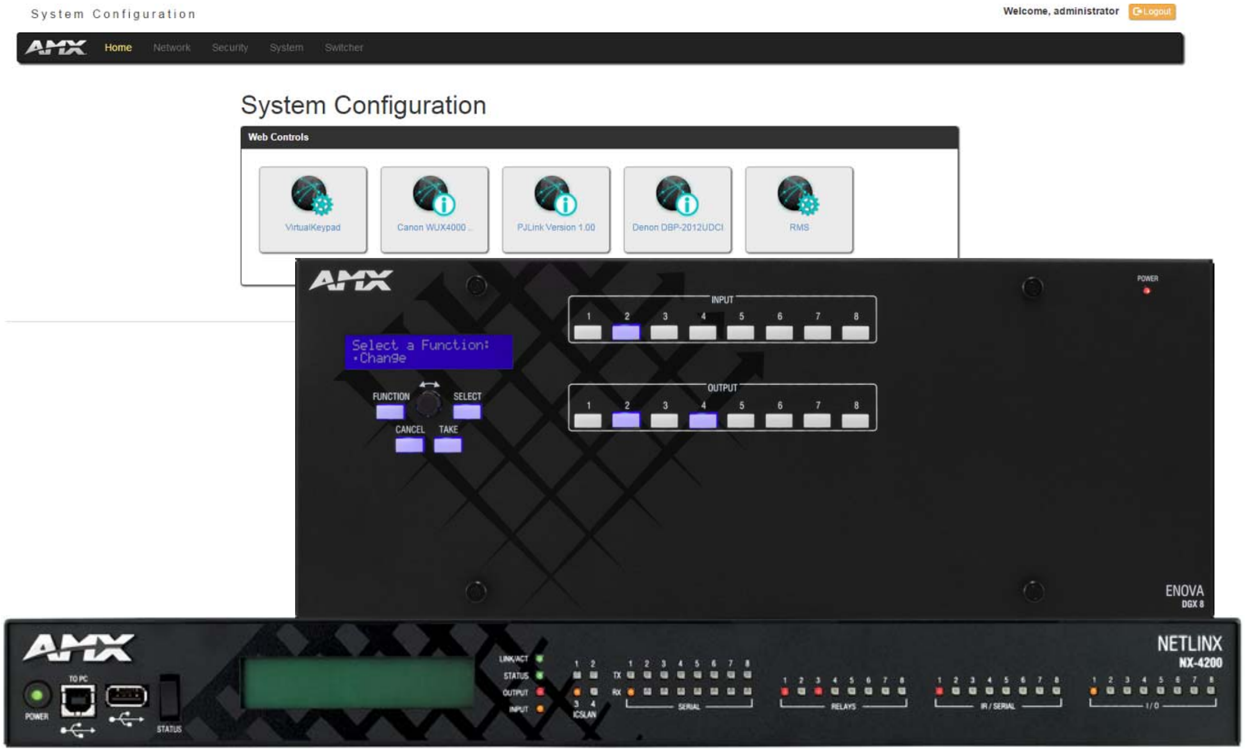
WEBCONSOLE AND PROGRAMMING GUIDE

# NX-SERIES CONTROLLERS
# ENOVA® DVX ALL-IN-ONE PRESENTATION SWITCHERS
# ENOVA® DGX DIGITAL MEDIA SWITCHERS
# MASSIO™ CONTROLPADS

NX-1200, NX-2200, NX-3200, NX-4200
DVX-3250HD-SP, DVX-3250HD-T, DVX-3255HD-SP, DVX-3255HD-T, DVX-3256HD-SP, DVX-3256HD-T
DVX-2250HD-SP, DVX-2250HD-T, DVX-2255HD-SP, DVX-2255HD-T, DVX-2210HD-SP, DVX-2210HD-T
DGX8-ENC, DGX16-ENC, DGX32-ENC-A, DGX64-ENC
MCP-106, MCP-108



AV FOR AN IT WORLD

## IMPORTANT SAFETY INSTRUCTIONS

1. READ these instructions.
2. KEEP these instructions.
3. HEED all warnings.
4. FOLLOW all instructions.
5. DO NOT use this apparatus near water.
6. CLEAN ONLY with dry cloth.
7. DO NOT block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. DO NOT install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. DO NOT defeat the safety purpose of the polarized or grounding type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wider blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. PROTECT the power cord from being walked on or pinched, particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. ONLY USE attachments/accessories specified by the manufacturer.
12. USE ONLY with a cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.
13. UNPLUG this apparatus during lightning storms or when unused for long periods of time.
14. REFER all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
15. DO NOT expose this apparatus to dripping or splashing and ensure that no objects filled with liquids, such as vases, are placed on the apparatus.
16. To completely disconnect this apparatus from the AC Mains, disconnect the power supply cord plug from the AC receptacle.
17. Where the mains plug or an appliance coupler is used as the disconnect device, the disconnect device shall remain readily operable.
18. DO NOT overload wall outlets or extension cords beyond their rated capacity as this can cause electric shock or fire.

The exclamation point, within an equilateral triangle, is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the product.

The lightning flash with arrowhead symbol within an equilateral triangle is intended to alert the user to the presence of uninsulated "dangerous voltage" within the product's enclosure that may be of sufficient magnitude to constitute a risk of electrical shock to persons.

ESD Warning: The icon to the left indicates text regarding potential danger associated with the discharge of static electricity from an outside source (such as human hands) into an integrated circuit, often resulting in damage to the circuit.

**WARNING:** To reduce the risk of fire or electrical shock, do not expose this apparatus to rain or moisture.

**WARNING:** No naked flame sources - such as candles - should be placed on the product.

**WARNING:** Equipment shall be connected to a MAINS socket outlet with a protective earthing connection.

**WARNING:** To reduce the risk of electric shock, grounding of the center pin of this plug must be maintained.

## COPYRIGHT NOTICE

## LIABILITY NOTICE

No patent liability is assumed with respect to the use of information contained herein. While every precaution has been taken in the preparation of this publication, AMX assumes no responsibility for error or omissions. No liability is assumed for damages resulting from the use of the information contained herein. Further, this publication and features described herein are subject to change without notice.

## AMX WARRANTY AND RETURN POLICY

The AMX Warranty and Return Policy and related documents can be viewed/downloaded at www.amx.com.

# Table of Contents

# Overview

## NetLinx NX Integrated Controllers

NetLinx NX Integrated Controllers (Masters) can be programmed to control RS-232/422/485, Relay, IR/Serial, and Input/Output devices using the NetLinx Studio application (version 4.0 or higher).

| NetLinx NX Integrated Controllers | |
|---|---|
| **Name** | **Description** |
| NX-1200 | NetLinx NX Integrated Controller |
| NX-2200 | NetLinx NX Integrated Controller |
| NX-3200 | NetLinx NX Integrated Controller |
| NX-4200 | NetLinx NX Integrated Controller |

**NOTE:** *Refer to the Products > Central Controllers > NetLinx NX Integrated Controllers page at www.amx.com for details and variations available for these products.*

NX controllers feature an on-board Web Console which allows you to connect to the NX controller via a web browser and make various configuration and security settings. The WebConsole is described in this document (starting with the *On-Board WebConsole User Interface* section on page 35).

NX controllers are 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® MicroEdition (Java Standard Edition Embedded)* platform. Duet simplifies the programming of a system that includes the NX controller and other 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 beaconing technology.

## Enova DVX All-in-One Presentation Switchers

| Enova Digital Media Switchers | |
|---|---|
| **Name** | **Description** |
| DVX-3250HD | 10x4 All-In-One Presentation Switchers with NX Control (Multi-Format, HDMI Inputs) |
| DVX-3255HD | 10x4 All-In-One Presentation Switchers with NX Control (Multi-Format, HDMI, 2 DXLink Inputs) |
| DVX-3256HD | 10x4 All-In-One Presentation Switchers with NX Control (Multi-Format, HDMI, 4 DXLink Inputs) |
| DVX-2250HD | 6x3 All-In-One Presentation Switchers with NX Control (Multi-Format, HDMI Inputs) |
| DVX-2255HD | 6x3 All-In-One Presentation Switchers with NX Control (Multi-Format, HDMI, DXLink Inputs) |
| DVX-2210HD | 4x2 All-In-One Presentation Switchers with NX Control (Multi-Format, HDMI Inputs) |

**NOTE:** *Refer to the Products > All-in-One Presentation Switchers page at www.amx.com for details and variations available for these products.*

### Enova DVX-22xxHD & DVX-325xHD

Enova DVX-22xxHD All-in-One Presentation Switchers utilize an NX-2200 Controller, therefore all controller-related information that applies to the NX-2200 is fully applicable to DVX-22xxHD products.

Enova DVX-325xHD All-in-One Presentation Switchers utilize an NX-3200 Controller, therefore all controller-related information that applies to the NX-3200 is fully applicable to DVX-325xHD products.

- Enova DVX All-In-One Presentation Switchers features many functions that do not apply to NX-series Controllers, most of which relate directly to the Audio/Video capabilities of the DVX.
- Refer to the Enova DVX-325xHD/22xxHD All-in-One Presentation Switchers Instruction Manual for information specific to Enova DVX products.

## Enova DGX Digital Media Switchers

| Enova Digital Media Switchers | |
|---|---|
| **Name** | **Description** |
| DGX8-ENC | Enova DGX 8 Enclosure |
| DGX16-ENC | Enova DGX 16 Enclosure |
| DGX32-ENC-A | Enova DGX 32 Enclosure |
| DGX64-ENC | Enova DGX 64 Enclosure |

**NOTE:** *Refer to the Products > Digital Media Switchers page at www.amx.com for details and variations available for these products.*

## Massio™ ControlPads

| Massio ControlPads | |
|---|---|
| **Name** | **Description** |
| MCP-106 | 6-Button Massio ControlPad |
| MCP-108 | 8-Button Massio ControlPad |

**NOTE:** *Refer to the Products > ControlPads page at www.amx.com for details and variations available for these products.*

## About This Document

This document describes using the on-board WebConsole, as well as NetLinx send commands and terminal communications to configure the NX controllers:

- Each major section of the WebConsole is described in a separate section of this document. Refer to:
  - the *On-Board WebConsole User Interface* section on page 35,
  - the *WebConsole - Network Options* section on page 46,
  - the *WebConsole - Security Options* section on page 42,
  - the *WebConsole - System Options* section on page 58, and
  - the *WebConsole - Switching Options* section on page 68.)
- The *Initial Configuration and Firmware Upgrade* section on page 5 describes upgrading the firmware on NX controllers.
- The *NetLinx Programming* section on page 83 lists and defines the NetLinx send commands that are supported by the NX controllers.
- The *Terminal (Program Port/Telnet) Commands* section on page 105 describes the commands and options available via a Telnet terminal session with the NX controller.

## Differences in DEFINE_PROGRAM Program Execution

Due to differences in the underlying architecture of the X-Series masters, changing variables in the DEFINE_PROGRAM section of code can negatively impact program performance. It has always been considered poor programming practice to change a variable within the DEFINE_PROGRAM section of code. If you have legacy NetLinx code that does change a variable in this section it's very likely that timing differences will cause your code to run slower and appear less responsive on an NX-Series controller and can have other adverse effects on platform reliability in the area of connectivity and data throughput.

The DEFINE_PROGRAM section of NetLinx code contains the code known as mainline. Mainline is the section of the program that is executed on a periodic basis by the NetLinx Master Controller. Under normal operation, the DEFINE_PROGRAM section executes at least once every half second. Various system activities can cause the DEFINE_PROGRAM section to execute more frequently than every half second. For example, any time an external event occurs (button push, level change), the DEFINE_PROGRAM section must re-execute to ensure that any change caused by the event processes through the DEFINE_PROGRAM section code block. This is also the case for changes to global variables. Any variable change requires the DEFINE_PROGRAM section to re-execute to process the new variable value through the DEFINE_PROGRAM code block.

Because high CPU usage can be detrimental to the system functionality on an NX master, AMX recommends the complete deprecation of the DEFINE_PROGRAM section. Syntactically, it is still valid to use the DEFINE_PROGRAM section in your NetLinx application, but it is no longer recommended. All logic that you would normally place in the DEFINE_PROGRAM section is handled better in the DEFINE_EVENT section.

Feedback statements remain the most common usage in the DEFINE_PROGRAM section. Because of periodically executing DEFINE_PROGRAM, you can rely on the program to update user feedback at a regular interval. However, if the DEFINE_PROGRAM section executes too frequently with the needless iterations expending the CPU to repetitively evaluate the feedback statements. TIMELINE_EVENTS provide a much more efficient mechanism for evaluating feedback statements. A single timeline triggering every 500ms provides the same periodic execution as the DEFINE_PROGRAM section without the unwanted recursive execution behavior.

Consider the following DEFINE_PROGRAM section containing feedback statements in PRGM EX. 1:

```
DEFINE_PROGRAM
[dvTP,1] = [dvDev,1]
[dvTP,2] = value1
[dvTP,3] = ![dvTP,3]
```

**PRGM EX. 1** DEFINE_PROGRAM with feedback statements

The code in PRGM EX. 1 would be better implemented using a timeline, as illustrated in PRGM EX. 2:

```
DEFINE_CONSTANTS
LONG FEEDBACK_TIMES[1] = {500}
INTEGER FEEDBACK_TIMELINE = 1
DEFINE_START
TIMELINE_CREATE(FEEDBACK_TIMELINE, FEEDBACK_TIMES, 1, TIMELINE_RELATIVE, TIMELINE_REPEAT)
DEFINE_EVENT
TIMELINE_EVENT[FEEDBACK_TIMELINE]
{
[dvTP,1] = [dvDev,1]
[dvTP,2] = value1
[dvTP,3] = ![dvTP,3]
}
```

**PRGM EX. 2** Using feedback statements in a timeline

The code in PRGM EX. 2 evaluates the feedback statements every half second regardless of other program activity. If a shorter feedback refresh is needed, you can specify a smaller constant in the FEEDBACK_TIMES constant. Even a time of 100ms executes far less frequently than a DEFINE_PROGRAM section stuck in an infinite execution loop due to a global variable change.

By moving all code out of the DEFINE_PROGRAM section, you ensure your NetLinx application is executing only when needed, and therefore not expending unnecessary CPU cycles.

If you choose to continue to use the DEFINE_PROGRAM section, it is critical that you ensure that you are not modifying a variable within the section. Any variable change will force a repeated execution of the section, thereby creating an infinite execution loop. Variables should never fall on the left-hand side of an evaluation statement, as in PRGM EX. 3.

```
DEFINE_PROGRAM
Var1 = !Var1
```

**PRGM EX. 3** Variable declared within the DEFINE_PROGRAM section

You must also take care to not inadvertently change a variable. For example, if a function is called within DEFINE_PROGRAM, then that function must likewise not change a global variable. Additionally, accessing global “values” such as TIME and DATE constitute a variable change. Take for example the code in PRGM EX. 4:

```
IF (TIME = ’22:00:00’)
{…}
```

**PRGM EX. 4** Time check

At first glance, this code does not appear to change a variable. It is simply checking to see if the current time is equal to 22:00:00. However, this code effectively changes the TIME variable by retrieving the current system time and assigning it to the TIME variable. If this code were present in a DEFINE_PROGRAM section, it would infinitely re-execute the DEFINE_PROGRAM section. You should place evaluations such as this in a TIMELINE_EVENT similar to the feedback timeline described earlier.

## CPU Usage

The new NX masters provide several diagnostics that can be used to determine if your program is overloading the CPU and, if so, what might be causing its excessive use. All of these commands are accessible through a Telnet or USB terminal connection with the master.

```
>cpu usage
Gathering CPU usage over a 10 second period. Please wait ...
CPU usage = 2.10% over a 10 second period.
```

An idle application normally runs below 5% of the CPU. If your idle application shows more usage than this, then it is probable that your application is experiencing excessive execution of the DEFINE_PROGRAM section.

You can use the following diagnostic to diagnose executions of the DEFINE_PROGRAM section:

```
>superuser 10
>enable interp stats
>show interp stats

-- Mainline Executions due to:
    Variable Change :     0
    Pending Int Event :   0
    Pulse Expiration :    0
    Hold Expiration :     0
    DoPush Expiration :   0
    Wait Expiration :     0
    Until Expiration :    0
    Timeline Expiration : 0
    Periodic Mainline :   0
  Current internal event count = 0
```

These statistics indicate how many times mainline has been executed and why it has been executed. Repeatedly executing “show interp stats” will give you an idea which code construct is causing mainline to execute. For example, if a variable is being changed, you will see the “Variable Change” count increasing. If a timeline is firing quickly, you will see the TIMELINE_EXPIRATION count increasing. A normal idle application that is executing DEFINE_PROGRAM every half second will only see the “Periodic Mainline” count increasing.

For example, consider this diagnostic output from a NetLinx application that is changing a variable in DEFINE_PROGRAM:

```
 >show interp stats

 -- Mainline Executions due to:
     Variable Change :     50927
     Pending Int Event :   1
     Pulse Expiration :    0
     Hold Expiration :     0
     DoPush Expiration :   0
     Wait Expiration :     0
     Until Expiration :    0
     Timeline Expiration : 0
     Periodic Mainline :   0
   Current internal event count = 1

 >show interp stats

 -- Mainline Executions due to:
     Variable Change :     62295
     Pending Int Event :   1
     Pulse Expiration :    0
     Hold Expiration :     0
     DoPush Expiration :   0
     Wait Expiration :     0
     Until Expiration :    0
     Timeline Expiration : 0
     Periodic Mainline :   0
   Current internal event count = 0

 >show interp stats

 -- Mainline Executions due to:
     Variable Change :     72386
     Pending Int Event :   1
     Pulse Expiration :    0
     Hold Expiration :     0
     DoPush Expiration :   0
     Wait Expiration :     0
     Until Expiration :    0
     Timeline Expiration : 0
     Periodic Mainline :   0
   Current internal event count = 1
```

Notice the “Variable Change” count is increasing rapidly.

These diagnostics will not tell you where in your application the offending code resides. Finding the offending code requires a process of code analysis and possibly selectively commenting out sections of code to isolate the offender.

**NOTE:** *NetLinx modules each have a DEFINE_PROGRAM section that must abide by the same rules as the main program, so the offending code could be in a module.*

# Quick Setup and Configuration Overview

## Installation Procedures

The general steps involved with most common installations of this device include:

- Unpack and confirm the contents of box (see the *Specifications* tables in the *Hardware Reference Guide* for each controller).
- Connect all rear panel components and supply power to the NX controller from the external power supply.

## Configuration and Communication

The general steps involved with setting up and communicating with the NX controller's on-board Master. In the initial communication process:

- Set the boot-time operations on the rear Configuration DIP switch. (The DIP switch is located on the front panel of the NX-1200.)
- Connect and communicate with the on-board Master via the Program port.
- Set the System Value being used with the on-board Master.
- Re-assign any Device values.
- Retrieve the DHCP Address for the on-board Master or assign a Static IP to the on-board Master.
- Once the IP information is determined, re-work the parameters for Master Communication to connect to the on-board Master via the LAN and not the Program port.

## Update the On-board Master and Controller Firmware

- Before using your new NX controller, you must first update your NetLinx Studio to the most recent release.
- Upgrade the Integrated Controller firmware through an IP address via the LAN connector (*Upgrading Firmware* section on page 28) (**IP recommended**).
- Upgrade the on-board Master firmware through an IP address via the LAN connector (*Upgrading Firmware* section on page 28) (**IP recommended**).

## Configure NetLinx Security on the NX Controller

- Setup and finalize your NetLinx Security Protocols (*WebConsole - Security Options* section on page 42).
- Program your NX controller (*NetLinx Programming* section on page 83).

# Using Zero Configuration

NetLinx Masters support using "zero-configuration" client software to quickly install multiple devices on the network.

## Bonjour (Zero-Configuration) Client

You can use a zero-configuration client to determine the IP address of the Controllers. There are many zero-configuration clients available which are free and widely available for download. NetLinx Studio includes a zero-configuration client which we will use for the purposes of this document.

If you don't already have it installed on your PC, download and install NetLinx Studio 4.0 before you begin.

## Connecting to a Network with a DHCP Server

By using the Controller's Zeroconf feature and the NetLinx Studio, you can install and configure multiple devices on the network without pre-configuring each device before installation.

The dealer only needs to match the serial number printed on the backside of the device or from the label on the box to the serial number that is displayed in the Bonjour browser pane.

1. Launch NetLinx Studio 4.0.
2. Once power is applied to the device, select the Zero-Config tab on the Workspace bar (see FIG. 1).

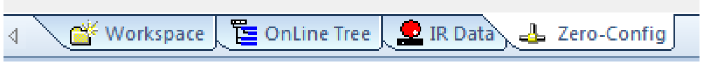
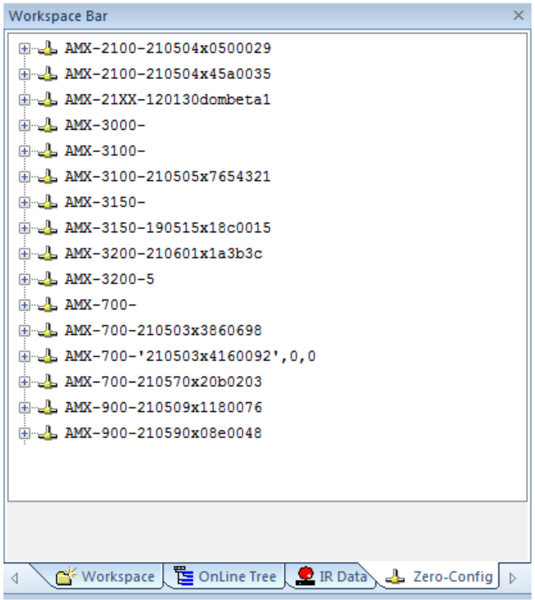


**FIG. 1** Zero-Config tab

3. In the Workspace area, right-click and select **Refresh Zero Config List**. The controller appears in the list of devices as shown in FIG. 2:



```
AMX-2100-210504x0500029
AMX-2100-210504x45a0035
AMX-21XX-120130dombeta1
AMX-3000-
AMX-3100-
AMX-3100-210505x7654321
AMX-3150-
AMX-3150-190515x18c0015
AMX-3200-210601x1a3b3c
AMX-3200-5
AMX-700-
AMX-700-210503x3860698
AMX-700-'210503x4160092',0,0
AMX-700-210570x20b0203
AMX-900-210509x1180076
AMX-900-210590x08e0048
```

**FIG. 2** Workspace bar (Zero-Config tab selected)

4. Double-click the Master you want to access it in the WebConsole.

   Accessing the Master requires valid login information. The browser will prompt you for User ID and Password before displaying the configuration pages for the selected device.

   Note that the serial number is appended to the name of the device.

After logging in, you can configure the device (changing IP settings, NetLinx settings, User settings, etc) via the pages in the WebConsole (see the *On-Board WebConsole User Interface* section on page 35).

# Initial Configuration

## Overview

This section describes using the NetLinx Studio software application to perform the initial configuration of the NetLinx Master. NetLinx Studio is used to setup a System number, obtain/assign the IP/URL for the NX controller, as described in this section (as well as to transfer firmware Kit files to the Master - see the *Upgrading Firmware* section on page 28).

## Before You Start

1. Verify you have the latest version of the NetLinx Studio application version 4.0 installed on your PC.

   NetLinx Studio is available to download from **www.amx.com**. Login to download the latest version. Alternatively, if it is already installed, use the **Web Update** option in NetLinx Studio's Help menu to obtain the latest version.

   The default location for the NetLinx Studio application is **Start** > **Programs** > **AMX Control Disc** > **NetLinx Studio** > **NetLinx Studio**.
2. Verify that a LAN cable is connected from the Master to the LAN Hub.
3. Connect a programming cable (Type-B USB) from the **Program Port** on the Master to a USB port on the PC being used for programming.
4. Apply power to the Master.

## Preparing the Master for USB Communication

To establish USB communication with the Master via the PROGRAM port with Type-B-to-Type-A cable:

1. Launch NetLinx Studio and select **Settings** > **Workspace Communication Settings** (FIG. 3):

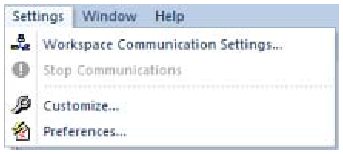
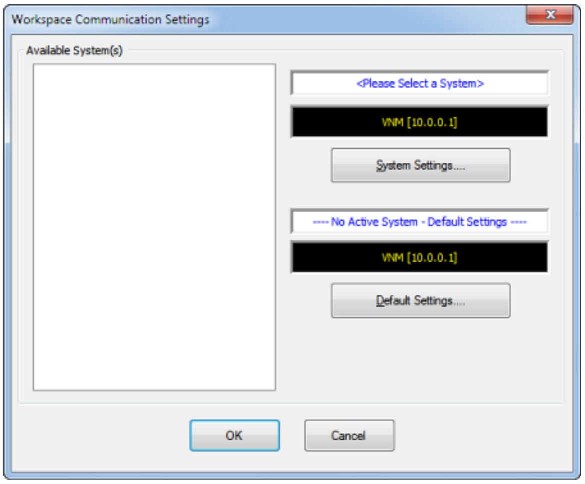


**FIG. 3** NetLinx Studio menu bar - Settings > Workspace Communication Settings

2. This opens the *Workspace Communication Settings* dialog (FIG. 4).



<Please Select a System>

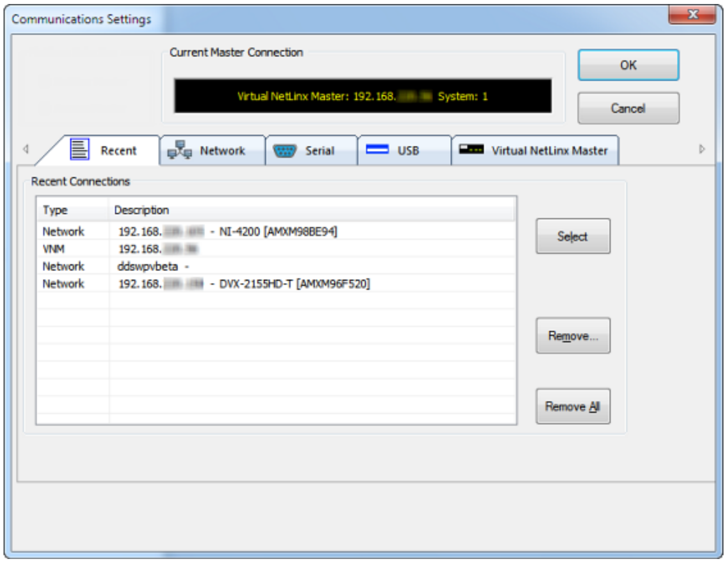
VNM [10.0.0.1]

---- No Active System - Default Settings ----

VNM [10.0.0.1]

**FIG. 4** Workspace Communication Settings dialog

3. Click the **System Settings** button to open the *Communications Settings* dialog (FIG. 5). If there is no system selected, click the **Default Settings** button to open the dialog.



Current Master Connection

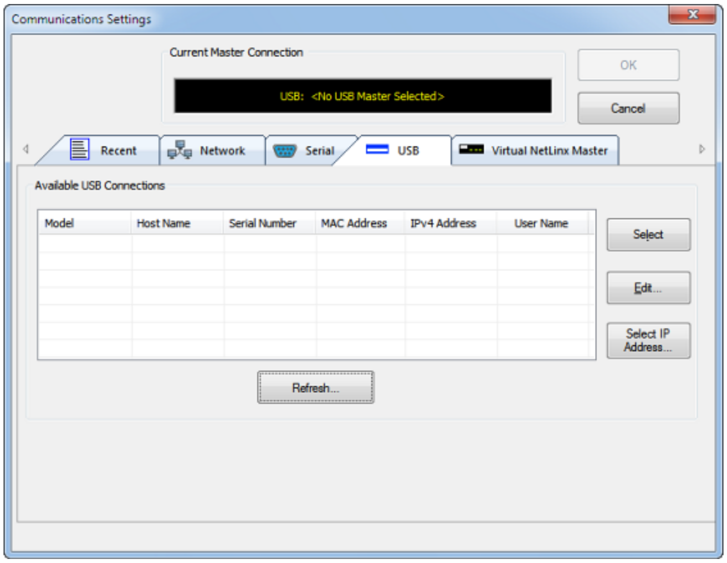
Virtual NetLinx Master: 192.168.[redacted] System: 1

Recent Connections

| Type | Description |
|---|---|
| Network | 192.168.[redacted] - NI-4200 [AMXM98BE94] |
| VNM | 192.168.[redacted] |
| Network | ddswpvbeta - |
| Network | 192.168.[redacted] - DVX-2155HD-T [AMXM96F520] |

**FIG. 5** Communication Settings dialog - Recent tab

4. Select the **USB** tab to view the USB options (FIG. 6).



Current Master Connection

USB: <No USB Master Selected>

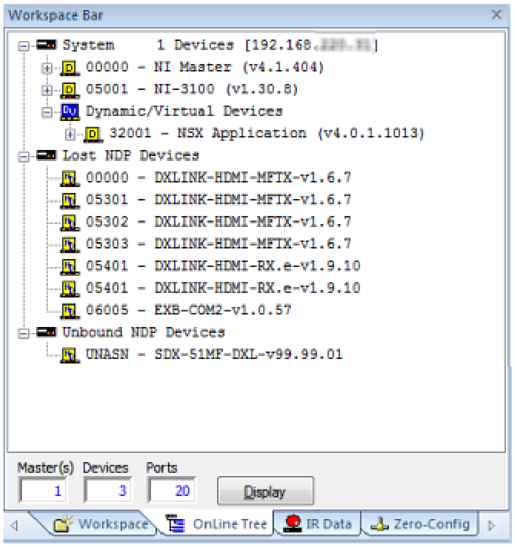
Available USB Connections

| Model | Host Name | Serial Number | MAC Address | IPv4 Address | User Name |
|---|---|---|---|---|---|

**FIG. 6** Communications Settings dialog - USB tab

5. On the USB tab, highlight the Master you want to connect to and click **Select**.
6. Click **Edit** to open the Edit USB Master's Username/Password dialog to set the user name and password for authentication access to the Master. This step is optional. You can only change the user name and password in the dialog. The additional fields are view-only.
7. Click **OK** to close the USB Master's Username/Password dialog, and click **OK** in the Communication Settings dialog to return to the Communication Settings dialog, now indicating the USB-connected Master as the current connection configuration.
8. Click **OK** to close the *Communication Settings* dialog and return to the main application.

9. Right-click the **Online Tree** tab entry and select **Refresh System:** the Controller should appear in the Device Tree (FIG. 7):



```
System      1 Devices [192.168.[redacted]]
   00000 - NI Master (v4.1.404)
   05001 - NI-3100 (v1.30.8)
   Dynamic/Virtual Devices
      32001 - NSX Application (v4.0.1.1013)
Lost NDP Devices
   00000 - DXLINK-HDMI-MFTX-v1.6.7
   05301 - DXLINK-HDMI-MFTX-v1.6.7
   05302 - DXLINK-HDMI-MFTX-v1.6.7
   05303 - DXLINK-HDMI-MFTX-v1.6.7
   05401 - DXLINK-HDMI-RX.e-v1.9.10
   05401 - DXLINK-HDMI-RX.e-v1.9.10
   06005 - EXB-COM2-v1.0.57
Unbound NDP Devices
   UNASN - SDX-51MF-DXL-v99.99.01
```

Master(s): 1 Devices: 3 Ports: 20

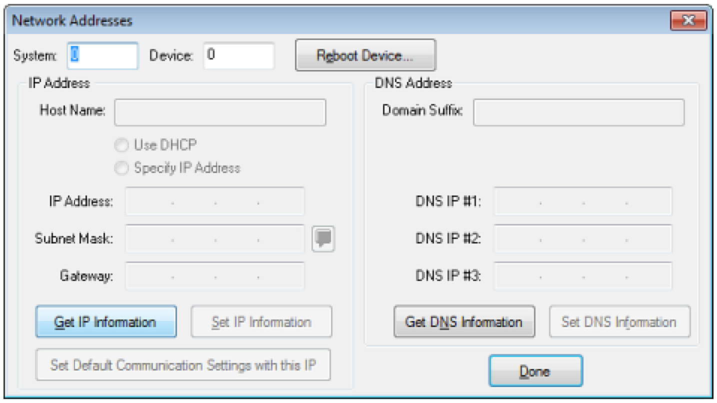
**FIG. 7** Workspace Bar - Online Tree

> **NOTE:** *If the Master does not appear in the list, verify that the USB cable is connected properly.*

Once USB communication has been established, use NetLinx Studio to configure the Controller for LAN Communication, as described in the next section.

## Configuring the NX Controller for LAN Communication

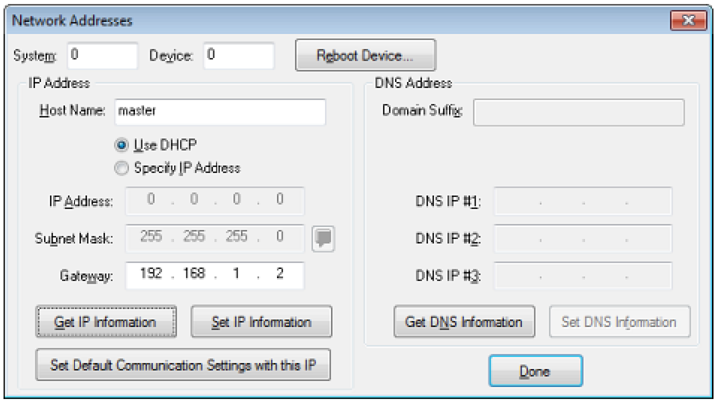
1. Use a LAN cable to connect the Controller to the LAN to which the PC running NetLinx Studio is connected.
2. Select **Diagnostics** > **Network Addresses** from the menu bar to open the *Network Addresses* dialog (FIG. 8). Use the options in this dialog to select to either use DHCP or specify an IP address.



System: 1 Device: 0

**FIG. 8** Network Addresses dialog

3. Click **Get IP Information** to enable the fields for editing (FIG. 9):



Network Addresses

System: 0 Device: 0

IP Address

Host Name: master

● Use DHCP

○ Specify IP Address

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 1 . 2

DNS Address

Domain Suffix:

DNS IP #1: . . .

DNS IP #2: . . .

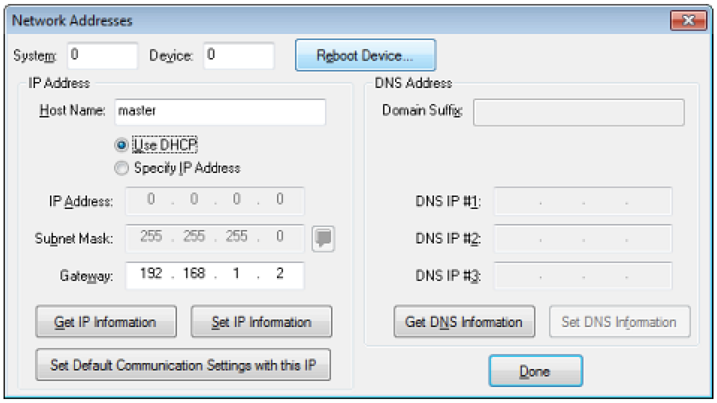
DNS IP #3: . . .

**FIG. 9** Network Addresses dialog showing initial IP information

4. Enter the *System*, *Device* (**0** for NetLinx Masters), and *Host Name* information.

**NOTE:** *Host names may contain only the ASCII letters 'a' through 'z' (in a case-insensitive manner), the digits '0' through '9', and the hyphen ('-').*

5. To configure a network address via **DHCP** (FIG. 10):



Network Addresses

System: 0 Device: 0

IP Address

Host Name: master

● Use DHCP

○ Specify IP Address

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 1 . 2

DNS Address

Domain Suffix:

DNS IP #1: . . .

DNS IP #2: . . .

DNS IP #3: . . .

**FIG. 10** Network Addresses dialog (DHCP)

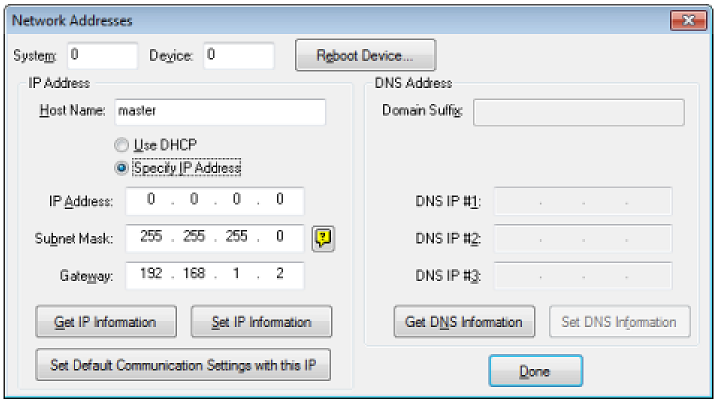
a. Select **Use DHCP**.

b. Click **Set IP Information** to retain the DHCP setting.

c. To finish the process, click **Reboot Device.**

d. Click **Done** to close the dialog.

6. To specify a network IP address (FIG. 11):



Network Addresses

System: 0 Device: 0

IP Address

Host Name: master

○ Use DHCP

● Specify IP Address

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 1 . 2

DNS Address

Domain Suffix:

DNS IP #1: . . .

DNS IP #2: . . .

DNS IP #3: . . .

