internal Sound Level:	Adjusts the volume level on the panel's internal speaker: • Use the Up/Down buttons to adjust the volume (range = 0 - 100) • The *Internal Sound Level* bargraph indicates the current sound level. Press the bargraph to the left or right of the graph marker to adjust the volume level in one-percent increments (range = 0 - 100), or press the bargraph and hold to move the graph marker to the desired level. • The **Mute** button mutes the internal speaker volume

Download from Www.Somanuals.com. All Manuals Search And Download.

Audio Settings Page (Cont.)	
Analog	
Line In Level:	Adjusts the volume level of any analog signal coming into the device: • Use the Up/Down buttons to adjust the input level (range = 0 - 100) • The Line In Level bargraph indicates the current input level. Press the bargraph to the left or right of the graph marker to adjust the volume level in one-percent increments (range 0 - 100), or press the bargraph and hold to move the graph marker to the desired level. • The **Mute** button mutes the line input.
Intercom	
Mic Level:	Adjusts the volume level on the intercom's microphone: • Use the Up/Down buttons to adjust the microphone level (range = 0 - 100). Press the bargraph to the left or right of the graph marker to adjust the volume level in one-percent increments (range 0 - 100), or press the bargraph and hold to move the graph marker to the desired level.
Intercom Volume:	Sets the volume level for intercom calls from another MVP-5200i: • Use the Up/Down buttons to adjust the Line-In volume level (range = 0 - 100). • The Line-In Level bargraph indicates the current Line-In level. Press the bargraph to the left or right of the graph marker to adjust the volume level in one-percent increments (range 0 - 100), or press the bargraph and hold to move the graph marker to the desired level. • The **Mute** button mutes the Line-In volume.
Audio Output	
Audio Output:	Enables USB headphone output.

WAV files - Supported sample rates

The following sample rates for WAV files are supported by MVP-5200i panels:

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Battery Settings Page

The options on the *Battery Settings* page allow setting of power warning preferences and battery status information, and adjustment of the display times for battery warnings (FIG. 56).

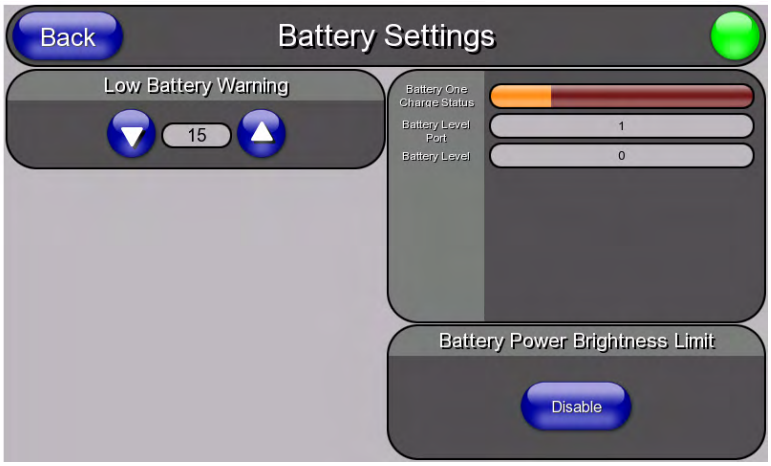


FIG. 56 Battery page

Features on this page include:

Battery Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*
Charge Status:	The **Charge Status** bargraph indicates the power charge available from the battery 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/Down buttons alter the timeout value (in minutes). A value of 0 disables this feature. Range = 0 - 240, default = 1200 min.
Low Battery Warning:	The Up/Down buttons adjust the time value (in minutes) available on the battery (for use) before the panel displays a low battery warning. Range - 10 - 45, default = 15 min.
Very Low Battery Warning:	The Up/Down 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). • Range = 3 - 15, default = 5 min. This value cannot exceed the Low Battery Warning value.
Battery One Charge Status:	The Battery One Charge Status field indicates the power charge currently available on the battery.
Battery One Quality:	The Battery One Quality field indicates the maximum charge the battery can take. Increased use and recharging of the battery will cause the battery's maximum charge to decrease over time.
Battery Level Port:	The **Battery Level Port** field indicates the port being used to report charge status levels back to the NetLinx Master (set in TPDesign4).
Battery Level:	The **Battery Level** field indicates the level being used to report status levels back to the NetLinx Master (set in TPDesign4).

Download from Www.Somanuals.com. All Manuals Search And Download.

Battery Page (Cont.)	
Battery Power Brightness Limit:	The DISABLE/DISABLED button acts as a power save feature with two options: • **Disable** - Clicking on this button deactivates this power save feature. The panel will use the Panel Brightness level. • **Disabled** - Clicking on this button activates the brightness limit set on the panel, conserving 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.

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

Protected Setup Pages

The *Protected Setup* page (FIG. 57) provides secured access to advanced panel configuration options, including communication and security settings. The Protected Setup page is accessed through the Setup page (please refer to the *Setup Pages* section on page 47).

To access the *Protected Setup* pages:

1. Press the center button of the navigation wheel and hold for 3 to 5 seconds to access the *Setup* pages.
2. Select the **Protected Setup** button on the left side of the screen.
3. Enter the factory default password (***1988)*** into the password keypad to access the page.

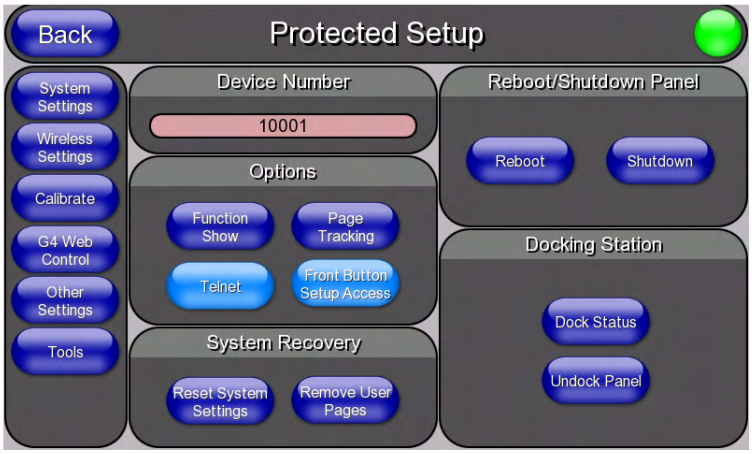


FIG. 57 Protected Setup page showing default values

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.
Connection Status icon:	The icon in the upper-right corner of each Protected Setup page provides a constant visual indication of current connection status. ***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 or change 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. 58). • **Telnet** - enables or disables the panel's telnet server, allowing or preventing direct telnet communication to the panel. • **Page Tracking** - toggles the page tracking function. When enabled, the panel reports page data to the NetLinx Master. • **Front Button Setup Access** - activates the navigation wheel for accessing the Setup and Calibration pages (see FIG. 57 on page 59). The default setting is On.

Download from Www.Somanuals.com. All Manuals Search And Download.

Protected Setup Page (Cont.)	
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. • **Remove User Pages** - Removes 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. 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/Shutdown Panel:	• Pressing the **Reboot** button causes the panel to reboot after saving any changes. • Pressing the **Shutdown** button causes the panel to shut down after saving any changes.
Docking Station	• **Dock Status** - Illuminates when the panel is docked and communicating with the Charging Station. • Undock Panel - Releases panel from Wall Mounted Charging Station.

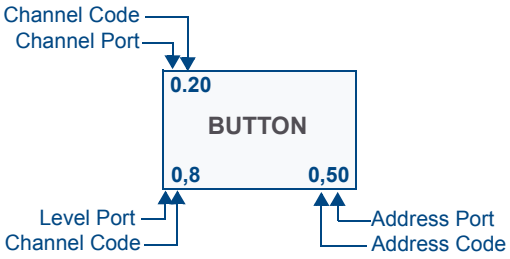


FIG. 58 Function Show example

NOTE

When the Function Show feature is displayed, the Channel Port and Code will appear in yellow, the Address Port and Code in green, and the Level Port and Channel Code in purple.

To reboot the panel:

1. Access the *Protected Setup* page.
2. Press the **Reboot** button.
3. Wait until the panel completes its reboot.
4. Log back into the *Protected Setup* page, if necessary.

To shut down the panel:

1. Access the *Protected Setup* page.
2. Press the **Shutdown** button.
3. Disconnect any power source plugs or USB connections, if necessary.

Download from Www.Somanuals.com. All Manuals Search And Download.

Protected Setup Navigation Buttons

The Protected Setup Navigation Buttons (FIG. 59) appear on the left edge of the Protected Setup page.

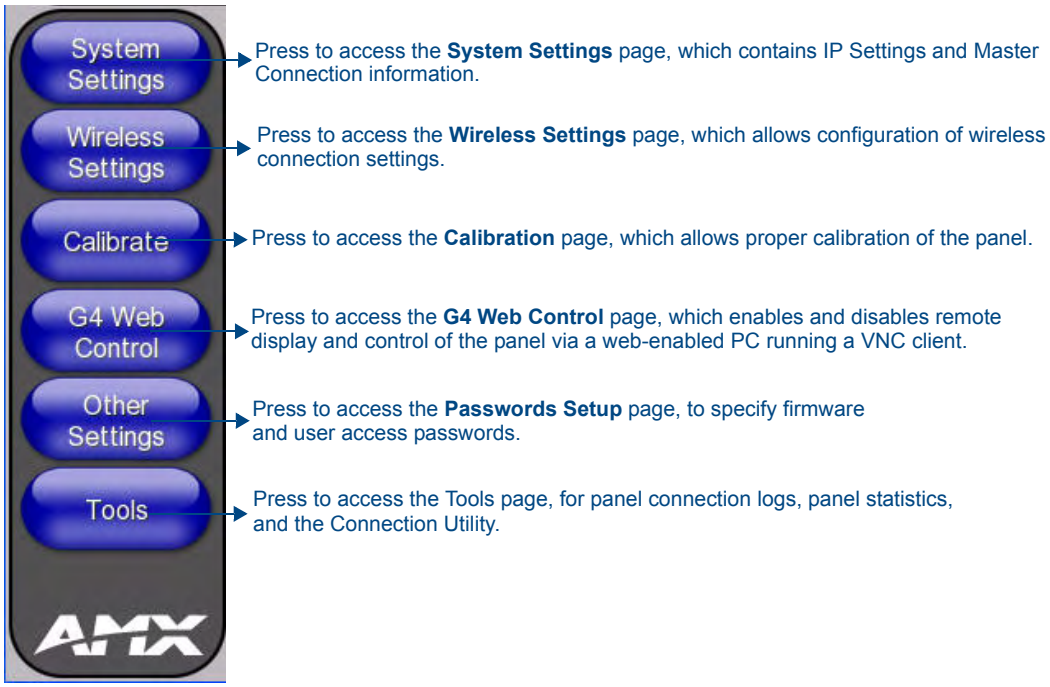


FIG. 59 Protected Setup Navigation Buttons

Download from Www.Somanuals.com. All Manuals Search And Download.

System Settings Page

The System Settings page (FIG. 60) displays sets the NetLinx Master's communication settings.

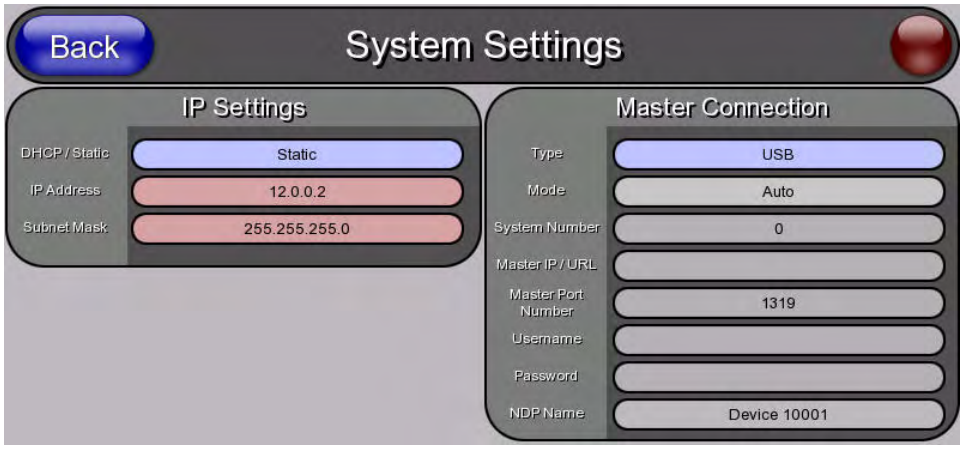


FIG. 60 System Settings page

The elements of this page include:

System Settings Page Elements	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Protected Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*
IP Settings:	Switches the IP settings between *DHCP* and *Static*. *DHCP* means that the IP address and the subnet mask fields are greyed out; in*Static*, press either of the fields to open the *IP Address* and *Subnet Mask* keypads.
Master Connection:	Sets the NetLinx Master communication values:
Type	Sets the NetLinx Master to communicate with the panel via Ethernet, USB, Mesh, or ICSNet. This is based on the cable connection from the rear. • *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. A Wireless Ethernet connection involves indirect communication from the panel to a Master via a wireless connection to the network. • 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).

Download from Www.Somanuals.com. All Manuals Search And Download.

System Setting Page Elements (Cont.)	
Mode	Cycles between the connection modes: URL, Listen, NDP(UDP,) URL(UDP), and Auto. *(Ethernet Only - disabled when USB is selected)* • **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. • **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. • NDP(UDP) - In this mode, The System Number and Master IP/URL fields are read-only. • URL(UDP) - In this mode, The System Number and Master IP/URL fields are read-only. • **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 entry of a system number. Default value is 0 (zero). *(ETHERNET in Auto Mode Only - disabled when USB is selected)*
Master IP/URL	Sets the Master IP or URL of the NetLinx Master. *(ETHERNET in URL and URL(UDP) Modes Only - disabled when USB is selected)*
Master Port Number	Allows entry of the port number used with the NetLinx Master. Default = 1319 (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.
NDP Name	Displays the name of the device connecting to the Master.

Refer to the *Step 3: Choose a Master Connection Mode* section on page 31 for more detailed information on using the *System Settings* page.

Download from Www.Somanuals.com. All Manuals Search And Download.

Wireless Settings Page

Use the options on the *Wireless Settings* page (FIG. 61) to configure communication settings for the wireless CF card (802.11b/g), and read the device number assigned to the panel.

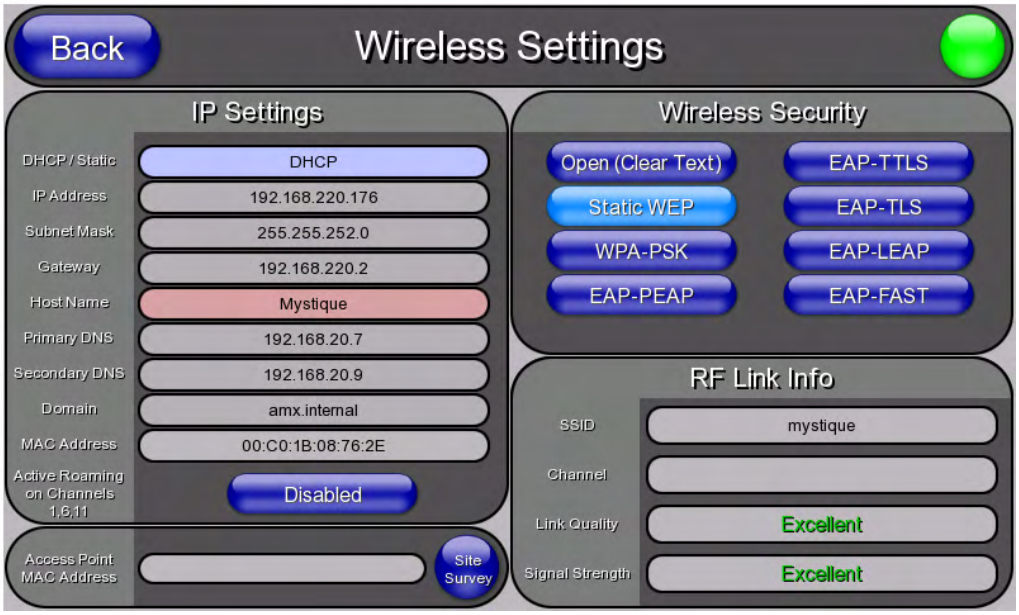


FIG. 61 Wireless Settings page (reads from and assigns values to the WAP)

Features on this page include:

Wireless Settings Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Protected Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*
IP Settings:	Sets the IP communication values for the panel:
DHCP/STATIC	Sets the panel to either DHCP or Static communication modes. • *DHCP* - a temporary IP Addresses is assigned to the panel by a DHCP server. If DHCP is selected, the other IP Settings fields are disabled (see below). • *Static IP* is a permanent IP Address assigned to the panel. If Static IP is selected, the other *IP Settings* fields are enabled (see 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&11	When enabled, connection allows active roaming between WAPs by switching between channels 1 and 11 if the other channel is unavailable.

Download from Www.Somanuals.com. All Manuals Search And Download.

Wireless Settings Page (Cont.)	
Access Point MAC Address:	This unique address identifies the Wireless Access Point (WAP) used by this panel for wireless communication (read-only). • **Site Survey** button: Launches the *Wireless Site Survey* page. The options on this page allow you to detect ("sniff-out") all WAPs transmitting within range of the panel's Wi-Fi card. Data displayed on the Site Survey page is categorized by: - **Network Name (SSID**) - WAP names - **Channel (RF)** - channels currently being used by the WAP - **Security Type** - security protocol enabled on the WAP, if detectable - **Signal Strength** - None, Poor, Fair, Good, Very Good, and Excellent - **MAC Address** - Unique identification of the transmitting Access Point • Refer to the *Using the Site Survey tool* section on page 23 for more detailed information on the *SIte Survey* page. • 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.
Wireless Security:	Sets the wireless security method to be used by the panel to connect to the network. Selecting any of the connection method buttons invokes the relevant configuration page, with options that allow you to define parameters specific to the selected method of connection.
Open (Clear Text)	This button opens the *Open (Clear Text) Settings* page (FIG. 63 on page 68). "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 *Open (Clear Text) Settings* section on page 68 for further details.
Static WEP	This button opens the *Static WEP Settings* page (FIG. 64 on page 69). "Static WEP" security requires that both a target WAP be identified and an encryption method be implemented prior to establishing communication. • Refer to the *Static WEP Settings* section on page 69 for further details.
WPA-PSK	This button opens the *WPA-PSK Settings* page (FIG. 65 on page 71). "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 71 for further details.
EAP-PEAP	This button opens the EAP-PEAP Settings page (FIG. 70 on page 77). "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 77 for further details. • For information on uploading a certificate file, refer to the *AMX Certificate Upload Utility* section on page 168.
EAP-TTLS	This button opens the EAP-TTLS Settings page (FIG. 71 on page 79). "EAP-TTLS" security is designed for wireless environments where having a Radius server directly validate the identity of the client (panel) is necessary before allowing it access to the network. • Refer to the *EAP-TTLS Settings* section on page 79 for further details. • For information on uploading a certificate file, refer to the *AMX Certificate Upload Utility* section on page 168.

