Operation/Reference Guide

NI-3101-SIG

Signature Series NetLinx Integrated Controller

Central Controllers

Last Revised: 9/13/2011

AMX Limited Warranty and Disclaimer

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

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

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

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

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

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

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

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

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

AMX Software License and Warranty Agreement

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

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

Table of Contents

Introduction

The NI-3101-SIG Signature Series NetLinx Integrated Controller satisfies the control and automation features common in a larger area or multiple rooms, which may include the integration of a larger number of devices including VCR and DVD players, projectors, lighting, thermostats and other electronic equipment. In technology-driven environments, this solution allows for the future addition of more devices and control capabilities.

The NI-3101-SIG features an easy-to-install form factor that mounts into 1 unit of rack space and provides extended rack depth to simplify rear connections. Its sleek, gloss black faceplate complements the Tango Distributed Audio line and Metreau Keypads. For smaller business and home applications, the NI-3101-SIG includes just the right mix of ports and features.

NetLinx Integrated Master Controller Features	
NI-3101-SIG (FG2105-08)	• 1 low-speed USB connection for configuration • 6 RS-232/RS-422/RS-485 ports • 8 IR/Serial Output ports • 8 Digital Input/Output ports • 8 Relays

The NI-3101-SIG is Duet-compatible and can be upgraded via firmware. Duet is a dual-interpreter firmware platform from AMX which combines the proven reliability and power of NetLinx with the extensive capabilities of the *Java®2 MicroEdition* (J2ME) platform. Duet simplifies the programming of a system that includes third party devices by standardizing device and function definitions, defaulting touch panel button assignments, and controlling feedback methods. Dynamic Device Discovery makes integration even easier by automatically identifying and communicating with devices which support this new beaconing technology. Refer to the *System Settings - Manage Other Devices - Dynamic Device Discovery Pages* section on page 80 for more detailed information on the use of *Dynamic Device Discovery* (DDD).

The NI-3101-SIG uses a combination lithium battery and clock crystal package called a ***Timekeeper***. Only one *Timekeeper* unit is installed within a given NI-3101. The battery can be expected to have up to 3 years of usable life under very adverse conditions. Actual life is appreciably longer under normal operating conditions. This calculation is based on storing the unit without power in 50° C (120° F) temperature until battery levels are no longer acceptable. The part number for a replacement battery is *57-0032*.

RISK OF EXPLOSION IF BATTERY IS REPLACED WITH AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO MANUFACTURER'S INSTRUCTIONS.

NI-3101-SIG Specifications

The NI-3101-SIG (FIG. 1) provides support for **6** configurable RS-232/RS-422/RS-485 Ports, **8** IR/Serial Output ports, **8** Digital Input/Output ports, and **8** Relays.

FIG. 1 NI-3101 NetLinx Integrated Controller (front view)

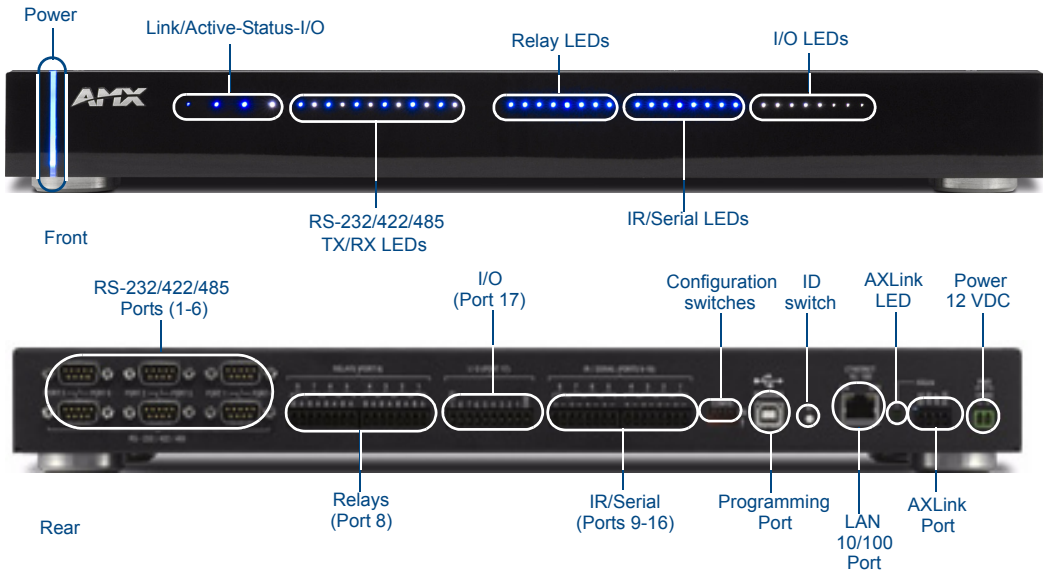


FIG. 2 NI-3101 front and rear panel connectors and components

NI-3101-SIG Specifications (Cont.)	
Dimensions (HWD):	• 2" (with feet) x 17" x 10" (5.1 cm x 43.2 cm x 26.35 cm) • 1 RU (rack unit) high
Power Requirement:	900 mA @ 12 VDC
Memory:	• 64 MB SDRAM • 256 MB Flash • 1 MB Non-volatile (NV) SRAM
Compact Flash:	128 MB Card (upgradeable) (refer to the Other AMX Equipment section for more information)
Weight:	6.95 lbs (3.15 kg)
Enclosure:	Metal with black matte finish and translucent polycarbonate faceplate
Certifications:	• FCC Part 15 Class B • CE • IEC 60950
Front Panel Components:	
POWER	Blue LED bar lights when powered up
LINK/ACTIVE	Blue LED blinks when the LAN cable is connected and an active link is established. This LED also blinks when receiving LAN data packets.
Status	Blue LED blinks to indicate that the system is programmed and communicating properly.

NI-3101-SIG Specifications (Cont.)	
Input/Output LEDs	White Output LED blinks when the Controller transmits data, sets channels On/Off, sends data strings, etc. White Input LED blinks when it receives data from button pushes, strings, commands, channel levels, etc.
RS-232/422/485 LEDs	Six sets of blue and white LEDs light to indicate the rear serial Ports 1 - 6 are transmitting or receiving RS-232, 422, or 485 data: • TX LEDs (blue) light when transmitting data • RX LEDs (white) light when receiving data • LED activity reflects transmission and reception activity
Relay LEDs	Eight blue LEDs light to indicate the rear relay channels 1 - 8 are active (closed). • These LEDs reflect the state of the relay on Port 8 • If the relay is engaged = LED On and if the relay is Off = LED Off
IR/Serial LEDs	Eight blue LEDs light to indicate the rear IR/Serial channels 1 - 8 are transmitting control data on Ports 9 - 16. • LED indicator for each IR port remains lit for the length of time that IR/Serial data is being generated.
I/O LEDs	Eight white LEDs light when the rear I/O channels 1-8 are active • LED indicator for each I/O port reflects the state of that particular port.
Rear Panel Connectors:	
RS-232/422/485 (**Ports 1 - 6**)	Six RS-232/422/485 control ports using DB9 (male) connectors with XON/XOFF (transmit on/transmit off), CTS/RTS (clear to send/ready to send), and 300-115,200 baud. • Channel range = 1-255 • Channels 1-254 provide feedback • Channel 255 (CTS Push channel): Reflects the state of the CTS Input if a 'CTSPSH' command was sent to the port • Output data format for each port is selected via software • Six DB9 connectors provide RS-232/422/485 termination
Relay (**Port 8**)	Eight-channel single-pole single-throw relay ports. • Each relay is independently controlled. • Supports up to 8 independent external relay devices • Channel range = 1-8 • Each relay can switch up to 24 VDC or 28 VAC @ 1 A • Two 8-pin 3.5 mm mini-Phoenix (female) connectors provide relay termination
Digital I/O (**Port 17**)	Eight-channel binary I/O port for contact closure. • Each input is capable of voltage sensing. Input format is software selectable. • Interactive power sensing for IR ports • Channel range = 1-8 • All inputs are assigned to respective IR/Serial ports for "automatic" power control through the use of software commands. Power control is provided via commands such as: 'PON', 'POF', 'POD', 'DELAY', I/O Link etc.). • Contact closure between GND and an I/O port is detected as a PUSH • When used as voltage input - I/O port detects a low signal (0- 1.5 VDC) as a PUSH and a high signal (3.5 - 5 VDC) as a RELEASE • When used as an output - each I/O port acts as a switch to GND and is rated at 200 mA @ 12 VDC • 10-pin 3.5 mm mini-Phoenix (female) connector provides I/O port termination ***Note**: This IO port uses 5V logic, but can handle up to 12V on the input without harm. Higher voltages run a higher risk of surge damage.*

NI-3101-SIG Specifications (Cont.)	
IR/Serial (**Ports 9 - 16**)	Eight IR/Serial control ports support high-frequency carriers up to 1.142 MHz. • Each output is capable of three electrical formats: IR, Serial, and Data • Eight IR/Serial data signals can be generated simultaneously. • Channel range = 1-32,767 • Channels 1-128 (output): IR commands • Channels 129-253: used as reference channels • Channel 254 (feedback): Power Fail (used with 'PON' and 'POF' commands) • Channel 255 (feedback): Power status (when IO Link is set) • IR ports support data mode (at limited baud rates and wiring distances). • Two 8-pin 3.5 mm mini-Phoenix (female) connectors provide IR/Serial port termination
Configuration Port	USB connector (male) can be connected to a USB port on a computer. This low-speed USB connection is used to configure system settings. Not recommended for firmware updates or large file transfers.
Configuration DIP switch	4 configuration DIP switches used solely for enabling or disabling NetLinx functionality.
ID pushbutton	Provides the NetLinx ID (**Device only**) assignment for the device. Refer to the *Changing the Device Address of a NetLinx Device* section on page 20. • The D notation is used to represent a device number.
LAN port	RJ-45 port for 10/100 Mbps communication. This port automatically negotiates the connection speed (10 Mbps or 100 Mbps) and whether to use half duplex or full duplex mode.
LAN Link/Activity LED	LEDs show communication activity, connection status, speeds, and mode information: • **SPD** (speed) - Yellow LED lights On when the connection speed is 100 Mbps and turns Off when the speed is 10 Mbps. • **L/A** (link/activity) - Green LED lights On when the LAN cables are connected/terminated correctly, and blinks when receiving LAN data packets.
AXlink LED	• Green LED indicates the state of the AXlink connector port. • Normal AXlink activity = 1 blink/second • Abnormal AXlink activity = cycle of 3 consecutive blinks and then Off
AXlink port	4-pin 3.5 mm mini-Phoenix (male) connector provides data and power to external control devices.
Power port	2-pin 3.5 mm mini-Phoenix (male) connector
Included Accessories:	• 2-pin 3.5 mm mini-Phoenix (female) PWR connector (**41-5025**) • 4-pin 3.5 mm mini-Phoenix (female) AXlink connector (**41-5047**) • 10-pin 3.5 mm mini-Phoenix (female) I/O connector (**41-5107**) • Installation Kit (**KA2105-02**): Two rack mount ears Four #8-32 Phillips flat head screws • NI-3101-SIG Quick Start Guide (**93-2105-08**) • Two 8-pin 3.5 mm mini-Phoenix (female) Relay connectors (**41-5083**) • Two CC-NIRC IR Emitters
Other AMX Equipment:	• 2-pin 3.5 mm mini-Phoenix male connector (**41-5026**) • CC-NIRC IR cables (**FG10-000-11**) • CC-NSER IR/Serial cables (**FG10-007-10**) • CSB Cable Support Bracket (**FG517**) • NCK, NetLinx Connector Kit (**FG2902**) • USB A to B cable (**FG10-2105**)

Installation and Upgrading

Device:Port:System (D:P:S)

A device is any hardware component that can be connected to an AXlink bus. Each device must be assigned a unique number to locate that device on the bus. **Only the Device value can be set through the DIP switch settings mentioned above.**

NetLinx requires a Device:Port:System (D:P:S) specification. This D:P:S triplet can be expressed as a series of constants, variables separated by colons, or a DEV structure. For example:

```
STRUCTURE DEV
{
INTEGER Number  // Device number
INTEGER Port    // Port on device
INTEGER System  // System the device belongs to
}
```

The D:P:S notation is used to explicitly represent a device number, port and system. For example, 128:1:0 represents the first port on device 128 on this system.

If a device is declared in a NetLinx program with just the Device number (**System and Port are omitted**), the NetLinx Compiler assumes it has a **Port number of 1 and a System number of 0**. However, all existing device declarations should be converted using the D:P:S (Device:Port:System) notation. This enables certain NetLinx specific debugging features and can help pinpoint other potentially obscure errors.

The syntax is as follows:

```
NUMBER:PORT:SYSTEM
```

where:

NUMBER:	16-bit integer represents the device number
PORT:	16-bit integer represents the port number (in the range 1 through the number of ports on the Controller or device)
SYSTEM:	16-bit integer represents the system number (0 = this system)

Installation into an Equipment Rack

Use the rack-mounting ears supplied with the NI-3101-SIG controller for equipment rack installations. The device comes installed with four rubber feet for flat surface installations.

The maximum operating ambient temperature is 40°C.
Connect the unit only to a properly-rated supply circuit.

Never restrict the airflow through the devices' fan or vents.
When installing equipment into a rack, distribute the units evenly. Otherwise, hazardous conditions may be created by an uneven weight distribution.
Reliable earthing (grounding) of rack-mounted equipment should be maintained.

Before completing the install process, completing any firmware upgrade of the NetLinx Control Cards is highly recommended. This upgrade involves physically cycling power to the unit and can become cumbersome if the unit is already installed into a rack.

1. Discharge the static electricity from your body by touching a grounded object.
2. Position and install the mounting ears, using the screws supplied with the unit. The mounting ears may be rotated to accommodate your mounting needs.

3. Thread the cables through the opening in the equipment rack. Allow for enough slack in the cables to accommodate for movement during the installation process.
4. Reconnect all cables to their appropriate source/terminal locations. Refer to the*Connections and Wiring* section on page 7 for more detailed wiring and connection information.
   - Verify that the terminal end of the power cable is not connected to the a power supply before plugging in the 2-pin power connector.

To prevent repetition of the installation, test the incoming wiring by connecting the Controller's connectors to their terminal locations and applying power. Verify that the unit is receiving power and functioning properly. Disconnect the terminal end of the power cable from the connected 12 VDC-compliant power supply.

5. Slide the device into the rack until the attachment holes, along both sides, align to their corresponding locations on the mounting ears.
6. Secure the device to the rack by using the four flat-head Phillips screws supplied in the kit.
7. Apply power to the unit to complete the installation.

CAUTION: RACK MOUNT SAFETY INSTRUCTIONS

1. If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature 50°C.
2. Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
3. Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
4. Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
5. Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Connections and Wiring

Setting the Configuration DIP Switch for the Configuration Port

Prior to installing the Controller, use the Configuration DIP switch to set the information used by the Configuration Port for communication. The DIP switchsets the starting address (the device number in the D:P:S specification) for the Control Cards installed in the controller with a range of 1-1536. The four-pin Configuration DIP switch is located on the rear of the device.

Program Run Disable (PRD) mode

The Configuration DIP switch is used to set the on-board Master to Program Run Disable (**PRD**) mode, according to the settings listed in the table below.

PRD Mode Settings

PRD Mode	**Position 1**	
Normal mode (default)	OFF	
PRD Mode	ON	

The **PRD** mode prevents the NetLinx program stored in the on-board Master from running during the device's power-up. This mode should only be used if the resident NetLinx program is causing inadvertent communication and/or control problems. If necessary, place the on-board Master in PRD mode and use the NetLinx Studio v 2.x program to resolve the communication and/or control problems with the resident NetLinx program. After doing so, download the corrected program, reset the configuration DIP switch to normal mode, recycle power, and try again.

NOTE

Think of the PRD Mode (On) equating to a PC's SAFE Mode setting. This mode allows a user to continue powering a unit, update the firmware, and download a new program while circumventing any problems with a currently downloaded program. Power must be cycled to the unit after activating/deactivating this mode on the Configuration Port DIP switch #1.

Working with the Configuration DIP switch

1. Disconnect the power supply from the 2-pin PWR (green) connector on the rear of the NetLinx Integrated Controller.
2. Set DIP switch positions according to the information listed in the*PRD Mode Settings* table.
3. Reconnect the 12 VDC power supply to the 2-pin 3.5 mm mini-Phoenix PWR connector.

Configuration Port Connections and Wiring

The NI-3101 is equipped with a low-speed USB connection located on the rear of the unit. Use a standard USB cable to establish a connection between the device and your PC's USB port. This connection provides communication with the NetLinx Integrated Controller. From there, configure the on-board Master as needed for your application.

Modes and Front Panel LED Blink Patterns

The following table lists the modes and blink patterns for the front panel LEDs associated with each mode. These patterns are not evident until after the unit is powered.

Modes and LED Blink Patterns

Mode	Description	LEDs and Blink Patterns		
		STATUS (blue)	OUTPUT (white)	INPUT (white)
OS Start	Starting the operating system (OS).	On	On	On
Boot	On-board Master is booting.	On	Off	On
Contacting DHCP server	On-board Master is contacting a DHCP server for IP configuration information.	On	Off	Fast Blink
Unknown DHCP server	On-board Master could not find the DHCP server.	Fast Blink	Off	Off
Downloading Boot firmware	Downloading Boot firmware to the Master's on-board flash memory. Do not cycle power during this process!	Fast Blink	Fast Blink	Fast Blink
No program running	Either no program is loaded, or the program is disabled.	On	Normal	Normal
Normal	On-board Master is functioning normally.	1 blink per second	Indicates activity	Indicates activity

Port Assignments and Functionality

The rear Port Assignments are as follows:

NI-3101 Port Assignments

Port	ICSP Port #	Port	ICSP Port #
Serial Port #1	1	IR Serial Port #1	9
Serial Port #2	2	IR Serial Port #2	10
Serial Port #3	3	IR Serial Port #3	11
Serial Port #4	4	IR Serial Port #4	12
Serial Port #5	5	IR Serial Port #5	13
Serial Port #6	6	IR Serial Port #6	14
Relays Ports (1-8)	8	IR Serial Port #7	15
		IR Serial Port #8	16
		I/O Port	17

AXlink Port and LED

All NI units have an AXlink port and adjacent status LED (FIG. 3). This port allows the NI to support AMX legacy AXlink devices such as G3 touch panels (*ex: CP4/A*) and PosiTrack Pilot devices. A green LED shows AXlink data activity. When the AXlink port is operating normally, blink patterns include:

- **Off** - No power, or the controller is not functioning properly.
- **1 blink per second** - Normal operation.
- **3 blinks per second** - AXlink bus error. Check all AXlink bus connections.

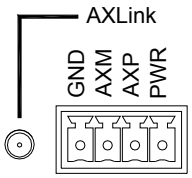


FIG. 3 AXlink connector and LED

The AXlink port can be used to supply power to downstream AXlink-compatible devices, so long as both the power required is LESS THAN 2 Amps total and the external power supply feeding the device has the necessary power capability.

Wiring Guidelines

The Integrated Controllers use a 12 VDC-compliant power supply to provide power through the rear 2-pin 3.5 mm mini-Phoenix PWR connector, or through the 4-pin 3.5 mm mini-Phoenix (female) captive-wire connector used for data communication and power transfer. Use the power requirements referenced in the product's Specifications table to determine the power draw.

The incoming PWR and GND cable from the power supply must be connected to the corresponding locations within the PWR connector.

Use only one power source for the device at a time. Using both the 2-pin mini-Phoenix PWR connector and the 4-pin mini-Phoenix AXLink connector at the same time may cause permanent damage to the device.

Apply power to the device only after installation is complete.

Wiring length guidelines

Refer to the following table for the wiring length information used with the NI-3101:

Wiring Guidelines - NI-3101 @ 900 mA	
Wire size	**Maximum wiring length**
18 AWG	120.41 feet (39.70 meters)
20 AWG	76.45 feet (23.30 meters)
22 AWG	49.36 feet (15.04meters)
24 AWG	30.08 feet (9.17 meters)

Preparing captive wires

You will need a wire stripper and flat-blade screwdriver to prepare and connect the captive wires.

Never pre-tin wires for compression-type connections.

1. Strip 0.25 inch (6.35 mm) of insulation off all wires.
2. Insert each wire into the appropriate opening on the connector (according to the wiring diagrams and connector types described in this section).
3. Tighten the screws to secure the wire in the connector. ***Do not tighten the screws excessively. Doing so may strip the threads and damage the connector.***

Wiring a power connection

To use the 2-pin 3.5 mm mini-Phoenix connector with a 12 VDC-compliant power supply, the incoming PWR and GND cables from the external source must be connected to their corresponding locations on the connector (FIG. 4).

1. Insert the PWR and GND wires on the terminal end of the 2-pin 3.5 mm mini-Phoenix cable. ***Match the wiring locations of the +/- on both the power supply and the terminal connector.***
2. Tighten the clamp to secure the two wires. *Do not tighten the screws excessively; doing so may strip the threads and damage the connector.*
3. Verify the connection of the 2-pin 3.5 mm mini-Phoenix to the external 12 VDC-compliant power supply.

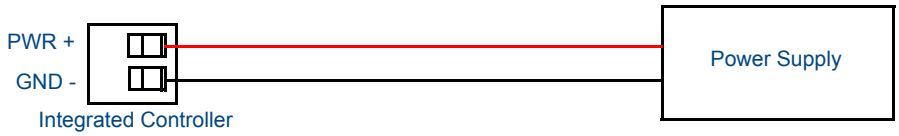


FIG. 4 2-pin mini-Phoenix connector wiring diagram (direct power)

Using the 4-pin mini-Phoenix connector for data and power

Connect the 4-pin 3.5 mm mini-Phoenix (female) captive-wire connector to an external NetLinx device as shown in FIG. 5.

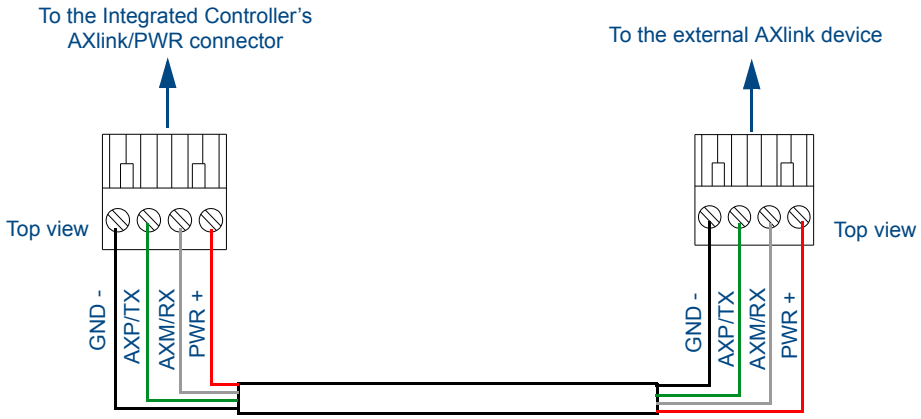


FIG. 5 Mini-Phoenix connector wiring diagram (direct data and power)

Using the 4-pin mini-Phoenix connector for data with external power

To use the 4-pin 3.5 mm mini-Phoenix (female) captive-wire connector for data communication and power transfer, the incoming PWR and GND cable from the 12 VDC-compliant power supply must be connected to the AXlink cable connector going to the device (FIG. 6). Always use a local power supply to power the device.

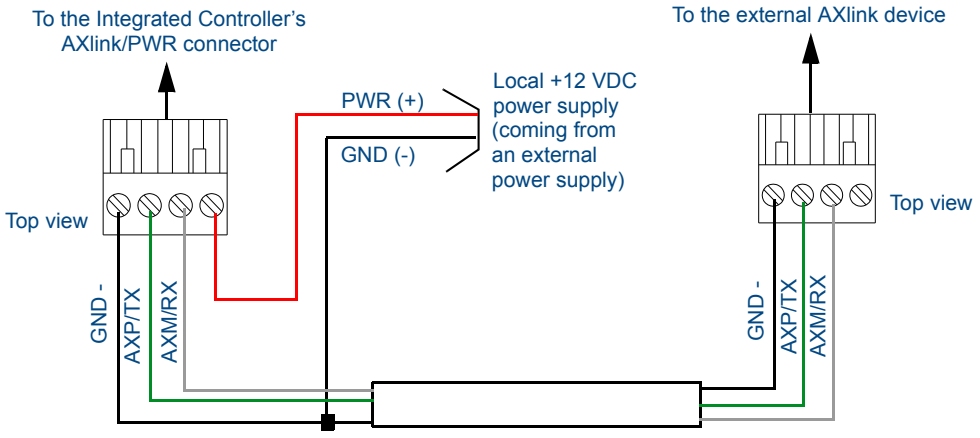


FIG. 6 4-pin mini-Phoenix connector wiring diagram (using external power source)

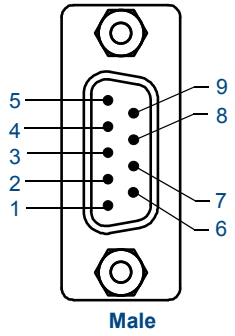
WARNING

*When you connect an external power supply, do not connect the wire from the PWR terminal (coming from the external device) to the PWR terminal on the Phoenix connector attached to the Controller unit. Make sure to connect **only** the AXM, AXP, and GND wires to the Controller's Phoenix connector when using an external power supply.*

Make sure to connect only the GND wire on the AXlink/PWR connector when using a separate 12 VDC power supply. Do not connect the PWR wire to the AXlink connector's PWR (+) opening.

DB9 Device Port: Connections and Wiring

FIG. 7 shows the connector pinouts for the rear RS-232/RS-422/RS-485 (DB9) Device Ports. These ports support most standard RS-232 communication protocols for data transmission. This figure gives a visual representation of the wiring specifications for the RS-232/422/485 Device connectors.



DB9 Serial Port pinouts (male connector)

RS-232	RS-422	RS-485
Pin 2: RX signal	Pin 1: RX -	Pin 1: A (strap to 9)
Pin 3: TX signal	Pin 4: TX +	Pin 4: B (strap to 6)
Pin 5: GND	Pin 5: GND	Pin 5: GND
Pin 7: RTS	Pin 6: RX +	Pin 6: B (strap to 4)
Pin 8: CTS	Pin 9: TX -	Pin 9: A (strap to 1)

FIG. 7 RS-232/422/485 DB9 (male) connector pinouts for the rear Device Ports

The table below provides information about the connector pins, signal types, and signal functions. This table's wiring specifications are applicable to the rear RS-232/422/485 Device Port connectors on the NI-3101-SIG (Ports 1-6).

RS-232/422/485 Device Port Wiring Specifications

Pin	Signal	Function	RS-232	RS-422	RS-485
1	RX-	Receive data		X	X (strap to pin 9)
2	RXD	Receive data	X		
3	TXD	Transmit data	X		
4	TX+	Transmit data		X	X (strap to pin 6)
5	GND	Signal ground	X	X	
6	RX+	Receive data		X	X (strap to pin 4)
7	RTS	Request to send	X		
8	CTS	Clear to send	X		
9	TX-	Transmit data		X	X (strap to pin 1)

WARNING

*When wiring the 422/485 connections, do **NOT** use pre-made 9-wire cable or connect the wire in the cable to any connection that will not be used by the DB9 serial port. Only use wiring that connects the needed pins.*

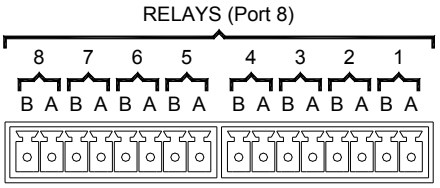
Relay Port: Connections and Wiring

Up to 8 independent external relay devices may be connected to the Relay connectors on the device.

- Connectors labeled A are for common; B are for output.
- Each relay is isolated and normally open.
- A metal commoning strip is supplied with each device to connect multiple relays.

Relay connections

Use A for common and B for output (FIG. 8). Each relay is isolated and normally open. A metal connector strip is also provided to common multiple relays.

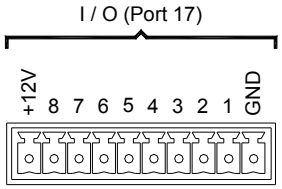


NI-3101-SIG relay connector configuration (Port 8)

FIG. 8 RELAY connector (male) NI-3101-SIG

Input/Output (I/O) Port: Connections and Wiring

The I/O port responds to either switch closures or voltage level (high/low) changes, or it can be used for logic-level outputs.



NI-3101-SIG I/O connector configuration (Port 17)

FIG. 9 INPUT/OUTPUT connector (male)

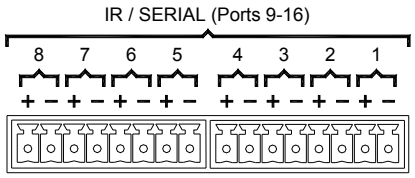
Up to eight devices may be connected to the I/O connectors on the NI-3101-SIG (FIG. 9). A contact closure between the GND and an I/O port is detected as a Push.

- When used for voltage inputs, the I/O port detects a low signal (0 - 1.5 VDC) as a Push, and a high signal (3.5 - 5 VDC) as a Release (*this IO port uses 5V logic but can handle up to 12V without harm).*
- When used for outputs, the I/O port acts as a switch to GND and is rated for 200 mA @ 12 VDC. This device can use up to 8 I/O ports.
- The PWR pin provides +12 VDC @ 200 mA and is designed as a power output for the PCS Power Current Sensors, VSS2 Video Sync Sensors (or equivalent).
- The GND connector is a common ground and is shared by all I/O ports. A common ground is shared with I/O ports 1 - 8.

I/O Port Wiring Specifications - NI-3101-SIG					
Pin	**Signal**	**Function**	**Pin**	**Signal**	**Function**
1	GND	Signal GND	6	I/O 5	Input/Output
2	I/O 1	Input/Output	7	I/O 6	Input/Output
3	I/O 2	Input/Output	8	I/O 7	Input/Output
4	I/O 3	Input/Output	9	I/O 8	Input/Output
5	I/O 4	Input/Output	10	12 VDC	PWR

IR/Serial Port: Connections and Wiring

Up to **eight** IR- or Serial-controllable devices may be connected to the IR/Serial connectors on the rear of the NI-3101 (FIG. 10). These connectors accept an IR Emitter (CC-NIRC) that mounts onto the device's IR window, or a mini-plug (CC-NSER) that connects to the device's control jack. A data 0 - 5 VDC device may also be connected. These units come with two CC-NIRC IR Emitters (**FG10-000-11**).



NI-3101-SIG IR/Serial connector configuration (Port 9-16)

FIG. 10 IR/SERIAL (male)

The IR/Serial connector wiring specifications are listed in the following table:

IR/Serial Connector Wiring Specifications (per Port)		
Number of IR connections	**NI-3101-SIG Port #**	**Function**
1	9	GND (-) Signal 1 (+)
2	10	GND (-) Signal 2 (+)
3	11	GND (-) Signal 3 (+)
4	12	GND (-) Signal 4 (+)
5	13	GND (-) Signal 5 (+)
6	14	GND (-) Signal 6 (+)
7	15	GND (-) Signal 7 (+)
8	16	GND (-) Signal 8 (+)

LAN (Ethernet/RJ-45 Port): Connections and Wiring

The following table lists the pinouts, signals, and pairing for the LAN connector.

LAN RJ-45 Pinouts and Signals				
Pin	**Signals**	**Connections**	**Pairing**	**Color**
1	TX +	1 --------- 1	1 --------- 2	Orange-White
2	TX -	2 --------- 2		Orange
3	RX +	3 --------- 3	3 --------- 6	Green-White
4	no connection	4 --------- 4		Blue
5	no connection	5 --------- 5		Blue-White
6	RX -	6 --------- 6		Green
7	no connection	7 --------- 7		Brown-White
8	no connection	8 --------- 8		Brown

FIG. 11 diagrams the RJ-45 pinouts and signals for the LAN RJ-45 connector and cable.

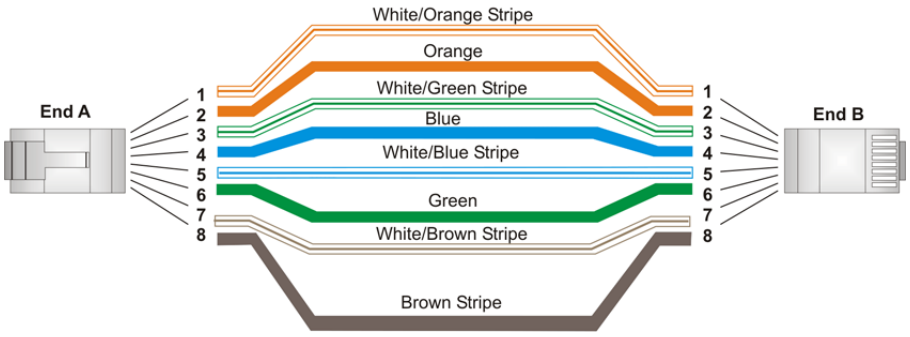


FIG. 11 RJ-45 wiring diagram

LAN LEDs

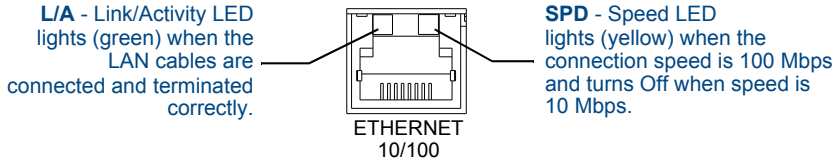


FIG. 12 LAN LEDs

LAN ports used by the Integrated Controllers

LAN Ports Used by the NetLinx Integrated Controllers		
Port type	**Description**	**Standard Port #**
FTP	The on-board Master has a built-in FTP server.	21/20 (TCP)
SSH	The SSH port functions using the same interface as Telnet but over a secure shell where it uses SSL as a mechanism to configure and diagnose a NetLinx system. This port value is used for secure Telnet communication. ***Note**: only SSH version 2 is supported.*	22 (TCP)
Telnet	The NetLinx Telnet server provides a mechanism to configure and diagnose a NetLinx system. For maximum flexibility, the Master can be configured to utilize a different port than 23, or disable Telnet completely from either Telnet or the Program port located on the rear of the Master itself. Once disabled, the only way to enable Telnet again is from the Master's Program port.	23 (TCP)
HTTP	The Master has a built-in web server that complies with the HTTP 1.0 specification and supports all of the required features of HTTP v1.1. This port is used for unsecure HTTP Internet communication between the web browser's UI and the target Master.	80 (TCP)
HTTPS/SSL	This port is used by a web browser for secure communication between the web server UI and the target Master. This port is also used for simultaneous encryption of this data, using the SSL certificate information on the Master as a key.	443 (TCP)
ICSP	Peer-to-peer protocol used for both Master-to-Master and Master-to-device communications. For maximum flexibility, the Master can be configured to utilize a different port than 1319, or disable ICSP over LAN completely from either Telnet or the Program Port located on the rear of the Master itself. This type of communication is used by the various AMX products for communication amongst themselves.	1319 (UDP/TCP)
integration! Solutions	This feature on the Master uses, by default, port 10500 for the XML based communication protocol. This port is connected to by the client web browser's JVM when integration! Solutions control pages are retrieved from the on-board Master's web server. For maximum flexibility, the on-board Master can be configured to utilize a different port than 10500 or to disable integration! Solutions completely.	10500 (TCP)

Replacing the Timekeeper Battery

The NI-3101-SIG uses a combination lithium battery and clock crystal package called a ***Timekeeper***. Only one *Timekeeper* unit is installed within a given NI-3101-SIG. The battery can be expected to have up to 3 years of usable life under very adverse conditions. Actual life is appreciably longer under normal operating conditions. This calculation is based on storing the unit without power in 50° C (120° F) temperature until battery levels are no longer acceptable. The part number for a replacement battery is *57-0032*.

To replace the Timekeeper battery:

1. Discharge the static electricity from your body by touching a grounded metal object.
2. Unplug all the connectors from the device.

3. Remove the rear panel from the device, and then disconnect the NXI control cable and remove the Master card.
4. Locate the battery behind the Configuration Port on the circuit board.
5. Carefully slide the battery out of its socket and insert the new battery.
6. Plug the 2-pin 3.5 mm mini-Phoenix PWR (green) connector to reapply power. Wait approximately 1 minute, then remove the PWR connector again.
7. Carefully slide the other battery out of its socket and insert the new battery
8. Re-connect the NXI control cable to the Master card.
9. Replace and secure the rear faceplate using the mounting screws and reconnect all communication connectors.
10. Reconnect the 12 VDC power supply to the respective PWR connector and apply power.

CAUTION: RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS

Configuration and Firmware Update

Overview

This section refers to steps necessary to both communicate with and upgrade the NI-3101-SIG.

WARNING

Before continuing, verify that you are using the latest version of NetLinx Studio and the latest firmware Kit file (this file contains both the NI Integrated Controller and on-board Master firmware).
The NI-3101-SIG Kit file begins with 2105_04_X100.

Before beginning:

1. Set up and configure the NI-3101-SIG. Refer to the previous *Installation and Upgrading* section.
2. Verify that the latest version of NetLinx Studio has been installed on the PC. If an update is necessary, download the latest NetLinx Studio software from **www.amx.com**.
3. If the LAN port will be used for programming, verify that an LAN cable connects the Controller to the PC being used for programming or to a LAN on the same subnet as the PC.
4. The low-speed USB connection is **not** recommended for firmware updates.
5. Verify that the NetLinx Master is receiving power and is turned ON. Refer to the previous *Connections and Wiring* section on page 7 for more information.

NOTE

If if communication has already been set up with the Controller via an IP Address, continue with the firmware update procedures outlined in the Communicating with the NI Device via an IP section on page 26.

Communicating with the Master via the Program Port

1. From your computer, launch NetLinx Studio 2.x.
2. Select **Settings** > **Master Communication Settings**, from the Main menu, to open the Master Communication Settings dialog (FIG. 13).

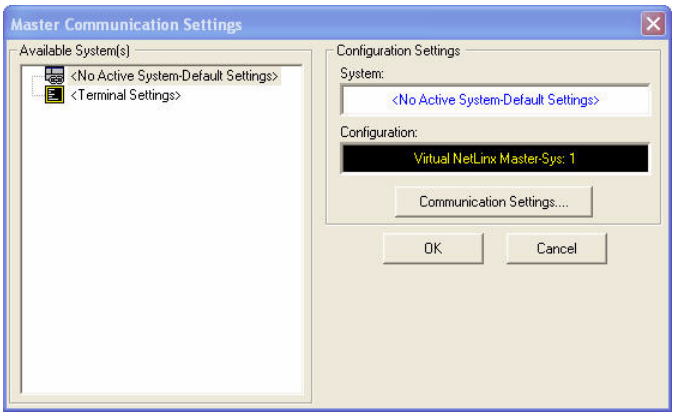


FIG. 13 Master Communication Settings dialog

3. Click the **Communications Settings** button to open the *Communications Settings* dialog (FIG. 14).
4. Click the **NetLinx Master** radio button (*from the Platform Selection section*) to choose a NetLinx Master such as the NI-3101-SIG.
5. Click the **Serial** radio button (*from the Transport Connection Option section*) to select communication to the on-board Master via a (Serial) COM port.
6. Click the **Edit Settings** button to open the *Serial Settings* dialog (FIG. 15).

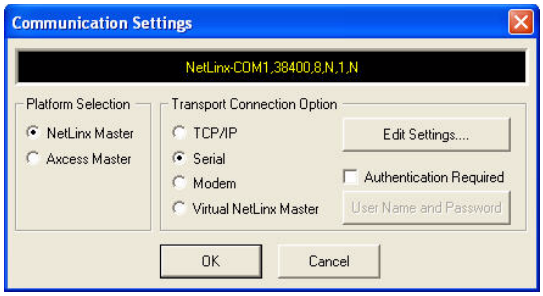


FIG. 14 Communication Settings dialog box

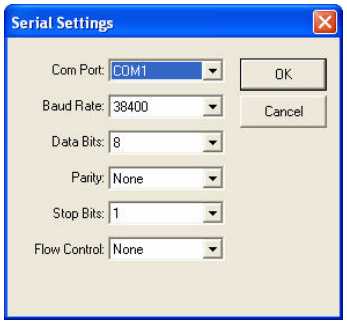


FIG. 15 Serial Settings dialog box

NOTE

No authentication username or password information is required when selecting a direct connection such as USB or Serial.

7. Set the COM port parameters for the selected COM port used for communication to the NetLinx Master. Default parameters are:
   - COM1
   - 115200
   - 8 Data Bits
   - No Parity
   - 1 Stop Bit
   - No Flow Control

   If communication fails on a known COM port, change the baud rate to 115200 and try again.
8. Click **OK** three times to close the open dialogs and save the chosen settings.

NOTE

*If the connection fails to establish, select a different COM port, press the **Retry** button to reconnect using the same communication parameters, or press the **Change** button to alter your communication parameters and repeat steps 2 thru 8.*

Setting the System Value

1. Access/open the Device Addressing dialog (FIG. 16) by either one of these two methods:
   - Right-click on any System item listed (such as the NI Master entry) in the **OnLine Tree** tab of the Workspace and select **Device Addressing** (from the popup list).
   - Select **Diagnostics** > **Device Addressing** from the Main menu.

CAUTION

This process should be done while communicating to the Master via a Serial connection.

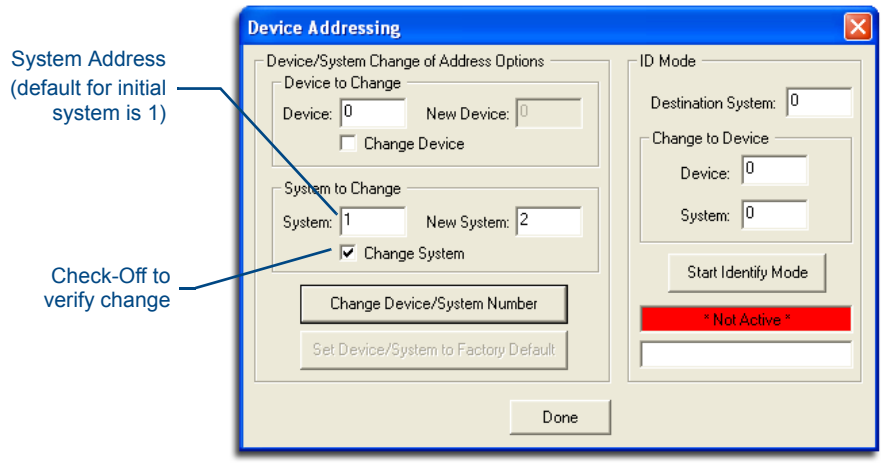


FIG. 16 Device Addressing tab (changing the system value)

NOTE

This tab represents the only way to change the System Number associated to the active on-board NI Master. ***The Master must have its power cycled to incorporate the new System number, as often a simple reboot via Studio will not be enough to incorporate this new number).***

2. Select the **Change System** selection box from the *System to Change* section.
3. Enter both the current and new system address values.
4. Click the **Change Device/System Number** button. This configures the Master to accept the new value and incorporate the information. *The system information in the OnLine Tree tab of the Workspace window refreshes and then displays the new information.*
5. Click **Done** to close the *Device Addressing* dialog and return to the main program.
6. Click **Reboot** (from the **Tools > Reboot the Master Controller** dialog) and wait for the System Master to reboot. *The STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*
7. Press **Done** once until the *Master Reboot Status* field reads **Reboot of System Complete**.
8. Click the **OnLine Tree** tab in the Workspace window to view the devices on the System. The default System value is 1.
9. Right-click the associated System number (*or anywhere within the tab itself*) and select **Refresh System**. This establishes a new connection to the specified System and populates the list with devices on that system.
10. Use **Ctrl**+**S** to save your existing NetLinx Project with the new changes.

NOTE

If the NetLinx device does not appear within the OnLine Tree tab, make sure that the Integrated Controller's on-board Master System Number (from within the Device Addressing tab) is correctly assigned.
If there is a problem, use a system value of zero (0) on the NetLinx device.

NOTE

The Master is set by default to DEVICE 0*. Connected NetLinx device addresses can only be changed through the Protected Setup page. The new address is reflected within the OnLine Tree tab of the Workspace window only after the devices are rebooted and the system is refreshed.*

NOTE

The system value on a Modero touch panel cannot be changed from the Device Addressing dialog box and MUST be altered through the panel Protected Setup page.

Using Multiple NetLinx Masters

When using more than one Master, each unit must be assigned to a separate System value.

A Master's System value can be changed but **its device Address must always be set to zero (00000)**. The Device Addressing dialog will not allow you to alter the NetLinx Master address value.

Example: Using NetLinx Studio v 2.x to work with an NXC-ME260/64 and NI-3101-SIG:

- The NXC-ME260/64 could be assigned to **System 1** (with a value of 00000).
- The NI-3101-SIG could be assigned to **System 2** (with a value of 00000).

Changing the Device Address of a NetLinx Device

1. Access the Device Addressing dialog (FIG. 17) by either one of these two methods:
   - Right-click on any system device (***such as a Modero panel***) listed in the **OnLine Tree** tab of the Workspace and select **Device Addressing** (from the popup list).
   - Select **Diagnostics** > **Device Addressing** from the Main menu.