**FIG. 11** Network Addresses dialog (Specify IP Address)

a. Select **Specify IP Address.**

b. Enter the IP parameters into the available fields.

c. Click **Set IP Information** to retain the pre-reserved IP address to the Master.

d. To finish the process, click **Reboot Device.**

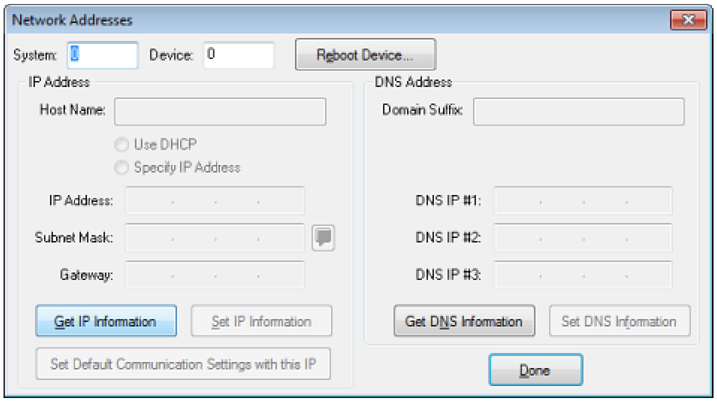
e. Click **OK** to close the dialog.

7. Repeat steps 1 - 5 from the previous section, but rather than selecting the **USB** tab, select **Network** and edit the settings to match the IP address you are using (Static or Dynamic).
8. If you want the Master to require authentication for access, enter a User Name and Password in the provided fields to secure the Master.
9. Click the **OK** to close all dialogs and return to the main application.

## Obtaining the NX Controller's IP Address (using DHCP)

**NOTE:** *Verify there is an active LAN connection on the NX controller's LAN port before beginning these procedures.*

1. In NetLinx Studio, select **Diagnostics** > **Network Addresses** from the Main menu to access the Network Addresses dialog (FIG. 12).



System: 1

Device: 0

**FIG. 12** NetLinx Studio: Network Addresses dialog

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 Manage System - System Number section on page 46 for more detailed instructions on setting a system value.*

3. Click **Get IP Information** to enable the Use DHCP and Specify IP Address options.
4. Select **Use DHCP**.

**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.*

5. Click **Reboot Device**.
6. After the device has booted, repeat steps 1-3.
7. Note the obtained IP address *(read-only*). This information is later entered into the *Communication Settings* dialog and used by NetLinx Studio to communicate to the NX controller 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.*

**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.*

8. Click **Done** to close the dialog.

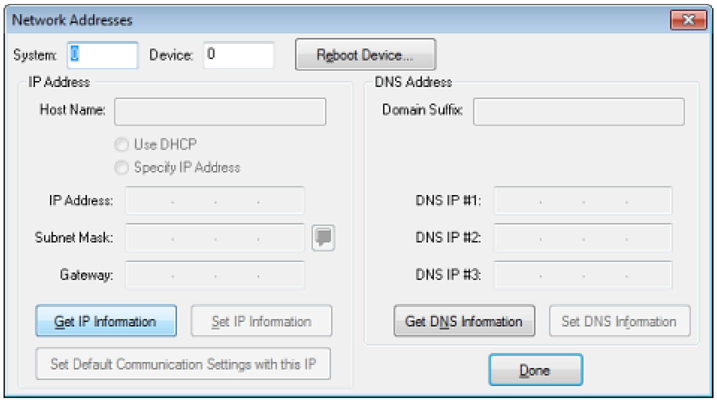
**NOTE:** *On the front panel of the NetLinx Master, the STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*

Complete the communication process by continuing on to the *Communicating via IP Address* section on page 25.

# Assigning a Static IP to the NX Controller

**NOTE:** *Verify there is an active LAN connection on the LAN port of the Master before beginning these procedures.*

1. In NetLinx Studio, select **Diagnostics** > **Network Addresses** to open the *Network Addresses* dialog (FIG. 13):



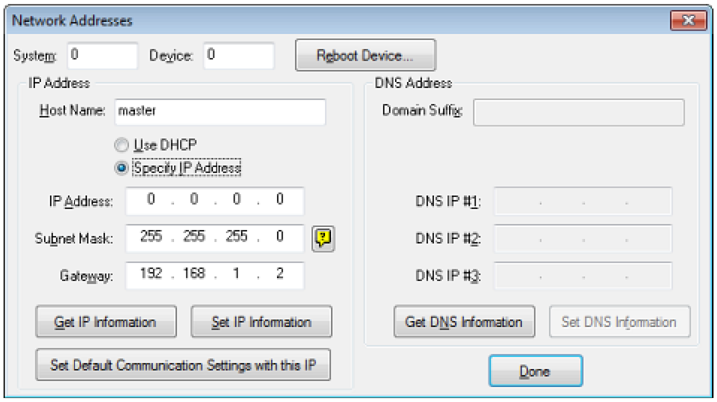
System: 1
Device: 0

**FIG. 13** NetLinx Studio: Network Addresses dialog

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 Manage System - System Number section on page 46 for more detailed instructions on setting a system value.*

3. Click the **Get IP Information** button to enable the *Use DHCP* and *Specify IP Address* options.
4. Select **Specify IP Address** to enable the IP fields for editing (FIG. 14):



System: 0
Device: 0
Host Name: master
○ Use DHCP
● Specify IP Address
IP Address: 0 . 0 . 0 . 0
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 192 . 168 . 1 . 2

**FIG. 14** NetLinx Studio: Network Addresses dialog (Specify IP Address)

5. Enter the *IP Address*, *Subnet Mask*, and *Gateway* information into their respective fields (as defined by the System Administrator).

**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.*

6. Click **Set IP Information** to cause the on-board Master to retain this new IP address.
7. Click **Reboot Master**.
8. Click **Done** to close the dialog.

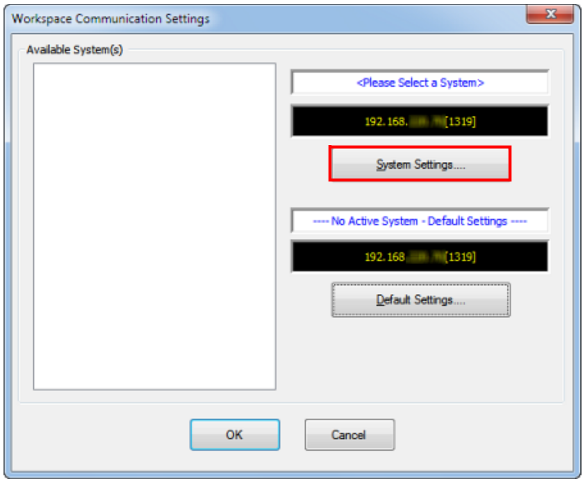
**NOTE:** *On the front panel of the NetLinx Master, the STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*

Complete the communication process by continuing on to the *Communicating via IP Address* section on page 25.

# Communicating via IP Address

Whether the on-board Master's IP address was set or obtained via DHCP, use the IP address information from the *Network Addresses* dialog to establish communication via the LAN-connected Master.

1. Use NetLinx Studio to obtain the IP address of the NX controller. If you do not have an IP address, follow the steps outlined in either the *Obtaining the NX Controller's IP Address (using DHCP)* section on page 23, or the *Assigning a Static IP to the NX Controller* section on page 24.
2. Select **Settings** > **Workspace Communication Settings** from the Main menu to open the *Workspace Communication Settings* dialog (FIG. 15):

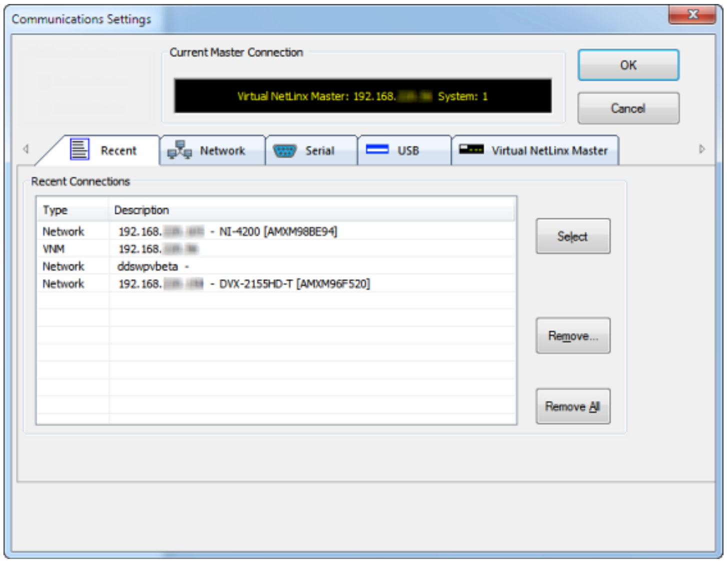


192.168.[redacted][1319]

192.168.[redacted][1319]

**FIG. 15** NetLinx Studio - Workspace Communication Settings dialog

3. Click **System Settings** to open the *Communications Settings* dialog. If you do not have a system selected, click the **Default Settings** button (FIG. 16).

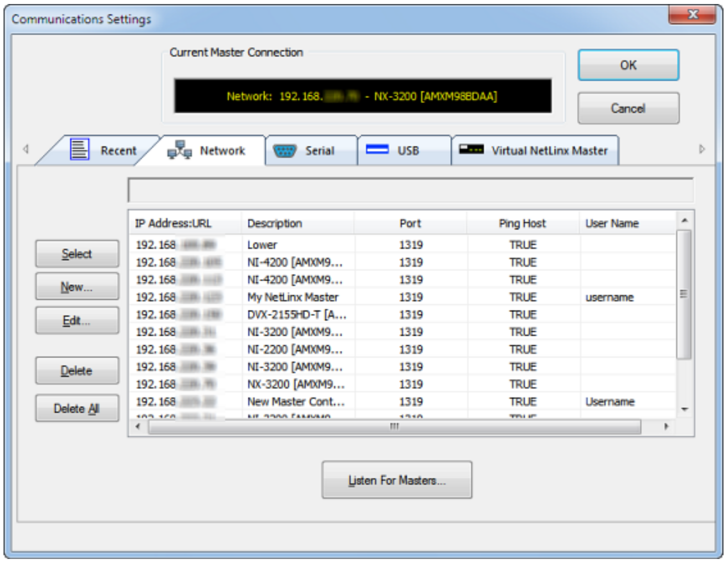


Virtual NetLinx Master: 192.168.[redacted] System: 1

| Type | Description |
|---|---|
| Network | 192.168.[redacted] - NI-4200 [AMXM98BE94] |
| VNM | 192.168.[redacted] |
| Network | ddswpvbeta - |
| Network | 192.168.[redacted] - DVX-2155HD-T [AMXM96F520] |

**FIG. 16** NetLinx Studio - Communication Settings dialog (TCP/IP selected)

4. Select the Network tab (FIG. 17).

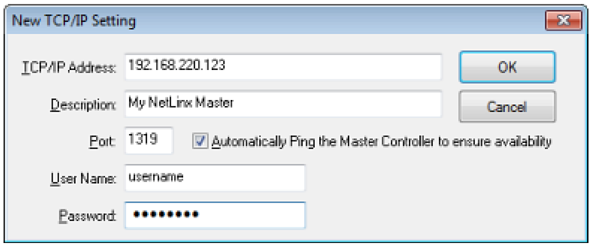


Network: 192.168.[redacted] - NX-3200 [AMXM98BDAA]

| IP Address:URL | Description | Port | Ping Host | User Name |
|---|---|---|---|---|
| 192.168.[redacted] | Lower | 1319 | TRUE | |
| 192.168.[redacted] | NI-4200 [AMXM9... | 1319 | TRUE | |
| 192.168.[redacted] | NI-4200 [AMXM9... | 1319 | TRUE | |
| 192.168.[redacted] | My NetLinx Master | 1319 | TRUE | username |
| 192.168.[redacted] | DVX-2155HD-T [A... | 1319 | TRUE | |
| 192.168.[redacted] | NI-3200 [AMXM9... | 1319 | TRUE | |
| 192.168.[redacted] | NI-2200 [AMXM9... | 1319 | TRUE | |
| 192.168.[redacted] | NI-3200 [AMXM9... | 1319 | TRUE | |
| 192.168.[redacted] | NX-3200 [AMXM9... | 1319 | TRUE | |
| 192.168.[redacted] | New Master Cont... | 1319 | TRUE | Username |

**FIG. 17** Communications Settings dialog - Network tab

5. Click **New** to open the *New TCP/IP Setting* dialog. In this dialog, you can enter both a previously obtained DHCP or static IP address and an associated *Description* for the connection into their respective fields. (FIG. 18):



TCP/IP Address: 192.168.220.123

Description: My NetLinx Master

Port: 1319 ☑ Automatically Ping the Master Controller to ensure availability

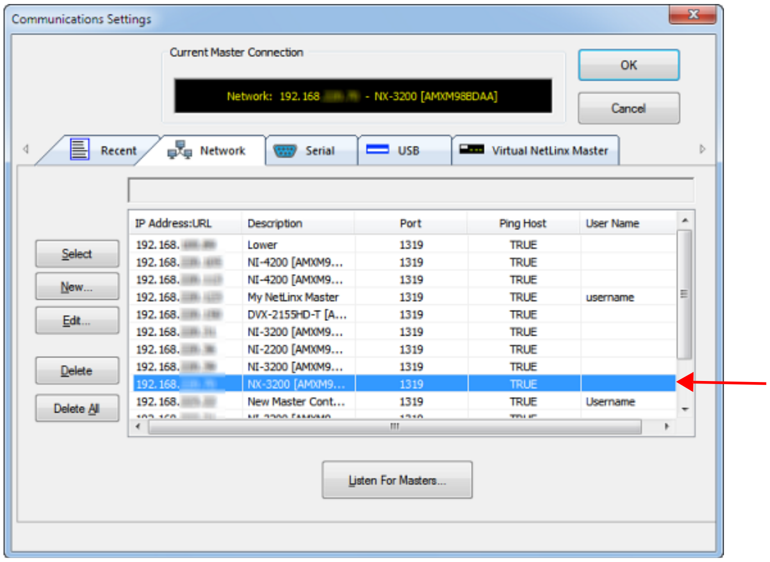
User Name: username

Password: ••••••••

**FIG. 18** NetLinx Studio - New TCP/IP Setting dialog

- Verify that the *Automatically Ping the Master Controller to ensure availability* option is selected to make sure the Master is initially responding on-line before establishing full communication.
- If the authentication is required for connecting to the Master at this address, enter a *User Name* and *Password* in the text fields provided.

6. Click **OK** to close the *New TCP/IP Settings* dialog and return to the *Communication Settings* dialog: (FIG. 19).



Network: 192.168.[redacted] - NX-3200 [AMXM98BDAA]

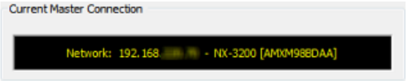
| IP Address:URL | Description | Port | Ping Host | User Name |
|---|---|---|---|---|
| 192.168.[redacted] | Lower | 1319 | TRUE | |
| 192.168.[redacted] | NI-4200 [AMXM9... | 1319 | TRUE | |
| 192.168.[redacted] | NI-4200 [AMXM9... | 1319 | TRUE | |
| 192.168.[redacted] | My NetLinx Master | 1319 | TRUE | username |
| 192.168.[redacted] | DVX-2155HD-T [A... | 1319 | TRUE | |
| 192.168.[redacted] | NI-3200 [AMXM9... | 1319 | TRUE | |
| 192.168.[redacted] | NI-2200 [AMXM9... | 1319 | TRUE | |
| 192.168.[redacted] | NI-3200 [AMXM9... | 1319 | TRUE | |
| 192.168.[redacted] | NX-3200 [AMXM9... | 1319 | TRUE | |
| 192.168.[redacted] | New Master Cont... | 1319 | TRUE | Username |

**FIG. 19** NetLinx Studio - Communication Settings dialog

a. Click on the new IP address entry in the *List of Addresses* window

b. Click **Select** to use the selected IP address as the current IP address.

7. Click **OK** to save your newly entered information and close the *Communication Settings* dialog and return to the *Communication Settings* dialog. Note the selected IP address is indicated in the *Configuration* field (FIG. 20):



Current Master Connection

Network: 192.168.[redacted] - NX-3200 [AMXM988DAA]

**FIG. 20** NetLinx Studio - Communication Settings dialog (Current Master Connection field indicating the selected IP address)

8. Click **OK** to begin the communication process to your Master (and close the dialog).
   - If you are currently connected to a Master, a pop-up asks whether you would want to stop communication to the current Master and apply the new settings.
   - Click **Yes** to interrupt the current communication from the Master and apply the new settings.

**NOTE:** *On the front panel of the NetLinx Master, the STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*

9. Click the **OnLine Tree** tab in the Workspace window to view the devices on the System. *The default System value is one (1)*.
10. 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.*

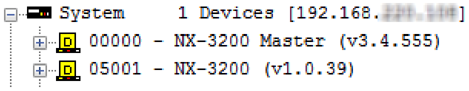
**NOTE:** *If the connection fails to establish, a Connection Failed dialog appears. Try selecting a different IP address if communication fails. Press the Retry button to reconnect using the same communication parameters. Press the Change button to alter your communication parameters and repeat the steps above.*

# Upgrading Firmware

## Overview

The basic process of upgrading firmware on NX-series controllers involves downloading the latest firmware files from *www.amx.com* and using NetLinx Studio to transfer the files to a target NX controller.

Use the OnLine Device tree in NetLinx Studio to view the firmware files currently loaded on the Central Controller. FIG. 21 shows an example OnLine Tree indicating an NX-3200:



```
System     1 Devices [192.168.[redacted]]
  00000 - NX-3200 Master (v3.4.555)
  05001 - NX-3200 (v1.0.39)
```

**FIG. 21** NetLinx Studio - Sample OnLine Tree

While the method of upgrading firmware files is the same for all Central Controllers, there are some specific points relative to the specific model and type of controller that must be noted:

### NX Controllers - Firmware Files

NX controllers contain two devices (*NX Master* and *Device Controller*), each of which require a separate firmware (*.kit) file.

The NX Master firmware file is not the same as the Device Controller firmware file. These two devices must be kept at compatible firmware versions for proper operation. Therefore, both files should be used when upgrading any firmware associated with the Integrated Controllers.

| NX Controllers - Firmware Files | |
|---|---|
| **NX Master Firmware** | The on-board **NX Master** is listed first in the OnLine Tree as<br>"**00000 NX Master (<firmware version>)**"<br>For example, the NX Master in FIG. 21 above is "*00000 - NX-3200 Master (v3.4.555)*".<br>• "**00000**" represents *Device ID 0*, which is reserved for the Master<br>• The number in parenthesis (in this case "*v3.4.555*") is the current NX Master firmware version. |
| **Device Controller Firmware** | The **Device Controller** is listed next as "**05001 NX-XXXX (<firmware version>)**"<br>For example, the Device Controller in FIG. 21 above is "*05001 - NX-3200 (v1.0.35)*".<br>• "**05001**" represents *Device ID 5001*, which is reserved for the Device Control ports.<br>• The number in parenthesis (in this case "*v1.0.35*") is the current Device Controller firmware version. |

### Enova DVX

Enova DVX All-In-One Presentation Switchers contain three devices (*NX Master*, *Device Controller*, and *A/V Switcher/ Scaler*), each of which require a separate Kit file. These three devices must be kept at compatible firmware versions for proper operation. Therefore, all three files should be used when upgrading any firmware associated with the Enova DVX All-In-One Presentation Switchers.

| DVX Controllers - Firmware Files | |
|---|---|
| **NX Master Firmware** | The on-board **NX Master** is listed first in the Online Tree as<br>**"00000 NX Master (<firmware version>)"**<br>• **"00000"** represents **Device ID 0**, which is reserved for the Master<br>• The number in parenthesis is the current Master firmware version. |
| **Device Controller Firmware** | The **Device Controller** is listed next as<br>**"05001 NX-XXXX (<firmware version>)"**<br>• **"05001"** represents **Device ID 5001**, which is reserved for the Device Control ports.<br>• The number in parenthesis is the current Device Controller firmware version. |
| **A/V Switcher/Scaler Firmware** | The A/V Switcher/Scaler is listed third as<br>**"05002 NX-XXXX (<firmware version>)"**<br>• **"05002"** represents **Device ID 5002**, which is reserved for the A/V Switcher/Scaler.<br>• The number in parenthesis is the current Device Controller firmware version. |

## Before You Start

1. Verify you have the latest version of the NetLinx Studio application installed on your PC.

   NetLinx Studio is available to download from *www.amx.com*. Login to download the latest version. Alternatively, if it is already installed, use the **Web Update** option in NetLinx Studio's Help menu to obtain the latest version.

   The default location for the NetLinx Studio application is **Start** > **Programs** > **AMX Control Disc** > **NetLinx Studio** > **NetLinx Studio**.
2. Verify that a LAN cable is connected from the controller to the LAN Hub.
3. Verify that the controller is powered on.
4. Connect to the controller via IP address.
5. Establish what version of firmware is currently loaded on the controller (see *Verifying the Current Firmware Version* below).

## Verifying the Current Firmware Version

Use the OnLine Tree in NetLinx Studio (see FIG. 21 on page 28) to verify which version of each firmware file is currently installed.

**NOTE:** *These steps assume that you have already established a connection with the target Central Controller (see the Initial Configuration section on page 19 for details).*

1. In NetLinx Studio, click on the **OnLine Tree** tab (in the Workspace Bar) to view the devices on the System.
2. Click **Display** and select **Refresh System** from the context menu. This establishes a new connection to the System and populates the device tree with devices on that system.
3. After the *Communication Verification* dialog indicates active communication between the PC and the Central Controller, verify the Central Controller and associated devices are listed in the OnLine Tree.
4. Check the appropriate product page on *www.amx.com* for the latest *NX Master* and *Device Controller* firmware files for your device.

If necessary, follow the procedures outlined in the following sections to obtain these firmware (*.kit) files from *www.amx.com* and then transfer the new firmware files to the device.

## Downloading the Latest Firmware Files from www.amx.com

### NetLinx Integrated Controllers

NX-series Controllers require two firmware (*.kit) files: *Master* firmware and *Device* firmware. The Master firmware file is not the same as the Device firmware file.

Both files should be used when upgrading any firmware associated with the Integrated Controllers.

**IMPORTANT:** *The process of downloading and transferring firmware files is the same for all types of firmware. However, it is important that the firmware files are upgraded in specific following order for NX-series Controllers (see the Required Order of Firmware Updates* section on page 31*).*

### Master and Device Firmware Kit Files for NX-Series Controllers

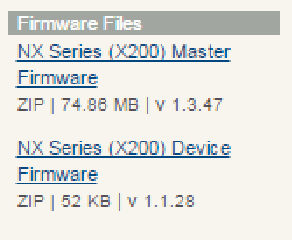
Below is a table outlining the *Master* and *Device* Firmware (*.kit) files used by NetLinx Integrated Controllers:

| Master and Device Firmware Files for NX-Series Controllers | |
|---|---|
| NX-4200 / 3200 / 2200 / 1200 | **Master** Firmware: **SW2106_NX_X200_Master_vx_x_xxx.kit** |
| | **HTTP Firmware Kit**: **SW2106_NX_X200_10x_vx_x_xxx-http.kit** |

**NOTE:** *The HTTP firmware kit enables you to upgrade firmware via an HTTP server. Follow the same steps in NetLinx Studio as you would with a typical firmware upgrade. Upgrading firmware via HTTP server is typically much faster than upgrading with the standard firmware kit files. See the Upgrading Firmware via NetLinx Studio section on page 31 for more information.*

### Downloading NX-Series Controller Firmware Files on www.amx.com

Visit the appropriate product page on www.amx.com for the latest *NX Master* and *Device Controller* firmware (*.kit) files for your NX controller. Firmware file links are available along the right-side of the catalog page (FIG. 22):



Firmware Files

NX Series (X200) Master Firmware
ZIP | 74.86 MB | v 1.3.47

NX Series (X200) Device Firmware
ZIP | 52 KB | v 1.1.28

**FIG. 22** www.amx.com - sample NX Controller Firmware File links

Firmware files are bundled in a ZIP file, along with a Readme.TXT file that provides details on this firmware release.

1. Accept the *AMX Licensing Agreement*.
2. Download the ZIP file and unzip the contents to a known location.

## Enova DVX All-In-One Presentation Switchers

Enova DVX All-In-One Presentation Switchers require an additional *Switcher Firmware* file for the built-in switcher. ALL files should be used when upgrading any firmware associated with the Integrated Controllers.

**NOTE:** *The process of downloading and transferring firmware files is the same for all types of firmware. However, it is important that the firmware files are upgraded in specific following order for DVX Controllers (see the Required Order of Firmware Updates for DVX Controllers section on page 31).*

### Master, Switcher and Device Firmware Files for Enova DVX All-In-One Presentation Switchers

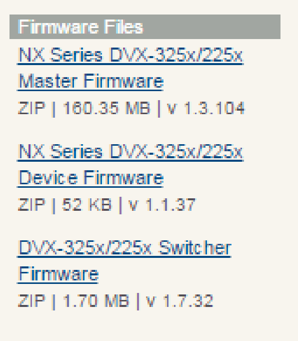
Below is a table outlining the *Master*, *Device,* and *Switcher* firmware (*.kit) files used by Enova DVX Controllers:

| Master Firmware Kit File Usage for Enova DVX Controllers | |
|---|---|
| DVX-3250/3255/3256<br>2250/2255/2210HD | **Master** Firmware: **SW2106_NX-X200_Master_v1_x_xxx.kit** |
| | **Device** Firmware: **SW2106_NX_X200_Device_v1_x_xx.kit** |
| | **HTTP Firmware Kit**: **SW2106_NX_X200_10x_vx_x_xxx-http.kit** |

**NOTE:** *The HTTP firmware kit enables you to upgrade firmware via an HTTP server. Follow the same steps in NetLinx Studio as you would with a typical firmware upgrade. Upgrading firmware via HTTP server is typically much faster than upgrading with the standard firmware kit files. See the Upgrading Firmware via NetLinx Studio section on page 31 for more information.*

### Downloading Enova DVX Firmware Files on www.amx.com

Visit the appropriate product page on www.amx.com for the latest *NX Master*, *Device Controller,* and *A/V Switcher/Scaler* firmware (*.kit) files for your Enova DVX All-In-One Presentation Switcher. Firmware file links are available along the right-side of the catalog page (FIG. 23):



Firmware Files

NX Series DVX-325x/225x Master Firmware
ZIP | 160.35 MB | v 1.3.104

NX Series DVX-325x/225x Device Firmware
ZIP | 52 KB | v 1.1.37

DVX-325x/225x Switcher Firmware
ZIP | 1.70 MB | v 1.7.32

**FIG. 23** www.amx.com - sample Enova DVX Firmware File links

Firmware files are bundled in a ZIP file, along with a Readme.TXT file that provides details on this firmware release.

1. Accept the *AMX Licensing Agreement*.
2. Download the ZIP file and unzip the contents to a known location.

### Master and Device Firmware Kit Files for Massio ControlPads

Below is a table outlining the *Master* and *Device* Firmware (*.kit) files used by Massio ControlPads:

| Master and Device Firmware Files for Massio ControlPads | |
|---|---|
| MCP-106/108 | **Master** Firmware: **SW2102_MCP_10x_vx_x_xxx.kit** |
| | **Device** Firmware: **SW2102_MCP_10x_Device_vx_xx_x.kit** |
| | **HTTP Firmware Kit**: **SW2102_MCP_10x_vx_x_xxx-http.kit** |

**NOTE:** *The HTTP firmware kit enables you to upgrade firmware via an HTTP server. Upgrading a Massio ControlPad to firmware version 1.4 or higher requires the current firmware version on the ControlPad to be version 1.3.106 or higher. Follow the same steps in NetLinx Studio as you would with a typical firmware upgrade. Upgrading firmware via HTTP server is typically much faster than upgrading with the standard firmware kit files. See the Upgrading Firmware via NetLinx Studio section on page 31 for more information.*

## Required Order of Firmware Updates

The *Upgrading Firmware via NetLinx Studio* instructions (below) apply equally to all types of firmware files. However, it is important that the firmware files are upgraded in the following order:

1. First, upgrade the **Master** firmware.
2. When that process is complete, upgrade the **Device** firmware.

**IMPORTANT:** *ALWAYS consult the Readme.TXT file bundled with the firmware file for any special instructions before upgrading to a newer firmware version. If no specifics are provided, use the order provided above.*

### Required Order of Firmware Updates for DVX Controllers

Upgrade firmware in the following order:

1. First, upgrade the **A/V Switcher/Scaler** firmware.
2. When that process is complete, upgrade the **Master** firmware.
3. When that process is complete, upgrade the **Device** firmware.

**IMPORTANT:** *ALWAYS consult the Readme.TXT file bundled with the firmware file for any special instructions before upgrading to a newer firmware version. If no specifics are provided, use the order provided above.*

## Upgrading Firmware via USB

All X-Series controllers support firmware upgrades via a USB solid-state drive. You can upgrade via USB by selecting the appropriate .kit file and initiating the upgrade via telnet. The “IMPORT KIT” telnet command causes the controller to search the attached USB drive for all valid .kit files and display the files as a list. From here you can select the .kit file to use and initiate the firmware upgrade. See the *IMPORT KIT* section on page 108 for more information.

## Upgrading Firmware via NetLinx Studio

**NOTE:** *These steps assume that you have already established a connection with the target Central Controller (IP connection is preferred.) See the Initial Configuration* section on page 19 *for details.*

1. In NetLinx Studio. click on the **OnLine Tree** tab (in the Workspace Bar) to view the devices on the System.
2. In the OnLine Tree tab, click **Display** and select **Refresh System** from the context menu. Doing so establishes a new connection to the System and populates the device tree with devices on that system.
3. After the *Communication Verification* dialog indicates active communication between the PC and the Central Controller, verify the Master and associated devices (including the *Device Controller*) are listed in the OnLine Tree.
4. In NetLinx Studio, select **Tools** > **Firmware Transfers > Send to NetLinx Device** (FIG. 24):

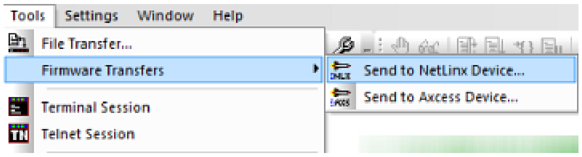
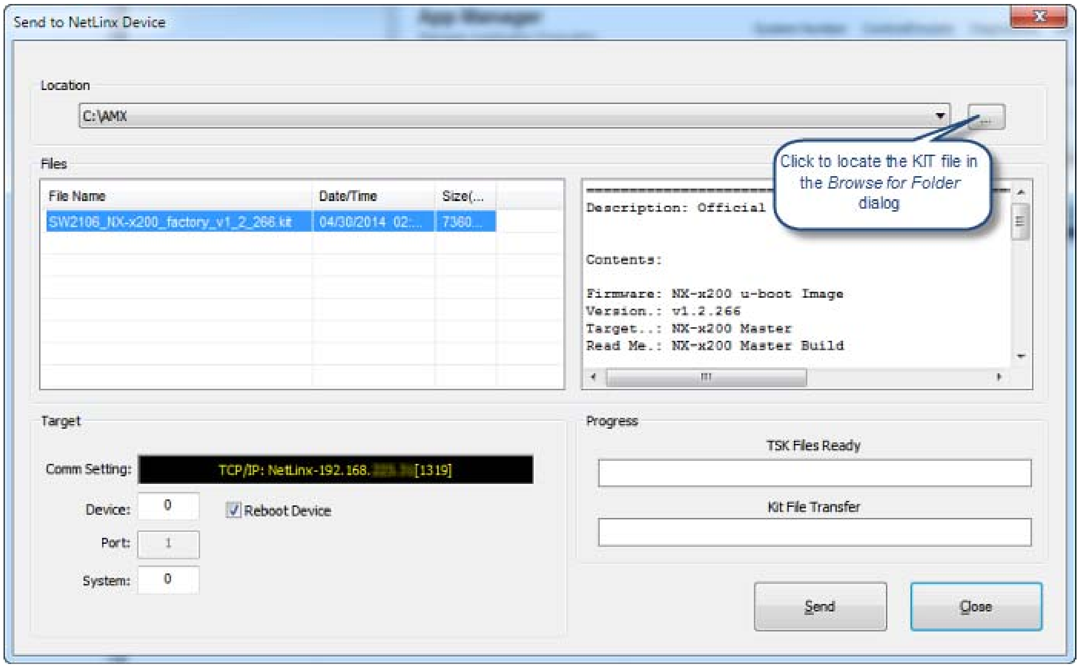


**FIG. 24** NetLinx Studio - Tools > Firmware Transfers > Send to NetLinx Device

This step opens the *Send to NetLinx Device* dialog.

5. Click the *Browse* button (**...**) to locate and select the firmware (*.kit) file that will be transferred, in the *Browse for Folders* dialog (FIG. 25):



Location: C:\AMX

| File Name | Date/Time | Size(... |
|---|---|---|
| SW2106_NX-x200_factory_v1_2_266.kit | 04/30/2014 02:... | 7360... |

```
Description: Official

Contents:

Firmware: NX-x200 u-boot Image
Version.: v1.2.266
Target..: NX-x200 Master
Read Me.: NX-x200 Master Build
```

Comm Setting: TCP/IP: NetLinx-192.168.[redacted][1319]

Device: 0 ☑ Reboot Device

Port: 1

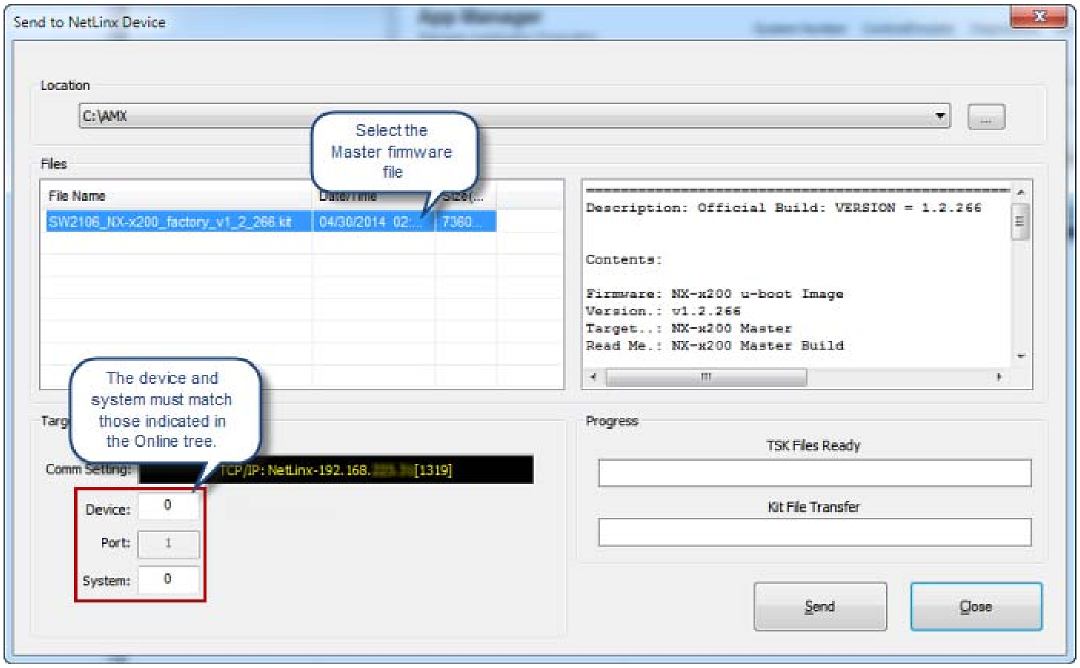
System: 0

Click to locate the KIT file in the *Browse for Folder* dialog

**FIG. 25** NetLinx Studio - Send to NetLinx Device dialog

The selected file is indicated in the *Files* window.

6. Verify the target's *System* number matches the value listed within the active System folder in the OnLine Tree.
   - The *Device* number is always **0** for the NX Master.
   - Note that the *Port* field is disabled (FIG. 26).



Location: C:\AMX

| File Name | Date/Time | Size(... |
|---|---|---|
| SW2106_NX-x200_factory_v1_2_266.kit | 04/30/2014 02:... | 7360... |

```
Description: Official Build: VERSION = 1.2.266

Contents:

Firmware: NX-x200 u-boot Image
Version.: v1.2.266
Target..: NX-x200 Master
Read Me.: NX-x200 Master Build
```

Comm Setting: TCP/IP: NetLinx-192.168.[redacted][1319]

Device: 0

Port: 1

System: 0

Select the Master firmware file

The device and system must match those indicated in the Online tree.

**FIG. 26** Send to NetLinx Device dialog (showing on-board NX Master firmware update)

7. Click **Send** to begin the transfer. The file transfer progress is indicated in the *Progress* section of the dialog. The Master reboots when the file transfer is complete.
8. Click **Close** once the Master is finished rebooting.
9. In the OnLine Tree, right-click on the Master and select **Refresh System**. This establishes a new connection and refreshes the device list and their firmware versions in your system.