Download from Www.Somanuals.com. All Manuals Search And Download.

Wireless Settings Page (Cont.)	
Wireless Security (Cont.):	
EAP-TLS	This button opens the EAP-TLS Settings page (FIG. 72 on page 81). "EAP-TLS" security is designed for wireless environments where securely transmitting data over a wireless network by adding an additional level of security protocol is necessary via the use of a private key. • Refer to the *EAP-TLS Settings* section on page 81 for further details. • For information on uploading a certificate file, refer to the *AMX Certificate Upload Utility* section on page 168.
EAP-LEAP	This button opens the EAP-LEAP Settings page (FIG. 67 on page 73). "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 73.
EAP-FAST	This button opens the EAP-FAST Settings page (FIG. 69 on page 75). "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 75 for further details.
RF Link Info:	These options set communication values for the wireless interface card:
SSID	Displays the currently used SSID of the target WAP.
Channel	The RF channel being used for connection to the WAP (*read -only*).
Link Quality	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. ***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	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*). 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.

Download from Www.Somanuals.com. All Manuals Search And Download.

Wireless Security

The options on the *Wireless Security* section (FIG. 62) include 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 162 for further information.

Some encryption and security features may or may not be supported:

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

Refer to the *Configuring Wireless Network Access* section on page 21 for more information on configuring the panel for wireless network access using the various security options.

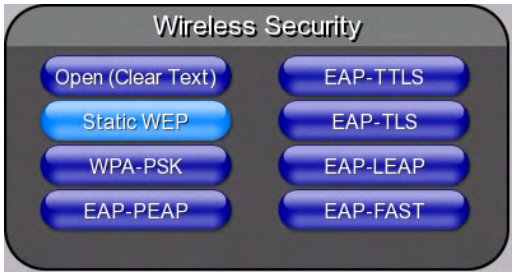


FIG. 62 Wireless Security section

Download from Www.Somanuals.com. All Manuals Search And Download.

Open (Clear Text) Settings

Press the **Open (Clear Text)** button to open the *Open (Clear Text) Settings* page (FIG. 63).

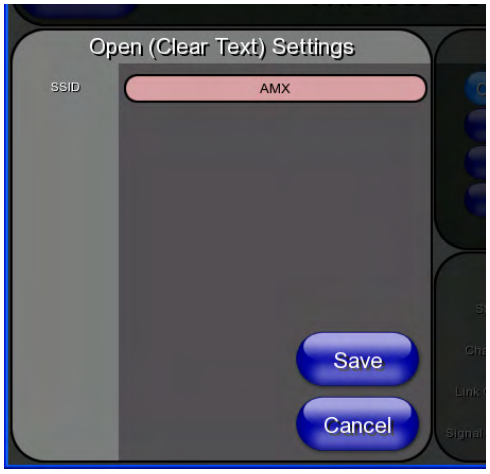


FIG. 63 Wireless Settings page - Open (Clear Text) Settings

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 (Clear Text) 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. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in your wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • If this field is left blank, the panel will attempt to connect to the first available WAP.
Save/Cancel:	• **Save** - store the new security information, apply changes, and return to the previous page. • **Cancel** - discard changes and return to the previous page.

Refer to the *Configuring Wireless Network Access* section on page 21 and the *Using the Site Survey tool* section on page 23 for further details on these security options.

Download from Www.Somanuals.com. All Manuals Search And Download.

Static WEP Settings

Press the **Static WEP** button to open the *Static WEP Settings* page (FIG. 64).

FIG. 64 Wireless Settings page - Static WEP Settings

Static 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.

Static WEP 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. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in your wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • 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*. "WEP" (Wired Equivalent Privacy) is an 802.11 security protocol designed to provide wireless security equivalent to wired networks. • **WEP64** enables WEP encryption using a 64 Bit Key Size. All packets are transmitted with their contents encrypted using the Default WEP Key. • **WEP128** enables WEP encryption using a 128 Bit Key Size. All packets are transmitted with their contents encrypted using the Default WEP Key. • 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.

Download from Www.Somanuals.com. All Manuals Search And Download.

Static WEP Settings (Cont.)	
Generate (Passphrase):	This button displays an on-screen keyboard which allows you to enter a passphrase. The panel then automatically generates four WEP keys that are compatible only with Modero panels. Enter these WEP keys into the target WAP. When working with multiple panels, WEP Keys must be entered into the WAP for each panel. • All Modero panels use the same code key generator. Therefore, this Passphrase generates identical keys on any Modero panel. • The Passphrase generator is case sensitive. ***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. This feature is useful for accessing different networks without having to re-enter that networks' WEP key. It is also sometimes used to set up a rotating key schedule to provide an extra layer of security.
WEP Keys:	This feature provides another level of security by selecting up to four WEP Keys. 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. • An ASCII key utilizes either 5 or 13 ASCII characters • A HEX key utilizes either 10 or 26 Hexidecimal characters Press **Done** to accept any changes and save the new value. ***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. • When working with a single panel and a single WAP, manually entering the *Current Key* from the WAP into the selected WEP Key is recommended. • When working with a single WAP and multiple panels, generating a Current Key using the same passphrase on all panels and then entering the panel-produced WEP key manually into the Wireless Access Point is recommended. • Keys may also be examined by touching the key buttons and noting the keyboard initialization text. • Use the on-screen keyboard's **Clear** button to erase stored key information.
Authentication:	Toggles between the two authentication modes: *Open* (broadcast publicly) or *Shared* (encrypted). • An *Open* network allows connections from any client without authentication. • A *Shared* 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. 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. • **Cancel** - discard changes and return to the previous page.

Refer to the *Configuring Wireless Network Access* section on page 21 and the *Using the Site Survey tool* section on page 23 for further details on these security options.

Download from Www.Somanuals.com. All Manuals Search And Download.

WPA-PSK Settings

Press the **WPA-PSK** button to opens the *WPA-PSK* dialog (FIG. 65).

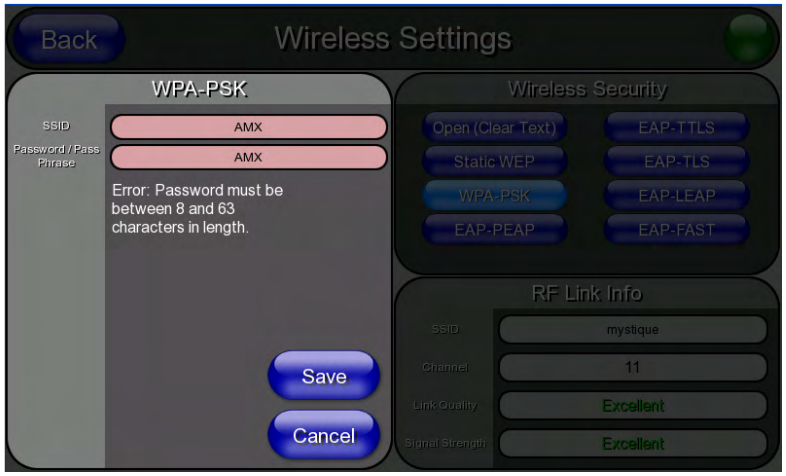


FIG. 65 Wireless Settings page - WPA-PSK Settings

WPA-PSK security is designed for environments where using WPA or WPA2 is desirable, 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.

WPA-PSK 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. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in your wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • If this field is left blank, the panel will attempt to connect to the first available WAP.
Password/Pass Phrase:	Opens an on-screen keyboard to enter a passphrase (password). • This alpha-numeric string must use a minimum of 8 characters and a maximum of 63. • The exact pass phrase string (including capitalization) must be entered on the target WAP.

Download from Www.Somanuals.com. All Manuals Search And Download.

WPA-PSK Settings (Cont.)	
Save/Cancel:	• **Save** - store the new security information, apply changes, and return to the previous page. • **Cancel** - discard changes and return to the previous page.

- Refer to the *Configuring Wireless Network Access* section on page 21 for details on these security options.
- Refer to the *Using the Site Survey tool* section on page 23 for more information on using this tool.

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 simply 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. 66). Please note that no user intervention is necessary during this process, as it proceeds automatically based on the configuration parameters entered into the panel.

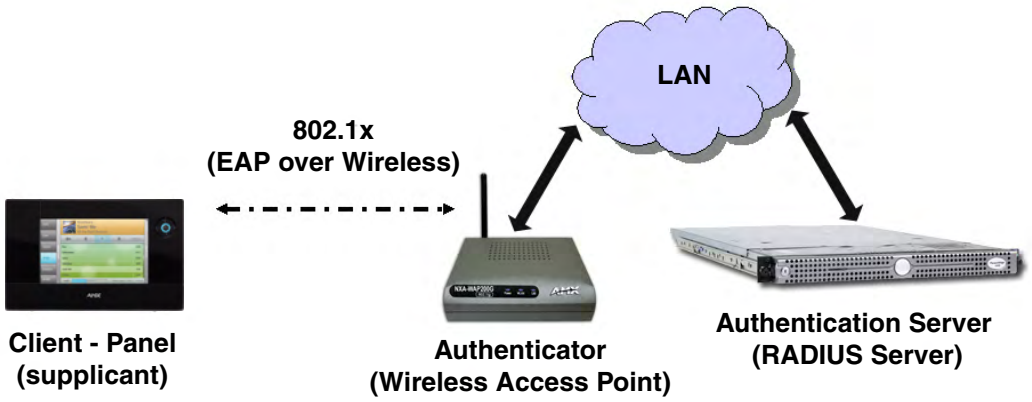


FIG. 66 EAP security method in process

A server certificate file uses a certificate 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, 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.

Download from Www.Somanuals.com. All Manuals Search And Download.

EAP-LEAP Settings

Press the **EAP-LEAP** button to open the *EAP-LEAP Settings* page (FIG. 67).

FIG. 67 Wireless Settings page - 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.

NOTE

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

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

Download from Www.Somanuals.com. All Manuals Search And Download.

EAP-LEAP 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. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in the wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • 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). ***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) ***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. • **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 FIG. 68 for an example of how a typical EAP-LEAP system configuration page should appear.

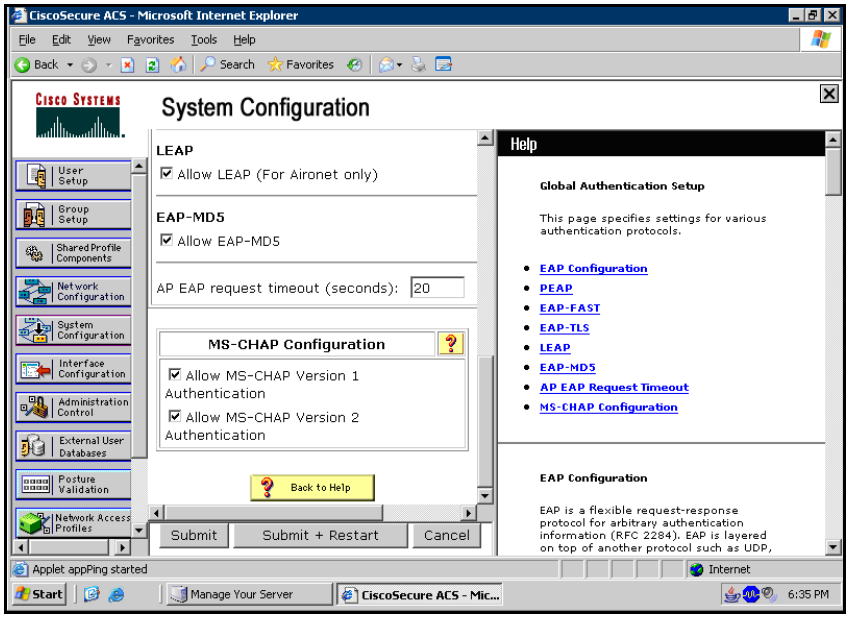


FIG. 68 EAP-LEAP sample Cisco System Security page

Download from Www.Somanuals.com. All Manuals Search And Download.

EAP-FAST Settings

Press the **EAP-FAST** button to open the *EAP-FAST Settings* dialog (FIG. 69).

FIG. 69 Wireless Settings 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. 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. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in the wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • 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 to enter an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server). ***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.*

Download from Www.Somanuals.com. All Manuals Search And Download.

EAP-FAST Settings (Cont.)	
Anonymous Identity:	Opens an on-screen keyboard to enter an IT provided alphanumeric string which (similar to the username) is used as the identity, but that does not represent a real user. 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) ***Note**: This information is similar to the password entered to gain access to a secured workstation.*
Automatic PAC Provisioning:	This selection toggles PAC (Protected Access Credential) Provisioning - **Enabled** *(automatic)* or **Disabled** *(manual)*. • If **Enabled** is selected, the following *PAC File Location* field is disabled, because the search for the PAC file is done automatically. • 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. **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. In that case, the panel must be forced to download a new PAC file. 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**. • 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. • 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. • **Cancel** - discard changes and return to the previous page.

Refer to the *EAP Authentication* section on page 166 and the *Using the Site Survey tool* section on page 23 for further details on these security options.

Download from Www.Somanuals.com. All Manuals Search And Download.

EAP-PEAP Settings

Press the **EAP-PEAP** button to open the EAP-PEAP Settings page (FIG. 70).

FIG. 70 Wireless Settings page - 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

Download from Www.Somanuals.com. All Manuals Search And Download.

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. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in the wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • 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 to enter an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server). ***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 to 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) ***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. 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. Use the on-screen keyboard's **Clear** button to erase completely 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**.
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**. • MSCHAPv2 (*used with PEAPv0*) • GTC (*used with PEAPv1*) • OTP • MD5
Save/Cancel:	• **Save** - store the new security information, apply changes, and return to the previous page. • **Cancel** - discard changes and return to the previous page.

Refer to the *EAP Authentication* section on page 166 and the *Using the Site Survey tool* section on page 23 for further details on these security options.

Download from Www.Somanuals.com. All Manuals Search And Download.

EAP-TTLS Settings

Press the **EAP-TTLS** button to opens the EAP-TTLS Settings page (FIG. 71).

FIG. 71 Wireless Settings page - 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 the Radius server needs to validate directly 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. 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. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in the wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • 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.

Download from Www.Somanuals.com. All Manuals Search And Download.

EAP-TTLS Settings (Cont.)	
Identity:	Opens an on-screen keyboard. Enter an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server). ***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. 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) ***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. 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. 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: • EAP-MSCHAPv2 • EAP-GTC • EAP-OTP • EAP-MD5 • MSCHAPv2 • MSCHAP • PAP • CHAP
Save/Cancel:	• **Save** - store the new security information, apply changes, and return to the previous page. • **Cancel** - discard changes and return to the previous page.

Refer to the *EAP Authentication* section on page 166 and the *Using the Site Survey tool* section on page 23 for further details on these security options.

Download from Www.Somanuals.com. All Manuals Search And Download.

EAP-TLS Settings

Press the **EAP-TLS** button to open the *EAP-TLS Settings* page (FIG. 72).

FIG. 72 Wireless Settings page - 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 for entering 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. • The SSID is case sensitive and must not exceed 32 characters. • Make sure this setting is the same for all points in the wireless network. • NXA-WAP200Gs use **AMX** as their default SSID. • 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 for entering an EAP Identity string (used by the panel to identify itself to an Authentication (RADIUS) Server). ***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.*

Download from Www.Somanuals.com. All Manuals Search And Download.

EAP-TLS Settings (Cont.)	
Certificate Authority:	When pressed, the panel displays an on-screen Certificate Authority (CA) File Location keyboard, for entering the name of the certificate authority file which is used to validate the server certificate. This field is optional. 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. • Use the on-screen keyboard's **Clear** button to completely erase any previously stored network path information.
Client Certificate:	Opens an on-screen keyboard for entering the name of the file containing the client (panel) certificate for use in certifying the identity of the client (panel). • Refer to the *Client certificate configuration* section on page 83 for information regarding Client Certificates and their parameters.
Private Key:	When pressed, the panel displays an on-screen Client Private Key File Location keyboard for entering the name of the file containing the private key. • 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 no password protection is associated with the Private Key, then this field should be left ***blank***. • When pressed, the panel displays an on-screen Private Key Password keyboard which allows you to enter an alpha-numeric password string. • 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. • **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 23 for more information on using this feature.

Download from Www.Somanuals.com. All Manuals Search And Download.

Client certificate configuration

A client certificate can be configured by an IT department in several ways. 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)

NOTE

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 .pem .pvk
DER	.cer .der
PKCS12	.pfx

Please 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

Download from Www.Somanuals.com. All Manuals Search And Download.

Calibration Page

The *Calibration* page (FIG. 73) allows you to calibrate the touch panel for accurate button selection.