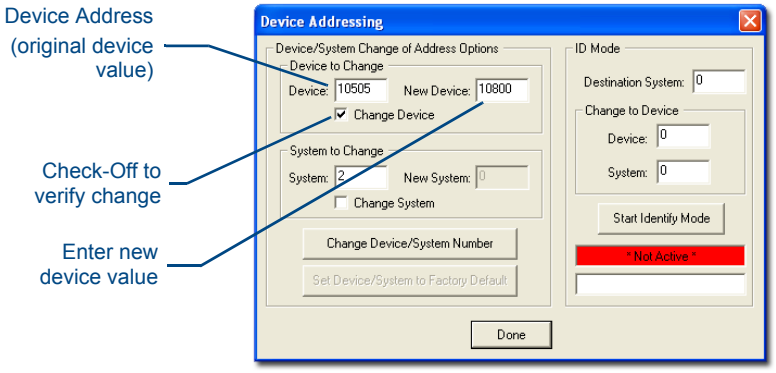


FIG. 17 Device Addressing dialog (changing the device value)

NOTE

This dialog represents the only way to change the device value of a selected NetLinx device. Modero panels are one of the only devices that can have their ***Device values*** *changed within both this dialog and through the on-board firmware page.*

2. Select the **Change Device** checkbox from the *Device to Change* section.
3. Verify the **Current** value and enter the **New Device** value for the target NetLinx device.
4. Click the **Change Device/System Number** button. This configures the specified Master to accept the new value for the NetLinx device and incorporate the information (the system information in the Workspace window refreshes and then displays the new information).
5. Click **Done** to close the Device Addressing dialog.
6. Click **Reboot** (*from the Tools > Reboot the Master Controller dialog*) and wait for the System Master to reboot. *The STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*
7. Press **Done** once until the *Master Reboot Status* field reads **Reboot of System Complete**.
8. Click the **OnLine Tree** tab in the Workspace window to view the devices on the System. *The default System value is one (1).*
9. Right-click the associated System number (*or anywhere within the tab itself*) and select **Refresh System**. This establishes a new connection to the specified System and populates the list with devices on that system.
10. Use **Ctrl**+**S** to save your existing NetLinx Project with the new changes.

NOTE

If the Master does not appear in the Workspace window, make sure that the Master's System Number (from within the Device Addressing tab) is correctly assigned. ***If this issue persists, use a system value of zero (0) on the Master.***

Recommended NetLinx Device Numbers

• 1 - 255	• Axcess Devices use Axcess standards
• 301 - 3072	• NetLinx CardFrames start at frame number 25 - (frame# * 12) + Card #
• 5001 - 5999	• ICSNet NetLinx devices: NXI, NXM-COM2, NXM-IRS4, etc.
• 6001 - 6999	• ICSNet Landmark devices: PLH-VS8, PLH-AS16, PLB-AS16
• 7001 - 7999	• InConcert Devices
• 8001 - 8999	• PCLink Device: PCLink devices are PC programs
• 10000 - 31999	• ICSNet Panels: DMS, IMS, and future panels
• 33001 - 36863	• Virtual devices: these start at 33001
• 32001 - 32767	• Dynamic devices: the actual range used by Master
• 32768 - 36863	• Virtual devices: the actual range used by Master

Using the ID Button to Change the Controller's Device Value

Use the ID Button on the rear panel (in conjunction with ID Mode function in NetLinx Studio) to establish a NetLinx Device ID for the device.

The steps described and the dialogs shown in this section are in the *NetLinx Studio* application.

- NetLinx Studio is available to download from www.amx.com.
- Refer to the NetLinx Studio on-line help for information on using NetLinx Studio.

1. Access the *Device Addressing* dialog (FIG. 18) by selecting **Diagnostics** > **Device Addressing**.

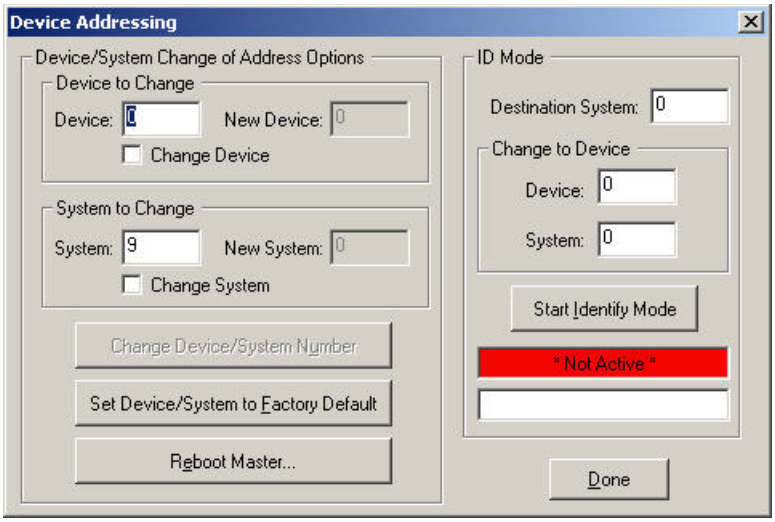


FIG. 18 Device Addressing dialog

2. Enter the system number in the **Destination System** field.
3. Enter the desired device number in the **Change to Device** box (*Device* field), and again enter the system number (in the *System* field).
4. Click the **Start Identify Mode** button. This action activates Identify Mode on the named System.

NOTE

"Identify Mode" means that the system is put on hold while it waits for an event from any NetLinx device in the named system (for example, pushing the ID button on a NetLinx device). The device that generates the first event is the device that gets identified.

The Device Addressing dialog displays the "*Waiting...Press Cancel to Quit...*" message, indicating that Identify Mode is currently active (NetLinx Studio is waiting to detect a device - FIG. 19).

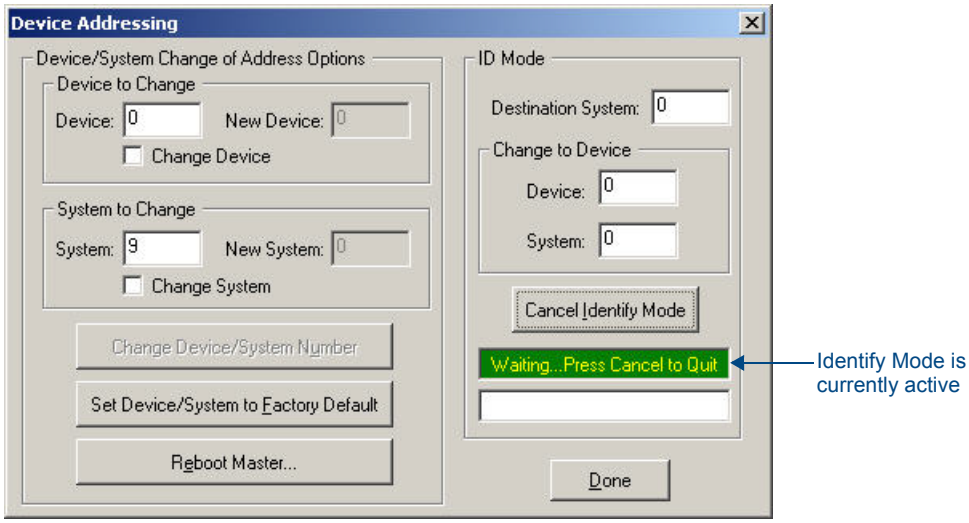


FIG. 19 Device Addressing dialog - Identify Mode active

5. Press the NI Controller's **ID** button to assign the new Device / System values entered in step 3 to the Controller. At this point, the "*Successful Identification Made* " message is displayed (FIG. 20):

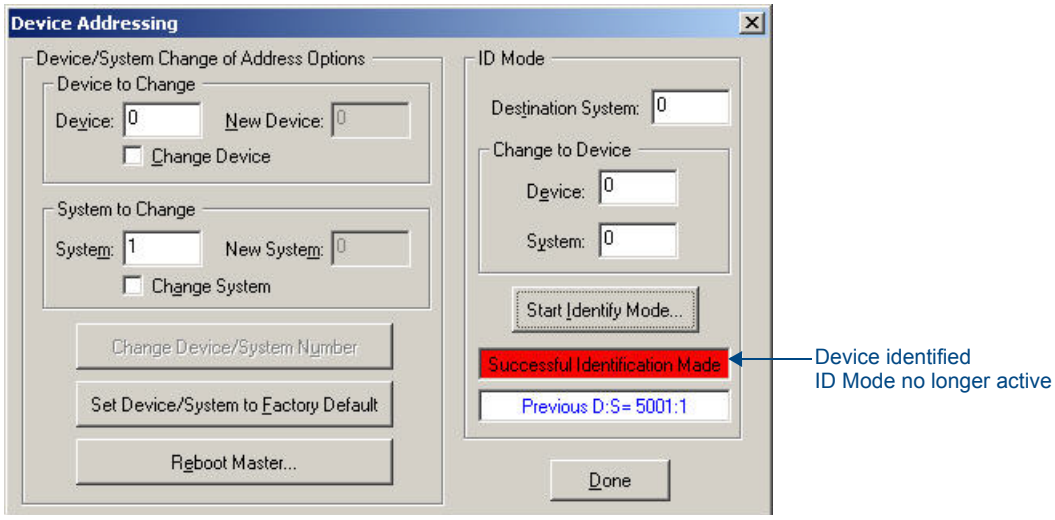


FIG. 20 Device Addressing dialog - Successful Identification Made

- The previous Device and System numbers of the NI Controller are displayed below the red field.
  Example: *Previous D:S=5001:1*,
  where "**5001**" represents the previous device value of the NI Controller (**D**) and "**1**" represents the NI Controller's System value (**S**).

Resetting the Factory Default System and Device Values

1. Access the Device Addressing dialog (FIG. 17 on page 20) by either one of these two methods:
- Right-click on any system device listed in the Workspace and select **Device Addressing**.
- Select **Diagnostics** > **Device Addressing** from the Main menu.

2. Click the **Set Device/System to Factory Default** button. This resets both the system value and device addresses (for definable devices) to their factory default settings. The system information (in the **OnLine Tree** tab of the Workspace window) refreshes and then displays the new information.

NOTE

*By setting the system to its default value (#1), Modero panels that were set to connect to the Master on another System value will not appear in the **OnLine Tree** tab of the Workspace window.*
For example: A Modero touch panel was previously set to System #2. The system is then reset to its default setting of System #1 and then refreshed from within the Workspace window. The panel will not reappear until the system is changed (from within the System Connection page on the Modero) to match the new value and both the Master and panel are rebooted.

3. Click **Done** to close the Device Addressing dialog.
4. Click **Reboot** (*from the Tools > Reboot the Master Controller dialog*) and wait for the System Master to reboot. *The STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*
5. Press **Done** once until the *Master Reboot Status* field reads **Reboot of System Complete**.
6. Click the **OnLine Tree** tab in the Workspace window to view the devices on the System. *The default System value is one (1).*
7. Right-click the associated System number (*or anywhere within the tab itself*) and select **Refresh System**. This establishes a new connection to the specified System and populates the list with devices on that system.
8. Use **Ctrl**+**S** to save the existing NetLinx Project with the new changes.

Obtaining the Master's IP Address (using DHCP)

NOTE

Verify there is an active LAN connection on the LAN port of the NI-Series Controller before beginning these procedures.

1. Select **Diagnostics** > **Network Addresses** from the Main menu to access the Network Addresses dialog (FIG. 21).

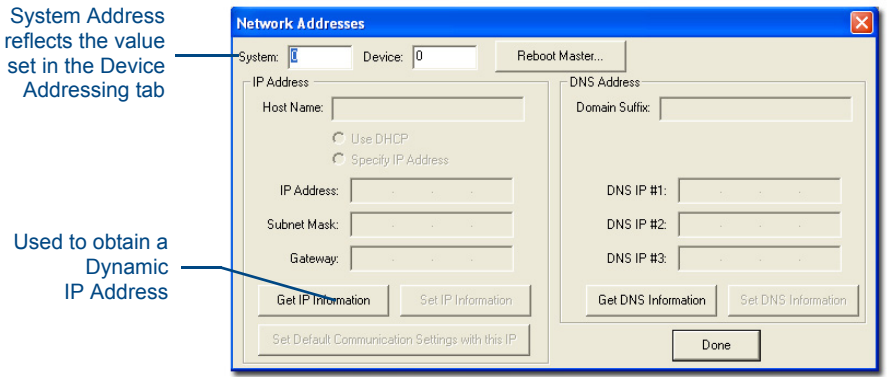


FIG. 21 Network Addresses dialog (for a DHCP IP Address)

2. Verify that both the **System** number corresponds to the System value previously assigned within the Device Addressing tab and that zero (0) is entered into the *Device* field.

NOTE

The system value must correspond to the Device Address entered in the Device Addressing dialog. Refer to the Setting the System Value section on page 18 *for more detailed instructions on setting a system value.*

3. Click the **Get IP Information** button to configure the on-board Master for DHCP usage and then read the IP Address obtained from the DHCP Server.

NOTE

DO NOT enter ANY IP information at this time; this step only gets the System Master to recognize that it should begin using an obtained DHCP Address.

4. Note the obtained IP Address (*greyed-out and read-only*). This information is later entered into the **Master Communication Settings** dialog and used by NetLinx Studio v 2.x to communicate to the Master via an IP. This address is reserved by the DHCP server and then given to the Master.

NOTE

If the IP Address field is empty, give the Master a few minutes to negotiate a DHCP Address with the DHCP Server, and try again. The DHCP Server can take anywhere from a few seconds to a few minutes to provide the Master with an IP Address.

5. Verify that **NetLinx** appears in the *Host Name* field (*if not, then enter it in at this time*).
6. Click the **Use DHCP** radio button from the IP Address section (*if not greyed-out*).
7. Click the **Set IP Information** button to retain the IP Address from the DHCP server and assign it to the on-board Master. A popup window then appears to notify you that Setting the IP information was successful and it is recommended that the Master be rebooted.
8. Click **OK** to accept the change to the new IP/DNS information.
9. Click the **Reboot Master** button and select **Yes** to close the Network Addresses dialog.
10. Click **Reboot** from the **Tools > Reboot the Master Controller** dialog, and wait for the System Master to reboot and retain the newly obtained DHCP Address. *The STATUS and OUTPUT LEDs should begin to blink alternately during the incorporation. Wait until the STATUS LED is the only LED blinking.*
11. Press **Done** once until the *Master Reboot Status* field reads **Reboot of System Complete**.

NOTE

Verify that these IP values are also entered into the related fields within either the IP Settings section of the System Connection page (on the touch panel) or within the Address field on the web browser.

12. Complete the communication process by continuing on to the *Communicating with the NI Device via an IP* section on page 26.

Assigning a Static IP to the NetLinx Master

NOTE

Verify that the Controller has an active LAN connection before beginning these procedures.

1. Select **Diagnostics** > **Network Addresses** from the Main menu to access the Network Addresses dialog (FIG. 22).

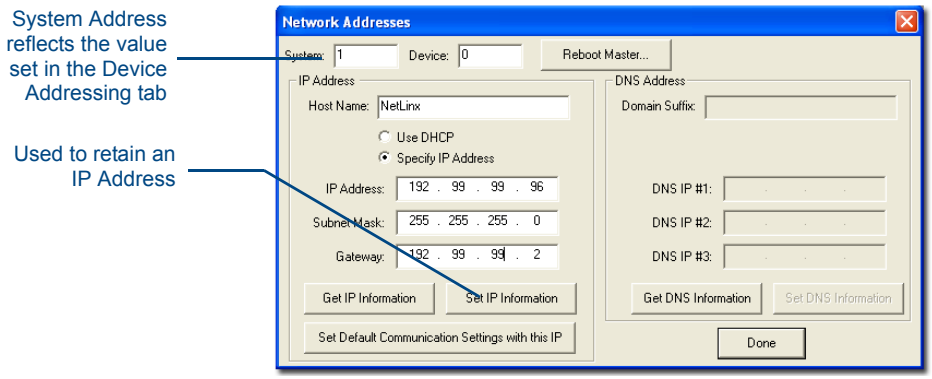


FIG. 22 Network Addresses dialog (for a pre-obtained Static IP Address)

2. Verify that both the **System** number corresponds to the System value previously assigned within the Device Addressing tab and that zero (0) is entered into the *Device* field.

NOTE

The system value must correspond to the Device Address previously entered in the Device Addressing tab. Refer to the Setting the System Value section on page 18 *for more detailed instructions on setting a system value.*

3. Click the **Get IP Information** button to temporarily configure the on-board Master for DHCP usage and then read the IP Address obtained from the DHCP Server.
4. Click the **Specify IP Address** radio button from the IP Address section. With this action, all IP fields become editable.
5. Verify that **NetLinx** appears in the *Host Name* field. If not, then enter it in at this time.
6. Enter the IP Address, Subnet Mask, and Gateway information into their respective fields.
7. Click the **Set IP Information** button to cause the on-board Master to retain the new IP Address pre-obtained from the System Administrator.
8. Click **OK** to accept the change to the new IP/DNS information.
9. Click the **Reboot Master** button and select **Yes** to close the Network Addresses dialog.
10. Click **Reboot** from the **Tools > Reboot the Master Controller** dialog, and wait for the System Master to reboot and retain the newly obtained DHCP Address. *The STATUS and OUTPUT LEDs should begin to blink alternately during the incorporation. Wait until the STATUS LED is the only LED blinking.*
11. Press **Done** once until the *Master Reboot Status* field reads **Reboot of System Complete**.

NOTE

Verify that these IP values are also entered into the related fields within either the IP Settings section of the System Connection page (on the touch panel) or within the Address field on the web browser.

12. Complete the communication process by continuing on to the *Communicating with the NI Device via an IP* section on page 26.

Communicating with the NI Device via an IP

Whether the on-board Master's IP Address was Static Set (Set IP Info) or Dynamically obtained (Get IP Info), use the IP Address information from the Network Addresses dialog to establish communication via the LAN-connected Integrated Controller.

1. From your PC, launch NetLinx Studio 2.
2. Obtain the IP Address of the Master from the System Administrator. If you still do not have an IP Address, follow the steps outlined in either the *Obtaining the Master's IP Address (using DHCP)* section on page 23 or *Assigning a Static IP to the NetLinx Master* section on page 24.
3. Select **Settings** > **Master Communication Settings** from the Main menu to open the *Master Communication Settings* dialog (FIG. 23).

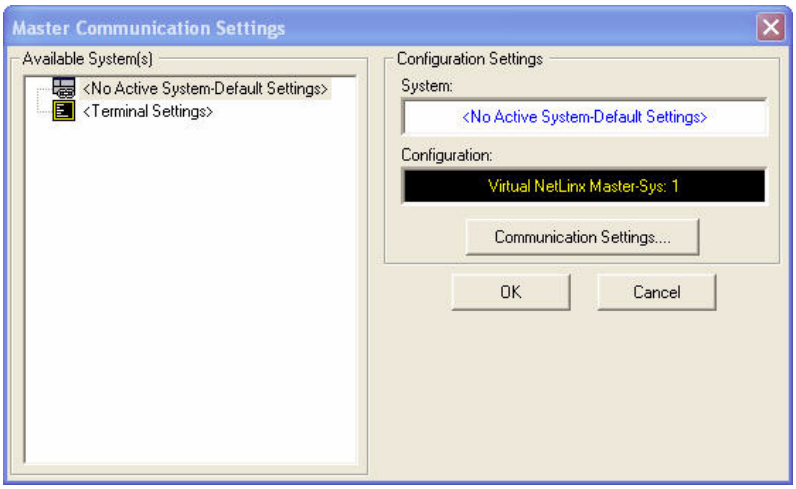


FIG. 23 Master Communication Settings dialog

4. Click the **Communications Settings** button to open the Communications Settings dialog (FIG. 24).

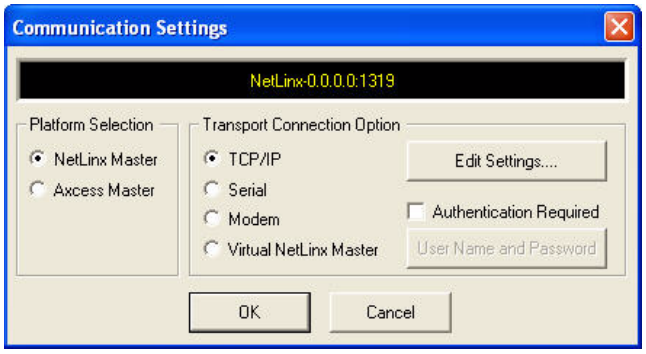


FIG. 24 Communications Settings dialog

5. Click on the **NetLinx Master** radio button to indicate you are working with a NetLinx Master, and click on the **TCP/IP** radio button to indicate a connection to the Master via an IP Address.
6. Click the **Edit Settings** button (*on the Communications Settings dialog*) to open the *TCP/IP Settings* dialog (FIG. 25). This dialog contains a series of previously entered IP Address/URLs and their associated names, all of which are stored within NetLinx Studio and are user-editable.

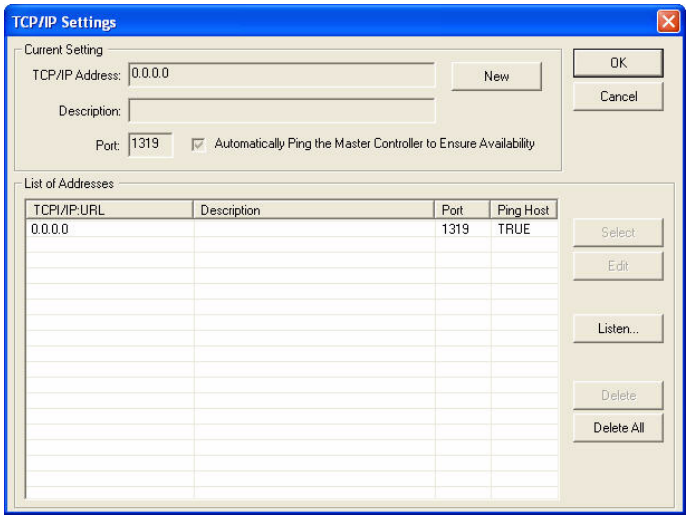


FIG. 25 TCP/IP Settings dialog

7. Click the **New** button to open the *New TCP/IP Setting* dialog box (FIG. 26), where you may enter both a previously obtained DHCP or Static IP Address and an associated description for the connection into their respective fields.

FIG. 26 New TCP/IP Setting dialog

8. Place a checkmark within the *Automatically Ping the Master Controller to ensure availability* radio box to make sure the Master is initially responding online before establishing full communication.
9. Click **OK** to close the current *New TCP/IP Settings* dialog box and return to the previous *TCP/IP Settings* dialog box. Locate the new entry within the *List of Addresses* section.
10. Click the **Select** button to make the new entry the currently used IP Address communication parameter.
11. Click **OK** to return to the *Communications Settings* dialog and place a checkmark within the *Authentication Required* radio box if the Master has been previously secured with a username/password.
12. Press the **User Name and Password** button to open the *Master Controller User Name and Password* dialog box (FIG. 27). Within this dialog, enter a previously configured username and password (with sufficient rights) before attempting to connect to the Master.

FIG. 27 Master Controller User Name and Password dialog box

13. Click **OK** to save the newly entered information and return to the previous *Communication Settings* dialog box. Click **OK** again to begin the communication process to the Master.

NOTE

If currently connected to the assigned Master, a popup asks about temporarily stopping communication to the Master and applying the new settings.

14. Click **Yes** to interrupt the current communication from the Master and apply the new settings.
15. Click **Reboot** from the **Tools > Reboot the Master Controller** dialog and wait for the System Master to reboot. The STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.
16. Press **Done** once until the *Master Reboot Status* field reads **Reboot of System Complete**.
17. Click the **OnLine Tree** tab in the Workspace window to view the devices on the System. *The default System value is one (1).*
18. Right-click the associated System number and select **Refresh System**. This establishes a new connection to the specified System and populates the list with devices on that system. *The communication method is then highlighted in green on the bottom of the NetLinx Studio window.*

NOTE

*If the connection fails to establish, a Connection Failed dialog appears. Try selecting a different IP Address if communication fails. Press the **Retry** button to reconnect using the same communication parameters. Press the **Change** button to alter the communication parameters and repeat steps 4 thru 18.*

Verifying the current version of NetLinx Master Firmware

All NI Controllers contain both an on-board NI Master and an Integrated Controller.

- The on-board Master shows up within the Online Tree as **00000 NI Master**
- The Integrated Controller of the NI device shows up as **0XXXX NI-XXXX (ex: 050001 NI-700)**

Each of these components has its own corresponding firmware shown in parenthesis ().

1. After Studio has establish a connection to the target Master, click on the **OnLine Tree** tab in the Workspace window to view the devices on the System. *The default System value is one (1).*
2. Right-click the associated System number and select **Refresh System**. This establishes a new connection to the specified System and populates the list with devices on that system. *The communication method is highlighted in green on the bottom of the NetLinx Studio window.*

NOTE

*The current installed firmware version of the on-board NI Master is displayed to the right of the device within the Online Tree tab as **00000 NI Master**.*

3. After the Communication Verification dialog window indicates active communication between the PC and the Master, verify the NetLinx Master (***00000 NI Master***) appears within the **OnLine Tree** tab of the Workspace window (FIG. 28). *The default NI Master value is zero (00000) and cannot be changed.*
4. If either the on-board NI Master or Integrated Controller is not the latest firmware version, follow the procedures outlined in the following sections to obtain these Kit files from **www.amx.com** and then transfer the new firmware Kit files to the device.

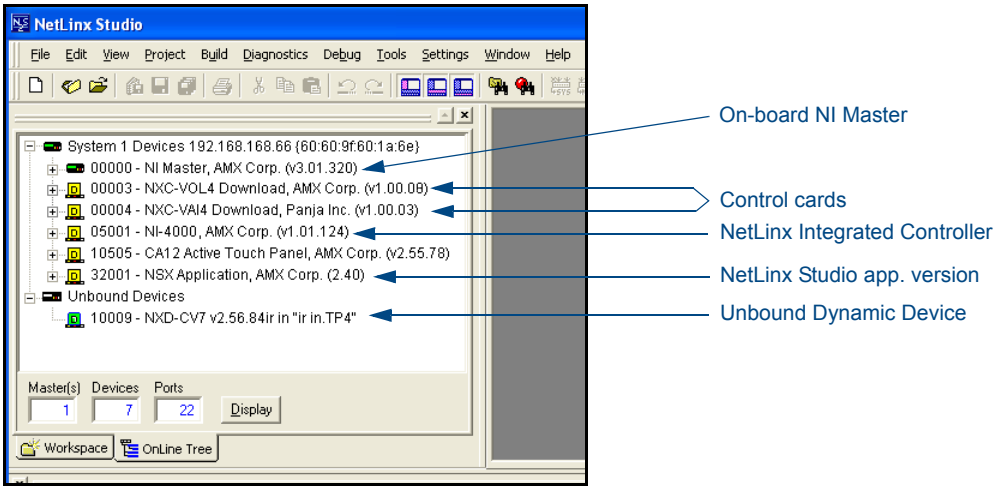


FIG. 28 Sample NetLinx Workspace window (showing OnLine Tree tab)

Upgrading the On-board Master Firmware via an IP

The on-board Master firmware Kit file is not the same as the Integrated Controller Kit file. Below is a table outlining the current sets of on-board Master and Integrated Controller Kit files used by the NI-Series of products:

Firmware Kit File usage for NI Controllers	
NI-3101 (FG2105-05/15)	On-board Master Kit file: 2105_04_NI-X100_**Master**
	Integrated Controller Kit file: 2105_04_NI-X100

NOTE

Only Master firmware Kit files use the word _Master in the Kit file name.

1. Follow the procedures outlined within the *Communicating with the NI Device via an IP* section on page 26 to connect to the target NI device via the web.
2. After Studio has established a connection to the target Master, click the **OnLine Tree** tab of the Workspace window to view the devices on the System. *The default System value is one (1).*
3. Right-click the associated System number and select **Refresh System**. This establishes a new connection to the specified System and populates the list with devices on that system. *The communication method is highlighted in green on the bottom of the NetLinx Studio window.*
4. After the Communication Verification dialog window verifies active communication between the PC and the Master, verify the NetLinx Master (***00000 NI Master***) appears in the **OnLine Tree** tab of the Workspace window. *The default NI Master value is zero (00000).*

NOTE

***First** upgrade of the on-board Master using the Master's Kit file.*
The Integrated Controller can later be upgraded using the Controller's Kit file.
BOTH Kits should be used when upgrading any firmware associated with the Integrated Controllers.

5. If the on-board Master firmware being used is not current, download the latest Kit file by first logging in to **www.amx.com** and then navigating to **Tech Center** > **Firmware Files** to locate the desired file from within the NetLinx section of the web page.
6. Click on the desired Kit file link, accept the Licensing Agreement, and verify download of the correct NI Master firmware (Kit) file to a known location.
7. From within Studio, select **Tools** > **Firmware Transfers > Send to NetLinx Device** from the Main menu to open the Send to NetLinx Device dialog (FIG. 29). Verify the target's System number matches the

value listed within the active System folder in the **OnLine Tree** tab of the Workspace. **The Device number is always 0 for the NI Master**.

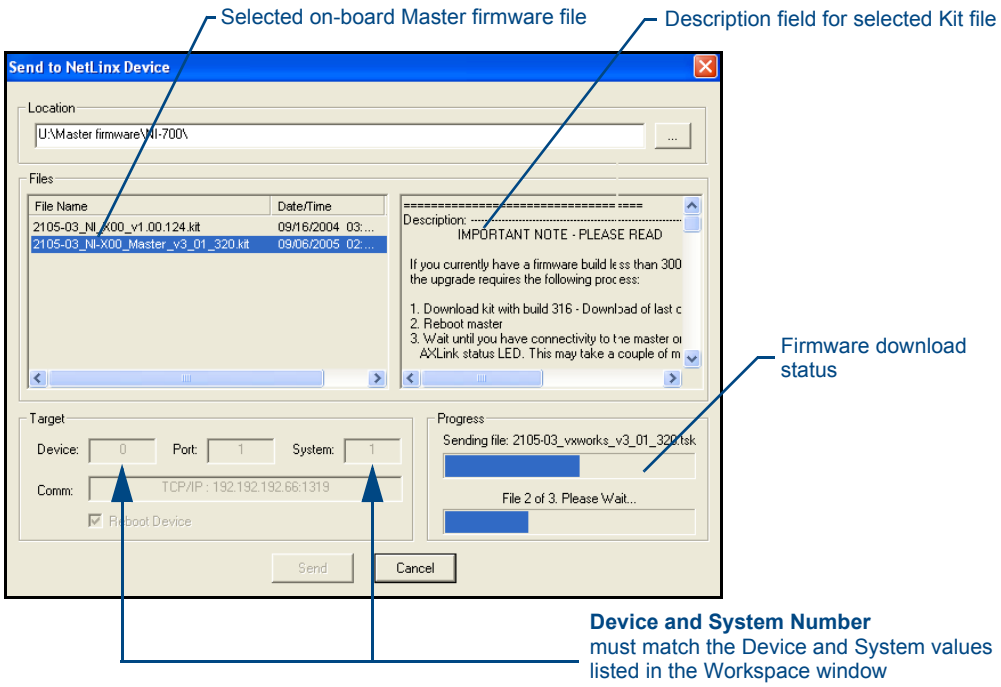


FIG. 29 Send to NetLinx Device dialog (showing on-board NI_Master firmware update via IP)

8. Select the NI Master's Kit file from the **Files** section (FIG. 29).

NOTE

The Kit file for the NI-2100/3100/3101-SIG/4100 Series of NI Masters begins with 2105_04_NI-X100_Master.
DO NOT use any Master Kit file other than the one specified, since each Master Kit file is specifically configured to function on a specific NI unit.

9. Enter the **System** number associated with the target Master (*listed in the OnLine Tree tab of the Workspace window*) and verify the Device number value. *The Port field is greyed-out.*

- **The Device number is always 0 for the NI Master**.

10. Click the **Reboot Device** checkbox to reboot the NI unit after the firmware update process is complete.

11. Click **Send** to begin the transfer. The file transfer progress is indicated on the bottom right of the dialog box (FIG. 29).

NOTE

***Only upon the initial installation** of a new Kit file to an on-board Master will there be a error message displayed indicating a failure of the last component to successfully download. This is part of the NI Master update procedure and requires that the firmware be reloaded after a reboot of the unit. This consecutive process installs the final component of the new Kit file.*

12. After the last component fails to install, click **Done.**

13. Click **Reboot** (*from the Tools > Reboot the Master Controller dialog*) and wait for the System Master to reboot. *The STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*

14. Press **Done** once until the *Master Reboot Status* field reads **Reboot of System Complete**.

15. Repeat steps 5 - 9 again (the last component will now successfully be installed).

16. Click **Close** once the download process is complete.

NOTE

The OUTPUT and INPUT LEDs alternately blink to indicate the on-board Master is incorporating the new firmware. Allow the Master 20 - 30 seconds to reboot and fully restart.

17. Right-click the System number and select **Refresh System**. This establishes a new connection to the System and populates the list with the current devices (*and their firmware versions*) on your system.

Upgrading the NI Controller Firmware via IP

1. Follow the procedures outlined within the *Communicating with the NI Device via an IP* section on page 26 to connect to the target NI device via the Web.
2. After NetLinx Studio has established a connection to the target Master, click the **OnLine Tree** tab of the Workspace window to view the devices on the System. The default System value is one (1).
3. Right-click the associated System number and select **Refresh System**. This establishes a new connection to the specified System and populates the list with devices on that system. The communication method is highlighted in green on the bottom of the NetLinx Studio window.
4. After the Communication Verification dialog window verifies active communication between the PC and the NI unit, verify that the device appears in the **OnLine Tree** tab (FIG. 30) of the Workspace window (***ex: NI-3101***). This entry is different than that of the NI Master, which uses a device value of *00000* (see below):

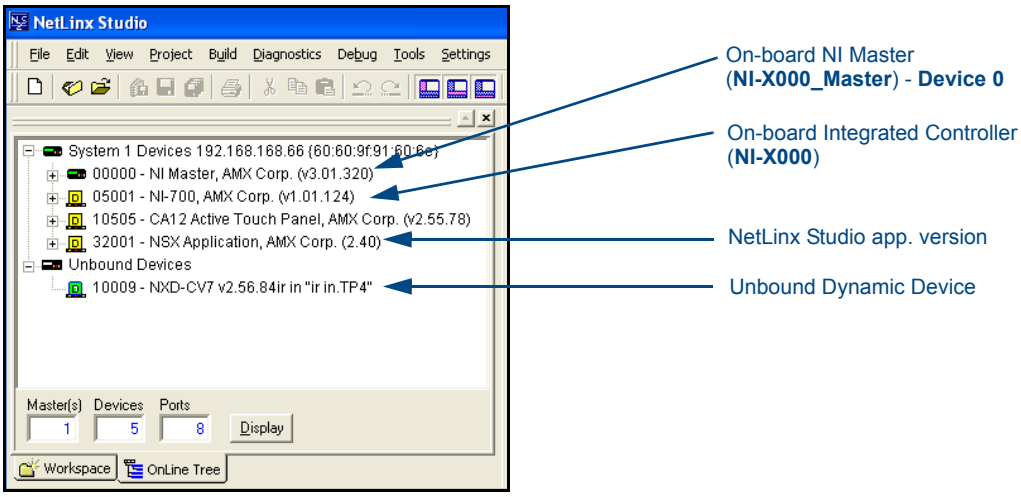


FIG. 30 Sample NetLinx Workspace window (showing SEPERATE NI-Master and Controller)

5. If the NI Controller firmware being used is not current, download the latest Kit file by first logging in to **www.amx.com** and then navigating to **Tech Center** > **Firmware Files**, locating the desired file from within the *NI Series Device* (Integrated Controller) section of the web page.
6. Click on the desired Kit file link, accept the Licensing Agreement, and verify that the Integrated Controller firmware (Kit) file has been downloaded to a known location.
7. From within NetLinx Studio, select **Tools** > **Firmware Transfers > Send to NetLinx Device** from the Main menu to open the *Send to NetLinx Device* dialog (FIG. 31). Verify that the target's System number matches the value listed within the active System folder in the **OnLine Tree** tab of the Workspace. **The Device must match the entry for the on-board Integrated Controller (NI-X000/NI-X000) device**.

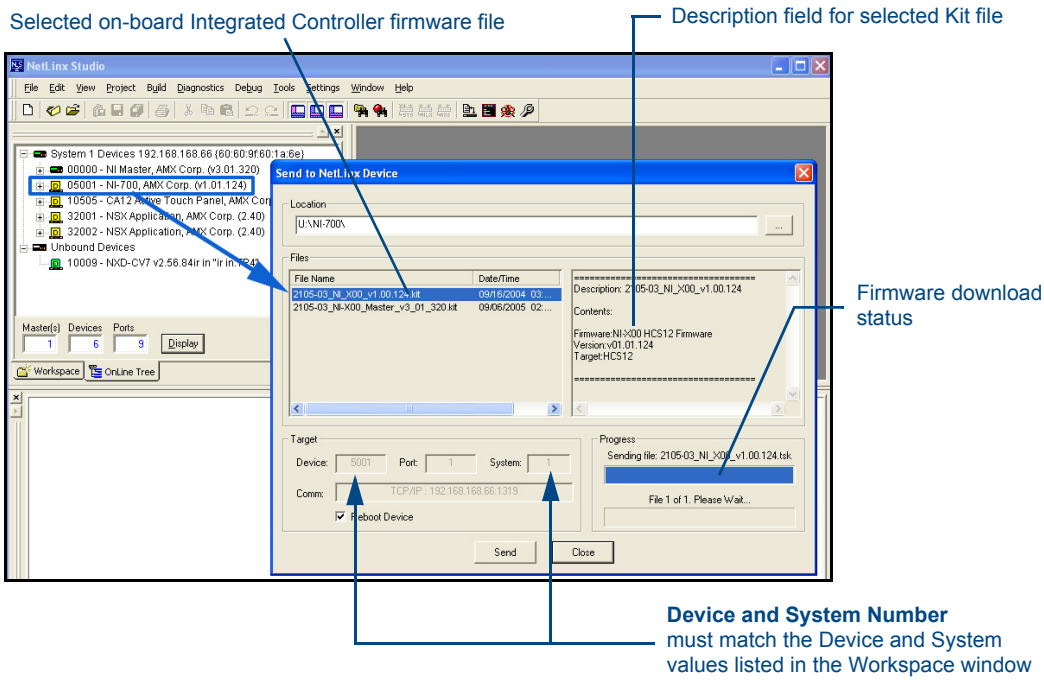


FIG. 31 Send to NetLinx Device dialog (showing on-board Integrated Controller firmware update via IP)

NOTE

*The Kit file for the Integrated Controller on the NI-2100/3100/3101-SIG/4100 Series begins with **2105_04_NI_X100.***
DO NOT use any Kit file other than the one specified, since each Kit file is specifically configured to function on a specific NI unit.

8. Select the Integrated Controller's (**_X00**) from the **Files** section (FIG. 31).
9. Enter the **System** and **Device** numbers associated with the target Master (*listed in the Workspace window*). *The Port field is greyed-out.*
10. Click the **Reboot Device** checkbox to reboot the NI device after the firmware update process is complete.
11. Click **Send** to begin the transfer. The file transfer progress is indicated on the bottom-right of the dialog (FIG. 31).
12. Click **Close** once the download process is complete.

NOTE

The OUTPUT and INPUT LEDs alternately blink to indicate the unit is incorporating the new firmware. Allow the unit 20 - 30 seconds to reboot and fully restart.

13. Right-click the System number and select **Refresh System**. This establishes a new connection to the System and populates the list with the devices and their firmware versions currently on the system.

NOTE

If the connection fails to establish, a Connection Failed dialog appears.
Try selecting a different IP Address if communication fails.
*Press the **Retry** button to reconnect using the same communication parameters.*
*Press the **Change** button to alter the communication parameters and repeat steps 2 thru 11.*

NetLinx Security within the Web Server

NetLinx Masters incorporate built-in security for HTTPS and Terminal sessions (*enhanced with SSL and SSH respectively*), ICSP data verification/encryption, and Server Port configuration. By using both SSL certificate verification and encryption over a *secured HTTP* (HTTPS) connection, this version of NetLinx firmware provides users with a more convenient web-based method of securing both the Master and its data communications. Additional features in this release are the use of both authentication protocols and the ability to perform online NetLinx Diagnostics via the web server.

Terminal setup and security configuration are still valid and supported in this build of the NetLinx Master firmware.

This NetLinx Web Server is used to power Master security, data encryption, and SSL certificate/encryption features on current AMX Masters such as the ME260/64 and NI-Series of Controllers. This web server not only provides username and password security for the target Master, but also a new level of secure encryption for ICSP data communication among the various AMX software and hardware components. New security features for the Masters include:

- Enhanced Username and Password requirements
- HTTPS and SSL certificate interaction
- Use of a pre-installed AMX SSL certificate
- ICSP communication and encryption

The first layer of security for the Master involves prompting a user to enter a valid username and password before gaining access to a secured feature on the target Master. This data is pre-configured by the administrator within the Group and User Level pages of the Security section. **If an option is enabled within the System Security page**, a user is prompted to enter a valid username and password before gaining access to the corresponding feature. This access is only granted if their information matches a previously created profile assigned sufficient rights for that action. An already logged in user can enter a new profile by using the *Login* field to enter a new profile's
username and profile.

- This username and password information is also used by both G4 touch panels (within the System Connection firmware page) and AMX software applications such as NetLinx Studio v 2.4 (via the Master Communications dialog) to communicate securely with a Master using encrypted communication.

The second layer of security uses a combination of *secure HTTP* (HTTPS) communication and SSL encryption to secure data being transferred from the web server application and the target Master.

To ensure this higher degree of security on the Master, an administrator can disable the HTTP Port access, enable HTTPS Port access (both from within the same **Manage System** > **Server** page), and then alter the level of encryption on the current SSL Certificate to meet their security needs.

- **SSL** (*Secure Sockets Layer*) is a protocol that works by encrypting data being transferred over an HTTPS connection. URLs that require a secure connection begin with **https:** instead of **http:** (in the browser's *Address* field). These security capabilities are configured to function via a web session within your browser. The encryption level (64 or 128-bit) achieved over the HTTPS Port is done via the SSL Certificate currently in use on the target Master. Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, HTTPS is designed to transmit individual messages securely. Therefore both HTTPS and SSL can be seen as complementary and are configured to communicate over the same port on the Master.

The third layer of protection is an SSL Certificate (specifically identifying the target Master and using a unique key to encrypt data). SSL works by using a private key to encrypt data that's transferred over the SSL connection. By default, current Masters are shipped with a default AMX SSL certificate called *sslexample.amx.com*. This pre-configured certificate can be used as a road map to create a unique certificate. The Master's SSL certificate can be either requested (from an external CA) or self-generated, and then installed/imported onto the target Master. This action adds the certificate to the trusted site certificate listing within the computer's Internet browser.

A fourth layer of security enables the encryption of data communication amongst the various AMX hardware and software components (such as between NetLinx Studio and the Master, or TPDesign4 and the touch panel (*communicating through the Master*)). Refer to the*Security Features* section on page 38 for more information.

NetLinx Security Terms

The following table lists some commonly used NetLinx Security terms:

NetLinx Security Terms	
User	A user is a single potential client of the NetLinx Master.
Administrator	An administrator has privileges to modify existing NetLinx Master access groups, users, and their rights. The administrator can also assign NetLinx communication access rights for different users or groups (ex: Telnet and HTTP access) and configure the Master's SSL server certificate.
Group	A group is a logical collection of users. Note that any properties possessed by a group (ex: access rights, directory associations, etc.) are inherited by all members of that group.
Username	A username is a valid character string (4 - 20 alpha-numeric characters) defining the user. This string is ***case sensitive*** and each username must be unique.
Group name	A group name is a valid character string (4 - 20 alpha-numeric characters) defining the group. This string is ***case sensitive*** and each group name must be unique.
Password	A password is a valid character string (4 - 20 alpha-numeric characters) to supplement the username in defining the potential client. This string is also ***case sensitive***.
Access Rights	Each of the NetLinx Master's features has pre-defined security procedures. The access right for a particular feature determines if a user or group has access to that feature by entering a valid username and password.

NOTE

*The maximum length of a username or password is 20 characters. The minimum length of a username or password is four characters. Characters such as **#** (pound) **&** (ampersand) and **' "** (single and double quotes) are invalid and should not be used in usernames, group names, or passwords.*

Accessing an Unsecured Master via an HTTP Address

Refer to the*Upgrading the On-board Master Firmware via an IP* section on page 29 for more 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

*Although Telnet security configuration access can no longer be used on a Master with this firmware, a Terminal connection (using HyperTerminal) can still be established using the Master's USB low-speed connection (if the Telnet Port is enabled via the **Manage System** > **Server** page).*

Once the Master's IP Address has been set through NetLinx Studio version 2.4 or higher:

1. Launch your web browser.
2. Enter the IP Address of the target Master (***ex: http://198.198.99.99***) into the web browser's *Address* field.
3. Press the **Enter** key on your keyboard to begin the communication process between the target Master and your computer.
   - Initially, the Master Security option is disabled (from within the **System Security** page) and no username and password is required for access or configuration.
   - Both HTTP and HTTPS Ports are enabled by default (via the **Manage System** > **Server** page).
4. The first active page displayed within your open browser page is **Manage WebControl Connections**.

NOTE

*Once HTTP Access is enabled for a Master; certificate verification and username and password verification must occur. Refer to the*Accessing an SSL-Enabled Master via an IP Address section on page 92 *for more information.*

Browser Application Frames

A web page (FIG. 32) can be divided into separate sections or frames, each of which can be independent of one another and display their own information.

Located on the left side of the populated Browser window is the Navigation frame which allows a user to navigate throughout the application. Located on the right side of the Browser window is the Active frame which displays the pages corresponding to the currently selected option from within the Navigation frame.