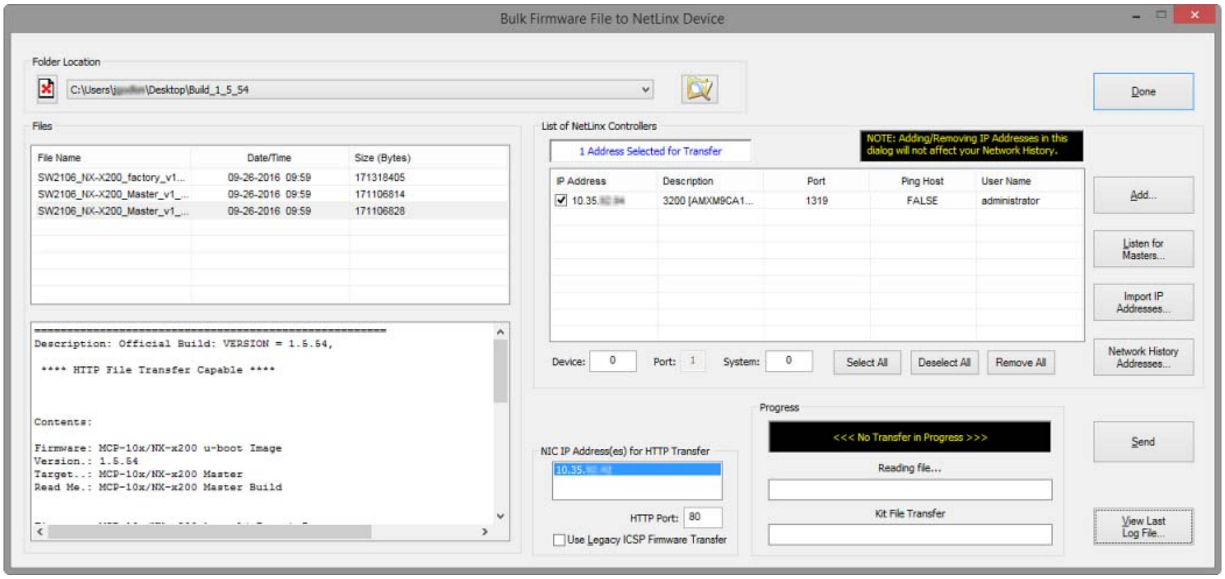
Once the process is complete, you can upgrade the remaining firmware files. All device files must be kept at compatible firmware versions for proper operation. Therefore, all files should be used when upgrading any firmware associated with the Integrated Controllers.

Be sure to follow the required order for installing firmware files. See the *Required Order of Firmware Updates* section on page 31 for more information.

## Sending Firmware to Multiple NetLinx Devices

You can send one version of firmware to multiple NetLinx devices sequentially with one click of a button through the Bulk Firmware to NetLinx Device dialog. You can access this dialog from the context menu of the online tree and from the “Tools-Firmware Transfers-Bulk Firmware Transfers...” menu item.

1. In NetLinx Studio, select **Tools > Firmware Transfers > Bulk Firmware Transfers**. The Bulk Firmware to NetLinx Device dialog opens (FIG. 27).



Folder Location

C:\Users\[redacted]\Desktop\Build_1_5_54

Files

| File Name | Date/Time | Size (Bytes) |
|---|---|---|
| SW2106_NX-X200_factory_v1... | 09-26-2016 09:59 | 171318405 |
| SW2106_NX-X200_Master_v1_... | 09-26-2016 09:59 | 171106814 |
| SW2106_NX-X200_Master_v1_... | 09-26-2016 09:59 | 171106828 |

```
=======================================================
Description: Official Build: VERSION = 1.5.54,

 **** HTTP File Transfer Capable ****


Contents:

Firmware: MCP-10x/NX-x200 u-boot Image
Version.: 1.5.54
Target..: MCP-10x/NX-x200 Master
Read Me.: MCP-10x/NX-x200 Master Build
```

List of NetLinx Controllers

1 Address Selected for Transfer

NOTE: Adding/Removing IP Addresses in this dialog will not affect your Network History.

| IP Address | Description | Port | Ping Host | User Name |
|---|---|---|---|---|
| ☑ 10.35.[redacted] | 3200 [AMXM9CA1... | 1319 | FALSE | administrator |

Device: 0 Port: 1 System: 0

NIC IP Address(es) for HTTP Transfer

10.35.[redacted]

HTTP Port: 80

☐ Use Legacy ICSP Firmware Transfer

Progress

<<< No Transfer in Progress >>>

Reading file...

Kit File Transfer

**FIG. 27** Bulk Firmware File to NetLinx Device Dialog

**NOTE:** *This dialog can also be accessed by right-clicking on the target device in the Online Device Tree and selecting Bulk Firmware Transfer from the Online Device Tree context menu.*

2. Click the **Browse for KIT Directories** button to navigate to the target directory (in the Select Folder dialog). The selected directory path is displayed in the Folder Location field. Assuming that the specified target directory contains one or more Kit files, the Kit files in the selected directory are displayed in the Files list box (with the file's last modified date and time).
3. Select the appropriate KIT file from the Files list.
4. Under **List of NetLinx Controllers**, set the Device and System number of the device that is the target for this firmware transfer. The port is preset to 1, so you cannot edit the Port field.
5. Select one or more NetLinx controllers from the table to receive the KIT file by clicking the check box beside its IP address. If you want to add more NetLinx devices to the list of controllers, perform any of the following tasks:
    - Click **Add** to open the New TCP/IP Setting dialog and configure a new TCP/IP connection.
    - Click **Listen for Masters** to open the Listen for Masters dialog and listen for Masters on the same subnet.
    - Click **Import IP Addresses** to open the Import IP Address List File dialog and import a saved list of IP addresses.
    - Click **Network History Addresses** to open the Network History Selection dialog so you can select one or more controllers from your history to receive the KIT file.
6. If your PC has more than one NIC Card, use the NIC IP Address(es) for HTTP Transfer option to select which NIC card to use for this transfer.
    - **HTTP Port**: Specify which port to use for HTTP transfers. In most cases, the default setting of 80 should work.
    - **Use Legacy ICSP Firmware Transfer**: Check this option to use ICSP (rather than HTTP) for this transfer.
7. Click **Send** to initiate the firmware transfer. The progress of the transfer is indicated in the Progress area.
8. When the transfer is complete, each Master reboots.

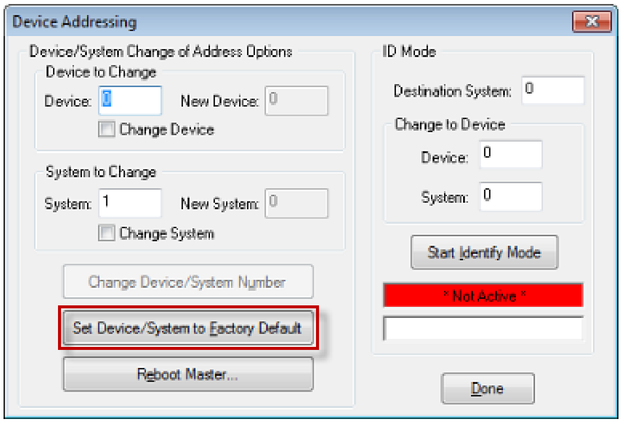
**NOTE:** *Allow 20-30 seconds for NetLinx Masters to reboot. When the Master has rebooted, the Status LED on the front panel blinks once a second to indicate that it is functioning properly.*

**NOTE:** *If for any reason a Kit file transfer to a NetLinx Master should fail, continue to retry the transfer until you are successful. DO NOT reboot the Master, or change connections until the transfer is complete. Failure to complete this operation successfully may result in a factory repair of the Master.*

9. When finished, click **Done** to close the dialog.

# Resetting the Factory Default System and Device Values

1. In NetLinx Studio, access the *Device Addressing* dialog:
   - 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 (FIG. 28):



Device Addressing

Device/System Change of Address Options

Device to Change

Device: 0 New Device: 0

□ Change Device

System to Change

System: 1 New System: 0

□ Change System

ID Mode

Destination System: 0

Change to Device

Device: 0

System: 0

* Not Active *

Change Device/System Number
Set Device/System to Factory Default
Reboot Master...
Start Identify Mode
Done

**FIG. 28** Device Addressing dialog

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.

**NOTE:** *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. Click **Done**. Wait 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.
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 these changes to your NetLinx Project.

# On-Board WebConsole User Interface

## WebConsole UI Overview

NetLinx Masters have a built-in System Configuration interface that allows you to make various configuration settings via a web browser on any PC that has access to the Master. The System Configuration interface (an on-board web configuration) contains a comprehensive set of web pages that can be used during setup to manage your system's network, security, and system needs, as well as configure its inputs and outputs while executing switches (FIG. 29).

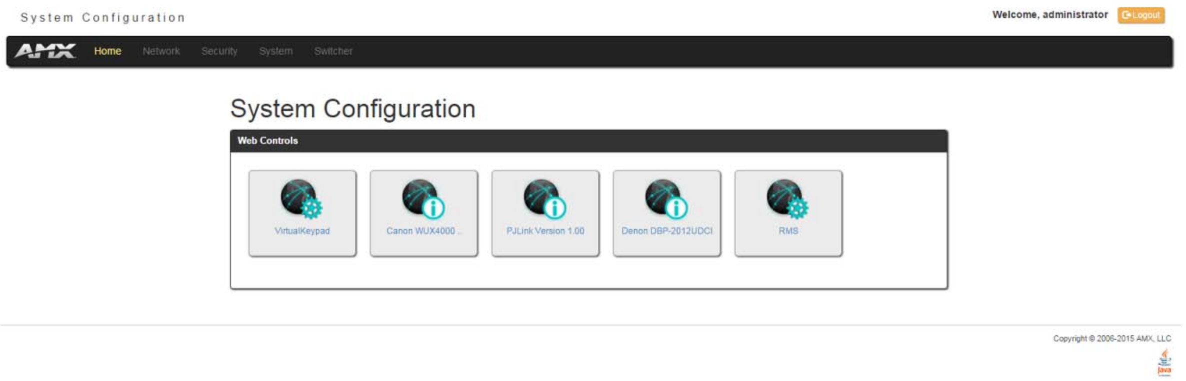


**FIG. 29** WebConsole - Web Controls page (initial view)

The WebConsole offers five primary sections from a menu located at the top of the page, indicated by five menu options across the top of the main page (FIG. 30):

**FIG. 30** System Configuration Menu Options

- **Home**: This option appears when you access the System Configuration page. Use these options to view any connected device or access a module.
- **Network**: Click to access the Network Settings for the Master. The options on these pages enable you to view and modify the IPv4 and IPv6 network settings and the clock settings for the system (see the *WebConsole - Network Options* section on page 37).
- **Security**: Click to access the System Security page. The options in this page allow you to configure various aspects of NetLinx System and Security on the Master, including network configuration and creating users and roles (see the *WebConsole - Security Options* section on page 42).
- **System**: Click to access the System Details page. The options on this page allow you to view and configure various aspects of the NetLinx System (see the *WebConsole - System Options* section on page 58).
- **Modules**: Click to access several different device-related pages (see the *WebConsole - Modules Options* section on page 60).
- **Switcher**: Click to access the Enova Switcher Configuration page (see the *WebConsole - Switching Options* section on page 68). This page only appears for Enova devices.

From the Home page, Web Control options become available (e.g., RMS, Virtual Keypad, and device details pages for any connected devices).

### System Configuration Interface Tips:

- It is recommended that you use the latest, industry accepted version of HTML5 browsers. If a browser is inconsistent, upgrade or try a different browser. To-date, browsers tested include Google Chrome (preferred), Mozilla Firefox, Apple Safari, and Microsoft Internet Explorer 10+/Edge.
- To access the interface after initial setup, simply type the integrated Master's IP address in the address bar of the browser and press the Enter key. On the DVX, DGX, and NX-4200, the IP address is available on the front panel display.
- Some devices run on a secured file-system. As such, file-system operations (e.g., Load and Save operations) may not be supported by the device's default capabilities and may require downloading a file manager application.
- When selecting Inputs and Outputs for switches – you may select an input followed by multiple outputs, but only one input is selectable if you select an output first.
- Inputs and Outputs can only have one name each, regardless of whether the name is set via the Video tab or the Audio tab in the Configuration page (or via NetLinx SEND_COMMANDs VIDIN_NAME, VIDOUT_NAME, AUDIN_NAME, AUDOUT_NAME). Inputs and Outputs may be named independently.

## Accessing the WebConsole

From any PC that has access to the LAN that the target Master resides on:

1. Open a web browser and type the IP Address of the target Master in the Address Bar.
2. Press Enter to access WebConsole for that Master. The initial view is the *Web Control* page (FIG. 29).

When using the Microsoft Internet Explorer browser in Windows 8, you may not be able to login and connect to the Master via the WebConsole. If you cannot login and connect, try any of the following options:

- Shift+Right-click Internet Explorer icon and select **Run as administrator**.
- Select Internet Options | Advanced | Security Settings, and check **Enable Enhanced Protection Mode**. A Windows 8 restart will be required.
- Use the Master's Hostname instead of its IP numeric address to enter the URL (e.g.: http://AMXM98A1A2B rather than http://192.168.1.123)
- Use a non-Windows 8 device if Internet Explorer 10+ is required.

## Default User Names and Passwords

The following table lists the default user names and passwords for accessing the NX-series controllers through NetLinx Studio or the WebConsole.

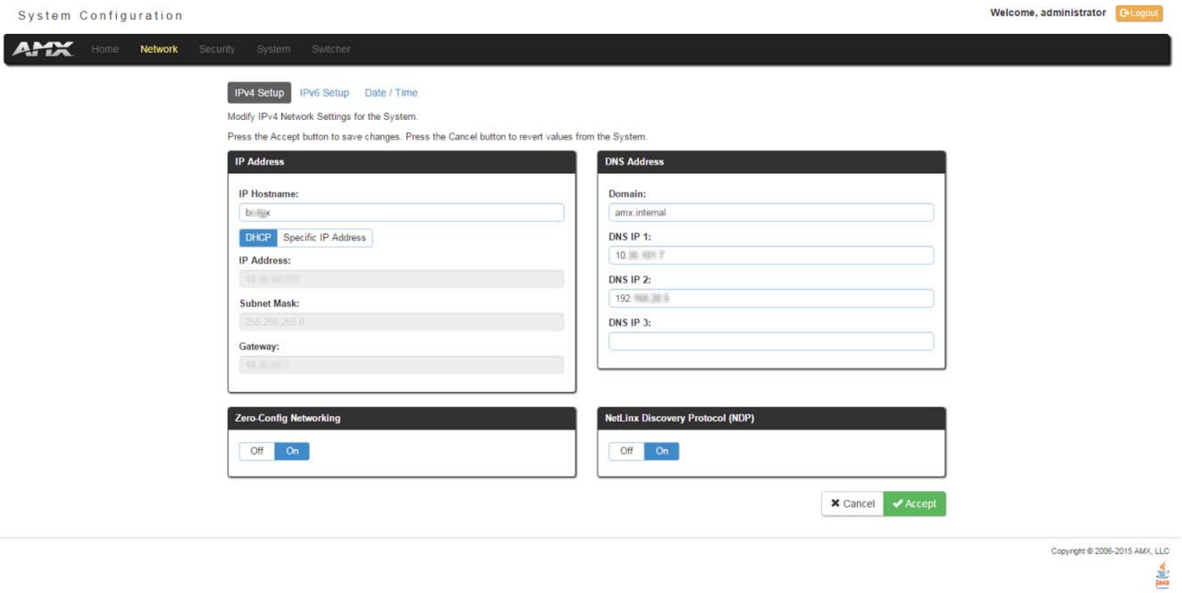
| Default User Names and Passwords | | |
|---|---|---|
| | **User Name** | **Password** |
| NetLinx Studio | netlinx | password |
| WebConsole | administrator | password |

# WebConsole - Network Options

## Network Overview

The *Network* page (FIG. 31) is accessed by clicking **Network** on the page's main heading. This page allows you to view and configure various aspects of the Master's network:

- **IPv4 Setup** - Options on this page allow you to view/change the Master's IP and DNS address information. See the *Network - IPv4 Setup* section on page 38 for details.
- **IPv6 Setup** - This page allows you to view the IPv6 address, subnet mask, and gateway for the Master. See the *Network - IPv6 Setup* section on page 39 for details.
- **Date/Time** - Options on this page allow you to enable/disable using a network time source and provide access to Daylight Saving configuration and which NIST servers to use as a reference. See the *Network - Date/Time* section on page 39 for details.



Modify IPv4 Network Settings for the System.

Press the Accept button to save changes. Press the Cancel button to revert values from the System.

**IP Address**

IP Hostname: b[redacted]x

[✓ DHCP] Specific IP Address

IP Address: 10.[redacted]

Subnet Mask: 255.255.255.0

Gateway: 10.[redacted]

**DNS Address**

Domain: amx.internal

DNS IP 1: 10.[redacted]

DNS IP 2: 192.[redacted]

DNS IP 3:

**Zero-Config Networking**

Off [✓ On]

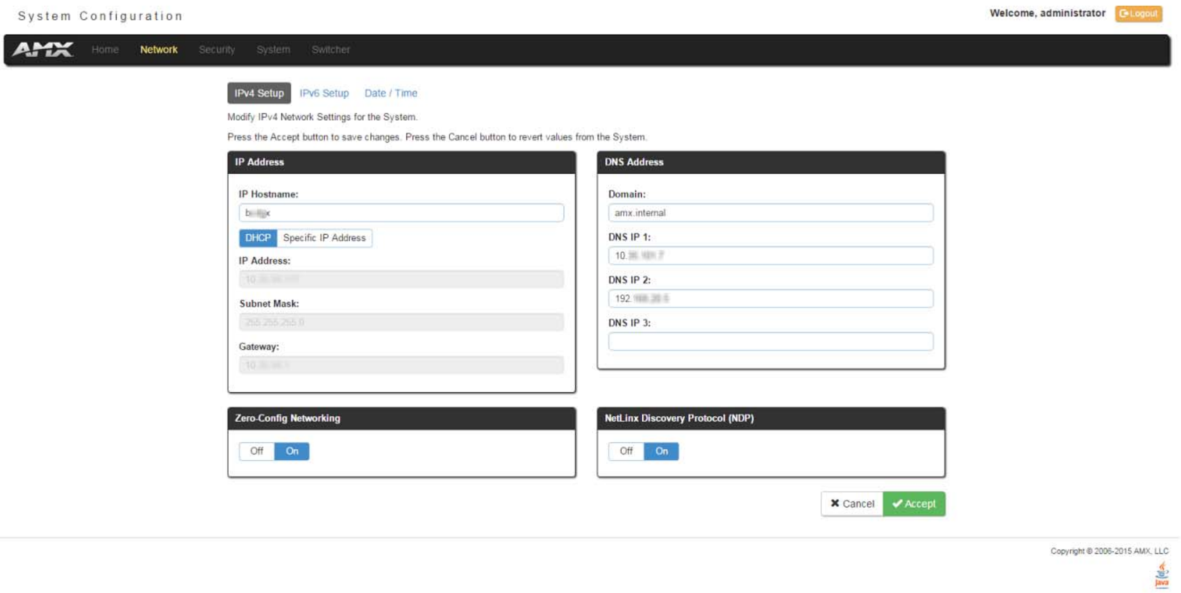
**NetLinx Discovery Protocol (NDP)**

Off [✓ On]

**FIG. 31** Network page

# Network - IPv4 Setup

Click **IPv4 Setup** to access the IPv4 page (FIG. 32) and view and configure IP and DNS addresses for the Master. Use the options on this page to view/edit the Master's network settings. A user can only modify the information on this page if it is assigned a Role that includes the Network Configuration permission. Without the proper permission, a user can only view the information on this page.



System Configuration

Welcome, administrator

Modify IPv4 Network Settings for the System.

Press the Accept button to save changes. Press the Cancel button to revert values from the System.

**IP Address**

IP Hostname: b[redacted]

[✓ DHCP] Specific IP Address

IP Address: 10.[redacted]

Subnet Mask: 255.255.255.0

Gateway: 10.[redacted]

**DNS Address**

Domain: amx.internal

DNS IP 1: 10.[redacted]

DNS IP 2: 192.[redacted]

DNS IP 3:

**Zero-Config Networking**

Off [✓ On]

**NetLinx Discovery Protocol (NDP)**

Off [✓ On]

Copyright © 2006-2015 AMX, LLC

**FIG. 32** Network - IPv4 Setup page

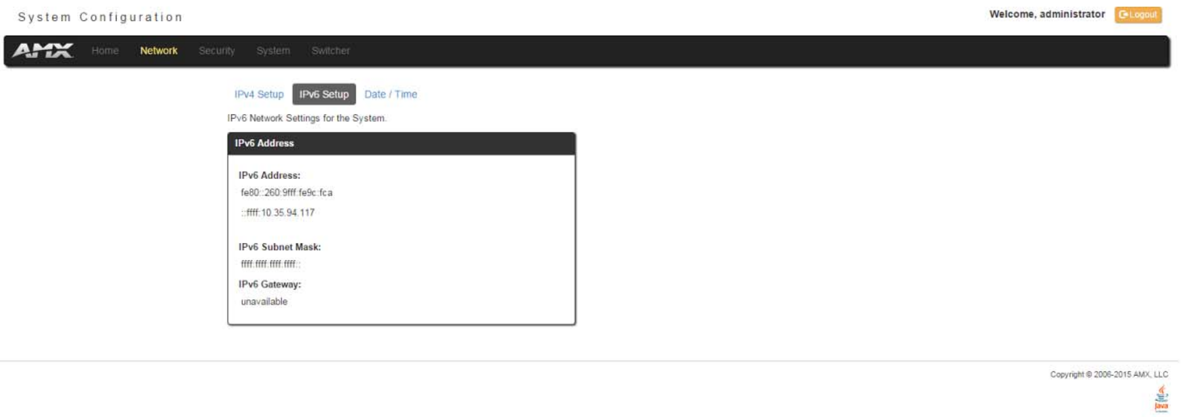
## IPv4 Options

The IPv4 options are described in the following table:

| **IPv4 Options** | |
|---|---|
| **Option** | **Description** |
| IP Address: | This section enables you to set IP information for the Master's network. |
| IP Hostname | Enter the IP host name in this field. |
| DHCP/Specific IP Address | Use the buttons to select a DHCP or static IP address. Additional options in this area become available if you select Specific IP Address. |
| IP Address | Enter the IPv4 address in this field. This field is only available if you select Specific IP Address. |
| Subnet Mask | Enter the IPv4 subnet mask in this field. This field is only available if you select Specific IP Address. |
| Gateway | Enter the gateway IPv4 address in this field. This field is only available if you select Specific IP Address. |
| DNS Address: | This section enables you to set DNS information for the Master's network. |
| Domain | Enter the domain name of the DNS server in this field. |
| DNS IP | Enter up to three DNS server addresses in the provided fields. |
| Zero-Config Networking | Use the buttons to activate zero-config networking functionality on the Master's network. Zero-config networking provides the ability to automatically discover devices that are present on the LAN. By default, zeroconf is enabled (On option selected). With zeroconf enabled, the Master's web interface will be registered via zeroconf and can be viewed through a zeroconf browser plug-in such as Bonjour for IE. |
| NetLinx Discovery Protocol (NDP) | Use the buttons to indicate whether you want the Master to search for any NDP-capable devices currently connected to the Master. |

## Network - IPv6 Setup

Click **IPv6 Setup** to access the IPv6 page (FIG. 33) and view the IPv6 address, subnet mask, and gateway for the Master. This information is view-only.



IPv6 Network Settings for the System.

**IPv6 Address**

IPv6 Address:
fe80::260:9fff:fe9c:fca
::ffff:10.35.94.117

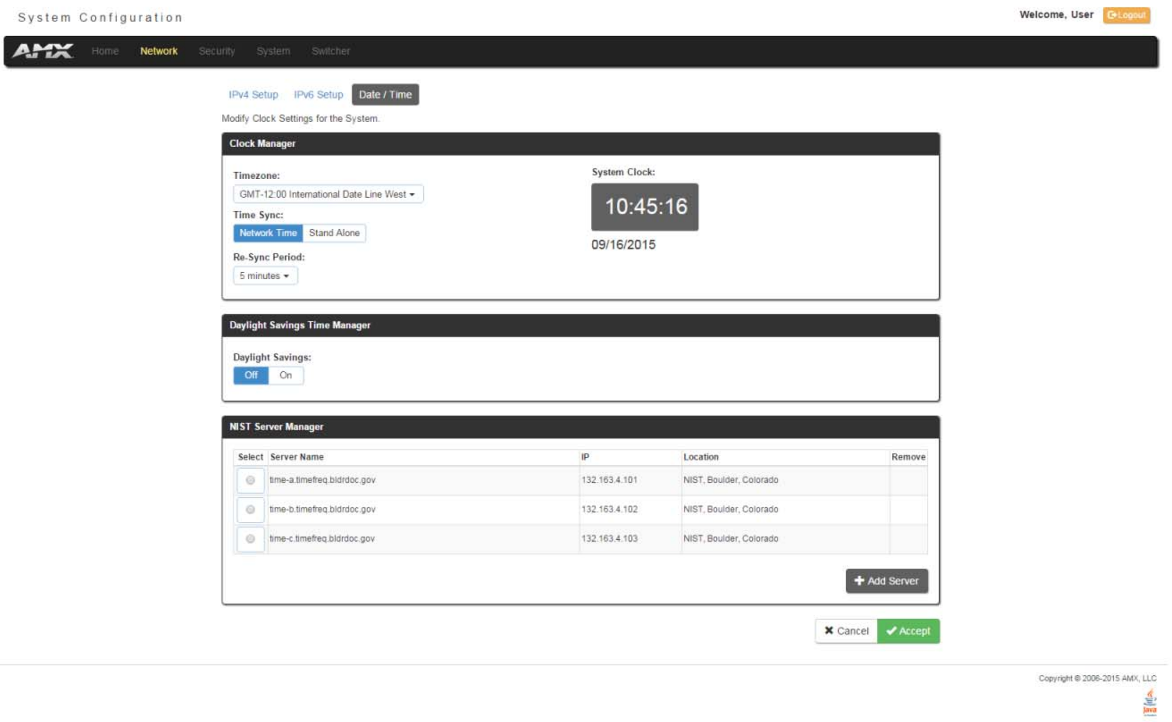
IPv6 Subnet Mask:
ffff:ffff:ffff:ffff::

IPv6 Gateway:
unavailable

**FIG. 33** Network - IPv6 Setup page

## Network - Date/Time

Click the **Date/Time** link (on the *Network* page) to access the *Date/Time* page (FIG. 34). The options on this page allow you to enable/disable using a network time source and provide access to Daylight Saving configuration and which NIST servers to use as a reference.



Modify Clock Settings for the System.

**Clock Manager**

Timezone: GMT-12:00 International Date Line West

Time Sync: [✓ Network Time] Stand Alone

Re-Sync Period: 5 minutes

System Clock: 10:45:16
09/16/2015

**Daylight Savings Time Manager**

Daylight Savings: [✓ Off] On

**NIST Server Manager**

| Select | Server Name | IP | Location | Remove |
|---|---|---|---|---|
| ○ | time-a.timefreq.bldrdoc.gov | 132.163.4.101 | NIST, Boulder, Colorado | |
| ○ | time-b.timefreq.bldrdoc.gov | 132.163.4.102 | NIST, Boulder, Colorado | |
| ○ | time-c.timefreq.bldrdoc.gov | 132.163.4.103 | NIST, Boulder, Colorado | |

**FIG. 34** Network - Date/Time page

The Clock Manager Options are separated into three areas:

- **Clock Manager** - The Clock Manager allows you to set the Clock Manager Mode (Network Time or Stand Alone).
- **Daylight Savings Time Manager** - The Daylight Savings Time Manager allows you to specify how and when to implement Daylight Savings rules on the clock.
- **NIST Server Manager** - The NIST Server Manager allows you to connect to a specific NIST (Internet Time Service) Server.

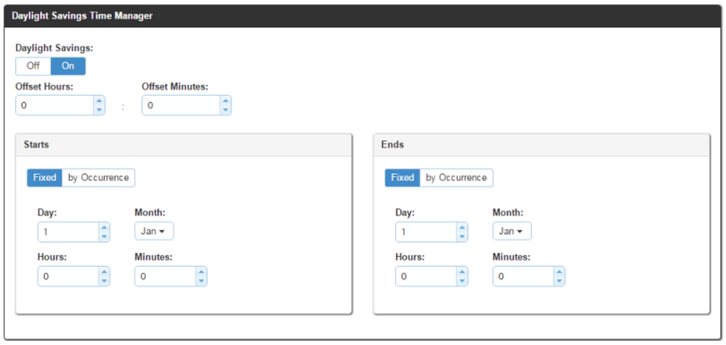
## Setting the Mode for the Clock Manager

1. In the *Manage System* tab (FIG. 34), select a **Time Sync** option.
   - **Network Time**: This option allows the Master to manage it's clock by connecting to a NIST (Internet Time Service) Server. When this option is selected, the Master will connect to the default NIST Server to get date and time information.

     You can select a different NIST Server (or specify the IP Address of a known NIST Server) in the *NIST Server Manager* section (see the *Selecting a Custom NIST Server* section on page 40).
   - **Stand Alone**: This option lets the Master use its own internal clock. When this option is selected, two additional fields are available on this tab:
     - **Date** - Enter the current date in this field (mm/dd/yyyy).
     - **Time** - Enter the current time in these fields (Hours/Minutes/Seconds).
2. Click **Accept** to save these settings to the Master.

## Setting Daylight Savings Rules

1. In the *Daylight Savings Time Manager* section (FIG. 35), enable Daylight Savings mode by clicking the **On** button. Clicking **On** reveals additional Daylight Savings options.



Daylight Savings Time Manager

Daylight Savings: Off [✓ On]

Offset Hours: 0 : Offset Minutes: 0

Starts

[✓ Fixed] by Occurrence

Day: 1 Month: Jan

Hours: 0 Minutes: 0

Ends

[✓ Fixed] by Occurrence

Day: 1 Month: Jan

Hours: 0 Minutes: 0

**FIG. 35** Date/Time Options - Daylight Savings Time Manager

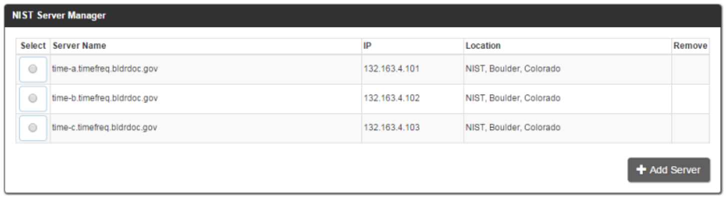
2. Use the **Offset** drop-down menus to adjust the amount of time (hours and minutes) to offset Daylight Savings. By default, the offset is set to 1 hour.

**NOTE:** *Although most places that support Daylight Savings usually adjust the local time by one hour this doesn't cover all locations. To provide flexibility for such locations it is possible to configure a different daylight savings time offset.*

3. Use the **Starts** fields to specify when Daylight Savings should start. The Starts rules include:
   - Select **Fixed** to specify the calendar date when the rule applies as a specific date ("March 21"). When *Fixed* is selected, use the **Day**, **Month**, **Hours,** and **Minutes** fields to specify the date and time (hh:mm) to start Daylight Savings time.
   - Select **by Occurrence** to specify the calendar date when the rule applies as a heuristic, ("the 3rd Sunday in March"). When *by Occurrence* is selected, use the **Wk of the Month**, **Day**, **Month**, **Hours**, and **Minutes** fields to specify the occurrence to start Daylight Savings time.

     The range for **Wk of the Month** is 1 through *Last*, where **Last** indicates the last occurrence of a particular day of the month. This is to accommodate months that include four weeks as well as those that include five.
4. Use the **Ends** fields to specify when Daylight Savings should end. The Ends rules match the Start rules, and follow the same logic. Select **Fixed** or **by Occurrence**, and specify the End date/time information accordingly.
5. Click **Accept** to save these settings to the Master.

## Selecting a Custom NIST Server



NIST Server Manager

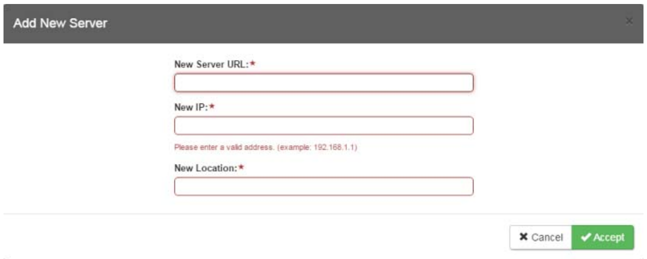
| Select | Server Name | IP | Location | Remove |
|---|---|---|---|---|
| ○ | time-a.timefreq.bldrdoc.gov | 132.163.4.101 | NIST, Boulder, Colorado | |
| ○ | time-b.timefreq.bldrdoc.gov | 132.163.4.102 | NIST, Boulder, Colorado | |
| ○ | time-c.timefreq.bldrdoc.gov | 132.163.4.103 | NIST, Boulder, Colorado | |

**FIG. 36** Date/Time Options - NIST Server Manager

1. In the *NIST Server Manager* section (FIG. 36), use the option buttons to select one of the NIST Servers in the list.
2. Click **Accept** to save the selection to the Master.

## Adding a Custom NIST Server to the List

1. Click **Add Server**. The Add New Server dialog opens (FIG. 37).



Please enter a valid address. (example: 192.168.1.1)

**FIG. 37** Add New Server dialog

2. In the **New Server URL** field, enter the URL of the NIST Server. The URL is used only to help you manage entries, and is not verified or used internally by the clock manager.
3. Enter the NIST Server's IP Address in the **New IP** field. This is used internally and must be a valid IP address.

   **NOTE:** *The strings entered into the URL and Location fields are not used to connect to NIST Servers. The IP Address (entered into the IP field) specifies the NIST Server(s) that will be used. As stated above, the address entered into the IP field must be must be a valid IP address (not a URL).*

4. Enter the NIST Server's location in the **New Location** field. This is used only to help the user manage entries and it is not verified or used internally by the clock manager.
5. Click **Accept** to save these settings to the Master.

## Removing an NIST Server From the List

1. Click on the **Remove** (x) button to the right of a *user-added* NIST Server in the *NIST Server Manager* list.
2. Click **Accept** to save these settings to the Master.

   **NOTE:** *The built-in entries cannot be removed.*

## Clock Manager NetLinx Programming API

Refer to *Appendix C: Clock Manager NetLinx Programming API* section on page 145 for a listing and description of the Types/ Constants and Library Calls that are included in the NetLinx.AXI to support Clock Manager functions.

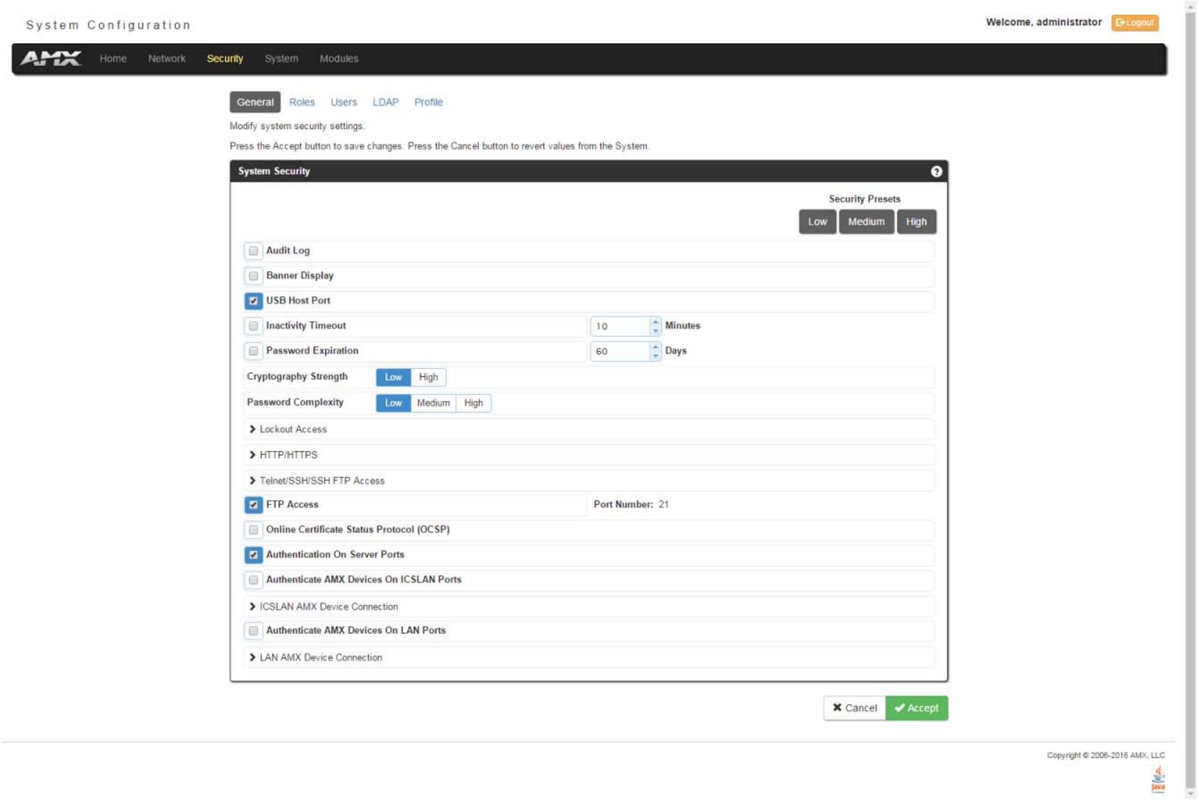
# WebConsole - Security Options

## Security Overview

The *Security* page is accessed by clicking **Security** on the page's main heading. This page allows you to view configure and modify the Master's security settings at three levels (System, Role, and User). See the *Security Presets* section on page 46 for more information on the three presets.