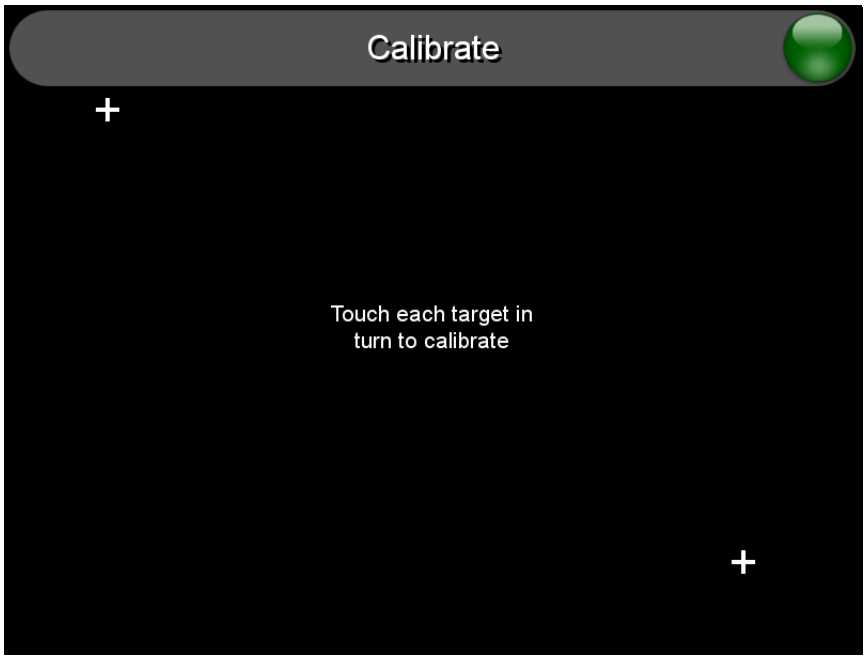


FIG. 73 Calibration page

1. Press and hold the center button on the navigation wheel for 6 seconds to access the *Calibration* page (see FIG. 57).
2. Press the crosshairs in turn. If the crosshairs are not touched within ten seconds, the MVP-5200i will return to the *Protected Setup* page.
3. The page will read "Calibration Successful. Touch to continue." Touch anywhere on the screen to return to the *Protected Setup* page.

NOTE

If the screen is not touched at that point, the device will automatically return to the Protected Setup *page within 10 seconds.*

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

Download from Www.Somanuals.com. All Manuals Search And Download.

G4 Web Control Settings 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 this page allow you to enable/disable G4 Web Control functionality(FIG. 74).

FIG. 74 G4 Web Control page

Features on this page include:

G4 Web Control Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Protected Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*
G4 Web Control Settings:	Sets the IP communication values for the touch panel:
Enable/Enabled	The Enable/Enabled button toggles between the two G4 activation settings: • **Enable** - deactivates G4 Web Control on the panel. • **Enabled** - activates G4 Web Control on the panel.
Network Interface Select	Toggles between the two network interface options: • **Wireless -** the panel is communicating via a Wireless Access Point (WAP). • Wired - the panel is communicating via its mini-USB port.
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	Use this field to 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, detecting no cursor movements, before the G4 Web Control session is terminated. • Minimum value = 0 minutes (panel never times out) • Maximum value = 240 minutes (panel times out after 240 minutes)

Download from Www.Somanuals.com. All Manuals Search And Download.

Refer to the Using G4 Web Control to Interact with a G4 Panel section on page 41 *for instructions on using the G4 Web Control page with the web-based NetLinx Security application.*

Download from Www.Somanuals.com. All Manuals Search And Download.

Other Settings

Press the **Other Settings** button to display the two settings options for **Cache** and **Password**. Press one of the options within three seconds, or the two options buttons will slide back behind the **Other Settings** button.

Cache Settings Page

The options on the *Cache Settings* page (FIG. 75) allow setting and clearing of the flash memory cache, as well as viewing the status of the current cache settings. Since image files take up a significant amount of the MVP-5200i's flash memory, being able to examine the current limits and contents is useful in deciding whether to increase or decrease the total flash cache size.

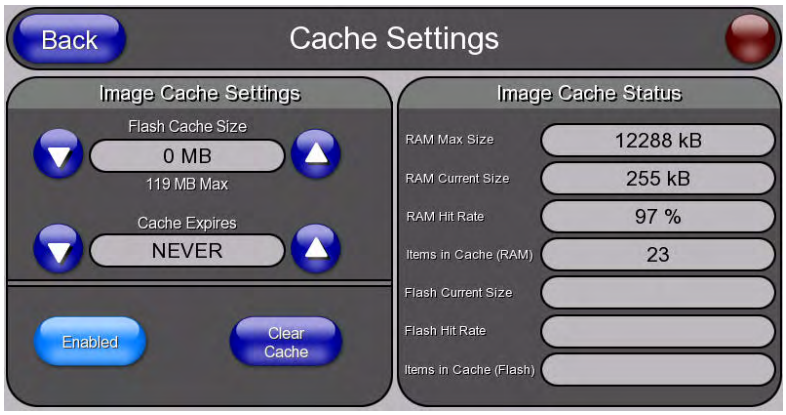


FIG. 75 Cache Settings Page

Cache Settings Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Protected Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*
Image Cache Settings	
Flash Cache Size:	Use the **Up/Down** buttons to increase or decrease the total size of the flash memory cache, up to a maximum of 171MB.
Cache Expires:	Use the **Up/Down** buttons to control the amount of time elapsed before the panel automatically deletes its cache, with increments of 2 hours, 8 hours, 1 day, 2 days, 5 days, and "NEVER".
Enable:	Saves any changes made to the *Flash Cache Size* or *Cache Expires* fields.
Clear Cache:	Clears all files previously stored in the flash memory cache.
Image Cache Status	
RAM Max Size:	The maximum size allocated to the RAM cache.
RAM Current Size:	The size of the current RAM cache contents.
RAM Hit Rate:	The number of times the RAM cache was referenced since the last cache clearing.
Items In Cache (RAM):	The total number of cached images in the RAM cache.
Flash Current Size:	The maximum size allocated to the flash cache.
Flash Hit Rate:	The number of times the flash cache was referenced since the last cache clearing.
Items in Cache (Flash):	The total number of cached images in the flash cache.

Download from Www.Somanuals.com. All Manuals Search And Download.

Password Settings Page

The options on the *Password Settings* page (FIG. 76) allow assignment of passwords required for users to access the *Protected Setup* page, and to release the device from a MVP-WCS-52 Charging Station.

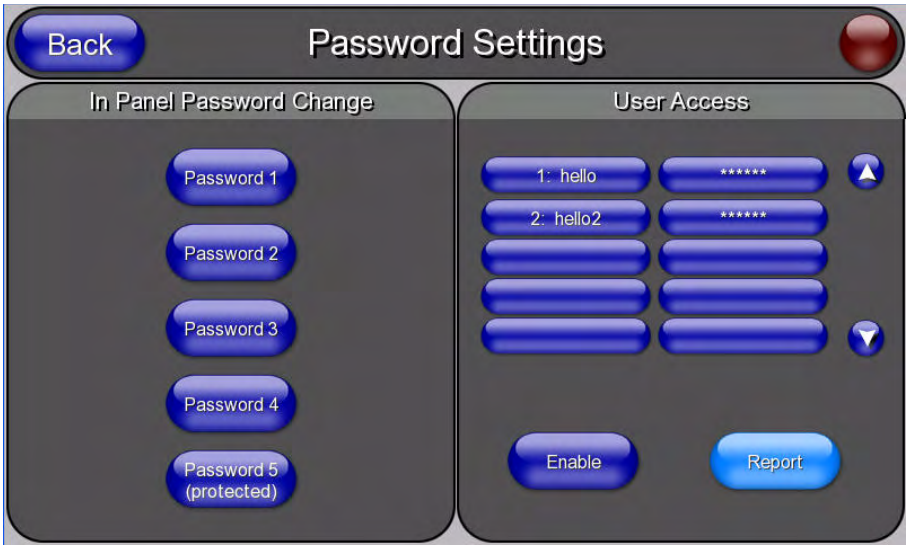


FIG. 76 Password Setup page

Features on this page include:

Password Setup Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Protected Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*
In Panel Password Change:	Accesses the alphanumeric values associated to particular password sets. • The PASSWORD 1, 2, 3, 4 and 5 (protected) buttons open a keyboard to enter alphanumeric values associated to the selected password group. ***Note**: Clearing Password #5 removes the need to enter a password before accessing the Protected Setup page.*
User Access:	Lists all previous password users, in the order in which they accessed the device.
Enable/Enabled:	When enabled, this button notes that all password entry attempts will be recorded.
Report:	When enabled, this button sends a report to the Master on any attempts or successes at entering a password.

To change a previously established password:

1. In the *Password Settings* page, press the button in the *In Panel Password Change* section for the particular password to be changed.

NOTE

Password 5 is protected, and can only be changed by the Administrator.

2. In the *Password* keyboard, enter the new alphanumeric password.
3. Press **Done** when complete.

Download from Www.Somanuals.com. All Manuals Search And Download.

The *User Access* section allows the Administrator to control access of all individuals using or attempting to use the MVP-5200i. From this section, new users may be given access rights to the device; however, they will NOT be given access to the *Protected Settings* page.

Only one of the main passwords may be used to access the Protected Settings page. An individual user password may not be used to access the Protected Settings page unless it matches one of the main passwords.

To list a new user within the *User Access* section:

1. Press a blank button in the *User Access* section.
2. In the *Name* keyboard, enter the user's name or nickname and press **Done** when finished.
3. In the *Password* keyboard, enter the selected alphanumeric password and press **Done** when finished.
4. The new user's name will appear in the left column of *User Access* section. The password will also appear in the right column, but its characters will be replaced with asterisks.

No matter how many characters are in an actual password, the Password column in the User Access section will always show five asterisks.

To change a User Access password:

1. Press the button corresponding to the user's name in the *User Access* section.
2. In the *Password* keyboard, enter the user's password and press *Done*.
3. Press the password button in the right column of the *User Access* section.
4. Enter the new password into the *Password* keyboard and press **Done**.

To view all previous instances of users accessing the device:

1. From the *Password Settings* page, press the **Enable** button to highlight it. The MVP-5200i will record all successful and unsuccessful attempts to access the touch panel.
2. Press the **Record** button to send a record to the network Master of all recorded attempts to access the device. This record may be retrieved from the Master at any time.

Download from Www.Somanuals.com. All Manuals Search And Download.

Tools

Press and hold the **Tools** button to access the MVP-5200i's **Panel Logs**, **Panel Statistics**, and **Connection Utility** buttons (FIG. 77). Each of these buttons opens a separate page, covered in detail below.

FIG. 77 Tools button menu

NOTE

*The **Tools** button menu will remain visible for three seconds, regardless of whether or not the button continues to be held.*

Panel Connection Logs Page

The *Panel Connection Logs* page (FIG. 78) chronicles all previous connections between the device and the network.

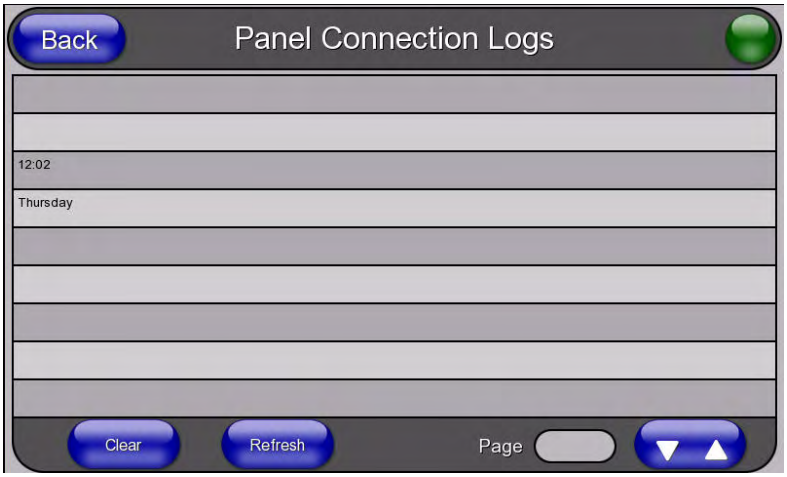


FIG. 78 Panel Connection Logs Page

Panel Connection Logs Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Protected Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*
Clear:	Clears all connection logs.
Refresh:	Refreshes displayed log information.
Page:	Displays the current log page number. Use the Up/Down arrows to select log pages.

Download from Www.Somanuals.com. All Manuals Search And Download.

Panel Statistics Page

The *Panel Statistics* page (FIG. 79) displays activity between the device and the network in proportions of ICSP messages, blink messages, and Ethernet versus wireless use.

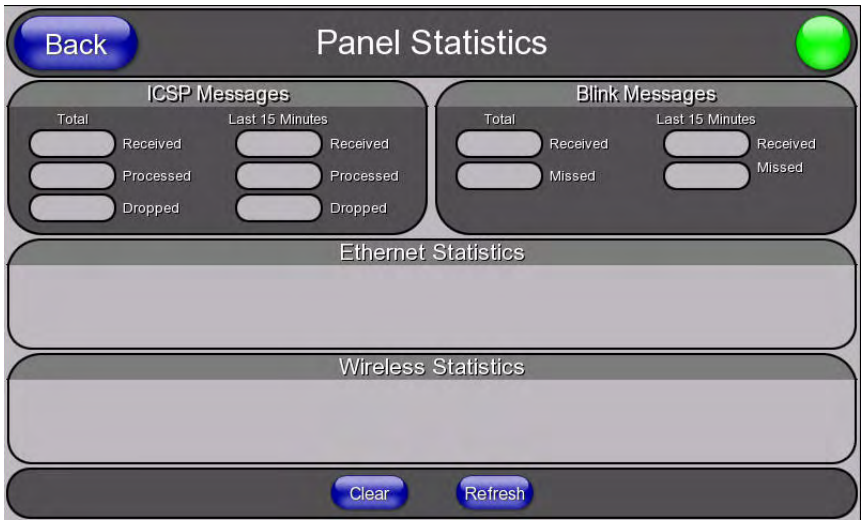


FIG. 79 Panel Statistics Page

Panel Statistics Page	
Back:	Saves all changes and returns to the previous page.
Connection Status icon:	The icon in the upper-right corner of each Protected Setup page provides a constant visual indication of current connection status. ***Note**: a Lock appears on the icon if the panel is connected to a secured NetLinx Master.*
ICSP Messages:	Lists the number of ICSP messages received, processed, and dropped, both in total and within the last 15 minutes.
Blink Messages:	Lists the number of blink messages received and missed, both in total and within the last 15 minutes.
Ethernet Statistics:	Displays the percentage of connection time via Ethernet.
Wireless Statistics:	Displays the percentage of connection time via wireless connections.
Clear:	Clears all fields on the *Panel Statistics* page.
Refresh:	Refreshes all data on the *Panel Statistics* page.

Download from Www.Somanuals.com. All Manuals Search And Download.

Connection Utility Page

The *Connection Utility* page (FIG. 80) displays the current wired and wireless connection information, including the latest link quality and signal strength information.

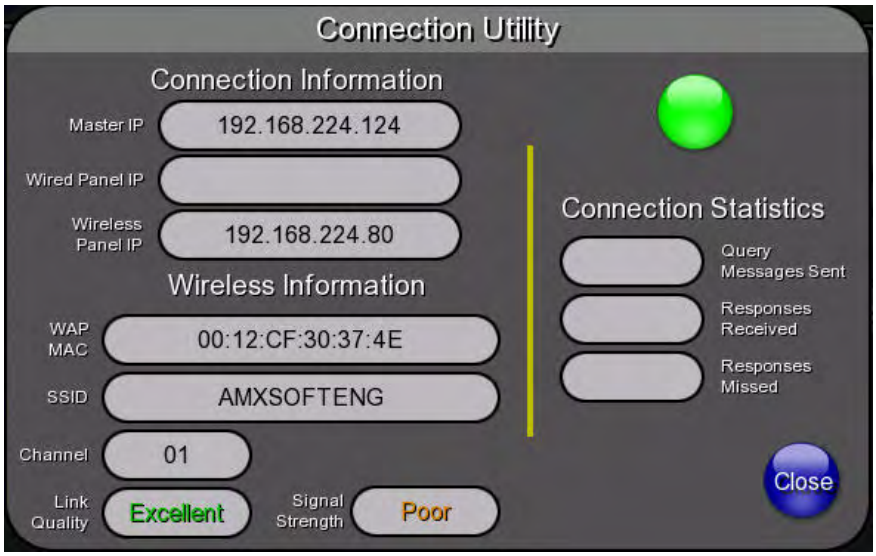


FIG. 80 Connection Utility Page

Connection Utility Page	
Connection Information:	
Master IP:	The IP address for the network's Master.
Wired Panel IP:	The IP address used by the device for wired connections.
Wireless Panel IP:	The IP address used by the device for wireless connections.
Wireless Information:	
WAP MAC:	The WAP's MAC address.
SSID:	Displays the currently used SSID of the target WAP.
Channel:	The channel being used for the current connection.
Link Quality:	Displays the current quality of the target WAP link.
Signal Strength:	Displays the current strength of the target WAP signal.
Connection Status icon:	The icon in the upper-right corner of each Protected Setup page provides a constant visual indication of current connection status.
Connection Statistics:	
Query Messages Sent:	Lists the number of queries sent to the WAP.
Responses Received:	Lists the number of responses received from the WAP.
Responses Missed:	Lists the number of responses missed by the WAP.
Close:	Closes the *Connection Utility* page and returns to the *Protected Setup* page.

Download from Www.Somanuals.com. All Manuals Search And Download.

Upgrading Firmware

For the purpose of panel downloads, the MVP-5200i's download procedure is not compatible with other AMX panel devices. This is due to the unique configuration of the device.

The first major change from other AMX devices is that the MVP-5200i uses dynamic Setup Pages for its displays. Instead of requiring a separate Setup Page project built within TPDesign 4, the MVP-5200i uses only a single set of Setup Pages for all of its supported resolutions.

To enable a single Setup Page project to support all resolutions, this requires including images for the largest supported resolution with the Setup Page project and scaling the images to fit for lower resolutions. This modification would apply to state-level bitmaps and chameleon images; previously, image scaling has only applied to dynamic images.

These features require a separate G4SupportFiles installation to be posted for download independently of the TPDesign4, NetLinx Studio, and Visual Architect applications.

Scale Images For Setup Pages

To provide the Setup Page designer with the ability to design pages at the target device's lowest supported resolution, TPDesign4 performs image scaling for both standard and chameleon images for button and page states. This functionality is not extended to icon images.