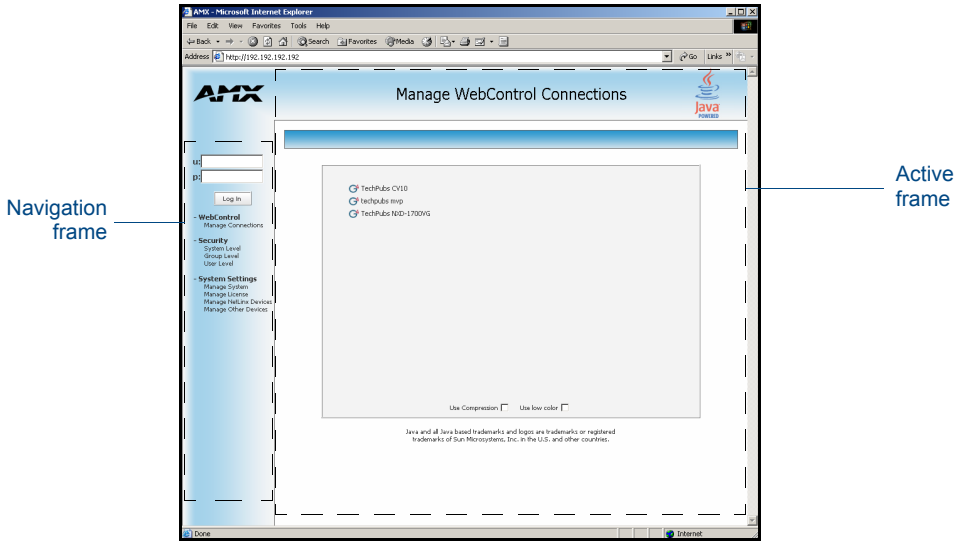


FIG. 32 Browser Application frames

The first Active frame displayed within the Browser is the Manage WebControl Connections page.

Default Security Configuration

Security for web pages is separated into two access groups: HTTP and Configuration:

- **HTTP Access** allows an authorized user to view these web pages by first requiring the entry of a username and password at the beginning of every connection session with the target Master. If **Master Security** is not enabled, the *username* and *password* fields are not displayed and the Master is openly accessible. *The Master Security configuration prevents users from altering any security or operational parameters. Unless this option is enabled, all subordinate options are inaccessible and greyed-out.*
- **Configuration** access is initially greyed-out until the Master Security option is enabled. This feature requires an authorized user provide a valid username and password before being granted access to change configuration and communication parameters on the target Master. *Only with this type of access can a user begin to alter security or operational parameters such as access rights, Port assignments, System values, and SSL certificate usage.*

If a user is not currently logged-into the Master (*via the initial Login screen*) and they attempt to access a feature wherein authentication is required, they are prompted with a message to log into the Master (via the **Log In** button) (FIG. 33). After the user's information and rights are confirmed, the login process is successfully completed and the button changes state and displays **Log Out**. A user must be logged into the system before their associated rights can be activated for the current session.

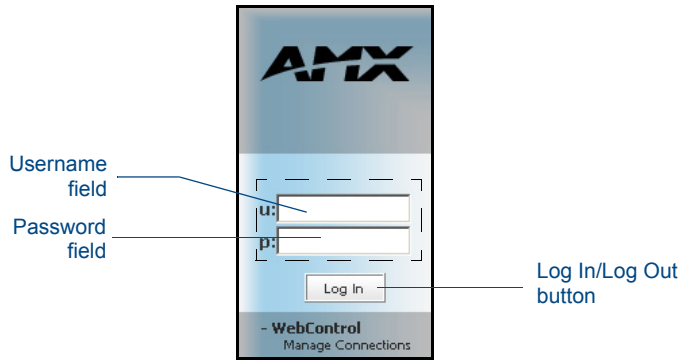


FIG. 33 Log In/Log Out fields

NOTE

*Authentication is based upon matching the user's data to pre-configured username and password information, and then assigning the rights assigned to that user. The maximum length of a username or password is 20 characters. The minimum length of a username or password is four characters. Characters such as **#** (pound) **&** (ampersand) and **' "** (single and double quotes) are invalid and should not be used in usernames, group names, or passwords.*

There is no limit to the number of concurrent logins allowed for a single user. This feature facilitates the creation of a single user *(which is really an ICSP device such as a touch panel)* that is provided to a number of ICSP devices using the same login to obtain access to the Master.

- As an example, if you had 50 devices connected to a Master, you would not have to create 50 individual user accounts-one for each device. Instead, you only need to create one to which all 50 devices use for access.

By default, the NetLinx Master creates the following accounts, access rights, directory associations, and security options:

Default Security Configuration (case-sensitive)		
Account 1	Account 2	Group 1
Username: administrator	Username: NetLinx	Group: administrator
Password: password	Password: password	Rights: All
Group: administrator	Group: none	Directory Association: /*
Rights: All	Rights: FTP Access	
Directory Association: /*	Directory Association: none	

Security Options: FTP Security - Enabled
Admin Change Password Security - Enabled
All other options - Disabled

NOTE

By default, Master Security (and all subordinate options) are disabled. If the user/group is given FTP access rights by the administrator, all directories can become accessible (read/write/modify).

- The ***administrator*** user account cannot be deleted or modified with the exception of its password. Only a user with both **Configuration** access and administrator rights can alter the administrator's password.
- The ***NetLinx*** user account was created to be compatible with previous NetLinx Master firmware versions. This account is initially created by default and can later be deleted or modified.
- The ***administrator*** group account cannot be deleted or modified.

Master Firmware Security Access Parameters

- Master Security Configuration
- Terminal (RS232/USB Configuration port) security
- HTTP (Web Server) Security (*allows for access via a secure HTTP connection (if enabled) by requiring a username and password*)
- Telnet Security
- Configuration *(allows the alteration of current communication, system, and security settings by requiring a username and password)*
- ICSP Connectivity (*for AMX product communication*)
- Encryption Requirement (*only used if ICSP Connectivity is enabled - encrypts the data being transferred among the different AMX products*)

NOTE

Installation of SSL functionality onto your Master causes security setup via Telnet to be disabled. Although Telnet security configuration access can no longer be used on the Master, a Terminal connection (using HyperTerminal) can still be established using the Master's RS232 Program port.

Web Control

This section of the Navigation frame contains the Mange Connections feature which allows control of compatible devices communicating with the target Master.

Managing WebControl Connections

This page (FIG. 34) is accessed by clicking on the **Manage connections** link. Once activated, this page displays links to G4 panels running the latest G4 Web Control feature.

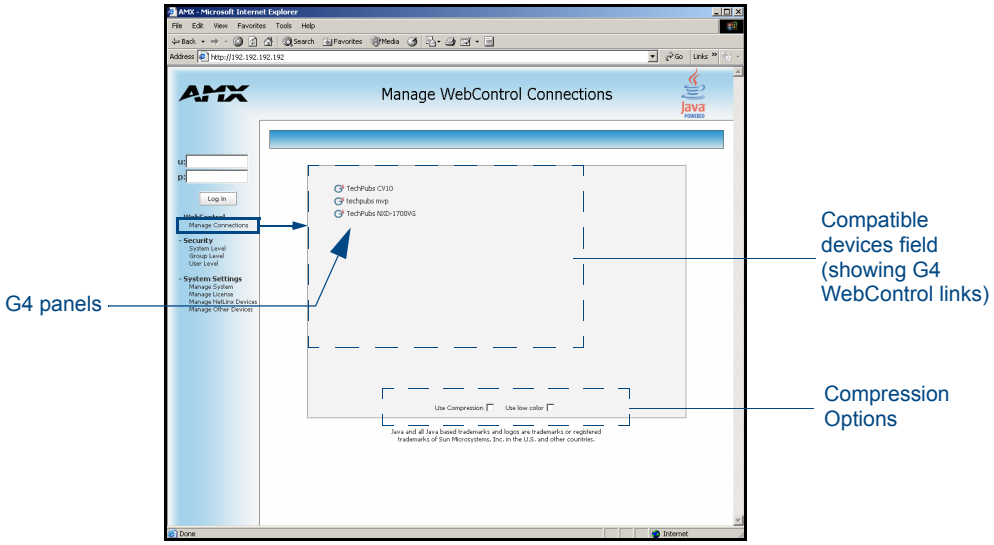


FIG. 34 Manage WebControl Connections page (populated with compatible panels)

If the **Master Security** and **HTTP Access** options have not been previously enabled on the target Master, a user does not need to Log into the Master to gain access to the Manage WebControl Connections page. This page allows a user to view all G4 enabled touch panels running G4 WebControl.

- To establish a secure connection between the touch panel and the target Master, the panel must be using a valid username and password (*that can be matched to a previously configured user on the target Master*) and the **ICSP Connectivity** option must be enabled within the System Level page.
- If at some later point, that user profile is removed from the Master, reboot both the panel and Master. After reboot, the connection status of the panel (from with the firmware Setup page) shows *"No Encryption"*.

Clicking on a G4 WebControl link opens a separate browser window which is configured to display the current information from the panel using the native resolution of the target panel. *An example is a CA15 panel link opening a new window using an 800 x 600 resolution.*

The following table lists the features available to an administrator or other authorized user from the Manage WebControl Connections page:

Manage WebControl Connection Page Features	
Feature	**Description**
Compatible Devices Field:	This area displays G4 icons (with associated links) if a G4 panel running Web Control is communicating with the target Master.
Communication Compression Options:	Allows you to choose from among two compression options: • These compression settings are most useful when working either over a bandwidth-restricted LAN or over the Internet. • **Use Compression** allows the user to specify that the transmitted data packets be compressed. This speeds up the visual responses from the panel by minimizing the size of the information relayed through the web and onto the screen. • **Use Low Color** allows the user to specify the number of colors used to display the image from the panel be reduced. By reducing the numbers of colors, both the size of the information is reduced and the response delay is decreased.

Security Features

This section of the Navigation frame (FIG. 35) contains the NetLinx system security parameter links which allow an authorized user to define access rights at the system level and those for the various groups or users.

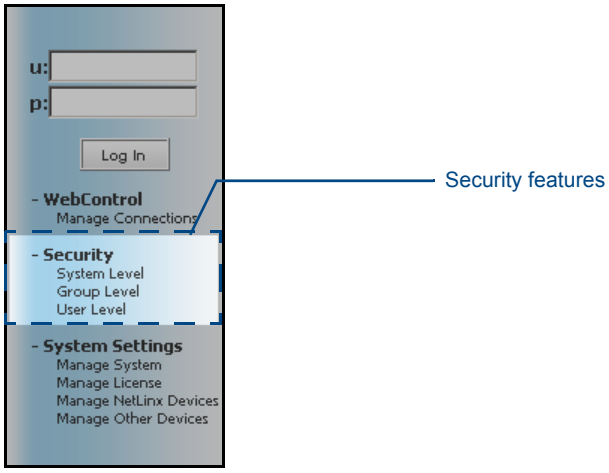


FIG. 35 System Level Security - Enable/Disable System Security page

NOTE

*Security settings on related pages (such as the System Level, Group Level, and User Level) require that an authorized user be logged into the Master and have **Configuration Access** rights either directly assigned with that user or associated with the related Group.*

The following table lists the NetLinx System Security options that can be granted or denied by an administrator or other authorized user:

Security Features	
Feature	**Description**
System Level:	Provides an authorized user with the ability to alter the current security options of the system assigned to the target Master.
Group Level:	Provides an authorized user with the ability to assign and alter group properties such as creating, modifying, or deleting a group's rights, and also allows for the definition of the files/ directories accessible by a particular group. • Any properties possessed by a group (access rights/directory associations, etc.) are inherited by all members of that group.
User Level:	Provides an authorized user with the ability to assign and alter user properties such as creating, modifying, or deleting a users' communication rights, and defining the files/directories accessible by a particular user.

WARNING

Enabling the Master Security option after the groups, users, and passwords have been set up is highly recommended. If not, when the user accesses the Master from within another session, the default administrator username and password must be used for access.

Security - System Level Security page

To access this page, click the **Security Level** link from within the Security section of the Navigation frame. This page is strictly used to guarantee that a valid username and password is entered prior to gaining access to the listed features and options.

NOTE

If the Master Security option is not selected, the Master is completely open and can be modified by anyone accessing the target Master via the web server's UI.

The options on the NetLinx Master Security page (FIG. 36) are only accessible and configurable if the **Master Security** checkbox is selected. The **Master Security** checkbox selection toggles the appearance of the NetLinx Master security options and makes them accessible. Enabling an option on this page requires that a user enter a valid username and password before they are granted access to the specific feature. Some examples are:

- Requiring verification before accessing the Master - **HTTP Access** must be enabled.
- Requiring verification before altering a current Master security setting - **Master Security** and **Configuration** must be enabled.
- Requiring verification from a communicating AMX software (such as NetLinx Studio v 2.4 or TPD4 v 2.5) before accepting communication for file/firmware transfers, the **Configuration**, **ICSP Connectivity** and **Require Encryption** options must be enabled.

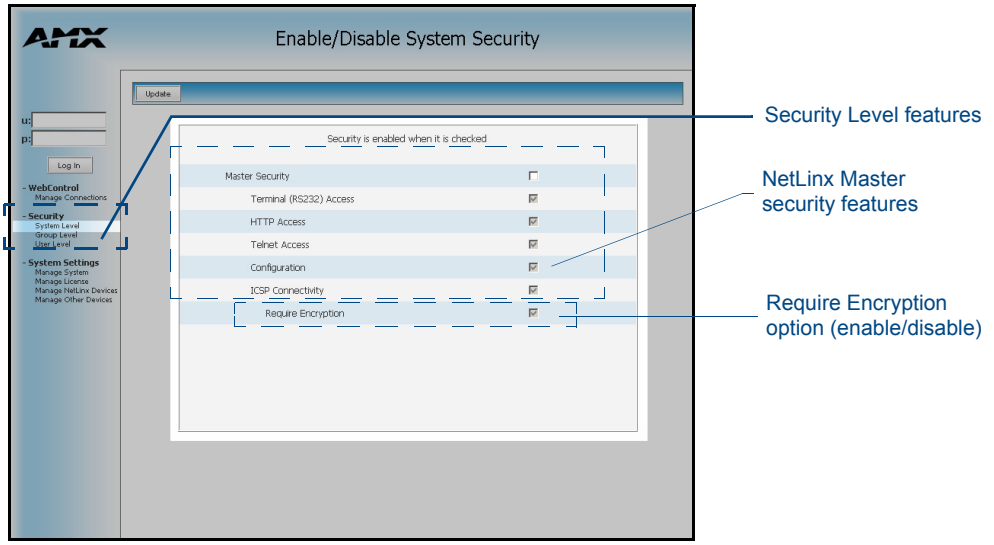


FIG. 36 System Level Security - Enable/Disable System Security page

System Level Security Page	
Feature	**Description**
Master Security:	This option allows an authorized user to require that a valid username and password be required for access to a feature listed on this page. • These are global options that enable or disable the login requirement for both users and groups. • If the Master Security checkbox is not enabled, all subordinate options are greyed-out and not selectable, meaning that the Master is completely unsecured and can be altered by any user (regardless of their rights).
Terminal (RS232/USB) Access:	This selection determines if a username and password is required for Terminal communication (*through the USB connector*). • If Terminal Security is enabled, a user must have sufficient access rights to login to a Terminal session and communicate with the Master.
HTTP Access:	This selection determines if a username and password is required for communication over HTTP or HTTPS Ports (see FIG. 37). • If enabled, a user must have sufficient access rights to browse to the NetLinx Master via a Web Browser. • Enabling this field requires the user (within a new session) submit a valid username and password before being able to view the web server pages. • If disabled, the Master is open for viewing and does not ask for this information during any consecutive sessions (until the user attempts to access a feature which is enabled within this page). • This requirement of a valid username and password affects both HTTP and HTTPS communication with the target Master using the web server.

System Level Security Page (Cont.)	
Feature	**Description**
Telnet Access:	This selection determines if a username and password is required for Telnet Access (see FIG. 37). • If Telnet access is enabled, a username and password is required before allowing communication over either the Telnet and/or SSH Ports. ***SSH version 2 is only supported.*** • This authorized user must have sufficient access rights to login through a Telnet session to the Master. • To establish a secure Telnet connection, an administrator can decide to disable the Telnet Port and then enable the SSH Port. Refer to the*Setting the Master's Port Configurations* section on page 61.
Configuration (security):	This selection determines if a username and password is required before allowing a group/user to alter the current Master's security configuration and communication settings (see FIG. 37). • Configuration access provides the user with the ability to perform configuration functions on the NetLinx system through NetLinx Studio. ***This includes such things as: IP configuration/Reset, URL list settings, Master communication settings, and security parameters***. • If security Configuration is enabled, a user/group must have sufficient access rights to access the Main Security Menu. • Any time a configuration operation is performed, the Master verifies the current access rights for that feature and then requires a valid username and password (*if not already logged in*). - An example would be if you are trying to add a New User or modify the rights of an existing Group.
ICSP Connectivity:	This selection determines if a username and password is required prior to communication with a target NetLinx Master via an ICSP connection using any transport method (TCP/IP, UDP/IP, and RS-232) (see FIG. 37). • If this access is enabled and the user is not logged-in, when the user attempts to connect, the authentication fails and displays an "Access not allowed" message. • This feature allows communication amongst various AMX hardware and software components. This feature works in tandem with the Require Encryption option to require that any application or hardware communicating with the Master must provide a valid username and password. • Refer to the*ICSP Authentication* section below for more detailed information.
Require Encryption:	Requires that any data being transmitted or received via an ICSP connection (among the various AMX products) be encrypted and that any application or hardware communicating with the Master over ICSP must provide a valid username and password.

- The following graphic illustrates the Ports which can be enabled for the validation of rights by using a valid username and password. When one of the above options is enabled, the Master then requires the entry of a valid username and password to validate rights for that action and then grant or deny access.

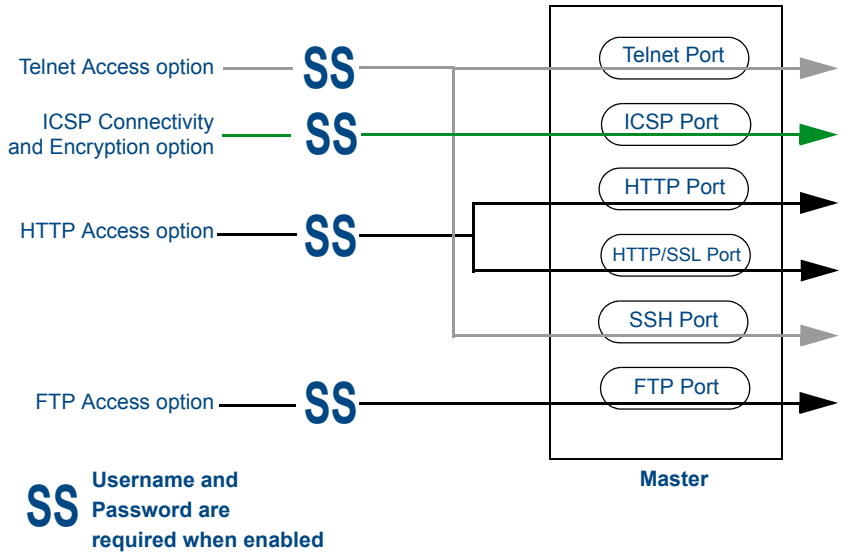


FIG. 37 Port Communication Settings

Setting the system security options for a NetLinx Master

This page simply toggles the requirement of a user to enter a valid username and password before gaining access to a particular feature. For every action, the Master validates whether a username and password are required and whether the user has sufficient rights. Refer to the*Security - Group Level Security page* section on page 44 for more information on the assignment of the Group/User rights. For example, if the user were attempting to modify the configuration parameters of the Master, their username and password must be associated with a profile which was previously granted Configuration Access privileges within the web server. If they their profile didn't have enough rights to accomplish their action an *"Insufficient Rights..."* message appears on top of the active page.

1. Enter the URL/IP Address of the target Master into the *Address/URL* field within the web browser. *Initially the connection is unsecured and communication can be made via an HTTP connection.* Refer to the*Accessing an Unsecured Master via an HTTP Address* section on page 34 for more detailed instructions.
2. Click the **Security Level** link (*from within the Security section of the Navigation frame*) to open the System Security page. The **Master Security** checkbox selection (FIG. 38) toggles the appearance of the NetLinx Master security options.
3. Click on the **Master Security** checkbox to access to the security parameters on the target Master and allow an authorized user (*with configuration access rights such as an Administrator*) the ability to alter the subordinate security parameters. Refer to the*Security - System Level Security page* section on page 39 for more detailed field descriptions.

NOTE

Each selection simply toggles the security setting from enabled to disabled. By default, the Master Security option is disabled (unchecked), including the subordinate Master Security components (even though they might show a checkmark, they are greyed out). An open Master does not require a user to enter a valid username and password.

4. Click on the desired access parameters and configuration checkboxes necessary to require user validation prior to usage.
   - Enabling the Terminal, HTTP, and Telnet Access options require that a valid username and password be entered prior to gaining access to the desired action. **If the HTTP Access option is enabled, upon the initial connection to the Master (via the web browser) the Login page appears and requires a valid username and password be entered before allowing access to the web server pages.**
   - Enabling the Configuration option requires that the user be logged in and their rights validated before allowing any modification to the current Master security configuration and communication

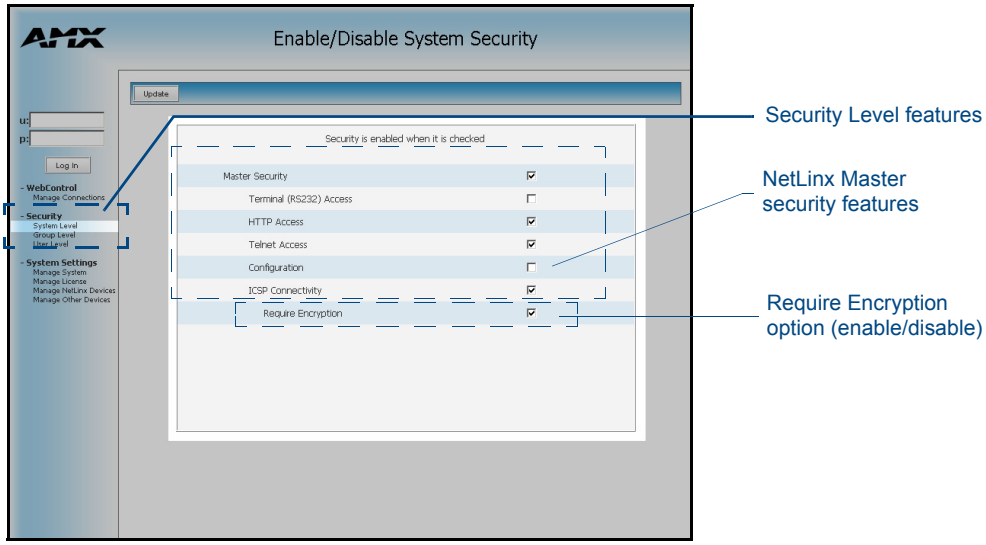


FIG. 38 System Level Security - Enable/Disable System Security page with selections

parameters. **If the Configuration option is enabled and the user wants to modify the Master's IP Address; they would either be prompted to log in (via the Login button) or if already logged in, notified whether their rights are sufficient to allow them to change the current parameter.**

- The **ICSP Connectivity** option is required to allow authenticated and/or secure communication between the Master and other AMX hardware/software. To establish an authenticated ICSP connection (where the external AMX hardware/software would have to provide a valid username and password). This option **must be enabled** (checked).

5. Click on the checkbox next to **Require Encryption** to enable the requirement of data encryption over the ICSP connection. Note that this is optional and if enabled, requires more processor cycles to maintain.
6. Click the **Update** button to accept and save any changes on this page back to the Master. Updating these changes is instantaneous and does not require a reboot. Successful incorporation of the changes to the Master's security configurations results in an on-screen message stating: *"Security is enabled when it is checked"*.

NOTE

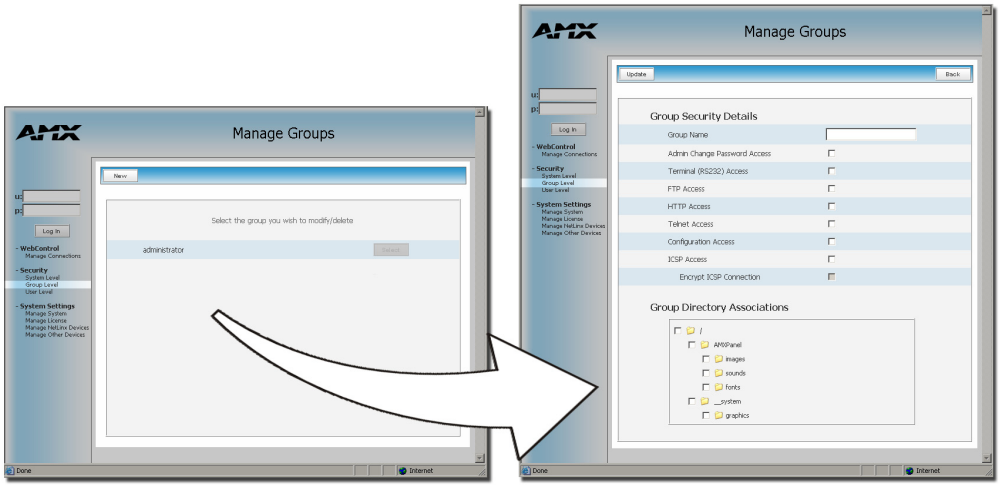
A Group represents a logical collection of individual users. Any properties possessed by a group (ex: access rights, directory associations, etc.) are inherited by all members of that group.
The "administrator" group account cannot be deleted or modified.

ICSP Authentication

In a Master-to-Master system, the Master which accepts the IP connection initiates the authentication process. This configuration provides compatibility with existing implementations and provides more flexibility for the implementation of other devices.

Security - Group Level Security page

To access this page, click the **Group Level** link (*from within the Security section of the Navigation frame*). This page (FIG. 39) allows an authorized user to both select and modify an existing group, delete an existing group, or add a new group. *Unless you are logged in with administrator privileges, you will not be allowed to modify the default administrator profile.*



Manage Groups page

Configure Group Properties page (adding a new group)

FIG. 39 Group Level Security - Manage Groups Security page

Manage Group Page	
Feature	**Description**
Manage Groups page:	This page allows a user to either modify the rights for a group available from the displayed list or use the **New** button to access a secondary window where a user can modify the rights for either the new or existing group.
New	• Clicking this button allows a user to add a new group and configure its settings through the Configure Group Properties page.
Select	• Clicking this button takes you to the selection's corresponding Configure Group Properties page. • This button is greyed-out if the current user doesn't have the right to modify the rights for that group. Note: The "administrator" group can't be modified unless you are logged in as a user with Configuration Access rights.

Configure Group Properties Page	
Feature	**Description**
Configure Group Properties:	This page allows an authorized user to configure the options for either a pre-existing or new group. Configuration on this page consists of both the options and directories to which the group is granted access.
Update	• This button submits the modified page (form) information back to the server. • If the group was successfully added after pressing the **Update** button; a status message of "Group XYZ was successfully added" is displayed.
Back	• This button returns the user to the Manage Groups page.
Delete	• This button is only available when modifying/deleting an existing group.
Group Security Details:	• This section provides the user with several rights which can either be enabled or disabled.
Group Name	• A valid character string defining the name of the group (4 - 20 alpha-numeric characters). • The string is case sensitive and must be unique.
Admin Change Password Access	• This selection enables or disables the group's right to change the administrator's user passwords. ***Note:*** Once the Administrator's password has been changed, the default password can no longer be used to gain access.
Terminal (RS232/USB) Access	• This selection enables or disables Terminal Security Access for the target group (through the USB connector).
FTP Access	• This selection enables or disables FTP Access for the target group.
HTTP Access	• This selection enables or disables Web Server access for the target group.
Telnet Access	• This selection enables or disables Telnet Security access for the target group.
Configuration Access	• This selection enables or disables the ability of a group to alter the security Configuration settings such as: ***- IP configuration/Reset, URL list settings, Master communication settings, and file transfers***.
ICSP Access	• This selection grants the members of this Group ICSP access. • ICSP communication allows a user to connect to the target NetLinx Master via ICSP connection using any transport method (TCP/IP, UDP/IP, and RS-232/USB).
Encrypt ICSP Connection	• This selection enables encryption of the ICSP communication. • This checkbox is greyed-out until ICSP Access is enabled.
Group/Directory Associations:	• Provides an authorized user with a view of current directories on the target Master that are available to the selected group. • A Directory Association defines the directory paths and files a particular user or group can access via the Web Server on the NetLinx Master. • The displayed folders are the directory pathnames present on the target Master. These folder/files can be placed on the target Master via an FTP connection to the target Master.

*A **User** represents a single potential client of the NetLinx Master, while a **Group** represents a logical collection of users. Any properties possessed by groups (example: access rights, directory associations, etc.) are inherited by all the members of the group.*

Adding a new Group

1. Click the **Group Level** link (*from within the Security section of the Navigation frame*) to open the Manage Groups page.
2. Click the **New** button to be transferred to the Configure Group Properties page (FIG. 39).
3. From within the Group Security Details section, enter a unique name for the new group. The name must be a valid character string consisting of 4 - 20 alpha-numeric characters. **The word *administrator* cannot be used for a new group name since it already exists by default.**
4. Enable the security access rights you want to provide to the group. By default, all of these options are disabled.
5. From within the Group Directory Associations section, place a checkmark next to the directories (available on the target Master) to provide an authorized group with access rights to the selected directories. *If you select a group directory note that all lower groups in that tree will be selected.*
6. Click the **Update** button to save your changes to the target Master. If there are no errors within any of the page parameters, a "*Group added successfully*" is displayed at the top of the page.
7. Click the **Back** button to return to the Manage Groups page.

NOTE

Any security changes made to the Master from within the web browser are instantly reflected within a Terminal session without the need to reboot.
Security changes made to the Master from within a Terminal window are not reflected within the web browser until the Master is rebooted and the web browser connection is refreshed.

Modifying the properties of an existing Group

1. Click the **Group Level** link (*from within the Security section of the Navigation frame*) to open the Manage Groups page.

NOTE

The fields displayed when modifying groups are the same as those available when adding a new group, except for the Group Name field which is pre-populated.
*The Administrator's rights are not editable and its **Select** button is greyed-out.*

2. Click the **Select** button (*next to the selected Group name*) to open the Configure Group Properties page for the particular group.
3. From within the Group Security Details section, modify the previously configured access rights by either enabling or disabling any of the available checkboxes shown within the Configure Group Properties page.
4. From within the *Group Directory Associations* section, place or remove any checkmarks next to the available directories to modify an authorized group's directory access rights.
5. Click the **Update** button to save the changes to the target Master. If the modification of any of this page's parameters has no errors, a "*Group updated successfully*" notice is displayed at the top of the page.
6. Click the **Back** button to return to the Manage Groups page.

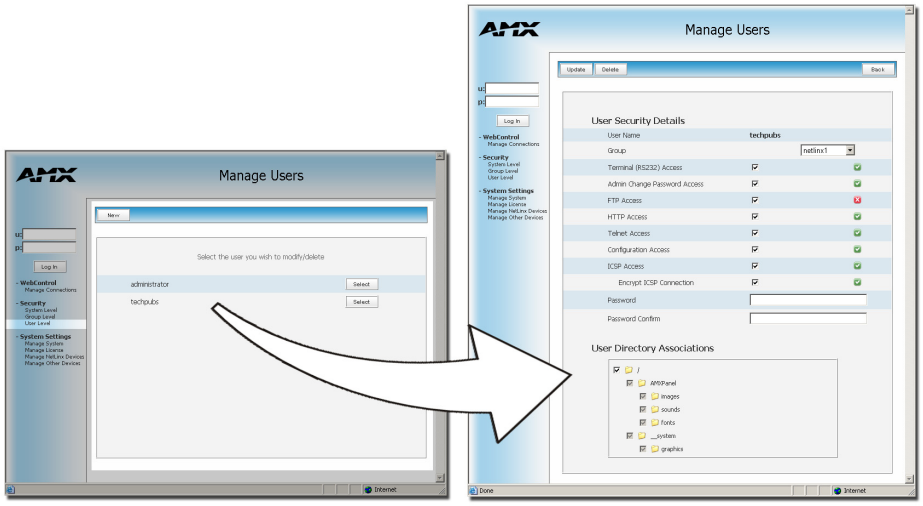
Deleting an existing Group

1. Click the **Group Level** link (*from within the Security section of the Navigation frame*) to open the *Manage Groups* page.
2. Press the **Select** button (*next to the selected Group name*) to open the *Configure Group Properties* page (FIG. 39) for the particular group.
3. Click the **Delete** button to remove the selected group and return to the Manage Groups page.
   - If you are not logged into the Master, you receive a reminder message: *"You must login before Security Settings can be changed"*.
   - Log into the Master and repeat the previous steps.
   - If the group is associated with several users, trying to delete the group might give an error notice. If this happens, change the group association of those specific users utilizing the old group and either

give them a new group or assign them (none) as a group. When returning to delete the desired group, the *"Group deleted successfully"* notice is displayed.

Security - User Level Security page

To access the User Level Security page (FIG. 40), click on the **User Level** link (*from within the Security section of the Navigation frame*). This page allows an authorized user to add a user account (FIG. 30) and then assign that user's current access rights.



Manage Users page

Configure User Properties page (adding a new user)

FIG. 40 User Level Security - Manage Users Security page

Manage Users Page	
Feature	**Description**
Manage Users page:	This page allows a user to either modify the rights for an existing user (*available from the displayed list*) or use the **New** button to access a secondary window to create a new user.
New	• Clicking this button allows an authorized user to add a new user and configure their settings through the *Configure User Properties* page.
Select	• Clicking this button opens the selection's corresponding Configure User Properties page. • This button is greyed-out if the current authorized user doesn't have the right to modify the rights for that user.

Configure User Properties Page	
Feature	**Description**
Configure User Properties:	This page allows an authorized user to configure the options for either a pre-existing or new user. Configuration on this page consists of both the options and directories to which the user is granted access.
Update	• This button submits the modified page (form) information back to the server. • If the user was successfully added after pressing the **Update** button; a status message of "User XYZ was successfully added" is displayed. • Always press the Update button after making any changes to this page.
Back	• This button returns the user to the Manage Users page.
Delete	• This button is only available when modifying/deleting an existing user.
User Security Details:	• This section provides the user with several rights which can either be enabled or disabled.
User Name	• A valid character string defining the name of the user (4 - 20 alpha-numeric characters). • If a user is selected from the Manage Users page, this row is populated with the name of the selected user. • The string is case sensitive and must be unique.
Group	• This drop-down list allows the user to associate a pre-defined series of Group rights to the current user profile. • Once the **Update** button is clicked, the group rights then are transferred to the user by placing a checkmark next to those rights which are available to the associated group. • Any properties possessed by groups (ex: access rights, directory associations, etc.) are inherited by users assigned to a particular group. • Unchecking a security option (which is available within the associated group) does not remove that right from the user. The only way to remove a group's available security right from a target user is to either NOT associate a group to a user or to alter the security rights of the group being associated.
Terminal (RS232USB) Access	• This selection enables or disables Terminal Security Access for the target user (through the USB connector).
Admin Change Password Access	• This selection enables or disables the user's right to change the administrator's user passwords. ***Note:*** Once the Administrator's password has been changed, the default password can no longer be used to gain access.
FTP Access	• This selection enables or disables FTP Access for the target user.
HTTP Access	• This selection enables or disables Web Server access for the target user.
Telnet Access	• This selection enables or disables Telnet Security access for the target group.
Configuration Access	• This selection enables or disables the ability of a user to alter the global Configuration settings. Example: IP, Reset URL, etc.

ICSP Access	• This selection grants this user ICSP access. • ICSP communication allows a user to connect to the target NetLinx Master via ICSP connection using any transport method (TCP/IP, UDP/IP, and RS-232/USB).

Configure Users Properties Page (Cont.)	
Feature	**Description**
User Security Details (Cont.):	
Encrypt ICSP Connection	• This selection enables encryption of the ICSP communication. • This checkbox is greyed-out until ICSP Access is enabled.
Password/Password Confirm	Enter a password for the new user. • A user password is a valid character string (4 - 20 alpha-numeric characters) that is used to supplement the username/ID in defining the potential client. **The string is case sensitive and must be unique.** • If this field is left blank (*during a user modification*) the current password is left unchanged. • If a new alpha-numeric string is entered during modification of the user, it becomes incorporated as the new password after pressing the **OK** button.
User/Directory Associations:	• Provides an authorized user with a view of current directories on the target Master that are available to the selected group. • A Directory Association is a path that defines the directories and files a particular user or group can access via the Web Server on the NetLinx Master. • The displayed folders are the directory pathnames present on the target Master.

Adding a new User

The information entered within this page can be used by Modero touch panels to verify and establish a secure connection by encrypting the data being transmitted between the Master and the panel. This information must be entered into the System Connection page of the panel's firmware.

1. Click the **User Level** link (*from within the Security section of the Navigation frame*) to open the *Manage Users* page.
2. Click the **New** button to be transferred to the *Configure User Properties* page (FIG. 40).
3. From within the User Security Details section, enter a unique name for the new group. The name must be a valid character string consisting of 4 - 20 alpha-numeric characters. **The usernames *administrator* and *NetLinx* cannot be used since they already exist.**
4. From within the Group drop-down list, choose from a list of pre-configured Groups and associate these rights to the new user.

NOTE

Any properties possessed by groups (ex: access rights, update rights, directory associations, etc.) are inherited by users assigned to that particular group. Unchecking a security option (which is available within the associated group) does not remove that right from the user. The only way to remove a group's available security right from a target user is to either NOT associate a group to a user or to alter the security rights of the group being associated.

5. Enable any additional security access rights you want to provide to the user. *By default, all of these options are disabled*.
6. Enter a user password within both the *Password* and *Password Confirm* fields. This password is a valid character string (4 - 20 alpha-numeric characters) that is used to supplement the username/ID in defining the potential client. The string is case sensitive.
7. From within the User Directory Associations section, place a checkmark next to the directories (on the target Master) to provide an authorized user with access rights to them.

8. Click the **Update** button to save the changes to the target Master. A "*User added successfully*" notice is displayed at the top of the page if the page parameters have no errors.
9. Click the **Back** button to return to the Manage User page.

Modifying the properties of an existing User

1. Click the **User Level** link (*from within the Security section of the Navigation frame*) to open the Manage Users page.

NOTE

The fields displayed when modifying users are the same as those available when adding a new user, except for the pre-populated User Name field.

2. Click the **Select** button next to the selected User's name to open the *Configure User Properties* page for the particular user (FIG. 41).
3. From within the User Security Details section, modify any previously configured access rights by either placing or removing a checkmark from within any of the available checkboxes (FIG. 41).

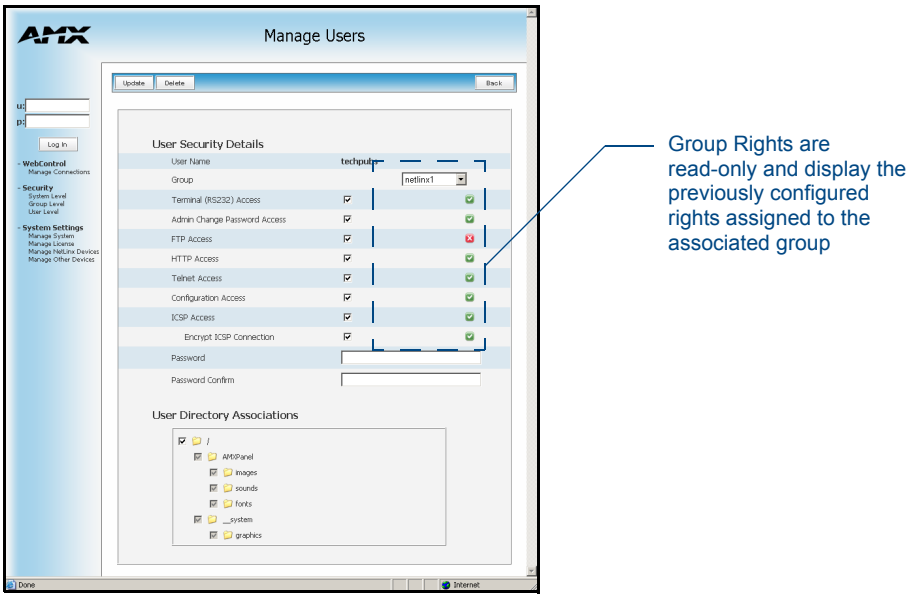


FIG. 41 User Level Security - Modifying a User's Security rights

4. From within the User Directory Associations section, place or remove any checkmarks next to the available directories to modify an authorized user's directory access rights. *Removing a checkmark from any folder prohibits that user from accessing any files contained therein via the Web Server.*
5. Enter the same password for the user into both the *Password* and *Password Confirm* fields, if you want to change the password. *Leaving this field blank retains the current or previous password.*
   - A user password is a valid character string (4 - 20 alpha-numeric characters) that is used to supplement the Username/ID in defining the potential client. The string is case sensitive.
6. Click the **Update** button to save your changes to the target Master. If there are no errors with the modification of any of this page's parameters, a "*User updated successfully*" is displayed at the top of the page.
7. Click the **Back** button to return to the *Manage Users* page.

Deleting an existing User

1. Click on the **User Level** link (*from within the Security section of the Navigation frame*) to open the *Manage Users* page.
2. Press the **Select** button next to the selected Username to open the *Configure User Properties* page (FIG. 40) for the particular user.

3. Click the **Delete** button to remove the selected user and return to the Manage Users page.

NOTE

*The **NetLinx** account can be deleted from the* Manage User *page.**The administrator account cannot be deleted, nor can it have its directory associations modified.***

System Settings

This section of the Navigation frame (FIG. 42) provides the ability to both manage existing and pending license keys, manage the active NetLinx system communication parameters, and configure/modify the SSL certificates on the target Master.

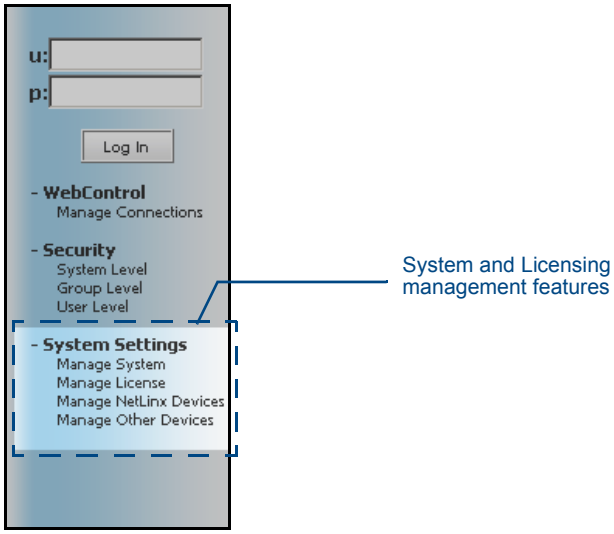


FIG. 42 System Settings - System an Licensing Management

System Settings - Manage System page

To view all of the available options within the right frame, it is recommended that you maximize the browser window.

To access this page (FIG. 43), click on the **Manage System** link (*from within the System Settings section of the Navigation frame*).

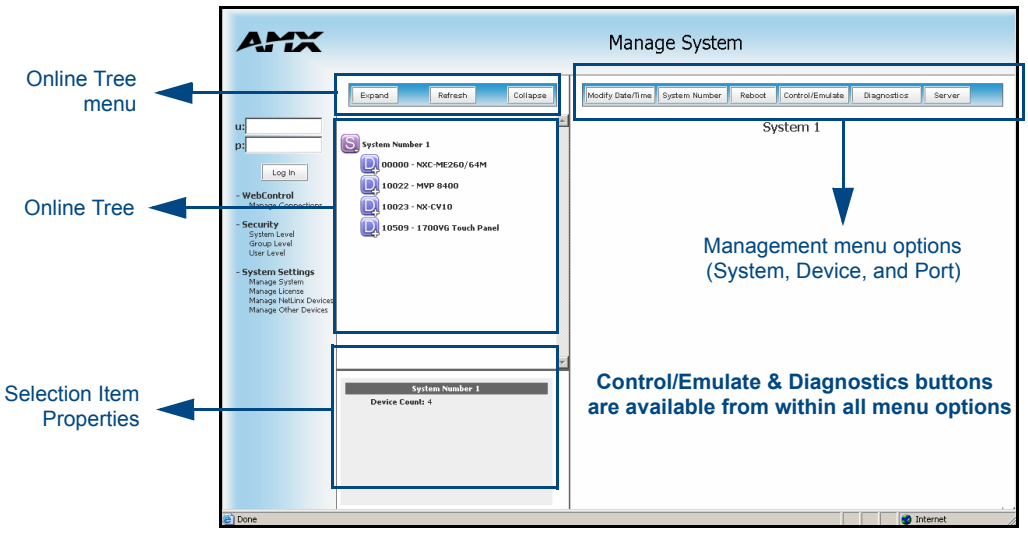


FIG. 43 System Settings - Manage System page

Manage System Page Components	
Feature	**Description**
Online Tree menu:	The Online Tree menu contains button options relating to the entries within the Online Tree. • **Expand** - Expands the selected level to expose any subfolders. • **Refresh** - Refreshes the contents of the Online Tree frame. • **Collapse** - Collapses the selected level to hide any subfolders.
Online Tree:	This frame displays a snapshot list of devices detected as currently online by the Master (*and the firmware version for each*). • By default, the Tree view begins fully collapsed. • The online devices are organized according to the System they belong to. • Double-click any System icon (FIG. 44) to display a list of devices that are currently online, within that System. • Double-clicking on any of the colored blocks causes that section of the Tree to expand. ***Note**: Sub-devices are hardware components contained within a parent device, which may require their own firmware. Refreshing/Rebooting the Master updates this Online Tree.*
Selection Item Properties:	This frame displays the properties of the last selected (clicked) item from the Online Tree. • **Commands** and **Strings** are not displayed, but a user is directed to the Control/Emulate window. • **Channel** properties show a list of all channels within the range available to the port. Clicking a channel takes the user to the Control/Emulate window where information such as the channel, System, Device, and Port are already pre-populated.