- **System Level** - changes made at this level affect the system globally. See the *Security - General* section on page 44 for details.
- **Role Level** - changes made at this level affect specific Roles. See the *Security - Roles* section on page 48 for details.
- **User Level** - changes made at this level affect individual Users. See the *Security - Users* section on page 52 for details.

The default view for the option is System Security Settings (FIG. 38).



Modify system security settings.

Press the Accept button to save changes. Press the Cancel button to revert values from the System.

□ Audit Log

□ Banner Display

☑ USB Host Port

□ Inactivity Timeout 10 Minutes

□ Password Expiration 60 Days

Cryptography Strength [✓ Low] High

Password Complexity [✓ Low] Medium High

> Lockout Access

> HTTP/HTTPS

> Telnet/SSH/SSH FTP Access

☑ FTP Access Port Number: 21

□ Online Certificate Status Protocol (OCSP)

☑ Authentication On Server Ports

□ Authenticate AMX Devices On ICSLAN Ports

> ICSLAN AMX Device Connection

□ Authenticate AMX Devices On LAN Ports

> LAN AMX Device Connection

**FIG. 38** System Security Settings

**NOTE:** *By default, all System-level security options are disabled, except for Authentication On Server Ports, which requires a login for access to the web or command line interface.*

Additional security configuration options are available via Terminal/Telnet Commands. See the *Accessing the Security Configuration Options* section on page 123.

### Login Rules

There is no limit to the number of concurrent logins allowed for a single user. This allows for the creation of a single user that is provided to multiple ICSP devices (touch panels, for example) using the same login to obtain access to the Master.

For example, if you have 50 devices connected to a Master, you do not have to create 50 individual user accounts, with one for each device. Instead, you only need to create one which all 50 devices use for access.

The first layer of security for the Master is to prompt a user to enter a valid user name and password before gaining access to a secured feature on the target Master.

Depending on the Security configuration, users may be prompted to enter a valid user name and password before gaining access to various features of the WebConsole. User access is specified by the administrator in the Role and User Level pages of the Security section.

**NOTE:** *This user name and password information is also used by both G5 touch panels (within the System Connection firmware page) and AMX software applications such as NetLinx Studio v 4.0 and above to communicate securely with a Master using encrypted communication.*

### User and Role Name Rules

User account and role names must follow these rules:

- Case-sensitive
- Must be between 4 and 20 alpha-numeric characters: A-Z, a-z, 0-9
- The following characters are allowed: - _ . # and <space>.

### Password Rules

The rules for changing a password vary according to the Password Complexity setting for the user. A user's password complexity can be set to Low, Medium, or High.

- **Low** - Minimum length is 4 characters, and must be different from previous password.
- **Medium** - Minimum length is 8 characters, must contain characters from 3 character classes listed in the table below, must contain at least 4 changes from the previous password, and must be different from the previous 10 passwords.
- **High** - Minimum length is 15 characters, must contain characters from all of the characters classes listed in the table below, must contain at least 8 changes from the previous password, and must be different from the previous 30 passwords.

The requirements for each setting are listed in the following table:

| Password Complexity Requirements | | | |
|---|---|---|---|
| **Requirement** | **Low** | **Medium** | **High** |
| Case Change Only | No | No | Yes |
| Character Classes Required | 0 | 3 | 4 |
| Library Check | No | No | Yes |
| Minimum Length | 4 | 8 | 15 |
| Palindrome Check | No | No | Yes |
| Same Consecutive Characters | No check | 5 | 3 |
| Similarity Check | 1 | 4 | 8 |
| User Name Check (straight or reversed) | No | Yes | Yes |
| Different from Previous # of Passwords | 1 | 10 | 30 |

The definitions of each requirement are listed below:

- **Case Change Only:** A new password cannot differ from the previous passwords solely by a change in case (upper/lower)
- **Character Classes Required:** A password must contain characters from a set number of character classes. See the Character Classes table below for the list and definitions of character classes.
- **Library Check:** The password cannot contain a word from a dictionary file supplied with the OS.
- **Minimum Length:** The password must contain a minimum set number of characters.
- **Palindrome Check:** The password does not contain a palindrome of a 7-letter length or greater.
- **Same Consecutive Characters:** The password does not contain more than a set number of the same consecutive characters.
- **Similarity Check:** The password differs from the previous password by a set number of characters.
- **User Name Check:** The password does not contain the user's user name.
- **Different from Previous # of Passwords:** The password differs from a set number of previous passwords.

The following table lists the characters available in each character class:

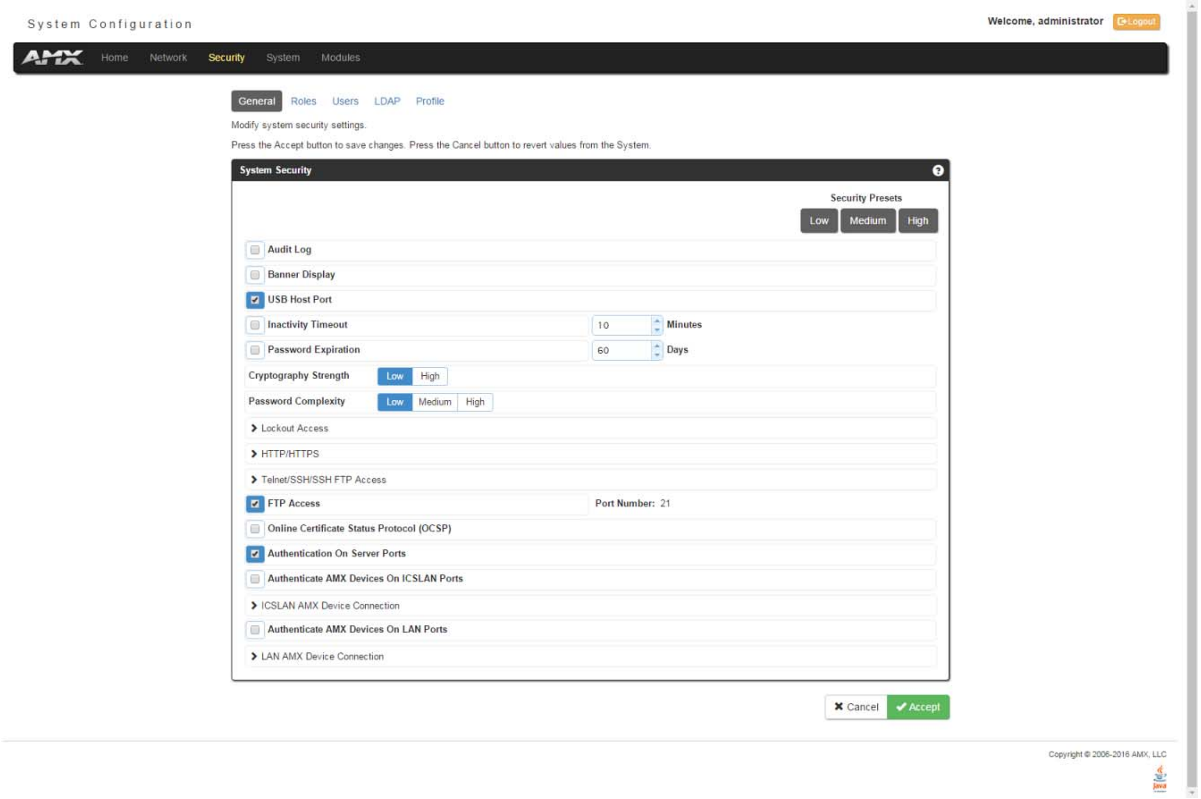
| Character Classes | |
|---|---|
| **Character Class** | **Example** |
| Uppercase Letters | A-Z |
| Lowercase Letters | a-z |
| Numbers | 0-9 |
| Other Characters | ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ \| : ; " ' <> , . ?/ (including "space") |

# Security - General

The General Security Settings page provides global permissions for various options that may be individually selected and applied to all users. The Master provides 3 levels of security settings presets: Low, Medium, and High. The levels are simply presets of various security settings. When a preset is selected, the settings are not applied until you click **Accept**. You can customize any settings as needed on the security preset before accepting and applying the settings. The default for the settings will match the Low presets.

## System Level Security - System Security Settings

Click the **System Security Settings** link to access the System Security Details page (FIG. 39). The options in this page allow you to establish whether the Master will require a valid user name and password be entered prior to gaining access to the configuration options.



Modify system security settings.

Press the Accept button to save changes. Press the Cancel button to revert values from the System.

□ Audit Log

□ Banner Display

☑ USB Host Port

□ Inactivity Timeout 10 Minutes

□ Password Expiration 60 Days

Cryptography Strength [✓ Low] High

Password Complexity [✓ Low] Medium High

> Lockout Access

> HTTP/HTTPS

> Telnet/SSH/SSH FTP Access

☑ FTP Access Port Number: 21

□ Online Certificate Status Protocol (OCSP)

☑ Authentication On Server Ports

□ Authenticate AMX Devices On ICSLAN Ports

> ICSLAN AMX Device Connection

□ Authenticate AMX Devices On LAN Ports

> LAN AMX Device Connection

**FIG. 39** System Security Settings

These are global options that enable or disable the login requirement for both users and roles.

## System Security Options

The System Security options are described in the following table:

| System Security Options | |
|---|---|
| **Option** | **Description** |
| Security Presets | The Master provides three levels of security setting presets: Low, Medium, and High. Each level is a preset of various security settings (see the *Security Presets* section on page 46 for more information.) When a preset is selected, that setting is applied after clicking Accept.<br>**NOTE:** *If a security preset is not selected, all subordinate options are grayed-out and not selectable, meaning that the Master is completely unsecured and can be altered by any user (regardless of their rights).* |
| Audit Log | Select to enable/disable remote syslog. See the *Audit Logs* section on page 47 for more information. |
| Banner Display | Select to turn on or turn off banner messages. Banners enable you to display pre- and post-login text in the WebConsole. See the *Banners* section on page 47 for more information. |
| USB Host Port | Select to enable all Type-A USB connectors on the Master. |
| Inactivity Timeout | Select to enable the Master to log out a user after a defined period of inactivity. After enabling the inactivity timeout option, use the spin box to set the number of minutes before the timeout activates. You can set a timeout in the range of 1 to 60 minutes. The default setting is 10 minutes. The timeout applies to Program Port, Telnet, SSH, HTTP, and HTTPS sessions. |

| System Security Options (Cont.) | |
|---|---|
| **Option** | **Description** |
| Password Expiration | Select to force a user to change its password after a set period of time. After enabling the password expiration options, use the spin box to set the interval for password expiration. You can set an amount of time in the range of 1 to 180 days. The default setting is 60 days.<br>**NOTE:** *This option is only valid on locally-maintained accounts. When external LDAP is enabled, only the administrator and device user accounts are affected.* |
| Cryptography Strength: | Set the cryptography strength of the Master to Low or High. On the High setting, only FIPS 140-2 validated binaries are used. |
| Password Complexity | Set the password complexity to Low, Medium, or High. When the password complexity level is raised from a lower level to a higher level, the Master requires confirmation from the user. When the user confirms the change, all passwords are marked as expired on all local user accounts, and the passwords must be changed to meet the new complexity requirements. Password complexity requirements are as follows:<br>• **Low** - Minimum length is 4 characters, and must be different from previous password.<br>• **Medium** - Minimum length is 8 characters, must contain characters from 3 of the following characters sets (uppercase letters, lowercase letters, numbers, other characters), must contain at least 4 changes from the previous password, and must be different from the previous 10 passwords.<br>• **High** - Minimum length is 15 characters, must contain characters from all of the following characters sets (uppercase letters, lowercase letters, numbers, other characters), must contain at least 8 changes from the previous password, and must be different from the previous 30 passwords.<br>**NOTE:** *This option is only valid on locally-maintained accounts. When external LDAP is enabled, only the administrator and device user accounts are affected.* |
| Lockout Access | Select to enable a lock on a user account after a set number of failed logins. When enabled, use the Attempts spin box to set the number of login attempts allowed. Use the Lockout Duration options menu to indicate the amount of time you want the lockout to last. The default setting is 60 minutes.<br>**NOTE:** *This option is only valid on locally-maintained accounts. When external LDAP is enabled, only the administrator user is affected.* |
| HTTP/HTTPS | Select to enable HTTP and HTTPS access to the Master.<br>**HTTP:** The port value used for unsecure HTTP Internet communication between the web browser's UI and the target Master. 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.<br>By default, the Master does not have security enabled and must be communicated with using **http://** in the *Address* field. The default port value is **80**.<br>**NOTE:** *One method of adding security to HTTP communication is 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). An example is if the port were changed to 99, the new address information would be: http://192.192.192.192:99.*<br>**HTTPS:** 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.<br>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. The default port value is **443**.<br>**NOTE:** *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). An example is if the port were changed to 99, the new address information would be: http://192.192.192.192:99.* |
| Telnet/SSH/SSH FTP Access | Select to enable Telnet, SSH, and SSH FTP access to the Master.<br>**Telnet:** The port value used for Telnet communication to the target Master. Enabling this feature allows future communication with the Master via a separate Telnet application.<br>• The default port value for Telnet is **23**.<br>• Refer to the *NetLinx Security with a Terminal Connection* section for more information on the related procedures.<br>**SSH:** The port value used for secure Telnet communication. 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.<br>• SSH **version 2** is supported.<br>• The default port value is **22**.<br>**NOTE:** *If this port's value is changed, make sure to use it within the Address field of the SSH Client application.* |

| System Security Options (Cont.) | |
|---|---|
| **Option** | **Description** |
| FTP Access | Select to enable FTP access to the Master. The default port value used for FTP communication is 21.<br>**NOTE:** *This port can be disabled/enabled, but its value cannot be changed.* |
| Online Certificate Status Protocol (OCSP) | Select to enable usage of the OCSP to validate received certificates before trusting the sending site. |
| Authenticate on Server Ports | Select to require user name and password authentication on Telnet, Program, and HTTP/HTTPS ports. Authentication is always required on FTP/SFTP and SSH ports.<br>**NOTE:** *If Authenticate on Server Ports is disabled but LDAP is enabled, a login is still required. If you do not desire a login, LDAP must also be disabled.* |
| Authenticate AMX Devices On ICSLAN Ports | Select to require user name and password authentication on devices connected to the ICSLAN ports on the Master. |
| ICSLAN AMX Device Connection | Select to allow ICSP access to the Master for Device-type users connected to the ICSLAN ports. Expand the ICSLAN AMX Device Connection section to view this option. |
| ICSLAN Encryption | Select to enable encryption on the ICSLAN ports on the Master. Expand the ICSLAN AMX Device Connection section to view this option. |
| Authenticate AMX Devices On LAN Ports | Select to require user name and password authentication on devices connected to the LAN ports on the Master. |
| LAN AMX Device Connection | Select to allow ICSP access to the Master for Device-type users connected to the LAN ports. Expand the LAN AMX Device Connection section to view this option. |
| LAN Encryption | Select to enable encryption on the LAN ports on the Master. Expand the LAN AMX Device Connection section to view this option. |

## Security Presets

The Master provides three levels of security setting presets: Low, Medium, and High. Each level is a preset of various security settings. The following table describes each of the Security Presets presented on the General section of the Security page:

| Security Presets | | | |
|---|---|---|---|
| **Preset** | **Low** | **Medium** | **High** |
| Audit Log | Off | On | On |
| Banner Display | Off | On | On |
| USB Host Port | Enabled | Enabled | Disabled |
| Authentication On Server Ports | Required | Required | Required |
| Inactivity Timeout | Off | On | On |
| Password Expiration | Disabled | Enabled | Enabled |
| Cryptography Strength | Low | Low | High |
| Password Complexity | Low | Medium | High |
| Lockout Access | Off | On | On |
| FTP Access | Both enabled | Disabled/Enabled | Disabled/Disabled |
| HTTP/HTTPS | Both enabled | Disabled/Enabled | Disabled/Disabled |
| Telnet/SSH/SSH FTP Access | Both enabled | Disabled/Enabled | Disabled/Disabled |
| OCSP | Disabled | Disabled | Enabled |
| Authenticate AMX Devices on ICSLAN Ports | Not required | Required | Required |
| ICSLAN AMX Device Connection | ICSPS enabled, ICSP enabled - without encryption | ICSPS enabled, ICSP enabled - with encryption | ICSPS enabled, ICSP disabled |
| Authenticate AMX Devices on LAN Ports | Not required | Required | Required |
| LAN AMX Device Connection | ICSPS enabled, ICSP enabled - without encryption | ICSPS enabled, ICSP enabled - with encryption | ICSPS enabled, ICSP disabled |

Once any of the settings have been modified, press the **Accept** button to save these changes to the Master. Once these changes are saved, the following message appears: *"Device must be rebooted for the setting to take effect. To reboot, go to the System Devices page."* A link appears which you can click to jump to the System Devices page (see the *System - Devices* section on page 59 for more information.) Click the **Reboot** button to remotely reboot the target Master.

## Audit Logs

An audit log includes the date/time of the event, the event type, the software or hardware component where the event occurred, the source of the event, the subject identity, and the outcome of the event. For events related to a remote device, the audit log includes the source and destination network addresses and ports or protocol identifiers.

The Master generates an audit record for the following events:

- Each successful or unsuccessful attempt to access security files
- Alerts and errors
- Starting/Shutting down audit logging
- Any blocking (including the reason) of access based on a UID, terminal, or access port
- Any configuration change. The record includes the source and destination network addresses and ports or protocol identifiers.
- Denial of access due to excessive login attempts
- Each log off
- Each successful or unsuccessful attempt to log on to the application
- Successfully or unsuccessfully loading and starting a Duet module
- Modification of permissions associated with roles
- Connection and loss of connection to an NTP server. (Loss of connection is defined as three successive failed polls. A single successful poll constitutes a re-connection.
- System reboot
- Software or firmware updates
- Creation, modification, and deletion of user accounts

**NOTE:** *The Master retains audit log records for 30 days (or less depending on available space), after which they are automatically purged.*

## Banners

Banners enable you to display pre- and post-login text in the WebConsole and terminal interfaces. Banner files are text files containing up to 500 characters in each file. (Any additional characters are discarded.)

**NOTE:** *Banner files are user-provided and optional. If no files are found, no banner appears.*

The following special characters are allowed for use in banner text messages:

! ” # $ % & ’ ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~

Also allowed are any printable ASCII characters (including "space"): A-Z, a-z, 0-9.

Pre-login banners must be named "banner.txt" and stored in the /user directory on the Master. Post-login banners are obtained from one or more files in the /user directory. Post-login banner text is a concatenation of the allroles_banner.txt file, followed by all of the applicable <role>_banner.txt files, where <role> is the name of a defined Role in the system. The applicable files are those that match the Roles assigned to the user that logged in. If a Role is currently locked, its banner file is not included.

**NOTE:** *If you load a new "banner.txt" file with new content to the Master, you must reboot the Master to display the new file.*

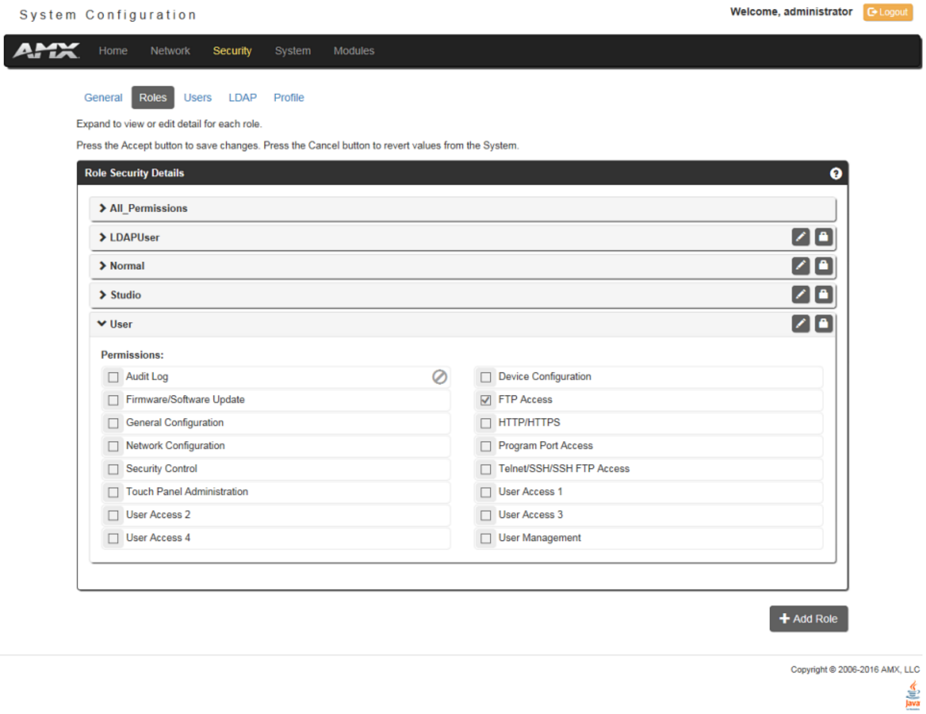
# Security - Roles

A Role is a set of privileges or permissions assigned to one or more users. The privileges and permissions can involve various functions or allow access to specific ports. Any privileges or permissions set for a role are inherited by all users sharing that role. Multiple roles can be assigned to a user, but at the same time, roles are not required for users. A user can have zero roles assigned to it.

**NOTE:** *You cannot assign a permission directly to a user. All user permissions are determined by the Role assigned to the user.*

**NOTE:** *If you have a remote directory such as LDAP enabled, the common name of the LDAP group on the LDAP server must match the name of the Role assigned to the user on the Master.*

Select the *Roles* option of the Security Page to access the **Role Security Details** page (FIG. 40).



Expand to view or edit detail for each role.

Press the Accept button to save changes. Press the Cancel button to revert values from the System.

**Role Security Details**

- All_Permissions
- LDAPUser
- Normal
- Studio
- User

Permissions:

| | |
|---|---|
| □ Audit Log | □ Device Configuration |
| □ Firmware/Software Update | ☑ FTP Access |
| □ General Configuration | □ HTTP/HTTPS |
| □ Network Configuration | □ Program Port Access |
| □ Security Control | □ Telnet/SSH/SSH FTP Access |
| □ Touch Panel Administration | □ User Access 1 |
| □ User Access 2 | □ User Access 3 |
| □ User Access 4 | □ User Management |

**FIG. 40** Security - Roles page

The options in this page allow authorized users to assign and alter role properties such as creating, modifying, or deleting a role's rights, locking a role, and defining the files/directories accessible by a particular role. Locking a role disables the role without deleting it.

## Default Roles

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

| Default User Accounts | |
|---|---|
| **All_Permissions** | **Studio** |
| *Permissions: All* | *Permissions:*<br>• Device Management<br>• Firmware/Software Update<br>• Network Management<br>• Security Control |

## Role Permissions

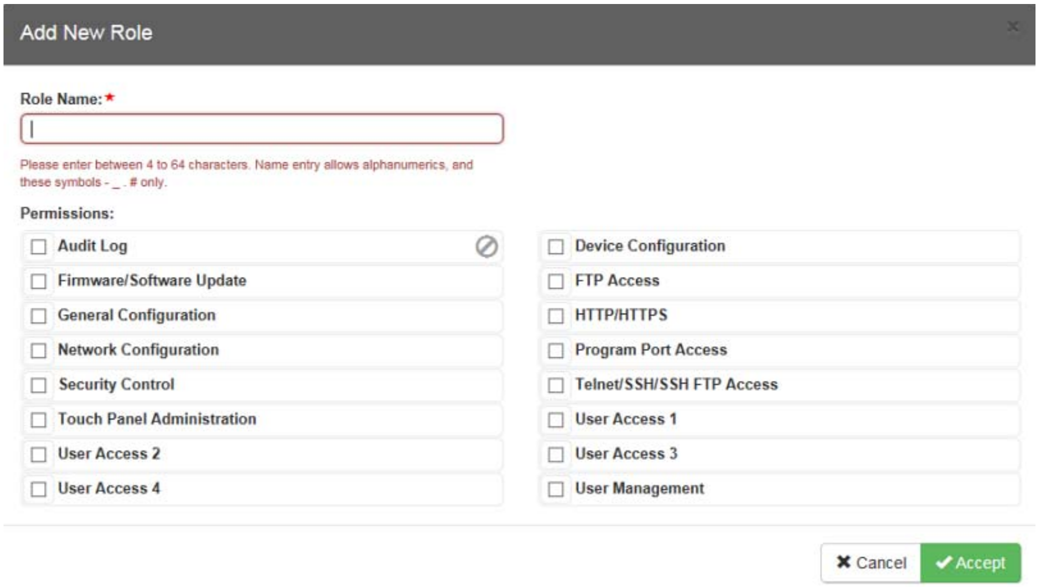
The following table lists the permissions available for Roles:

| Role Permissions | |
|---|---|
| **Option** | **Description** |
| Audit Log | Select to allow the role to view and configure the audit log. |
| Device Configuration | Select to allow the role to modify the configuration of NetLinx and 3rd party devices including the following:<br>• System number<br>• Device number<br>• Integrated device settings<br>• Switcher device settings (DVX or DGX)<br>• Reboot<br>**NOTE:** *This permission is not required to view the information, only to change it.* |
| Firmware/Software Update | Select to allow the role to update firmware and software. This setting allows Device access via ICSP with user credentials.<br>**NOTE:** *This permission also includes the right to reboot the Master after the update. It does not include the right to reboot the Master outside of this context or to reboot any other devices.* |
| FTP Access | Select to allow the role to have FTP access. |
| General Configuration | Select to allow the role to modify general configuration including access to WebControl for RMS and RPM configuration, importing and exporting configuration files, and the following parameters:<br>• Auto-locate enable/disable<br>• Device Holdoff setting<br>• Duet memory allocation<br>• ICSP TCP timeout<br>• Master-to-master route mode<br>• Message log length<br>• Message thresholds for threads<br>• Queue sizes for threads<br>• UDP broadcast rate<br>**NOTE:** *This permission also includes the right to reboot the Master after the configuration change. It does not include the right to reboot the Master outside of this context or to reboot any other devices.*<br>**NOTE:** *This permission is not required to view the information, only to change it.* |
| HTTP/HTTPS | Select to allow the role to have HTTP and HTTPS access through the web interface. |
| Network Configuration | Select to allow the role to modify network configuration including the following:<br>• Clock Manager settings<br>• DHCP/Static setting (Gateway IPv4 address, IPv4 address, IPv4 subnet mask (if static selected))<br>• DNS server addresses<br>• Domain name<br>• Hostname<br>• zeroconfig enable/disable<br>**NOTE:** *This permission also includes the right to reboot the Master after the configuration change. It does not include the right to reboot the Master outside of this context or to reboot any other devices.*<br>**NOTE:** *This permission is not required to view the information, only to change it.* |
| Program Port Access | Select to allow the role to have terminal access via the Program Port. |
| Security Control | Select to allow the role to view and configure security including the following:<br>• Audit log enable<br>• Authentication on server ports enable<br>• Authentication on ICSP LAN ports enable<br>• Authentication on ICSP ICSLAN ports enable<br>• Banner display enable<br>• Cryptographic options<br>• Lockout on failed logins enable<br>• FTP/SFTP enable<br>• HTTP/HTTPS enable<br>• Inactivity timeout enable<br>• ICSP options on ICSLAN<br>• ICSP options on LAN<br>• Password complexity<br>• Password expiration enable<br>• Telnet/SSH enable<br>• USB Host port disable<br>**NOTE:** *This permission also includes the right to reboot the Master after the configuration change. It does not include the right to reboot the Master outside of this context or to reboot any other devices.*<br>**NOTE:** *This permission is not required to view the information, only to change it.* |
| Telnet/SSH/SSH FTP Access | Select to allow the role to have Telnet, SSH, and SSH FTP access. |

| Role Permissions (Cont.) | |
|---|---|
| **Option** | **Description** |
| Touch Panel Administration | Select to allow the Master to access a touch panel's settings page. |
| User Access 1-4 | Select to allow the role access generic access permissions. These privileges are to be used by NetLinx programs. |
| User Management | Select to allow the role to view, create, modify, lock, and remove user accounts.<br>**NOTE:** *A user has the ability to change its own password, regardless of whether it has the User Management permission.* |

## Adding a New Role

1. Select the **Roles** option (*in the Security section*) to open the Role Security Details page.
2. Click the **Add Role** button (see FIG. 41) to access the **Add New Role** page (FIG. 41).



Add New Role

Role Name: *

Please enter between 4 to 64 characters. Name entry allows alphanumerics, and these symbols - _ . # only.

Permissions:

- □ Audit Log
- □ Firmware/Software Update
- □ General Configuration
- □ Network Configuration
- □ Security Control
- □ Touch Panel Administration
- □ User Access 2
- □ User Access 4
- □ Device Configuration
- □ FTP Access
- □ HTTP/HTTPS
- □ Program Port Access
- □ Telnet/SSH/SSH FTP Access
- □ User Access 1
- □ User Access 3
- □ User Management

**FIG. 41** Add New Role

3. In the **Role Name** field, enter a unique name for the new role.
   - The name must be a valid character string consisting of 4 - 20 alpha-numeric characters. See the *User and Role Name Rules* section on page 43 for a complete list of valid characters.
   - The string is case sensitive and must be unique.
   - The terms "*All_Permissions*" and "Studio" cannot be used for a new role name since the names already exist by default.

   **NOTE:** *If you have a remote directory such as LDAP enabled, the common name of the LDAP group on the LDAP server must match the name of the Role assigned to the user on the Master.*

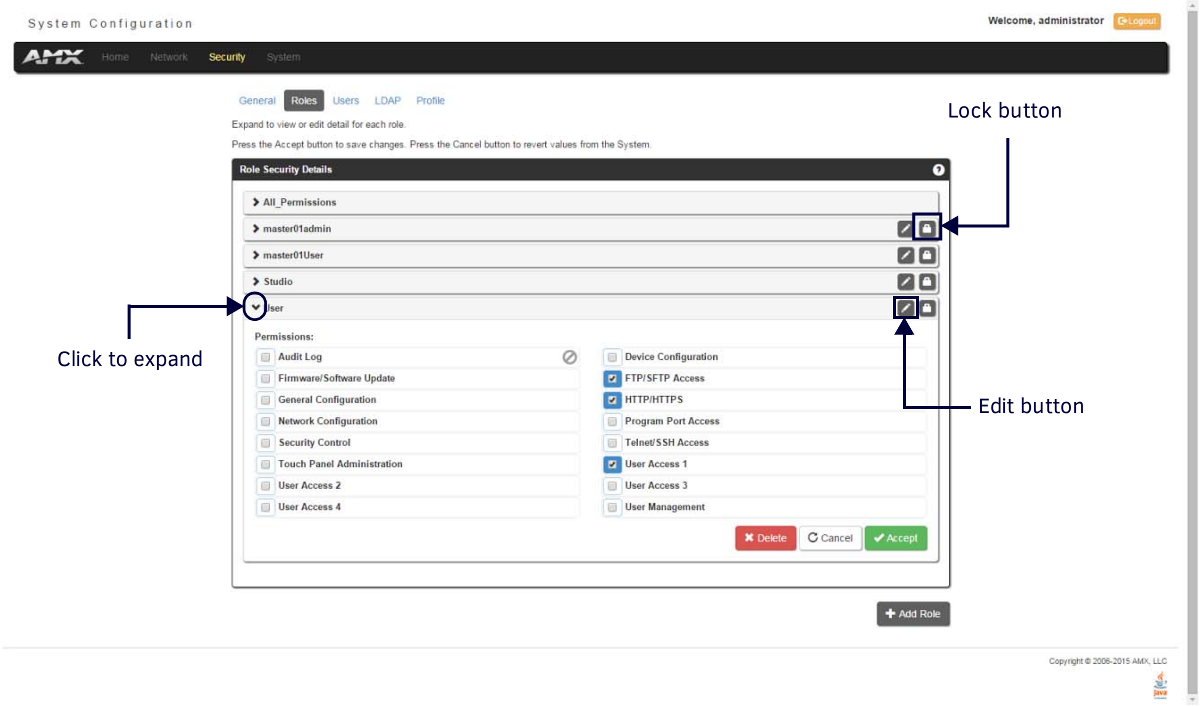
4. Enable the security access rights you want to provide to the role. By default, all of these options are disabled. See the *Role Permissions* section on page 49 for details.
5. Click the **Accept** button to save your changes to the target Master.

   If there are no errors within any of the page parameters, a "*Role added successfully*" message displays at the top of the page.

**NOTE:** *Security changes made from within the web browser are applied instantly without the need to reboot.*

## Viewing and Modifying Role Security Settings Details

Click any Role listed on the *Role Security Details* page to expand the view to show details for the selected user Role (FIG. 42):



Expand to view or edit detail for each role.

Press the Accept button to save changes. Press the Cancel button to revert values from the System.

Permissions:

| | |
|---|---|
| □ Audit Log | □ Device Configuration |
| □ Firmware/Software Update | ☑ FTP/SFTP Access |
| □ General Configuration | ☑ HTTP/HTTPS |
| □ Network Configuration | □ Program Port Access |
| □ Security Control | □ Telnet/SSH Access |
| □ Touch Panel Administration | ☑ User Access 1 |
| □ User Access 2 | □ User Access 3 |
| □ User Access 4 | □ User Management |

**FIG. 42** Role Security Details Page

1. Select the **Roles** option (in the *Security* section) to open the Role Security Details page.
2. Click any Role listed on the *Role Security Details* page to expand the view to show details for the selected user Role.
3. Modify the previously configured access rights by enabling/disabling the check boxes. See the *Role Permissions* section on page 49 for details.
4. Click **Accept** to save your changes to the Master.

   If there are no errors with the modification of any of this page's parameters, a "*Role updated successfully*" is displayed at the top of the page.

**NOTE:** *The "All_Permissions" user name cannot be modified or deleted.*

Any properties possessed by roles (ex: access rights, update rights, directory associations, etc.) are inherited by users assigned to that particular role.

Unchecking a security option (which is available within the associated role) does not remove that right from the user. The only way to remove a role's available security right from a target user is either to not associate a role to a user or to alter the security rights of the role being associated.

## Deleting a Role

1. Select the **Roles** option (in the *Security* section) to open the *Role Security Details* page.
2. Click the **Edit** button (see FIG. 42) for any Role listed on the *Role Security Details* page to expand the view to show details for the selected Role.
3. Click **Delete** to remove the selected role and refresh the page. The system will prompt you to verify this action - click **OK** to proceed.

   If the role is associated with several users, you might get an error while trying to delete the role. If this happens, change the role association of those specific users utilizing the old role and either give them a new role or assign them (none) as a role. When you return to delete the desired role, you receive a message saying "*Role deleted successfully*".
4. Click the **Accept** button to save your changes to the Master.

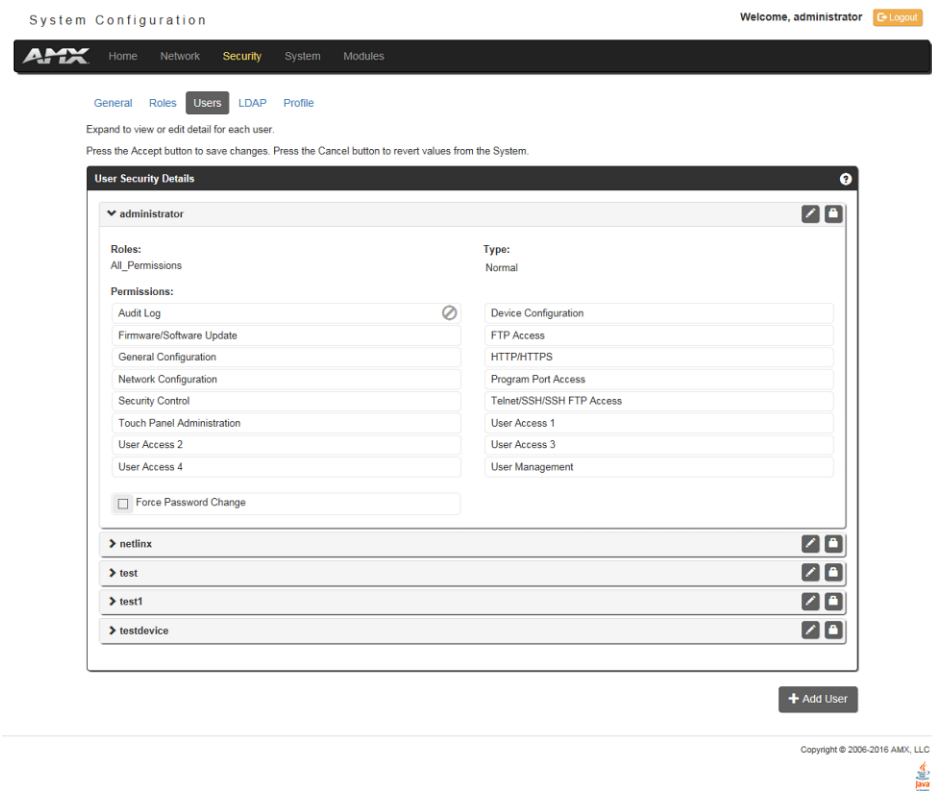
## Locking/Disabling a Role

1. Select the **Roles** option (in the *Security* section) to open the *Role Security Details* page.
2. Click the **Lock** button (see FIG. 42) for any Role listed on the *Role Security Details* page to lock and disable the Role. Click the Lock button again to unlock and enable the Role

**NOTE:** *Any Role can be disabled except for the All_Permissions role.*

# Security - Users

Select the *Users* option on the Security Page to access the **User Security Details** page (FIG. 43). The options on this page allow authorized users to add/delete/lock User accounts and configure User’s access rights. Locking a user account disables the account without deleting it.