The MVP-5200i comes already loaded with on-board firmware, which is upgradeable through the use of the latest version of NetLinx Studio. Refer to the *NetLinx Studio version 2.x or higher Instruction Manual* for more information on how to download firmware to a touch panel.

*Programming the MVP-5200i requires the use of NetLinx Studio and TPDesign 4, both available from **www.amx.com**.*

Upgrading the Modero Firmware via the USB port

The MVP-5200i uses a 5-pin CC-USB (Type A) to Mini-B 5-Wire programming cable (**FG10-5965**) for programming, firmware updates, and touch panel file transfer between the PC and the target device. If a programming cable is not available, it may be purchased from **www.amx.com**. The Mini-USB port for the connector is located on the left side of the device as viewed from the front.

Before beginning with this section, verify that the device is powered and the Type-A end of the USB connector is inserted and secure the PC's USB port. **The panel must be powered *On* before connecting the mini-USB connector to the panel.** To guarantee that the upgrade is not interrupted by power loss, putting the panel in the Table Charging Station before beginning the upgrade is highly recommended.

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 completing the installation of the USB driver, 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, hold the navigation wheel to display the *Setup* Page, and open the *Protected Setup* page.
3. Press **System Settings** to open the *System Settings* page.

Download from Www.Somanuals.com. All Manuals Search And Download.

4. Toggle the blue *Type* field in the *Master Connection* section until the choice cycles to **USB**.

NOTE

***ALL** fields are then grayed 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 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 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 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 and select **Settings > Master Communication Settings** from the Main menu to open the *Master Communication Settings* dialog (FIG. 81).

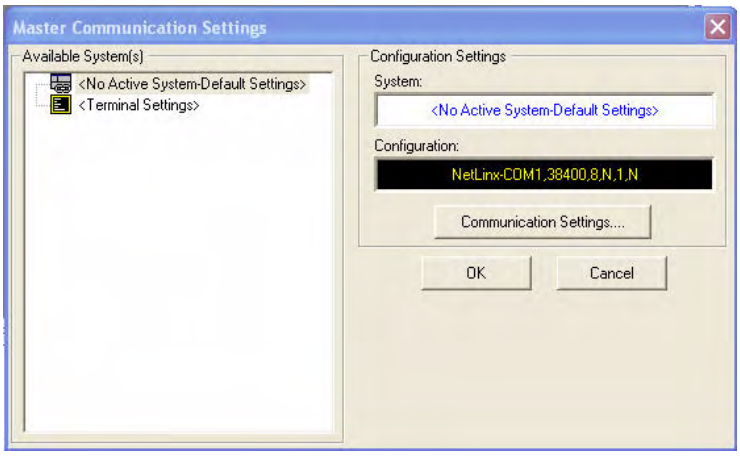


FIG. 81 Master Communications Settings dialog box

Download from Www.Somanuals.com. All Manuals Search And Download.

2. Click the **Communications Settings** button to open the *Communications Settings* dialog (FIG. 82).

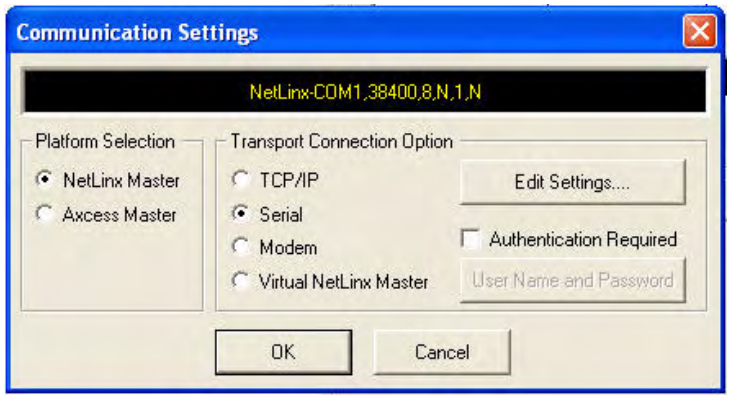


FIG. 82 Communications Settings dialog box

3. Click on the **NetLinx Master** radio button from the *Platform Selection* section.
4. Click on the **Virtual Master** radio box from the *Transport Connection Option* section to configure the PC to communicate directly with a panel. Everything else, such as the Authentication, is greyed-out because this connection is not going through the Master's UI.
5. Click the **Edit Settings** button on the *Communications Settings* dialog to open the *Virtual NetLinx Master Settings* dialog.
6. From within this dialog, enter the *System number*. The default is **1**.
7. Click **OK** three times to close the open dialogs, save your settings, and return to the main NetLinx Studio application.
8. Click the **OnLine Tree** tab in the Workspace window to view the devices on the Virtual System. *The default System value is one*.
9. Right-click on the *Empty Device Tree/System* entry and select **Refresh System** to re-populate the list.

NOTE

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 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 causes the panel to reboot, allows the PC to detect the panel, and assigns an appropriate USB driver.

1. Verify that the 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, verify that the panel is ready to receive files.

Download from Www.Somanuals.com. All Manuals Search And Download.

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. 83) to view the devices on the Virtual System. *The default System value is **1**.*
4. Right-click on the System entry (FIG. 83) 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.*

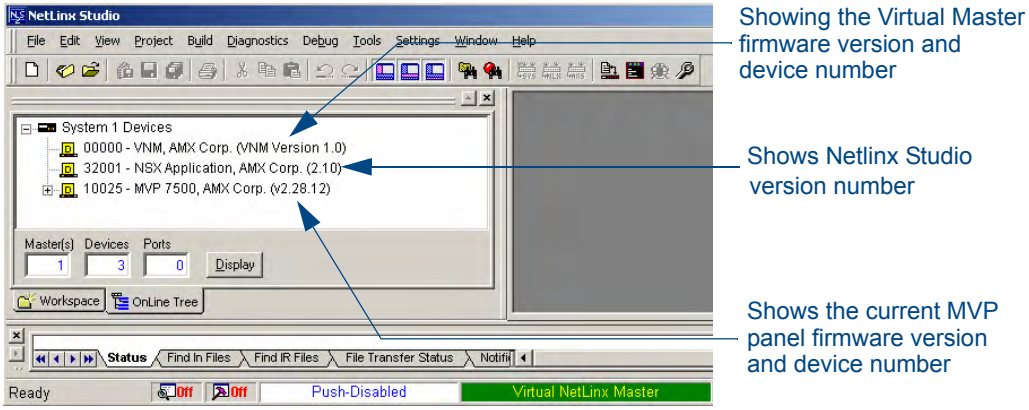


FIG. 83 NetLinx Workspace window (showing panel connection via a Virtual NetLinx Master)

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 accepting the Licensing Agreement, verify download of the Modero Kit file to a known location.

Download from Www.Somanuals.com. All Manuals Search And Download.

7. Select **Tools > Firmware Transfers > Send to NetLinx Device** from the Main menu to open the *Send to NetLinx Device* dialog (**B** in FIG. 84). Verify that 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. 84).

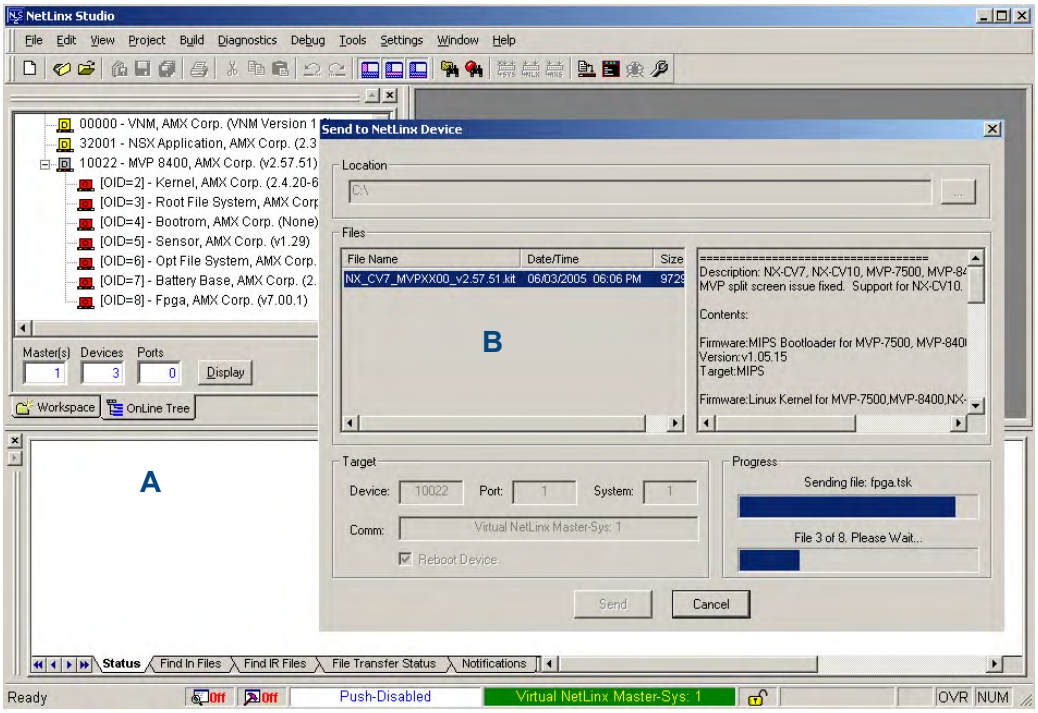


FIG. 84 Using USB for a Virtual Master transfer

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 to 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. 84).
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 that the panel has been properly updated to the correct firmware version.

NOTE

*Verify you have downloaded the latest firmware file from **www.amx.com** and then save the Kit file to your computer.*

Download from Www.Somanuals.com. All Manuals Search And Download.

A Special Note for Network Interface Connections

Due to any USB connection to your PC being made through a Network Interface Connection (NIC), Windows will automatically make any new NIC connection the Primary connection. If this happens, the USB address of 12.0.0.x will show up across the PC's network switches as the PC's source address. In some cases, network administrators will notice the NIC connection and reconfigure any PC that has connected to the MVP-5200i. Business, college, and government installations would the type of installations that would be most affected, and most home installations would not be affected.

To prevent the NIC connection from becoming the primary connection:

1. From the Windows *Start* menu, select *Settings* > *Control Panel* to open the *Control Panel* window.
2. In the *Control Panel* window, click on the **Network Connections** icon to open the Network Connections window (FIG. 85)

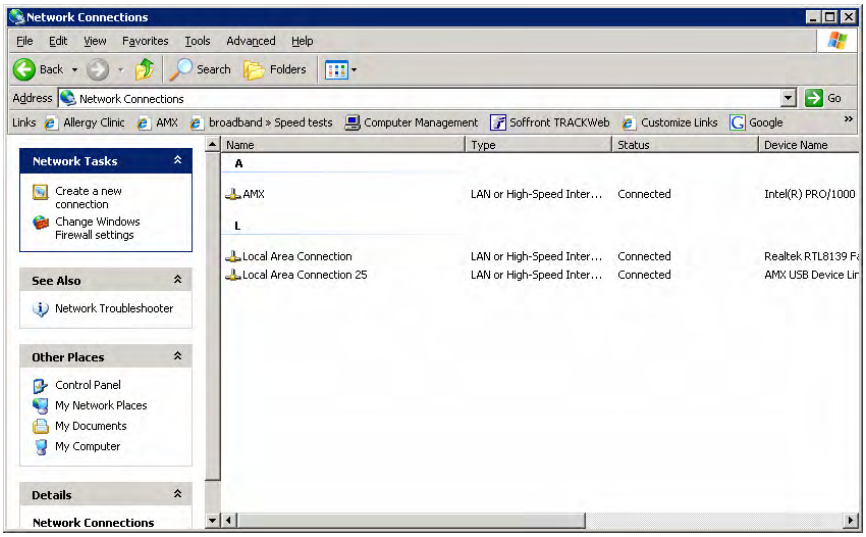


FIG. 85 Network Connections window

Download from Www.Somanuals.com. All Manuals Search And Download.

3. From the *Advanced* menu, select *Advanced Settings...* to open the *Advanced Settings* window (FIG. 86).

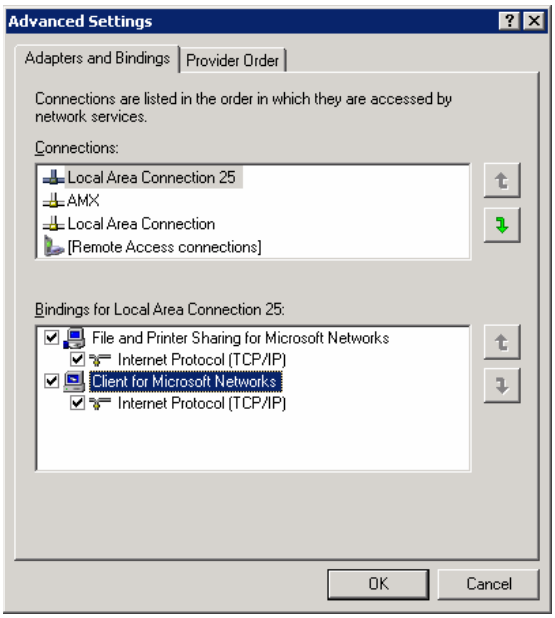


FIG. 86 Advanced Settings window

4. Under the *Adapters And Bindings* tab, the user needs to make sure the Local Area Connection is not at the top of the *Connections* list. If it is at the top of the list (FIG. 86), select it and use the *down* arrow to the right of the list to move it to the bottom of the list (FIG. 87).

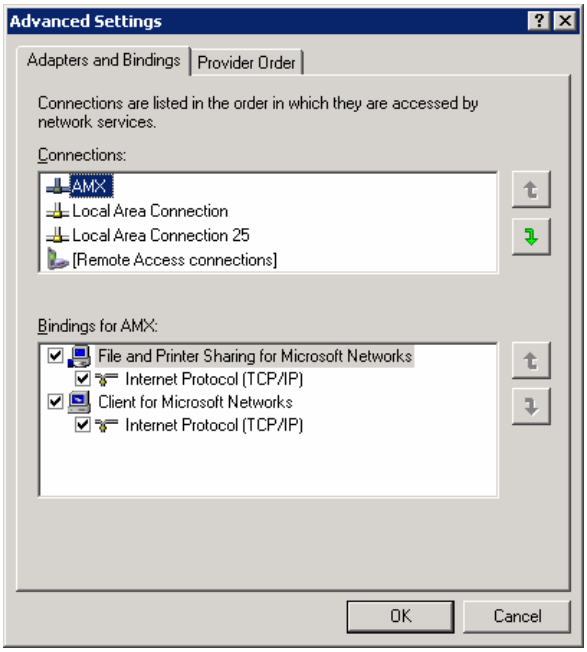


FIG. 87 Moving the Local Area Connection

5. In the lower *Bindings for Local Area Connection* field, unselect ALL bindings by clicking on the checkboxes by each binding to remove the checks from each box (FIG. 88).

Download from Www.Somanuals.com. All Manuals Search And Download.

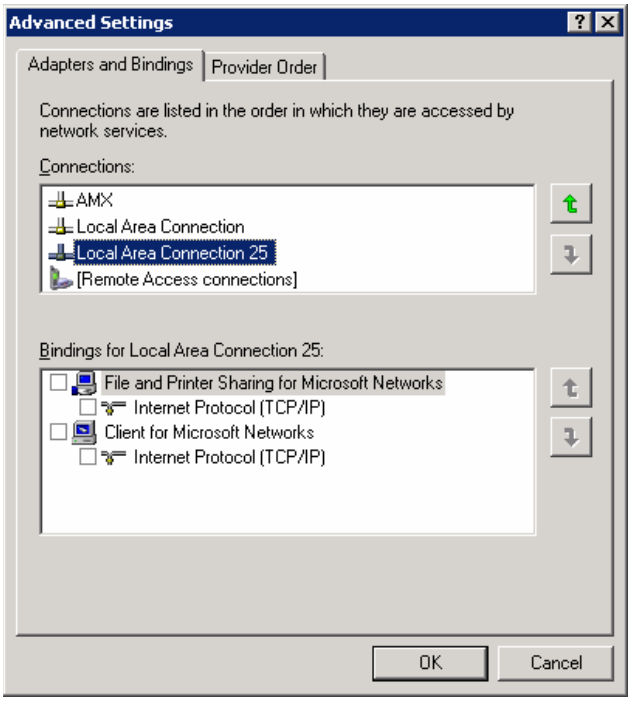


FIG. 88 Bindings for Local area list detail

6. When finished, click **OK** to close the *Advanced Settings* window and save all changes.

Download from Www.Somanuals.com. All Manuals Search And Download.

Programming

Overview

You can program the MVP-5200i, 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, as well as the latest version of NetLinx Studio and TPD4.

Navigation Wheel Programming

The navigation wheel on the front of the MVP-5200i has multiple programming functions. The device has four buttons mounted underneath the wheel, assigned as, select, left, right, top, and bottom. These buttons are fully programmable.

The wheel itself is also fully programmable. The wheel generated two pulses as it rotates. The phase difference between these pulses determines the direction of the rotation, and these periods can be a measure of its speed. A one-third rotation of this wheel causes a level change.

Page Commands

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

Page Commands	

@APG
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.
	Syntax:
	`"'@APG-<popup page name>;<popup group name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	popup group name = 1 - 50 ASCII characters. Name of the popup group.
	Example:
	`SEND_COMMAND Panel,"'@APG-Popup1;Group1'"`
	Adds the popup page 'Popup1' to the popup group 'Group1'.

@CPG
Clear all popup pages from specified popup group.
	Syntax:
	`"'@CPG-<popup group name>'"`
	Variable:
	popup group name = 1 - 50 ASCII characters. Name of the popup group.
	Example:
	`SEND_COMMAND Panel,"'@CPG-Group1'"`
	Clears all popup pages from the popup group 'Group1'.

Download from Www.Somanuals.com. All Manuals Search And Download.

Page Commands (Cont.)	

@DPG
Delete a specific popup page from specified popup group if it exists.
	Syntax:
	`"'@DPG-<popup page name>;<popup group name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	popup group name = 1 - 50 ASCII characters. Name of the popup group.
	Example:
	`SEND_COMMAND Panel,"'@DPG-Popup1;Group1'"`
	Deletes the popup page 'Popup1' from the popup group 'Group1'.