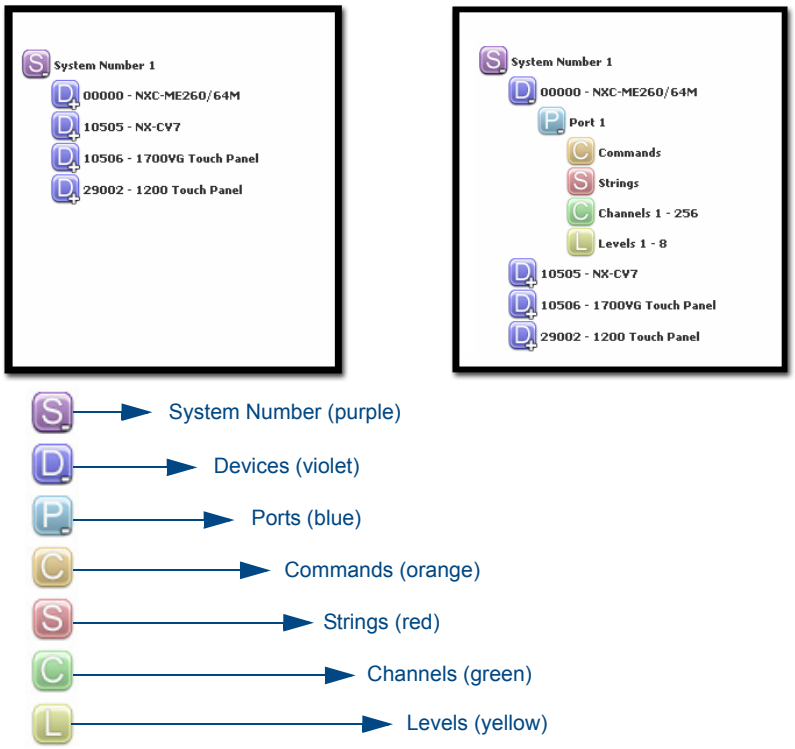


FIG. 44 System - Online Tree frame

Manage System Page Components (Cont.)	
Feature	**Description**
Management menu options:	These management buttons change depending on the source chosen from the Online Tree. • There are three menu groupings available: - System Menu (to configure Master properties). - Device Menu (to configure device specific properties). - Port Menu (to configure specific Port settings).
System menu buttons:	The selected system number is displayed below these menu buttons.
Modify Date/Time	• Allows a user to set the date and time on the target Master.
System Number	• Allows a user to change the current system number (value).
Reboot	• Allows a user to reboot the target Master.
Control/Emulate	• Allows a user to both control and emulate devices on a target Master. • This is done by allowing the user to control a device's channels, levels, and send both send commands and strings to the target device. • This button is available from within all Management menus.
Diagnostics	• Allows a user to watch the system activity to/from a selected device. • This button is available from within all Management menus.
Server	• Allows a user to both change the port numbers (*used for various Web services*) and configure the SSL settings used on the Master.
Device menu buttons:	The selected system number: device number are displayed below these menu buttons.
Network Settings	• Allows a user to configure the LAN IP/DNS settings.
URL List	• Allows a user to setup the URL List for the specified device. • Not all devices allow this functionality.
Device Number	• Allows a user to change the device number of a selected device.
Control/Emulate	• Allows a user to both control and emulate devices on a target Master. • This is done by allowing the user to control a device's channels, levels, and send both send commands and strings to the target device. • This button is available from within all Management menus.
Log	• Allows a user to view the log for the selected device. • Not all devices allow this functionality.
Diagnostics	• Allows a user to watch the system activity to/from a selected device. • This button is available from within all Management menus.
Port menu buttons:	The selected system number:device & number:port number are displayed below these menu buttons.
Control/Emulate	• Allows a user to both control and emulate devices on a target Master. • This button is available from within all Management menus.
Diagnostics	• Allows a user to watch the system activity to/from a selected device. • This button is available from within all Management menus.

Manage System - System Menu Buttons

These buttons appear (on the right) when a user clicks on the purple System icon from within the Online Tree. The selected system number is displayed below these System menu buttons.

System Menu - Modifying the Date/Time

1. Click the **Manage System** link (*from within the System Settings section of the Navigation frame*).
2. Click on the purple System icon from within the Online Tree to open the System menu buttons within the right frame.
3. Click the **Modify Date/Time** button to open the Modify System Date/Time dialog (FIG. 45). This dialog shows the current Date and Time settings for the target Master.

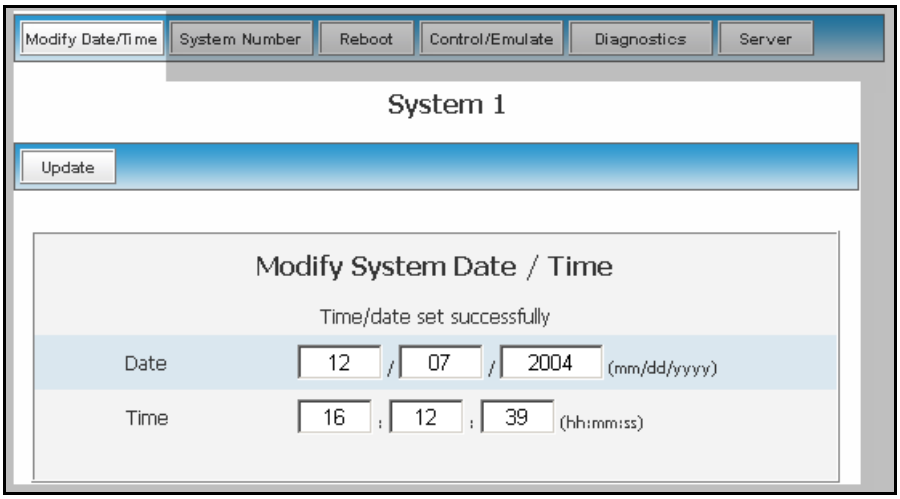


FIG. 45 Modify System/Date dialog

4. Alter any of these values by selecting the appropriate field and entering a new numeric value.
   - Highlighting any of the *Date* fields displays a small popup calendar window which assists with selecting a new date.
   - Navigate through the calendar and click on a new date, which is then reflected back within the *Modify System Date/Time* dialog.
   - Any of the *Time* fields can be modified by either manually entering the new values or highlighting a field and using the arrow keys.
5. Click the **Update** button to save these settings to the target Master. The message "*Time/date set successfully*" is displayed if the update process had no problems.

System Menu - Changing the System Number

1. Click the **Manage System** link (*from within the System Settings section of the Navigation frame*).
2. Click on the purple System icon from within the Online Tree to open the System menu buttons within the right frame.
3. Click the **System Number** button to open the Change System Number dialog (FIG. 46). This dialog shows the current system number (read-only) on the target Master.
   - The current system number is also shown just below the System menu buttons.

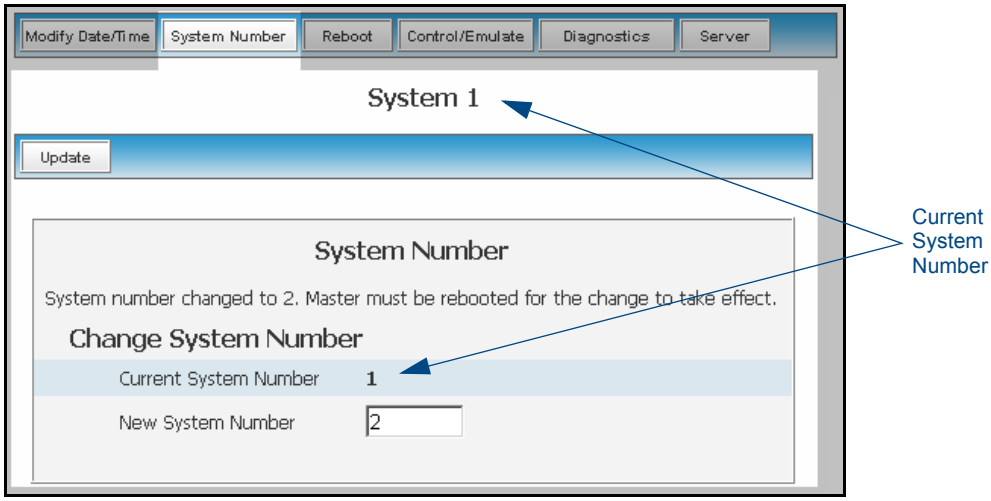


FIG. 46 Change System Number dialog

4. Enter a new numeric value into the *New System Number* field.
5. Click the **Update** button to save this new value to the system on the target Master. The following message, "*System number changed to X. Master must be rebooted for the change to take effect*", reminds the user the Master must first be rebooted before the new settings take effect. ***Once the Master is rebooted, the IP Address must be re-entered and an authorized user must re-establish communication with the target Master.***

System Menu - Rebooting the Master

1. Click the **Manage System** link (*from within the System Settings section of the Navigation frame*).
2. Click on the purple System icon from within the Online Tree to open the System menu buttons within the right frame.
3. Click the **Reboot** button to remotely reboot the target Master. No dialog appears while using this button. The Online Tree then reads *"Rebooting...."*. After a few seconds, the Online Tree refreshes with the current system information (showing the newly updated system number).
   - If the Online Tree contents do not refresh within a few minutes, press the browser's **Refresh** button and reconnect to the Master.

System Menu - Controlling/Emulating Devices on the Master

This button allows a user to either Control a device or Emulate a device. This is done by controlling a device's channels, levels, and sending both send commands and strings to the target device.

NOTE

The Control/Emulate and Diagnostics buttons are common to all menus. These fields are populated depending upon the items selected from the Online Tree (left frame). For example, when navigating down to a specific channel on a device, the Control/Emulate page then populates the D:P:S and Channel Code fields.

1. Click the **Manage System** link (*from within the System Settings section of the Navigation frame*).
2. Clicking on any of the Online Tree items opens menu items with the Control/Emulate button option available.
3. Click the **Control/Emulate** button to open the Control/Emulate dialog (FIG. 47).
4. Click the **Update Status** button to query the Master for the status of the currently entered level and channel.

NOTE

The System Number, Device Number, and Port Number value fields are read-only (disabled) if this window was opened by from a selection of an Online Tree item. By default, these fields are otherwise editable.

5. Select either the **Control** or **Emulate** option.

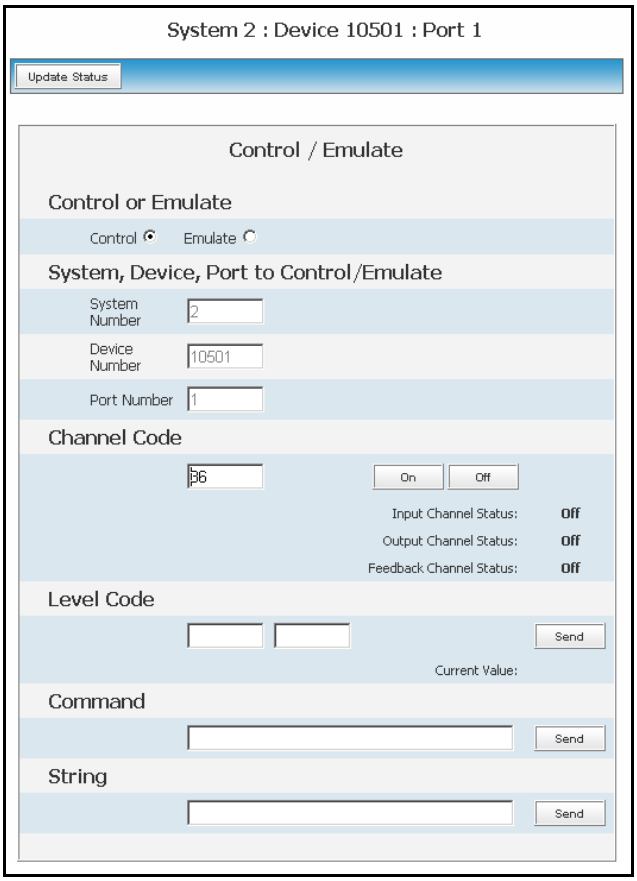


FIG. 47 Control/Emulate dialog

- To **Control** a device means that the program generates messages which appear to a specified device to have come from the Master. The options in this frame specify the <D:P:S> combination for the device to be controlled.
- To **Emulate** a device means that the program generates messages which appear to the Master to have come from a specified <D:P:S> combination (real or fictitious). The options in this frame specify the <D:P:S> combination for the device to be emulated.
  - Selecting this option adds a **Push** button with the Channel Code section of this page.

6. Enter a System Number, Device Number, and Port Number into the appropriate fields. These values correspond to the device to be controlled, whether real or fictitious.
   - The Device, Port, and System value ranges are **1 - 65535**.
7. Within the Channel Code section, enter a valid Channel number to emulate Channel messages (i.e., Push/Release, CHON, and CHOFF) for the specified <D:P:S>.
   - The Channel number range is **1 - 65535**.
8. Select the **On** or **Off** buttons to Emulate Channel ON (CHON) and Channel OFF (CHOFF) messages for the specified <D:P:S>.
9. Select the **Push** button to Emulate a push/release on the channel specified. You can click and hold down the **Push** button to see how the device/Master responds to the push message.
10. Within the Level Code section, enter a valid Level number and Level data value for the specified <D:P:S> and press the **Send** button to transmit this data.
    - The Level number range is **1 - 65535**.
    - The list below contains the valid Level data types and their ranges:

Valid Level Data Types and Ranges		
	Minimum Value	Maximum Value
CHAR	0	255
INTEGER	0	65535
SINTEGER	-32768	32767
LONG	0	429497295
SLONG	-2147483648	2147483647
FLOAT	-3.402823466e+38	3.402823466e+38

11. Within the *Command* and *String* fields, you can enter any number of messages that can be sent as either a String or Command.
12. To Emulate sending a String or Command, type a String or Command within the corresponding field and press the **Send** button to transmit this data.
    - When entering a send command (in the context of this dialog) do not include the "send c" or "send_command" in the statement - only type what would normally occur within the quotes, but don't include the quotes either. For example to send the "CALIBRATE" send command, simply type CALIBRATE (no quotes) rather than SEND_COMMAND <dev> "CALIBRATE".
    - String Expressions start and end with double quotes (**" "**). Double quotes are not escaped; instead, they are embedded within single quotes. String expressions may contain string literals, decimal numbers, ASCII characters and hexadecimal numbers (prepended with a $), and are comma-delimited.
    - String Literals start and end with single quotes (**'**). To escape a single quote, use **'''** (three single quotes).

Manage System - Diagnostics

This page allows an authorized user to setup and monitor diagnostic messages coming from and going to devices available on the Online Tree. This dialog also allows the user to watch the ICSP commands being sent to/from a device. There are several different types of asynchronous notifications that can be selected for a device:port:system (D:P:S) combination. Each notification type is represented by a column in the table. All messages are displayed in the Notifications tab of the Output Display window within NetLinx Studio v 2.4.

1. Click the **Manage System** link (*from within the System Settings section of the Navigation frame*).
2. Clicking on any of the Online Tree items opens menu items with the Diagnostics button option available.
3. Click the **Diagnostics** button to open the Diagnostics dialog (FIG. 48).
4. Use the **Refresh Interval** drop-down to select from the following values: 2 seconds, 5 seconds, or 10 seconds. This refresh interval allows you to select how often the messages are updated.

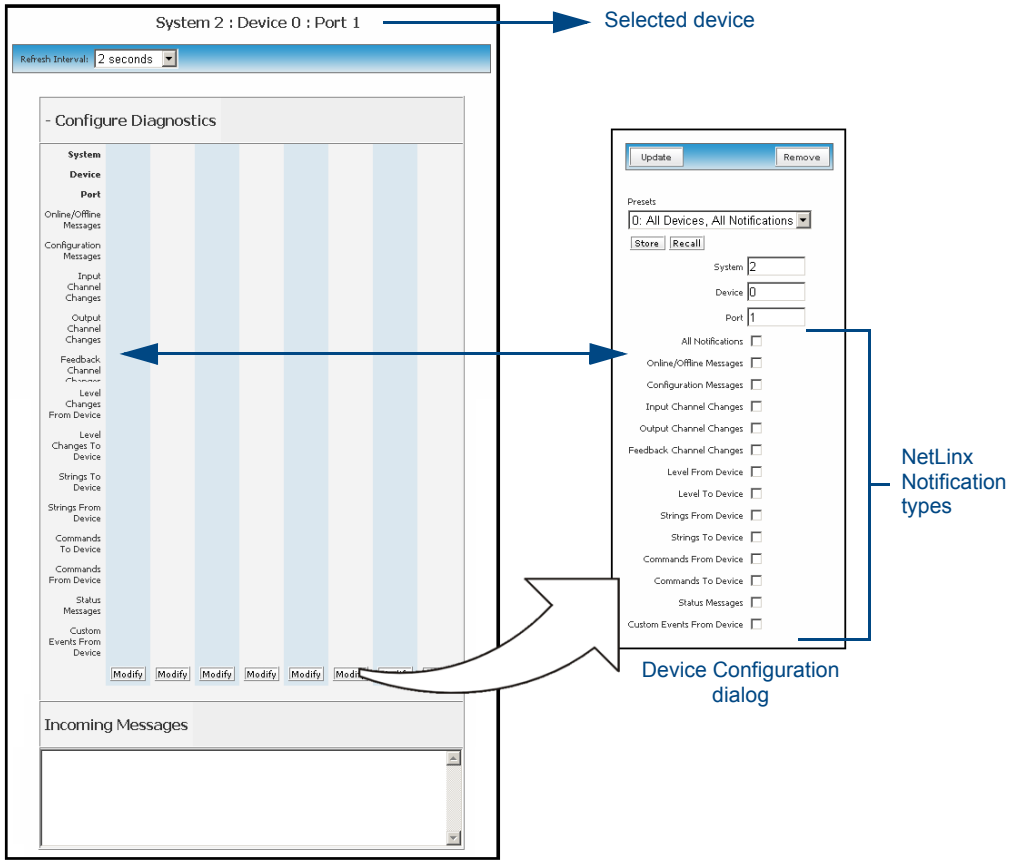


FIG. 48 Diagnostics dialog (showing modify popup)

Setting up and removing a Diagnostic Filter

1. Setup a diagnostic filter by scrolling down the page and clicking the **Modify** button below the first empty column. This action opens the Device Configuration dialog as a secondary popup window.

NOTE

Up to 8 concurrent diagnostic filter slots can be simultaneously active using any eight of the 10 available user-configurable Presets available through the Device Configuration dialog.

2. Configure a diagnostic filter using the parameters available within the Diagnostic Configuration dialog.
   - The **Diagnostic Configuration** dialog allows you to select both the notifications you wish to receive and the target devices (within the Online Tree) for these notifications. Several different types of asynchronous notifications can be selected for a device:port:system (D:P:S) combination. Each notification type is represented by a column in the table. All messages are displayed in the Notifications tab of the Output Display window within NetLinx Studio v 2.4.
3. A user can choose to either store these selections to a profile or recall a previously stored profile configuration by either:
   - Select an open Preset number entry from within **Presets** drop-down list. Make all desired notification selection and press the **Store** button. Pressing this button opens a popup field labeled *Explorer User Prompt - Preset Name?*, intended for entering the name associated with this new Preset.
     - Press **OK** to return to the previous *Device Configuration* popup dialog.
     - Click **Cancel** to exit this popup and return to the previous dialog box without making any changes.

- Press the down arrow (*adjacent to the Preset drop-down list*) to display a listing of all currently available Presets. Select a previously configured Preset and press the **Recall** button to populate all available fields and radio buttons with the selections associated with this chosen Preset.
  - This preset mechanism is done via cookies so it does not persist across multiple browsers/ computers.

4. Once all modifications/selections within this dialog have been made, press the **Update** button to save the changes and return to the Diagnostics dialog.

Diagnostic Configuration Dialog	
Feature	**Description**
Update:	Click this button once you have completed setting up your filter. The popup then closes and returns you to the Diagnostics window. • Watch the bottom Incoming Message pane for messages to begin coming in from the target device(s).
Remove:	Click this button to remove a selected Preset from being available within the Presets drop-down list.
Presets:	This list of up to 10 presets comes defaulted with Preset 0: All Devices, All Notifications • **Store**: Save the current notification selections to a Preset profile. Pressing this button opens a popup field labeled *Explorer User Prompt - Preset Name?* where you enter the name associated with this new Preset. - Click **OK** to save both the Preset parameters and name, and then return to the Diagnostic Configuration Dialog. - Click **Cancel** to exit this popup and return to the previous dialog without making any changes. • **Recall**: Allows a user to recall a previously existing Preset. This action then populates every field and radio button with the selections associated with the chosen Preset. - This preset mechanism is done via cookies so that it does not persist across multiple browsers/computers. Note: A Preset MUST be Recalled before clicking the Update button. If you do not press this button, none of the fields or checkboxes are modified or selected. In essence, all options become disabled. Note: The All Devices entry cannot be removed. Note: The only way to modify the information within a Diagnostic filter is to remove the assigned Preset, change the information, and assign a new Preset. Refer to step 5 of this section for more information.
System/Device/Port:	Device, Port, System: Use these fields to enter a device:port:system (D:P:S) combination for the device that you want to enable notifications for. • The specified device then appear in the Device field within the Diagnostic Configuration Dialog. • A value of **0** for any option gives you all of the systems, devices, or ports. This dialog also allows you to store/recall presets.

Diagnostic Configuration Dialog (Cont.)	
Feature	**Description**
NetLinx Notification Types:	***All Notifications***: Enables (selects) every notification field. • ***Online/Offline Messages***: Generates a message with a change in the target device's online/offline status. • ***Configuration Messages***: Generates a message with a change in the target device's configuration. • ***Input Channel Changes***: Generates a message with an input channel change (i.e. Push/Release) in the target device. • ***Output Channel Changes***: Generates a message with an output channel change (i.e. CHON/CHOFF) in the target device. • ***Feedback Channel Changes***: Generates a message with a feedback channel change in the target device. • ***Level Changes From Device***: Generates a message with a level channel change from the target device. • ***Level Changes To Device***: Generates a message with a level channel change to the target device. • ***String From Device***: Generates a message with a string from the target device. • ***String To Device***: Generates a message with a string sent to the target device. • ***Command From Device***: Generates a message with a command from the target device. • ***Command To Device***: Generates a message with a command to the target device. • ***Status Messages***: Generates a message with a change in the target device's status. • ***Custom Events From Device***: Generates a message with a custom event occurring from the target device.

5. Remove a diagnostic filter by clicking the **Modify** button below it (from the Diagnostics dialog), then pressing the **Remove** button to delete this filter from the Diagnostics dialog.
   - Once a Preset is assigned to a specific Diagnostic filter "slot" (**up to 8**), its *System*:*Device*:*Port* fields are greyed-out, and can't be modified unless the Preset in that slot is removed and replicated with new information within these fields.
   - To modify a Diagnostic filter's information (such as System/Device/Port):
     - Navigate to an empty Diagnostic filter slot and click the **Modify** button below the filter.
     - Select a previously unused Preset and store it with a new name.
     - Click the **Remove** button to remove this duplicate Preset from the specific filter slot.
     - Re-open the empty slot by clicking the **Modify** button, select the duplicated Preset and click **Recall**.
     - Change the necessary information (such as the System/Device/Port), then save it as the original Preset name, and click the **Update** button.
6. Use the *Incoming Message* field to view all the internal system diagnostic messages that are generated by a NetLinx Master controller. This message field is a text box, where the text within it may be selected and then copied or pasted for storage.

Setting the Master's Port Configurations

Manage System - Server

This page allows a user to both change the port numbers (*used for various Web services*) and configure the SSL settings used on the Master by bringing up a submenu of options such as:

Server Submenu Options	
Feature	**Description**
Port Settings:	Allows a user to modify the server settings; specifically those port assignments associated with individual services. • All items can be either enabled/disabled via the adjacent checkbox. • The port number values can also be modified (except the FTP port). • The default port for each service is listed to the right.
Create SSL Certificate:	Takes the authorized user to the Server Certificate page to create a self-generated SSL certificate. • This dialog provides the ability to display an installed certificate, create a certificate request, self-generate, and regenerate SSL Server Certificates.
Export SSL Certificate Request:	Takes the user to the Server Certificate page to view a previously created certificate. • An authorized user can also copy the raw text from a generated Certificate request into their clipboard and then send it to the CA.
Import SSL Certificate:	Takes the user to the Import Certificate page where they can import and paste the raw text from a CA issued Certificate.

1. Click on the **Manage System** link (*from within the System Settings section of the Navigation frame*).
2. Click on the purple System icon from within the Online Tree to open the System menu buttons within the right frame.
3. Click the **Server** button to open the Server dialog and its associated submenu options (FIG. 49).

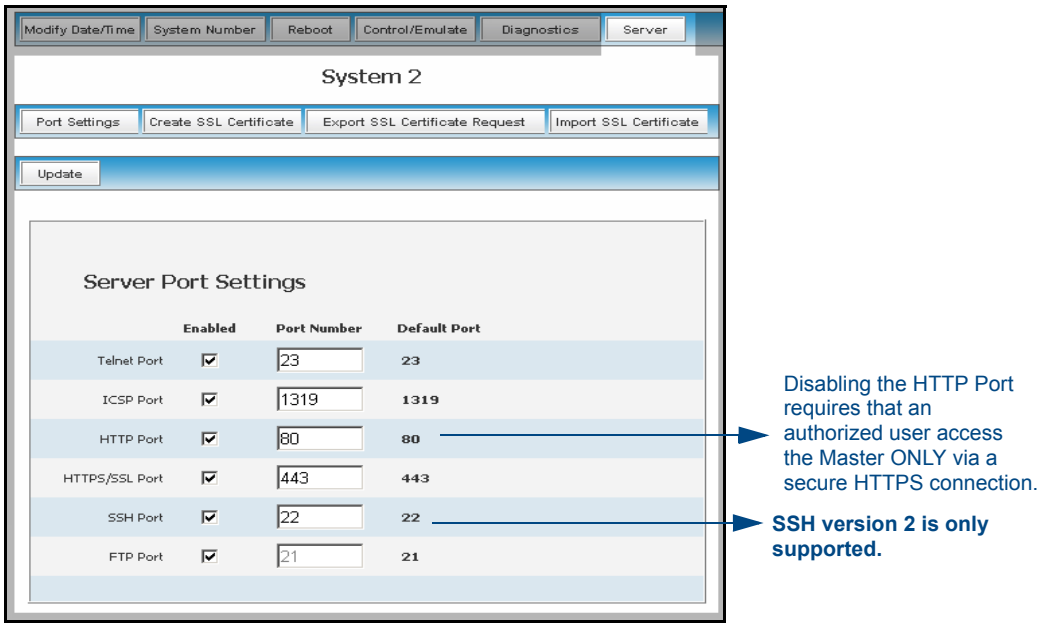


FIG. 49 Server dialog and associated submenu options

- The following graphic illustrates the Ports which can be enabled for validation using a valid username and password, as well as what method of communication is used with each.

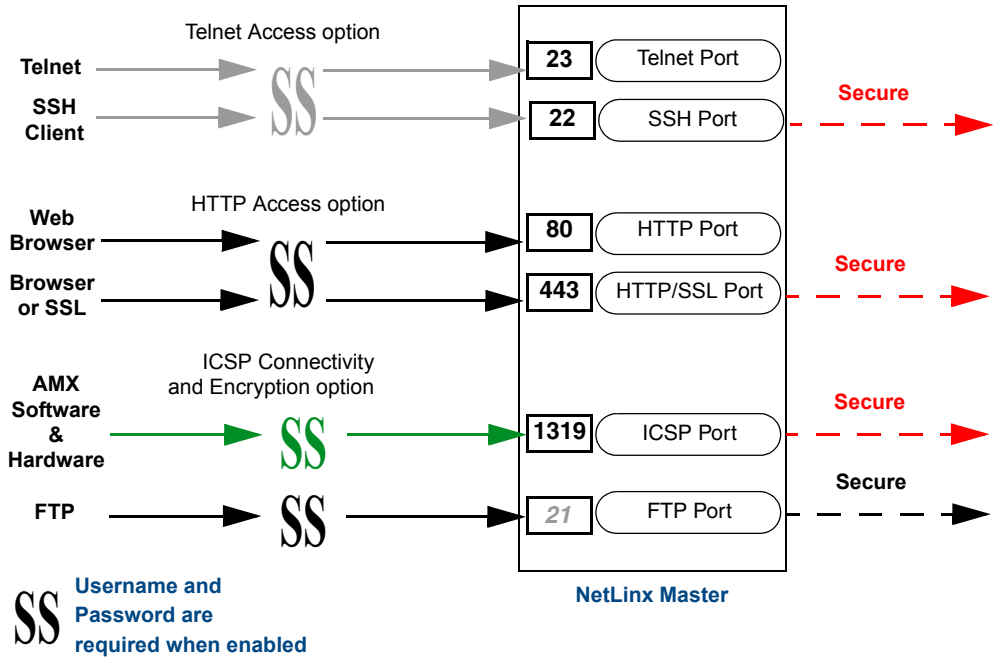


FIG. 50 Port Communication Settings

Modifying the Server Port Settings

1. From within the Server submenu, press the **Port Settings** button to open the Server Port Settings dialog seen above in FIG. 49.
2. Uncheck any services (and corresponding ports) to disable their functionality.
3. Modify any preset service port value by first enabling that service with a checkmark within the **Enabled** checkbox and then entering a value within the *Port Number* field.

Server Port Settings	
Feature	**Description**
Telnet Port:	The port value used for Telnet communication to the target Master. • The default port value is 23. • Enabling this feature allows future communication with the Master via a separate Telnet application (such as HyperTerminal). • Refer to the *NetLinx Security with a Terminal Connection* section for more information on the related procedures.
ICSP Port:	The port value used for ICSP data communication among the different AMX software and hardware products. • The default port value is 1319. • This type of communication is used by the various AMX product for communication amongst themselves. Some examples would be: NetLinx Studio communicating with a Master (for firmware or file information updates) and TPDesign4 communicating with a touch panel (for panel page and firmware updates). ***Note**: To further ensure a secure connection within this type of communication, a user can enable the Require Encryption option which requires additional processor cycles. Enabling of the encryption feature is determined by the user.*

Server Port Settings (Cont.)	
Feature	**Description**
HTTP Port:	The port value used for unsecure HTTP Internet communication between the web browser's UI and the target Master. • The default port value is 80. • By default, the Master does not have security enabled and must use **http://** in the *Address* field for communication. • One method of adding security to HTTP communication would be to change the port value. - If the port value is changed, any consecutive session to the target Master has to add the port value at the end of the address (within the *Address* field). For example, if the port were changed to 99, the new address information would be: **http://192.192.192.192:99**. • By disabling this port, the administrator (or other authorized user) can require that any consecutive sessions between the UI and the target Master are done over a more secure HTTPS connection.
HTTPS/SSL Port:	The port value used by web browser to securely communicate between the web server UI and the target Master. This port is also used to simultaneously encrypt this data using the SSL certificate information on the Master as a key. • The default port value is 443. • This port is used not only used to communicate securely between the browser (using the web server UI) and the Master using HTTPS but also provide a port for use by the SSL encryption key (embedded into the certificate). • Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, HTTPS is designed to transmit individual messages securely. Therefore both HTTPS and SSL can be seen as complementary and are configured to communicate over the same port on the Master. • These two methods of security and encryption are occurring simultaneously over this port as data is being transferred. • Another method of adding security to HTTPS communication would be to change the port value. - If the port value is changed, any consecutive session to the target Master has to add the port value at the end of the address (within the *Address* field). For example, if the port were changed to 99, the new address information would be: **http://192.192.192.192:99**.
SSH Port:	The port value used for secure Telnet communication. Note: SSH version 2 is only supported. • The default port value is 22. • A separate secure SSH Client would handle communication over this port. • When using a secure SSH login, the entire login session (including the transmission of passwords) is encrypted; therefore it is secure method of preventing an external user from collecting passwords. Note: If this port's value is changed, make sure to use it within the Address field of the SSH Client application.
FTP Port:	The port value used for FTP communication. ***This port can be disabled/ enabled but the value can not be changed.*** • The default port value is 21. • When an application such as TPDesign uploads information to the target Master via an FTP connection; it is this port which is used by default.

4. Once an authorized user has modified any of the server port settings, press the **Update** button to save these changes to the Master. Once these changes are saved, the following message appears: *"Unit must be rebooted for the change to take effect"*.
5. Click the **Reboot** button (*from the top of the page*) to remotely reboot the target Master. No dialog appears while using this button. The Online Tree then reads *"Rebooting...."*. After a few seconds, the

Online Tree refreshes with the current system information and showing the newly updated system number.

- If the Online Tree contents do not refresh within a few minutes, press the browser's **Refresh** button and reconnect to the Master.

SSL Server Certificate Creation Procedures

Initially, a NetLinx Master is not equipped with any installed certificates. **In order to prepare a Master for later use with CA** (*officially issued*) **server certificates**, it is necessary to:

- **First create a self-generated certificate** which is automatically installed onto the Master.
- **Secondly, enable the SSL feature** from the Enable Security page. Enabling SSL security after the certificate has been self-generated insures that the target Master is utilizing a secure connection during the process of importing a CA server certificate over the web.

NOTE

A self-generated certificate has lower security than an external CA generated certificate.

A certificate consists of two different Keys:

- **Master Key** is generated by the Master and is incorporated into the text string sent to the CA during a certificate request. It is unique to a particular request made on a specific Master.
- **Public Key** is part of the text string that is returned from the CA as part of an approved SSL Server Certificate. This public key is based off the submitted Master key from the original request.
- Regenerating a previously requested and installed certificate invalidates that certificate because the Master Key has been changed.

1. Navigate to the Server Certificate page by clicking **System Settings** > **Manage System > Server > Create SSL Certificate** to open the Server Certificate page (FIG. 51).

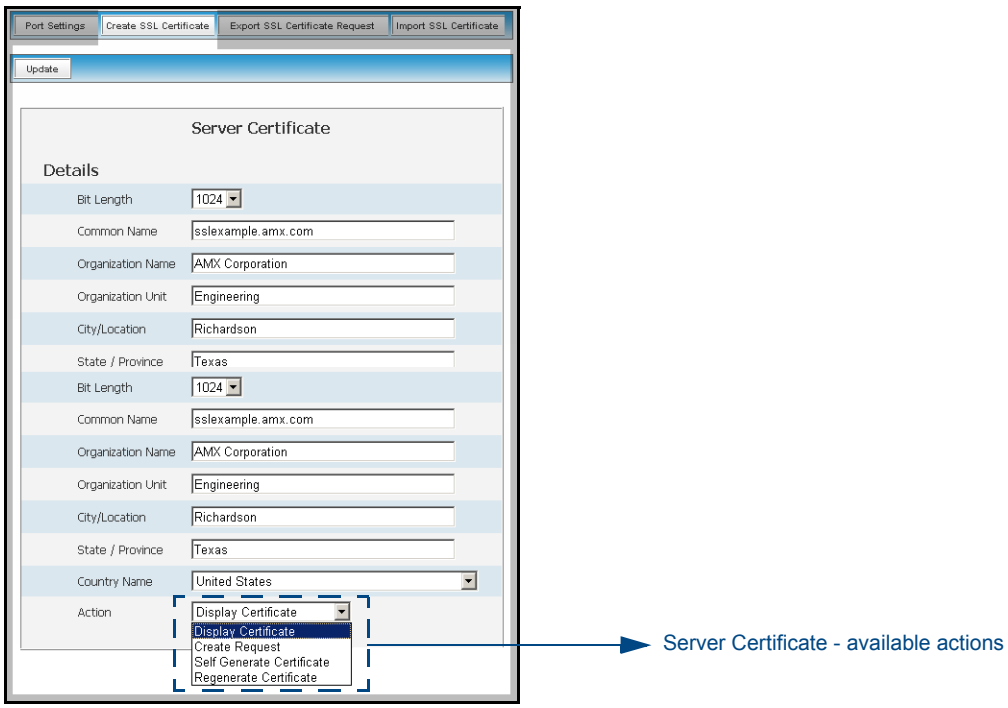


FIG. 51 Create an SSL Certificate dialog

This page allows an authorized user to display an installed certificate, create a certificate request, self-generate, and regenerate SSL Server Certificates.

Server Certificate Entries	
Feature	**Description**
Server Certificate Field Information:	
Update	Updates the target Master with the information entered on this page. • This process can take a few minutes.
Bit Length	Provides a drop-down selection with three available public key lengths: 512, 1024, and 2048. • Longer key lengths result in increased certificate processing times. • A longer key length results in more secure certificates.
Common Name	The Common Name of the certificate MUST be the URL Domain Name used. • Example: If the address used is www.amxuser.com, that must be the Common name and format used. • The Common Name can not be an IP Address. • If the server is internal, the Netbios name must be used. • For every website using SSL that has a distinct DNS name, there must be a certificate installed. Each website (external or Internet) for SSL MUST also have a distinct IP Address.
Organization Name	Name of your business or organization. This is an alpha-numeric string (1 - 50 characters in length).
Organizational Unit	Name of the department using the certificate. This is an alpha-numeric string (1 - 50 characters in length).
City/Location	Name of the city where the certificate is used. This is an alpha-numeric string (1 - 50 characters in length).
State/Province	Name of the state or province where the certificate is used. This is an alpha-numeric string (1 - 50 characters in length).
Country Name	Provides a drop-down selection with a listing of currently selectable countries.
Action	Provides a drop-down selection with a listing of available certificate options: • Display Certificate - Populates the Server Certificate fields with the information from the certificate currently installed on the Master. ***This action is used only to display the information contained in the certificate on the target Master.*** • Create Request - Takes the information entered into the previous fields and formats the certificate so it can be exported to the external Certificate Authority (CA) for later receipt of an SSL Certificate. ***This action is used to request a certificate from an external source.*** • Self Generate Certificate - Takes the information entered into the previous fields and generates its own SSL Certificate. ***This action is used when no previous certificate has been installed on the target Master, or a self-signed certificate is desired.*** • Regenerate Certificate - Takes the information entered into the previous fields and regenerates an SSL Certificate. This action changes the Master Key. ***This method of certificate generation is used to modify or recreate a previously existing certificate already on the Master.***

Server - Display SSL Server Certificate Information

1. Navigate to the Server Certificate page by clicking **System Settings** > **Manage System > Server > Create SSL Certificate** to open the Server Certificate page.

By default, the Display Certificate Action is selected and these fields are populated with information from an installed certificate. If the Master does not have a previously installed certificate, these fields are blank.

2. Click the down arrow from the *Action* field to open a drop-down listing of available certificate generation options.
3. Choose **Display Certificate** from the drop-down list.
4. Click **Update** to accept the action and populate the fields with the certificate information presently on the Master.

Server - Creating a self-generated SSL Certificate

1. Navigate to the Server Certificate page by clicking **System Settings** > **Manage System > Server > Create SSL Certificate** to open the Server Certificate page.
2. Click the down arrow from the *Bit length* field to open a drop-down listing of available public key lengths.
   - The three available public key lengths are: 512, 1024, and 2048. Higher selected key lengths result in increased certificate processing times. A longer key length results in more secure certificates.
3. Enter the used Domain Name into the *Common Name* field.
   - Example: If the address being used is www.amxuser.com, that must be the Common name and format used in the *Common Name* field. This string provides a unique name for the desired user.
   - This domain name must be associated to a resolvable URL Address when creating a request for a purchased certificate. The address does not need to be resolvable when obtaining a free certificate.
4. Enter the name of the business or organization into the *Organization Name* field. This is an alpha-numeric string, 1 - 50 characters in length.
5. Enter the name of the department using the certificate into the *Organizational Unit* field. This is an alpha-numeric string, 1 - 50 characters in length.
6. Enter the name of the city where the certificate resides into the *City/Location* field. This is an alpha-numeric string, 1 - 50 characters in length.
7. Enter the name of the state or province where the certificate resides into the *State/Province* field. This is an alpha-numeric string, 1 - 50 characters in length. **The state/province name must be fully spelled out.**
8. Click the down arrow from the *Country Name* field to open a drop-down listing of listing of currently selectable countries.
9. Click the down arrow from the *Action* field to open a drop-down listing of available certificate generation options.
10. Choose **Self Generate Certificate** from the drop-down list. *When this request is submitted, the certificate is generated and installed into the Master in one step.*
11. Click **Update** to save the new encrypted certificate information to the Master.

*ONLY use the Regenerate certificate option when you have Self Generated your own certificate. **DO NOT** regenerate an external CA-generated certificate.*

Server - Regenerating an SSL Server Certificate Request

1. Navigate to the Server Certificate page by clicking **System Settings** > **Manage System > Server > Create SSL Certificate** to open the Server Certificate page.

NOTE

This method of certificate generation is used to modify or recreate a previously existing certificate already on the Master.
By default, if a certificate is already present on the target Master, the Display Certificate Action is selected and these fields are populated with information.
Example: if the company has moved from Dallas to Houston, all of the information is reentered exactly except for the City.

2. Enter any new or changed information into its respective field.
3. Click the down arrow from the *Action* field to open a drop-down listing of available certificate generation options.
4. Choose **Regenerate Certificate** from the drop-down list.

NOTE

When this request is submitted, the certificate is generated and installed into the Master in one step.

5. Click **OK** to save the newly modified certificate information to the Master or click **Cancel** to void any changes made within this page and exit without making changes to the target Master.
6. **Before exiting the Master and beginning another session**:
   - Verify that all users have been assigned the correct rights, and are using the correct passwords.
   - In the Enable Security window of the Security tab, verify that the Master Security and HTTP Access are enabled. Enabling HTTP Access prompts users to enter pre-configured usernames and passwords.

Server - Creating a Request for an SSL Certificate

1. Navigate to the Server Certificate page by clicking **System Settings** > **Manage System > Server > Create SSL Certificate** to open the Server Certificate page.
2. Click the down arrow from the *Bit length* field to open a drop-down listing of available public key lengths.
   - The three available public key lengths are 512, 1024, and 2048. Higher selected key lengths result in increased certificate processing times. A longer key length results in more secure certificates.
3. Enter the used Domain Name into the *Common Name* field.
   - Example: If the address being used is www.amxuser.com, that must be the Common name and format used in the *Common Name* field. This string provides a unique name for the desired user.
   - This domain name must be associated to a resolvable URL Address when creating a request for a purchased certificate. The address does not need to be resolvable when obtaining a free certificate.
4. Enter the name of the business or organization into the *Organization Name* field. This is an alpha-numeric string, 1 - 50 characters in length.
5. Enter the name of the department using the certificate into the *Organizational Unit* field. This is an alpha-numeric string, 1 - 50 characters in length.
6. Enter the name of the city where the certificate resides into the *City/Location* field. This is an alpha-numeric string, 1 - 50 characters in length.
7. Enter the name of the state or province where the certificate resides into the *State/Province* field. This is an alpha-numeric string, 1 - 50 characters in length.
   The state/province name must be fully spelled out.
8. Click the down arrow from the *Country Name* field to open a drop-down listing of listing of currently selectable countries.
9. Click the down arrow from the *Action* field to open a drop-down listing of available certificate generation options.

10. Choose **Create Request** from the drop-down list.
11. Click the **Update** button to accept the information entered into the above fields and generate a certificate file. Refer to the*Server - Exporting an SSL Certificate Request* section on page 68.
    - This refreshed the Server Certificate page and if the certificate request was successful, displays a *"Certified request generated"* message.
12. Follow the exporting and importing an SSL certificate procedures outlined within the following section.

Common Steps for Requesting a Certificate from a CA

Once the request has begun, a user has the choice to either remain using their self-generated SSL certificate or obtain a CA created certificate by exporting their request for the certificate and then, once received, import the returned certificate information onto the Master.

Communicating with the CA

A certificate is a cryptographically signed object that associates a public key and an identity. Certificates also include other information in extensions such as permissions and comments. A "**CA**" is short for Certification Authority and is an internal entity or trusted third party that issues, signs, revokes, and manages these digital certificates.

1. Navigate to the Web Server Certificate HTML page on your CA's web site.
    - A Web Server certificate allows you to authenticate through a Web browser via SSL In order to successfully verify other certificates it is also necessary to import the CA key into the Web Server. Refer to the*Server - Creating a Request for an SSL Certificate* section on page 67.
    - This is done as part of the process of receiving your Web Server certificate.
    - Only a user with administrator privileges can request a server certificate.
2. Enter in the company information, such as: name, e-mail, address, state, and country.
3. Agree to any licensing agreements and continue to the next part of the registration process.
4. Enter the name of the server being used (this is the Master).
    - The server name is the name as it shows up in the URL of the Master you are securing with this server certificate. For example, if the URL of the Master is **https://www.myNetLinxMaster.com/**, then enter the server name as www.myNetLinx Master.com.
5. Send the CA the text created by your certificate request through the Master by exporting this information within the Server Certificate page. Refer to the*Server - Creating a Request for an SSL Certificate* section on page 67 for the procedures necessary to generate the certificate text file.
6. Follow the procedures outlined in the following section to export the data to the CA.

Server - Exporting an SSL Certificate Request

1. First follow the procedures outlined in the*Server - Creating a Request for an SSL Certificate* section on page 67 to begin the process of requesting an SSL by creating a session-specific Master certificate.
2. Click the **Export Certificate Request** button to display the certificate text file within the Server Certificate page (FIG. 52).