Expand to view or edit detail for each user.

Press the Accept button to save changes. Press the Cancel button to revert values from the System.

User Security Details

administrator

Roles:
All_Permissions

Type:
Normal

Permissions:

| | |
|---|---|
| Audit Log | Device Configuration |
| Firmware/Software Update | FTP Access |
| General Configuration | HTTP/HTTPS |
| Network Configuration | Program Port Access |
| Security Control | Telnet/SSH/SSH FTP Access |
| Touch Panel Administration | User Access 1 |
| User Access 2 | User Access 3 |
| User Access 4 | User Management |

□ Force Password Change

netlinx

test

test1

testdevice

**FIG. 43** Security - Users page

A **User** represents a single client of the Master, while a **Role** specifies a set of privileges and permissions which can be assigned to a user. An administrator can assign up to 5 roles to a single user. Any properties possessed by a role are inherited by all of the users assigned to the role.

## Default User Accounts

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

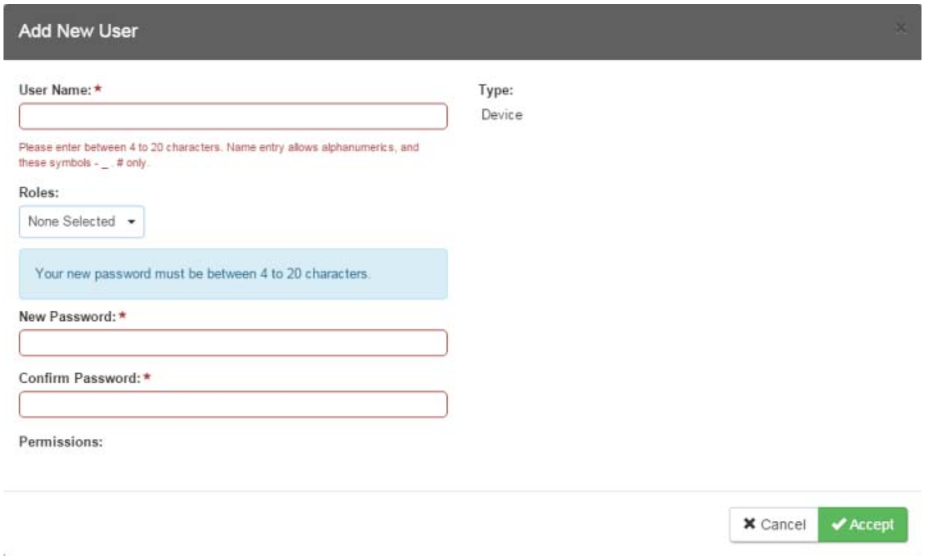
| Default User Accounts | |
|---|---|
| **administrator** | **netlinx** |
| *Username*: administrator | *Username*: netlinx |
| *Password*: password | *Password*: password |
| *Role*: All_Permissions | *Role*: Studio |
| *Directory Association*: /* | *Directory Association*: none |
| **NOTE:** *You can delete and/or modify the "administrator" user account to optimize system security. If deleted, you can create a new user with the "administrator" user name with its own proper settings, provided LDAP is not enabled.* | **NOTE:** *The "netlinx" user account is compatible with previous NetLinx Master firmware versions. This account is initially created by default and can later be deleted or modified.* |

- FTP Security is always enabled on the Masters.
- All other security options are **disabled** by default.

## Adding a New User

**TIP:** *For a quicker configuration, it is recommended to define all roles and permissions before defining users.*

1. Select the **Users** option (in the *Security* section) to view the User Security Details page.
2. Click the **Add User** button (see FIG. 43) to access the **Add New User** page (FIG. 44).



Add New User

User Name: *

Please enter between 4 to 20 characters. Name entry allows alphanumerics, and these symbols - _ . # only.

Type:

Device

Roles:

None Selected

Your new password must be between 4 to 20 characters.

New Password: *

Confirm Password: *

Permissions:

**FIG. 44** Add New User

3. In the **User Name** field, enter a unique name for the new role.
   - The name must be a unique alpha-numeric character string (4 - 20 characters), and is case sensitive.
   - The words "*administrator" and "NetLinx"* cannot be used since they already exist by default.

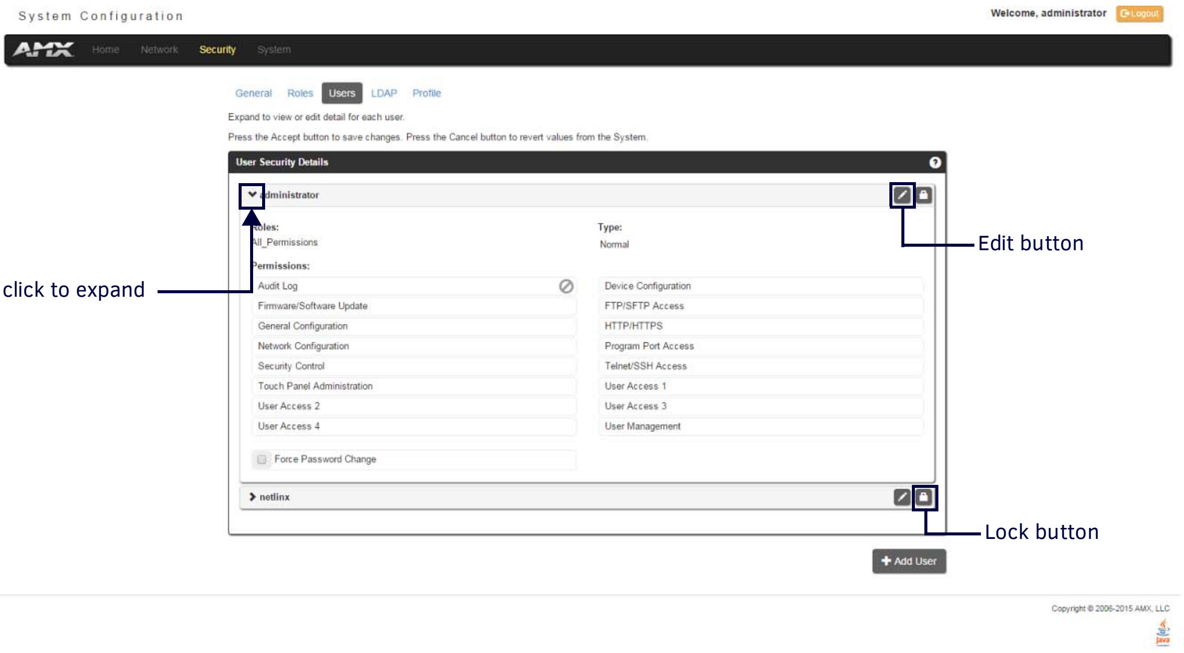
**NOTE:** *The Type field indicates the type of account for the user. This field lists either Normal or Device. Normal users are any users which access the web interface, Telnet, or NetLinx Studio, and must be assigned to a Role with those permissions assigned to it. Device connections are required for machine to machine over ICSP, such as touch panels and ICSLan device control boxes. Device-type users are stored only in the local user database and are able to be modified even when a remote directory service is enabled.*

4. From the **Roles** options menu, choose from a list of roles and associate the rights of the role to the new user. You can assign up to 5 roles to a user.
5. Enter a user password in both the **Password** and **Password Confirm** fields. The password must conform to the rules set by the Password Complexity level set on the User account. See the *Password Rules* section on page 43 for more information.
6. Select **Force Password Change** if you want the user to change its password on its next login. This option is not available for Device users.
7. Click the **Accept** button to save your changes to the Master.

**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, unless otherwise notified.*

## Viewing and Editing User Security Settings

Click any User listed in the *User Security Details* page to view the security settings for the selected User (FIG. 45):



Expand to view or edit detail for each user.

Press the Accept button to save changes. Press the Cancel button to revert values from the System.

User Security Details

administrator

Roles: All_Permissions

Type: Normal

Permissions:

| | |
|---|---|
| Audit Log | Device Configuration |
| Firmware/Software Update | FTP/SFTP Access |
| General Configuration | HTTP/HTTPS |
| Network Configuration | Program Port Access |
| Security Control | Telnet/SSH Access |
| Touch Panel Administration | User Access 1 |
| User Access 2 | User Access 3 |
| User Access 4 | User Management |

□ Force Password Change

netlinx

Copyright © 2006-2015 AMX, LLC

**FIG. 45** Security - Users page

1. Click the Edit button for the User you want to edit to expand the User's details.
2. Make any necessary changes to the selected User, and click **Accept** for the changes to take effect.

## Deleting a User

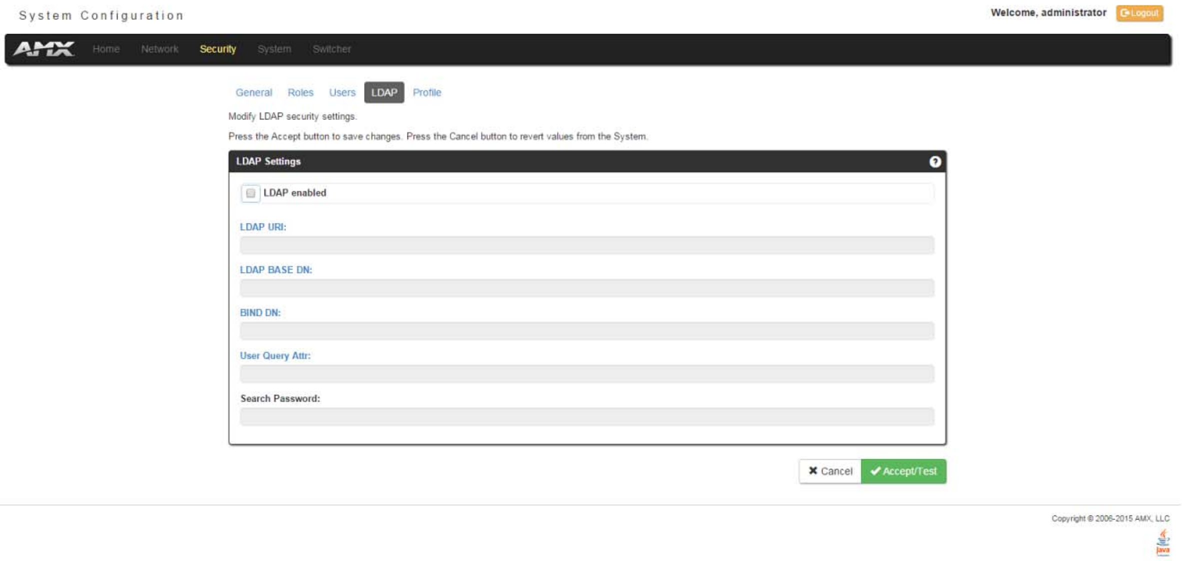
1. Select the **Users** options (in the *Security* section) to open the User Security Details page.
2. Click the Edit button for the User you want to delete to expand the User's details.
3. Press the **Delete** button to remove the selected User and refresh the page. The system will prompt you to verify this action - click **OK** to proceed.
4. Reboot the Master via the **Reboot** button on the Manage System Page (select the **System** control button to access).

## Locking/Disabling a User

1. Select the **Users** option (in the *Security* section) to open the *User Security Details* page.
2. Click the **Lock** button (see FIG. 43) for any user listed on the *User Security Details* page to lock and disable the user. Click the Lock button again to unlock and enable the user.

# Security Settings - LDAP

The LDAP page provides configuration and tests connection to a remote directory service via LDAPv3. The master supports the option of an insecure or secure connection. The secure option is supported via the StartTLS command in LDAP and also via "LDAPS", or LDAP over SSL/TLS on port 636. Select the *LDAP* option on the Security Page to access the **LDAP Settings** page (FIG. 43). The options on this page allow authorized users to enable and modify LDAP security settings.



Modify LDAP security settings.

Press the Accept button to save changes. Press the Cancel button to revert values from the System.

**FIG. 46** Security - LDAP page

## LDAP Options

All parameters are case sensitive and must be entered exactly as they are entered into the LDAP database. You can also perform LDAP Client Configuration via terminal commands to the NetLinx Master's Program Port - see the *Enabling LDAP via the Program Port* section on page 125 for details.

See *Appendix A: LDAP Implementation Details* on page 127 for additional information on implementing LDAP on the NetLinx Master.

The LDAP options are described in the following table:

| **LDAP Options** | |
|---|---|
| **Option** | **Description** |
| LDAP Enabled: | This parameter enables the LDAP configuration parameters described below.<br>**NOTE:** *When LDAP is enabled, you can only create device users. If the administrator user has been deleted, you must perform a factory reset of the Master via pushbutton to restore the administrator user.* |
| LDAP URI | This parameter has the syntax **ldap[s]://hostname:port**.<br>• The **ldap:// URL** is used to connect to LDAP servers over unsecured connections.<br>• The **ldaps:// URL** is used to connect to LDAP server over Secure Sockets Layer (SSL) connections.<br>• The **hostname** parameter is the name or IP address, in dotted format, of the LDAP server (for example, *LDAPServer01* or *192.202.185.90*).<br>• The **port** parameter is the port number of the LDAP server (for example, *696*).<br>**NOTE:** *The standard unsecured port number is 389 and the standard secured port number is 636.* |
| LDAP BASE DN | This parameter specifies the Distinguished Name (DN) of an entry in the directory. It identifies the entry that is the starting point of the user search. |
| BIND DN | This parameter specifies the Distinguished Name (DN) to use to bind to the LDAP server for the initial search for the user's DN. |
| User Query Attr | This LDAP attribute is used for the AMX equipment user search (for example, UID).<br>**NOTE:** *This attribute MUST be unique in the context of the LDAP BASEDN or the search will fail.* |
| Search Password | This is the password used for the initial bind to the LDAP server - it is the password associated with BIND DN. |

Click the **LDAP enabled** check box to make the LDAP options available for selection.

- When LDAP is enabled, users are authenticated using the configuration set up on the LDAP server.
- The "*administrator*" user is handled by the local NetLinx Master, and does not connect to the LDAP server for user verification.

- If an administrator password change is desired, LDAP must be disabled, the password changed and saved and then LDAP re-enabled.
- Users may not be added or deleted via the web pages when LDAP is enabled.
- User access privileges cannot be changed via the web pages.
- As users log onto a NetLinx Master, their user name and access privileges are displayed on the User Security Details page (see *Security - Users* section on page 52). This information is stored in the master's RAM but is not written to non-volatile memory, and is lost after rebooting the Master.
- If a user is removed from the LDAP directory tree, access is denied, and if that user name is on the master's User Security Details web page it is removed.

## Accepting Changes

Click the **Accept/Test** button to save changes on this page. Accepting changes is instantaneous and does not require rebooting the Master.

## Testing the Connection to the LDAP Server

After entering and accepting the parameters, the **Accept/Test** button can be used to test the connection to the LDAP server. This test does a bind to the BIND DN using the Search Password entered.

- If the bind is successful, the message *Connection successful* is displayed.
- If the server could not be reached or the bind is unsuccessful, the message *Could not connect to server -- Please check LDAP URI, BIND DN and Search Password settings* is displayed.

Refer to *Appendix A: LDAP Implementation Details* on page 127 for additional information.

**IMPORTANT:** *For the NX-series Masters to work with LDAP over SSL (LDAPS), you must upload a CA server certificate in .pem format to the Master's FTP server. The certificate's file name must be "ldap_ad.pem" and the file must be saved in a folder named "certs". Once the file is uploaded, you must reboot the Master for the certificate file to be read and employed by the system. LDAPS requires Master Firmware version 1.3.78 or greater.*

## Wired 802.1X support

IEEE 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). PNAC provides the ability to grant or deny network access to devices wishing to attach to a LAN based on credentials tied to the device rather than to a user. Until the device has been verified and permitted access, no network traffic is passed through the connected port, effectively keeping the device disconnected from the network.

The NX-Series controller acts as a supplicant (client device) to a wired 802.1X enabled network and presents customer-provided X.509 certificates to be allowed access to protected networks. The following EAP Encryption Methods are supported.

- PEAPv0/MSCHAPv2
- TTLS/MSCHAPv2
- TTLS/PAP
- MD5

Customer provided X.509 certificates are uploaded to the NX-Series controller using NetLinx Studio, and 802.1x is configured via the Command Line Interface and the syntax:

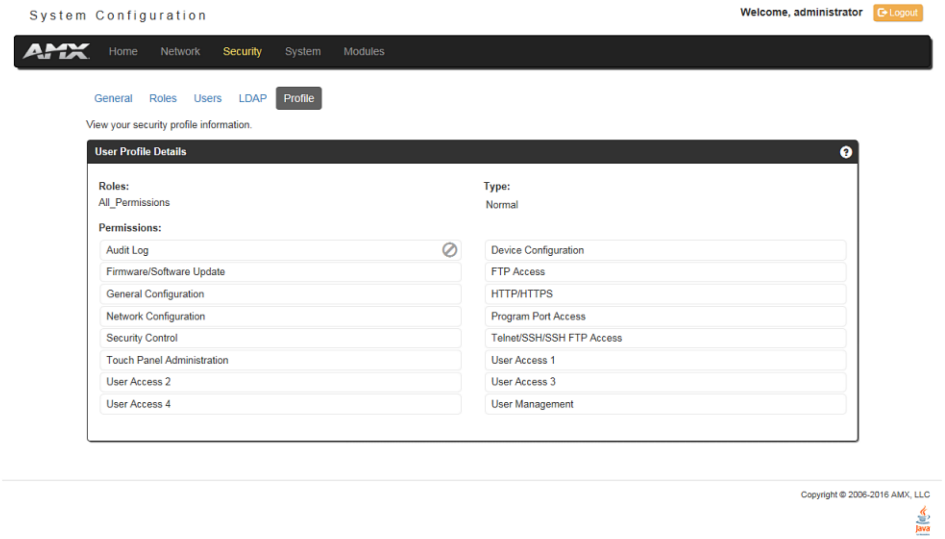
```
DOT1X[status|enable|disable]
```

Once you add the certificate file to your workspace, NetLinx Studio transfers the file to the appropriate directory on the controller.

1. Click to select (highlight) a System (in the Workspace tab of the Workspace Bar).
2. Right-click on the **Other** folder to access the Other File Folder context menu, and select **Add Existing Other File**.
3. In the Add Existing Other File dialog, locate and select the certificate file (.crt) that you want to add to the selected System. Change the Files of Type option to All Files (*.*) to look for other file types, if necessary.
4. Click **Open** to access the File Properties dialog, where you can view/edit general file information for the selected file.
5. Click **OK** to add the file to the selected System. The file should now appear in the Other folder under the selected System.

# Security - Profile

The Profile page (FIG. 47) enables a user to see its own roles and permissions. The user cannot change the roles and permissions on this page.



View your security profile information.

**User Profile Details**

**Roles:**
All_Permissions

**Type:**
Normal

**Permissions:**

Audit Log
Firmware/Software Update
General Configuration
Network Configuration
Security Control
Touch Panel Administration
User Access 2
User Access 4

Device Configuration
FTP Access
HTTP/HTTPS
Program Port Access
Telnet/SSH/SSH FTP Access
User Access 1
User Access 3
User Management

Copyright © 2006-2016 AMX, LLC

**FIG. 47** Security - Profile page

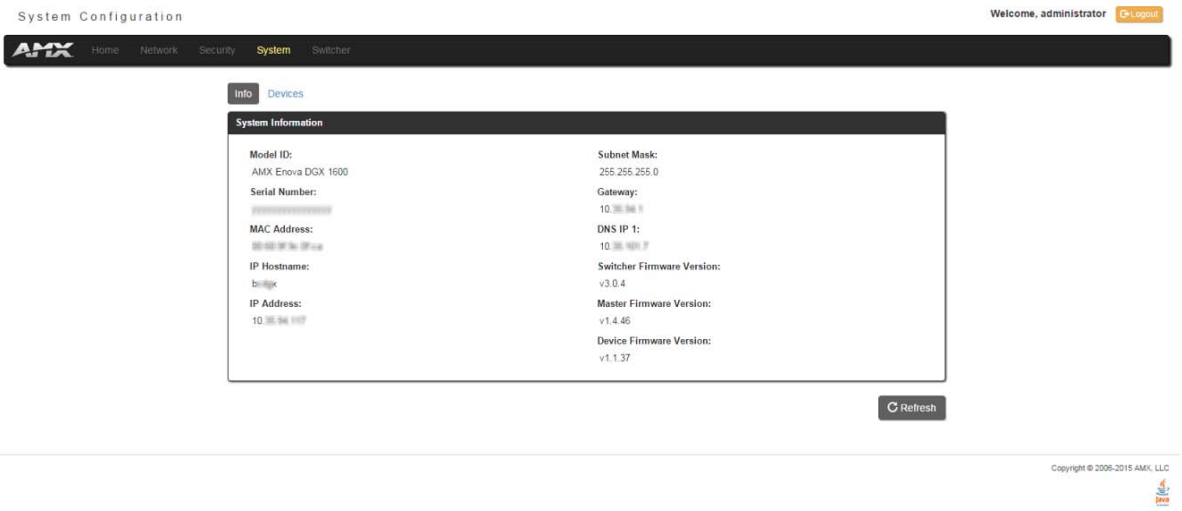
# WebConsole - System Options

## System Overview

The *System* page is accessed by clicking **System** on the page's main heading. This page allows you to view and configure various aspects of the NetLinx System:

- **System Information** - Options on this page allow you to view a detailed list of the properties of the Master. See the *System - Info* section on page 58 for details.
- **Devices** - Options in this tab allow you to view the details of additional attached devices (including module-supported third-party devices). See the *System - Devices* section on page 59 for details.

The default view for the System option is Manage System / System Number (FIG. 48).



System Information

Model ID:
AMX Enova DGX 1600

Serial Number:
[redacted]

MAC Address:
[redacted]

IP Hostname:
b[redacted]x

IP Address:
10.[redacted]

Subnet Mask:
255.255.255.0

Gateway:
10.[redacted]

DNS IP 1:
10.[redacted]

Switcher Firmware Version:
v3.0.4

Master Firmware Version:
v1.4.46

Device Firmware Version:
v1.1.37

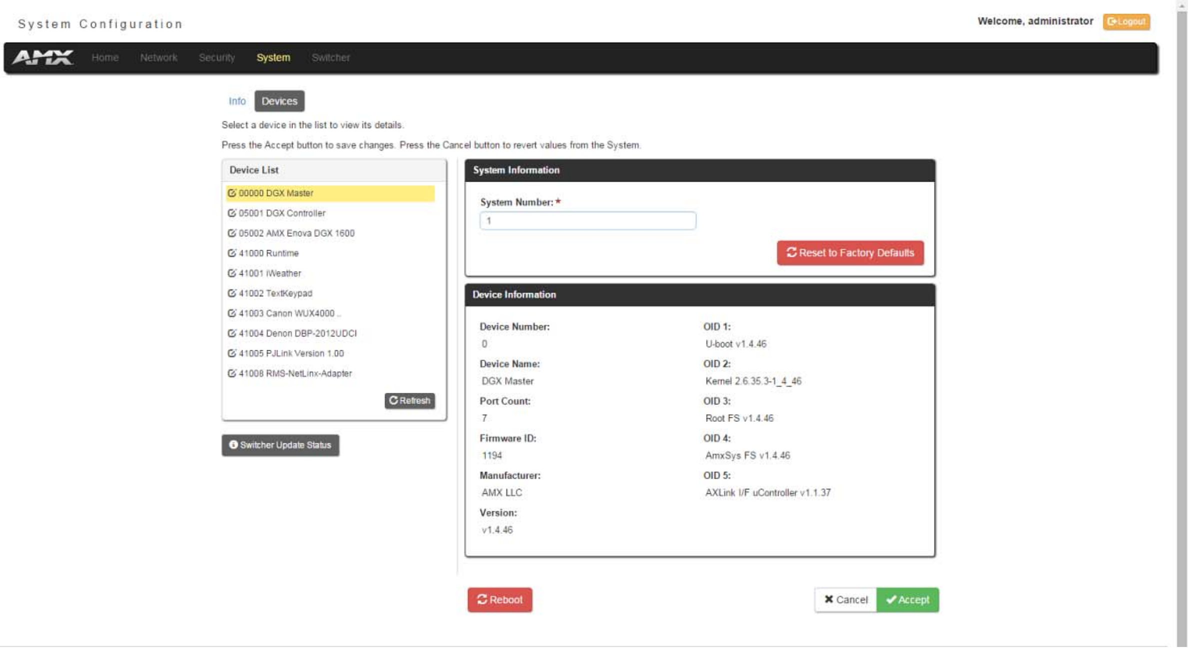
**FIG. 48** System - Info page

## System - Info

The **Info** page (FIG. 48) enables you to view a detailed list of the properties of the Master. The properties include the Model ID and serial number of the Master, network addresses, and firmware versions. This information is view-only. See the *WebConsole - Network Options* section on page 37 for information on changing the network address of the Master.

# System - Devices

The **Devices** page (FIG. 49) contains information about the Master and any connected devices. Select a device from the Device List and its information appears in the Device Information area. The information in this area is view-only, unless the device allows a change to its device number. If so, you can change the device number on this page (see *Changing the Device Number on a Device* below for more information.) Masters also include a system number which a user can change with proper access (see *Changing the System Number on the Master* below for more information.)



Select a device in the list to view its details.

Press the Accept button to save changes. Press the Cancel button to revert values from the System.

Device List

- 00000 DGX Master
- 05001 DGX Controller
- 05002 AMX Enova DGX 1600
- 41000 Runtime
- 41001 iWeather
- 41002 TextKeypad
- 41003 Canon WUX4000 ..
- 41004 Denon DBP-2012UDCI
- 41005 PJLink Version 1.00
- 41008 RMS-NetLinx-Adapter

System Information

System Number: * 1

Device Information

| | |
|---|---|
| Device Number:<br>0 | OID 1:<br>U-boot v1.4.46 |
| Device Name:<br>DGX Master | OID 2:<br>Kernel 2.6.35.3-1_4_46 |
| Port Count:<br>7 | OID 3:<br>Root FS v1.4.46 |
| Firmware ID:<br>1194 | OID 4:<br>AmxSys FS v1.4.46 |
| Manufacturer:<br>AMX LLC | OID 5:<br>AXLink I/F uController v1.1.37 |
| Version:<br>v1.4.46 | |

**FIG. 49** System - Devices page

## Changing the System Number on the Master

1. Select the Master from the Device List.
2. Enter the new numeric value into the **New System Number** field.
3. Click the **Accept** button to save this new value to the system on the target Master. The message "*System number changed to X. Master must be rebooted for the change to take effect.*" reminds you that the Master must be rebooted before the new settings take effect.
4. Click **Reboot** to reboot the target Master. The Device Tree then reads "*Rebooting...*". After a few seconds, the Device Tree refreshes with the current system information (including the updated system number assignment.) If the Device Tree does not refresh within a few minutes, press the **Refresh** button and reconnect to the Master.

## Changing the Device Number on a Device

Note that in most cases, the Device Number for Masters should remain set to zero.

1. Select the device from the Device List. Ensure the device has a device number.
2. Enter the new numeric value into the **Device Number** field.
3. Click the **Accept** button to save this new value to the system on the target device.

## Resetting the Master Controller to the Factory Defaults Configuration

Click the **Reset to Factory Defaults** button. This resets the Master to its' factory default state. This includes the following:

- Removal of all security settings
- Removal of all user files; creation of *administrator* and *netlinx* user accounts.
- Removal of all roles; creation of *All_Permissions* and *Studio* roles.
- Resetting to DHCP
- Loading an empty NetLinx program.

Once reset, the Master will be effectively in an out-of-box state.

**NOTE:** *It may be necessary to refresh the browser window after the master has finished booting (click Refresh).*

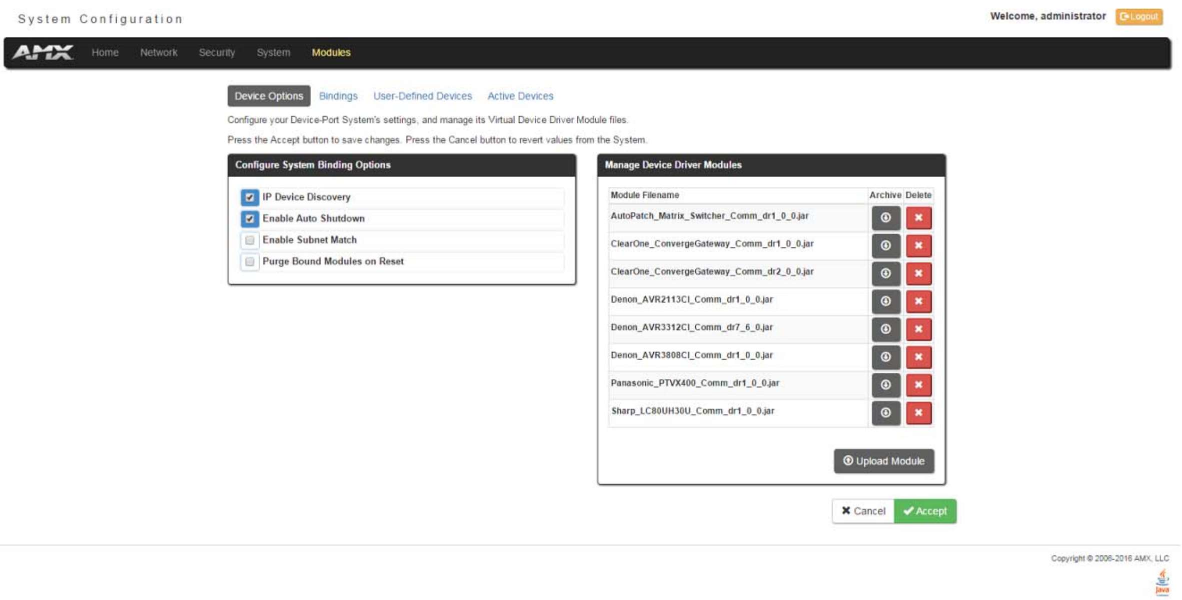
# WebConsole - Modules Options

## Modules Overview

The *Modules* page is accessed by clicking **Modules** on the page's main heading. This page allows you to view and configure various aspects of the NetLinx System:

- **Device Options** - Options on this page display various details specific to additional (non-NetLinx) System Devices. See the *Modules - Device Options* section on page 61 for details.
- **Bindings** - Options on this page allow you to view the details of additional attached devices (including module-supported third-party devices). See the *Modules - Bindings* section on page 62 for details.
- **User-Defined Devices** - Options on this page provide a listing with all of the dynamic devices that have been discovered in the system, and allow you to add and delete User-Defined Devices. See the *Modules - User-Defined Devices* section on page 65 for details.
- **Active Devices** - Options on this page allow you to check devices for compatible Duet Modules. See the *Modules - Active Devices* section on page 66.

The default view for the Modules option is Device Options (FIG. 50).



Configure your Device-Port System's settings, and manage its Virtual Device Driver Module files.

Press the Accept button to save changes. Press the Cancel button to revert values from the System.

**Configure System Binding Options**

☑ IP Device Discovery
☑ Enable Auto Shutdown
□ Enable Subnet Match
□ Purge Bound Modules on Reset

**Manage Device Driver Modules**

| Module Filename | Archive | Delete |
|---|---|---|
| AutoPatch_Matrix_Switcher_Comm_dr1_0_0.jar | | ✖ |
| ClearOne_ConvergeGateway_Comm_dr1_0_0.jar | | ✖ |
| ClearOne_ConvergeGateway_Comm_dr2_0_0.jar | | ✖ |
| Denon_AVR2113CI_Comm_dr1_0_0.jar | | ✖ |
| Denon_AVR3312CI_Comm_dr7_6_0.jar | | ✖ |
| Denon_AVR3808CI_Comm_dr1_0_0.jar | | ✖ |
| Panasonic_PTVX400_Comm_dr1_0_0.jar | | ✖ |
| Sharp_LC80UH30U_Comm_dr1_0_0.jar | | ✖ |

**FIG. 50** Modules - Device Options page

# Modules - Device Options

Click the **Device Options** link (in the *Manage Devices* tab) to access the **Details for Additional Devices** page (FIG. 50). The options on this page display various details specific to additional (non-NetLinx) System Devices.

## Configuring Device Binding Options

1. Use the **Configure System Binding Options** to specify how the Master will manage Bound Devices:

**Configure System Binding Options**

| Option | Description |
|---|---|
| IP Device Discovery | This option enables you to specify whether you want the Master to scan your network and locate any devices connected to it. |
| Enable Auto Shutdown | Auto-Shutdown forces the termination of modules that have lost communication with their respective physical device. This capability is needed for plug-and-play support.<br>By default, Auto-Shutdown is enabled. If automatic termination of modules when they have lost communication is not desired, this selection should be disabled. |
| Enable Subnet Match | This selection allows you to specify 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.<br>During the binding process, the associated Duet modules for a device are copied from the **/unbound** directory into a protected **/bound** area.<br>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.<br>This selection is a one-time occurrence. Upon the next reboot, the selection is cleared. |

2. Press the **Accept** button to save your changes.

## Managing Device Driver Modules

Use the **Manage Device Driver Modules** set of options to upload, archive, or delete modules from the Master. All modules currently present on the Master are indicated in the Module list.

### Uploading a Module

Perform the following steps to browse for a Module file and then upload it to the Master:

1. Click **Upload Module** to browse for Duet Modules on your PC/Network.
2. Select the JAR file that you want to upload to the Master.
3. Click the **Open** button to upload a copy of the selected JAR file to the target Master's **/unbound** directory. Only JAR file types are allowed for Upload to the target Master.

### Archiving a Module

Click the **Archive** button next to the module you want to archive. This action copies the selected module (*.JAR) file to your PC. Your PC may require you to confirm this action depending on its security settings.

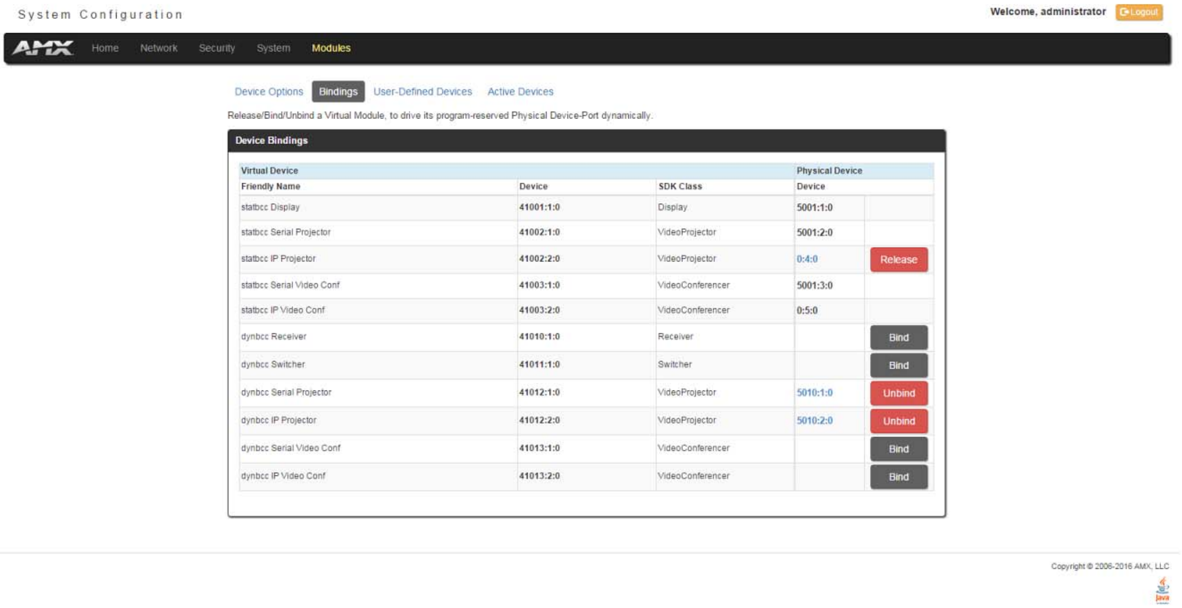
### Deleting a Module

Select a module and click the **Delete Module** button. This action deletes the selected module from the **/unbound** directory.

**NOTE:** *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 in the Configure System Binding Options section.*

## Modules - Bindings

Click **Bindings** to access the **Device Bindings** page (FIG. 51). Use the options on this page to configure application-defined Duet virtual devices with discovered physical devices.



Release/Bind/Unbind a Virtual Module, to drive its program-reserved Physical Device-Port dynamically.

Device Bindings

| Virtual Device | | | Physical Device | |
|---|---|---|---|---|
| Friendly Name | Device | SDK Class | Device | |
| statbcc Display | 41001:1:0 | Display | 5001:1:0 | |
| statbcc Serial Projector | 41002:1:0 | VideoProjector | 5001:2:0 | |
| statbcc IP Projector | 41002:2:0 | VideoProjector | 0:4:0 | Release |
| statbcc Serial Video Conf | 41003:1:0 | VideoConferencer | 5001:3:0 | |
| statbcc IP Video Conf | 41003:2:0 | VideoConferencer | 0:5:0 | |
| dynbcc Receiver | 41010:1:0 | Receiver | | Bind |
| dynbcc Switcher | 41011:1:0 | Switcher | | Bind |
| dynbcc Serial Projector | 41012:1:0 | VideoProjector | 5010:1:0 | Unbind |
| dynbcc IP Projector | 41012:2:0 | VideoProjector | 5010:2:0 | Unbind |
| dynbcc Serial Video Conf | 41013:1:0 | VideoConferencer | | Bind |
| dynbcc IP Video Conf | 41013:2:0 | VideoConferencer | | Bind |

Copyright © 2006-2016 AMX, LLC

**FIG. 51** Modules - Bindings

The table on this page displays a list of all application-defined devices, including each device’s "Friendly Name", the Duet virtual device’s D:P:S assignment, the associated Duet Device SDK class (indicating the type of the device), and the physical device’s D:P:S assignment. This information has to be pre-coded into the NetLinx file currently on the Master.