@PDR
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.
	Syntax:
	`"'@PDR-<popup page name>;<reset flag>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	reset flag = 1 = Enable reset flag
	0 = Disable reset flag
	Example:
	`SEND_COMMAND Panel,"'@PDR-Popup1;1'"`
	Popup1 will return to its default location when turned On.

@PHE
Set the hide effect for the specified popup page to the named hide effect.
	Syntax:
	`"'@PHE-<popup page name>;<hide effect name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	hide effect name = Refers to the popup effect names being used.
	Example:
	`SEND_COMMAND Panel,"'@PHE-Popup1;Slide to Left'"`
	Sets the Popup1 hide effect name to 'Slide to Left'.

@PHP
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.
	Syntax:
	`"'@PHP-<popup page name>;<x coordinate>,<y coordinate>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'@PHP-Popup1;75,0'"`
	Sets the Popup1 hide effect x-coordinate value to 75 and the y-coordinate value to 0.

@PHT
Set the hide effect time for the specified popup page.
	Syntax:
	`"'@PHT-<popup page name>;<hide effect time>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	hide effect time = Given in 1/10ths of a second.
	Example:
	`SEND_COMMAND Panel,"'@PHT-Popup1;50'"`
	Sets the Popup1 hide effect time to 5 seconds.

Download from Www.Somanuals.com. All Manuals Search And Download.

Page Commands (Cont.)	

@PPA
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.
	Syntax:
	`"'@PPA-<page name>'"`
	Variable:
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'@PPA-Page1'"`
	Close all pop-ups on Page1.

@PPF
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.
	Syntax:
	`"'@PPF-<popup page name>;<page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'@PPF-Popup1;Main'"`
	Example 2:
	`SEND_COMMAND Panel,"'@PPF-Popup1'"`
	Deactivates the popup page 'Popup1' on the current page.

@PPG
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.
	Syntax:
	`"'@PPG-<popup page name>;<page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'@PPG-Popup1;Main'"`
	Toggles the popup page 'Popup1' on the 'Main' page from one state to another (On/Off).
	Example 2:
	`SEND_COMMAND Panel,"'@PPG-Popup1'"`
	Toggles the popup page 'Popup1' on the current page from one state to another (On/Off).

@PPK
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.
	Syntax:
	`"'@PPK-<popup page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	Example:
	`SEND_COMMAND Panel,"'@PPK-Popup1'"`
	Kills the popup page 'Popup1' on all pages.

Download from Www.Somanuals.com. All Manuals Search And Download.

Page Commands (Cont.)	

@PPM
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.
	Syntax:
	`"'@PPM-<popup page name>;<mode>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	mode = NONMODAL converts a previously Modal popup page to a NonModal.
	MODAL converts a previously NonModal popup page to Modal.
	modal = 1 and non-modal = 0
	Example:
	`SEND_COMMAND Panel,"'@PPM-Popup1;Modal'"`
	Sets the popup page 'Popup1' to Modal.
	`SEND_COMMAND Panel,"'@PPM-Popup1;1'"`
	Sets the popup page 'Popup1' to Modal.

@PPN
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.
	Syntax:
	`"'@PPN-<popup page name>;<page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'@PPN-Popup1;Main'"`
	Activates 'Popup1' on the 'Main' page.
	Example 2:
	`SEND_COMMAND Panel,"'@PPN-Popup1'"`
	Activates the popup page 'Popup1' on the current page.

@PPT
Set a specific popup page to timeout within a specified time.
	If timeout is empty, popup page will clear the timeout.
	Syntax:
	`"'@PPT-<popup page name>;<timeout>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	timeout = Timeout duration in 1/10ths of a second.
	Example:
	`SEND_COMMAND Panel,"'@PPT-Popup1;30'"`
	Sets the popup page 'Popup1' to timeout within 3 seconds.

@PPX
Close all popups on all pages.
	This command works in the same way as the 'Clear All' command in TPDesign 4.
	Syntax:
	`"'@PPX'"`
	Example:
	`SEND_COMMAND Panel,"'@PPX'"`
	Close all popups on all pages.

Download from Www.Somanuals.com. All Manuals Search And Download.

Page Commands (Cont.)	

@PSE
Set the show effect for the specified popup page to the named show effect.
	Syntax:
	`"'@PSE-<popup page name>;<show effect name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	show effect name = Refers to the popup effect name being used.
	Example:
	`SEND_COMMAND Panel,"'@PSE-Popup1;Slide from Left'"`
	Sets the Popup1 show effect name to 'Slide from Left'.

@PSP
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.
	Syntax:
	`"'@PSP-<popup page name>;<x coordinate>,<y coordinate>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'@PSP-Popup1;100,0'"`
	Sets the Popup1 show effect x-coordinate value to 100 and the y-coordinate value to 0.

@PST
Set the show effect time for the specified popup page.
	Syntax:
	`"'@PST-<popup page name>;<show effect time>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	show effect time = Given in 1/10ths of a second.
	Example:
	`SEND_COMMAND Panel,"'@PST-Popup1;50'"`
	Sets the Popup1 show effect time to 5 seconds.

PAGE
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.
	Syntax:
	`"'PAGE-<page name>'"`
	Variable:
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'PAGE-Page1'"`
	Flips to page1.

Download from Www.Somanuals.com. All Manuals Search And Download.

Page Commands (Cont.)	

PPOF
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.
	Syntax:
	`"'PPOF-<popup page name>;<page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'PPOF-Popup1;Main'"`
	Deactivates the popup page 'Popup1' on the Main page.
	Example 2:
	`SEND_COMMAND Panel,"'PPOF-Popup1'"`
	Deactivates the popup page 'Popup1' on the current page.

PPOG
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.
	Syntax:
	`"'PPOG-<popup page name>;<page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'PPOG-Popup1;Main'"`
	Toggles the popup page 'Popup1' on the Main page from one state to another (On/Off).
	Example 2:
	`SEND_COMMAND Panel,"'PPOG-Popup1'"`
	Toggles the popup page 'Popup1' on the current page from one state to another (On/Off).

PPON
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.
	Syntax:
	`"'PPON-<popup page name>;<page name>'"`
	Variable:
	popup page name = 1 - 50 ASCII characters. Name of the popup page.
	page name = 1 - 50 ASCII characters. Name of the page the popup is displayed On.
	Example:
	`SEND_COMMAND Panel,"'PPON-Popup1; Main'"`
	Activates the popup page 'Popup1' on the Main page.
	Example 2:
	`SEND_COMMAND Panel,"'PPON-Popup1'"`
	Activates the popup page 'Popup1' on the current page.

Download from Www.Somanuals.com. All Manuals Search And Download.

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
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

Download from Www.Somanuals.com. All Manuals Search And Download.

RGB Values for all 88 Basic Colors (Cont.)				
Index No.	**Name**	**Red**	**Green**	**Blue**
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
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

Download from Www.Somanuals.com. All Manuals Search And Download.

RGB Values for all 88 Basic Colors (Cont.)				
Index No.	**Name**	**Red**	**Green**	**Blue**
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.		

NOTE

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

Download from Www.Somanuals.com. All Manuals Search And Download.

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.

The following number values cannot be used for programming purposes when changing border styles. TPD4 border styles may ONLY be changed by using the name.

TPD4 Border Styles by Name			
No.	**Border styles**	**No.**	**Border styles**
1	None	27	Cursor Bottom
2	AMX Elite -L	28	Cursor Bottom with Hole
3	AMX Elite -M	29	Cursor Top
4	AMX Elite -S	30	Cursor Top with Hole
5	Bevel -L	31	Cursor Left
6	Bevel -M	32	Cursor Left with Hole
7	Bevel -S	33	Cursor Right
8	Circle 15	34	Cursor Right with Hole
9	Circle 25	35	Custom Frame
10	Circle 35	36	Diamond 15
11	Circle 45	37	Diamond 25
12	Circle 55	38	Diamond 35
13	Circle 65	39	Diamond 45
14	Circle 75	40	Diamond 55
15	Circle 85	41	Diamond 65
16	Circle 95	42	Diamond 75
17	Circle 105	43	Diamond 85
18	Circle 115	44	Diamond 95
19	Circle 125	45	Diamond 105
20	Circle 135	46	Diamond 115
21	Circle 145	47	Diamond 125
22	Circle 155	48	Diamond 135
23	Circle 165	49	Diamond 145
24	Circle 175	50	Diamond 155
25	Circle 185	51	Diamond 165
26	Circle 195	52	Diamond 175

Download from Www.Somanuals.com. All Manuals Search And Download.

TPD4 Border Styles by Name (Cont.)			
No.	**Border styles**	**No.**	**Border styles**
53	Diamond 185	97	Menu Bottom Rounded 185
54	Diamond 195	98	Menu Bottom Rounded 195
55	Double Bevel -L	99	Menu Top Rounded 15
56	Double Bevel -M	100	Menu Top Rounded 25
57	Double Bevel -S	101	Menu Top Rounded 35
58	Double Line	102	Menu Top Rounded 45
59	Fuzzy	103	Menu Top Rounded 55
60	Glow-L	104	Menu Top Rounded 65
61	Glow-S	105	Menu Top Rounded 75
62	Help Down	106	Menu Top Rounded 85
63	Neon Active -L	107	Menu Top Rounded 95
64	Neon Active -S	108	Menu Top Rounded 105
65	Neon Inactive -L	109	Menu Top Rounded 115
66	Neon Inactive -S	110	Menu Top Rounded 125
67	Oval H 60x30	111	Menu Top Rounded 135
68	Oval H 100x50	112	Menu Top Rounded 145
69	Oval H 150x75	113	Menu Top Rounded 155
70	Oval H 200x100	114	Menu Top Rounded 165
71	Oval V 30x60	115	Menu Top Rounded 175
72	Oval V 50x100	116	Menu Top Rounded 185
73	Oval V 75x150	117	Menu Top Rounded 195
74	Oval V 100x200	118	Menu Right Rounded 15
75	Picture Frame	119	Menu Right Rounded 25
76	Quad Line	120	Menu Right Rounded 35
77	Single Line	121	Menu Right Rounded 45
78	Windows Style Popup	122	Menu Right Rounded 55
79	Windows Style Popup (Status Bar)	123	Menu Right Rounded 65
80	Menu Bottom Rounded 15	124	Menu Right Rounded 75
81	Menu Bottom Rounded 25	125	Menu Right Rounded 85
82	Menu Bottom Rounded 35	126	Menu Right Rounded 95
83	Menu Bottom Rounded 45	127	Menu Right Rounded 105
84	Menu Bottom Rounded 55	128	Menu Right Rounded 115
85	Menu Bottom Rounded 65	129	Menu Right Rounded 125
86	Menu Bottom Rounded 75	130	Menu Right Rounded 135
87	Menu Bottom Rounded 85	131	Menu Right Rounded 145
88	Menu Bottom Rounded 95	132	Menu Right Rounded 155
89	Menu Bottom Rounded 105	133	Menu Right Rounded 165
90	Menu Bottom Rounded 115	134	Menu Right Rounded 175
91	Menu Bottom Rounded 125	135	Menu Right Rounded 185
92	Menu Bottom Rounded 135	136	Menu Right Rounded 195
93	Menu Bottom Rounded 145	137	Menu Left Rounded 15
94	Menu Bottom Rounded 155	138	Menu Left Rounded 25
95	Menu Bottom Rounded 165	139	Menu Left Rounded 35
96	Menu Bottom Rounded 175	140	Menu Left Rounded 45

Download from Www.Somanuals.com. All Manuals Search And Download.

TPD4 Border Styles by Name (Cont.)			
No.	**Border styles**	**No.**	**Border styles**
141	Menu Left Rounded 55	149	Menu Left Rounded 135
142	Menu Left Rounded 65	150	Menu Left Rounded 145
143	Menu Left Rounded 75	151	Menu Left Rounded 155
144	Menu Left Rounded 85	152	Menu Left Rounded 165
145	Menu Left Rounded 95	153	Menu Left Rounded 175
146	Menu Left Rounded 105	154	Menu Left Rounded 185
147	Menu Left Rounded 115	155	Menu Left Rounded 195
148	Menu Left Rounded 125		

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" 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
Run a button animation (in 1/10 second).
	Syntax:
	`"'^ANI-<vt addr range>,<start state>,<end state>,<time>'"`
	Variable:
	variable text address range = 1 - 4000.
	start state = Beginning of button state (0= current state).
	end state = End of button state.
	time = In 1/10 second intervals.
	Example:
	`SEND_COMMAND Panel,"'^ANI-500,1,25,100'"`
	Runs a button animation at text range 500 from state 1 to state 25 for 10 second.

^APF
Add page flip action to a button if it does not already exist.
	Syntax:
	`"'^APF-<vt addr range>,<page flip action>,<page name>'"`
	Variable:
	variable text address range = 1 - 4000.
	page flip action = **Stan**[dardPage] - Flip to standard page
	Prev[iousPage] - Flip to previous page
	Show[Popup] - Show Popup page
	Hide[Popup] - Hide Popup page
	Togg[lePopup] - Toggle popup state
	ClearG[roup] - Clear popup page group from all pages
	ClearP[age] - Clear all popup pages from a page with the specified page name
	ClearA[ll] - Clear all popup pages from all pages
	page name = 1 - 50 ASCII characters.
	Example:
	`SEND_COMMAND Panel,"'^APF-400,Stan,Main Page'"`
	Assigns a button to a standard page flip with page name 'Main Page'.

^BAT
Append non-unicode text.
	Syntax:
	`"'^BAT-<vt addr range>,<button states range>,<new text>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	new text = 1 - 50 ASCII characters.
	Example:
	`SEND_COMMAND Panel,"'^BAT-520,1,Enter City'"`
	Appends the text 'Enter City' to the button's OFF state.

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	

^BAU
Append unicode text.
	Same format as ^UNI.
	Syntax:
	`"'^BAU-<vt addr range>,<button states range>,<unicode text>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	unicode text = 1 - 50 ASCII characters. Unicode characters must be entered in Hex format.
	Example:
	`SEND_COMMAND Panel,"'^BAU-520,1,00770062'"`
	Appends Unicode text '00770062' to the button's OFF state.

^BCB
Set the border color to the specified color.
	Only if the specified border color is not the same as the current color.
	Note: Color can be assigned by color name (without spaces), number or R,G,B value (RRGGBB or RRGGBBAA).
	Syntax:
	`"'^BCB-<vt addr range>,<button states range>,<color value>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	color value = Refer to the RGB Values for all 88 Basic Colors table on page 107 for more information.
	Example:
	`SEND_COMMAND Panel,"'^BCB-500.504&510,1,12'"`
	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 the RGB Values for all 88 Basic Colors table on page 107.

^BCF
Set the fill color to the specified color.
	Only if the specified fill color is not the same as the current color.
	Note: Color can be assigned by color name (without spaces), number or R,G,B value (RRGGBB or RRGGBBAA).
	Syntax:
	`"'^BCF-<vt addr range>,<button states range>,<color value>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	color value = Refer to the RGB Values for all 88 Basic Colors table on page 107 for more information.
	Example:
	`SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,12'"`
	`SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,Yellow'"`
	`SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,#F4EC0A63''"`
	`SEND_COMMAND Panel,"'^BCF-500.504&510.515,1,#F4EC0A'"`
	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).

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	

^BCT
Set the text color to the specified color.
	Only if the specified text color is not the same as the current color.
	***Note**: Color can be assigned by color name (without spaces), number or R,G,B value (RRGGBB or RRGGBBAA).*
	Syntax:
	`"'^BCT-<vt addr range>,<button states range>,<color value>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	color value = Refer to the RGB Values for all 88 Basic Colors table on page 107 for more information.
	Example:
	`SEND_COMMAND Panel,"'^BCT-500.504&510,1,12'"`
	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
Set the button draw order.
	Determines what order each layer of the button is drawn.
	Syntax:
	`"'^BDO-<vt addr range>,<button states range>,<1-5><1-5><1-5><1-5><1-5>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	layer assignments = Fill Layer = 1
	Image Layer = 2
	Icon Layer = 3
	Text Layer = 4
	Border Layer = 5
	***Note**: The layer assignments are from bottom to top. The default draw order is* **12345**.
	Example:
	`SEND_COMMAND Panel,"'^BDO-530,1&2,51432'"`
	Sets the button's variable text 530 ON/OFF state draw order (from bottom to top) to Border, Fill, Text, Icon, and Image.
	Example 2:
	`SEND_COMMAND Panel,"'^BDO-1,0,12345'"`
	Sets all states of a button back to its default drawing order.

^BFB
Set the feedback type of the button.
	ONLY works on General-type buttons.
	Syntax:
	`"'^BFB-<vt addr range>,<feedback type>'"`
	Variable:
	variable text address range = 1 - 4000.
	feedback type = (None, Channel, Invert, On (Always on), Momentary, and Blink).
	Example:
	`SEND_COMMAND Panel,"'^BFB-500,Momentary'"`
	Sets the Feedback type of the button to 'Momentary'.

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	
^BIM Set the input mask for the specified address.	Syntax: "'^BIM-<vt addr range>,<input mask>'" Variable: variable text address range = 1 - 4000. input mask = Refer to the Text Area Input Masking table on page 158 for character types. Example: SEND_COMMAND Panel,"'^BIM-500,AAAAAAAAAA'" Sets the input mask to ten 'A' characters, that are required, to either a letter or digit **(entry is required).**
^BLN 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. Syntax: "'^BLN-<vt addr range>,<button states range>,<number of lines>'" Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). number of lines = 0 - 240. Example: SEND_COMMAND Panel,"'^BLN-500,55'" Equally removes 55 lines from the top and 55 lines from the bottom of the video button.