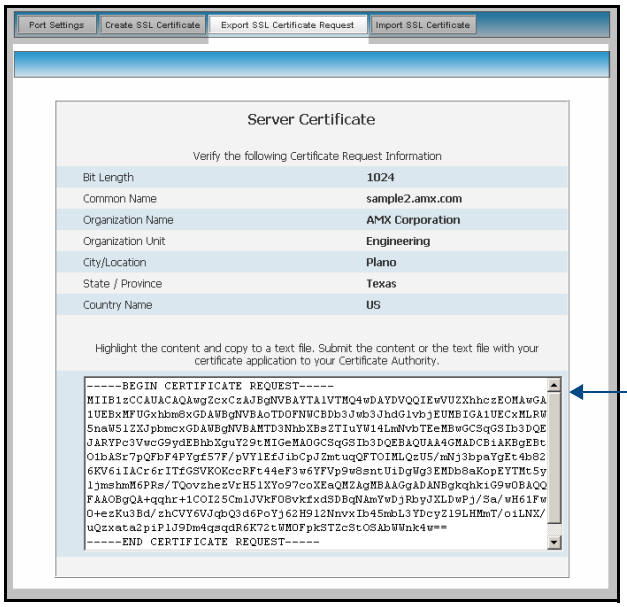


FIG. 52 Export SSL Certificate dialog

3. Place your cursor within the certificate text field.
4. Press the **Ctrl** + **A** keys simultaneously on your keyboard (this selects all the text within the field).

NOTE

YOU MUST COPY ALL OF THE TEXT *within this field, including the* ***-----BEGIN CERTIFICATE REQUEST-----*** *and the* ***-----END CERTIFICATE REQUEST-----.*** *This text in the CA submission must be included to receive a CA-approved certificate.*

5. Press the **Ctrl** + **C** keys simultaneously on your keyboard (this takes the blue selected text within the field and copies it to your temporary memory/clipboard).
6. Paste this text into the *Submit Request* field on the CA's Retrieve Certificate web page.
7. Choose to view the certificate response in raw DER format.
8. Note the **Authorization Code** and **Reference Number** (for use in the e-mail submission of the request).
9. Submit the request.
10. Paste this certificate text field (copied from steps 4 & 5 above) into your e-mail document and then send that information to a CA with its accompanying certificate application.

WARNING

When a certificate request is generated, you are creating a private key on the Master. ***YOU CANNOT REQUEST ANOTHER CERTIFICATE UNTIL THE PREVIOUS REQUEST HAS BEEN FULFILLED.*** *Doing so voids any information received from the previously requested certificate and it becomes nonfunctional if attempted to be used.*

11. Once the returned CA certificate has been received, follow the procedures outlined in the following section to import the returned certificate (*over a secure connection*) to the target Master.

Server - Importing a CA created SSL Certificate

Before importing a CA server certificate:

- **First**, have a self-generated certificate installed onto the target Master.
- **Secondly**, enable the SSL security feature from the Enable Security page, to establish a secure connection to the Master prior to importing the encrypted CA certificate. Refer to the*Security - System Level Security page* section on page 39 for more information about enabling SSL security.

1. Take the returned certificate (signed by the CA and encrypted with new information which makes it different from the text string that was previously sent) and copy it into the clipboard.

2. Navigate to the Server Certificate page by clicking **System Settings** > **Manage System > Server > Import SSL Certificate** to open the Import Certificate page (FIG. 53).

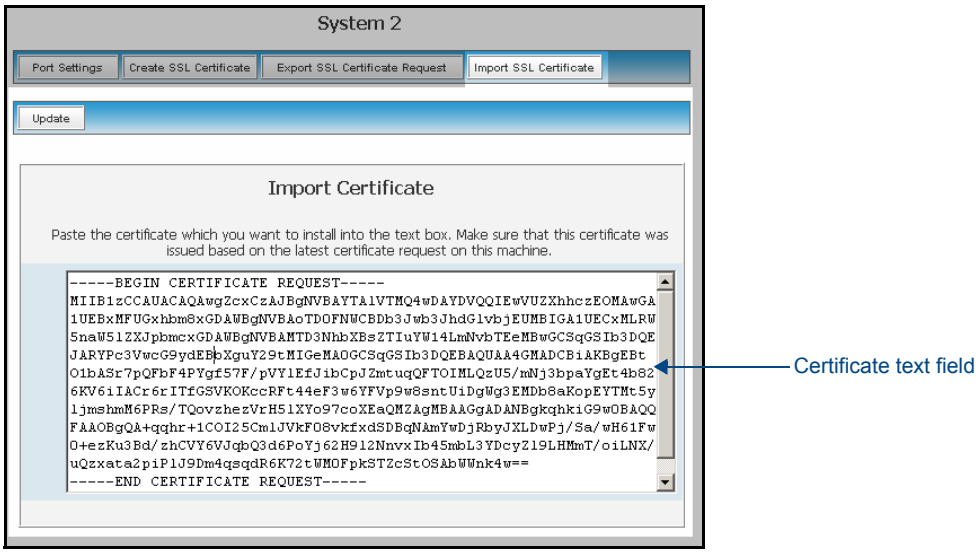


FIG. 53 Import SSL Certificate dialog

3. Place the cursor within the empty window and paste the raw text data (in its entirety) into the field.
4. Click the **Update** button to enter the new encrypted certificate information and save it to the Master.

CAUTION

*Once a certificate has been purchased from an external CA and then installed onto a specific Master, **DO NOT regenerate the certificate or alter its properties** (example: bit length, city, etc.). If the purchased certificate is regenerated, it becomes invalid.*

A certificate consists of two different Keys:

- **Master Key** is generated by the Master and is incorporated into the text string sent to the CA during a certificate request. It is specific to a particular request made on a specific Master.
- **Public Key** is part of the text string that is returned from the CA as part of an approved SSL Server Certificate. This public key is based off the submitted Master key from the original request.
- Regenerating a previously requested and installed certificate invalidates the previously purchased certificate because the Master Key has been changed.

5. Use the **Server** > **Create SSL Certificate** > **Display Certificate** option to confirm that the new certificate was imported properly to the target Master.

CAUTION

A CA server certificate can only be imported to a target Master only after both a self-generated certificate has been created and the SSL Enable feature has been selected on the Master. These actions configure the Master to the secure communication necessary during the importing of the CA certificate.

Manage System - Device Menu Buttons

The Device Menu buttons appear when a user clicks on any violet Device icon from within the Online Tree. The selected system number: device number are displayed below these menu buttons.

Device Menu - Configuring the LAN Settings

1. Click the **System Settings** > **Manage System** link from within the System Settings section of the Navigation frame.
2. Click on a violet Device icon from within the Online Tree to open the Device menu buttons within the right frame.
3. Click the **Network Settings** button to open the Network Settings dialog (FIG. 54). This dialog allows a user to set up the LAN settings for the specified device. The fields are populated with the current settings when initially loaded.

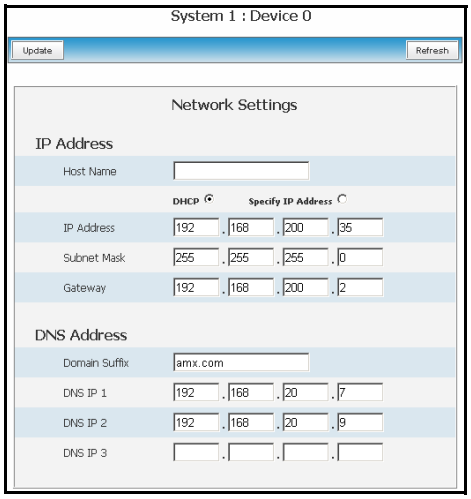


FIG. 54 Network Settings dialog

Network Settings Dialog	
Feature	**Description**
IP Address:	
Host Name	Use this field to view/edit the target Master's current Host Name.
DHCP/Specify IP Address	Use these radio buttons to specify an address for the target Master: • **DHCP** - obtained from a DHCP Server. • **Specify an IP Address** - typically obtained from a System Administrator.
IP Address	Use this field to view/edit the target Master's current IP Address.
Subnet Mask	Use this field to view/edit the target Master's current Subnet Mask assignment.
Gateway	Use this field to view/edit the target Master's current Gateway assignment.
DNS Address:	
Domain Suffix	Use this field to view/edit the target Master's current Domain Suffix.
DNS IP #1, #2, #3	Use these fields to view/edit the target Master's current DNS IP addresses.

4. Enter a new or updated name within the *Host Name* field. This entry can be 1 - 50 alphanumeric characters in length.
5. Select either the **DHCP** or **Specify and IP Address** checkbox to choose the source of the IP Address information being used within the remaining fields.
6. Enter or change any IP Address or DNS Address information within the remaining fields.
7. Click **Update** to save any changes. If the changes are successfully updated to the Master, the following message appears: "*Network Settings updated. Device must be rebooted for the setting to take effect*".

8. Return to the System menu by clicking on the purple System icon from within the Online Tree, click the **Reboot** button, and then allow the Master a short time to reboot itself.
9. Click on the **Refresh** macro from the browser's menu bar. If no security is currently enabled on the target Master, the browser is directed back to the Manage WebControl Connections page. If security is enabled, the browser is directed to the initial Username/Password page to enter personal access information.

Device Menu - Developing a URL List

1. Click the **System Settings** > **Manage System** link from within the System Settings section of the Navigation frame.
2. Click on a violet Device icon from within the Online Tree to open the Device menu buttons within the right frame.
3. Click the **URL List** button to open the URL List dialog (FIG. 55). This dialog allows the user to view, add, and remove URLs from the specified devices URL list.

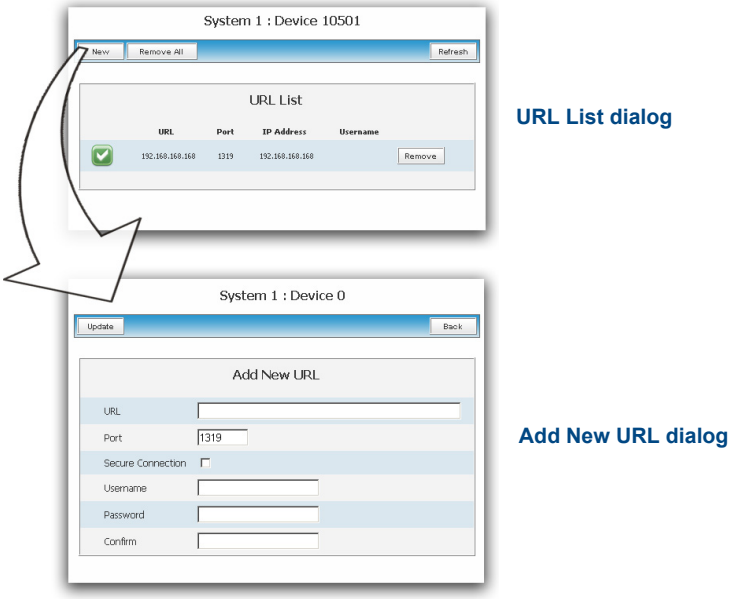


FIG. 55 URL List dialog

4. Add a new URL to the list by pressing the **New** button, which opens the *Add New URL* dialog.
5. Enter either an IP Address or a resolvable name (ex: **www.amx.com**) into the *URL* field.
6. Enter the Port number used to connect to the other device within the *Port* field. The default port provided in 1319, which is used for ICSP communication. Refer to the*Manage System - Server* section on page 61 for more information on the default Ports used for communication.
7. If a Username and/or Password is required for successful communication with the target URL, place a checkmark in the **Secure Connection** checkbox and enter the necessary information within the Username, Password, and Confirm (password) fields.
   - If this box is unchecked, the fields are greyed-out and the user is prevented from entering any text into any of the remaining fields.

NOTE

These fields are not greyed-out within Internet Explorer, even though they become read-only.

8. Click the **Update** button to accept and save your changes. If you are able to enter your information, a "*URL added successfully*" message is displayed at the top of the Add New URL dialog.
9. Click the **Back** button to return to the main URL List dialog.

10. Confirm that the newly added URLs appear within the URL List dialog (FIG. 56).

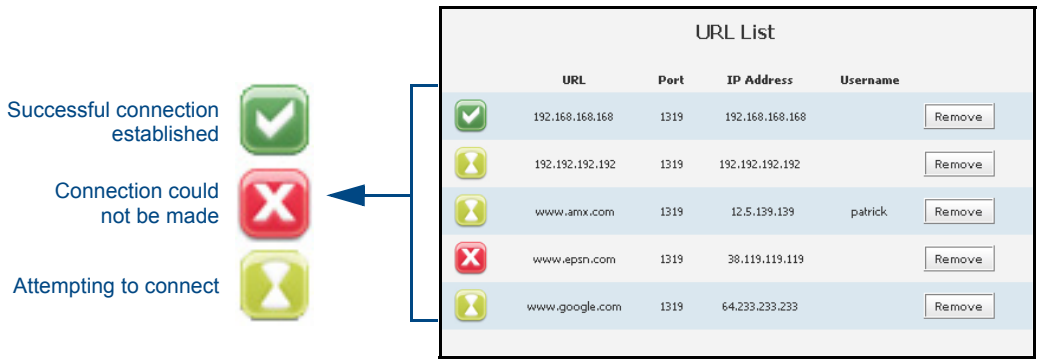


FIG. 56 URL List dialog (with entries)

- If the newly added URL doesn't appear on this page, click the **Refresh** button.

11. URL entries can be removed either individually or as a whole:

- Remove an individual URL entry by pressing the **Remove** button on that URLs row listing within the URL List dialog (FIG. 56).
- Remove all previously entered URLs by pressing the **Remove All** button. To confirm the removal of all items, press the **Refresh** button.

Device Menu - Changing the Device Number

1. Click the **System Settings** > **Manage System** link from within the System Settings section of the Navigation frame.

2. Click on a violet Device icon from within the Online Tree to open the Device menu buttons within the right frame.

3. Click the **Device Number** button to open the Device Number (FIG. 57). This dialog allows the user to change the device number for the selected device.

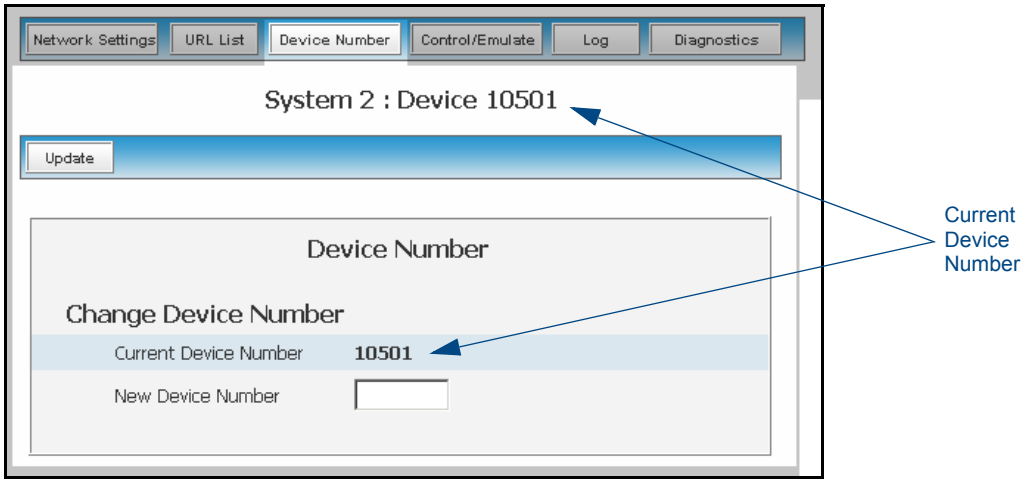


FIG. 57 Device Number dialog

- The current device number is also shown just below the System menu buttons.

4. Enter a new numeric value into the *New Device Number* field.

5. Click the **Update** button to save this new value to the device. The following message; "*Device number changed to XXX. Device must be rebooted for the change to take effect.*", reminds the user that the Master must first be rebooted before the new settings take effect.

Device Menu - Controlling or Emulating a device

Refer to the procedures outlined within the*System Menu - Controlling/Emulating Devices on the Master* section on page 55 for more information.

Device Menu - Viewing the Log

1. Click on the **System Settings** > **Manage System** link from within the System Settings section of the Navigation frame.
2. Click on a violet Device icon from within the Online Tree to open the Device menu buttons within the right frame.
3. Click the **Log** button (FIG. 58). This dialog allows the user to view the log for the selected device (*currently only the Master supports this feature*).

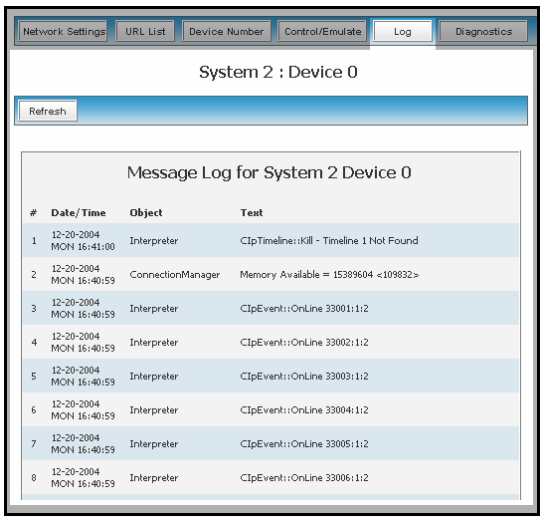


FIG. 58 Log dialog

4. Click the **Refresh** button to update the information on-screen.

Device Menu - Running a Diagnostic Filter

Refer to the procedures outlined within the*Manage System - Diagnostics* section on page 57 for more information.

System Settings - Manage License

This page (FIG. 59) displays both the currently used license keys and the pending keys.

- The **New** button allows for the addition of new license keys associated with currently used modules/products.
- Adding new License Keys requires the use of both a Product ID and a Serial Key.
- An example of this type of product is i!-Voting. The Master confirms this registration information before running the module.

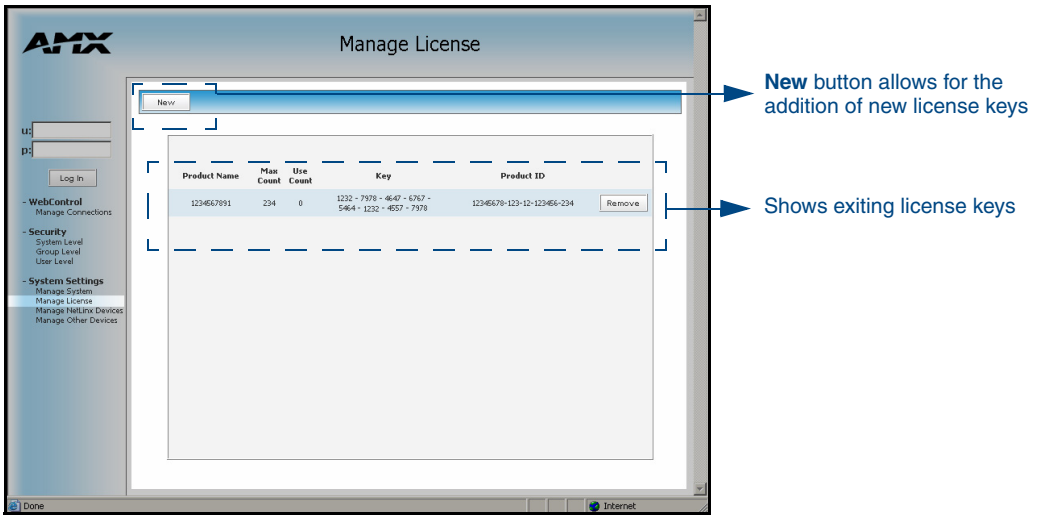


FIG. 59 System Settings - Manage License page

Adding a new license

1. Click on the **System Settings** > **Manage License** link from within the System Settings section of the Navigation frame.
2. Click the **New** button to be transferred to the *Add new License Key* page (FIG. 60).

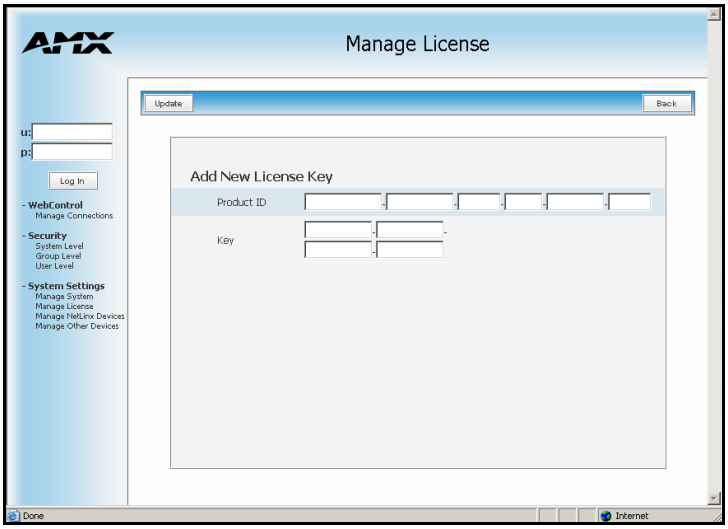


FIG. 60 System Settings - Add New License Key page

3. Enter the Product ID (certificate number) provided with the product into the *Product ID* fields.
4. Contact the AMX Sales department with both the product serial number (or certificate number) and the serial number of target Master to register your product and in turn receive the necessary Key information (typically 32 to 36 digits in length) which is then entered into the *Key* fields on this page.
   - The Key is Master specific and is typically provided by AMX upon registration.
   - **Example:** AMX Meeting Manger and i!-Voting applications are examples of products that would require both a Product serial number and a Master-specific key prior to usage.
5. Press the **Update** button to save the information. A "*Key successfully added for Product ID XXXX*" notice is displayed at the top of the page if the information on this page has no errors.
6. Press the **Back** button to return to the previously active Manage License page.

Removing a license

1. Click on the **System Settings** > **Manage License** link from within the System Settings section of the Navigation frame.
2. Click the **Remove** button.
3. Click **OK** from the *"Are you sure you want to remove this?"* popup.

System Settings - Manage NetLinx Devices

To access this page, click on the **Manage NetLinx Devices** link (*from within the System Settings section of the Navigation frame*). These pages (FIG. 61) have some additions that have been incorporated as part of ***build 323 (or higher)***. These features include the display the device status as well as some background color changes which indicate system groupings. These enhancements are visual changes which allow for easier recognition of the information on a visual basis. IP connections are then able to utilize a LAN's higher layers of multicast to broadcast their existence.

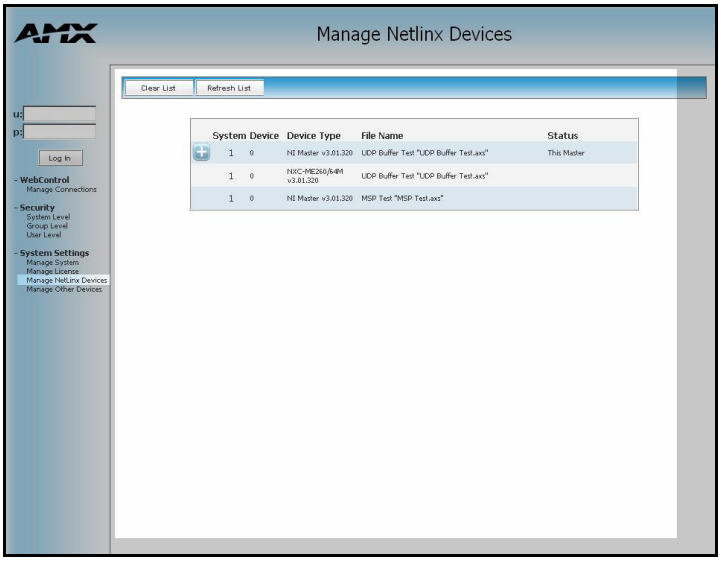


FIG. 61 System Settings - Manage NetLinx Devices page

Manage NetLinx Devices Page	
Feature	**Description**
Clear List:	Clicking this button causes the entries to be temporarily deleted from the page until either the user chooses to refresh the entries (using the **Refresh List** button) or the Master begins to detect any multi-cast transmissions as devices send out their announcements.
Refresh List:	• Clicking this button allows the target Master to regenerate the listing by looking for broadcasting devices. • The button causes the Master to send out a message asking devices to resend their NDP device announcements. The list is then updated as those devices send back their announcements to the "listening" Master. • Due to system delays, message collisions, and multicast routing, not all devices may respond immediately. • The information displayed can not only include Masters and devices on this system but Masters and devices on other systems as well. By default, the target Master always appears in the list.

A large number of NDP-capable devices on the LAN can result in a large amount of LAN traffic occurring at the same time.

Manage NetLinx Devices Page (Cont.)	
Feature	**Description**
Device Listings:	• This page (*in addition to the target Master which is typically the first entry*) lists those NetLinx Masters which have sent out NetLinx Discovery Master Announce packets (NDPs). • Each entry contains the data necessary to describe the devices detected by the system. • If a Master has a '**+**' icon next to it, this indicates that this Master is reading the presence of a NDP-capable devices currently connected to it. This state can be toggled closed to show a '**-**' icon.
System	Displays the System value being used by the listed NetLinx Master.
Device	• Displays the assigned device value of the listed unit. This Device entry applies to both the Master and those NDP-capable devices currently connected to that Master.
Device Type	• Displays a description of the target Master or connected device, and its current firmware version. An example is: NI Master v3.01.323.
File Name	Displays the program name and/or file resident on the device.
Status	Displays the Master or device state. Those states include: • **This Master**: Indicates its the target Master currently being used and being browsed to. Its this Master's web pages which are currently being viewed. • **Orphan**: Indicates that the device is currently not yet "bound" or assigned to communicate with a particular Master. - This state shows an adjacent **Bind** button which is used to bind the device to the Master whose web pages are currently being viewed. • **Searching**: Indicates that the device is trying to establish communication with it's associated Master. • **Bound**: Indicates that the device has established communication with it's associated Master. - This state shows an adjacent **Unbind** button which is used to release/disassociate the device from communicating with its current Master. • **Lost**: Indicates that the device has tried to establish communication with it's associated or "bound" Master, but was after a period of time, unable to establish communication.

Manage NetLinx Devices - Displaying NDP-capable devices

Note that in the previous example (FIG. 61), the first NetLinx Master has a "+" icon next to it, which shows that this Master is indicating the presence of NDP-capable devices currently connected to it.

1. Click the "+" icon to expand the particular Master's listing and reveal those NDP-capable devices connected to it, as shown below in FIG. 62.

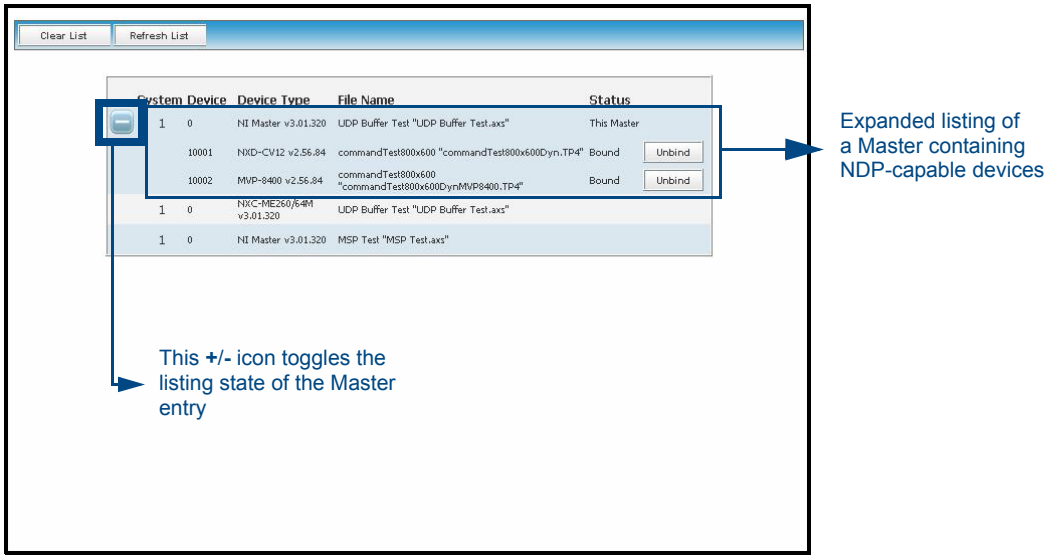


FIG. 62 Manage NetLinx Devices page - showing an expanded view

- Note that in this example, the currently active Master's Status description reads - **This Master** and that the sub-devices are **Bound** to communicate with that Master. Even though they are currently bound, clicking the adjacent **Unbind** button will release them from communication with a particular Master.

2. Click the "-" icon to collapse the particular Master's listing.

Manage NetLinx Devices - Binding/Unbinding - Explained

From below the **Status** column (*which displays the Master or device state*) you can determine whether a device is Bound or Orphaned. For more information, refer to the section on page 82.

- A **Bound** device is one which has established communication with it's associated Master. This device was previously bound to communicate with a specific Master.
  - This state shows an adjacent **Unbind** button which is used to release/disassociate the device from its current Master.
  - Once this button is pressed, the device then shows up as **Orphan**ed (*within the Status column*).
- An **Orphan** is an NDP-capable device which has not yet been assigned to communicate (bound) with a specific Master.
  - This state shows an adjacent **Bind** button which is used to then bind the device to the Master whose pages are currently being viewed (*displayed as **This Master** within the Status column*).
  - Once this button is pressed, the device then shows up as Bound (*within the Status column*).

Manage NetLinx Devices - Obtaining NetLinx Device information

To obtain more description than is provided by the listing:

1. Hover the cursor over a particular device within the listing to display a mouse-over popup dialog (FIG. 63).

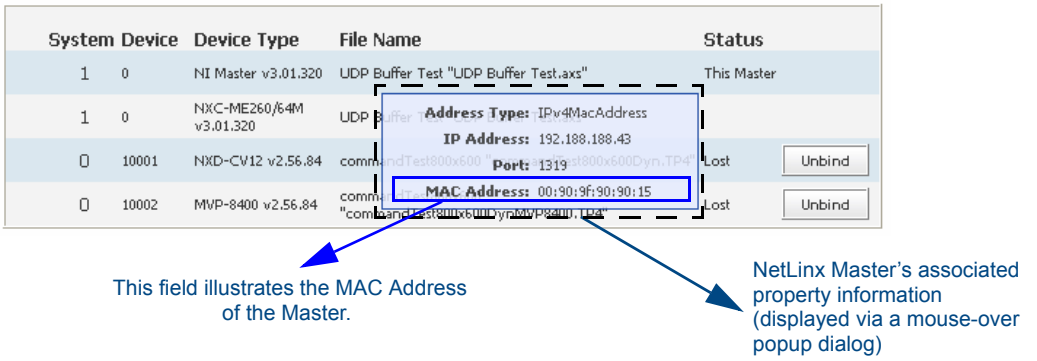


FIG. 63 Manage NetLinx Devices page - showing a sample mouse-over popup dialog

- The previous popup dialog shows the Master's IP settings including the IP Address, ICSP Port, and a MAC Address.
- If the device is one that is bound to a Master, the popup also displays an additional Master *MAC Address* field, which should match the MAC Address information for the bound target Master (FIG. 64). **Notice that the Master MAC Address in FIG. 64 should match the MAC Address of the Master in FIG. 63.**

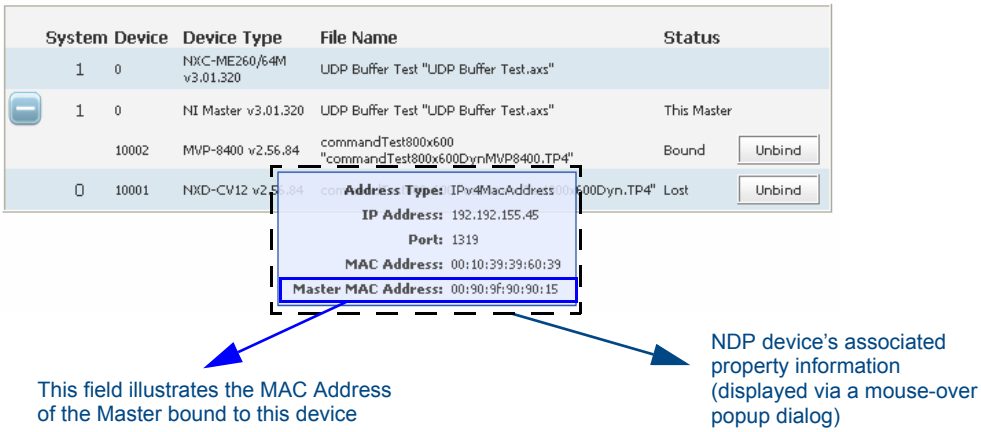


FIG. 64 Manage NetLinx Devices page - showing a sample mouse-over popup dialog

- In the above example, the moused-over device is bound to an NI Master on System 1 running firmware v3.01.320. The device's popup shows the MAC Address of the Master with which it is bound (00:90:9f:90.....).
- If this device is ever unbound from this Master (using the Unbind button), its Master MAC Address would be left blank.

System Settings - Manage Other Devices - Dynamic Device Discovery Pages

NOTE

Before beginning to manage any other devices, the target Master must be loaded with the program which defines the new devices and modules. In addition to this code, all IP/Serial devices must be pre-configured and connected to the system.

To access this page, click on the **Manage Other Devices** link (*from within the System Settings section of the Navigation frame*). This page (FIG. 65) (***within build 323 or higher***) is used as the entry point for the management of all 3rd party Dynamically Discovered Devices.

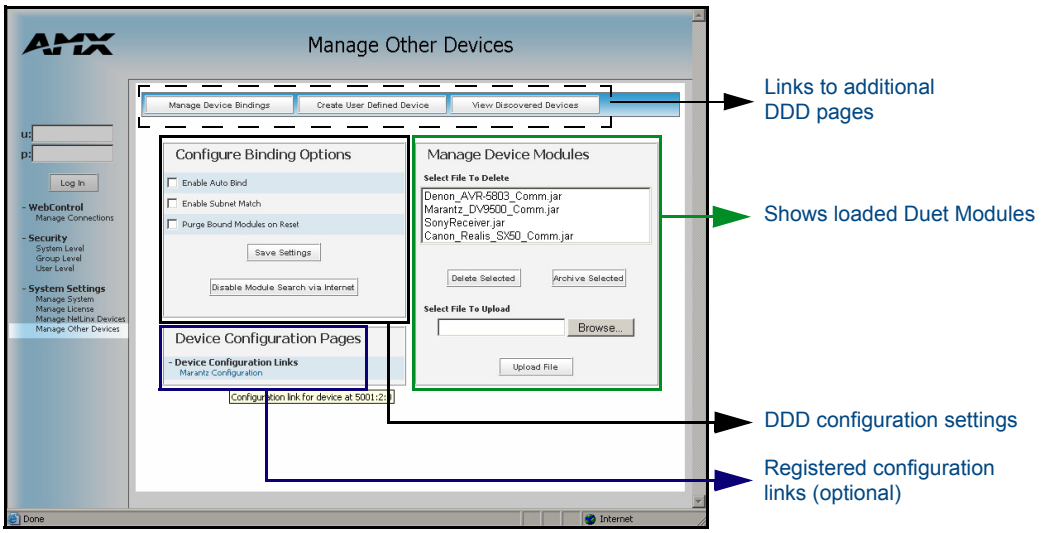


FIG. 65 System Settings - Manage Other Devices page

Manage Other Devices Page	
Feature	**Description**
Dynamic Device Discovery links:	These links direct the user to additional Dynamic Device Discovery (DDD) configuration pages which include: • **Manage Device Bindings** page is used for configuring application-defined Duet virtual devices by using discovered physical devices. - If your current NetLinx program (*running on the target Master*) has been written, and you have notified the Master of a set of Dynamic Devices on your system, you will then want to start by managing those devices through this page. • **Create User Defined Device** page provides a Web interface used in creating and managing the values necessary to add a dynamic physical device to the system. The devices added on this page do not support the DDD beaconing technology. - If after confirming the presence of your programmed Dynamic Devices (*provided to the Master via the NetLinx code*), and have allowed the Master to confirm the presence of any other Dynamic Devices, manually enter those remaining devices on the system via the UserDefined Device page. ***Note**: IR-controlled devices (such as a VCR or Receiver) must always be User-Defined devices.*

Manage Other Devices Page (Cont.)	
Feature	**Description**
Dynamic Device Discovery links (Cont.):	• **View Discovered Devices** page displays a listing of all the dynamic devices that have been discovered within the system. - After confirming the presence of those previously coded Dynamic Devices within the Manage Device Bindings page, navigate to the View Discovered Devices page to continue the process of detecting Dynamic Devices which have been detected by the system, and then assign Module/drivers to those devices via the View Discovered Devices page.
Configure Binding Options:	This section contains configuration settings regarding the DDD process.
Enable Auto Bind	• This selection allows an end-user to toggle the state of the automatic binding for DDD (On/Off). • When auto-binding is enabled, the Master automatically attempts to connect any newly discovered device with an associated application device (*defined in the running NetLinx application*). • Auto-binding can only be accomplished if the Master's firmware determines a one-to-one correlation between the newly discovered device and a single entry within the list of defined application devices (*accessed by pressing the **Manage Device Bindings** button at the top of the page*). • For example, if the application only has one VCR defined and a VCR is detected in the system, auto-binding can then be accomplished. - If there were two VCRs defined within the application, auto-binding could not be completed due to the lack of a clearly defined one-to-one correspondence. • When the ***Enable Auto Bind*** option is not selected, no auto-binding activity takes place and all binding of the newly discovered devices must be accomplished manually via the Web control interface*Manage Other Devices - Manage Device Bindings* section on page 85.
Enable Subnet Match	This selection allows an end-user to toggle whether or not IP devices should only be detected/discovered if they are on the same IP Subnet as the Master.
Purge Bound Modules on Reset	• This selection indicates that all modules should be deleted from the **/bound** directory upon the next reboot. • During the binding process, the associated Duet modules for a device are copied from the **/unbound** directory into a protected **/bound** area. • Due to the dynamic nature of Java class loading, it is not safe to delete a running .JAR file. Therefore, this selection provides the administrator the capability of removing existing modules upon reboot by forcing a re-acquisition of the module at bind time. • This selection is a one-time occurrence. Upon the next reboot, the selection is cleared.
Save Settings	Clicking this button causes the current selected checkbox values to be saved into the system.

Manage Other Devices Page (Cont.)	
Feature	**Description**
Enable/Disable Module Search via Internet	• Clicking this button toggles the capability of searching the Internet (*either AMX's site or a device specified site*) for a device's compatible Duet modules. This capability is automatically disabled if the Master does not have Internet connectivity. • Upon enabling Internet connectivity, the AMX License Agreement is displayed for acceptance (FIG. 66). The AMX License Agreement must be accepted (*by pressing the **Accept** button on the upper-right of the page*) for the Internet Module search to be enabled. • When the Internet search for modules feature is enabled (the button then reads ***Disable Module Search via Internet***), the Master queries either AMX's Online database of device Modules and/or pulls Modules from a separate site specified by the manufacturer's device. • This feature may be disabled later by toggling the button.
Device Configuration Pages:	This section is optional and is only present when either configuration links have been previously registered by a running Duet Module, or if a discovered device supplies configuration link information. • If present, this section displays each link along with a mouse-over tool-tip. • For Duet Modules this tool-tip describes the module configuration link. • For discovered devices this tool-tip indicates the physical device the configuration link is associated with.
Manage Device Modules:	This section displays a list of all currently loaded Duet Modules/.JAR files on the Master (*resident within the **/unbound** directory*); as well as providing those interfaces necessary to delete, add, and retrieve these modules.
Select File to Delete	• This field provides the listing of loaded Modules/.JAR files. • These entries can be selected for deletion or archiving.
Delete Selected	• Clicking this button deletes a selected module from the **/unbound** directory. Any corresponding module within the **/bound** directory will NOT be deleted. Bound modules must be deleted via the **Purge Bound Modules on Reset** selection described within the previous *Configure Device Bindings* section.
Archive Selected	• Clicking this button copies the selected JAR file to the PC which the user is browsing from. • This option allows an administrator to archive those Duet Modules resident on a target Master back to a PC.
Select File to Upload	• This section allows a user to browse for a target Module/.JAR file and then upload it to a target Master. • **Browse**: Allows the user to browse for Duet Modules on the PC/LAN. • **Upload File**: Copies the specified Duet Module to the target Master's **/unbound** directory. - If a file of the same specified name already exists within the **/unbound** directory; a prompt is displayed to confirm the over-write of the existing .JAR file. Only JAR file types are allowed for Upload to the target Master.

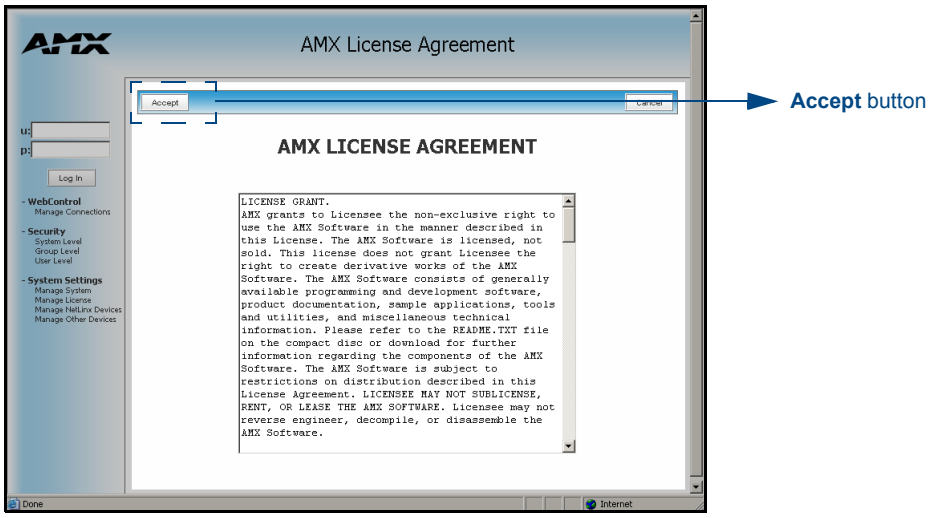


FIG. 66 System Settings - AMX License Agreement page

What is Dynamic Device Discovery?

The Dynamic Device Detector (DDD) monitors the system for newly connected devices. New devices can be detected via either an external discovery protocol manager (*built into firmware build 320 or higher*), Multicast reception of a Dynamic Device Beacon, or via the receipt of a beacon response on an application specified list of serial devices. This DDD process begins by detecting new devices within a NetLinx/Duet system, binding those devices to application instances, and then starting a Duet module to control those new devices.

Dynamic Device Discovery was created to take advantage of Java's Dynamic Class Loading and the Duet Standard NetLinx API (SNAPI). Java loads classes as they are needed. Therefore it is feasible to load a Duet control/protocol module on the fly as each new device is discovered. SNAPI provides a fixed interface for communicating with a certain type of device. The "glue code" refers to the developer defined NetLinx program that runs on a Master and controls a system.

Take for example a VCR. The majority of control features are common to all VCRs (play, stop, pause, etc.). SNAPI provides the "glue code" developer the ability to write common code that will control any type of VCR having an associated Duet module. The underlying Duet module could be swapped in and out based on the actual physical device with no changes needed to the higher level "glue code".

Dynamic Device Discovery Concepts	
Feature	**Description**
Application Device:	• A Duet Device (41000-42000) that is used as a control interface to a physical device. This is also referred to as the *Duet virtual device*. • All control requests are made to the application device rather than to the physical device.
Binding:	• In concrete programming, the application device is forever associated with the NetLinx physical device. In DDD, this association is dynamic. • The act of associating an application device with a physical device is called “binding".
Device Discovery:	• In DDD, physical devices are detected in the system at run-time. • There are two different methods of detection: via Dynamic Device Discovery Protocol (DDDP) or via user definition within the Master’s Web interface (page 89).
SDK Class:	• Each application device in the DDD world is associated with a particular device type as defined by SNAPI. • When using a VCR or a Receiver as an example, each of these device types would correspond with a Java Interface within the Duet Device Software Development Kit (SDK). • When writing programs for DDD, the developer specifies the device type of a particular application device by using one of these SDK Class names.

Polling:	• Dynamic physical devices can be detected by DDDP through both Serial and IP interfaces. • While IP connections are then able to utilize the LAN's higher layers of multicast to broadcast their existence, Serial devices speak a fixed protocol that is incompatible with DDDP. • Serial devices are passive and will only broadcast their existence if polled to do so. The program developer must specify which NetLinx interfaces/ports (i.e. serial ports) should be polled for devices.

What is the difference between Program and Run-time defined binding?

In DDD, the device discovery activity is always dynamic because the devices will always be detected at run-time. Note that DDD splits the binding activity into two different categories:

- **Program defined binding** (also known as static)
- **Run-time defined binding** (also known as dynamic).

With program defined/static binding, the developer specifies a permanent binding between an application device and a physical port, such as a particular serial or IR port. At run-time, any device detected on that port is automatically associated with the designated application device. This binding type would be used when the developer wants to hard code what port is used for a device, but does not know what manufacturer's device will actually be connected. Static binding is not available for IP connected devices, since the IP Address value of a device is subject to change due to IP LAN topology.

- An example of its use would be if DHCP is enabled for the peripheral device. A hard-coded IP Address within the NetLinx "glue-code" would be inadequate due to the nature of the dynamically acquired DHCP IP Addresses. Only actual NetLinx D:P:S values are allowed for static binding of physical ports.

With run-time defined/dynamic binding, the application device and the physical port are completely disassociated (in a program sense). The developer defines the application devices and their associated SDK class but does not specify what physical port they are bound to. At run-time, as those devices are discovered, the new physical devices are then bound to an application device either automatically or via the Master's Web access. Dynamic binding is the only binding option available for IP-connected peripheral devices due to the dynamic nature of IP Addresses as discussed earlier.

Manage Other Devices - Manage Device Bindings

To access this page, click on the **Manage Device Bindings** button (*from within the Manage Other Device page*). This page is used to configure application-defined Duet virtual devices with discovered physical devices. The on-screen table (FIG. 68) displays a list of all application-defined devices (including the defined "friendly name"), the Duet virtual D:P:S, and the associated Duet Device SDK class (indicating the type of the device). This information would have been pre-coded into the NetLinx file currently on the target Master (FIG. 67).