## Configuring Application-Defined Devices

Elements such as DUET_DEV_TYPE_DISPLAY and DUET_DEV_POLLED are defined within the NetLinx.axi file.

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_DISPLAY).

**NOTE:** *Physical device names are typically prefixed with "dv" and Virtual device names are typically prefixed with "vdv".*

Example Code:

```
PROGRAM_NAME='DDD'
DEFINE_DEVICE
COM1 = 5001:1:0
COM2 = 5001:2:0
dvDisplay = 41001:1:0
dvVideoProjector = 41002:1:0

DEFINE_CONSTANT
DEFINE_TYPE
DEFINE_VARIABLE
DEFINE_START


STATIC_PORT_BINDING(dvDisplay, COM1, DUET_DEV_TYPE_DISPLAY,
    'statbcc Display', DUET_DEV_POLLED)


DYNAMIC_POLLED_PORT(COM2)

DYNAMIC_APPLICATION_DEVICE(dvVideoProjector, DUET_DEV_TYPE_VIDEO_PROJECTOR,
   'statbcc Serial Projector')

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

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

You can find this example code within the DEFINE_START section of your code. This code is reflected in the first two entries listed in FIG. 51. The code gives the Master a “heads-up” notification to look for those devices meeting the criteria outlined within the code.

## Application Devices and 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 displayed in a mouse-over popup dialog when the cursor hovers over the physical device ID (see FIG. 52).

Each entry in the table has one of four buttons to the right of the Physical Device D:P:S assignment:

- **Static Bound** application devices will either be **blank,** or display a **Release** button:
  - Static Bound application devices that have not yet detected a physical device attached to their associated port have a **blank** button.
  - Once a physical device is detected and its associated Duet module has been started, a **Release** button appears. Click **Release** to force the associated Duet module to be destroyed. 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 you select **Unbind**, any associated Duet module is destroyed and the "link" between the application device and the physical device is 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.

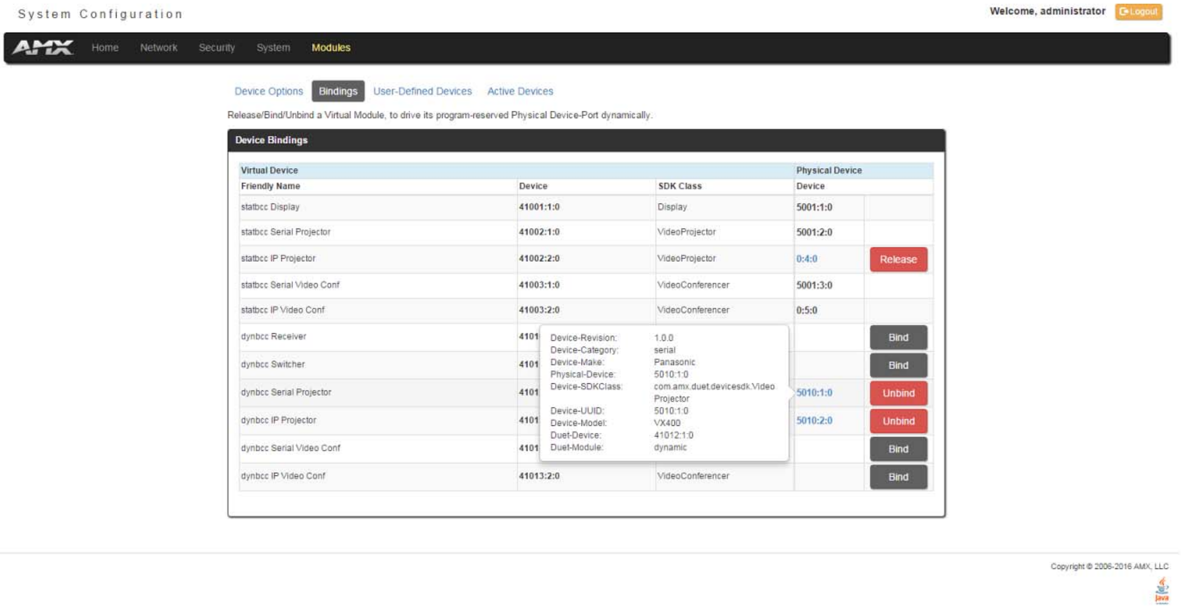
**NOTE:** *If a currently bound device needs to be replaced or a Duet Module needs to be swapped out, the device should be unbound and the new module/driver should then be bound.*

The administrator/user can select one of the available physical devices to bind with the associated application device. When you click **Accept**, the binding is created and the target Master attempts to locate the appropriate Duet Module driver. Once the Master locates a driver, the Duet Module started and becomes associated with the specified application device (Duet virtual device). If the you click **Cancel** button, the binding activity aborts.

**NOTE:** *If the manufacturer device does not support Dynamic Device Discovery (DDD) beaconing, you must use the Add Device page to both create and manage those values necessary to add a dynamic physical device. This process is described in detail in the Modules - User-Defined Devices* section on page 65.

## Viewing Physical Device Properties

Hold the mouse cursor over the Physical Device entry in the table to display detailed device properties for that device in a pop-up window (FIG. 52). You can only view the device properties for bound devices.



Release/Bind/Unbind a Virtual Module, to drive its program-reserved Physical Device-Port dynamically.

**Device Bindings**

| Virtual Device | | | Physical Device | |
|---|---|---|---|---|
| **Friendly Name** | **Device** | **SDK Class** | **Device** | |
| statbcc Display | 41001:1:0 | Display | 5001:1:0 | |
| statbcc Serial Projector | 41002:1:0 | VideoProjector | 5001:2:0 | |
| statbcc IP Projector | 41002:2:0 | VideoProjector | 0:4:0 | Release |
| statbcc Serial Video Conf | 41003:1:0 | VideoConferencer | 5001:3:0 | |
| statbcc IP Video Conf | 41003:2:0 | VideoConferencer | 0:5:0 | |
| dynbcc Receiver | 4101 | | | Bind |
| dynbcc Switcher | 4101 | | | Bind |
| dynbcc Serial Projector | 4101 | | 5010:1:0 | Unbind |
| dynbcc IP Projector | 4101 | | 5010:2:0 | Unbind |
| dynbcc Serial Video Conf | 4101 | | | Bind |
| dynbcc IP Video Conf | 41013:2:0 | VideoConferencer | | Bind |

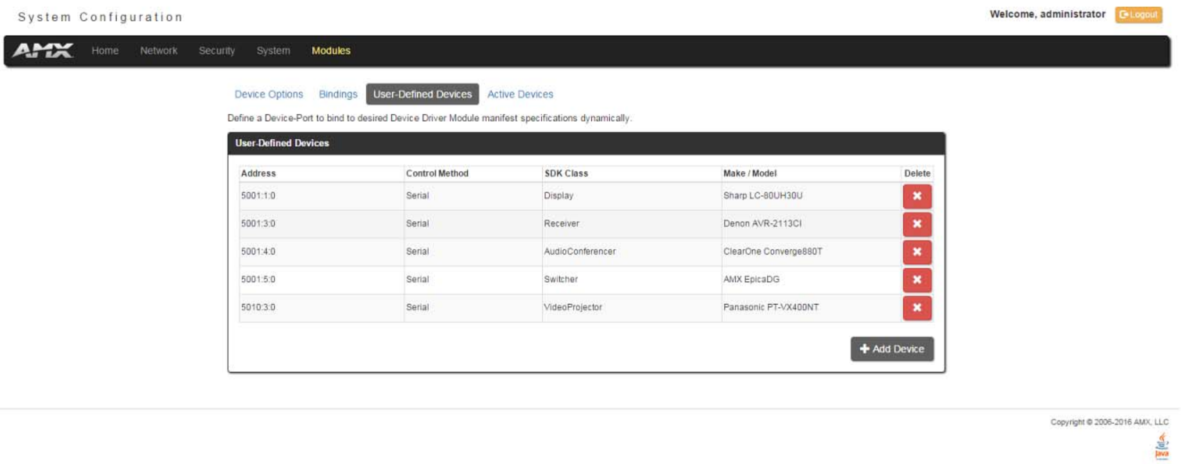
| | |
|---|---|
| Device-Revision: | 1.0.0 |
| Device-Category: | serial |
| Device-Make: | Panasonic |
| Physical-Device: | 5010:1:0 |
| Device-SDKClass: | com.amx.duet.devicesdk.Video Projector |
| Device-UUID: | 5010:1:0 |
| Device-Model: | VX400 |
| Duet-Device: | 41012:1:0 |
| Duet-Module: | dynamic |

Copyright © 2006-2016 AMX, LLC

**FIG. 52** Device Bindings - Device Properties pop-up

# Modules - User-Defined Devices

Click the **User-Defined Devices** link (in the *Manage Devices* tab) to access the **User-Defined Devices** page (FIG. 53). This page provides a listing with all of the dynamic devices that have been discovered in the system, and allows you to add and delete User-Defined Devices.



Define a Device-Port to bind to desired Device Driver Module manifest specifications dynamically.

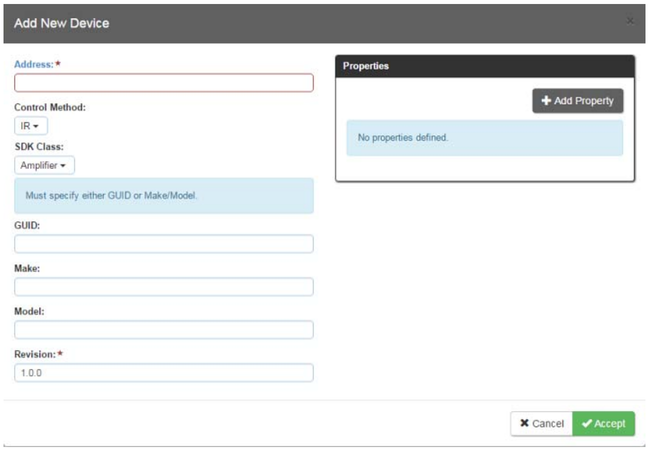
User-Defined Devices

| Address | Control Method | SDK Class | Make / Model | Delete |
|---|---|---|---|---|
| 5001:1:0 | Serial | Display | Sharp LC-80UH30U | ✖ |
| 5001:3:0 | Serial | Receiver | Denon AVR-2113CI | ✖ |
| 5001:4:0 | Serial | AudioConferencer | ClearOne Converge880T | ✖ |
| 5001:5:0 | Serial | Switcher | AMX EpicaDG | ✖ |
| 5010:3:0 | Serial | VideoProjector | Panasonic PT-VX400NT | ✖ |

**FIG. 53** Modules - User-Defined Devices

## Adding a User-Defined Device

1. Click the **Add Device** button (in the User-Defined Devices page) to access the **Add User Defined Device** page (FIG. 54):



Address: *

Control Method: IR

SDK Class: Amplifier

Must specify either GUID or Make/Model.

GUID:

Make:

Model:

Revision: * 1.0.0

No properties defined.

**FIG. 54** User-Defined Devices - Add New Device

2. Fill in the device information fields, as described in the following tables:

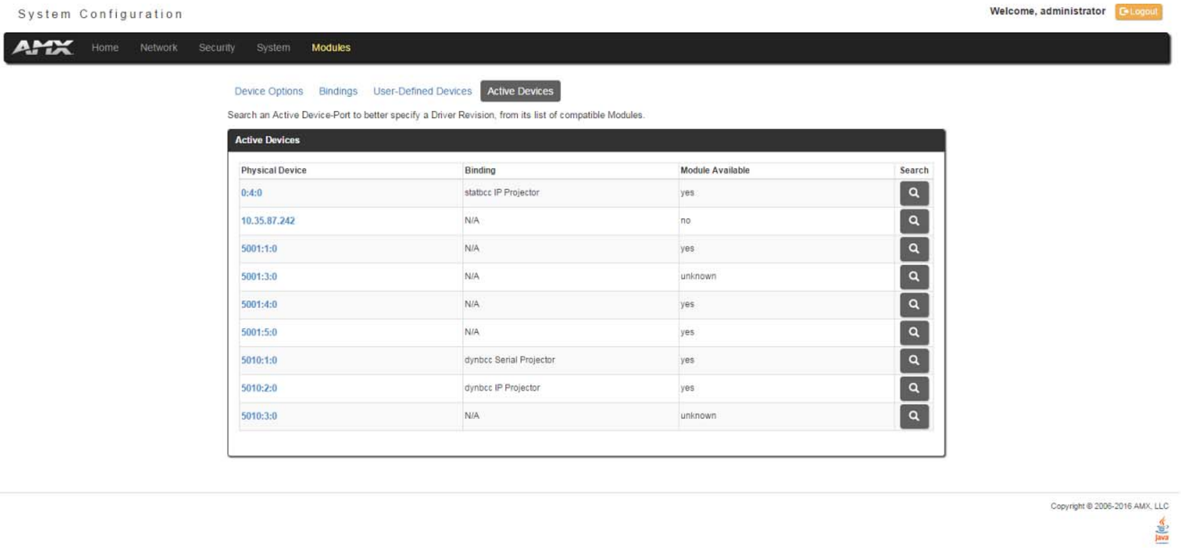
| User-Defined Device Information Fields | |
|---|---|
| Address: | Enter the address of the physical device in the Address field. This information can be either the NetLinx Master port value (D:P:S) or an IP Address (#.#.#.#). |
| Control Method: | Use the drop-down list to select the control method associated with the physical target device (*IR*, *IP*, *Serial*, *Other*). |
| SDK Class: | Use the drop-down list to select the closest Device SDK class type match for the physical target device. The SDK Class Types table on page 66 provides a listing of the available choices. |
| GUID: | Enter the manufacturer-specified device's GUID (Global Unique Identification) information. You must specify either the GUID or Make/Model. |
| Make: | Enter the name of the manufacturer for the device being used (ex: Sony, ONKYO, etc.)<br>• Up to 55 alpha-numeric characters<br>• Spaces in the name will be converted to underscores. |
| Model: | Enter the model number of the device being used (ex: Mega-Tuner 1000). You can enter up to 255 alpha-numeric characters. |
| Revision | Enter the firmware version used by the target device. 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). |

| SDK Class Types | | | |
|---|---|---|---|
| Amplifier | Digital Video Recorder | MultiWindow | Text Keypad |
| AudioConferencer | Disc Device | PoolSpa | TV |
| AudioMixer | Display | PreAmp Surround Sound Processor | UPS |
| AudioProcessor | Document Camera | Receiver | Utility |
| AudioTape | HVAC | RelayDevice | VCR |
| AudioTunerDevice | IODevice | RFID System | Video Conferencer |
| Camera | Keypad | Security System | Video Processor |
| Digital Media Decoder | Light | Sensor Device | Video Projector |
| Digital Media Encoder | Light System | Set Top Box | Video Wall |
| Digital Media Server | Monitor | Slide Projector | Volume Controller |
| Digital Satellite System | Motor | Switcher | Weather |

3. When you are finished with creating the profile for the new device, click the **Add Property** button to access the **Name** and **Value** fields property information for association with the new User Defined Device. This information appears in the Physical Device Properties for each device. See the *Viewing Physical Device Properties* section on page 67 for more information.
4. Click the **Accept** button. The new device is indicated in the list of discovered physical devices (in the *User-Defined Devices* page).

# Modules - Active Devices

Click the **Active Devices** link (in the *Manage Devices* tab) to access the **Active Devices** page (FIG. 55). The options on this page allow you to check devices for compatible Duet Modules.



Search an Active Device-Port to better specify a Driver Revision, from its list of compatible Modules.

Active Devices

| Physical Device | Binding | Module Available | Search |
|---|---|---|---|
| 0:4:0 | statbcc IP Projector | yes | 🔍 |
| 10.35.87.242 | N/A | no | 🔍 |
| 5001:1:0 | N/A | yes | 🔍 |
| 5001:3:0 | N/A | unknown | 🔍 |
| 5001:4:0 | N/A | yes | 🔍 |
| 5001:5:0 | N/A | yes | 🔍 |
| 5010:1:0 | dynbcc Serial Projector | yes | 🔍 |
| 5010:2:0 | dynbcc IP Projector | yes | 🔍 |
| 5010:3:0 | N/A | unknown | 🔍 |

Copyright © 2006-2016 AMX, LLC

**FIG. 55** Modules - Active Devices

## Searching For All Compatible Duet Modules for a Selected Device

1. Click the Search button for any device to search for a Duet Module for that particular device. This action initiates a search for compatible modules. 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.

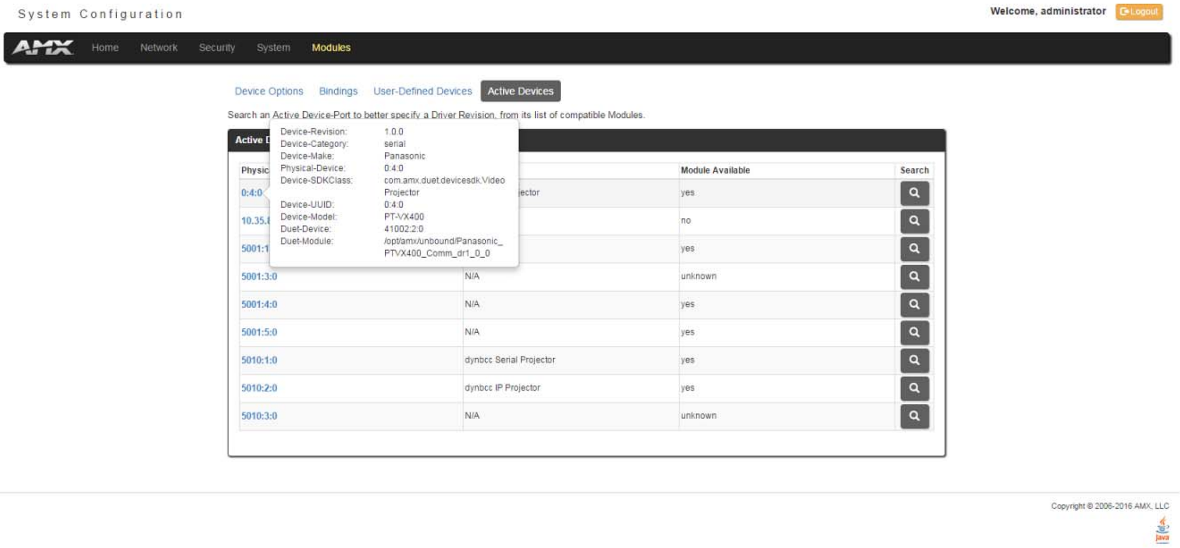
   If the device specified a **URL** in its DDD beacon, the file is retrieved from the URL either over the Internet or from the physical device itself, provided the device has an inboard HTTP or FTP server.
2. Once a list of all compatible modules is compiled, the list of available Duet Modules appears on this page.

   Each module is listed 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.
3. Select a module and click the **Accept** button to associate the selected Duet module 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.*

## Viewing Physical Device Properties

Hold the mouse cursor over the **Device** entry in the table to display detailed device properties for that device, in a pop-up window (FIG. 56).



Search an Active Device-Port to better specify a Driver Revision, from its list of compatible Modules.

| | |
|---|---|
| Device-Revision: | 1.0.0 |
| Device-Category: | serial |
| Device-Make: | Panasonic |
| Physical-Device: | 0:4:0 |
| Device-SDKClass: | com.amx.duet.devicesdk.Video Projector |
| Device-UUID: | 0:4:0 |
| Device-Model: | PT-VX400 |
| Duet-Device: | 41002:2:0 |
| Duet-Module: | /opt/amx/unbound/Panasonic_ PTVX400_Comm_dr1_0_0 |

| Physic | | Module Available | Search |
|---|---|---|---|
| 0:4:0 | jector | yes | |
| 10.35.8 | | no | |
| 5001:1 | | yes | |
| 5001:3:0 | N/A | unknown | |
| 5001:4:0 | N/A | yes | |
| 5001:5:0 | N/A | yes | |
| 5010:1:0 | dynbcc Serial Projector | yes | |
| 5010:2:0 | dynbcc IP Projector | yes | |
| 5010:3:0 | N/A | unknown | |

**FIG. 56** Active Devices - Device Properties pop-up

# WebConsole - Switching Options

## Switching Overview

The Switching page is used to route the system's inputs to its outputs during system setup. Each input and output can be labeled by filling in the Input Name or Output Name field on the Configuration page. The one exception to this statement is the audio input "Downmix" button, which cannot be renamed.

**NOTE:** *The number of available video and audio inputs and outputs depends on the Enova DGX 100 Series model and the number and type of boards it contains.*

### Color-coded Switch Selection and Switching Orientation

Yellow buttons indicate they have been selected but not switched; blue buttons indicate an already routed switch.

**TIP:** *When disconnecting switches, selecting an input or an output in an already routed switch will turn the button from blue to white, but will leave a thin blue line around the button to indicate it is still active until Take is pressed.*

From a cleared state, switching is accomplished from either an input-orientation or an output-orientation depending on whether an input or an output is selected first. When an input is selected first, the Inputs title bar turns yellow (see FIG. 57) and "input-orientation switching" is enabled. Multiple outputs can then be selected for the input followed by Take to execute the switch(es). When an output is selected first, the Outputs title bar turns yellow and "output-orientation switching" is enabled. A single input can then be selected for the output followed by Take to execute the switch.

Pressing Clear before pressing Take allows you to start over.

**NOTE:** *The default selection (input button highlighted blue) for the Switching pane is Input 1, which also appears in the Input section of the vertical "Selected" bar to the right. All output buttons that the default selection is routed to are highlighted and also appear in the Outputs section of the Selected bar. FIG. 57 shows the factory default switch of one-to-all.*

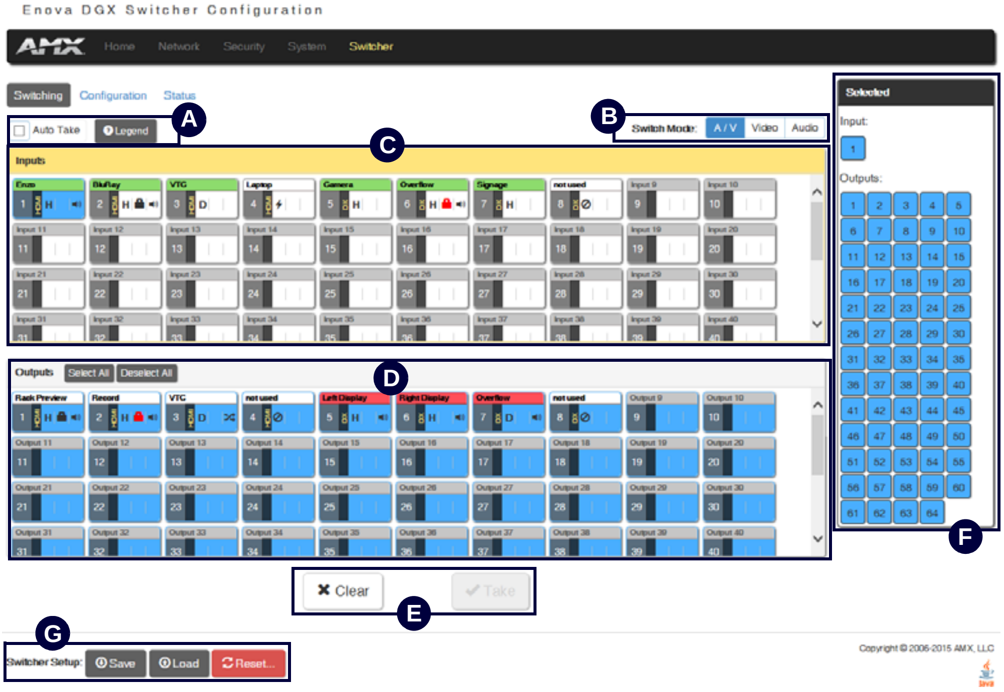


**FIG. 57** Switching page allows routing of inputs to outputs during system setup

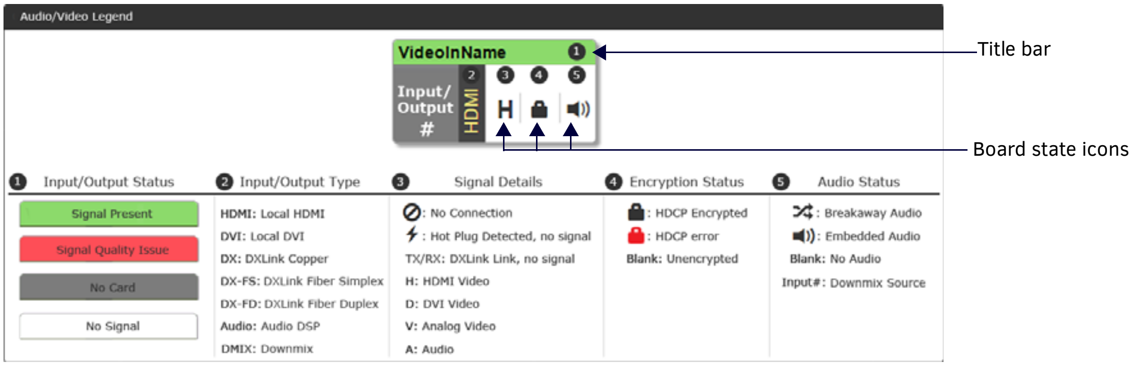
## Switching Page Components

The Switching page features the following components (labeled alphabetically to correspond to FIG. 57 on previous page):

A **Auto Take** button (default is unselected) – when checked, this button persists the Auto Take function and remains illuminated until unchecked. Once an input or output is selected, a click on an output for the input or on an input for an output will execute a switch. This allows for quick cycling through several inputs for a selected output. Note that when a button is selected, it also appears in the Configuration page with signal details (for button/signal details, click the Legend button).

**Legend** button – click to open an additional browser tab (Audio/Video Legend) which displays the legend key with details regarding the state of the input (source) and output (destination) connections. The browser tab opens in a tearaway tab/window that can be dragged and dropped as a standalone desktop window for side-by-side reference with the Switcher/Configuration pages.

**NOTE:** *The label on the title bar can be edited in the Input or Output Name field on the Configuration page.*



| 1 Input/Output Status | 2 Input/Output Type | 3 Signal Details | 4 Encryption Status | 5 Audio Status |
|---|---|---|---|---|
| Signal Present | HDMI: Local HDMI | ⊘: No Connection | 🔒: HDCP Encrypted | 🔀: Breakaway Audio |
| Signal Quality Issue | DVI: Local DVI | ⚡: Hot Plug Detected, no signal | 🔒: HDCP error | 🔊: Embedded Audio |
| No Card | DX: DXLink Copper | TX/RX: DXLink Link, no signal | Blank: Unencrypted | Blank: No Audio |
| No Signal | DX-FS: DXLink Fiber Simplex | H: HDMI Video | | Input#: Downmix Source |
| | DX-FD: DXLink Fiber Duplex | D: DVI Video | | |
| | Audio: Audio DSP | V: Analog Video | | |
| | DMIX: Downmix | A: Audio | | |

**NOTE:** *If the enclosure does not include a full set of input/output boards, input and output buttons for connectors that are not available display with a gray Title bar (i.e., No Card).*

B **Switch Mode** buttons – click the A/V (default), Video, or Audio button to select the type of signal to be switched. These buttons correspond to the available video and audio Virtual Matrices (VMs) in the system. For additional information on the Switch Mode, see page 70.

C **Inputs** section – this section contains buttons for each of the available input signals (per selected Switch Mode) in the system. Click the input button that needs to be switched. Scroll bars on the right-hand side provide access to any inputs on large systems which are not currently visible.

**Downmix** button – the Audio Switch Mode must be selected before the Downmix button displays. The input source used for the downmix signal is selected on the Configuration page.

D **Outputs** section – this section contains buttons for each of the available output signals in the system. Click the output button(s) that needs to receive the signal from the currently selected input button. Note that when the currently selected button is an output, it also appears in the Configuration page with signal details (for button/signal details, click the Legend button). Scroll bars on the right-hand side provide access to any outputs on large systems which are not currently visible.

**Select All** and **Deselect All** buttons – these buttons appear only after an input is selected. Click as necessary to select or deselect all output buttons.

E **Clear** button – click to deselect all inputs and outputs (if selected, the Auto Take button state persists) and clear routing status in the Configuration pane. Note that the Clear button *does not* disconnect switches. After the Clear button is selected and the input or one of the outputs already routed is selected, the buttons turn blue to indicate current status. Selecting an output will show status for the input routed to it, not the other outputs also routed from the same input.

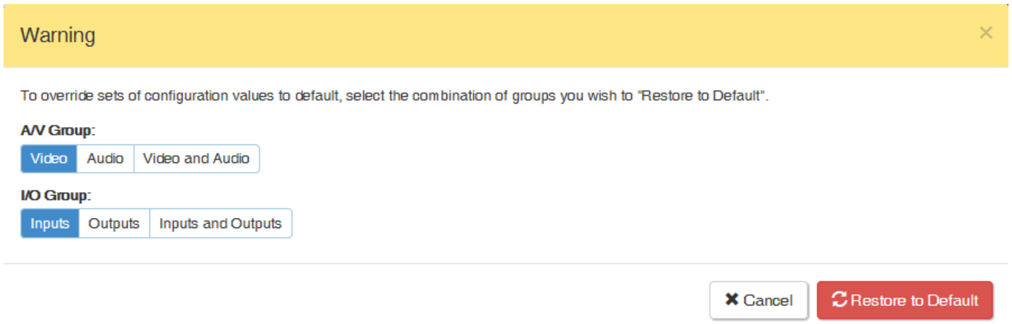
**Take** button – click to execute the switch for the selected input and output(s). After the switch is made, the current content in the Switching and Configuration pages persists until further action is taken. Note that the Take button is grayed out until one input and one or more outputs have been selected for routing; once these conditions are met, the Take button becomes active. After the Take button is clicked, all of the buttons clear their status.

F **Selected** status bar (non-editable) – this status bar provides quick visual confirmation of input and output selections and their status (blue = currently routed; yellow = ready to route, waiting further action; blue outline = currently routed, but deselected in preparation to disconnect).

G **Switcher Setup** button options are available on both the Switching page and the Configuration page.

**Save and Load** buttons – after a system has been set up per the installation's requirements, the configuration values for the entire switcher's state (i.e., currently routed switches, video settings, and audio settings) can be saved and reloaded onto another system(s) or backup system(s) for reuse. The file type is .xdg with XML content. When the Save button is clicked, the file is saved as a managed content (non-editable text) file.

**Group Restore to Default** button – click to open the Warning dialog box below, which requires you to select an A/V Group and an I/O Group to restore to their factory default settings.



Warning

To override sets of configuration values to default, select the combination of groups you wish to "Restore to Default".

A/V Group:

I/O Group:

## Switch Mode

The Switch Mode buttons allow you to choose between switching Audio follow Video (A/V), Video (with embedded audio), or Audio only.

**IMPORTANT:** *Support for the Audio Switch Mode (VM 2) requires Audio Switching Boards in the enclosure.*

- A/V and Video input and output ranges cover the basic switching size of the system:
  - 8x8, 16x16, 32x32, or 64x64
- Audio only input and output ranges cover the embedded audio as part of the basic switching size of the system, plus the audio available on the Audio Switching Boards (ASB) in the expansion slots, plus the assignment of one input as a downmixed audio channel:
  - Enova DGX 800: 1-8 embedded audio, 9-16 audio only, 17 downmix audio only
  - Enova DGX 1600: 1-16 embedded audio, 17-24 audio only, 25 downmix audio only
  - Enova DGX 3200: 1-32 embedded audio, 33-40 audio only, 41 downmix audio only
  - Enova DGX 6400: 1-64 embedded audio, 65-80 audio only, 81 downmix audio only

**To execute** a switch, click the Switch Mode button (otherwise the switch will default to A/V), an Input button, an Output button(s), and the Take button. (This is called input-oriented switching, also known as one-to-many switching.)

**NOTE:** *If you select an output button first (output-oriented switching, which can only be one-to-one switching), you must select an input button next followed by the Take button, i.e., you cannot select additional outputs before you select the input. If you select an output button first and then the input button, the only way to select multiple outputs is to click the Clear button and click the input button followed by the output buttons.*

**To deselect** (clear status) of an input button that has already been selected, click another input button *or* click Clear.

**To deselect** (clear status) of a single output button that has already been selected (before an input button), click another output button *or* Click Clear.

**To clear status** of an input and any or all output buttons, click Clear.

**To disconnect** all currently selected outputs for an input, click the Deselect All button followed by clicking Take.

**To execute** a switch with a downmixed signal,* the Audio Switch Mode must be selected and the input used for the Downmix signal must be selected on the Configuration page. Click the Downmix button, click the output(s), and click Take.

* Audio Switching Boards must be present for this functionality to work.

## Configuring/Switching the Downmix Signal

When the system contains Audio Switching Boards, *one* embedded audio signal** can be downmixed and routed at any given time.

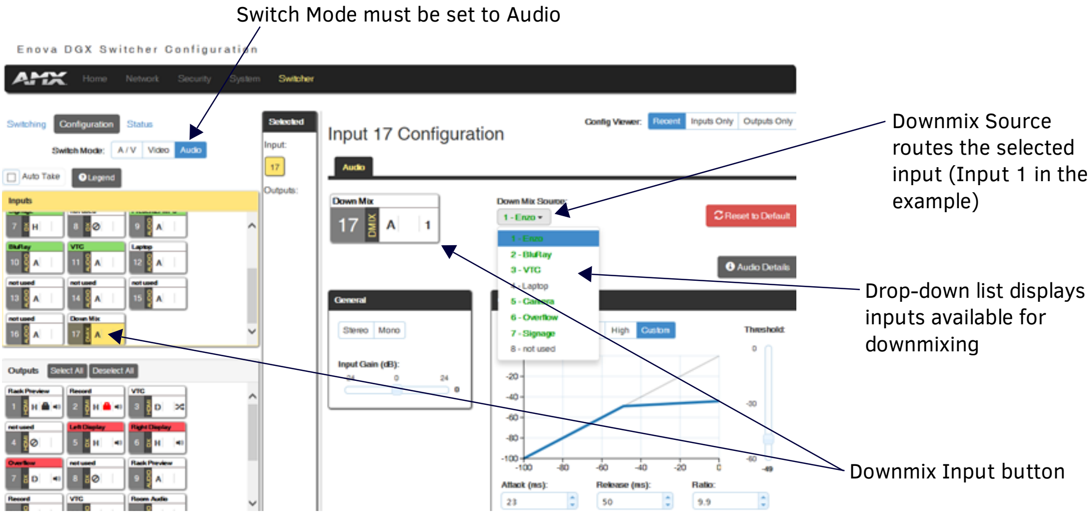
** Signal *must be* Dolby, TrueHD, Dolby Digital, DTS-HD Master Audio, DTS, or 2 CH through 8 CH L-PCM.

When Audio Switch Mode is selected, the "Downmix" input automatically displays as the last analog audio input+1. The Downmix Input number for each of the Enova 100 Series models is shown in the following table.

| Downmix Input # | |
|---|---|
| Enova DGX 800 | 17 |
| Enova DGX 1600 | 25 |
| Enova DGX 3200 | 41 |
| Enova DGX 6400 | 81 |

**NOTE:** *The table above also applies to Enova 8/16/32/64 enclosures that have been upgraded with an Enova DGX 100 Series CPU and that contain Audio Switching Boards.*

From the Configuration page – to designate which source will be routed on the Downmix Input, click the Downmix button in the Switching pane on the left and then select the input from the Downmix Source drop-down list in the Configuration pane on the right.



Switch Mode must be set to Audio

Downmix Source routes the selected input (Input 1 in the example)

Drop-down list displays inputs available for downmixing

Downmix Input button

**FIG. 58** Downmix input ready to switch or configure

## Designating an Input for Downmixing (from Configuration page)

1. In the Switching pane on the left, select Audio Switch Mode.
   The Downmix button displays at the end of the input buttons.
2. Select the Downmix button.
3. In the Configuration pane on the right, select the input from the Downmix Source drop-down list.
   The Downmix signal is ready to apply any of the configuration options or to execute switches.
4. To use a different input source for downmixing, repeat Steps 1-3 (only *one* input can be downmixed at a time).

# Configuration Page

The Configuration page is used to configure inputs and outputs in the system. The most recently selected input or output displays in the Configuration page in accordance with the currently selected Config Viewer button (Recent, Inputs Only, or Outputs Only). The Configuration page displays the Switching page components compressed on the left. Note that the components are active, i.e., they can be used for all switching functionality without needing to return to the full Switching page.

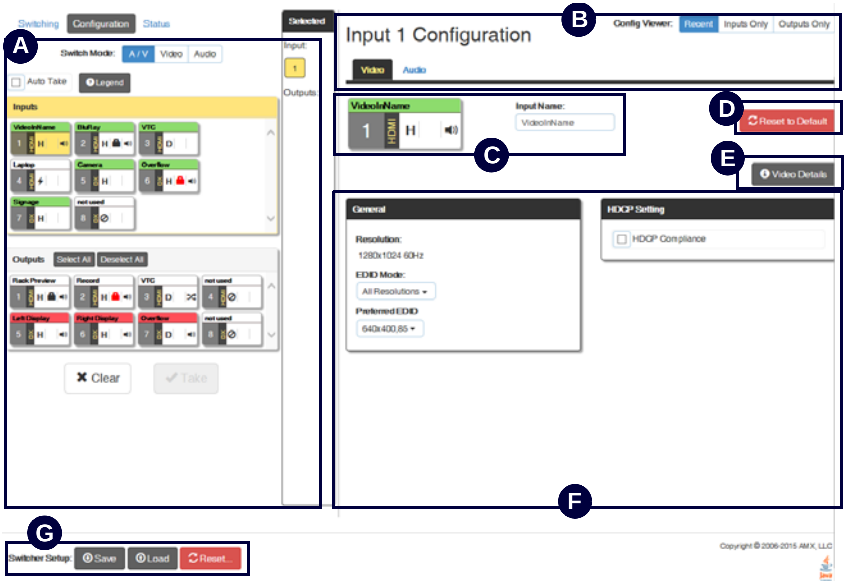


**FIG. 59** Configuration page allows configuration of inputs and outputs

## Configuration Components

Any changes made in the Configuration page occur instantaneously on the attached devices. In addition, when you select an input or an output on the left, the options on the right side of the page change to reflect the current settings. Configuration is not affected by power loss, restarting the enclosure, or upgrading the firmware.

**NOTE:** *The number of available video and audio inputs and outputs depends on the Enova DGX 100 Series model and the number and type of boards it contains.*

A **Switching** page components – all of the components from the Switching page are compressed and displayed (for details, see previous section on the “Switching Page”).

**Input** and **Output** buttons are selected individually for configuration.

B **Input #** or **Output # Configuration** heading (large text above the Video and Audio tabs) – changes according to the input or output currently selected for configuration.

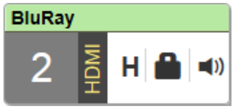
**Video** (default) and **Audio** tabbed views – click tabs to configure the video or audio signal that is selected in the Switching view. The signal will be either input or output depending on the Config Viewer button selection. The setting options vary depending on the signal.

**Config Viewer** buttons – the Recent, Inputs Only, and Outputs Only buttons allow you to choose the source or destination signal to be configured. Settings for the current Config Viewer remain when leaving the page and reactivate upon return. When the Recent button is clicked, the last selected input or output and its settings display. If no inputs or outputs are selected before opening the page, then the information will be cleared.

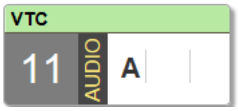
**NOTE:** *When the Inputs Only button is selected, clicking an output button in the Switching components will result in blank Configuration information; the same is true for selecting the Outputs Only button and then clicking an input button.*

C Selecting any video or audio signal button will display corresponding information as follows:

**Input** or **Output** button – an enlargement of the button selected under Switching (or from the Switching page) appears on the Configuration side with the source name and number, plus signal details (for an explanation of the button’s details, click the Legend button).



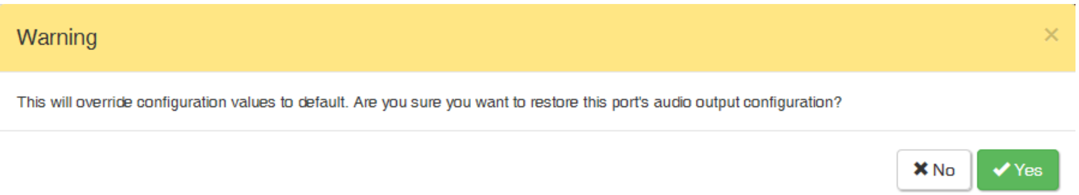
Video button



Audio button

**Input Name** or **Output Name** field – use to label the buttons in the Switching pane (and on the Switching page). Type the name in the field and press Enter on the keyboard.

D **Restore to Default** (red) button – click to open the Warning dialog box below, which requires you to select the Yes button to restore the currently selected input or output to its factory default settings.

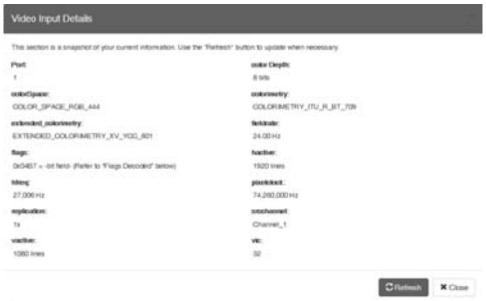


Warning ×

This will override configuration values to default. Are you sure you want to restore this port's audio output configuration?

✖ No ✔ Yes

E **Video Details** or **Audio Details** button – click to display additional video or audio details for inputs or outputs, depending on current selection (video: colorSpace, flags, pixelclock, etc.; audio: CTS Value, N Value, Audio Mute State, etc.). Examples of both Video Input and Output Details are shown below. Audio details are similar.



Video Input Details

This section is a snapshot of your current information. Use the "Refresh" button to update when necessary.

Port:
1

colorSpace:
COLOR_SPACE_RGB_444

extended_colorimetry:
EXTENDED_COLORIMETRY_XV_YCC_601

flags:
0x0487 = -bit field- (Refer to "Flags Decoded" below)

tdfreq:
27,000 Hz

replication:
1x

vactive:
1080 lines

color Depth:
8 bits

colorimetry:
COLORIMETRY_ITU_R_BT_709