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	

^BMC
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.
	Syntax:
	`"'^BMC-<vt addr range>,<button states range>,<source port>,<source address>,<source state>,<codes>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	• source port = 1 - 100.
	• source address = 1 - 4000.
	• source state = 1 - 256.
	codes:
	BM - Picture/Bitmap
	BR - Border
	CB - Border Color
	CF - Fill Color
	CT - Text Color
	EC - Text effect color
	EF - Text effect
	FT - Font
	IC - Icon
	JB - Bitmap alignment
	JI - Icon alignment
	JT - Text alignment
	LN - Lines of video removed
	OP - Opacity
	SO - Button Sound
	TX - Text
	VI - Video slot ID
	WW - Word wrap on/off
	Example:
	`SEND_COMMAND Panel,"'^BMC-425,1,1,500,1,BR'"`
	`or`
	`SEND_COMMAND Panel,"'^BMC-425,1,1,500,1,%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.
	Example 2:
	`SEND_COMMAND Panel,"'^BMC-150,1,1,315,1,%BR%FT%TX%BM%IC%CF%CT'"`
	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.

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" 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: '%B<border style>' = Set the border style name. See the Border Styles and Programming Numbers table on page 110. '%B',<border 0-27,40,41> = Set the borer style number. See the Border Styles and Programming Numbers table on page 110. '%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 115 for more information. '%F',<font 1-8,10,11,20-29,32-xx> = Set the font. See the Default Font Styles and ID Numbers table on page 109. '%F<font 01-08,10,11,20-29,32-xx>' = Set the font. See the Default Font Styles and ID Numbers table on page 109. '%MI<mask image>' = Set the mask image. Refer to the ^BMI command on page 120 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>'**

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	
^BMF (Cont.)	*For some of these commands and values, refer to* the RGB Values for all 88 Basic Colors table on page 107. '%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 126 more information. '%GU<bargraph ramp up>' = Set the bargraph ramp up time in intervals of 1/10 second. '%GD<bargraph ramp down>' = Set the bargraph ramp down time in 1/10 second. '%GG<bargraph drag increment> = Set the bargraph drag increment. Refer to the ^GDI command on page 126 for more information. '%VI<video ON/OFF>' = Set the Video either ON (value=1) or OFF (value=0). '%OT<feedback type>' = Set the Feedback (Output) Type to one of the following: None, Channel,Invert, ON (Always ON), Momentary, or Blink. '%SM' = Submit a text for text area button. '%SF<1 or 0>' = Set the focus for text area button. '%OP<0-255>' = Set the button opacity to either Invisible (value=0) or Opaque (value=255). '%OP#<00-FF>' = Set the button opacity to either Invisible (value=00) or Opaque (value=FF). '%UN<Unicode text>' = Set the Unicode text. See the ^*UNI* section on page 132 for the text format. '%LN<0-240>' = Set the lines of video being removed. ^*BLN* section on page 116 for more information. '%EF<text effect name>' = Set the text effect. '%EC<text effect color>' = Set the text effect color. '%ML<max length>' = Set the maximum length of a text area. '%MK<input mask>' = Set the input mask of a text area. '%VL<0-1>' = Log-On/Log-Off the computer control connection '%VN<network name>' = Set network connection name. '%VP<password>' = Set the network connection password. Example: `SEND_COMMAND Panel,"'^BMF-500,1,%B10%CFRed%CB Blue %CTBlack%Ptest.png'"` Sets the button OFF state as well as the Border, Fill Color, Border Color, Text Color, and Bitmap.

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	

^BMI
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.
	Syntax:
	`"'^BMI-<vt addr range>,<button states range>,<mask image>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	mask image = Graphic file used.
	Example:
	`SEND_COMMAND Panel,"'^BMI-530,1&2,newMac.png'"`
	Sets the button with variable text 530 ON/OFF state mask image to 'newmac.png'.

^BML
Set the maximum length of the text area button.
	If this value is set to zero (0), the text area has 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.
	Syntax:
	`"'^BML-<vt addr range>,<max length>'"`
	Variable:
	variable text address range = 1 - 4000.
	max length = 2000 (0=no max length).
	Example:
	`SEND_COMMAND Panel,"'^BML-500,20'"`
	Sets the maximum length of the text area input button to 20 characters.

^BMP
Assign a picture to those buttons with a defined address range.
	Syntax:
	`"'^BMP-<vt addr range>,<button states range>,<name of bitmap/picture>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	name of bitmap/picture = 1 - 50 ASCII characters.
	Example:
	`SEND_COMMAND Panel,"'^BMP-500.504&510.515,1,bitmap.png'"`
	Sets the OFF state picture for the buttons with variable text ranges of 500-504 & 510-515.

^BNC
Clear current TakeNote annotations.
	Syntax:
	`"'^BNC-<vt addr range>,<command value>'"`
	Variable:
	variable text address range = 1 - 4000.
	command value = (0= clear, 1= clear all).
	Example:
	`SEND_COMMAND Panel,"'^BNC-973,0'"`
	Clears the annotation of the TakeNote button with variable text 973.

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	

^BNN
Set the TakeNote network name for the specified Addresses.
	Syntax:
	`"'^BNN-<vt addr range>,<network name>'"`
	Variable:
	variable text address range = 1 - 4000.
	network name = Use a valid IP Address.
	Example:
	`SEND_COMMAND Panel,"'^BNN-973,192.168.169.99'"`
	Sets the TakeNote button network name to 192.168.169.99.

^BNT
Set the TakeNote network port for the specified Addresses.
	Syntax:
	`"'^BNT-<vt addr range>,<network port>'"`
	Variable:
	variable text address range = 1 - 4000.
	network port = 1 - 65535.
	Example:
	`SEND_COMMAND Panel,"'^BNT-973,5000'"`
	Sets the TakeNote button network port to 5000.

^BOP
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.
	Syntax:
	`"'^BOP-<vt addr range>,<button states range>,<button opacity>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	button opacity = 0 (invisible) - 255 (opaque).
	Example:
	`SEND_COMMAND Panel,"'^BOP-500.504&510.515,1,200'"`
	Example 2:
	`SEND_COMMAND Panel,"'^BOP-500.504&510.515,1,#C8'"`
	Both examples set the opacity of the buttons with the variable text range of 500-504 and 510-515 to 200.

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	

^BOR
Set a border to a specific border style associated with a border value for those buttons with a defined address range.
	Refer to the Border Styles and Programming Numbers table on page 110 for more information.
	Syntax:
	`"'^BOR-<vt addr range>,<border style name or border value>'"`
	Variable:
	variable text address range = 1 - 4000.
	border style name = Refer to the Border Styles and Programming Numbers table on page 110.
	border value = 0 - 41.
	Examples:
	`SEND_COMMAND Panel,"'^BOR-500.504&510.515,10'"`
	Sets the border by number (#10) to those buttons with the variable text range of 500-504 & 510-515.
	`SEND_COMMAND Panel,"'^BOR-500.504&510,AMX Elite -M'"`
	Sets the border by name (AMX Elite) to those buttons with the variable text range of 500-504 & 510-515.
	The border style is available through the TPDesign4 border-style drop-down list. Refer to theTPD4 Border Styles by Name table on page 110 for more information.

^BOS
Set the button to display either a Video or Non-Video window.
	Syntax:
	`"'^BOS-<vt addr range>,<button states range>,<video state>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	video state = Video Off = 0 and Video On = 1.
	Example:
	`SEND_COMMAND Panel,"'^BOS-500,1,1'"`
	Sets the button to display video.

^BPP
Set or clear the protected page flip flag of a button.
	Zero clears the flag.
	Syntax:
	`"'^BPP-<vt addr range>,<protected page flip flag value>'"`
	Variable:
	variable text address range = 1 - 4000.
	protected page flip flag value range = 0 - 4 (**0 clears the flag**).
	Example:
	`SEND_COMMAND Panel,"'^BPP-500,1'"`
	Sets the button to protected page flip flag 1 (sets it to password 1).

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	

^BRD
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.
	Syntax:
	`"'^BRD-<vt addr range>,<button states range>,<border name>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	border name = Refer to the Border Styles and Programming Numbers table on page 110.
	Example:
	`SEND_COMMAND Panel,"'^BRD-500.504&510.515,1&2,Quad Line'"`
	Sets the border by name (Quad Line) to those buttons with the variable text range of 500-504 & 510-515.
	Refer to theTPD4 Border Styles by Name table on page 110.

^BSF
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.
	Syntax:
	`"'^BSF-<vt addr range>,<selection value>'"`
	Variable:
	variable text address range = 1 - 4000.
	selection value = Unselect = 0 and select = 1.
	Example:
	`SEND_COMMAND Panel,"'^BSF-500,1'"`
	Sets the focus to the text area of the button.

^BSM
Submit text for text area buttons.
	This command causes the text areas to send their text as strings to the NetLinx Master.
	Syntax:
	`"'^BSM-<vt addr range>'"`
	Variable:
	variable text address range = 1 - 4000.
	Example:
	`SEND_COMMAND Panel,"'^BSM-500'"`
	Submits the text of the text area button.

^BSO
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.
	Syntax:
	`"'^BSO-<vt addr range>,<button states range>,<sound name>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	sound name = (**blank** - sound cleared, **not matched** - button sound not changed).
	Example:
	`SEND_COMMAND Panel,"'^BSO-500,1&2,music.wav'"`
	Assigns the sound 'music.wav' to the button Off/On states.

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	
^BVL Log-On/Log-Off the computer control connection.	Syntax: "'^BVL-<vt addr range>,<connection>'" Variable: variable text address range = 1 - 4000. connection = 0 (Log-Off connection) and 1 (Log-On connection). Example: SEND_COMMAND Panel,"'^BVL-500,0'" Logs-off the computer control connection of the button.
^BVN Set the computer control remote host for the specified address.	Syntax: SEND_COMMAND <DEV>,"'^BVN-<vt addr range>,<remote host>'" Variables: variable text address range = 1 - 4000. remote host = 1 - 50 ASCII characters. Example: SEND_COMMAND Panel,"'^BVN-500,191.191.191.191'" Sets the remote host to '191.191.191.191' for the specific computer control button.
^BVP Set the network password for the specified address.	Syntax: "'^BVP-<vt addr range>,<network password>'" Variable: variable text address range = 1 - 4000. network password = 1 - 50 ASCII characters. Example: SEND_COMMAND Panel,"'^BVP-500,PCLOCK'" Sets the password to PCLOCK for the specific PC control button.
^BVT Set the computer control network port for the specified address.	Syntax: "'^BVT-<vt addr range>,<network port>'" Variable: variable text address range = 1 - 4000. network port = 1 - 65535. Example: SEND_COMMAND Panel,"'^BVT-500,5000'" Sets the network port to 5000.
^BWW Set the button word wrap feature to those buttons with a defined address range.	By default, word-wrap is Off. Syntax: "'^BWW-<vt addr range>,<button states range>,<word wrap>'" Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). word wrap = (0=Off and 1=On). Default is Off. Example: SEND_COMMAND Panel,"'^BWW-500,1,1'" Sets the word wrap on for the button's Off state.

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	
^CPF Clear all page flips from a button.	Syntax: "'^CPF-<vt addr range>'" Variable: variable text address range = 1 - 4000. Example: SEND_COMMAND Panel,"'^CPF-500'" Clears all page flips from the button.
^DLD Set the disable cradle LED flag.	Syntax: "'^DLD-<status>'" Variable: status = (**0**= cradle operates normally, **1**= forces the cradle LEDs to always be dim). Example: SEND_COMMAND Panel,"'^DLD-1'" Disables the cradle LEDs.
^DPF Delete page flips from button if it already exists.	Syntax: "'^DFP-<vt addr range>,<actions>,<page name>'" Variable: variable text address range = 1 - 4000. actions = **Stan**[dardPage] - Flip to standard page **Prev**[iousPage] - Flip to previous page **Show**[Popup] - Show Popup page **Hide**[Popup] - Hide Popup page **Togg**[lePopup] - Toggle popup state **ClearG**[roup] - Clear popup page group from all pages **ClearP**[age] - Clear all popup pages from a page with the specified page name **ClearA**[ll] - Clear all popup pages from all pages page name = 1 - 50 ASCII characters. Example: SEND COMMAND Panel,"'^DPF-409,Prev'" Deletes the assignment of a button from flipping to a previous page.
^ENA Enable or disable buttons with a set variable text range.	Syntax: "'^ENA-<vt addr range>,<command value>'" Variable: variable text address range = 1 - 4000. command value = (0= disable, 1= enable) Example: SEND_COMMAND Panel,"'^ENA-500.504&510.515,0'" Disables button pushes on buttons with variable text range 500-504 & 510-515.

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	

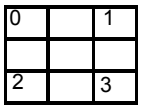
^FON
Set a font to a specific Font ID value for those buttons with a defined address range.
	Font ID numbers are generated by the TPDesign4 programmers report.
	Syntax:
	`"'^FON-<vt addr range>,<button states range>,<font value>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	font value = range = 1 - XXX. Refer to the *Default Font Styles and ID Numbers* section on page 109.
	Example:
	`SEND_COMMAND Panel,"'^FON-500.504&510.515,1&2,4'"`
	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.

NOTE

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
Change the bargraph drag increment.
	Syntax:
	`"'^GDI-<vt addr range>,<bargraph drag increment>'"`
	Variable:
	variable text address range = 1 - 4000.
	bargraph drag increment = The default drag increment is 256.
	Example:
	`SEND_COMMAND Panel,"'^GDI-7,128'"`
	Sets the bargraph with variable text 7 to a drag increment of 128.

^GIV
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.
	Syntax:
	`"'^GIV-<vt addr range>,<joystick axis to invert>'"`
	Variable:
	variable text address range = 1 - 4000.
	joystick axis to invert = 0 - 3.
	 
	
	0 = Normal
	1 = Invert horizontal axis
	2 = Invert vertical axis
	3 = Invert both axis locations
	For a bargraph 1 = Invert, 0 = Non Invert
	Example:
	`SEND_COMMAND Panel,"'^GIV-500,3'"`
	Inverts the joystick axis origin to the bottom right corner.

Download from Www.Somanuals.com. All Manuals Search And Download.

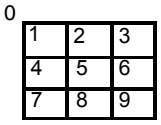
"^" Button Commands (Cont.)	
^GLH Change the bargraph upper limit.	Syntax: "'^GLH-<vt addr range>,<bargraph hi>'" Variable: variable text address range = 1 - 4000. bargraph limit range = 1 - 65535 (*bargraph upper limit range*). Example: SEND_COMMAND Panel,"'^GLH-500,1000'" Changes the bargraph upper limit to 1000.
^GLL Change the bargraph lower limit.	Syntax: "'^GLL-<vt addr range>,<bargraph low>'" Variable: variable text address range = 1 - 4000. bargraph limit range = 1 - 65535 (*bargraph lower limit range*). Example: SEND_COMMAND Panel,"'^GLL-500,150'" Changes the bargraph lower limit to 150.
^GRD Change the bargraph ramp-down time in 1/10th of a second.	Syntax: "'^GRD-<vt addr range>,<bargraph ramp down time>'" Variable: variable text address range = 1 - 4000. bargraph ramp down time = In 1/10th of a second intervals. Example: SEND_COMMAND Panel,"'^GRD-500,200'" Changes the bargraph ramp down time to 20 seconds.
^GRU Change the bargraph ramp-up time in 1/10th of a second.	Syntax: "'^GRU-<vt addr range>,<bargraph ramp up time>'" Variable: variable text address range = 1 - 4000. bargraph ramp up time = In 1/10th of a second intervals. Example: SEND_COMMAND Panel,"'^GRU-500,100'" Changes the bargraph ramp up time to 10 seconds.
^GSC Change the bargraph slider color or joystick cursor color.	A user can also assign the color by Name and R,G,B value (RRGGBB or RRGGBBAA). Syntax: "'^GSC-<vt addr range>,<color value>'" Variable: variable text address range = 1 - 4000. color value = Refer to the RGB Values for all 88 Basic Colors table on page 107. Example: SEND_COMMAND Panel,"'^GSC-500,12'" Changes the bargraph or joystick slider color to Yellow.

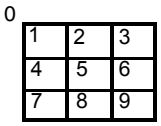
Download from Www.Somanuals.com. All Manuals Search And Download.

<table>
<tr><th colspan="2">"^" Button Commands (Cont.)</th></tr>
<tr><td>^GSN
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.
Syntax:
<code>"'^GSN-<vt addr range>,<bargraph slider name>'"</code>
Variable:
variable text address range = 1 - 4000.
bargraph slider name = See table below.
<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>Example:
<code>SEND_COMMAND Panel,"'^GSN-500,Ball'"</code>
Changes the bargraph slider name or the Joystick cursor name to 'Ball'.</td></tr>
<tr><td>^ICO
Set the icon to a button.</td><td>Syntax:
<code>"'^ICO-<vt addr range>,<button states range>,<icon index>'"</code>
Variable:
variable text address range = 1 - 4000.
button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
icon index range = 0 - 9900 (a value of 0 is clear).
Example:
<code>SEND_COMMAND Panel,"'^ICO-500.504&510.515,1&2,1'"</code>
Sets the icon for On and Off states for buttons with variable text ranges of 500-504 & 510-515.</td></tr>
<tr><td>^IRM
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).
Note: The port number of the IR will be the port number assigned in TPD4.
Syntax:
<code>"'^IRM-<port>,<channel>,<onTime>,<offTime>'"</code>
Variable:
port = User-defined port on the device (panel).
channel = 1 - 255 (channel to pulse).
onTime = 1/10th of a second.
offTime = 1/10th of a second.
Example:
<code>SEND_COMMAND Panel,"'^IRM-10,5, 20, 10'"</code>
Sets the port 10 IR channel 5 on time to 1 second and off time to 2 seconds.</td></tr>
</table>

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	

^JSB
Set bitmap/ picture 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.
	Syntax:
	`"'^JSB-<vt addr range>,<button states range>,<new text alignment>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	new text alignment = Value of 1- 9 corresponds to the following locations:
	 
	
	Zero can be used for an absolute position
	Example:
	`SEND_COMMAND Panel,"'^JSB-500.504&510.515,1&2,1'"`
	Sets the off/on state picture alignment to upper left corner for those buttons with variable text ranges of 500-504 & 510-515.

^JSI
Set icon 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.
	Syntax:
	`"'^JSI-<vt addr range>,<button states range>,<new icon alignment>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	new icon alignment = Value of 1 - 9 corresponds to the following locations:
	 
	
	Zero can be used for an absolute position
	Example:
	`SEND_COMMAND Panel,"'^JSI-500.504&510.515,1&2,1'"`
	Sets the Off/On state icon alignment to upper left corner for those buttons with variable text range of 500-504 & 510-515.