Configuring application-defined devices

Elements such as `DUET_DEV_TYPE_DISC_DEVICE` and `DUET_DEV_POLLED` are defined within the NetLinx axi. The latest version of the NetLinx.axi file contains both the new API definitions, as well as the pre-defined constants that are used as some of the API arguments (ex: `DUET_DEV_TYPE_DISC_DEVICE`). Sample code can be found within the DEFINE_START section seen in FIG. 67:

*Physical device names are typically prefixed with "**dv**" and Virtual device names are typically prefixed with "**vdv**". It is recommended that anyone working with these modules should become familiar with this naming convention.*

```
PROGRAM_NAME='DDD'
DEFINE_DEVICE
COM1 = 5001:1:0
COM2 = 5001:2:0
dvRECEIVER1 = 41000:1:0
dvDiscDevice = 41001:1:0

DEFINE_CONSTANT
DEFINE_TYPE
DEFINE_VARIABLE

DEFINE_START

STATIC_PORT_BINDING(dvDiscDevice, COM1, DUET_DEV_TYPE_DISC_DEVICE,
    'My DVD', DUET_DEV_POLLED)

DYNAMIC_POLLED_PORT(COM2)

DYNAMIC_APPLICATION_DEVICE(dvRECEIVER1, DUET_DEV_TYPE_RECEIVER,
   'My Receiver')

(***********************************************************)
(*                THE EVENTS GO BELOW                      *)
(***********************************************************)
DEFINE_EVENT

DATA_EVENT [dvRECEIVER1]
{
    // Duet Virtual device data events go here
}
```

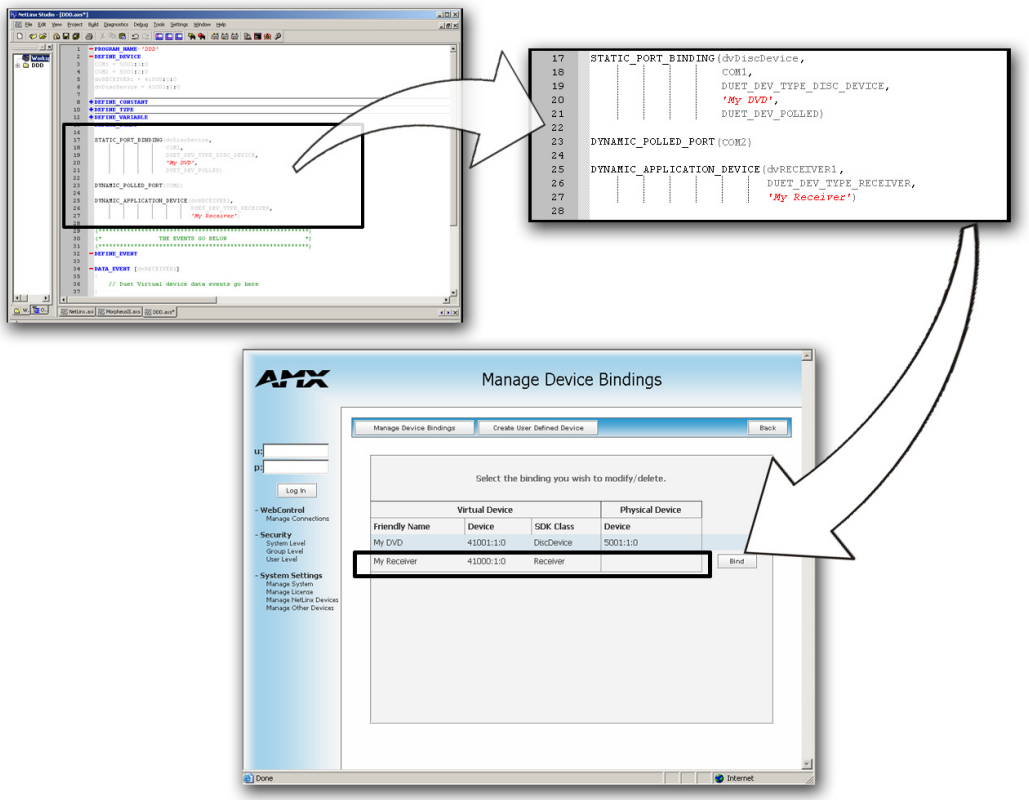


FIG. 67 Manage Device Bindings page - showing the NetLinx code relation

This code would have given the Master a previous “heads-up” notification to look for those devices meeting the criteria outlined within the code.

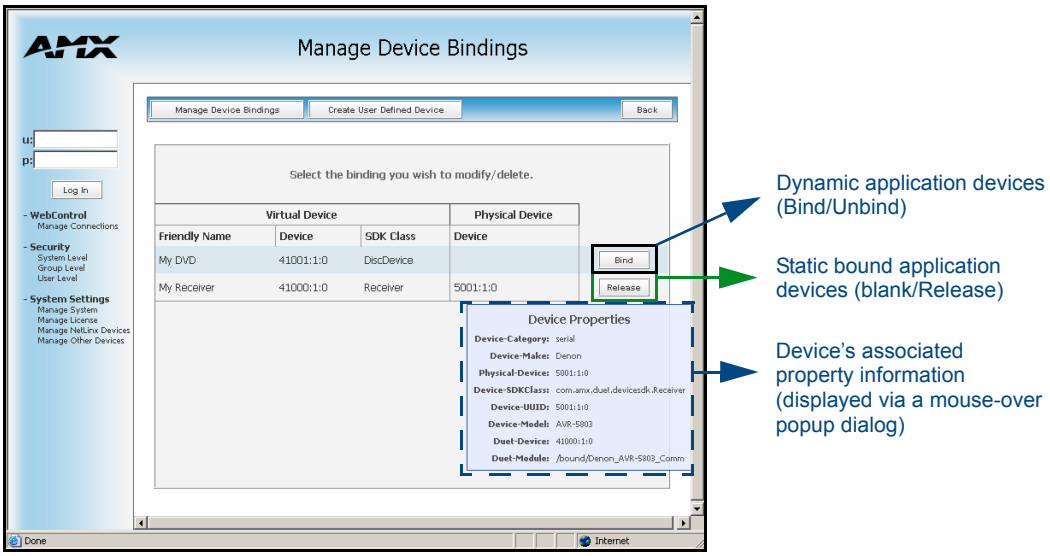


FIG. 68 Manage Device Bindings page

What are Application Devices and their association status?

There are two types of application devices: Static Bound application devices and Dynamic application devices.

- **Static Bound application devices** specify both a Duet virtual device and its associated Device SDK class type, as well as a NetLinx physical device port to which the application device is **ALWAYS** associated (i.e. statically bound).
- **Dynamic application devices** specify both the Duet virtual device and its associated Device SDK with no association to a physical port. Binding of an application device to a physical device/port occurs at run-time either via auto-binding or manual binding.

Application devices that have a "bound" physical device display their physical device ID within the **Physical Device** column. If an associated Duet module has been started to communicate with the device, its associated property information is then displayed in a mouse-over popup dialog when the cursor hovers over the physical device ID.

Each entry in the table has one of four values appear within the far right of the Manage Device Bindings page (FIG. 68).

- **Static bound application devices** will either be *blank* or display a **Release** button.
  - Static application devices that have not yet detected a physical device attached to their associated port are left *blank*. Once a physical device is detected and its associated Duet module has been started, a **Release** button is then displayed.
  - By selecting **Release**, the administrator is forcing the associated Duet module to be destroyed and the firmware then returns to detecting any physical devices attached to the port.
- **Dynamic application devices** either display a **Bind** or **Unbind** button.
  - Dynamic application devices that have been bound display an **Unbind** button. When the user selects **Unbind**, any associated Duet module is then destroyed and the "link" between the application device and the physical device is then broken.
  - Dynamic application devices that have not been bound to a physical device display a **Bind** button. When this button is selected, a secondary display appears with a listing of all available unbound physical devices that match the application device's Device SDK class type (FIG. 69).
  - If a currently bound device needs to be replaced or a Duet Module needs to be swapped out, the device should be unbound and the new module/driver should then be bound.

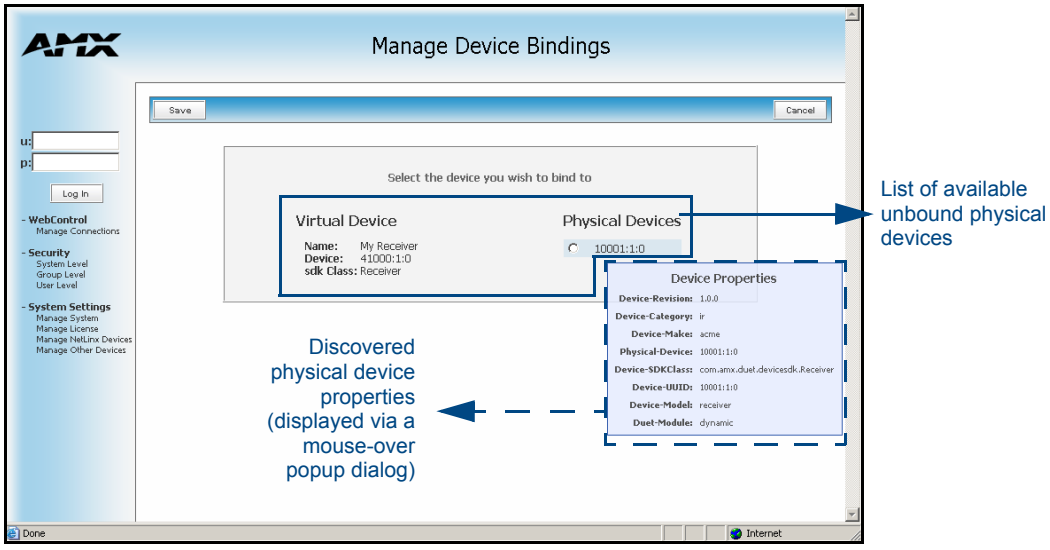


FIG. 69 Manage Device Bindings - showing a listing of all unbound devices

- The administrator/user can then select one of the available physical devices to bind with the associated application device. When the **Save** button is selected, the binding is created and a process begins within the target Master to find the appropriate Duet Module driver. Once a driver is found, the Duet Module is then started and associated with the specified application device (Duet

virtual device). If the **Cancel** button is selected, the binding activity is then aborted.
- A mouse-over popup dialog is provided to display the properties associated with each discovered physical device that is listed (FIG. 69).

NOTE

If the manufacturer device does not support Dynamic Device Discovery (DDD) beaconing, you must use the Add New Device page to both create and manage those values necessary to add a dynamic physical device. This process is described in detail within the following section.

Manage Other Devices Menu - Viewing Discovered Devices

This page (FIG. 70) provides a listing with all of the dynamic devices that have been discovered in the system.

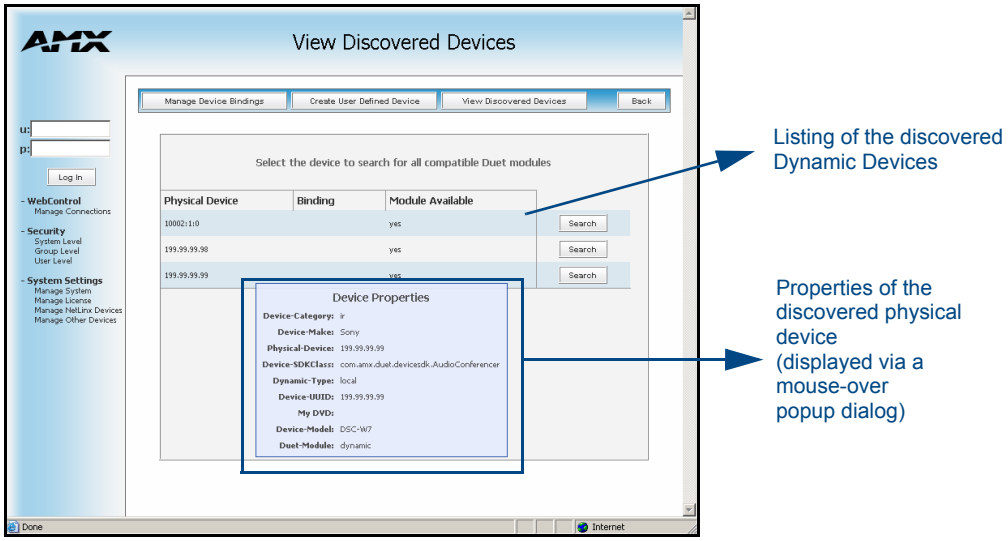


FIG. 70 View Discovered Devices page

Mousing-over a listed entry presents a popup which displays all of the properties associated with the physical device. If the physical device is bound to an application device, the associated application device's "friendly name" will be displayed in the **Binding** column. The **Module Available** column indicates if a Duet module is currently available on the system for the target physical device (the results are: **yes**, **no**, or **unknown**).

For each physical device, a **Search** button is provided which initiates a search for compatible modules.

- If the **Module Search via the Internet** option has been previously ***enabled*** (*via the corresponding button within the Configure Binding Options section of the Manage Other Devices page*), the search includes a query of the AMX online database for a compatible module based on the device's properties.
- If the device specified a **URL** in its DDD beacon, the file is retrieved from the URL either over the Internet or from the physical device itself, provided the device has an inboard HTTP or FTP server.
- If **Module Search via Internet** is ***NOT enabled***, the search does NOT query the AMX online database nor will it pull any manufacturer specified URLs that do not match the IP Address of the physical device itself.

Modules that are retrieved from either the Internet or from the manufacturer's device are then placed into the **/ unbound** directory and automatically overwrite any existing module of the same name.

Once a list of all compatible modules is compiled, the Select Device Module page (FIG. 71) is then displayed with a listing of each module along with its calculated "match" value. The greater the "match" value, the better the match between the Duet Module's properties and the physical device's properties.

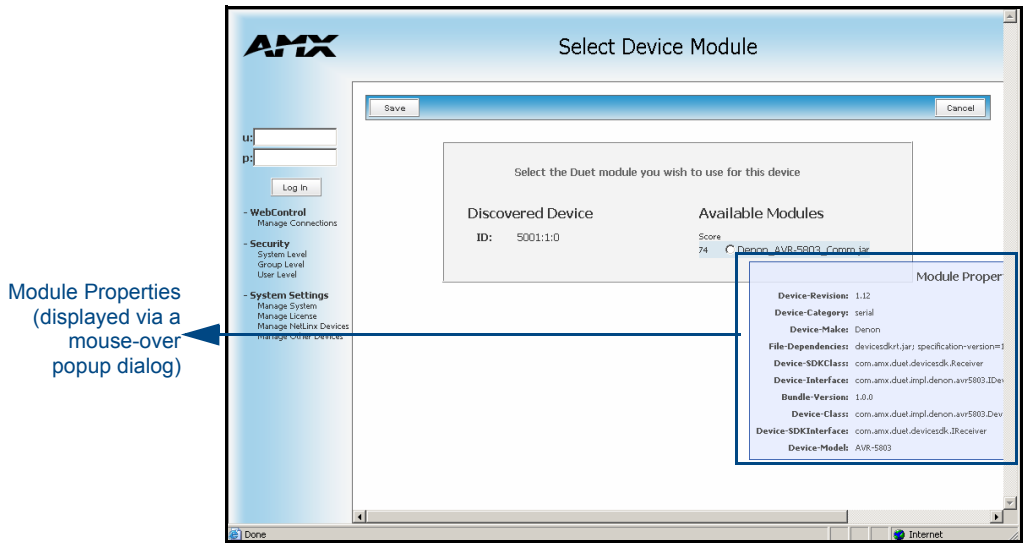


FIG. 71 Select Device Module page

Mousing-over a listed module entry presents a popup which displays the properties associated with the selected module.

By selecting the module and clicking the **Save** button, the administrator can assign a Duet module to be associated with the physical device.

NOTE

This action will NOT affect any currently running Duet module associated with the physical device. The module is associated with the device upon reboot.

Clicking the **Cancel** button aborts the association of a Duet module with the physical device **BUT** it does not undo the process of pulling new modules from the Internet/device into the **/unbound** directory on the target Master. These modules will remain resident in the **/unbound** directory until they are manually deleted via the Manage Other Devices main web page. Refer to the*System Settings - Manage Other Devices - Dynamic Device Discovery Pages* section on page 80.

Manage Other Devices Menu - Creating a new User-Defined Device

This page provides the ability to both add and remove any user-defined devices. Existing user-defined devices are listed at the bottom of the display along with a corresponding **Remove** button alongside each new entry. Although FIG. 72 shows a populated page, by default, all fields are blank and no devices are pre-populated.

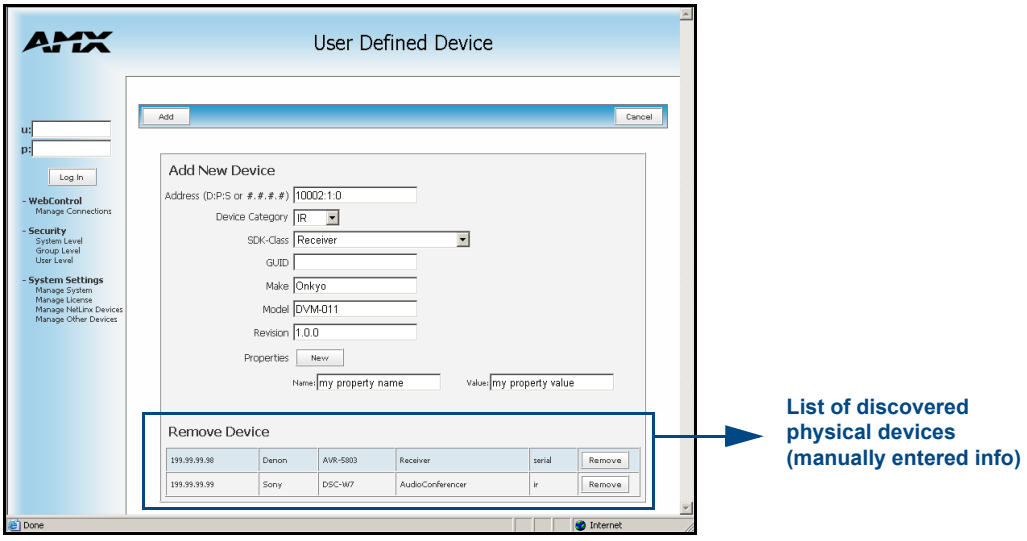


FIG. 72 Add New Device page

1. Click on the **Create User Defined Device** button (*from within the Manage Other Device page*).
2. Begin by entering the address of the physical device within the *Address* field. This information can be either the NetLinx Master port value (D:P:S) or an IP Address (#.#.#.#).
3. From within the *Device Category* field, use the drop-down list to select the control method associated with the physical target device (IR, IP, Serial, Relay, Other).
4. From within the *SDK Class* field, use the drop-down list to select the closest Device SDK class type match for the physical target device. The following table provides a listing of the available choices.

SDK-Class Types		
Amplifier	DocumentCamera	SlideProjector
AudioConferencer	HVAC	Switcher
AudioMixer	Keypad	Text Keypad
AudioProcessor	Light	TV
AudioTape	Monitor	Utility
AudioTunerDevice	Motor	VCR
Camera	MultiWindow	VideoConferencer
Digital Media Decoder	PoolSpa	VideoProcessor
Digital Media Encoder	PreAmpSurroundSoundProcessor	VideoProjector
Digital Media Server	Receiver	VideoWall
Digital Satellite System	Security System	VolumeController
Digital Video Recorder	Sensor Device	Weather
Disc Device	SettopBox	

5. Use the *GUID* field to enter the manufacturer-specified device's Global Unique Identification information. *Either the GUID or Make/Model must be specified within this field.*
6. Enter the name of the manufacturer for the device being used (up to 55 alpha-numeric characters) (ex: Sony, ONKYO, etc.) into the *Make* field. *Either the GUID or Make/Model must be specified within this field. Note that spaces in the name will be converted to underscores.*
7. Enter the model number of the device being used (up to 255 alpha-numeric characters) (ex: Mega-Tuner 1000) into the *Model* field. *Either the GUID or Make/Model must be specified within this field.*
8. Enter the firmware version used by the target device into the *Revision* field. *Text is required within this field.*
   - The version must be in the format: **major.minor.micro** (where major, minor, and micro are numbers). An example is: *1.0.0* (revision 1.0.0 of the device firmware).
9. Once you are done creating the profile for the new device, click the **New** button to assign additional **Name** and **Value** property information for association with the new User Defined Device.
   - When the **Add** button is selected, the user-defined device is then inserted into the list of discovered physical devices which appears within the lower section of the display (FIG. 72).
   - When the **Cancel** button is selected, the addition of the user defined device is aborted, no amendment to the existing list is made, and the user is returned back to the *Manage Device Bindings* page.
10. Once you have finished entering your devices, click the **Back** button (from within the *Manage Device Bindings* page) and then navigate to the *View Discovered Devices* page to view the listing of all Dynamic Devices discovered in the system.

How do I write a program that uses Dynamic Device Discovery

These procedures assume the NetLinx developer does not have the Manufacturer device information necessary at the time of the initial setup. For more detailed UI information, refer to the *Manage Other Devices - Manage Device Bindings* section on page 85. For information on the referenced NetLinx calls, refer to the NetLinx Keywords Help file (found within NetLinx Studio).

1. Decide whether the application interface is to be Dynamic or Static bound and how the device will be connected to the system (Serial, IP, IR, etc).
   - Refer to page 87 for a definition of Static and Dynamic Application devices.

IP devices cannot be statically bound because they do not have an associated NetLinx D:P:S port value to associate with the application device.

2. To configure a Static application interface:
   - Add the NetLinx STATIC_PORT_BINDING API call to the section of the NetLinx program (FIG. 67 on page 86) containing the: Duet Virtual Device D:P:S, the NetLinx physical device D:P:S, the Duet Device type constant, and the associated friendly name string.

     - ***STATIC_PORT_BINDING*** designates an application device along with its SDK class and the physical interface it is bound to. The complete API is:

     ```
     STATIC_PORT_BINDING (DEV duetDevice,  DEV netlinxDevice,  char[]
     deviceType, char[] friendlyName,  integer polled)
     ```

   - Determine whether the physical device D:P:S should be polled to discover the connected devices. ***Only serial ports should be polled. Polled is a boolean integer which is part of the NetLinx AXI file.***
3. To configure a Dynamic application interface:
   - Add the DYNAMIC_APPLICATION_DEVICE API call to the section of the NetLinx program (FIG. 67 on page 86) containing the Duet Virtual Device D:P:S, the Duet Device type constant, and the associated friendly name string.

     - ***DYNAMIC_APPLICATION_DEVICE*** specifies a Duet device that is completely dynamic. A dynamically discovered device matching the specified deviceType could be bound to the duetDevice from anywhere in the system.

     ```
     DYNAMIC_APPLICATION_DEVICE (DEV duetDevice,  char[] deviceType,
     char[] friendlyName)
     ```

   - Add the DYNAMIC_POLLED_PORT API call for any NetLinx physical device D:P:S's that should be polled to discover connected devices.

     - ***DYNAMIC_POLLED_PORT*** designates a NetLinx serial port that should be polled for dynamic device detection. This API must be called for each serial port that can dynamically have a device plugged into it.

     ```
     DYNAMIC_POLLED_PORT (DEV netlinxDevice)
     ```

4. Write the remainder of the NetLinx application to communicate with the device via the Duet Virtual Device (D:P:S) using the Standard NetLinx API for that device type.
5. Compile the program file and then download it to the target Master via the **Tools > File Transfer** dialog.
6. Run the NetLinx application on the target Master.

How do I configure a Run-time installation

To utilize Dynamic binding, execute step 1 then step 2 then proceed to Step 3.

To utilize Static binding, execute step 2 then step 1 because the static bindings will try to bring up the Duet module as soon as the device is discovered. The module should be already available on the Master.

1. Connect the device to the system.
   - If the device is a DDD enabled Serial or IP device, then the device will be automatically discovered and show up in the Master's View Discovered Devices UI page under Manage Other Devices. (FIG. 70 on page 88).
   - If the device is not DDD enabled and/or cannot be automatically discovered (ex. IR device) the installer must enter the device information into the Master via the User Defined Device Web page under manage Other Devices. (FIG. 72 on page 89)
2. Verify the appropriate Duet module is available.

- If the Master is connected to the Internet, the **Module Search via Internet** button (FIG. 65 on page 80) can be enabled (*via toggling*).
- From within the View Discovered Devices UI page, click the **Search** button adjacent to the appropriate device to begin the search of an appropriate module.
- Any available modules on either the amx.com, AMX's partner website, or within the physical device itself are downloaded to the Master and then displayed back within the Select Device Module page (FIG. 71 on page 89). The discovered device is then shown with an adjacent listing of available modules ranked with associated "match" score.

  - The location of these modules can be either indeterminate (in which case they will reside on the amx.com website) or in some cases be required by the manufacturer to reside in their own specific source location (such as the manufacturer's own website or found within the target unit itself).
- The installer can then select which module to use with that discovered device by selecting the corresponding radio box and then clicking the upper-left **Save** button. This action then returns the installer back to the *View Discovered Devices* page.

NOTE

If the installer has the Duet module on a PC, the file can be downloaded to the Master via the Manage Device Modules section of the Manage Other Devices web page (FIG. 65 on page 80).

3. For Dynamically bound modules:
   - Begin the process of binding the Dynamic application device with the newly discovered physical device by navigating to the **Manage Other Devices > Manage Device Bindings** page. Dynamic application devices that have not been bound to a physical device display a **Bind** button.
   - Click the **Bind** button adjacent to the desired device.
   - From the secondary window, choose the appropriate physical device from the listing of all available unbound physical devices which matches the application device's Device SDK class type (FIG. 69 on page 87).

The Duet Module is started immediately after being "bound," which then causes an ONLINE event to be received by the NetLinx program for the Duet Virtual device.

Accessing an SSL-Enabled Master via an IP Address

Once the target Master has been fully configured with an SSL certificate, user/group access rights, and System level security parameters, the administrator (or comparably authorized user) can decide to require additional security on the Master by making any consecutive access to the Master be done via a HTTPS (*a secure version of HTTP communication*). Refer to the*Setting the Master's Port Configurations* section on page 61 for more information on this process.

1. Launch a web browser.
2. Enter the IP Address of the target Master into the web browser's *Address* field, but preface this information with the word **https** (***ex: https://198.198.99.99***). This https is used to communicate with the target Master via the pre-configured HTTPS/SSL Port.
3. Press **Enter** to begin the communication process between the target Master and your computer.
4. The user is then presented with a Security Alert popup window and Certificate information (FIG. 73).

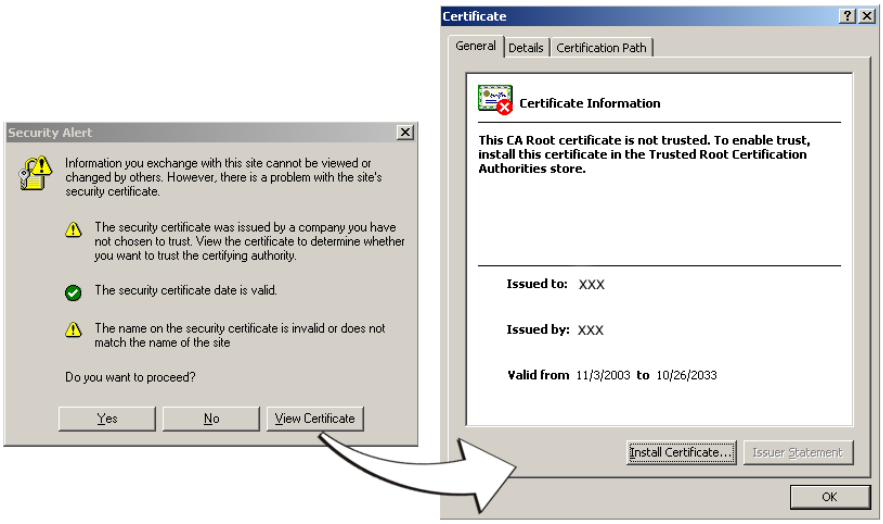


FIG. 73 Security Alert and Certificate popups

NOTE

The above alert only appears if an SSL Server Certificate has been installed on the target Master, the SSL Enable options has been enabled, from within the Enable Security window of the Security tab, and there is a problem with the site's certificate.

Problems with the certificate can result from:

- The default AMX certificate, self generated, or self-signed certificate has not been approved by a CA.
- The above mentioned certificates are not part of that computer's web browser list of trusted sites. This changes after the certificate is installed into the user's browser list of trusted sites.
- The date period given to the certificate has expired. CA-approved certificates typically come with a 2 year window of validity. Self generate certificates come defaulted with a 30 year window of validity (FIG. 73).
- The name on the security certificate site information doesn't match the domain name of the target Master.

5. Click the **View Certificate** button on the Security Alert popup to view more detailed information about the certificate. A secondary Certificate popup window is then displayed.
6. Review the information presented within the certificate and if you trust that both the site and certificate information are correct, click the **Install Certificate** button to begin installing the certificate into computer's web browser list of trusted sites.
7. The user is then presented with a Certificate Import Wizard that begins the process of adding the certificate (FIG. 74).

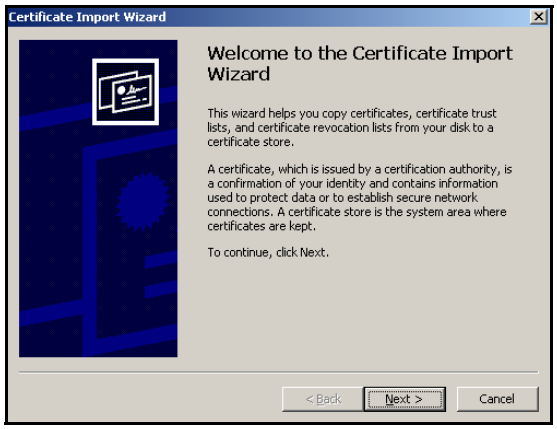


FIG. 74 Certificate Import Wizard

8. Click **Next** to proceed with the certificate importation process.

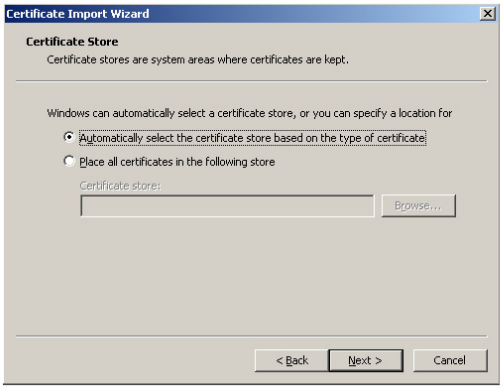


FIG. 75 Certificate Import Wizard- storing the certificate

9. Click **Next** to automatically use the default certificate store settings and locations (FIG. 75).
10. Click **Finish** button to finalize the certificate installation process.
11. Click **Yes**, from the next popup window to *"...ADD the following certificate to the Root Store?"*.
12. Click **OK** from the *Import was successful* popup window.
13. To close the still open *Certificate* popup window click **OK**.
14. To close the still open *Security Alert* popup window, click **Yes**.
15. From the *Network Password* window, click the down arrow from the *username* field to select a username.
16. Enter a valid password into the *password* field.
17. Click the *save password* check mark field to have the browser remember this password during consecutive login sessions.
18. Click **OK** to access the target Master.
19. The first page displayed within the open browser window is the *Manage WebControl Connections* page.

Using your NetLinx Master to control the G4 panel

Refer to the specific panel instruction manual for detailed information on configuring and enabling WebControl. 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.

Once the Master's IP Address has been set through NetLinx Studio version 2.4 or higher:

1. Launch the web browser.

NOTE

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

2. Enter the IP Address of the target Master (***ex: http://198.198.99.99***) into the web browser's *Address* field.
3. Press the **Enter** key on the keyboard to begin the communication process between the target Master and your computer.
   - Initially, the Master Security option is disabled (from within the **System Security** page) and no username and password is required for access or configuration.
   - Both HTTP and HTTPS Ports are enabled by default (via the **Manage System** > **Server** page).
   - If the Master has been previously configured for secured communication, click **OK** to accept the AMX SSL certificate (*if SSL is enabled*) and then enter a valid username and password into the fields within the *Login* dialog.
4. Click **OK** to enter the information and proceed to the Master's Manage WebControl Connections window.
5. Enter a valid username and password into the fields within the Login dialog.
6. Click **OK** to enter the information and proceed to the Master's Manage WebControl Connections window.
7. This Manage WebControl Connections page (FIG. 76) is accessed by clicking on the **Manage connections** link (*within the Web Control section within the Navigation frame*). Once activated, this page displays links to G4 panels running the latest G4 Web Control feature (*previously setup and activated on the panel*).

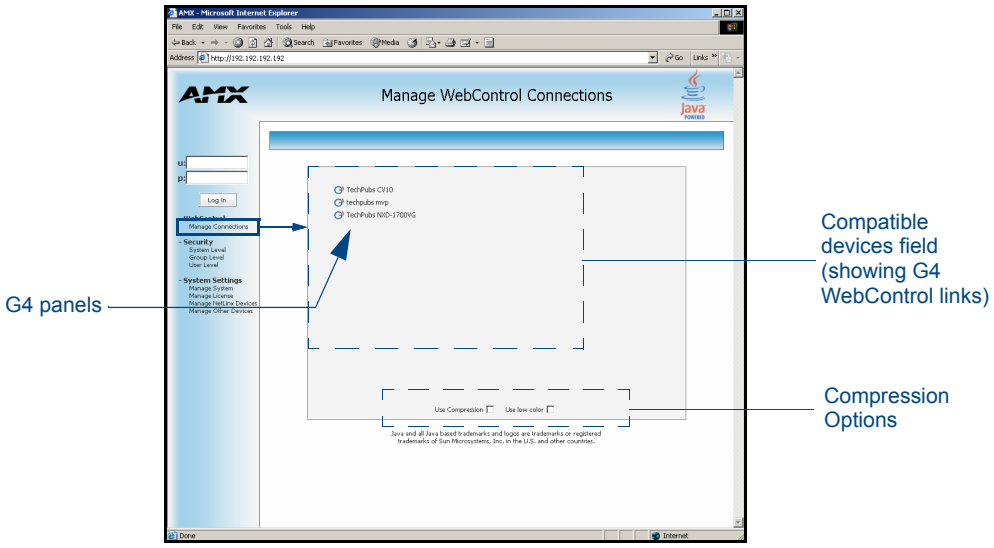


FIG. 76 Manage WebControl Connections page (populated with compatible panels)

8. Click on the G4 panel name link associated with the target panel. A secondary web browser window appears on the screen (FIG. 77).

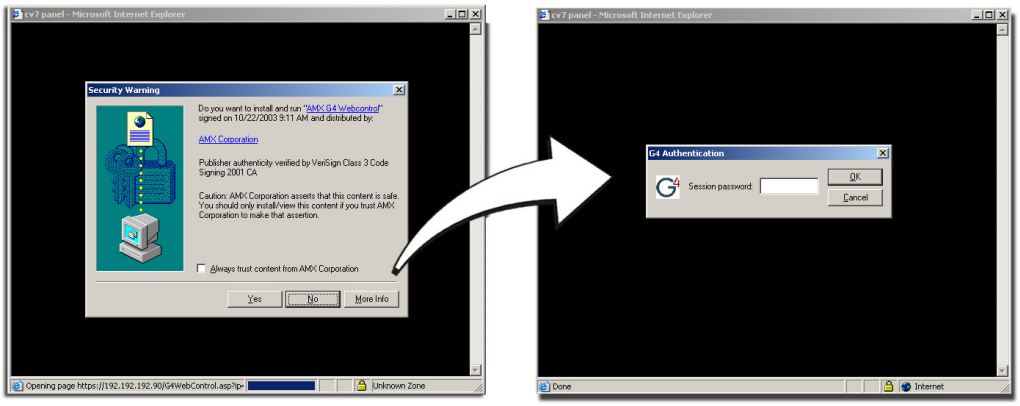


FIG. 77 WebControl VNC installation and Password entry screens

9. 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 WebControl application is sent by the panel to the computer that is used for communication. Once the application is installed, this popup no longer appears. This popup only appears if connecting to the target panel using a different computer.

10. Some circumstances might open a Connection Details dialog (FIG. 78) requesting a VNC Server IP Address. This is not the IP of the Master but of the target touch panel. Depending on which method of communication you are using, it can be found in either the:

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

  If this field does not appear, continue to step 11.

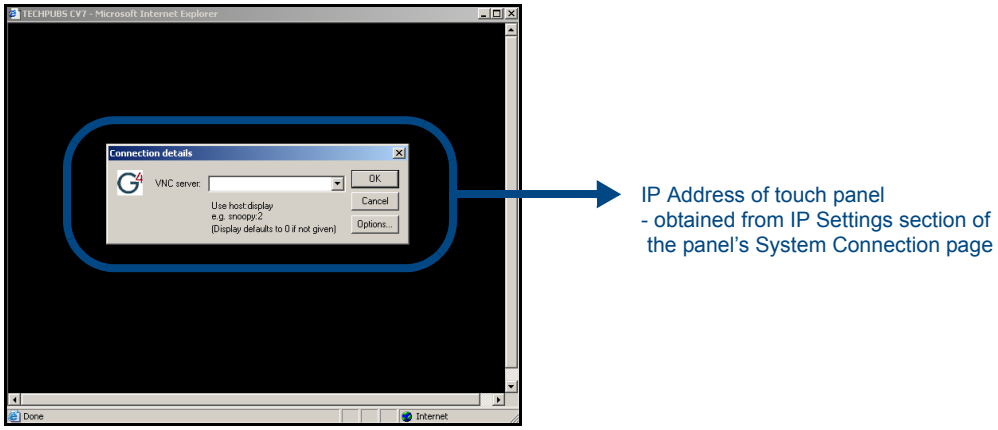


FIG. 78 Connection Details dialog

11. If a WebControl password was setup on the G4 WebControl page, a G4 Authentication Session password dialog box appears on the screen within the secondary browser window.

12. Enter the WebControl session password into the Session *Password* field (FIG. 77). *This password was previously entered into the Web Control Password field within the G4 Web Control page on the panel.*

13. Click **OK** to send the password to the panel and begin the session. A confirmation message appears stating *"Please wait, Initial screen loading..".*

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

What to do when a Certificate Expires

Self-generated certificates have a duration period of approximately 30 years. Most externally requested CA certificates are generally valid for a period of approximately 1 - 5 years.

The only way to avoid a CA certificate becoming invalid due to a time expiration is to request a new certificate from your current CA.

Refer to the*Server - Creating a Request for an SSL Certificate* section on page 67 for more information on how to request an externally generated certificate.

NetLinx Security with a Terminal Connection

Overview

NetLinx Masters currently have built-in security capabilities. They require a user entering a valid username and password to access the NetLinx System's Telnet, HTTP, ICSP, and FTP services.

The security capabilities are configured and applied via a Telnet connection or the NetLinx Master's RS-232/ USB terminal interface (the RS232/USB Configuration Port).

Always use the RS232/USB Configuration Port when entering potentially sensitive security information. The Telnet server interface exposes this security information to the LAN in clear text format, which could be intercepted by an unauthorized LAN client. Using the RS232/USB Configuration Port offers security during the configuration of the database due to the physical proximity of the user to the system.

NetLinx Security Features

NetLinx security allows a qualified user to define access rights for users or groups.

A "User" represents a single potential client of the NetLinx Master, while a "Group" represents a logical collection of users. Any properties possessed by groups (i.e., access rights, directory associations, etc.) are inherited by all the members of the group.

The following table lists the NetLinx features that the administrator (or other 'qualified' user) may grant or deny access to.

NetLinx Security Features	
NetLinx Master Security Configuration	The user has access to the security configuration commands of the Master. Only those users with security configuration access rights granted will have access to the security configuration commands.
Telnet Security	The user has access to the Telnet server functionality. All basic commands are available to the user.
Terminal (RS232/USB) Security	The user has access to the Terminal server functionality through the USB connector. All basic commands are available to the user.
HTTP (web server) Security	The user has access to the HTTP server functionality. Directory associations assign specific directories/files to a particular user.
FTP Security	The user has access to the FTP server functionality. Only the administrator account has access to the root directory; all other 'qualified' clients are restricted to the /user/ directory and its 'tree'.
ICSP	The user has access to the ICSP communication functionality. Communication and encryption rights are available to an authorized user.
ICSP Encryption	The user has access to the ICSP data encryption functionality. Enabling encryption of ICSP data requires that both: - AMX hardware or software communicating with the target Master provide a valid username and password. - All communication is encrypted.

Initial Setup via a Terminal Connection

Security administration and configuration is done via a Terminal communication through the RS232/USB Configuration Port on the NetLinx Master. If connecting to the target Master via the ***TCP/IP (Winsock)*** option, some command sets (such as the security setup) will not be available. ***If a valid IP connection method has been made to the Master, making changes to the parameters via the browser-based UI pages is highly recommended.***

NOTE

*Although these procedures are written for a Terminal connection, a user can also connect to a Master via a Telnet connection. Do this by going to **Start > Run**, enter **cmd** within the Run dialog's Open field and click **OK**. Then from within the CMD command prompt use the IP Address info to type >**telnet XXX.XXX.XXX.XXX** <Enter>.*

Establishing a Terminal connection via the RS-232/USB Configuration Port

1. Launch the HyperTerminal application from its' default location (**Start** > **Programs** > **Accessories** > **Communications**).
2. Apply power to the NetLinx Master and allow it to boot up.
3. Connect the USB port from your computer to the USB connector on the NetLinx Master.
4. Enter any text into the *Name* field of the HyperTerminal Connection Description dialog window and click **OK** when done.
5. From the *Connect Using* field, click the down-arrow and select the PC COM port being used for communication by the target Master and click **OK** when done.
6. From the *Bits per second* field, click the down-arrow and select the baud rate being used by the target Master.
   - Configure the remaining communication parameters as follows: Data Bits: **8**, Parity: **None**, Stop bits: **1**, and **Flow control: None** *(default is Hardware)*.
   - Click **OK** to complete the communication parameters and open a new Terminal window.
7. Type **echo on** to view the characters while entering commands. If that does not work, press the **Enter** key on your keyboard.

NOTE

It is very important that a user properly execute the 'logout' command prior to disconnecting from a Master. Simply removing the USB connector from the Configuration Port maintains a logged-in status until either a return to logout via a new session or reboot of the target Master.

Accessing the Security configuration options

1. In the Terminal session, type **help security** to view the available security commands. Here is a listing of the security help:

```
---- These commands apply to the Security Manager and Database ----
logout                  Logout and close secure session
setup security          Access the security setup menus
```

NOTE

The 'help security' and 'setup security' functions are only available via a direct RS232/USB connection. They are not available under telnet (such as via a TCP/IP (Winsock) connection).

2. Type **setup security** to access the Main Security Menu, shown below:

```
>setup security

--- These commands apply to the Security Manager and Database ----
 1) Set system security options for NetLinx Master
 2) Display system security options for NetLinx Master
 3) Add user
 4) Edit user
 5) Delete user
 6) Show the list of authorized users
 7) Add group
 8) Edit group
 9) Delete group
10) Show list of authorized groups
11) Set Telnet Timeout in seconds
```

```
12) Display Telnet Timeout in seconds
      13) Make changes permanent by saving to flash

Or <ENTER> to return to previous menu

Security Setup ->
```

3. The Main Security Menu shows a list of choices and a prompt. To select one of the listed choices, simply enter the number of the choice (**1** - **13**) at the prompt and press **Enter**.

NOTE

Options 14 and 15 are only visible to the System Administrator. Refer to theTable , "Main Security Menu (Cont.)," on page 110.

4. Each option in the Main Security Menu displays a submenu specific to that option.

The following subsection describe using each of the Main Security Menu options. For a detailed description of each option in the Main Security Menu, refer to *Main Security Menu* section on page 109.

Option 1 - Set system security options for NetLinx Master (Security Options Menu)

Type **1** and <Enter> at the Security Setup prompt (at the bottom of the Main Security Menu) to display the **Security Options Menu**.

The Security Options Menu sets the "global" options for the NetLinx Master. It is accessed by the Set Security system options of the Main Security Menu. This first thing that will happen is you will be asked one of two questions. If NetLinx Master security is enabled, you will see the following:

```
NetLinx Master security is Enabled

Do you want to keep NetLinx Master security enabled? (y or n):
```

- If you answer **y** for yes, security will remain enabled and you will be taken to the Security Options Menu.
- If you answer **n** for no, all security settings (except FTP security) will be disabled and you will be taken back to the Main Security Menu.

If NetLinx Master security is not enabled, you will see the following:

```
NetLinx Master security is Disabled
Do you want to enable security for the NetLinx Master? (y or n):
```

- If you answer **y** for yes, security will be enabled and you will be taken to the Security Options Menu.
- If you answer **n** for no, all security settings (except FTP security) will remain disabled and you will be taken back to the Main Security Menu.

The Security Options Menu is displayed as follows:

```
Select to change current security option
 1) Terminal (RS232) Security.................. Enabled
 2) HTTP Security.............................. Disabled
 3) Telnet Security............................ Enabled
 4) Configuration Security..................... Enabled
 5) ICSP Security.............................. Enabled
 6) ICSP Encryption Required................... Enabled
Or <ENTER> to return to previous menu

Security Options ->
```

The selection listed will display what the current settings. To change an option, select the number listed next to the option.

For example, if selection **2)** is selected (from the Select to change current security option listing), the security options for the Master are listed and HTTP Security becomes enabled. The listing is then displayed as follows:

```
Select to change current security option
 1) Terminal (RS232) Security.................. Enabled
 2) HTTP Security.............................. Enabled
 3) Telnet Security............................ Enabled
 4) Configuration Security..................... Enabled
```

```
 5) ICSP Security.............................. Enabled
 6) ICSP Encryption Required................... Enabled
Or <ENTER> to return to previous menu

Security Options ->
```

Each selection simply toggles the security setting selected. Press <Enter> to exit the menu and return to the Main Security Menu.