fieldrate:
24.00 Hz

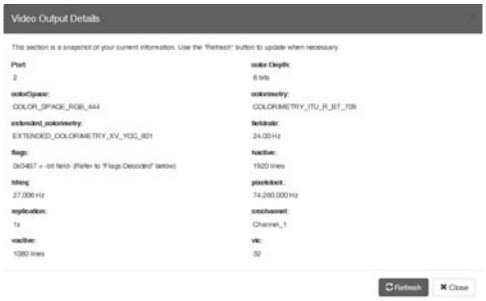
hactive:
1920 lines

pixelclock:
74,250,000 Hz

srcchannel:
Channel_1

vic:
32

Refresh ✖ Close



Video Output Details

This section is a snapshot of your current information. Use the "Refresh" button to update when necessary.

Port:
2

colorSpace:
COLOR_SPACE_RGB_444

extended_colorimetry:
EXTENDED_COLORIMETRY_XV_YCC_601

flags:
0x0487 = -bit field- (Refer to "Flags Decoded" below)

tdfreq:
27,000 Hz

replication:
1x

vactive:
1080 lines

color Depth:
8 bits

colorimetry:
COLORIMETRY_ITU_R_BT_709

fieldrate:
24.00 Hz

hactive:
1920 lines

pixelclock:
74,250,000 Hz

srcchannel:
Channel_1

vic:
32

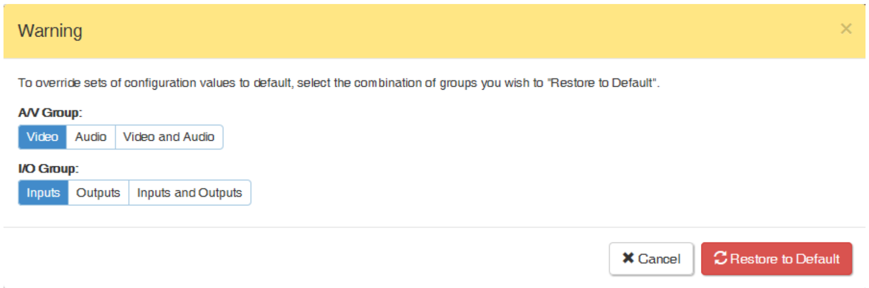
Refresh ✖ Close

F **Video**, **DXLink**, and **Audio** settings – the settings section of the Configuration page changes depending on the type of signal, whether it is an input or an output, and whether a DXLink unit is attached. A variety of interface controls are used to change the settings (e.g., buttons, sliders, drop-down lists) depending on the values involved. Details for these settings follow this section.

G **Switcher Setup** button options are available on both the Switching and the Configuration pages.

**Save** and **Load** buttons – after a system has been set up per the installation's requirements, the configuration values for the entire switcher's state (i.e., currently routed switches, video settings, and audio settings) can be saved and reloaded onto another system(s) or backup system(s) for reuse. The file type is .xdg with XML content. When the Save button is clicked, the file is saved as a non-editable text file.

**Group Restore to Default** button – click to open the Warning dialog box below, which requires you to select an A/V Group and an I/O Group to restore to their factory default settings.



Warning ×

To override sets of configuration values to default, select the combination of groups you wish to "Restore to Default".

A/V Group:

Video | Audio | Video and Audio

I/O Group:

Inputs | Outputs | Inputs and Outputs

✖ Cancel | Restore to Default

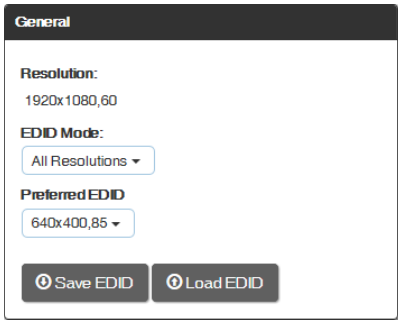
**IMPORTANT:** *When selecting a signal to configure, the Config Viewer button selection, Inputs Only or Outputs Only, must correspond to the input or output button selected.*

## Video Settings

Video settings display when the Switch Mode is A/V or Video, the Video tabbed view is selected, and a specific input or output is selected.

### Inputs Only

- General:



General

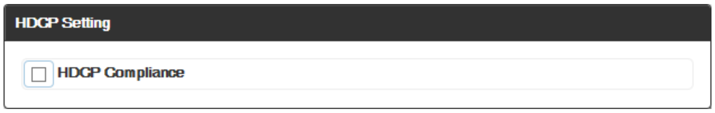
Resolution: 1920x1080,60

EDID Mode: All Resolutions

Preferred EDID 640x400,85

- Resolution – displays Resolution (read-only).
- EDID Mode – in the drop-down list, select the resolution type (All Resolutions, Wide-Screen, Full-Screen, or Custom).
- Preferred EDID – in the drop-down list, select the specific resolution/refresh rate.
- Save EDID button – use to save (persist them in memory) the EDID settings for the currently selected input
- Load EDID button – use to load the EDID settings for the currently selected input to other inputs.

- HDCP Setting:



HDCP Setting

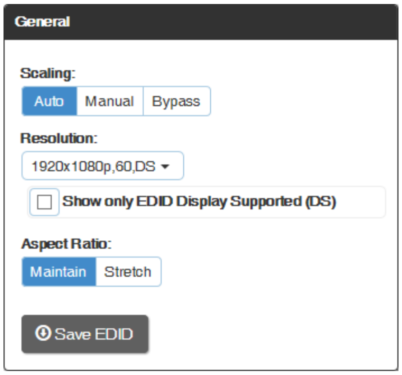
☐ HDCP Compliance

- HDCP Compliance – if desired, click the check box to enable HDCP compliance.

**NOTE:** *When EDID Mode/All Resolutions is selected, the Preferred EDID drop-down list includes both standard EDIDs and Video Information Code (VIC) EDIDs (denoted by either a “p” or an “i”). For a complete list of VIC EDIDs for your input boards see the “EDID Resolutions Supported through Local DDC” section of the applicable board chapter.*

### Outputs Only

- General:



General

Scaling: [✓ Auto] Manual Bypass

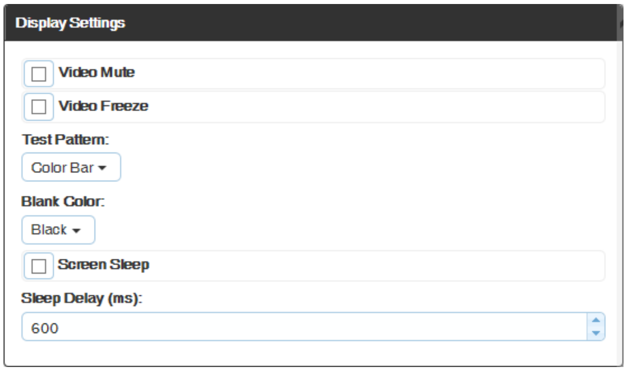
Resolution: 1920x1080p,60,DS

☐ Show only EDID Display Supported (DS)

Aspect Ratio: [✓ Maintain] Stretch

- Scaling (Mode) – click the button for the mode (Auto, Manual, or Bypass)
- Resolution – in the drop-down list, select the resolution/refresh rate; select the “Show only EDID Display Supported (DS)” check box if desired.
- Aspect Ratio – click either Maintain or Stretch (Zoom and Anamorphic are also available for DXLink outputs).
- Save EDID – click this button to save the EDID setting for the currently selected output.

- Display Settings:



Display Settings

□ Video Mute

□ Video Freeze

Test Pattern:

Color Bar ▾

Blank Color:

Black ▾

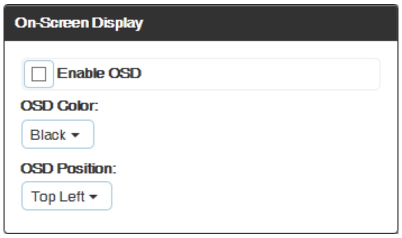
□ Screen Sleep

Sleep Delay (ms):

600

  - Video Mute – click the check box to mute the video.
  - Video Freeze – click the check box to freeze the video.
  - Test Pattern – in the drop-down list, select Off, Color Bar, Gray Ramp, SMPTE Bar, HiLo Trak, Pluge, or X-Hatch.
  - Blank Color – in the drop-down list, select Black or Blue.
  - Screen Sleep – click the check box to place the display in sleep mode; in the Sleep Delay (ms) box, set the delay time in milliseconds.

- On-Screen Display:



On-Screen Display

□ Enable OSD

OSD Color:

Black ▾

OSD Position:

Top Left ▾

  - Enable OSD – click check box to enable.
  - OSD Color – in the drop-down list, select Black, Blue, White, or Yellow.
  - OSD Position – in the drop-down list, select Top Left, Top Right, Bottom Left, or Bottom Right.

- Image Adjustments:

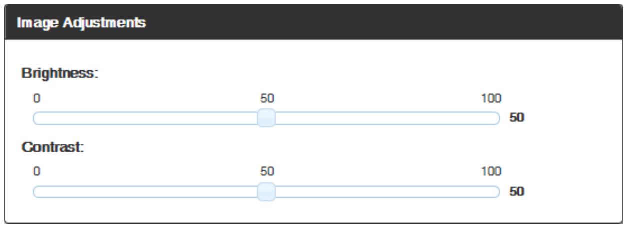


Image Adjustments

Brightness:

0 50 100

50

Contrast:

0 50 100

50

  - Brightness – use the slider bar to adjust (range: 0 to 100).
  - Contrast – use the slider bar to adjust (range: 0 to 100).

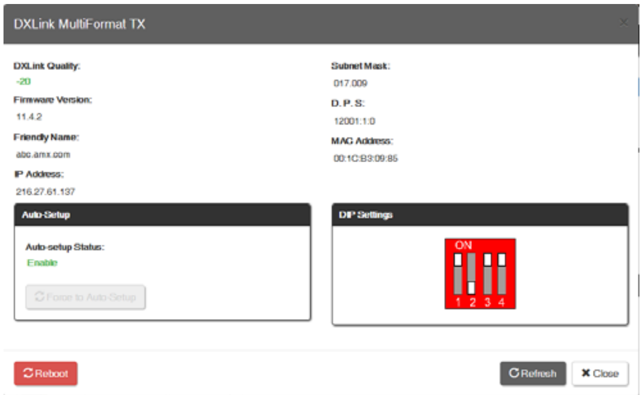
**NOTE:** *For additional EDID configuration information, see page 80.*

## DXLink Video Settings

DXLink specific video settings display when a DXLink Twisted Pair or DXLink Fiber Transmitter or Receiver (or other DXLink equipment) is connected to the selected input or output. These settings display in addition to the normal video settings for the input or output described in the previous section. The Video tabbed view *must* be selected.

### DXLink (Twisted Pair or Fiber) Transmitters (for selected video input)

- Video Priority – click either the HDMI, Analog, or Manual button.
- AV Source – click Analog or Digital.
- Video Type – non-editable.
- DXLink Details button – click to display additional settings for the DXLink Transmitter.



DXLink MultiFormat TX

DXLink Quality:
-20

Firmware Version:
11.4.2

Friendly Name:
abc.amx.com

IP Address:
216.27.61.137

Subnet Mask:
017.009

D. P. S:
12001:1:0

MAC Address:
00:1C:B3:09:85

Auto-Setup

Auto-setup Status:
Enable

TX Settings:

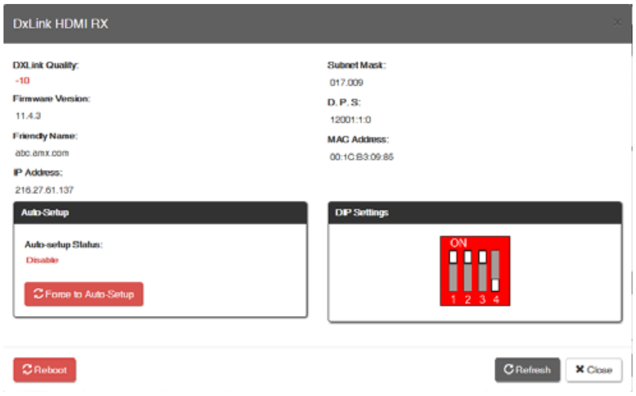
- DXLink Quality – green = good; red = poor; number indicates degree or lack of quality
- Firmware Version – current version
- Friendly Name – current name
- IP Address – for auto-setup, displays integrated Master's IP address
- Subnet Mask – current setting
- D. P. S. – current setting
- MAC Address – current setting
- Auto-Setup – Status (Enable/Disable) and Force to Auto-setup button
- DIP Settings – indicates settings on DIP switch
- Reboot button – reboots TX
- Refresh button – updates status of TX settings

- VGA Settings (DXLink Twisted Pair only) – use sliders to adjust Phase, Horizontal Shift, and Vertical Shift settings.

**IMPORTANT:** *The DXLink settings are not asynchronous. To obtain the latest information, the Refresh button in the dialog box that opens when the DXLink Details button is clicked must be clicked.*

### DXLink (Twisted Pair or Fiber) Receivers (for selected video output)

- DXLink Details button – click to display additional settings for the DXLink Receiver.



DxLink HDMI RX

DXLink Quality:
-10

Firmware Version:
11.4.3

Friendly Name:
abc.amx.com

IP Address:
216.27.61.137

Subnet Mask:
017.009

D. P. S:
12001:1:0

MAC Address:
00:1C:B3:09:85

Auto-Setup

Auto-setup Status:
Disable

RX Settings:

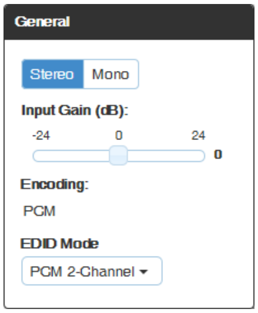
- DXLink Quality – green = good; red = poor; number indicates degree or lack of quality
- Firmware Version – current version
- Friendly Name – current name
- IP Address – for auto-setup, displays integrated Master's IP address
- Subnet Mask – current setting
- D. P. S. – current setting
- MAC Address – current setting
- Auto-Setup – Status (Enable/Disable) and Force to Auto-setup button
- DIP Settings – indicates settings on DIP switch
- Reboot button – reboots RX
- Refresh button – updates status of RX settings

## Audio Settings

Audio settings display when the Switch Mode is A/V or Audio (for details, see page 70), the Audio tabbed view is selected, and a specific input or output is selected. The audio settings can be used to configure any digital signal processing required for the audio signal that is selected in the Switching view.

### Inputs Only

- General:



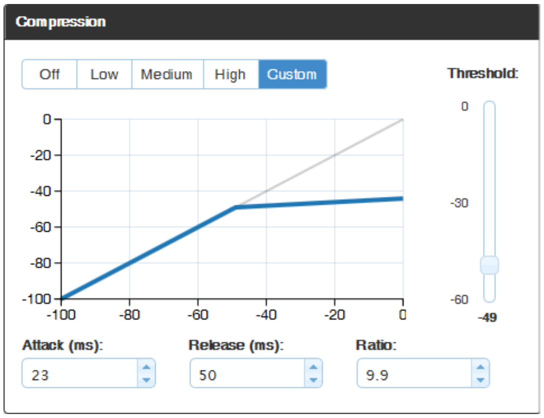
Input Gain (dB): 0

Encoding: PCM

EDID Mode: PCM 2-Channel

  - Stereo or Mono buttons – click either.*
  - Input Gain (dB) – use the slider bar to adjust (-24 dB to +24 dB),
  - Encoding – PCM (read only)
  - EDID Mode – from the drop-down list, select the mode (Basic, PCM 2-Channel, PCM Multi-Channel, Dolby Digital, Dolby Digital + DTS, Dolby Digital + MPEG, Dolby Digital + AAC, Dolby TrueHD, or DTS HD Master).

- Compression:



Threshold: -49

Attack (ms): 23

Release (ms): 50

Ratio: 9.9

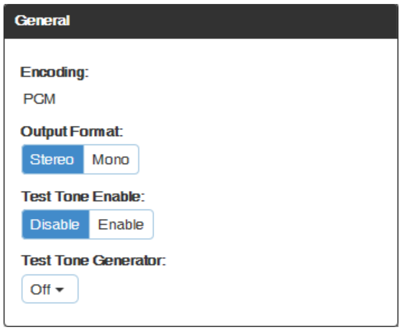
  - Buttons at top – click Off, Low, Medium, High, or Custom.
  - Threshold – use the slider bar to adjust (range: 0 to -60).
  - Attack (ms), Release (ms), and Ratio – adjust the values in the boxes (either enter values or use the arrows)

**NOTE:** *When in Low, Medium, or High, changes to any of the other Compression settings will automatically change the Compressor mode to Custom.*

* Setting this option to “Mono” audio on the input results in the left channel being sent to both the left and right output channels.

### Outputs Only

- General settings:



General

Encoding:
PCM

Output Format:
Stereo Mono

Test Tone Enable:
Disable Enable

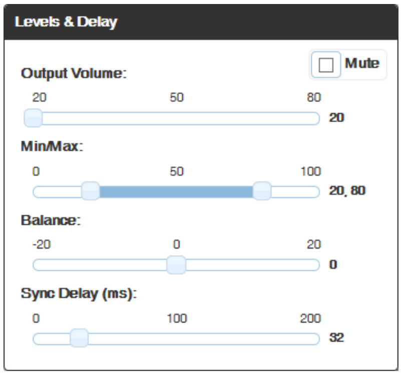
Test Tone Generator:
Off ▾

  - Encoding – PCM (read only).
  - Output Format – click Stereo or Mono.*
  - Test Tone Enable – click Disable or Enable.
  - Test Tone Generator – from the drop-down list, select Off, 60Hz, 250Hz, 400Hz, 1kHz, 3kHz, 5kHz, 10kHz, Pink Noise, or White Noise.
  - Audio Routing – click Embedded or Switched.**

* Setting this option to “Mono” audio on the output results in the left and right channels being combined and sent to both the left and right output channels equally.

** With Audio Switching Boards in the system, Audio Routing defaults to Switched.

- Levels & Delay:



Levels & Delay

□ Mute

Output Volume:
20 50 80
20

Min/Max:
0 50 100
20, 80

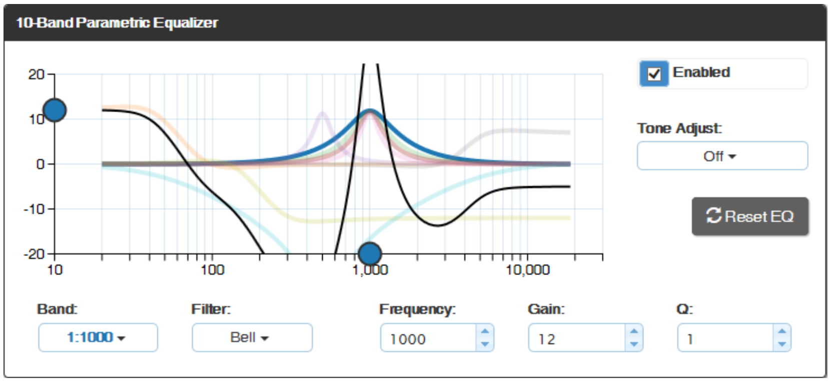
Balance:
-20 0 20
0

Sync Delay (ms):
0 100 200
32

  - Mute – click Mute if desired.***
  - Output Volume (0 to 100)
  - Min/Max (0 to 100)
  - Balance (-20 to 20, left to right)
  - Sync Delay (ms) (0 to 200).

*** Changing the volume level will not un-mute the signal; however, the new volume level is saved and when the Mute button is deselected, the volume returns at the new level.

- 10-Band Parametric Equalizer:



10-Band Parametric Equalizer

☑ Enabled

Tone Adjust:
Off ▾

Reset EQ

Band: 1:1000 ▾

Filter: Bell ▾

Frequency: 1000

Gain: 12

Q: 1

  - Enabled – this check box *must* be selected before the Equalizer options are available.*
  - Tone Adjust – use the drop-down box to select: Off, Voice, Music, or Movie (Tone Adjust is applied on top of any equalizer adjustments).
  - Reset EQ – click this button to reset the all of the Equalizer values.

- Blue Handles – use the sliders (blue handles) to adjust Equalizer values.
- The following drop-down lists can also be used to adjust Equalizer values.
- Band – numbered from 1 to 10.
- Filter – the options are Bell, Band Pass, Band Stop, High Pass, Low Pass, Treble Shelf, and Bass Shelf.
- Frequency – the adjustment range is from 20 to 20000 (Hz).
- Gain – the adjustment range is from -12 to 12.
- Q – the adjustment range depends on the filter selected:

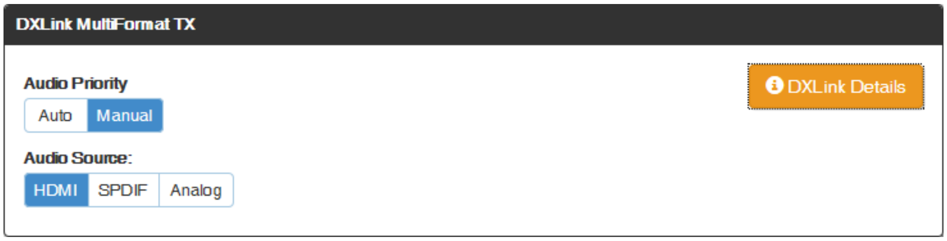
Bell = 0.1 to 20
Band Pass = 0.1 to 20
Band Stop = 0.1 to 20
High Pass = 0.5 to 1.4
Low Pass = 0.5 to 1.4
Treble Shelf = 0.5 to 1
Bass Shelf = 0.5 to 1

* On reboot, the Enabled box always returns to the checked (default) state. To disable the Equalizer options over a reboot, set the "y" (vertical) vertex to 0 (zero).

## DXLink Audio Settings

DXLink specific audio settings display when a DXLink Twisted Pair or DXLink Fiber Transmitter or Receiver (or other DXLink equipment) is connected to the selected input or output. These settings display in addition to the normal audio settings for the input or output described in the previous section. The Audio tabbed view *must* be selected.

### DXLink (Twisted Pair or Fiber) Transmitter (for selected audio input)

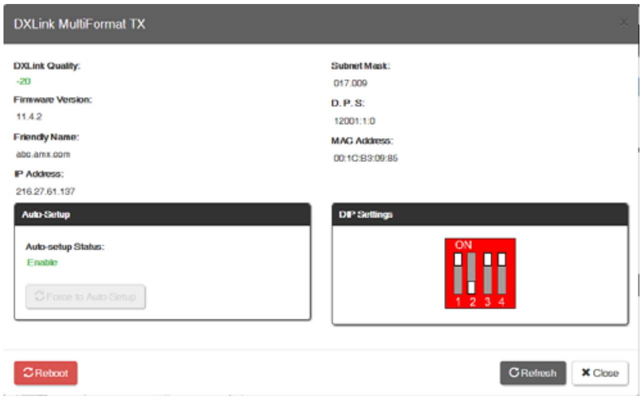


DXLink MultiFormat TX

Audio Priority: Manual

Audio Source: HDMI

- Audio Priority – click either the Auto or Manual button.
- Audio Source – click either the HDMI, SPDIF, or Analog button
- DXLink Details button – click to display additional settings for the DXLink Transmitter.



DXLink MultiFormat TX

DXLink Quality: -20
Firmware Version: 11.4.2
Friendly Name: abc.amx.com
IP Address: 216.27.61.137
Subnet Mask: 017.009
D. P. S: 12001:1:0
MAC Address: 00:1C:B3:09:85

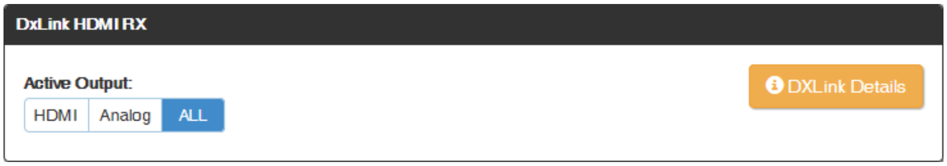
Auto-Setup
Auto-setup Status: Enable

DIP Settings

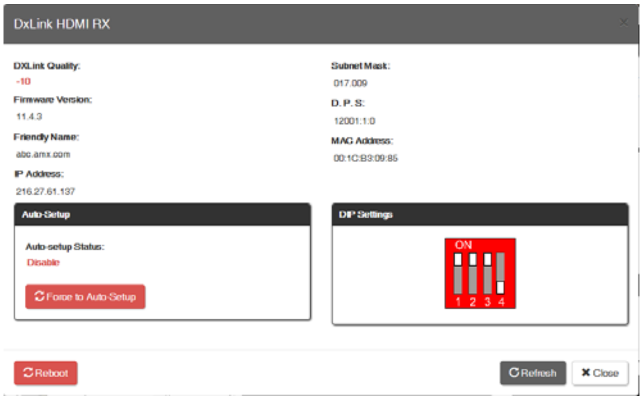
TX Settings:

- DXLink Quality – green = good; red = poor; number indicates degree or lack of quality
- Firmware Version – current version
- Friendly Name – current name
- IP Address – for auto-setup, displays integrated Master's IP address
- Subnet Mask – current setting
- D. P. S. – current setting
- MAC Address – current setting
- Auto-Setup – Status (Enable/Disable) and Force to Auto-setup button
- DIP Settings – indicates settings on DIP switch
- Reboot button – reboots TX
- Refresh button – updates status of TX settings

### DXLink (Twisted Pair or Fiber) Receivers (for selected audio output)



- Active Output – click either the HDMI, Analog, or All button.
- DXLink Details button – click to display additional settings for the DXLink Receiver.



DXLink Quality:
-10

Firmware Version:
11.4.3

Friendly Name:
abc.amx.com

IP Address:
216.27.61.137

Subnet Mask:
017.009

D. P. S:
12001:1:0

MAC Address:
00:1C:B3:09:85

Auto-Setup

Auto-setup Status:
Disable

RX Settings:

- DXLink Quality – green = good; red = poor; number indicates degree or lack of quality
- Firmware Version – current version
- Friendly Name – current name
- IP Address – for auto-setup, displays integrated Master's IP address
- Subnet Mask – current setting
- D. P. S. – current setting
- MAC Address – current setting
- Auto-Setup – Status (Enable/Disable) and Force to Auto-Setup button
- DIP Settings – indicates settings on DIP switch
- Reboot button – reboots RX
- Refresh button – updates status of RX settings

## EDID Configuration

**NOTE:** *Because signals routed through HDMI, DVI, DXLink Twisted Pair, and DXLink Fiber Boards in an Enova DGX 100 Series Switcher normally produce a quality image, you will not need the information in this section unless the installation has special EDID requirements.*

A default EDID (Extended Display Identification Data) is stored on the boards. This data is provided by the display and presented to the video source and includes timing and display size/format information for best performance.

### Setting an EDID for an Input:

1. From Configuration page / Switch Mode (on the left), click the Video button.
2. Check to be sure the Config Viewer on the top right is set to Inputs Only.
3. From the Switching pane on the left, select the video input.
4. Under General settings from the EDID Mode drop-down list, select the mode (All Resolutions, Wide-Screen, Full-Screen, or Custom).
5. Select the Preferred EDID from the drop-down list of resolutions/refresh rates.
6. Click the Save EDID button.*

* Once the preferred EDID is saved, it can be loaded to another input(s).

### Setting an EDID for an Output:

1. From Configuration page / Switch Mode (on the left), click the Video button.
2. Check to be sure the Config Viewer on the top right is set to Outputs Only.
3. From the Switching pane on the left, select the video output.
4. Under General settings from the Resolution drop-down list, select the resolution/refresh rate.**
5. Under General settings, click the Save EDID button.

** Click the "Show only EDID Display Supported (DS)" check box to narrow the drop-down list to show only those resolution/refresh rate options marked DS (Display Supported).

### Setting the EDID Mode for an Audio Input:

1. From Configuration page / Switch Mode (on the left), click the Audio button.
2. Check to be sure the Config Viewer on the top right is set to Inputs Only.
3. From the Switching page components on the left, select the audio input.
4. Under General settings from the EDID Mode drop-down list, select the mode: Basic, PCM 2-Channel, PCM Multi-Channel, Dolby Digital, Dolby Digital + DTS, Dolby Digital + MPEG, Dolby Digital + AAC, Dolby TrueHD, or DTS HD Master.

### Loading and Saving EDIDs

For custom EDIDs, click the Load EDID button and browse for the .edid file on your device/computer. Once the EDID is loaded, make any necessary changes and use the Save EDID button to save the altered .edid file to your device/computer.

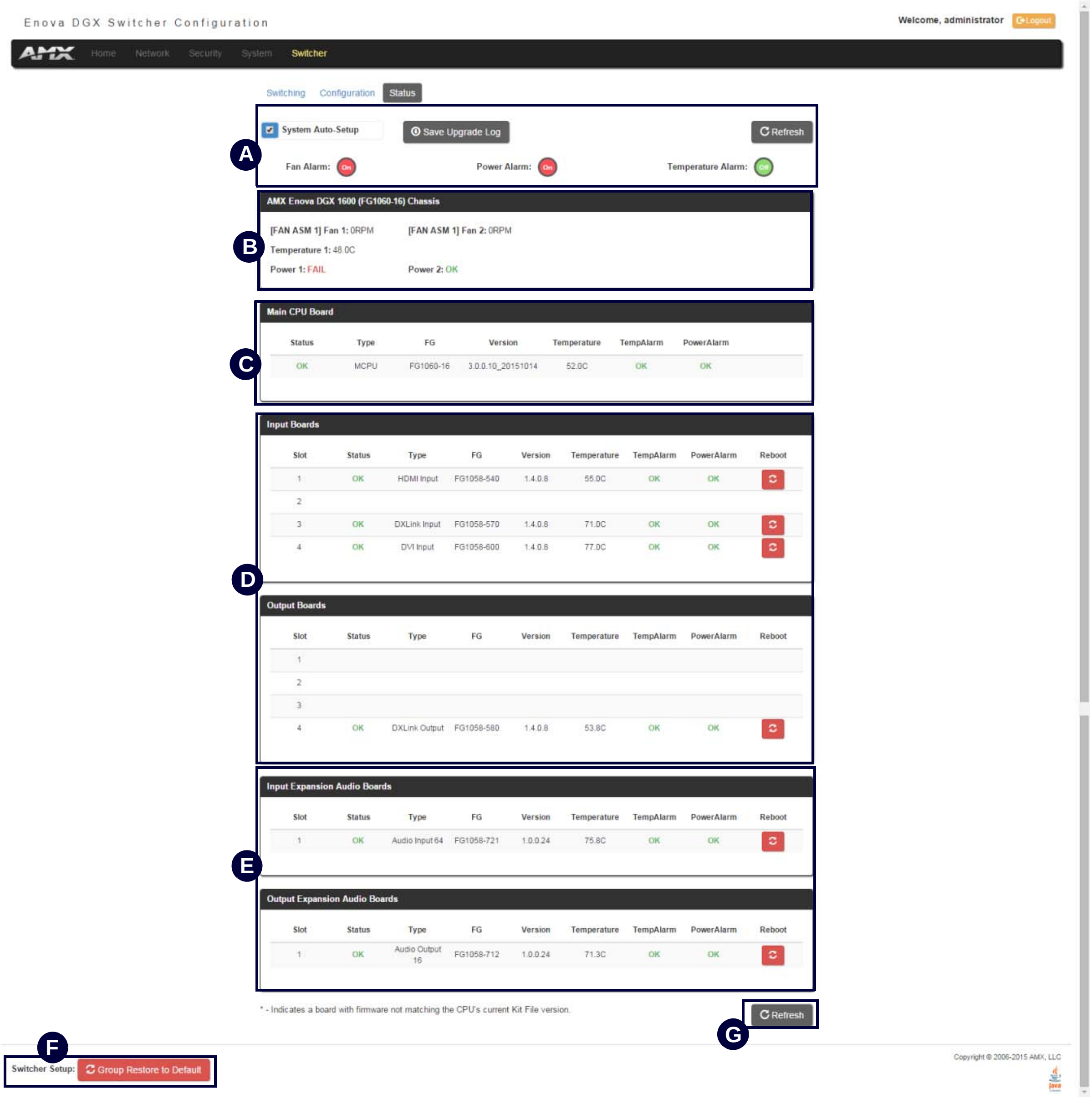
**NOTE:** *Some devices run on a secured file-system. As such, file-system operations (e.g., Load and Save operations) may not be supported by the device's default capabilities and may require downloading a file manager application.*

# Status Page

The Status page is used to check a number of the switcher's components and their states. The components (from top to bottom of page) display status for Alarms, the Chassis, the Master CPU Board, Input and Output Boards, and Input and Output Expansion Audio Boards. A quick glance at this page will indicate whether the system is running okay (green text will state OK) or if any thing is failing (red text will state FAIL.)

**IMPORTANT:** *The Status page settings are not asynchronous. To obtain the latest information, the Refresh button must be clicked.*

The example provided in the figure below is based on an Enova DGX 3200 Switcher with two each standard Input and Output Boards, as well as two Expansion Audio Boards.



**AMX Enova DGX 1600 (FG1060-16) Chassis**

[FAN ASM 1] Fan 1: 0RPM    [FAN ASM 1] Fan 2: 0RPM

Temperature 1: 48.0C

Power 1: FAIL    Power 2: OK

**Main CPU Board**

| Status | Type | FG | Version | Temperature | TempAlarm | PowerAlarm |
|---|---|---|---|---|---|---|
| OK | MCPU | FG1060-16 | 3.0.0.10_20151014 | 52.0C | OK | OK |

**Input Boards**

| Slot | Status | Type | FG | Version | Temperature | TempAlarm | PowerAlarm | Reboot |
|---|---|---|---|---|---|---|---|---|
| 1 | OK | HDMI Input | FG1058-540 | 1.4.0.8 | 55.0C | OK | OK | ↻ |
| 2 | | | | | | | | |
| 3 | OK | DXLink Input | FG1058-570 | 1.4.0.8 | 71.0C | OK | OK | ↻ |
| 4 | OK | DVI Input | FG1058-600 | 1.4.0.8 | 77.0C | OK | OK | ↻ |

**Output Boards**

| Slot | Status | Type | FG | Version | Temperature | TempAlarm | PowerAlarm | Reboot |
|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | |
| 2 | | | | | | | | |
| 3 | | | | | | | | |
| 4 | OK | DXLink Output | FG1058-580 | 1.4.0.8 | 53.8C | OK | OK | ↻ |

**Input Expansion Audio Boards**

| Slot | Status | Type | FG | Version | Temperature | TempAlarm | PowerAlarm | Reboot |
|---|---|---|---|---|---|---|---|---|
| 1 | OK | Audio Input 64 | FG1058-721 | 1.0.0.24 | 75.8C | OK | OK | ↻ |

**Output Expansion Audio Boards**

| Slot | Status | Type | FG | Version | Temperature | TempAlarm | PowerAlarm | Reboot |
|---|---|---|---|---|---|---|---|---|
| 1 | OK | Audio Output 16 | FG1058-712 | 1.0.0.24 | 71.3C | OK | OK | ↻ |

* - Indicates a board with firmware not matching the CPU's current Kit File version.

Copyright © 2006-2015 AMX, LLC

**FIG. 60** Status page indicates status of system components

A **System Auto-Setup check box –** select to place the system in auto-setup mode (i.e., the mode wherein the system requires only a single IP address for the integrated Master, and each endpoint is automatically configured for communication via a private LAN hosted by the integrated Master).

The following must be adhered to when using auto-setup mode (default):

- ❑ Endpoints *must* be set to DHCP Mode (default)
- ❑ Endpoints *must* use NDP Master connection mode (default)
- ❑ Endpoints *must not* be currently bound (traditional NetLinx binding) to a Master
- ❑ Endpoints DIP switch setting for Toggle #3 (network connectivity) is ignored while in auto-setup mode

**NOTE:** *Some devices run on a secured file-system. As such, file-system operations (e.g., Load and Save operations) may not be supported by the device's default capabilities and may require downloading a file manager application.*

**Alarms** – if any are red, consult the individual Fan, Power, and Temperature components on the page to help pinpoint the location of the problem.

**Refresh button** – if necessary, use the Refresh button to view system status changes.

B **Chassis field** – this field contains readouts for individual fan speeds, individual power supply status, and the current temperature of the chassis (shown in degrees Celsius). Each readout displays in a color to convey statuses of **OK**, **Fail**, or no problems detected (black). Fan speed information is displayed by individual fans (Fan #) and the fan assembly where each fan is located (FAN ASM #). Power supply and temperature information is available in each switcher's General Specifications table in the "Product Overview and General Specifications" chapter.

C **Master CPU (MCPU) Board field** – this field displays information for Status, Model number of the integrated Master, FG (part) number, Version, Temperature (actual degrees in Celsius with OK or FAIL status), and Power (OK or FAIL status).

D **Input and Output Board fields** – these fields give detailed information for each input or output board in the enclosure: Slot, Status, Type, FG (part) number, Version, Temperature (actual degrees in Celsius with OK or FAIL status), and Power (OK or FAIL status). A red Reboot button at the right cycles power to the individual board.

E **Input and Output Audio Expansion Boards fields** – these fields give detailed information for each expansion input or output board in the enclosure: Slot, Status, Type, FG (part) number, Version, Temperature (actual degrees in Celsius with OK or FAIL status), and Power (OK or FAIL status). A red Reboot button at the right cycles power to the individual board.

F **Switcher Setup** (**Save**, **Load**, and **Group Restore to Default**) buttons – after a system has been set up per the installation's requirements, the configuration can be saved and reloaded onto another system(s) or backup system(s) for reuse. The Group Restore to Default button returns the system to its last previously saved state. This button will restore control values to default (initial) values. (This Restore button performs the same function for the entire system as the Configuration page's Restore to Default button does for individual inputs or outputs.)

G **Refresh button –** if necessary, use the Refresh button to view system status changes.

### System Configuration Interface Tips

- To change the network connection type from DHCP (default) to Static IP – navigate to Network/IPv4; click on Specific IP Address; enter values into the IP Address, Subnet Mask, and Gateway fields; then click Accept.
- To enable/disable auto-setup ¡V navigate to Switcher/Status; click the System Auto-Setup check box to add a check mark (enabled) or remove a check mark (disabled).
- To route audio without the benefit of audio options available via the interface – navigate to Switcher/Configuration; select Audio Switch Mode; select Outputs Only in the Config Viewer options; select the desired output; select Switched Audio Routing from the General options.

# NetLinx Programming

## Overview

This section describes the Send_Commands, Send_Strings, and Channel commands you can use to program the Master. 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.

**NOTE:** *All file names on the X-Series controllers are case sensitive. This includes all user files created or used within NetLinx or Java code. If you have legacy code that uses files, it is important that you verify that every reference to each file is consistent with regard to case. If your legacy code generates an error when accessing a file, it is likely due to inconsistent use of case in the filename.*

## Port Assignments by NetLinx Master

The following table lists the port assignments for NetLinx Masters:

**Port Assignments By Master**

| Master | RS-232 | RS-232/422/485 | IR/Serial | IR/RX | Relays | I/O | PoE |
|---|---|---|---|---|---|---|---|
| NX-1200 | Port 2 | Port 1 | Ports 11-12 | Port 20 | N/A | Port 22 | N/A |
| NX-2200 | Ports 2-4 | Port 1 | Ports 11-14 | N/A | Port 21 | Port 22 | N/A |
| NX-3200 | Ports 2-4, 6-8 | Ports 1, 5 | Ports 11-18 | N/A | Port 21 | Port 22 | N/A |
| NX-4200 | Ports 2-4, 6-8 | Ports 1, 5 | Ports 11-18 | N/A | Port 21 | Port 22 | Ports 24-27 |

## Port Assignments by All-in-One-Presentation Switcher

The following table lists the port assignments for Enova All-in-One Presentation Switchers:

**Port Assignments By Enova All-in-One Presentation Switcher**

| Master | RS-232 | RS-232/422/485 | IR/Serial | Relays | I/O |
|---|---|---|---|---|---|
| DVX-22xxHD | Ports 2-4 | Port 1 | Ports 11-14 | Port 21 | Port 22 |
| DVX-325xHD | Ports 2-4, 6-8 | Ports 1, 5 | Ports 11-18 | Port 21 | Port 22 |

## Port Assignments by Massio ControlPad

The following table lists the port assignments for Massio ControlPads:

**Port Assignments By ControlPad**

| ControlPad | RS-232 | IR/Serial | Relays | I/O | NetLinx |
|---|---|---|---|---|---|
| MCP-106 | Port 1 | Port 11 | N/A | N/A | Port 28 |
| MCP-108 | Ports 1-2 | Ports 11-12 | Port 21 | Port 22 | Port 28 |

## Serial, IR, AxLink, and PoE Port Diagnostics

When a string is sent to a serial port or an IR pulse to an IR port, the X-Series controllers can detect and report if the port being used is in a fault condition. The controllers can also detect certain fault conditions on the AxLink bus. The following fault conditions are recognized:

- The serial cable is not connected
- The Serial pin is connected to another pin
- The IR emitter is not connected
- The IR emitter is wired backwards
- One or both AxLink bus data pins are shorted to power or ground
- The maximum power for all PoE ports (72W) has been exceeded or the power supply voltage is outside of the recommended limits
- The maximum current for a single PoE port has been exceeded or the load has disconnected from an individual port

On the first attempt to use a port that is in a fault condition, the controller will do the following:

- Quickly flash the front panel LED of the port being used 10 times
- Generate an ONERROR data event in NetLinx
- Report the error to any Duet Module that has claimed the port
- Report the error to RMS if the controller is connected to an RMS server
- Set an error flag for that port

The status of the error flag can be queried using the GET FAULT NetLinx command, which will result in a DATA EVENT where the return status can be parsed.