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	

^JST
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.
	Syntax:
	`"'^JST-<vt addr range>,<button states range>,<new text alignment>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	new text alignment = Value of 1 - 9 corresponds to the following locations:
	Example:
	`SEND_COMMAND Panel,"'^JST-500.504&510.515,1&2,1'"`
	Sets the text alignment to the upper left corner for those buttons with variable text ranges of 500-504 & 510-515.

^MBT
Set the Mouse Button mode On for the virtual PC.
	Syntax:
	`"'^MBT-<pass data>'"`
	Variable:
	pass data:
	0 = None
	1 = Left
	2 = Right
	3 = Middle
	Example:
	`SEND COMMAND Panel,"'^MBT-1'"`
	Sets the mouse button mode to 'Left Mouse Click'.

^MDC
Turn On the 'Mouse double-click' feature for the virtual PC.
	Syntax:
	`"'^MDC'"`
	Example:
	`SEND COMMAND Panel,"'^MDC'"`
	Sets the mouse double-click for use with the virtual PC.

^SHO
Show or hide a button with a set variable text range.
	Syntax:
	`"'^SHO-<vt addr range>,<command value>'"`
	Variable:
	variable text address range = 1 - 4000.
	command value = (0= hide, 1= show).
	Example:
	`SEND_COMMAND Panel,"'^SHO-500.504&510.515,0'"`
	Hides buttons with variable text address range 500-504 & 510-515.

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	

^TEC
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).
	Syntax:
	`"'^TEC-<vt addr range>,<button states range>,<color value>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	color value = Refer to the RGB Values for all 88 Basic Colors table on page 107.
	Example:
	`SEND_COMMAND Panel,"'^TEC-500.504&510.515,1&2,12'"`
	Sets the text effect color to Very Light Yellow on buttons with variable text 500-504 and 510-515.

^TEF
Set the text effect.
	The Text Effect is specified by name and can be found in TPD4.
	Syntax:
	`"'^TEF-<vt addr range>,<button states range>,<text effect name>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	text effect name = **Refer to the Text Effects table on page 133 for a listing of text effect names**.
	Example:
	`SEND_COMMAND Panel,"'^TEF-500.504&510.515,1&2,Soft Drop Shadow 3'"`
	Sets the text effect to Soft Drop Shadow 3 for the button with variable text range 500-504 and 510-515.

^TXT
Assign a text string to those buttons with a defined address range.
	Sets Non-Unicode text.
	Syntax:
	`"'^TXT-<vt addr range>,<button states range>,<new text>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	new text = 1 - 50 ASCII characters.
	Example:
	`SEND_COMMAND Panel,"'^TXT-500.504&510.515,1&2,Test Only'"`
	Sets the On and Off state text for buttons with the variable text ranges of 500-504 & 510-515.

Download from Www.Somanuals.com. All Manuals Search And Download.

"^" Button Commands (Cont.)	

^UNI
Set Unicode text.
	For the ^UNI command (%UN and ^BMF command), the Unicode text is sent as ASCII-HEX nibbles.
	Syntax:
	`"'^UNI-<vt addr range>,<button states range>,<unicode text>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	unicode text = Unicode HEX value.
	Example:
	`SEND_COMMAND Panel,"'^UNI-500,1,0041'"`
	Sets the button's unicode character to 'A'.
	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:
	`SEND_COMMAND TP,"'^UNI-1,0,0041'"`
	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.

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. • If the panel has no information within the User Access Passwords list, 'none' is sent as a user. • If the undock button on the Protected Setup page is used, 'setup' is sent as a user. • This string can be disabled from within the firmware setup pages.
dock	This is sent to the target Master when the MVP is docked. • 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. With the MVOP-5200i, a password must be entered to remove the panel from the Wall Charging Station. Only the passcode is entered. The user entry is just for identifying the passcodes.

MVP Panel Lock Passcode Commands	

^LPC
Clear all users from the User Access Passwords list on the Password Setup page.
	Syntax:
	`"'^LPC'"`
	Example:
	`SEND_COMMAND Panel,"'^LPC'"`
	Clear all users from the User Access Password list on the Password Setup page. Refer to the *Other Settings* section on page 87 for more information.

Download from Www.Somanuals.com. All Manuals Search And Download.

MVP Panel Lock Passcode Commands (Cont.)	

^LPR
Remove a given user from the User Access Passwords list on the Password Setup page.
	Syntax:
	`"'^LPR-<user>'"`
	Variable:
	user = 1 - 50 ASCII characters.
	Example:
	`SEND_COMMAND Panel,"'^LPR-Robert'"`
	Remove user named 'Robert' from the User Access Password list on the Password Setup page. Refer to the *Other Settings* section on page 87 for more information.

^LPS
Set the user name and password.
	This command allows you to:
	1. Add a new user name and password OR
	2. Set the password for a given user.
	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.
	Syntax:
	`"'^LPS-<user>,<passcode>'"`
	Variable:
	user = 1 - 50 ASCII characters.
	passcode = 1 - 50 ASCII characters.
	Example:
	`SEND_COMMAND Panel,"'^LPS-Manager,undock'"`
	Sets a new user name as "Manager" and the password to "undock".
	Example 2:
	`SEND_COMMAND Panel,"'^LPS-Manager,test'"`
	Changes the given user name password to "test".
	Refer to the *Other Settings* section on page 87 for more information.

Text Effects Names

The following is a listing of text effects names associated with the **^TEF** command on page 131.

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Text Effects (Cont.)	
• 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))"
}
```


Download from Www.Somanuals.com. All Manuals Search And Download.

All custom events have the following 7 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
Get the current border color.
	Syntax:
	`"'?BCB-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1011:**
	Flag - zero
	Value1 - Button state number
	Value2 - Actual length of string (should be 9)
	Value3 - Zero
	Text - Hex encoded color value (ex: #000000FF)
	Text length - Color name length (should be 9)
	Example:
	`SEND COMMAND Panel,"'?BCB-529,1'"`
	Gets the button 'OFF state' border color. information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1011
	Flag = 0
	VALUE1 = 1
	VALUE2 = 9
	VALUE3 = 0
	TEXT = #222222FF
	TEXT LENGTH = 9

Download from Www.Somanuals.com. All Manuals Search And Download.

Button Query Commands (Cont.)	

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

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Button Query Commands (Cont.)	

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

?BOP
Get the overall button opacity.
	Syntax:
	`"'?BOP-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1015:**
	Flag - Zero
	Value1 - Button state number
	Value2 - Opacity
	Value3 - Zero
	Text - Blank
	Text length - Zero
	Example:
	`SEND COMMAND Panel,"'?BOP-529,1'"`
	Gets the button 'OFF state' opacity information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1015
	Flag = 0
	VALUE1 = 1
	VALUE2 = 200
	VALUE3 = 0
	TEXT =
	TEXT LENGTH = 0

Download from Www.Somanuals.com. All Manuals Search And Download.

Button Query Commands (Cont.)	
?BRD Get the current border name.	Syntax: "'?BRD-<vt addr range>,<button states range>'" Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1014:** Flag - Zero Value1 - Button state number Value2 - Actual length of string Value3 - Zero Text - String that represents border name Text length - Border name length Example: SEND COMMAND Panel,"'?BRD-529,1'" Gets the button 'OFF state' border information. The result sent to the Master would be: ButtonGet Id = 529 Type = 1014 Flag = 0 VALUE1 = 1 VALUE2 = 22 VALUE3 = 0 TEXT = Double Bevel Raised -L TEXT LENGTH = 22
?BWW Get the current word wrap flag status.	Syntax: "'?BWW-<vt addr range>,<button states range>'" Variable: variable text address range = 1 - 4000. button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state). custom event type **1010:** Flag - Zero Value1 - Button state number Value2 - 0 = no word wrap, 1 = word wrap Value3 - Zero Text - Blank Text length - Zero Example: SEND COMMAND Panel,"'?BWW-529,1'" Gets the button 'OFF state' word wrap flag status information. The result sent to the Master would be: ButtonGet Id = 529 Type = 1010 Flag = 0 VALUE1 = 1 VALUE2 = 1 VALUE3 = 0 TEXT = TEXT LENGTH = 0

Download from Www.Somanuals.com. All Manuals Search And Download.

Button Query Commands (Cont.)	

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

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

Download from Www.Somanuals.com. All Manuals Search And Download.

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Button Query Commands (Cont.)	

?JST
Get the current text justification.
	Syntax:
	`"'?JST-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1004:**
	Flag - Zero
	Value1 - Button state number
	Value2 - 1 - 9 justify
	Value3 - Zero
	Text - Blank
	Text length - Zero
	Example:
	`SEND COMMAND Panel,"'?JST-529,1'"`
	Gets the button 'OFF state' text justification information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1004
	Flag = 0
	VALUE1 = 1
	VALUE2 = 1
	VALUE3 = 0
	TEXT =
	TEXT LENGTH = 0

?TEC
Get the current text effect color.
	Syntax:
	`"'?TEC-<vt addr range>,<button states range>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	custom event type **1009:**
	Flag - Zero
	Value1 - Button state number
	Value2 - Actual length of string (should be 9)
	Value3 - Zero
	Text - Hex encoded color value (ex: #000000FF)
	Text length - Color name length (should be 9)
	Example:
	`SEND COMMAND Panel,"'?TEC-529,1'"`
	Gets the button 'OFF state' text effect color information.
	The result sent to the Master would be:
	ButtonGet Id = 529 Type = 1009
	Flag = 0
	VALUE1 = 1
	VALUE2 = 9
	VALUE3 = 0
	TEXT = #5088F2AE
	TEXT LENGTH = 9

Download from Www.Somanuals.com. All Manuals Search And Download.

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Panel Runtime Operations

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

Panel Runtime Operation Commands	

ABEEP
Output a single beep even if beep is Off.
	Syntax:
	`"'ABEEP'"`
	Example:
	`SEND COMMAND Panel,"'ABEEP'"`
	Outputs a beep of duration 1 beep even if beep is Off.

ADBEEP
Output a double beep even if beep is Off.
	Syntax:
	`"'ADBEEP'"`
	Example:
	`SEND COMMAND Panel,"'ADBEEP'"`
	Outputs a double beep even if beep is Off.

@AKB
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.
	Syntax:
	`"'@AKB-<initial text>;<prompt text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	`prompt text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'@AKB-Texas;Enter State'"`
	Pops up the Keyboard and initializes the text string 'Texas' with prompt text 'Enter State'.

AKEYB
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.
	Syntax:
	`"'AKEYB-<initial text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'AKEYB-This is a Test'"`
	Pops up the Keyboard and initializes the text string 'This is a Test'.

AKEYP
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.
	Syntax:
	`"'AKEYP-<number string>'"`
	Variables:
	`number string = 0 - 9999.`
	Example:
	`SEND COMMAND Panel,"'AKEP-12345'"`
	Pops up the Keypad and initializes the text string '12345'.

AKEYR
Remove the Keyboard/ Keypad.
	Remove keyboard or keypad that was displayed using 'AKEYB', 'AKEYP', 'PKEYP', @AKB, @AKP, @PKP, @EKP, or @TKP commands.
	Syntax:
	`"'AKEYR'"`
	Example:
	`SEND COMMAND Panel,"'AKEYR'"`
	Removes the Keyboard/Keypad.

Download from Www.Somanuals.com. All Manuals Search And Download.

Panel Runtime Operation Commands (Cont.)	

@AKP
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.
	Syntax:
	`"'@AKP-<initial text>;<prompt text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	`prompt text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'@AKP-12345678;ENTER PASSWORD'"`
	Pops up the Keypad and initializes the text string '12345678' with prompt text 'ENTER PASSWORD'.

@AKR
Remove the Keyboard/ Keypad.
	Remove keyboard or keypad that was displayed using 'AKEYB', 'AKEYP', 'PKEYP', @AKB, @AKP, @PKP, @EKP, or @TKP commands.
	Syntax:
	`"'@AKR'"`
	Example:
	`SEND COMMAND Panel,"'@AKR'"`
	Removes the Keyboard/Keypad.

BEEP
Output a beep.
	Syntax:
	`"'BEEP'"`
	Example:
	`SEND COMMAND Panel,"'BEEP'"`
	Outputs a beep.

BRIT
Set the panel brightness.
	Syntax:
	`"'BRIT-<brightness level>'"`
	Variable:
	brightness level = 0 - 100.
	Example:
	`SEND COMMAND Panel,"'BRIT-50'"`
	Sets the brightness level to 50.

@BRT
Set the panel brightness.
	Syntax:
	`"'@BRT-<brightness level>'"`
	Variable:
	brightness level = 0 - 100.
	Example:
	`SEND COMMAND Panel,"'@BRT-70'"`
	Sets the brightness level to 70.

DBEEP
Output a double beep.
	Syntax:
	`"'DBEEP'"`
	Example:
	`SEND COMMAND Panel,"'DBEEP'"`
	Outputs a double beep.

Download from Www.Somanuals.com. All Manuals Search And Download.

Panel Runtime Operation Commands (Cont.)	

@EKP
Extend the Keypad.
	Pops up the keypad icon and initializes the text string to that specified. The Prompt Text is optional.
	Syntax:
	`"'@EKP-<initial text>;<prompt text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	`prompt text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'@EKP-33333333;Enter Password'"`
	Pops up the Keypad and initializes the text string '33333333' with prompt text 'Enter Password'.

PKEYP
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.
	Syntax:
	`"'PKEYP-<initial text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'PKEYP-123456789'"`
	Pops up the Keypad and initializes the text string '123456789' in '*'.

@PKP
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.
	Syntax:
	`"'@PKP-<initial text>;<prompt text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	`prompt text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'@PKP-1234567;ENTER PASSWORD'"`
	Pops up the Keypad and initializes the text string 'ENTER PASSWORD' in '*'.

SETUP
Send panel to SETUP page.
	Syntax:
	`"'SETUP'"`
	Example:
	`SEND COMMAND Panel,"'SETUP'"`
	Sends the panel to the Setup Page.

SHUTDOWN
Shut down the batteries providing power to the panel.
	Syntax:
	`"'SHUTDOWN'"`
	Example:
	`SEND COMMAND Panel,"'SHUTDOWN'"`
	Shuts-down the batteries feeding power to the panel. This function saves the battery from discharging.

SLEEP
Force the panel into screen saver mode.
	Syntax:
	`"'SLEEP'"`
	Example:
	`SEND COMMAND Panel,"'SLEEP'"`
	Forces the panel into screen saver mode.

Download from Www.Somanuals.com. All Manuals Search And Download.

Panel Runtime Operation Commands (Cont.)	

@SOU
Play a sound file.
	Syntax:
	`"'@SOU-<sound name>'"`
	Variables:
	`sound name = Name of the sound file. Supported sound file formats are: WAV & MP3.`
	Example:
	`SEND COMMAND Panel,"'@SOU-Music.wav'"`
	Plays the 'Music.wav' file.

@TKP
Present a telephone keypad.
	Pops up the keypad icon and initializes the text string to that specified. The Prompt Text is optional.
	Syntax:
	`"'@TKP-<initial text>;<prompt text>'"`
	Variables:
	`initial text = 1 - 50 ASCII characters.`
	`prompt text = 1 - 50 ASCII characters.`
	Example:
	`SEND COMMAND Panel,"'@TKP-999.222.1211;Enter Phone Number'"`
	Pops-up the Keypad and initializes the text string '999.222.1211' with prompt text 'Enter Phone Number'.

TPAGEON
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.
	Syntax:
	`"'TPAGEON'"`
	Example:
	`SEND COMMAND Panel,"'TPAGEON'"`
	Turns On page tracking.

TPAGEOFF
Turn Off page tracking.
	Syntax:
	`"'TPAGEOFF'"`
	Example:
	`SEND COMMAND Panel,"'TPAGEOFF'"`
	Turns Off page tracking.

@VKB
Popup the virtual keyboard.
	Syntax:
	`"'@VKB'"`
	Example:
	`SEND COMMAND Panel,"'@VKB'"`
	Pops-up the virtual keyboard.

WAKE
Force the panel out of screen saver mode.
	Syntax:
	`"'WAKE'"`
	Example:
	`SEND COMMAND Panel,"'WAKE'"`
	Forces the panel out of the screen saver mode.

Download from Www.Somanuals.com. All Manuals Search And Download.

Input Commands

These Send Commands are case insensitive.

Input Commands	

^CAL
Put panel in calibration mode.
	Syntax:
	`"'^CAL'"`
	Example:
	`SEND COMMAND Panel,"'^CAL'"`
	Puts the panel in calibration mode.

^KPS
Set the keyboard passthru.
	Syntax:
	`"'^KPS-<pass data>'"`
	Variable:
	pass data:
	<blank/empty> = Disables the keyboard.
	0 = Pass data to G4 application (default). This can be used with VPC or text areas.
	1 - 4 = Not used.
	5 = Sends out data to the Master.
	Example:
	`SEND COMMAND Panel,"'^KPS-5'"`
	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.
	Example 2:
	`SEND COMMAND Panel,"'^KPS-0'"`
	Disables the keyboard passthru to the Master.
	The following point defines how the parameters within this command work:
	• Accepts keystrokes from any of these sources: attached USB keyboard or Virtual keyboard.

^VKS
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.
	Refer to theEmbedded Codes table on page 148 that define special characters which can be included with the string but may not be represented by the ASCII character set.
	Syntax:
	`"'^VKS-<string>'"`
	Variable:
	string = Only 1 string per command/only one stroke per command.
	Example:
	`SEND COMMAND Panel,"'^VKS-'8"`
	Sends out the keystroke 'backspace' to the G4 application.

Download from Www.Somanuals.com. All Manuals Search And Download.

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Panel Setup Commands

These commands are case insensitive.

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Dynamic Image Commands

The following is a listing and descriptions of Dynamic Image Commands.

Dynamic Image Commands	

^BBR
Set the bitmap of a button to use a particular resource.
	Syntax:
	`"'^BBR-<vt addr range>,<button states range>,<resource name>'"`
	Variable:
	variable text address range = 1 - 4000.
	button states range = 1 - 256 for multi-state buttons (0 = All states, for General buttons 1 = Off state and 2 = On state).
	resource name = 1 - 50 ASCII characters.
	Example:
	`SEND_COMMAND Panel,"'^BBR-700,1,Sports_Image'"`
	Sets the resource name of the button to 'Sports_Image'.

^RAF	See page 151.

^RFR
Force a refresh for a given resource.
	Syntax:
	`"'^RFR-<resource name>'"`
	Variable:
	resource name = 1 - 50 ASCII characters.
	Example:
	`SEND_COMMAND Panel,"'^RFR-Sports_Image'"`
	Forces a refresh on 'Sports_Image'.

^RMF
Modify an existing resource.
	Syntax:
	`"'^RMF-<resource name>,<data>'"`
	Variable:
	resource name = 1 - 50 ASCII characters
	data = Refer to the table in the RAF command for more information.
	Example:
	`SEND_COMMAND Panel,"'^RMF-Sports_Image,%ALab_Test/Images%Ftest.jpg'"`
	Changes the resource 'Sports_Image' file name to 'test.jpg' and the path to 'Lab_Test/Images'.

^RSR
Change the refresh rate for a given resource.
	Syntax:
	`"'^RSR-<resource name>,<refresh rate>'"`
	Variable:
	resource name = 1 - 50 ASCII characters.
	refresh rate = Measured in seconds.
	Example:
	`SEND_COMMAND Panel,"'^RSR-Sports_Image,5'"`
	Sets the refresh rate to 5 seconds for the given resource ('Sports_Image').

Download from Www.Somanuals.com. All Manuals Search And Download.

Dynamic Image Commands (Cont.)

^RAF

Add new resources.

Adds any and all resource parameters by sending embedded codes and data.

Syntax:

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

Variable:

resource name = 1 - 50 ASCII characters.

data = Refers to the embedded codes, see table below.

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. The only exception to this is the inclusion of special escape sequences and in the case of the FTP protocol, regular expressions.
path	'%A<path>'	Set Directory path. The path must be a valid HTTP URL minus the protocol, host, and filename. The only exception to this is the inclusion of special escape sequences and in the case of the 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. The default value is 0 (only download the resource once).
newest	'%N<0-1>'	Set the newest file. A value of 1 means that only the most recent file matching the pattern is downloaded.
preserve	'%V<0-1>'	Set the value of the preserve flag. Default is 0. Currently preserve has no function.

Example:

```
SEND_COMMAND Panel,"'^RAF-New Image,%P0%HAMX.COM%ALab/
Test_file%Ftest.jpg'"
```

Adds a new resource. The resource name is 'New Image', %P (protocol) is an HTTP, %H (host name) is ***AMX.COM***, %A (file path) is Lab/Test file, and %F (file name) is ***test.jpg***.

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

Battery Life and Replacement

Overview

The battery powering the MVP-5200i is designed for upwards of 300 deep discharge rechargings. Regular shallow rechargings will extensively increase expected battery life, and the device should be stored in either the Table Charging Station or the Wall Charging Station when not in use to keep it at an optimum charge. The battery has reached its effective end of life after it can no longer hold more than a 70 percent charge.

Unlike traditional Lithium Ion batteries, the Lithium Polymer battery in the MVP-5200i has a very small charge retention decline as it is discharged and recharged.

This device has a risk of explosion if the battery is replaced with an incorrect type. Be sure to dispose of used batteries in a correct manner.

Power Management

Since the MVP-5200i is a battery-powered handheld device, power management is a necessary concern. Under active use, the charge on the integral Lithium Polymer battery can last for as long as five days. However, to maximize usability and minimize the chances of the device becoming completely discharged at a critical moment, the MVP-5200i should be kept in its charging cradle or wall station when not in use.

The MVP-5200i operates on three distinct power modes:

- **Awake** - This is the normal power mode of the panel during operation. In this mode, all necessary modules are powered up and their respective clocks are being driven appropriately. The device remains online with the Netlinx Master and continues to appear in the online tree of Netlinx Studio.
- **Sleep** - This mode of operation can be selected through the Setup Pages and only controls the backlight. In this case, the unit remains on all the time, and only the backlight will be turned off after the user-selectable time of inactivity has elapsed. The device remains online with the Netlinx Master and continues to be shown in the online tree of Netlinx Studio. The unit shall transfer to the Awake mode after it detects a touch on the touchscreen or navigation wheel. This mode uses 80 percent of the power required for the Awake mode.
- **Processor Shutdown** - The system enters this mode after a user selectable amount of inactivity time has elapsed or if the battery level falls below10 percent of its full charge. This is the absolute lowest mode of operation, during which power to all peripherals and components is turned off. It is not online with the NetLinx Master and will not appear in NetLinx Studio. The system remains in this mode until either it is rebooted or the battery is completely shut down. In the latter case, the panel has to be placed in a Table Charging Station in order for it to be operational.

Download from Www.Somanuals.com. All Manuals Search And Download.

Battery Replacement

The touch panel's battery is intended to last the life of the device, but in cases where the battery has reached its effective end of life, it may be replaced with the MVP-BP-52 Battery Pack Kit (**FG5966-20**). To replace the battery:

1. Shut down the device.
2. Place the device face-down and remove the five screws from the back of the device (FIG. 89).
   - Two of the screws are at each of the upper corners of the device, underneath screw covers. Remove the screw covers to access the screws.
   - Lift up the kickstand to reach the remaining three screws.

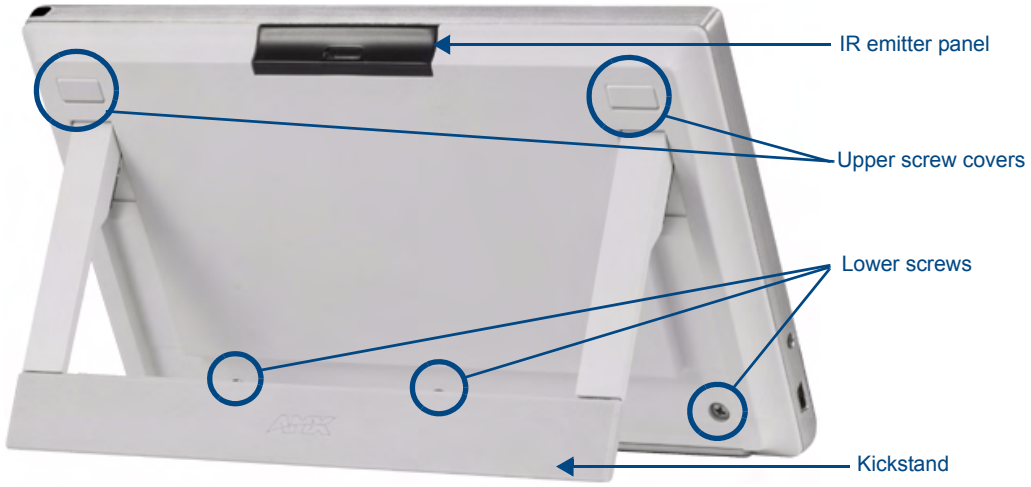


FIG. 89 Screw placement at the back of the MVP-5200i- GW

3. Carefully remove the back of the device, making sure not to dislodge the IR emitter panel.
4. Disconnect and remove the old battery from the female connector (FIG. 90).
5. Connect the new battery, making sure to seat fully the battery's female connector to the male connector in the device. Use a clean, nonconductive stick or probe to seat the connectors.
6. Install the new battery, making sure that the label faces outward and the battery connector wiring runs to the left (FIG. 90). Make sure that the excess battery wiring fits in the space to the bottom left of the battery.

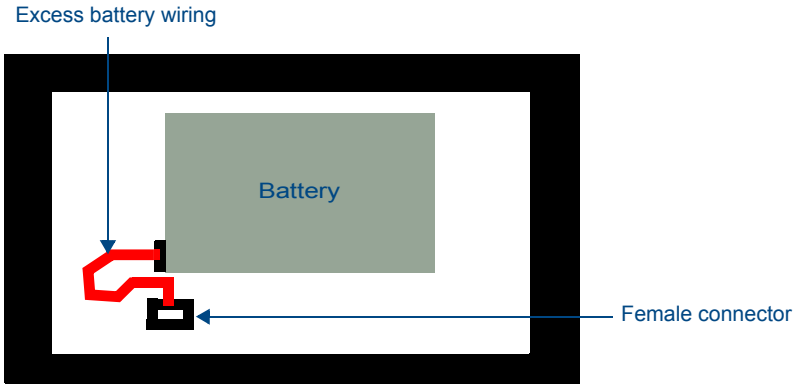


FIG. 90 Battery installation and connection diagram

7. Reattach the back of the device.

Download from Www.Somanuals.com. All Manuals Search And Download.

8. Insert the five screws and replace the screw covers atop the two upper screws, using the replacement upper screw covers included in the Battery Pack Kit.
9. Restart the device to confirm that the new battery is functioning correctly.

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

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

Download from Www.Somanuals.com. All Manuals Search And Download.

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

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 116).
- ^BMF subcommand **%MK** - sets the input mask of a text area (see the *^BMF* section on page 118).

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

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

Download from Www.Somanuals.com. All Manuals Search And Download.

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*.

NOTE

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

Download from Www.Somanuals.com. All Manuals Search And Download.

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

- **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.

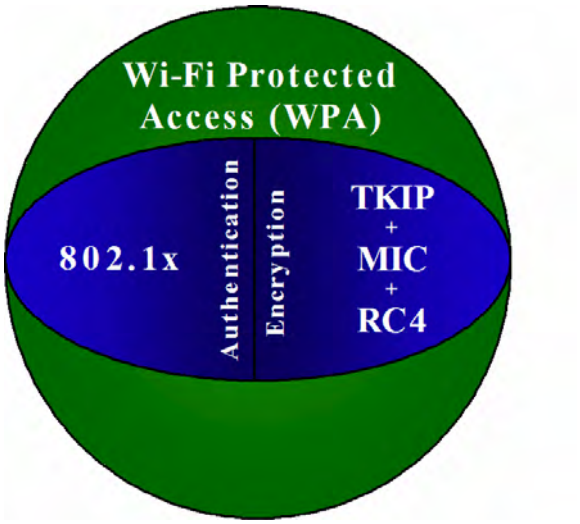


FIG. 91 WPA Overview

Download from Www.Somanuals.com. All Manuals Search And Download.

- **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).

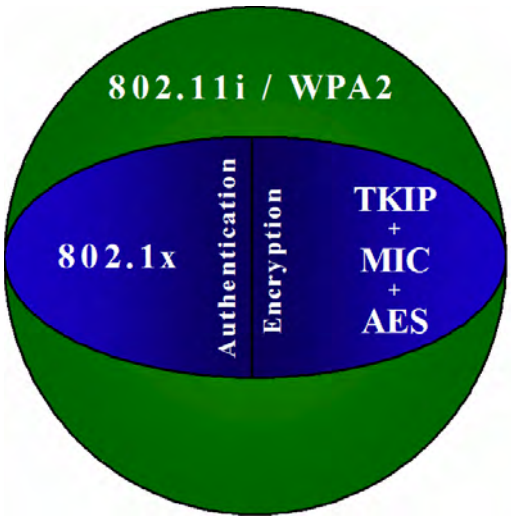


FIG. 92 WPA2 Overview

Download from Www.Somanuals.com. All Manuals Search And Download.

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 • Fixed Passwords • One-time passwords (tokens)	• Client authentication is done via password and certificates • Server authentication is done via certificates	• High Security	• Moderately difficult to deploy
EAP-PEAP	• Certificates • Fixed Passwords • One-time passwords (tokens)	• Client authentication is done via password and certificates • Server authentication is done via certificates	• High Security	• Moderately difficult to deploy
EAP-LEAP	• Certificates • Fixed Passwords • One-time passwords (tokens)	• Authentication is based on MS-CHAP and MS-CHAPv2 authentication protocols	• Easy deployment	• Susceptible to dictionary attacks
EAP-FAST	• Certificates • Fixed Passwords • One-time passwords (tokens)	• N/A	• N/A	• N/A

Download from Www.Somanuals.com. All Manuals Search And Download.

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.

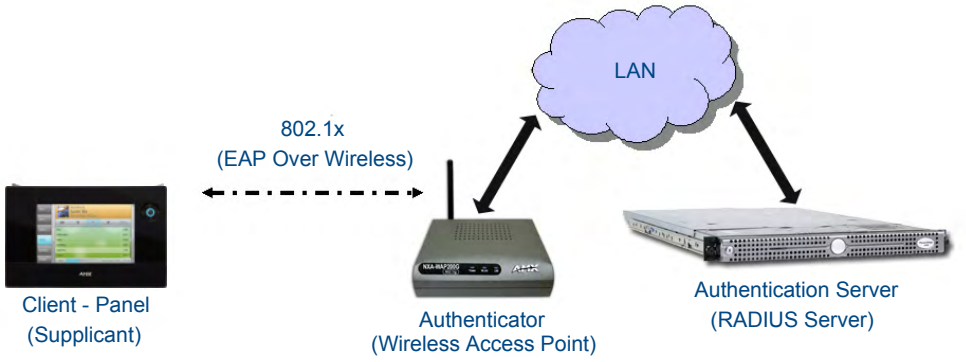


FIG. 93 EAP security method in process

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

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.

NOTE

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)

Configuring your MVP-5200i for USB Communication

For a personal computer to establish a connection to a Modero panel via USB, the target computer must have the appropriate AMX USB driver installed. This installation is bundled into the latest TPDesign4 and NetLinx Studio2 software setup process or can be downloaded independently from the main Application Files page on www.amx.com.

NOTE

Close the Certificate Upload Utility before configuring the touch panel's USB driver. Only after the panel has been successfully setup to communicate via USB can you then re-launch the utility.

Step 1: Setup the Panel and PC for USB Communication

1. If you do not currently have the latest version of TPDesign4, navigate to **www.amx.com > Tech Center > Downloadable Files > Application Files > NetLinx Design Tools** and locate the AMX USB Driver executable (AMX USBLAN Setup exe).
2. Download this executable file to a known location on your computer.
3. Launch the Setup.exe and follow the on-screen prompts to complete the installation.

Download from Www.Somanuals.com. All Manuals Search And Download.

Step 2: Confirm the Installation of the USB Driver on the PC

The first time each AMX touch panel is connected to the PC, it is detected as a new hardware device and the panel-specific USBLAN driver becomes associated with it. Each time thereafter, the panel is "recognized" as a unique USBLAN device and the association to the driver is done in the background. When the panel is detected for the first time, some user intervention is required during the association between panel and driver.

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.

If the panel is already powered, continue with steps 3. The panel MUST be powered and configured for USB communication before connecting the mini-USB connector to the panel's Program Port.

2. Feed power to the docked MVP-5200i by connecting the appropriate power supply to the Charging Station.
3. After the panel powers up, access the firmware setup pages by selecting the option from the main page.
4. Select *Protected Setup* > *System Settings* (located on the lower-left) to open the *System Settings* page.
5. Toggle the blue *Type* field (from the Master Connection section) until the choice cycles to **USB**.
   - The connection remains RED after changing the communication from Ethernet to USB until the panel is rebooted.
   - Once the panel restarts, the connection turns a dark green until connected to an active USB cable.
6. Press the **Back** button on the touch panel to return to the Protected Setup page.
7. 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.
8. Only **AFTER** the unit displays the first panel page should you 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 this is your first time installing the USB driver, a USB driver installation popup window appears on the PC.
9. Complete the USB driver installation process by clicking **Yes** and then installing the new AMX USB LAN LINK when told that a new USB device was found. This action accepts the installation of the new AMX USB driver.
10. Reboot the panel. Once restarted, the panel is now configured to communicate directly with the PC.

The mini-USB connector MUST be then plugged into an already active panel before the PC can recognize the connection and assign an appropriate USB driver. This driver is part of both the NetLinx Studio and TPDesign4 software application installations.

11. Launch the Certificate Upload Utility and confirm the utility has detected the new USB connection to the panel:
    - Click on the *Local Address* field's drop-down arrow.
    - Confirm the new USB entry shows up in the list as: **10.XX.XX.1**.

Download from Www.Somanuals.com. All Manuals Search And Download.

How to Upload 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 MVP-5200i.
   - Refer to Step 1 from within the previous *Step 1: Setup the Panel and PC for USB Communication* section on page 168.
2. Access the target panel's Protected Setup firmware page and configure the USB communication parameters.
   - Refer to Step 2 from within the previous *Step 2: Confirm the Installation of the USB Driver on the PC* section on page 169.
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.

Download from Www.Somanuals.com. All Manuals Search And Download.

Appendix C: Troubleshooting

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: *When calibrating the MVP-5200i, 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.*

Verify that the protective laminate 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.

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 Batteries page on the MVP to see any charging activity on the bar graphs.

   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:

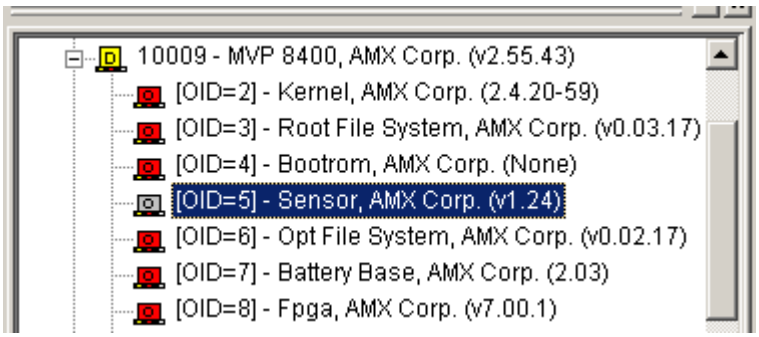


FIG. 94 "Sensor" device in the Online Tree tab

Download from Www.Somanuals.com. All Manuals Search And Download.

MVP-5200i 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.

Download from Www.Somanuals.com. All Manuals Search And Download.

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

Download from Www.Somanuals.com. All Manuals Search And Download.

4/08 ©2007 AMX. All rights reserved. AMX and the AMX logo are registered trademarks of AMX. AMX reserves the right to alter specifications without notice at any time.

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com