NOTE

Changes made to the target Master from within the Terminal window are not reflected within the web browser, until the Master is rebooted and the web browser connection is refreshed.
Any changes made to the Master, from within the web browser are instantly reflected within the Terminal session without the need to reboot.

The items in the Security Options Menu are described below:

Security Options Menu	
Command	**Description**
`1) Terminal (RS232/USB) Security (Enabled/Disabled)`	This selection enables/disables Terminal Security (through the USB connector). If Terminal Security is enabled, a user must have sufficient access rights to login to a Terminal session.
`2) HTTP Security (Enabled/Disabled)`	This selection enables/disables HTTP (Web Server) Security. If HTTP Security is enabled, a user must have sufficient access rights to browse to the NetLinx Master with a Web Browser.
`3) Telnet Security (Enabled/Disabled)`	This selection enables/disables Telnet Security. If Telnet Security is enabled, a user must have sufficient access rights to login to a Telnet session.
`4) Configuration Security (Enabled/Disabled)`	This selection enables/disables Configuration Access rights for the target Master. If the Configuration Security is enabled, a user must have sufficient access rights to access the Main Security Menu and make changes to the Master's security parameters.
`5) ICSP Security (Enabled/Disabled)`	This selection enables/disables security of ICSP data being transmitted between the target Master and external AMX components (software and hardware such as TPD4 and a Modero Touch Panel).
`6) ICSP Encryption Required (Enabled/Disabled)`	This selection enables/disables the need to require encryption of the ICSP communicated data. If enabled: - All communicating AMX components must authenticate with a valid username and password before beginning communication with the Master. - All communication must be encrypted.

Option 2 - Display system security options for NetLinx Master

Type **2** and <Enter> at the Security Setup prompt (at the bottom of the Main Security Menu) to display the current security options, and their current state (`Enabled/Disabled`). For example:

```
Master Security.....................Disabled
Terminal............................Disabled
HTTP................................Disabled
Telnet..............................Disabled
Configuration.......................Disabled
ICSP................................Disabled
ICSP Encryption.....................Disabled

Press <ENTER> key to continue
```

Option 3 - Add user

1. Type **3** and <Enter> at the Security Setup prompt (at the bottom of the Main Security Menu) to create a new user account. A sample session response is:

```
The following users are currently enrolled:
administrator
Fred
techpubs

Enter username ->
```

2. At the **Enter username** prompt, enter a new username (for example "techpubs"). A username is a valid character string (4 - 20 alpha-numeric characters) defining the user. This string is ***case sensitive***. Each username must be unique.
3. Press <Enter> to enter the new username. The session then prompts you for a password for the new user.
4. Enter a password for the new user. A password is a valid character string (4 - 20 alpha-numeric characters) to supplement the username in defining the potential client. This string is also ***case sensitive***.
5. The session then prompts you to verify the new password. Enter the password again, and press <Enter>.
6. Assuming the password was verified, the session then displays the Edit User menu (*see below*).

Option 4 - Edit User

1. Type **4** and <Enter> at the Security Setup prompt (at the bottom of the Main Security Menu) to edit an existing user account. A sample session response is:

```
Select from the following list of enrolled users:

1) administrator
2) NetLinx
3) techpubs
4) Pat
Select User ->
```

2. Select the user account (1-X) that you want to edit, and press <Enter> to display the Edit User Menu (described below).

Any changes made via the Edit User menu will affect the selected user account.

Edit User Menu

The Edit User Menu is accessed whenever you enter the Add user, or Edit user selections from the Main Security Menu. The Edit User Menu is displayed as follows:

```
Please select from the following options:

  1) Change User Password
  2) Change Inherits From Group
  3) Add Directory Association
  4) Delete Directory Association
  5) List Directory Associations
  6) Change Access Rights
  7) Display User Record Contents
Or <ENTER> to return to previous menu

Edit User ->
```

Each selection (1-7) accesses the named option. Press <Enter> by itself to exit the menu and return to the Main Security Menu.

The Edit User Menu options are described in the following table:

Edit User Menu

Command	Description
1) Change User Password	This selection prompts you to enter the new password (twice) for the user. Once the new password is entered, the user must use the new password from that point forward.

Edit User Menu (Cont.)	
Command	**Description**
2) Change Inherits From Group	This selection will display the current group the user is assigned to (if any). It will then display a list of current groups and prompts you to select the new group.
3) Add Directory Association	This selection will display any current Directory Associations assigned to the user, and then will prompt you for a path for the new Directory Association.
4) Delete Directory Association	This selection will display any current Directory Associations assigned to the user, and then will prompt you to select the Directory Association you want to delete.
5) List Directory Associations	This selection will display any current Directory Associations assigned to the user.
6) Change Access Rights	This selection will display access the Access Rights Menu for the user, which allows you to set the rights assigned to the user.
7) Display User Record Contents	This selection will display the group the user is assigned to and the current Access Rights assigned to the user.

Access Rights Menu

The Access Rights Menu is accessed whenever you select Change Access Rights (option **6**) from the Edit User Menu, or Change Access Rights from the Edit Group Menu. The Access Rights Menu is displayed as follows:

```
Select to change current access right
  1) Terminal (RS232) Access.................. Disabled
  2) Admin Change Password Access............. Disabled
  3) FTP Access............................... Disabled
  4) HTTP Access.............................. Enabled
  5) Telnet Access............................ Enabled
  6) Configuration Access..................... Enabled
  7) ICSP Access.............................. Enabled
  8) ICSP Encryption Required................. Enabled
Or <ENTER> to return to previous menu
Set Rights ->
```

The above listing displays the current access rights. Entering a selection value simply toggles the access right selected (if for example you enter **4**, the HTTP Access rights toggle from disabled to enabled upon a refresh of the listing).

Press <Enter> to exit the menu and return to the previous menu. The Access Rights Menu is described in the following table:

Access Rights Menu	
Command	**Description**
1) Terminal (RS232/USB) Access (Enable/Disable)	Enables/disables Terminal Access through the USB connector. The account has sufficient access rights to login to a Terminal session if this option is enabled.
2) Admin Change Password Access (Enable/Disable)	Enables/disables Administrator Change Password Access. The account has sufficient access rights to change the administrator password if this option is enabled.
3) FTP Access (Enable/Disable)	Enables/disables FTP Access. The account has sufficient access rights to access the NetLinx Master's FTP Server if this option is enabled.
4) HTTP Access (Enable/Disable)	This selection enables/disables HTTP (Web Server) Access. The account has sufficient access rights to browse to the NetLinx Master with a Web Browser if this option is enabled.
5) Telnet Access (Enable/Disable)	This selection enables/disables Telnet Access. The account has sufficient access rights to login to a Telnet session if this option is enabled.

Access Rights Menu (Cont.)	
Command	**Description**
6) Configuration Access (Enable/Disable)	This selection enables/disables Configuration Access rights for the target Master. The account has sufficient access rights to access the Main Security Menu if this option is enabled.
5) ICSP Security (Enabled/Disabled)	This selection enables/disables ICSP communication access. The account has sufficient access rights to initiate ICSP data communication.
6) ICSP Encryption Required (Enabled/Disabled)	This selection enables/disables the need to require encryption of the ICSP communicated data. If enabled: - All communicating AMX components must authenticate with a valid username and password before beginning communication with the Master. - All communication must be encrypted.

Option 5 - Delete user

1. Type **5** and <Enter> at the Security Setup prompt (at the bottom of the Main Security Menu) to delete an existing user account. A sample session response is:

```
Select from the following list of enrolled users:
1) administrator
2) NetLinx
3) techpubs
4) Pat
Select User ->
```

2. Enter the value associated to the user you want to delete and press <Enter>. This action deletes the user account and returns you to the Security Setup menu.

NOTE

Changes made to the target Master from within the Terminal window are not reflected within the web browser, until the Master is rebooted and the web browser connection is refreshed. Any changes made to the Master, from within the web browser are instantly reflected within the Terminal session without the need to reboot.

Option 6 - Show the list of authorized users

1. Type **6** and <Enter> at the Security Setup prompt (at the bottom of the Main Security Menu) to view a list of currently enrolled users.
2. Press <Enter> to return to the Security Setup menu.

Option 7 - Add Group

1. Type **7** and <Enter> at the Security Setup prompt (at the bottom of the Main Security Menu) to add a group account. A sample session response is:

```
The following groups are currently enrolled:
administrator

Enter name of new group:
```

2. Enter a name for the group. A group name is a valid character string (4 - 20 alpha-numeric characters) defining the group. This string is ***case sensitive***, and each group name must be unique.
3. Press <Enter> to display the following Edit Group menu:

Edit Group Menu

```
Please select from the following options:
1) Add Directory Association
2) Delete Directory Association
3) List Directory Associations
4) Change Access Rights
5) Display Access Rights
```

```
Or <ENTER> to return to previous menu

      Edit Group ->
```

Edit Group Menu: Add directory association

1. At the Edit Group prompt, type **1** to add a new directory association. A sample session response is:

```
There are currently no directories associated with this account
New directory:
```

A Directory Association is a path that defines the directories and/or files that a particular user or group can access via the HTTP (Web) Server on the NetLinx Master. This character string can range from 1 to 128 alpha-numeric characters. This string is ***case sensitive***. This is the path to the file or directory you want to grant access. Access is limited to the user (i.e. doc:user) directory of the Master. All subdirectories of the user directory can be granted access.

A single '/' is sufficient to grant access to all files and directories in the user directory and it's sub-directory. The '*' wildcard can also be added to enable access to all files. All entries should start with a '/'. Here are some examples of valid entries:

Path	Notes
`/`	Enables access to the user directory and all files and subdirectories in the user directory.
`/*`	Enables access to the user directory and all files and subdirectories in the user directory.
`/user1`	If `user1` is a file in the user directory, only the file is granted access. If `user1` is a subdirectory of the user directory, all files in the `user1` and its sub-directories are granted access.
`/user1/`	`user1` is a subdirectory of the user directory. All files in the `user1` and its sub-directories are granted access.
`/Room1/iWebControlPages/*`	`/Room1/iWebControlPages` is a subdirectory and all files and its subdirectories are granted access.
`/results.txt`	`results.txt` is a file in the user directory and access is granted to that file.

By default, all accounts that enable HTTP Access are given a '`/*`' Directory Association if no other Directory Association has been assigned to the account.

When you are prompted to enter the path for a Directory Association, the NetLinx Master will attempt to validate the path. If the directory or file is not valid (i.e. it does not exist at the time you entered the path), the NetLinx Master will ask you whether you were intending to grant access to a file or directory. From the answer, it will enter the appropriate Directory Association. The NetLinx Master will not create the path if it is not valid. That must be done via another means, most commonly by using an FTP client and connecting to the FTP server on the NetLinx Master.

Edit Group menu: Delete directory association

1. At the Edit Group prompt, type **2** to delete an existing directory association. A sample session response is:

```
Select a directory association from the following:
1) /directory1/*
2) /directory2/*
Select Directory ->
```

2. Select the directory association to be deleted, and press <Enter> to delete the directory association, and return to the Edit Group menu.

Edit Group menu: List directory associations

1. At the Edit Group prompt, type **3** to list all existing directory associations. A sample session response is:

```
The following directory associations are enrolled:
/directory1/*
/directory2/*

Press <ENTER> key to continue
```

2. Press <Enter> to return to the Edit Group menu.

Edit Group menu: Change Access Rights

1. At the Edit Group prompt, type **4** to change the current access rights for the selected group account. A sample session response is:

```
Select to change current access right
 1) Terminal (RS232) Access.................. Disabled
 2) Admin Change Password Access............. Disabled
 3) FTP Access............................... Disabled
 4) HTTP Access.............................. Enabled
 5) Telnet Access............................ Enabled
 6) Configuration Access..................... Enabled
 7) ICSP Access.............................. Enabled
 8) ICSP Encryption Required................. Enabled
Or <ENTER> to return to previous menu

Set Rights ->
```

2. Each selection simply toggles the security setting selected. <Enter> is entered by itself to exit the menu and return to the Main Security Menu.

NOTE

Changes made to the target Master from within the Terminal window are not reflected within the web browser, until the Master is rebooted and the web browser connection is refreshed.
Any changes made to the Master, from within the web browser are instantly reflected within the Terminal session without the need to reboot.

Edit Group menu: Display Access Rights

1. At the Edit Group prompt, type **5** to view the current access rights for the selected group account. A sample session response is:

```
Terminal (RS232)...................Disabled
Admin. Password Change.............Disabled
FTP................................Disabled
HTTP...............................Disabled
Telnet.............................Disabled
Configuration......................Disabled
ICSP...............................Disabled

Press <ENTER> key to continue
```

2. Press <Enter> to return to the Edit Group menu.

Option 8 - Edit Group

1. Type **8** and <Enter> at the Security Setup prompt (at the bottom of the Main Security Menu) to edit an existing group account. A sample session response is:

```
Select from the following list:
1) administrator
2) Group 1
3) Group 2
Select group ->
```

2. Select a group from the list of currently enrolled groups and press <Enter> to open the Edit Group Menu. This is the same Edit Group Menu that was access via the Add Group option:

```
1) Add Directory Association
2) Delete Directory Association
3) List Directory Associations
4) Change Access Rights
5) Display Access Rights
      Or <ENTER> to return to previous menu

Edit group ->
```

This menu is described on the previous pages (see *Edit Group Menu* section on page 105*)*.

Option 9 - Delete Group

1. Type **9** and <Enter> at the Security Setup prompt (at the bottom of the Main Security Menu) to delete an existing group account. A sample session response is:

```
Select from the following list:
1) Group 1
2) Group 2
Select group ->
```

2. Select the group account to be deleted, and press <Enter> to delete the group and return to the Security Setup menu.

Changes made to the target Master from within the Terminal window are not reflected within the web browser, until the Master is rebooted and the web browser connection is refreshed.
Any changes made to the Master, from within the web browser are instantly reflected within the Terminal session without the need to reboot.

Option 10 - Show List of Authorized Groups

1. Type **10** and <Enter> at the Security Setup prompt (at the bottom of the Main Security Menu) to display a list of all authorized group accounts. A sample session response is:

```
The following groups are currently enrolled:
administrator
Group 1

Press <ENTER> key to continue
```

2. Press <Enter> to return to the Security Setup Menu.

Option 11 - Set Telnet Timeout in seconds

This feature is disabled after the installation of firmware build 130 or higher onto your target Master.

1. Type **11** and <Enter> at the Security Setup prompt (at the bottom of the Main Security Menu) to set the Telnet Timeout value, in seconds. A sample session response is:

```
Specify Telnet Timeout in seconds:
```

2. Enter the number of seconds before you want The Telnet session to timeout, and press <Enter> to return to the Security Setup Menu.

Option 12 - Display Telnet Timeout in seconds

This feature is disabled after the installation of firmware build 130 or higher onto your target Master.

1. Type **12** and <Enter> at the Security Setup prompt (at the bottom of the Main Security Menu) to view the current Telnet Timeout value (in seconds). A sample session response is:

```
Telnet Timeout is 10 seconds.
```

2. Press <Enter> to return to the Security Setup Menu.

Option 13 - Make changes permanent by saving to flash

When changes are made to the security settings of the Master, they are initially only changed in RAM and are not automatically saved permanently into flash. This selection saved the current security settings into flash. Also, if you attempt to exit the Main Security Menu and the security settings have changed but not made permanent, you will be prompted to save the settings at that time.

Type **13** and <Enter> at the Security Setup prompt to (permanently) save all changes to flash.

NOTE

Changes made to the target Master from within the Terminal window are not reflected within the web browser, until the Master is rebooted and the web browser connection is refreshed.
Any changes made to the Master, from within the web browser are instantly reflected within the Terminal session without the need to reboot.

Main Security Menu

The Main Security menu is described below:

Main Security Menu	
Command	**Description**
1) Set system security options for NetLinx Master	This selection will bring up the Security Options Menu that allows you to change the security options for the NetLinx Master (refer to the*Security Options Menu* section on page 102 for details). These are "global" options that enable rights given to users and groups. For instance, if you want to disable Telnet security for all users, you would simply go to this menu and disable Telnet security for the entire Master. This would allow any user, whether they have the rights to Telnet or not. These options can be thought of as options to turn on security for different features of the NetLinx Master.
2) Display system security options for NetLinx Master	This selection will display the current security options for the NetLinx Master.
3) Add user	This selection will prompt you for a username and password for a user you would like to create. After the user is added, you will be taken to the Edit User Menu to setup the new users rights (see the*Edit User Menu* section on page 103 for details).
4) Edit user	This selection will prompt you select a user. Once you have selected the user you want to edit, it will take you to the Edit User Menu so you can edit the user's rights (see the*Edit User Menu* section on page 103 for details).
5) Delete user	This selection will prompt you select a user to delete.
6) Show the list of authorized users	This selection displays a list of users.
7) Add group	This selection will prompt you for a group name fro a group you would like to create. After the group is added, you will be taken to the Edit Group Menu to setup the new users right (see the*Edit Group Menu* section on page 105 for details).
8) Edit group	This selection will prompt you select a group. After selecting the group you want to edit, it will take you to the Edit Group Menu so you can edit the group's rights (see the*Edit Group Menu* section on page 105 for details).
9) Delete group	This selection will prompt you select a group to delete. A group can only be deleted if there are no users assigned to that group.
10) Show list of authorized groups	This selection displays a list of groups.
11) Set Telnet Timeout in seconds	This selection allows you to set the time a telnet session waits for a user to login. When a Telnet client connects to the NetLinx Master, it is prompted for a username. If the client does not enter a users name for the length of time set in this selection, the session will be closed by the NetLinx Master.
12) Display Telnet Timeout in seconds	This selection allows you to display the time a telnet session waits for a user to login.

Main Security Menu (Cont.)	
Command	**Description**
13) Make changes permanent by saving to flash	When changes are made to the security settings of the Master, they are initially only changed in RAM and are not automatically saved permanently into flash. This selection saved the current security settings into flash. Also, if you attempt to exit the Main Security Menu and the security settings have changed but not made permanent, you will be prompted to save the settings at that time.
14) Reset Database (administrator only function)	These functions are only visible to administrators. If a user has been given "administrator rights", this additional menu option is displayed. This selection will reset the security database to its Default Security Configuration settings, erasing all users and groups that were added. This is a permanent change and you will be asked to verify this before the database is reset.
15) Display Database (administrator only function)	These functions are only visible to administrators. If a user has been given "administrator rights", this additional menu option is displayed. This selection will display the current security settings to the terminal (excluding user passwords). It also displays all users (minus passwords), their group assignment (if any) and their rights, as well as all groups and their rights.

Default Security Configuration

By default, the NetLinx Master will create the following accounts, access rights, directory associations, and security options.

```
Account 1:              User Name: administrator
Password:               password
Group:                  administrator
Rights:                 All
Directory Association: /*

Account 2:              User Name: NetLinx
Password:               password
Group:                  none
Rights:                 FTP Access
Directory Association: none

Group 1:                Group: administrator
Rights:                 All
Directory Association: /*

Security Options:       FTP Security Enabled
                        Admin Change Password Security Enabled
                        All other options disabled
```

- The ***administrator*** user account cannot be deleted or modified with the exception of its password. Only a user with "Change Admin Password Access" rights can change the administrator password.
- The ***NetLinx*** user account is created to be compatible with previous NetLinx Master firmware versions.
- The ***administrator*** group account cannot be deleted or modified.
- The FTP Security and Admin Change Password Security are always enabled and cannot be disabled.

Help menu

Type **help** at the prompt in the Telnet session to display the following help topics:

Help Menu Options

Command	Description
----- Help ----- <D:P:S>	(Extended diag messages are OFF) <D:P:S>: Device:Port:System. If omitted, assumes Master.
? or Help	Displays this list.
DATE	Displays the current date.
DEVICE HOLDOFF ON|OFF	Sets the Master to holdoff devices (i.e. does not allow them to report ONLINE) until all objects in the NetLinx program have completed executing the DEFINE_START section. If set to ON, any messages to devices in DEFINE_START will be lost, however, this prevents incoming messages being lost in the Master upon startup. When DEVICE_HOLDOFF is ON, you must use ONLINE events to trigger device startup SEND_COMMANDs. By default, DEVICE HOLDOFF is OFF to maintain compatibility with Axcess systems where **f** devices are initialized in DEFINE_START.
DEVICE STATUS <D:P:S>	Provides information about the specified device.
DNS LIST <D:P:S>	Displays the DNS configuration of a device.
DISK FREE	Displays the amount of free space on the disk.
ECHO ON|OFF	Enables/Disables echo of typed characters.
GET DEVICE HOLDOFF	Displays the state of the Master's device holdoff setting.
GET DUET MEMORY	Display the amount of memory allocated for Duet Java pool. This is the current Java memory heap size as measured in Megabytes. An example is a value of 5 = 5 MB.
GET IP <D:P:S>	Displays the IP configuration of a device.
HELP SECURITY	Displays security related commands.
IP STATUS	Provides information about NetLinx IP Connections.
MEM	Shows size of the largest block of available memory.
MSG ON|OFF	Enables/Disables extended diagnostic messages.
OFF [D:P:S or NAME,CHAN]	Turns off the specified channel.
ON [D:P:S or NAME,CHAN]	Turns on the specified channel.
PASS [D:P:S or NAME]	Puts the Session in pass mode to the specified device. • Mode is exited by ++ ESC ESC. • Display Format is set by ++ ESC n - If n is A, format = ASCII, D, format = Decimal, and H = Hex
PING [ADDRESS]	Pings an address (IP or URL). Specify -a option for reverse lookup.
PROGRAM INFO	Displays a list of program modules loaded.
PULSE [D:P:S or NAME,CHAN]	Pulses the specified channel.
REBOOT <D:P:S>	Reboots the device.
RELEASE DHCP	Releases the current DHCP lease.
ROUTE MODE DIRECT|NORMAL	Sets the Master-Master route mode.
SEND_COMMAND D:P:S or NAME,COMMAND	Sends the specified command to the device. The Command uses NetLinx string syntax. • Ex: send_command 1:1:1,"'This is a test',13,10" • Ex: send_command RS232_1,"'This is a test',13,10"
SEND_STRING D:P:S or NAME,STRING	Sends the specified string to the device.
SET DATE	Sets the current date.

Help Menu Options (Cont.)	
Command	**Description**
SET DNS <D:P:S>	Sets up the DNS configuration of a device.
SET DUET MEMORY	Set the amount of memory allocated for Duet Java pool. This is the current Java memory heap size as measured in Megabytes. This feature is used so that if a NetLinx program requires a certain size of memory be allotted for its currently used Duet Modules, it can be reserved on the target Master. Valid values are 1 - 16 for 32 MB systems and 1 - 48 for a 64 MB system. This setting does not take effect until the next reboot. ***Note:*** *If you are trying to accomplish this setting of the Duet Memory size via a NetLinx program, the program command "DUET_MEM_SIZE_SET(int)" should call REBOOT() following a set.*
SET FTP PORT	Enables/Disables the IP port listened to for FTP connections.
SET HTTP PORT	Sets the IP port listened to for HTTP connections.
SET HTTPS PORT	Sets the IP port listened to for HTTPS connections.
SET ICSP PORT	Sets the IP port listened to for ICSP connections.
SET ICSP TCP TIMEOUT	Sets the timeout period for ICSP and i!-WebControl TCP connections.
SET IP <D:P:S>	Setup the IP configuration of a device.
SET LOG COUNT	Sets the number of entries allowed in the message log.
SET SSH PORT	Sets the IP port listened to for SSH connections.
SET TELNET PORT	Sets the IP port listened to for Telnet connections.
SET THRESHOLD	Sets the Master's internal message thresholds.
SET TIMELINE LOOPCNT	Sets the Master's timeline/event max loopcount.
SET TIME	Sets the current time.
SET UDP BC RATE	Sets the UDP broadcast rate. A broadcast message is sent by the Master to allow devices to discover the Master. This command allows the broadcast frequency to be changed or eliminate the broadcast message.
SET URL <D:P:S>	Setup the initiated connection list URLs of a device.
SHOW COMBINE	Displays a list of devices, levels, and channels that are currently combined.
SHOW DEVICE <D:P:S>	Displays a list of devices connected and attributes.
SHOW LOG <START>	Displays the message log. <start> specifies message to begin the display. 'all' will display all messages.
SHOW MEM	Displays the memory usage for all memory types.
SHOW NOTIFY	Displays the Notify Device List (Master-Master).
SHOW REMOTE	Displays the Remote Device List (Master-Master).
SHOW ROUTE	Displays the Master's routing information.
SHOW SYSTEM <S>	Displays a list of devices in a system.
TCP LIST	Displays a list of active TCP connections.
TIME	Displays the current time.
URL LIST <D:P:S>	Displays the initiated connection list URLs of a device.

Logging Into a Session

Until Telnet security is enabled, a session will begin with a welcome banner.

```
Welcome to NetLinx v3.01.320 Copyright AMX Corp. 1999-2005
>
```

NOTE

The welcome banner is not displayed for Terminal sessions.
It is very important for a user properly execute the 'logout' command prior to disconnecting from a Master. Simply removing the USB connector from the Configuration Port maintains your logged-in status until you either return to logout via a new session or reboot the target Master.

When Terminal security is enabled, the user should type in the word **login** to then be prompted for a username and password before they will be allowed to access any commands available from Telnet. No welcome banner will be displayed until a valid login is made. When the session is started, the user will see a login prompt as seen below:

```
Login:
```

The user (Login) name is case sensitive. The username must be entered with the exact combination of upper and lower letters as was assigned to them by the security administrator. The username must be at least 4 characters long and no more than 20 characters. Any combination of letters, numbers, or other characters may be used.

The user would enter their username and then would be prompted for a password:

```
Login: User1
Password:
```

The password is case sensitive. The password must be entered with the exact combination of upper and lower letters as was assigned to them by the security administrator. The password must be at least 4 characters long and no more than 20 characters. Any combination of letters, numbers, or other characters may be used.

After the password is entered, if the password is correct you will see a welcome banner as shown below:

```
Login: User1
Password: *****
Welcome to NetLinx v3.01.320 Copyright AMX Corp. 1999-2005
>
```

If the password is incorrect, the following will be displayed:

```
Login: User1
Password: *****
Login not authorized. Please try again.
```

After a delay, another login prompt will be displayed to allow the user to try again. If after 5 prompts, the login is not done correctly the following will be displayed and the connection closed:

```
Login not allowed. Goodbye!
```

If a user opens a connection but does not enter a username or password (i.e. they just sit at a login prompt), the connection will be closed after 1 minute.

Logout

The logout command will log the user out of the current secure telnet session. For a Terminal session, the user will be logged out and to access Terminal commands again the user will first have to login.

NOTE

It is very important for a user properly execute the 'logout' command prior to disconnecting from a Master. Simply removing the USB connector from the Configuration Port maintains your logged-in status until you either return to logout via a new session or reboot the target Master.

Help Security

The help security command will display the security menu as shown previously.

Setup Security

The security command displays a series of menus that allow the security administrator to create and edit users, create and edit groups, and setup directory associations for the Web Server.

A user must be given rights to access this command. Any user that does not have rights to Security Configuration will see the following message when trying to access the setup security command:

```
>setup security
You are not authorized to access security commands
```

If a user is authorized, or if Configuration Security is not enabled, the Main Security Menu will be displayed.

Programming

This section describes the Send_Commands, Send_Strings, and Channel commands you can use to program the Integrated Controller. The examples in this section require a declaration in the DEFINE_DEVICE section of your program to work correctly. Refer to the *NetLinx Programming Language* instruction manual for specifics about declarations and DEFINE_DEVICE information.

Converting Axcess Code to NetLinx Code

In order to compile existing Axcess code to NetLinx code, minor modifications will be required. These modifications include identifier names that conflict with NetLinx identifiers, warning on variable type conversions, and stricter syntax rules.

For more information on NetLinx standards and conversion recommendations, go to **www.amx.com** and click on **Dealers** > **Tech Center** > **Tech Notes**. You can either search for the documents (such as ***NetLinx Programming Standards*** and ***Converting Axcess Code to NetLinx Code***) or Tech Notes (TN numbers: 186, 249, 261, and 310).

Refer to the *NetLinx Programming* Instruction Manual for more detailed information on the differences between the two codes and how they can be re-written. The section is called *Converting Axcess Code to NetLinx Code*.

Master Send_Commands

These commands are specific to the Master and not the Controller. These commands are sent to the DPS 0:1:0 (the Master). A device must first be defined in the NetLinx programming language with values for the Device: Port: System.

In these programming examples, <DEV> = Device. The term <D:P:S> = Device:Port:System.

Master Send_Commands

Command	Description
CLOCK Set the date and time on the Master.	The date and time settings are propagated over the local bus. Syntax: `SEND_COMMAND <DEV>,"'CLOCK <mm-dd-yyyy> <hh:mm:ss>'"` Variables: mm-dd-yyyy = Month, day, and year. Month and day have 2 significant digits. Year has 4 significant digits. hh-mm-ss = Hour, minute, and seconds. Each using only 2 significant digits. Example: `SEND_COMMAND 0,"'CLOCK 04-12-2005 09:45:31'"` Sets the Master's date to April 12, 2005 with a time of 9:45 am.

Master Send_Commands (Cont.)	
Command	**Description**
G4WC Add G4 Web Control devices to Web control list displayed by the Web server in a browser.	The internal G4WC Send command (to Master 0:1:0) has been revised to add G4 WebControl devices to Web control list displayed in the browser. Syntax: `SEND_COMMAND <D:P:S>,"'G4WC "Name/Description",IP Address/URL,IP Port,Enabled'"` Variables: Name/Description = A string, enclosed in double quotes, that is the description of the G4 Web Control instance. It is displayed in the browser. IP Address/URL = A string containing the IP Address of the G4 Web Control server, or a URL to the G4 Web Control server. IP Port = A string containing the IP Port of the G4 Web Control Server. Enabled = 1 or 0. If it is a 1 then the link is displayed. If it is a 0 then the link is disabled. The combination of Name/Description, IP Address/URL, and IP Port are used to determine each unique listing. Example: `SEND_COMMAND 0:1:0,"'G4WC "Bedroom",192.168.1.2,5900,1'"` Adds the BEDROOM control device using the IP Address of 192.168.1.2.
~IGNOREEXTERNAL-CLOCKCOMMANDS Set the Master so that it cannot have it's time set by another device which generates a 'CLOCK' command.	Syntax: `SEND_COMMAND <D:P:S>,"'~IGNOREEXTERNALCLOCKCOMMANDS'"` Example: `SEND_COMMAND 0:1:0,"'~IGNOREEXTERNALCLOCKCOMMANDS'"`

Master IP Local Port Send_Commands

These commands are specific to the Master and not the Controller. These commands are sent to the DPS 0:1:0 (the Master). A device must first be defined in the NetLinx programming language with values for the Device: Port: System.

In these programming examples, <DEV> = Device. The term <D:P:S> = Device:Port:System.

Master IP Local Port Send_Commands

Command	Description
UDPSENDTO Set the IP and port number of the UDP local ports destination for sending future packets.	This is only available for Type 2 and Type 3 Local Ports. Type 2 and Type 3 are referring to the protocol type that is part of the IP_CLIENT_OPEN call (4th parameter). Type 1 is TCP. Type 2 is UDP (standard) Type 3 is UDP (2 way) The NetLinx.axi defines constants for the protocol types: CHAR IP_TCP = 1 CHAR IP_UDP = 2 CHAR IP_UDP_2WAY = 3 Syntax: `SEND_COMMAND <D:P:S>,"'UDPSENDTO-<IP or URL>:<UDP Port Number>'"` Variables: IP or URL = A string containing the IP Address or URL of the desired destination. UDP Port Number = A String containing the UDP port number of the desired destination. Example 1: `SEND_COMMAND 0:3:0,"'UDPSENDTO-192.168.0.1:10000'"` Any subsequent SEND_STRING to 0:3:0 are sent to the IP Address 192.168.0.1 port 10000. Example 2: `SEND_COMMAND 0:3:0,"'UDPSENDTO-myUrl.com:15000'"` Any subsequent SEND_STRING to 0:3:0 are sent to the URL myURL.com port 15000.

Using the ID Button

The ID Button on the rear panel of the Integrated Controller is used in conjunction with the NetLinx Studio 2.x software program to allow you to assign new Device and System numbers for the Integrated Controller.

1. Using NetLinx Studio 2.x, place the system in Identity (ID) Mode. ID Mode means the entire system is put on hold while it waits for an event from any NetLinx device in the named system (for example, pushing the ID button on the Integrated Controller). The device that generates the first event is the identified device.
2. Press the ID Mode button to generate an event from the Integrated Controller and assign new device and system numbers in NetLinx Studio.

Only the Device number can be changed on the Controllers using the ID button. Port and System can not be defined.

Device:Port:System (D:P:S)

A device is any hardware component that can be connected to an AXlink or ICSNet bus. Each device must be assigned a unique number to locate that device on the bus. The NetLinx programming language allows numbers in the range 1-32,767 for ICSNet (255 for AXlink).

NetLinx requires a Device:Port:System (D:P:S) specification. This D:P:S triplet can be expressed as a series of constants, variables separated by colons, or a DEV structure.

For example:

```
STRUCTURE DEV
{
INTEGER Number  // Device number
INTEGER Port    // Port on device
INTEGER System  // System the device belongs to
}
```

The D:P:S notation is used to explicitly represent a device number, port and system. For example, 128:1:0 represents the first port on device 128 on this system. If the system and Port specifications are omitted, (e.g. 128), system 0 (indicating this system) and port 1 (the first port) is assumed. Here's the syntax:

```
NUMBER:PORT:SYSTEM
```

where:

NUMBER:	16-bit integer represents the device number
PORT:	16-bit integer represents the port number (in the range 1 through the number of ports on the Controller or device)
SYSTEM:	16-bit integer represents the system number (0 = this system)

Configuration Port Commands

The Configuration Port commands listed in the following table can be sent directly to the Master Card using a terminal program (i.e. Telnet). Be sure that your PC's COM port and terminal program's communication settings match those in the table below:

PC COM Port Communication Settings	
Baud	115200 (default)
Parity	None
Data Bits	8
Stop Bits	1
Flow Control	None

Each of the NetLinx Integrated Controllers has specific port assignments:

NI-2x00 Port Assignments	
Serial	Ports 1 - 3
Relays	Port 4
IR	Ports 5 -8
I/Os	Port 9
Count	4 relays and 4 I/O's

NI-4x00 & NI-3x00) Port Assignments	
Serial	Ports 1 - 7
Relays	Port 8
IR	Ports 9 -16
I/Os	Port 17
Count	8 relays and 8 I/O's

In your terminal program, type "Help" or a question mark ("?") and <Enter> to display the Configuration Port commands listed in the following table.

Configuration Port Commands	
Command	**Description**
DATE	Displays the current date and day of the week. Example: `>DATE` `10/31/2004 Wed`

Configuration Port Commands (Cont.)	
Command	**Description**
DEVICE HOLDOFF ON|OFF	Sets the Master to holdoff devices and not allow them to report online until the NetLinx program has completed executing the DEFINE_START section. Example: `>Device Holdoff ON` `Device Holdoff Set.` This command sets the state of the device holdoff. The GET DEVICE HOLDOFF command reveals whether the state is On or Off.
DEVICE STATUS <D:P:S>	Displays a list of all active (on) channels for the specified D:P:S. Enter DEVICE STATUS without the D:P:S variable, the Master displays ports, channels, and version information. Displays status of the specified Master. Example (on a local Master): `>Device 0 AMX Corp.,NI-2000,v3.00.312 contains 1 Ports.` `Port 1 - Channels:256 Levels:8 MaxStringLen=64 Types=8 bit MaxCommandLen=64 Types=8 bit` `The following input channels are on:None` `The following output channels are on:None` `The following feedback channels are on:None` `Level 1=0 Supported data types=UByte,UInt` `Level 2=0 Supported data types=UByte,UInt` `Level 3=0 Supported data types=UByte,UInt` `Level 4=0 Supported data types=UByte,UInt` `Level 5=0 Supported data types=UByte,UInt` `Level 6=0 Supported data types=UByte,UInt` `Level 7=0 Supported data types=UByte,UInt` `Level 8=0 Supported data types=UByte,UInt`
DISK FREE	Displays the total bytes of free space available on the Master. Example: `>DISK FREE` `The disk has 2441216 bytes of free space.`
DNS LIST <D:P:S>	Displays: • Domain suffix· • Configured DNS IP Information Example: `>DNS LIST [0:1:0]` `Domain suffix:amx.com` `The following DNS IPs are configured` `Entry 1-192.168.20.5` `Entry 2-12.18.110.8` `Entry 3-12.18.110.7`
ECHO OFF	Disables terminal character's echo (display) function.
ECHO ON	Enables terminal character's echo (display) function.
GET DEVICE HOLDOFF	Displays the state of the device holdoff setting in the Master. Example: `>GET DEVICE HOLDOFF` `Device Holdoff is off.` This command reveals the state of the device holdoff set using the DEVICE HOLDOFF ON|OFF command.
GET DUET MEMORY	Display the amount of memory allocated for Duet Java pool. This is the current Java memory heap size as measured in Megabytes. An example is a value of 5 = 5 MB.

Configuration Port Commands (Cont.)	
Command	**Description**
GET ETHERNET MODE	Displays the current LAN configuration setting. Settings are either "auto" in which the LAN driver will discover it's settings based on the LAN it is connected to OR <speed> and <duplex> where speed is either 10 or 100 and duplex is either full or half. Example: `get ethernet mode` `Ethernet mode is auto.` ***Note**: See SET ETHERNET MODE.*
GET IP <D:P:S>	Displays the Master's D:P:S, Host Name, Type (DHCP or Static), IP Address, Subnet Mask, Gateway IP, and MAC Address. Example: `>GET IP [0:1:50]` `IP Settings for 0:1:50` `HostName MLK_INSTRUCTOR` `Type DHCP` `IP Address 192.168.21.101` `Subnet Mask 255.255.255.0` `Gateway IP 192.168.21.2` `MAC Address 00:60:9f:90:0d:39`
HELP SECURITY	Displays the related security commands: Example: `>HELP SECURITY` `>logout Logout and close secure session` `>setup security Access the security setup menus`
ICSPMON ENABLED|DISABLED [PORT]	Enables or disables ICSP monitoring out the specified IP port. By enabling icspmon on an IP port, an external application could connect to that port and "listen" on the ICSP traffic.
IP STATUS	Provides information about the current NetLinx IP Connections: Example: `>IP STATUS` `NetLinx IP Connections` `No active IP connections`
MEM	Displays the largest free block of the Master's memory. Example: `>MEM` `The largest free block of memory is 11442776 bytes.`
MSG ON or MSG OFF	MSG On sets the terminal program to display all messages generated by the Master. MSG OFF disables the display. Example: `> MSG ON` Extended diagnostic information messages turned on. `> MSG OFF` Extended diagnostic information messages turned off.
OFF <D:P:S, or NAME, CHAN>	Turns off a channel on a device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system, or the name of the device that is defined in the DEFINE_DEVICE section of the program. Syntax: OFF[name,channel] -or- OFF[D:P:S,channel] Example: `>OFF[5001:7:4]` `Sending Off[5001:7:4]`

Configuration Port Commands (Cont.)	
Command	**Description**
ON <D:P:S, NAME, CHAN>	Turns on a channel on a device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device that is defined in the DEFINE_DEVICE section of the program. Syntax: ON[name,channel] or ON[D:P:S,channel] Example: `>ON[5001:7:4]` `Sending On[5001:7:4]`
PASS <D:P:S or NAME>	Sets up a pass through mode to a device. In pass through mode, any string received by the device is displayed on the screen, and anything typed is sent as a string to the device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system, or the name of the device that is defined in the DEFINE_DEVICE section of the program. Example: `>pass[5001:7:4]` `Entering pass mode.` To exit pass mode, type + + esc esc. Refer to the *ESC Pass Codes* section on page 131 for more information.
PING <IP ADDRESS>	Tests LAN connectivity to and confirms the presence of another LAN device. The syntax is just like the PING application in Windows or Linux. Example: `>ping 192.168.29.209` `192.168.29.209 is alive.`
PROGRAM INFO	Displays the name of the NetLinx program residing on the Master. Example: `>PROGRAM INFO` `-- Program Name Info` `-- Module Count = 1` `1 Name is i!-PCLinkPowerPointTest` `-- File Names = 2` `1 = C:\Program Files\AMX Applications\i!-PCLinkPowerPoint` `2 = C:\Program Files\Common Files\AMXShare\AXIs\NetLinx.axi` `2 = Name is MDLPP` `-- File Names = 2` `1 C:\AppDev\i!-PCLink-PowerPoint\i!-PCLinkPowerPointMod.axs` `2 C:\Program files\Common Files\AMXShare\AXIs\NetLinx.axi`
PULSE <D:P:S, or NAME, CHAN>	Pulses a channel on a device on and off. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device that is defined in the DEFINE_DEVICE section of the program. Example: `>PULSE[50001:8:50,1]` `Sending Pulse[50001:8:50,1]`
PWD	Displays the name of the current directory. Example: `pwd` `The current directory is doc:`

Configuration Port Commands (Cont.)	
Command	**Description**
REBOOT <D:P:S>	Reboots the Master or specified device. Example: >REBOOT [0:1:0] Rebooting...
RELEASE DHCP	Releases the DHCP setting for the Master. Example: >RELEASE DHCP The Master must be rebooted to acquire a new DHCP lease.
ROUTE MODE DIRECT|NORMAL	Sets the Master-to-Master route mode: • Normal mode - allows a Master to communicate with any Master accessible via the routing tables (shown with the SHOW ROUTE command). This includes a directly-connected Master (route metric =1) and indirectly connected masters (route metric greater than 1, but less than 16). • Direct mode - allows communication only with masters that are directly connected (route metric = 1). Indirectly connected masters cannot be communicated within this mode. Examples: >ROUTE MODE DIRECT Route Mode "Direct" Set >ROUTE MODE NORMAL Route Mode "Normal" Set
SEND_COMMAND D:P:S or Name,Command	Sends a specified command to a device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device that is defined in the DEFINE_DEVICE section of the NetLinx Program. The data of the string is entered with NetLinx string syntax. The Command uses the following NetLinx string syntax: Example: >Ex: send_command 1:1:1,"'This is a test',13,10" Ex: send_command RS232_1,"'This is a test',13,10"
SEND_STRING D:P:S or Name,String	Sends a string to a device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device defined in the DEFINE_DEVICE section of the NetLinx Program. The data of the string is entered with NetLinx string syntax.
SET DATE	Prompts you to enter the new date for the Master. When the date is set on the Master, the new date will be reflected on all devices in the system that have clocks (i.e. touch panels). By the same token, if you set the date on any system device, the new date will be reflected on the system's Master, and on all connected devices. This will not update clocks on devices connected to another Master (in Master-to-Master systems). Example: >SET DATE Enter Date: (mm/dd//yyyy) ->

Configuration Port Commands (Cont.)	
Command	**Description**
SET DNS <D:P:S>	Prompts you to enter a Domain Name, DNS IP #1, DNS IP #2, and DNS IP #3. Then, enter Y (yes) to approve/store the information in the Master. Entering N (no) cancels the operation. Example: `>SET DNS [0:1:0]` `-- Enter New Values or just hit Enter to keep current settings --` `Enter Domain Suffix: amx.com` `Enter DNS Entry 1 : 192.168.20.5` `Enter DNS Entry 2 : 12.18.110.8` `Enter DNS Entry 3 : 12.18.110.7` `You have entered: Domain Name: amx.com` `DNS Entry 1: 192.168.20.5` `DNS Entry 2: 12.18.110.8` `DNS Entry 3: 12.18.110.7` `Is this correct? Type Y or N and Enter -> Y` `Settings written. Device must be rebooted to enable new settings`
SET DUET MEMORY	Set the amount of memory allocated for Duet Java pool. This is the current Java memory heap size as measured in Megabytes. This feature is used so that if a NetLinx program requires a certain size of memory be allotted for its currently used Duet Modules, it can be reserved on the target Master. Valid values are 1 - 16 for 32 MB systems and 1 - 48 for a 64 MB system. This setting does not take effect until the next reboot. ***Note:*** *If you are trying to accomplish this setting of the Duet Memory size via a NetLinx program, the program command "DUET_MEM_SIZE_SET(int)" should call REBOOT() following a set.*
SET ETHERNET MODE <CMD>	This command sets the current LAN configuration settings - auto OR speed = 10 | 100, duplex = full | half Example: `set ethernet mode auto` `set ethernet mode speed=100 duplex=full` ***Note****: See GET ETHERNET MODE.*
SET FTP PORT	Enables/Disables the IP port listened to for FTP connections. Example: `>SET FTP PORT` `FTP is enabled` `Do you want to enable (e) or disable (d) FTP (enter e or d) :` `FTP enabled, reboot the master for the change to take affect.`
SET HTTP PORT	Sets the IP port listened to for HTTP connections. Example: `>SET HTTP PORT` `Current HTTP port number = 80` `Enter new HTTP port number (Usually 80) (0=disable HTTP) :` `Setting HTTP port number to` `New HTTP port number set, reboot the master for the change to take effect.`

Configuration Port Commands (Cont.)	
Command	**Description**
SET HTTPS PORT	Sets the IP port listened to for HTTPS connections. Example: `>SET HTTPS PORT` `  Current HTTPS port number = 443` `  Enter new HTTPS port number (Usually 443) (0=disable HTTPS)` `:` Once you enter a value and press the ENTER key, you get the following message: `  Setting HTTPS port number to` `  New HTTPS port number set, reboot the master for the change to take affect.`
SET ICSP PORT	Sets the IP port listened to for ICSP connections. Example: `>SET ICSP PORT` `  Current ICSP port number = 1319` `  Enter new ICSP port number (Usually 1319) (0=disable ICSP)` `:` Once you enter a value and press the ENTER key, you get the following message: `  Setting ICSP port number to` `  New ICSP port number set, reboot the master for the change to take affect.`
SET ICSP TCP TIMEOUT	Sets the timeout period for ICSP and i!-WebControl TCP connections. Example: `>SET ICSP TCP TIMEOUT` ` This will set the timeout for TCP connections for both ICSP and i!-WebControl.When no communication has been detected for the specified number of seconds, the socket connection is closed.ICSP and i!-WebControl have built-in timeouts and reducing the TCP timeout below these will cause undesirable results. The default value is 45 seconds.` `The current ICSP TCP timeout is 45 seconds` `Enter new timeout (in seconds):` Once you enter a value and press the ENTER key, you get the following message: `New timeout value set (in affect immediately).`
SET IP <D:P:S>	Prompts you to enter a Host Name, Type (DHCP or Fixed), IP Address, Subnet Mask, and Gateway IP Address. Enter Y (yes) to approve/store the information into the Master. Entering N (no) cancels the operation. Example: `>SET IP [0:1:0]` `--- Enter New Values or just hit Enter to keep current settings ---` `Enter Host Name:  MLK_INSTRUCTOR` `Enter IP type. Type D for DHCP or S for Static IP and then Enter: DHCP` `Enter Gateway IP:  192.168.21.2` `You have entered: Host Name  MLK_INSTRUCTOR` `Type  DHCP` `Gateway IP  192.168.21.2` `Is this correct? Type Y or N and Enter -> y` `Settings written. Device must be rebooted to enable new settings.`

Configuration Port Commands (Cont.)	
Command	**Description**
SET LOG COUNT	Sets the number of entries allowed in the message log. Example: `>SET LOG COUNT` `  Current log count = 1000` `  Enter new log count (between 50-10000) :` Once you enter a value and press the ENTER key, you get the following message: `  Setting log count to` `  New log count set, reboot the Master for the change to take affect.`
SET QUEUE SIZE	Provides the capability to modify maximum message queue sizes for various threads. Example: `set queue size` This will set the maximum message queue sizes for several threads. Use caution when adjusting these values. Set Queue Size Menu: 1. Interpreter (factory default=2000, currently=600) 2. Notification Manager (factory default=2000, currently=200) 3. Connection Manager (factory default=2000, currently=500) 4. Route Manager (factory default=400, currently=200) 5. Device Manager (factory default=500, currently=500) 6. Diagnostic Manager (factory default=500, currently=500) 7. TCP Transmit Threads (factory default=600, currently=200) 8. IP Connection Manager (factory default=800, currently=500) 9. Message Dispatcher (factory default=1000, currently=500) 10. Axlink Transmit (factory default=800, currently=200) 11. PhastLink Transmit (factory default=500, currently=500) 12. ICSNet Transmit (factory default=500, currently=500) 13. ICSP 232 Transmit (factory default=500, currently=500) 14. UDP Transmit (factory default=500, currently=500) 15. NI Device (factory default=500, currently=500) Enter choice or press ESC.
SET SSH PORT	Sets the IP port listened to for SSH connections. Example: `>SET SSH PORT` `  Current SSH port number = 22` `  Enter new SSH port number (Usually 22) (0=disable SSH) :` Once you enter a value and press the ENTER key, you get the following message: `  Setting SSH port number to 22` `  New SSH port number set, reboot the Master for the change to take affect.`
SET TELNET PORT	Sets the IP port listened to for Telnet connections. Example: `>SET TELNET PORT` `  Current telnet port number = 23` `  Enter new telnet port number (Usually 23) (0=disable Telnet) :` Once you enter a value and press the ENTER key, you get the following message: `  Setting telnet port number to 23` `  New telnet port number set, reboot the Master for the change to take affect.`

Configuration Port Commands (Cont.)	
Command	**Description**
SET THRESHOLD	Sets the Master's internal message thresholds. Example: `>SET THRESHOLD` `-- This will set the thresholds of when particular tasks are pended. The threshold is the number of messages queued before a task is pended.--` `--Use extreme caution when adjusting these values.--` `Current Interpreter Threshold = 2000` `Enter new Interpreter Threshold (Between 1 and 2000) (Default=10):` Once you enter a value and press the ENTER key, you get the following message: `Current Lontalk Threshold = 50` `Enter new Lontalk Threshold (Between 1 and 2000) (Default=50):50` `Current IP Threshold = 600` `Enter new IP Threshold (Between 1 and 2000) (Default=200): 600` `Setting Thresholds to: Interpreter 2000` `Lontalk 50` `IP 600` `New thresholds set, reboot the Master for the changes to take affect.`
SET TIME	Prompts you to enter the new time for the Master. When the time is set on the Master, the new time will be reflected on all devices in the system that have clocks (i.e. touch panels). By the same token, if you set the time on any system device, the new time will be reflected on the system's Master, and on all connected devices. This will not update clocks on devices connected to another Master (in Master-to-Master systems). Example: `>SET TIME` `Enter Date: (hh:mm:ss) ->`
SET TIMELINE LOOPCNT	Sets the Master's timeline/event max loopcount.
SET UPD BC RATE	Set UDP broadcast rate. A broadcast message is sent by the Master to allow devices to discover the Master. This command allows the broadcast frequency to be changed or eliminate the broadcast message. Example: `>SET UPD BC RATE` `Current broadcast message rate is 5 seconds between messages.` `Enter broadcast message rate in seconds between messages (off=0 ; default=5) (valid values 0-300):` Once you enter a value and press the ENTER key, you get the following message: `Setting broadcast message rate to 300 seconds between messages` `New broadcast message rate set.`
SET URL <D:P:S>	Prompts you to enter the URL address and port number of another Master or device (that will be added to the URL list). Then, enter Y (yes) to approve/store the new addresses in the Master. Entering N (no) cancels the operation. Example: `>SET URL [0:1:0]` `No URLs in the URL connection list` `Type A and Enter to Add a URL or Enter to exit. -> a` `Enter URL -> 192.168.21.200` `Enter Port or hit Enter to accept default (1319) ->` `Enter Type (Enter for permanent or T for temporary) ->` `URL Added successfully.`

Configuration Port Commands (Cont.)	
Command	**Description**
SHOW BUFFERS	Displays a list of various message queues and the number of buffers in each queue Example: `show buffers` `Thread TX RX Queued` `Axlink 0` `UDP 0 0-Sent=NO Waiting=NO` `IPCon Mgr 0` `Con Manager 0` `Interpreter 0` `Device Mgr 0` `Diag Mgr 0` `Msg Dispatch 0` `Cfg Mgr 0` `Route Mgr 0` `Notify Mgr 0` `Total 0 0 0 GrandTotal 0` ***Note**: See SHOW MAX BUFFERS.*
SHOW COMBINE	Displays a list of any combined devices. Example: `> SHOW COMBINE` `Combines` `Combined Device([33096:1:1],[96:1:1])` `Combined Level([33096:1:1,1],[128:1:1,1],[10128:1:1,1])` `Combined Device([33128:1:1],[128:1:1],[10128:1:1])`
SHOW DEVICE <D:P:S>	Displays a list of all devices present on the bus. Example: `>SHOW DEVICE [0:1:0]` `Local devices for system #1 (This System)` `Device (ID)Model (ID)Mfg FWID Version` `00000 (00256)NXC-ME260/64M (00001)AMX Corp. 00336 v3.00.312` `(PID=0:OID=0) Serial=0,0,0,0,0,0,0,0,0,0,0,0,` `Physical Address=NeuronID 000531589201` `(00256)vxWorks Image (00001) 00337 v3.00.312` `(PID=0:OID=1) Serial=N/A` `(00256)BootROM (00001) 00338 v3.00.312` `(PID=0:OID=2) Serial=N/A` `(00256)AXlink I/F uContr(00001) 00270 v1.03.14` `(PID=0:OID=3) Serial=0000000000000000`

Configuration Port Commands (Cont.)	
Command	**Description**
SHOW LOG	Displays the log of messages stored in the Master's memory. The Master logs all internal messages and keeps the most recent messages. The log contains:· • Entries starting with first specified or most recent • Date, Day, and Time message was logged • Which object originated the message • The text of the message SHOW LOG [start] [end] SHOW LOG ALL If start is not entered, the most recent message will be first. If end is not entered, the last 20 messages will be shown. If ALL is entered, all stored messages will be shown, starting with the most recent. Example: >SHOW LOG Message Log for System 50 Version: v2.10.75 Entry Date/Time Object Text ---------- 1: 11-01-2001 THU 14:14:49 ConnectionManager Memory Available = 11436804 <26572> 2: 11-01-2001 THU 14:12:14 ConnectionManager Memory Available = 11463376 <65544> 3: 11-01-2001 THU 14:10:21 ConnectionManager Memory Available = 11528920 <11512> 4: 11-01-2001 THU 14:10:21 TelnetSvr Accepted Telnet connection:socket=14 addr=192.168.16.110 port=2979 5: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 10002:1:50 6: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 128:1:50 7: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OffLine 128:1:50 8: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 96:1:50 9: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OffLine 96:1:50 10: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 128:1:50 11: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 96:1:50 12: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:16:50 13: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:15:50 14: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:14:50 15: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:13:50 16: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:12:50 17: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:11:50 18: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:10:50 19: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:9:50 20: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:8:50

Configuration Port Commands (Cont.)	
Command	**Description**
SHOW MAX BUFFERS	Displays a list of various message queues and the maximum number of message buffers that were ever present on the queue. Example: `show max buffers` `Thread TX RX` `Axlink 1` `UDP 1` `IPCon Mgr 0 (Total for TCP Connections TX=0)` `Con Manager 8` `Interpreter 17` `Device Mgr 8` `Diag Mgr 1` `Msg Dispatch 0` `Cfg Mgr 0` `Route Mgr 0` `Notify Mgr 0` `Total 2 34 GrandTotal 36` See SHOW BUFFERS.
SHOW MEM	Displays the memory usage for all memory types.
SHOW NOTIFY	Displays a list of devices (up to 1000) that other systems have requested input from and the types of information needed. Note that the local system number is 1061. Example: `>SHOW NOTIFY` `Device Notification List of devices requested by other Systems` `Device:Port System Needs` `00128:00001 00108 Channels Commands Strings Levels` `33000:00001 00108 Channels Commands`
SHOW REMOTE	Displays a list of the devices this system requires input from and the types of information needed. If when a NetLinx Master connects to another NetLinx Master, the newly connecting system has a device that the local system desires input from; the new system is told what information is desired from what device. Note the local system number is 1062. Example: `>SHOW REMOTE` `Device List of Remote Devices requested by this System` `Device Port System Needs` `00001 00001 00001 Channels Commands` `00002 00001 00001 Channels Commands` `33000 00001 00001 Channels Commands` `00128 00001 00108 Channels Commands Strings Levels` `33000 00001 00108 Channels Commands`
SHOW ROUTE	Displays information about how this NetLinx Master is connected to other NetLinx Masters. Example: `>SHOW ROUTE` `Route Data:` `System Route Metric PhyAddress` `-> 50 50 0 Axlink`

Configuration Port Commands (Cont.)	
Command	**Description**
SHOW SYSTEM	Provides a list of all devices in all systems currently on-line. The systems lists are either directly connected to this Master (i.e. 1 hop away), or are referenced in the DEFINE_DEVICE section of the NetLinx program. Optionally, you may provide the desired system number as a parameter to display only that system's information (e.g. SHOW SYSTEM 2001). The systems listed are in numerical order. Example: `>SHOW SYSTEM` `Local devices for system #50 (This System)` `----------` `Device (ID)Model (ID)Mfg FWID Version` `00000 (00256)Master (00001)AMX Corp. 00256 v2.10.75` `(PID=0:OID=0) Serial='2010-12090',0,0,0,0,0,0` `Physical Address=NeuronID 000239712501` `(00256)vxWorks Image (00001) 00257 v2.00.77` `(PID=0:OID=1) Serial=N/A` `(00256)BootROM (00001) 00258 v2.00.76` `(PID=0:OID=2) Serial=N/A` `(00256)AXlink I/F uContr(00001) 00270 v1.02` `(PID=0:OID=3) Serial=0000000000000000` `00096 (00192)VOLUME 3 CONTROL BO(00001)AMX Corp. 00000 v2.10` `(PID=0:OID=0) Serial=0000000000000000` `Physical Address=Axlink` `00128 (00188)COLOR LCD TOUCH PAN(00001)AMX Corp. 32778 v5.01d` `(PID=0:OID=0) Serial=0000000000000000` `Physical Address=Axlink` `05001 (00257)NXI Download (00001)AMX Corp. 00260` `v1.00.20` `(PID=0:OID=0) Serial=0,0,0,0,0,0,0,0,0,0,0,0,` `Physical Address=NeuronID 000189145801` `(00257)NXI/NXI-1000 Boot(00001) 00261 v1.00.00` `(PID=0:OID=1) Serial=0,0,0,0,0,0,0,0,0,0,0,0,` `10002 (00003)PHAST PLK-IMS (00001)Phast Corp. 0003 v3.12` `(PID=0:OID=0) Serial=0000000000000000` `Physical Address=NeuronID 0100417BD800`
TCP LIST	Lists all active TCP/IP connections. Example: `>TCP LIST` `The following TCP connections exist(ed):` `1: IP=192.168.21.56:1042 Socket=0 (Dead)` `2: IP=192.168.21.56:1420 Socket=0 (Dead)`
TIME	Displays the current time on the Master. Example: `>TIME` `13:42:04`
URL LIST <D:P:S>	Displays the list of URL addresses programmed in the Master (or another system). Example: `>URL LIST` `The following URLs exist in the URL connection list` `->Entry 0-192.168.13.65:1319 IP=192.168.13.65` `State=Connected` `Entry 1-192.168.13.200:1319 IP=192.168.13.200 State=Issue` `Connect`

ESC Pass Codes

There are 'escape' codes in the pass mode. These codes can switch the display mode or exit pass mode. The following 'escape' codes are defined.

Escape Pass Codes	
Command	**Description**
+ + ESC ESC	Exit Pass Mode: Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by another escape exits the pass mode. The Telnet session returns to "normal".
+ + ESC A	ASCII Display Mode: Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by an 'A' sets the display to ASCII mode. Any ASCII characters received by the device will be displayed by their ASCII symbol. Any non-ASCII characters will be displayed with a \ followed by two hex characters to indicate the characters hex value.
+ + ESC D	Decimal Display Mode: Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by a 'D' sets the display to decimal mode. Any characters received by the device will be displayed with a \ followed by numeric characters to indicate the characters decimal value.
+ + ESC H	Hex Display Mode: Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by an 'H' sets the display to hexadecimal mode. Any characters received by the device will be displayed with a \ followed by two hex characters to indicate the characters hex value.

Notes on Specific Telnet/Terminal Clients

Telnet and terminal clients will have different behaviors in some situations. This section states some of the known anomalies.

Windows™ client programs

Anomalies occur when using a Windows client if you are not typing standard ASCII characters (i.e. using the keypad and the ALT key to enter decimal codes). Most programs will allow you to enter specific decimal codes by holding ALT and using keypad numbers.

For example, hold ALT, hit the keypad 1, then hit keypad 0, then release ALT. The standard line feed code is entered (decimal 10). Windows will perform an ANSI to OEM conversion on some codes entered this way because of the way Windows handles languages and code pages.

The following codes are known to be altered, but others may be affected depending on the computer's setup.

Characters 15, 21, 22, and any characters above 127.

This affects both Windows Telnet and Terminal programs.

Linux Telnet client

The Linux Telnet client has three anomalies that are known at this time:

- A null (\00) character is sent after a carriage return.
- If an ALT 255 is entered, two 255 characters are sent (per the Telnet RAFT).
- If the code to go back to command mode is entered (ALT 29 which is ^]), the character is not sent, but Telnet command mode is entered.

THE FOLLOWING SECTIONS ONLY APPLY TO THE INTEGRATED CONTROLLER COMPONENT OF THE NI-3101-SIG.

LED Disable/Enable Send_Commands

The following commands enable or disable the LEDs on the Integrated Controller.
In these examples: <DEV> = Port 1 of the device. Sending to port 1 of the NI-Controller (affects all ports).

LED Send_Commands	
Command	**Description**
LED-DIS Disable all LEDs (on 32 LED hardware) for a port.	Regardless of whether or not the port is active, the LED will not be lit. Issue this command to port 1 to disable all the LEDs on the Controller. When activity occurs on a port(s) or Controller, the LEDs will not illuminate. Syntax: `SEND_COMMAND <DEV>,"'LED-DIS'"` Example: `SEND_COMMAND Port_1,"'LED-DIS'"` Disables all the LEDs on Port 1 of the Controller.
LED-EN Enable the LED (on 32 LED hardware) for a port (by default).	When the port is active, the LED is lit. When the port is not active, the LED is not lit. Issue the command to port 1 to enable the LEDs on the Controller (default setting). When activity occurs on a port(s) or Controller, the LEDs illuminate. Syntax: `SEND_COMMAND <DEV>,'LED-EN'` Example: `SEND_COMMAND System_1,'LED-EN'` Enables the System_1 Controller's LEDs.

RS232/422/485 Ports Channels

RS232/422/485 ports are Ports 1-6.

RS232/422/485 Ports Channels	
255 - CTS push channel	Reflects the state of the CTS input if a 'CTSPSH' command was sent to the port.

RS-232/422/485 Send_Commands

In these examples: <DEV> = device.

RS-232/422/485 Send_Commands	
Command	**Description**
B9MOFF Set the port's communication parameters for stop and data bits according to the software settings on the RS-232 port (default).	Disables 9-bit in 232/422/455 mode. By default, this returns the communication settings on the serial port to the last programmed parameters. This command works in conjunction with the 'B9MON' command. Syntax: `SEND_COMMAND <DEV>,"'B9MOFF'"` Example: `SEND_COMMAND RS232_1,"'B9MOFF'"` Sets the RS-232 port settings to match the port's configuration settings.
B9MON Override and set the current communication settings and parameters on the RS-232 serial port to 9 data bits with one stop bit.	Enables 9-bit in 232/422/455 mode. This command works in conjunction with the 'B9MOFF' command. Syntax: `SEND_COMMAND <DEV>,"'B9MON'"` Example: `SEND_COMMAND RS232_1,"'B9MON'"` Resets the RS-232 port's communication parameters to nine data bits, one stop bit, and locks-in the baud rate.

RS-232/422/485 Send_Commands (Cont.)	
Command	**Description**
CHARD Set the delay time between all transmitted characters to the value specified (in 100 Microsecond increments).	Syntax: `SEND_COMMAND <DEV>,"'CHARD-<time>'"` Variable: time = 0 - 255. Measured in 100 microsecond increments. Example: `SEND_COMMAND RS232_1,"'CHARD-10'"` Sets a 1-millisecond delay between all transmitted characters.
CHARDM Set the delay time between all transmitted characters to the value specified (in 1 Millisecond increments).	Syntax: `SEND_COMMAND <DEV>,"'CHARDM-<time>'"` Variable: time = 0 - 255. Measured in 1 millisecond increments. Example: `SEND_COMMAND RS232_1,"'CHARDM-10'"` Sets a 10-millisecond delay between all transmitted characters.
CTSPSH Enable Pushes, Releases, and Status information to be reported via channel 255 using the CTS hardware handshake input.	This command turns On (enables) channel tracking of the handshaking pins. If Clear To Send (CTS) is set high, then channel 255 is On. Syntax: `SEND_COMMAND <DEV>,"'CTSPSH'"` Example: `SEND_COMMAND RS232_1,"'CTSPSH'"` Sets the RS232_1 port to detect changes on the CTS input.
CTSPSH OFF Disable Pushes, Releases, and Status information to be reported via channel 255.	This command disables tracking. Turns CTSPSH Off. Syntax: `SEND_COMMAND <DEV>,"'CTSPSH OFF'"` Example: `SEND_COMMAND RS232_1,"'CTSPSH OFF'"` Turns off CTSPSH for the specified device.
GET BAUD Get the RS-232/422/485 port's current communication parameters.	The port sends the parameters to the device that requested the information. The port responds with: <port #>,<baud>,<parity>,<data>,<stop> 485 <ENABLED | DISABLED> Syntax: `SEND_COMMAND <DEV>,"'GET BAUD'"` Example: `SEND_COMMAND RS232_1,"'GET BAUD'"` System response example: `Device 1,115200,N,8,1 485 DISABLED`
HSOFF Disable hardware handshaking (default).	Syntax: `SEND_COMMAND <DEV>,"'HSOFF'"` Example: `SEND_COMMAND RS232_1,"'HSOFF'"` Disables hardware handshaking on the RS232_1 device.
HSON Enable RTS (ready-to-send) and CTS (clear-to-send) hardware handshaking.	Syntax: `SEND_COMMAND <DEV>,"'HSON'"` Example: `SEND_COMMAND RS232_1,"'HSON'"` Enables hardware handshaking on the RS232_1 device.
RXCLR Clear all characters in the receive buffer waiting to be sent to the Master.	Syntax: `SEND_COMMAND <DEV>,"'RXCLR'"` Example: `SEND_COMMAND RS232_1,"'RXCLR'"` Clears all characters in the RS232_1 device's receive buffer waiting to be sent to the Master.

RS-232/422/485 Send_Commands (Cont.)	
Command	**Description**
RXOFF Disable the transmission of incoming received characters to the Master (default).	Syntax: `SEND_COMMAND <DEV>,"'RXOFF'"` Example: `SEND_COMMAND RS232_1,"'RXOFF'"` Stops the RS232_1 device from transmitting received characters to the Master.
RXON Start transmitting received characters to the Master (default).	Enables sending incoming received characters to the Master. This command is automatically sent by the Master when a 'CREATE_BUFFER' program instruction is executed. Syntax: `SEND_COMMAND <DEV>,"'RXON'"` Example: `SEND_COMMAND RS232_1,"'RXON'"` Sets the RS232_1 device to transmit received characters to the Master.
SET BAUD Set the RS-232/422/485 port's communication parameters.	Syntax: `SEND_COMMAND <DEV>,"'SET BAUD <baud>,<parity>,<data>,<stop> [485 <Enable | Disable>]'"` Variables: baud = baud rate is: 115200. parity = N (none), O (odd), E (even), M (mark), S (space). data = 7 or 8 data bits. stop = 1 and 2 stop bits. 485 Disable = Disables RS-485 mode and enables RS-422. 485 Enable = Enables RS-485 mode and disables RS-422. Note: The only valid 9 bit combination is (baud),N,9,1. Example: `SEND_COMMAND RS232_1,"'SET BAUD 115200,N,8,1 485 ENABLE'"` Sets the RS232_1 port's communication parameters to 115,200 baud, no parity, 8 data bits, 1 stop bit, and enables RS-485 mode.
TSET BAUD Temporarily set the RS-232/422/485 port's communication parameters for a device.	TSET BAUD works the same as SET BAUD, except that the changes are not permanent, and the previous values will be restored if the power is cycled on the device. Syntax: `SEND_COMMAND <DEV>,"'TSET BAUD <baud>,<parity>,<data>,<stop> [485 <Enable | Disable>]'"` Variables: baud = baud rate is: 115200. parity = N (none), O (odd), E (even), M (mark), S (space). data = 7, 8, or 9 data bits. stop = 1 or 2 stop bits. 485 Disable = Disables RS-485 mode and enables RS-422. 485 Enable = Enables RS-485 mode and disables RS-422. Note: The only valid 9 bit combination is (baud),N,9,1. Example: `SEND_COMMAND RS232_1,"'TSET BAUD 115200,N,8,1 485 ENABLE'"` Sets the RS232_1 port's communication parameters to 115,200 baud, no parity, 8 data bits, 1 stop bit, and enables RS-485 mode.
TXCLR Stop and clear all characters waiting in the transmit out buffer and stops transmission.	Syntax: `SEND_COMMAND <DEV>,"'TXCLR'"` Example: `SEND_COMMAND RS232_1,"'TXCLR'"` Clears and stops all characters waiting in the RS232_1 device's transmit buffer.

RS-232/422/485 Send_Commands (Cont.)	
Command	**Description**
XOFF Disable software handshaking (default).	Syntax: `SEND_COMMAND <DEV>,"'XOFF'"` Example: `SEND_COMMAND RS232_1,"'XOFF'"` Disables software handshaking on the RS232_1 device.
XON Enable software handshaking.	Syntax: `SEND_COMMAND <DEV>,"'XON'"` Example: `SEND_COMMAND RS232_1,"'XON'"` Enables software handshaking on the RS232_1 device.

RS-232/422/485 Send_String Escape Sequences

This device also has some special SEND_STRING escape sequences:

If any of the 3 character combinations below are found anywhere within a SEND_STRING program instruction, they will be treated as commands and not the literal characters.

In these examples: <DEV> = device.

RS-232/422/485 Send_String Escape Sequences	
Command	**Description**
27,17,<time> Send a break character for a specified duration to a specific device.	Syntax: `SEND_STRING <DEV>,"27,17,<time>"` Variable: time = 1 - 255. Measured in 100 microsecond increments. Example: `SEND_STRING RS232_1,"27,17,10"` Sends a break character of 1 millisecond to the RS232_1 device.
27,18,0 Clear the ninth data bit by setting it to 0 on all character transmissions.	Used in conjunction with the 'B9MON' command. Syntax: `SEND_STRING <DEV>,"27,18,0"` Example: `SEND_STRING RS232_1,"27,18,0"` Sets the RS232_1 device's ninth data bit to 0 on all character transmissions.
27,18,1 Set the ninth data bit to 1 for all subsequent characters to be transmitted.	Used in conjunction with the 'B9MON' command. Syntax: `SEND_STRING <DEV>,"27,18,1"` Example: `SEND_STRING RS232_1,"27,18,1"` Sets the RS232_1 device's ninth data bit to 1 on all character transmissions.
27,19,<time> Insert a time delay before transmitting the next character.	Syntax: `SEND_STRING <DEV>,"27,19,<time>"` Variable: time = 1 - 255. Measured in 1 millisecond increments. Example: `SEND_STRING RS232_1,"27,19,10"` Inserts a 10 millisecond delay before transmitting characters to the RS232_1 device.
27,20,0 Set the RTS hardware handshake's output to high (> 3V).	Syntax: `SEND_STRING <DEV>,"27,20,0"` Example: `SEND_STRING RS232_1,"27,20,0"` Sets the RTS hardware handshake's output to high on the RS232_1 device.

RS-232/422/485 Send_String Escape Sequences (Cont.)	
Command	**Description**
27,20,1 Set the RTS hardware handshake's output to low/inactive (< 3V).	Syntax: `SEND_STRING <DEV>,"27,20,1"` Example: `SEND_STRING RS232_1,"27,20,1"` Sets the RTS hardware handshake's output to low on the RS232_1 device.

IR / Serial Ports Channels

IR / Serial Ports Channels	
00001 - 00229	IR commands.
00229 - 00253	May be used for system call feedback.
00254	Power Fail. (Used w/ 'PON' and 'POF' commands).
00255	Power status. (Shadows I/O Link channel status).

NOTE

IR ports - Ports 9 - 16 (NI-4X000/3X00) and Ports 5 - 8 (NI-2X00).
The NI series of NetLinx Masters support Serial control via the IR port when using firmware version 300 or greater.

IR/Serial Send_Commands

The following IR and IR/Serial Send_Commands generate control signals for external equipment. In these examples: <DEV> = device.

IR/Serial Send_Commands	
Command	**Description**
CAROFF Disable the IR carrier signal until a 'CARON' command is received.	Syntax: `SEND_COMMAND <DEV>,"'CAROFF'"` Example: `SEND_COMMAND IR_1,"'CAROFF'"` Stops transmitting IR carrier signals to the IR_1 port.
CARON Enable the IR carrier signals (default).	Syntax: `SEND_COMMAND <DEV>,"'CARON'"` Example: `SEND_COMMAND IR_1,"'CARON'"` Starts transmitting IR carrier signals to the IR_1 port.

IR/Serial Send_Commands (Cont.)	
Command	**Description**
CH Send IR pulses for the selected channel.	All channels below 100 are transmitted as two digits. If the IR code for ENTER (function #21) is loaded, an Enter will follow the number. If the channel is greater than or equal to (>=) 100, then IR function 127 or 20 (whichever exists) is generated for the one hundred digit. Uses 'CTON' and 'CTOF' times for pulse times. Syntax: `SEND_COMMAND <DEV>,"'CH',<channel number>"` Variable: channel number = 0 - 199. Example: `SEND_COMMAND IR_1,"'CH',18"` This device performs the following: • Transmits IR signals for 1 (IR code 11). The transmit time is set with the CTON command. • Waits until the time set with the CTOF command elapses. • Transmits IR signals for 8 (IR code 18). • Waits for the time set with the CTOF command elapses. • If the IR code for Enter (IR code 21) is programmed, the Controller performs steps 5 and 6. • Transmits IR signals for Enter (IR code 21). • Waits for the time set with the CTOF command elapses.
CP Halt and Clear all active or buffered IR commands, and then send a single IR pulse.	You can set the Pulse and Wait times with the 'CTON' and 'CTOF' commands. Syntax: `SEND_COMMAND <DEV>,"'CP',<code>"` Variable: code = IR port's channel value 0 - 252 (253 - 255 reserved). Example: `SEND_COMMAND IR_1,"'CP',2"` Clears the active/buffered commands and pulses IR_1 port's channel 2.
CTOF Set the duration of the Off time (no signal) between IR pulses for channel and IR function transmissions.	Off time settings are stored in non-volatile memory. This command sets the delay time between pulses generated by the 'CH' or 'XCH' send commands in tenths of seconds. Syntax: `SEND_COMMAND <DEV>,"'CTOF',<time>"` Variable: time = 0 - 255. Given in 1/10ths of a second. Default is 5 (0.5 seconds). Example: `SEND_COMMAND IR_1,"'CTOF',10"` Sets the off time between each IR pulse to 1 second.
CTON Set the total time of IR pulses transmitted and is stored in non-volatile memory.	This command sets the pulse length for each pulse generated by the 'CH' or 'XCH' send commands in tenths of seconds. Syntax: `SEND_COMMAND <DEV>,"'CTON',<time>"` Variable: time = 0 - 255. Given in 1/10ths of a second. Default is 5 (0.5 seconds). Example: `SEND_COMMAND IR_1,"'CTON',20"` Sets the IR pulse duration to 2 seconds.

IR/Serial Send_Commands (Cont.)	
Command	**Description**
GET BAUD Get the IR port's current DATA mode communication parameters.	The port sends the parameters to the device that requested the information. Only valid if the port is in Data Mode (see SET MODE command). The port responds with: <port #> <baud>,<parity>,<data bits>,<stop bits> Syntax: `SEND_COMMAND <DEV>,"'GET BAUD'"` Example: `SEND_COMMAND IR_1,"'GET BAUD'"` System response example: `PORT 9 IR,CARRIER,IO LINK 0`
GET MODE Poll the IR/Serial port's configuration parameters and report the active mode settings to the device requesting the information.	The port responds with: <port #> <mode>,<carrier>,<io link channel>. Syntax: `SEND_COMMAND <DEV>,"'GET MODE'"` Example: `SEND_COMMAND IR_1,"'GET MODE"` The system could respond with: PORT 4 IR,CARRIER,IO LINK 0
IROFF Halt and Clear all active or buffered IR commands being output on the designated port.	Syntax: `SEND_COMMAND <DEV>,"'IROFF'"` Example: `SEND_COMMAND IR_1,"'IROFF"` Immediately halts and clears all IR output signals on the IR_1 port.
POD Disable previously active 'PON' (power on) or 'POF' (power off) command settings.	Channel 255 changes are enabled. This command is used in conjunction with the I/O Link command. Syntax: `SEND_COMMAND <DEV>,"'POD'"` Example: `SEND_COMMAND IR_1,"'POD"` Disables the 'PON' and 'POF' command settings on the IR_1 device.
POF Turn Off a device connected to an IR port based on the status of the corresponding I/O Link input.	If at any time the IR sensor input reads that the device is ON (such as if someone turned it on manually at the front panel), IR function 28 (if available) or IR function 9 is automatically generated in an attempt to turn the device back OFF. If three attempts fail, the IR port will continue executing commands in the buffer. If there are no commands in the buffer, the IR port will continue executing commands in the buffer and trying to turn the device OFF until a 'PON' or 'POD' command is received. If the IR port fails to turn the device OFF, a PUSH and RELEASE is made on channel 254 to indicate a power failure error. You can only use the 'PON' and 'POF' commands when an IR device has a linked I/O channel. Channel 255 changes are disabled after receipt of this command. You can only use the 'PON' and 'POF' commands when an IR device has a linked I/O channel. Syntax: `SEND_COMMAND <DEV>,"'POF'"` Example: `SEND_COMMAND IR_1,"'POF'"` Sends power down IR commands 28 (if present) or 9 to the IR_1 device.

IR/Serial Send_Commands (Cont.)	
Command	**Description**
PON Turn On a device connected to an IR port based on the status of the corresponding I/O Link input.	If at any time the IR sensor input reads that the device is OFF (such as if one turned it off manually at the front panel), IR function 27 (if available) or IR function 9 is automatically generated in an attempt to turn the device back ON. If three attempts fail, the IR port will continue executing commands in the buffer and trying to turn the device On. If there are no commands in the buffer, the IR port will continue trying to turn the device ON until a 'POF' or 'POD' command is received. If the IR port fails to turn the device ON, a PUSH and RELEASE is made on channel 254 to indicate a power failure error. You can only use the 'PON' and 'POF' commands when an IR device has a linked I/O channel. Channel 255 changes are disabled after receipt of this command. Syntax: `SEND_COMMAND <DEV>,"'PON'"` Example: `SEND_COMMAND IR_1,"'PON'"` Sends power up IR commands 27 or 9 to the IR_1 port.
PTOF Set the time duration between power pulses in .10-second increments.	This time increment is stored in permanent memory. This command also sets the delay between pulses generated by the 'PON' or 'POF' send commands in tenths of seconds. It also sets the delay required after a power ON command before a new IR function can be generated. This gives the device time to power up and get ready for future IR commands. Syntax: `SEND_COMMAND <DEV>,"'PTOF',<time>"` Variable: time = 0 - 255. Given in 1/10ths of a second. Default is 15 (1.5 seconds). Example: `SEND_COMMAND IR_1,"'PTOF',15"` Sets the time between power pulses to 1.5 seconds for the IR_1 device.
PTON Set the time duration of the power pulses in .10-second increments	This time increment is stored in permanent memory. This command also sets the pulse length for each pulse generated by the 'PON' or 'POF' send commands in tenths of seconds. Syntax: `SEND_COMMAND <DEV>,"'PTON',<time>"` Variable: time = 0 - 255. Given in 1/10ths of a second. Default is 5 (0.5 seconds). Example: `SEND_COMMAND IR_1,"'PTON',15"` Sets the duration of the power pulse to 1.5 seconds for the IR_1 device.
SET BAUD Set the IR port's DATA mode communication parameters.	Only valid if the port is in Data Mode (see SET MODE command). Syntax: `SEND_COMMAND <DEV>,"'SET BAUD <baud>,<parity>,<data>,<stop>'"` Variables: baud = baud rates are: 19200, 9600, 4800, 2400, and 1200. parity = N (none), O (odd), E (even), M (mark), S (space). data = 7 or 8 data bits. stop = 1 and 2 stop bits. ***Note**: AMX does not recommend using a cable longer than 10 feet (3.05 meters) for the IR Ports.* Example: `SEND_COMMAND IR_1,"'SET BAUD 9600,N,8,1'"` Sets the IR_1 port's communication parameters to 9600 baud, no parity, 8 data bits, and 1 stop bit.

IR/Serial Send_Commands (Cont.)	
Command	**Description**
SET IO LINK Link an IR or Serial port to a selected I/O channel for use with the 'DE', 'POD', 'PON', and 'POF' commands.	The I/O status is automatically reported on channel 255 on the IR port. The I/O channel is used for power sensing (via a PCS or VSS). A channel of zero disables the I/O link. Syntax: `SEND_COMMAND <DEV>,"'SET IO LINK <I/O number>'"` Variable: I/O number = 1 - 8. Setting the I/O channel to 0 disables the I/O link. Example: `SEND_COMMAND IR_1,"'SET IO LINK 1'"` Sets the IR_1 port link to I/O channel 1. The IR port uses the specified I/O input as power status for processing 'PON' and 'POF' commands.
SET MODE Set the IR/Serial ports for IR or Serial-controlled devices connected to a CardFrame or NetModule.	Sets an IR port to either IR, Serial, or Data mode. ***Note:*** *IR DATA Mode works best when using both a lower baud rate and a short cable length (< 10 feet).* Syntax: `SEND_COMMAND <DEV>, 'SET MODE <mode>'"` Variable: mode = IR, SERIAL, or DATA. Example: `SEND_COMMAND IR_1,"'SET MODE IR'"` Sets the IR_1 port to IR mode for IR control.
SP Generate a single IR pulse.	You can use the 'CTON' to set pulse lengths and the 'CTOF' for time Off between pulses. Syntax: `SEND_COMMAND <DEV>,"'SP',<code>"` Variable: code = IR code value 1 - 252 (253-255 reserved). Example: `SEND_COMMAND IR_1, "'SP',25"` Pulses IR code 25 on IR_1 device.
XCH Transmit the selected channel IR codes in the format/pattern set by the 'XCHM' send command.	Syntax: `SEND_COMMAND <DEV>,"'XCH <channel>'"` Variable: channel = 0 - 999. Example: For detailed usage examples, refer to the 'XCHM' command.

IR/Serial Send_Commands (Cont.)	
Command	**Description**
XCHM Changes the IR output pattern for the 'XCH' send command.	Syntax: `SEND_COMMAND <DEV>,"'XCHM <extended channel mode>'"` Variable: extended channel mode = 0 - 4. Example: `SEND_COMMAND IR_1,"'XCHM 3'"` Sets the IR_1 device's extended channel command to mode 3. Mode 0 Example (default): [x][x]<x><enter> `SEND_COMMAND IR_1,"'XCH 3'"` Transmits the IR code as 3-enter. `SEND_COMMAND IR_1,"'XCH 34'"` Transmits the IR code as 3-4-enter. `SEND_COMMAND IR_1,"'XCH 343'"` Transmits the IR code as 3-4-3-enter. Mode 1 Example: <x> <x> <x> <enter> `SEND_COMMAND IR_1,"'XCH 3'"` Transmits the IR code as 0-0-3-enter. `SEND_COMMAND IR_1,"'XCH 34'"` Transmits the IR code as 0-3-4-enter. `SEND_COMMAND IR_1,"'XCH 343'"` Transmits the IR code as 3-4-3-enter. Mode 2 Example: <x> <x> <x> `SEND_COMMAND IR_1,"'XCH 3'"` Transmits the IR code as 0-0-3. `SEND_COMMAND IR_1,"'XCH 34'"` Transmits the IR code as 0-3-4. `SEND_COMMAND IR_1,"'XCH 343'"` Transmits the IR code as 3-4-3. Mode 3 Example: [[100][100]…] <x> <x> `SEND_COMMAND IR_1,"'XCH 3'"` Transmits the IR code as 0-3. `SEND_COMMAND IR_1,"'XCH 34'"` Transmits the IR code as 3-4. `SEND_COMMAND IR_1,"'XCH 343'"` Transmits the IR code as 100-100-100-4-3. Mode 4: Mode 4 sends the same sequences as the 'CH' command. Only use Mode 4 with channels 0 - 199. Mode 5 Example: <x><x><x><x><x><enter> `SEND_COMMAND IR_1,"'XCH 3'"` Transmits the IR code as 0-0-0-3-enter. `SEND_COMMAND IR_1,"'XCH 34'"` Transmits the IR code as 0-0-3-4-enter. `SEND_COMMAND IR_1,"'XCH 343'"` Transmits the IR code as 0-3-4-3-enter. `SEND_COMMAND IR_1,"'XCH 1343'"` Transmits the IR code as 1-3-4-3-enter.

IR/Serial Send_Commands (Cont.)	
Command	**Description**
XCHM (Cont.)	Mode 6 Example: <x><x><x><x><x> `SEND_COMMAND IR_1,"'XCH 3'"` Transmits the IR code as 0-0-0-3. `SEND_COMMAND IR_1,"'XCH 34'"` Transmits the IR code as 0-0-3-4. `SEND_COMMAND IR_1,"'XCH 343'"` Transmits the IR code as 0-3-4-3. `SEND_COMMAND IR_1,"'XCH 1343'"` Transmits the IR code as 1-3-4-3.

Input/Output Send_Commands

The following Send_Commands program the I/O ports on the Integrated Controller.
In these examples: <DEV> = device.

NOTE

I/O ports: Port 17.
Channels: 1 - 8 I/O channels.

I/O Send_Commands	
GET INPUT Get the active state for the selected channels.	An active state can be high (logic high) or low (logic low or contact closure). Channel changes, Pushes, and Releases generate reports based on their active state. The port responds with either 'HIGH' or 'LOW'. Syntax: `SEND_COMMAND <DEV>,"'GET INPUT <channel>'"` Variable: channel = Input channel 1 - 8. Example: `SEND_COMMAND IO,"'GET INPUT 1'"` Gets the I/O port's active state. The system could respond with: `INPUT1 ACTIVE HIGH`
SET INPUT Set the input channel's active state.	An active state can be high (logic high) or low (logic low or contact closure). Channel changes, Pushes, and Releases generate reports based on their active state. Setting an input to ACTIVE HIGH will disable the ability to use that channel as an output. Syntax: `SEND_COMMAND <DEV>,"'SET INPUT <channel> <state>'"` Variable: channel = Input channel 1 - 8. state = Active state HIGH or LOW (default). Example: `SEND_COMMAND IO,"'SET INPUT 1 HIGH'"` Sets the I/O channel to detect a high state change, and disables output on the channel.

Troubleshooting

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

Troubleshooting Information

Symptom	Solution
My NI Controller 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 to the on-board Master. • Verify there is an active LAN connection attached to the rear of the NI-Series Controller before beginning these procedures. • Select **Diagnostics** > **Network Address** from the Main menu and verify the System number. • If the IP Address field is still empty, give the device a few minutes to negotiate a DHCP Address and try again.
My NI Controller shows the same IP Address after selecting DHCP Server and clicking the GET IP Information button.	In requesting a DHCP Address, the DHCP Server can take up to a few minutes to provide the address to the on-board Master. When using a controller that has previously been used, there may be an instance where the IP Address was set as a fixed IP. In this case, the address would need to be released so a new user could use a DHCP server provided address. • Access the HyperTerminal application and try to communicate to the controller via the COM port. • Type **echo on** and press ENTER to send the information to the unit. • Type **get ip** to display the actual IP Address used by the unit. • Release the static/fixed IP Addresses. • Recycle power to the device and retry obtaining a DHCP address through NetLinx Studio.
My NI Controller still can't obtain a DHCP Address even after completing the above troubleshooting tip.	If the NI Controller is not connected directly to an open LAN wall connector, but is rather connected to a LAN Hub: • Contact Technical Support for a resolution to issues with this type of connection scenario.
I can't detect the NI Controller and my Status LED is blinking irregularly.	The on-board Master is trying to establish communication. • Wait a few moments and retry establishing communication using the latest NetLinx Studio. • If the problem persists, cycle power to the unit and repeat the above procedure. Another solution is to attempt communication via another method (Configuration Port or IP). • Refer to the *Configuration and Firmware Update* section on page 17 for more information.
NetLinx Studio only detects one of my connected Masters.	Each Master is give 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-3101-SIG. In order to work with both units. The ME260/64 can be assigned System #1 and the NI-3101-SIG can then be assigned System #2 using two open sessions of NetLinx Studio.

Troubleshooting Information (Cont.)	
Symptom	**Solution**
I can't connect to my NI Controller via the rear Configuration Port using a USB cable.	A USB cable is used for Serial communication between the PC and the Master. • Verify the USB connectors are securely inserted into their respective ports on both the rear Configuration Port (on the NI) and on the PC. • The NI-3101-SIG is configured to a fixed Baud Rate of 115200.
My NetLinx devices drop offline periodically when communicating over LAN.	The benefit of setting the LAN mode is to keep the Master (NI Controller) from having to auto negotiate with the LAN. On NetLinx Masters (such as those onboard the NIs), from Telnet or Terminal, you can send the **SET ETHERNET MODE** command. Examples: `SET ETHERNET MODE 10 HALF` `SET ETHERNET MODE 10 FULL` `SET ETHERNET MODE 100 HALF` `SET ETHERNET MODE 100 FULL` `SET ETHERNET MODE AUTO` The NI Controllers can utilize all of the above LAN modes.
When plugging the Master into a fixed speed hub or switch (i.e. 10-BaseT Hub or Switch), the hub or switch acts erratically.	(see above for resolution)
I'm unable to connect to the NetLinx Master from a PC over TCP/IP.	(see above for resolution)
During the firmware upgrade process, NetLinx Studio failed to install the last component.	This occurs when initially upgrading the on-board Master from a previous firmware build (117 or lower), to the new Web Security firmware (build 300 or higher). • Only upon the initial installation of the new build will be a failure of a successful download of the last component. This is part of the initial update procedure and will not occur during uploads of later firmware. • After the last components fails to install, click **Close** and reboot the on-board Master by selecting **Tools** > **Reboot the Master Controller** > **Continue** to continue the process. • After the last components fails to install, click Close and reboot the Master by selecting Tools > Reboot the Master Controller > Continue to begin the process. • Refer to the *Upgrading the On-board Master Firmware via an IP* section on page 29 for detailed procedures.

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