**NOTE:** *If the fault condition persists, subsequent attempts to use the same port will only result in the quick flashing of the front panel LED. The ONERROR event and the reporting to a Duet Module or RMS only occur on the first attempt after booting or after the fault status is cleared. This prevents a flood of redundant error messages when a faulted port is used continuously.*

The fault status is cleared on a successful transmission over the port, and also can be cleared manually using the CLEAR FAULT NetLinx command.

For serial and IR ports, an error condition is only checked at the time the port is used, so unused serial and IR ports will not generate errors. AxLink bus errors are checked at boot time.

## 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 you are connected to).

A device (<DEV>) must first be defined in the NetLinx programming language with values for the Device: Port: System (<D:P:S>).

| 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.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'CLOCK <mm-dd-yyyy> <hh:mm:ss>'"`<br>Variables:<br>mm-dd-yyyy = Month, day, and year. Month and day have 2 significant digits. Year has 4 significant digits.<br>hh-mm-ss = Hour, minute, and seconds. Each using only 2 significant digits.<br>Example:<br>`SEND_COMMAND 0,"'CLOCK 04-12-2005 09:45:31'"`<br>Sets the Master's date to April 12, 2005 with a time of 9:45 am. |
| **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 Web Control devices to Web control list displayed in the browser.<br>Syntax:<br>`SEND_COMMAND <D:P:S>,"'G4WC "Name/Description",IP Address/URL,IP Port,Enabled'"`<br>Variables:<br>• Name/Description = A string, enclosed in double quotes, that is the description of the G4 Web Control instance. It is displayed in the browser.<br>• IP Address/URL = A string containing the IP Address of the G4 Web Control server, or a URL to the G4 Web Control server.<br>• IP Port = A string containing the IP Port of the G4 Web Control Server.<br>• Enabled = 1 or 0. If it is a 1 then the link is displayed. If it is a 0 then the link is disabled.<br>The combination of Name/Description, IP Address/URL, and IP Port are used to determine each unique listing.<br>Example:<br>`SEND_COMMAND 0:1:0,"'G4WC "Bedroom",192.168.1.2,5900,1'"`<br>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.<br>Syntax:<br>`SEND_COMMAND <D:P:S>,"'~IGNOREEXTERNALCLOCKCOMMANDS'"`<br>Example:<br>`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).<br>Type 1 is TCP.<br>Type 2 is UDP (standard)<br>Type 3 is UDP (2 way)<br>The NetLinx.axi defines constants for the protocol types:<br>CHAR IP_TCP = 1<br>CHAR IP_UDP = 2<br>CHAR IP_UDP_2WAY = 3<br>*Syntax*:<br>`SEND_COMMAND <D:P:S>,"'UDPSENDTO-<IP or URL>:<UDP Port Number>'"`<br>*Variables*:<br>• IP or URL = A string containing the IP Address or URL of the desired destination.<br>• UDP Port Number = A String containing the UDP port number of the desired destination.<br>Example 1:<br>`SEND_COMMAND 0:3:0,"'UDPSENDTO-192.168.0.1:10000'"`<br>Any subsequent SEND_STRING to 0:3:0 are sent to the IP Address 192.168.0.1 port 10000.<br>Example 2:<br>`SEND_COMMAND 0:3:0,"'UDPSENDTO-myUrl.com:15000'"`<br>Any subsequent SEND_STRING to 0:3:0 are sent to the URL myURL.com port 15000. |

## SSH SEND_COMMANDs

These command open or close SSH communication with a server:

| SSH SEND_COMMANDs | |
|---|---|
| **SSH_CLIENT_CLOSE** | Closes an open SSH communication port with a server.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'SSH_CLIENT_CLOSE(LocalPort)'`<br>Parameters:<br>• LocalPort - A user-defined (non-zero) integer value representing the local port on the client machine to use for this conversation. This local port number must be passed to SSH_CLIENT_OPEN to open the conversation.<br>Returns:<br>This function always returns 0. Errors are returned via the DATA_EVENT ONERROR method. The following errors may be returned from the call:<br>2 - General failure (out of memory)<br>4 - Unknown host<br>6 - Connection refused<br>7 - Connection timed out<br>8 - Unknown connection error<br>9 - Already closed<br>14 - Local port already used<br>16 - Too many open sockets<br>Example:<br>`SEND_COMMAND <DEV>,"'SSH_CLIENT_CLOSE(5000)'"` |
| **SSH_CLIENT_OPEN** | Opens a port for SSH communication with a server.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'SSH_CLIENT_OPEN(LocalPort, ServerAddress, remotePort, username, password, privateKeyPathname, privateKeyPassphrase)'"`<br>Parameters:<br>• LocalPort- A user-defined (non-zero) integer value representing the local port on the client machine to use for this conversation. This local port number must be passed to SSH_CLIENT_CLOSE to close the conversation.<br>• ServerAddress - A string containing either the IP address (in dotted-quad-notation) or the domain name of the server to which you want to connect.<br>• remotePort - The port number on the server that identifies the program or service that the client is requesting, typically 22<br>• username - Login user name<br>• password - Password for the user name, null if using PKI<br>• privateKeyPathname - Path to private key<br>• privateKeyPassphrase - Password for private key.<br>Returns:<br>This function always returns 0. Errors are returned via the DATA_EVENT ONERROR method. The following errors may be returned from the call:<br>2 - General failure (out of memory)<br>4 - Unknown host<br>6 - Connection refused<br>7 - Connection timed out<br>8 - Unknown connection error<br>9 - Already closed<br>14 - Local port already used<br>16 - Too many open sockets<br>Example:<br>`SEND_COMMAND <DEV>,"'SSH_CLIENT_OPEN(5000, '192.168.0.1', 22, 'user1', 'password', '/certs/id_rsa', '')'"` |

## LED SEND_COMMANDs

**NOTE:** *The following sections only apply to the integrated controller component of the NX-series controllers.*

The following commands enable or disable the LEDs on the Controller.

In the examples: <DEV> = Port 1 of the device. Sending to port 1 of the 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.<br>Issue this command to port 1 to disable all the LEDs on the Controller.<br>When activity occurs on a port(s) or Controller, the LEDs will not illuminate.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'LED-DIS'"`<br>Example:<br>`SEND_COMMAND Port_1,"'LED-DIS'"`<br>Disables all the LEDs on Port 1 of the Controller. |
| **LED-EN** | Enable the LED (on 32 LED hardware) for a port. When the port is active, the LED is lit. When the port is not active, the LED is not lit.<br>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.<br>Syntax:<br>`SEND_COMMAND <DEV>,'LED-EN'`<br>Example:<br>`SEND_COMMAND System_1,'LED-EN'`<br>Enables the System_1 Controller's LEDs. |

## RS232/422/485 Ports Channels

| RS-232/422/485 Port Assignments By Master | | |
|---|---|---|
| **Master** | **RS-232** | **RS-232/422/485** |
| NX-1200 | Port 2 | Port 1 |
| NX-2200 | Ports 2-4 | Port 1 |
| NX-3200 | Ports 2-4, 6-8 | Ports 1, 5 |
| NX-4200 | Ports 2-4, 6-8 | Ports 1, 5 |
| DVX-22xxHD | Ports 2-4 | Port 1 |
| DVX-325xHD | Ports 2-4, 6-8 | Ports 1, 5 |
| MCP-106 | Port 1 | N/A |
| MCP-108 | Ports 1-2 | N/A |

| 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. |

**NOTE:** *Massio ControlPads do not support RS-422 or RS-485 communications to other devices.*

# RS-232/422/485 SEND_COMMANDs

**RS-232/422/485 SEND_COMMANDs**

| Command | Description |
|---|---|
| **B9MOFF** | 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.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'B9MOFF'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'B9MOFF'"`<br>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. This command works in conjunction with the 'B9MOFF' command.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'B9MON'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'B9MON'"`<br>Resets the RS-232 port's communication parameters to nine data bits, one stop bit, and locks-in the baud rate. |
| **CHARD** | Set the delay time between all transmitted characters to the value specified (in 100 Microsecond increments).<br>Syntax:<br>`SEND_COMMAND <DEV>,"'CHARD-<time>'"`<br>Variable:<br>time = 0 - 255. Measured in 100 microsecond increments.<br>Example:<br>`SEND_COMMAND RS232_1,"'CHARD-10'"`<br>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).<br>Syntax:<br>`SEND_COMMAND <DEV>,"'CHARDM-<time>'"`<br>Variable:<br>time = 0 - 255. Measured in 1 millisecond increments.<br>Example:<br>`SEND_COMMAND RS232_1,"'CHARDM-10'"`<br>Sets a 10-millisecond delay between all transmitted characters. |
| **CLEAR FAULT** | Forces a reset back to normal status.<br>Syntax:<br>`SEND_COMMAND <DEV>, "'CLEAR FAULT'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'CLEAR FAULT'"` |
| **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.<br>If Clear To Send (CTS) is set high, then channel 255 is On.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'CTSPSH'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'CTSPSH'"`<br>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.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'CTSPSH OFF'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'CTSPSH OFF'"`<br>Turns off CTSPSH for the specified device. |

| RS-232/422/485 SEND_COMMANDs (Cont.) | |
|---|---|
| **Command** | **Description** |
| **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.<br>The port responds with:<br><port #>,<baud>,<parity>,<data>,<stop> [422] or [485] <ENABLED \| DISABLED><br>**NOTE:** *The RS-232 ports on Massio ControlPads are RS-232 only, so sending this SEND_COMMAND to enable or disable 422 or 485 mode on a Massio ControlPad via Telnet will have no effect on the ControlPad, and the ControlPad also will not return an error message.*<br>Syntax:<br>`SEND_COMMAND <DEV>,"'GET BAUD'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'GET BAUD'"`<br>System response example:<br>`Device 1,38400,N,8,1 422/485 DISABLED` |
| **GET FAULT** | Check the activation status of fault detection on the port.<br>Syntax:<br>`SEND_COMMAND <DEV>, "’GET FAULT’"`<br>Example:<br>`SEND_COMMAND RS232_1,"’GET FAULT’"`<br>Responds with a COMMAND event: DISABLED, NONE, or NO DEVICE. |
| **GET STATUS** | Check the fault detection status of the port.<br>Syntax:<br>`SEND_COMMAND <DEV>, "’GET STATUS’"`<br>Example:<br>`SEND_COMMAND RS232_1,"’GET STATUS’"`<br>Responds with a COMMAND event: STATUS: NORMAL or STATUS: FAULT. |
| **HSOFF** | Disable hardware handshaking (default).<br>Syntax:<br>`SEND_COMMAND <DEV>,"'HSOFF'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'HSOFF'"`<br>Disables hardware handshaking on the RS232_1 device. |
| **HSON** | Enable RTS (ready-to-send) and CTS (clear-to-send) hardware handshaking.<br>**NOTE:** *This SEND_COMMAND is not compatible with Massio ControlPads. While you may execute this command via Telnet, the command will have no effect on the ControlPad, and the ControlPad also will not return an error message.*<br>Syntax:<br>`SEND_COMMAND <DEV>,"'HSON'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'HSON'"`<br>Enables hardware handshaking on the RS232_1 device. |
| **RXCLR** | Clear all characters in the receive buffer waiting to be sent to the Master.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'RXCLR'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'RXCLR'"`<br>Clears all characters in the RS232_1 device's receive buffer waiting to be sent to the Master. |
| **RXOFF** | Disable the transmission of incoming received characters to the Master.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'RXOFF'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'RXOFF'"`<br>Stops the RS232_1 device from transmitting received characters to the Master. |
| **RXON** | Start transmitting received characters to the Master (default).<br>Enables sending incoming received characters to the Master.<br>This command is automatically sent by the Master when a 'CREATE_BUFFER' program instruction is executed.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'RXON'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'RXON'"`<br>Sets the RS232_1 device to transmit received characters to the Master. |

**RS-232/422/485 SEND_COMMANDs (Cont.)**

| Command | Description |
|---|---|
| **SET BAUD** | Set the RS-232/422/485 port's communication parameters.<br>**NOTE:** *On NX-series controllers, ports 1&5 support RS-232, RS-422, or RS485. The three modes are mutually exclusive. Setting any of the three modes disables the other two.*<br>**NOTE:** *The RS-232 ports on Massio ControlPads are RS-232 only, so sending the SEND_COMMAND to Enable 422 or 485 mode on a Massio ControlPad via Telnet will have no effect on the ControlPad, and the ControlPad will not return an error message.*<br>Syntax:<br>`SEND_COMMAND <DEV>,"'SET BAUD <baud>,<parity>,<data>,<stop> [422 Enable \| 485 Enable]'"`<br>**NOTE:** *Serial modes are mutually exclusive. RS-232 is specified by omitting 422 Enable and 485 Enable. Enabling 422 effectively disables 232 and 485. Enabling 485 effectively disables 232 and 422.*<br>*Variables:*<br>baud = baud rates are: 115200, 76800, 57600, 38400, 19200, 9600, 4800, 2400, 1200, 600, 300, 150.<br>parity = N (none), O (odd), E (even), M (mark), S (space).<br>data = 8 data bits.<br>stop = 1 and 2 stop bits.<br>422 Enable = Enables 422 (Disables 232/485)<br>485 Enable = Enables 485 (Disables 232/422)<br>**NOTE:** *The only valid 9 bit combination is (baud),N,9,1.*<br>Example:<br>`SEND_COMMAND RS232_1,"'SET BAUD 115200,N,8,1 485 ENABLE'"`<br>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. |
| **SET FAULT DETECT OFF** | Disables fault detection on the port. Fault detection is turned on by default.<br>Syntax:<br>`SEND_COMMAND <DEV>, "'SET FAULT DETECT OFF'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'SET FAULT DETECT OFF'"` |
| **SET FAULT DETECT ON** | Enables fault detection on the port. Fault detection is turned on by default.<br>Syntax:<br>`SEND_COMMAND <DEV>, "’SET FAULT DETECT ON’"`<br>Example:<br>`SEND_COMMAND RS232_1,"’SET FAULT DETECT ON’"` |
| **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.<br>**NOTE:** *On NX-series controllers, ports 1&5 support RS-232, RS-422, or RS485. The three modes are mutually exclusive. Setting any of the three modes disables the other two.*<br>**NOTE:** *The RS-232 ports on Massio ControlPads are RS-232 only, so sending the SEND_COMMAND to Enable 422 or 485 mode on a Massio ControlPad via Telnet will have no effect on the ControlPad, and the ControlPad will not return an error message.*<br>Syntax:<br>`SEND_COMMAND <DEV>,"'SET BAUD <baud>,<parity>,<data>,<stop> [422 Enable \| 485 Enable]'"`<br>**NOTE:** *Serial modes are mutually exclusive. RS-232 is specified by omitting 422 Enable and 485 Enable. Enabling 422 effectively disables 232 and 485. Enabling 485 effectively disables 232 and 422.*<br>*Variables:*<br>baud = baud rates are: 115200, 57600, 38400, 19200, 9600, 4800, 2400, 1200, 600, 300.<br>parity = N (none), O (odd), E (even), M (mark), S (space).<br>data = 8 or 9 data bits.<br>stop = 1 or 2 stop bits.<br>422 Enable = Enables 422 (Disables 232/485)<br>485 Enable = Enables 485 (Disables 232/422)<br>**NOTE:** *The only valid 9 bit combination is (baud),N,9,1.*<br>Example:<br>`SEND_COMMAND RS232_1,"'TSET BAUD 115200,N,8,1 485 ENABLE'"`<br>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. |

**RS-232/422/485 SEND_COMMANDs (Cont.)**

| Command | Description |
|---|---|
| **TXCLR** | Stop and clear all characters waiting in the transmit out buffer and stops transmission.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'TXCLR'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'TXCLR'"`<br>Clears and stops all characters waiting in the RS232_1 device's transmit buffer. |
| **XOFF** | Disable software handshaking (default).<br>Syntax:<br>`SEND_COMMAND <DEV>,"'XOFF'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'XOFF'"`<br>Disables software handshaking on the RS232_1 device. |
| **XON** | Enable software handshaking.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'XON'"`<br>Example:<br>`SEND_COMMAND RS232_1,"'XON'"`<br>Enables software handshaking on the RS232_1 device. |

## RS-232/422/485 SEND_STRING Escape Sequences

NX Controllers also use some special SEND_STRING escape sequences. Use the ESCSEQON and ESCSEQOFF NetLinx SEND_COMMANDS to control whether escape sequences are active. The ESCSEQON command must precede the Escape Sequences, otherwise strings will be processed normally. These commands are sent to Port 1. Escape sequences are disabled by default.

If any of the 3 character combinations below are found anywhere within a SEND_STRING program instruction, they will be treated as a command 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.<br>Syntax:<br>`SEND_STRING <DEV>,"27,17,<time>"`<br>Variable:<br>time = 1 - 255. Measured in 100 microsecond increments.<br>Example:<br>`SEND_STRING RS232_1,"27,17,10"`<br>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.<br>Used in conjunction with the 'B9MON' command.<br>Syntax:<br>`SEND_STRING <DEV>,"27,18,0"`<br>Example:<br>`SEND_STRING RS232_1,"27,18,0"`<br>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.<br>Used in conjunction with the 'B9MON' command.<br>Syntax:<br>`SEND_STRING <DEV>,"27,18,1"`<br>Example:<br>`SEND_STRING RS232_1,"27,18,1"`<br>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.<br>Syntax:<br>`SEND_STRING <DEV>,"27,19,<time>"`<br>Variable:<br>time = 1 - 255. Measured in 1 millisecond increments.<br>Example:<br>`SEND_STRING RS232_1,"27,19,10"`<br>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).<br>Syntax:<br>`SEND_STRING <DEV>,"27,20,0"`<br>Example:<br>`SEND_STRING RS232_1,"27,20,0"`<br>Sets the RTS hardware handshake's output to high on the RS232_1 device. |
| **27,20,1** | Set the RTS hardware handshake's output to low/inactive (< 3V).<br>Syntax:<br>`SEND_STRING <DEV>,"27,20,1"`<br>Example:<br>`SEND_STRING RS232_1,"27,20,1"`<br>Sets the RTS hardware handshake's output to low on the RS232_1 device. |
| **ESCSEQOFF** | Disables SEND_STRING escape sequences.<br>Syntax:<br>`SEND_STRING <DEV>,"ESCSEQOFF"` |
| **ESCSEQON** | Enables SEND_STRING escape sequences.<br>Syntax:<br>`SEND_STRING <DEV>,"ESCSEQON"` |

## IR/Serial Ports Channels

| IR / Serial Ports Channels | |
|---|---|
| **CHANNELS:** | **Description** |
| 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). |
| 00256 - 65000 | IR commands. |
| 65000 - 65534 | Future use. |

## IRRX Port Channels

| IRRX Ports Channels | |
|---|---|
| 00001 - 00255 | PUSH and RELEASE channels for the received IR code. |

## 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.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'CAROFF'"`<br>Example:<br>`SEND_COMMAND IR_1,"'CAROFF'"`<br>Stops transmitting IR carrier signals to the IR_1 port. |
| **CARON** | Enable the IR carrier signals (default).<br>Syntax:<br>`SEND_COMMAND <DEV>,"'CARON'"`<br>Example:<br>`SEND_COMMAND IR_1,"'CARON'"`<br>Starts transmitting IR carrier signals to the IR_1 port. |
| **CH** | Send IR pulses for the selected channel. All channels below 100 are transmitted as two digits.<br>• If the IR code for ENTER (function #21) is loaded, an Enter will follow the number.<br>• 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.<br>• Uses 'CTON' and 'CTOF' times for pulse times.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'CH',<channel number>"`<br>Variable:<br>channel number = 0 - 199.<br>Example:<br>`SEND_COMMAND IR_1,"'CH',18"`<br>This device performs the following:<br>• Transmits IR signals for 1 (IR code 11). The transmit time is set with the CTON command.<br>• Waits until the time set with the CTOF command elapses.<br>• Transmits IR signals for 8 (IR code 18).<br>• Waits for the time set with the CTOF command elapses. If the IR code for Enter (IR code 21) is programmed, the Controller performs the following steps.<br>1) Transmits IR signals for Enter (IR code 21).<br>2) Waits for the time set with the CTOF command elapses. |
| **CLEAR FAULT** | Forces a reset back to normal status.<br>Syntax:<br>`SEND_COMMAND <DEV>, "'CLEAR FAULT'"`<br>Example:<br>`SEND_COMMAND IR_1,"'CLEAR FAULT'"` |

| IR/Serial SEND_COMMANDs (Cont.) | |
|---|---|
| **Command** | **Description** |
| **CP** | Halt and clear all active or buffered IR commands, and then send a single IR pulse.<br>Set the Pulse and Wait times with the 'CTON' and 'CTOF' commands.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'CP',<code>"`<br>Variable:<br>code = IR port's channel value 0 - 252 (253 - 255 reserved).<br>Example:<br>`SEND_COMMAND IR_1,"'CP',2"`<br>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.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'CTOF',<time>"`<br>Variable:<br>time = 0 - 255. Given in 1/10ths of a second. Default is 5 (0.5 seconds).<br>Example:<br>`SEND_COMMAND IR_1,"'CTOF',10"`<br>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.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'CTON',<time>"`<br>Variable:<br>time = 0 - 255. Given in 1/10ths of a second. Default is 5 (0.5 seconds).<br>Example:<br>`SEND_COMMAND IR_1,"'CTON',20"`<br>Sets the IR pulse duration to 2 seconds. |
| **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).<br>Syntax:<br>`SEND_COMMAND <DEV>,"'GET BAUD'"`<br>The port responds with:<br><port #> <baud>,<parity>,<data bits>,<stop bits><br>Example:<br>`SEND_COMMAND IR_1,"'GET BAUD'"`<br>System response example:<br>`PORT 11,9600,N,8,1` |
| **GET FAULT** | Check the activation status of fault detection on the port.<br>Syntax:<br>`SEND_COMMAND <DEV>, "'GET FAULT'"`<br>Example:<br>`SEND_COMMAND IR_1,"'GET FAULT'"`<br>Responds with a COMMAND event: DISABLED, NONE, SHORT, or NO DEVICE. |
| **GET MODE** | Poll the IR/Serial port's configuration parameters and report the active mode settings to the device requesting the information.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'GET MODE'"`<br>The port responds with:<br>`<port #> <mode>,<carrier>,<io link channel>`<br>Example:<br>`SEND_COMMAND IR_1,"'GET MODE'"`<br>The system could respond with:<br>`PORT 4 IR,CARRIER,IO LINK 0` |
| **GET STATUS** | Check the fault detection status of the port.<br>Syntax:<br>`SEND_COMMAND <DEV>, "'GET STATUS'"`<br>Example:<br>`SEND_COMMAND IR_1,"'GET STATUS'"`<br>Responds with a COMMAND event: STATUS: NORMAL or STATUS: FAULT. |

| IR/Serial SEND_COMMANDs (Cont.) | |
|---|---|
| **Command** | **Description** |
| **IROFF** | Halt and Clear all active or buffered IR commands being output on the designated port.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'IROFF'"`<br>Example:<br>`SEND_COMMAND IR_1,"'IROFF"`<br>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.<br>Channel 255 changes are enabled.<br>This command is used in conjunction with the `I/O Link` command.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'POD'"`<br>Example:<br>`SEND_COMMAND IR_1,"'POD'"`<br>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.<br>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.<br>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.<br>You can only use the 'PON' and 'POF' commands when an IR device has a linked I/O channel.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'POF'"`<br>Example:<br>`SEND_COMMAND IR_1,"'POF'"`<br>Sends power down IR commands 28 (if present) or 9 to the IR_1 device. |
| **PON** | Turn On a device connected to an IR port based on the status of the corresponding I/O Link input.<br>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.<br>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.<br>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.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'PON'"`<br>Example:<br>`SEND_COMMAND IR_1,"'PON'"`<br>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.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'PTOF',<time>"`<br>Variable:<br>time = 0 - 255. Given in 1/10ths of a second. Default is 15 (1.5 seconds).<br>Example:<br>`SEND_COMMAND IR_1,"'PTOF',15"`<br>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.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'PTON',<time>"`<br>Variable:<br>time = 0 - 255. Given in 1/10ths of a second. Default is 5 (0.5 seconds).<br>Example:<br>`SEND_COMMAND IR_1,"'PTON',15"`<br>Sets the duration of the power pulse to 1.5 seconds for the IR_1 device. |

**IR/Serial SEND_COMMANDs (Cont.)**

| Command | Description |
|---|---|
| **SET BAUD** | Set the IR port's DATA mode communication parameters.<br>Only valid if the port is in Data Mode (see SET MODE command).<br>Syntax:<br>`SEND_COMMAND <DEV>,"'SET BAUD <baud>,<parity>,<data>,<stop>'"`<br>Variables:<br>baud = baud rates are: 19200, 9600, 4800, 2400, and 1200.<br>parity = N (none), O (odd), E (even), M (mark), S (space).<br>data = 7 or 8 data bits.<br>stop = 1 and 2 stop bits.<br>Example:<br>`SEND_COMMAND IR_1,"'SET BAUD 9600,N,8,1'"`<br>Sets the IR_1 port's communication parameters to 9600 baud, no parity, 8 data bits, and 1 stop bit.<br>**NOTE:** *The maximum baud rate for ports using SERIAL mode is 19200. Also, SERIAL mode works best when using a short cable length (< 10 feet).* |
| **SET FAULT DETECT OFF** | Disables fault detection on the port. Fault detection is turned on by default.<br>Syntax:<br>`SEND_COMMAND <DEV>, "'SET FAULT DETECT OFF'"`<br>Example:<br>`SEND_COMMAND IR_1,"'SET FAULT DETECT OFF'"` |
| **SET FAULT DETECT ON** | Enables fault detection on the port. Fault detection is turned on by default.<br>Syntax:<br>`SEND_COMMAND <DEV>, "'SET FAULT DETECT ON'"`<br>Example:<br>`SEND_COMMAND IR_1,"'SET FAULT DETECT ON'"` |
| **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.<br>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.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'SET IO LINK <I/O number>'"`<br>Variable:<br>I/O number = 1 - 8. Setting the I/O channel to 0 disables the I/O link.<br>Example:<br>`SEND_COMMAND IR_1,"'SET IO LINK 1'"`<br>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. |

| IR/Serial SEND_COMMANDs (Cont.) | |
|---|---|
| **Command** | **Description** |
| **SET MODE** | Set the IR/Serial ports for IR or Serial-controlled devices to either **IR**, **Serial**, or **Data** mode.<br>Syntax:<br>`SEND_COMMAND <DEV>, 'SET MODE <mode>'"`<br>Variable:<br>mode = IR, SERIAL, or DATA.<br>Example:<br>`SEND_COMMAND IR_1,"'SET MODE IR'"`<br>Sets the IR_1 port to IR mode for IR control.<br>**NOTE:** *The maximum baud rate for ports using SERIAL mode is 19200. Also, SERIAL mode works best when using a short cable length (< 10 feet).* |
| **SP** | Buffers IR commands which haven't had time to execute yet, and executes each command until the buffer is empty.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'SP',<code>"`<br>Variable:<br>code = IR code value 1 - 252 (253-255 reserved).<br>Example:<br>`SEND_COMMAND IR_1, "'SP',25"`<br>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.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'XCH <channel>'"`<br>Variable:<br>channel = 0 - 9999.<br>Example:<br>For detailed usage examples, refer to the 'XCHM' command.<br>**NOTE:** *This command supports 4-digit channels.* |

| IR/Serial SEND_COMMANDs (Cont.) | |
|---|---|
| **XCHM** | Changes the IR output pattern for the 'XCH' send command.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'XCHM-<extended channel mode>'"`<br>Variable:<br>extended channel mode = 0 - 4.<br>Example:<br>`SEND_COMMAND IR_1,"'XCHM-3'"`<br>Sets the IR_1 device's extended channel command to mode 3.<br>Mode 0 Example (default): **[x][x]<x><enter>**<br>`SEND_COMMAND IR_1,"'XCH-3'"`<br>Transmits the IR code as 3-enter.<br>`SEND_COMMAND IR_1,"'XCH-34'"`<br>Transmits the IR code as 3-4-enter.<br>`SEND_COMMAND IR_1,"'XCH-343'"`<br>Transmits the IR code as 3-4-3-enter.<br>Mode 1 Example: **<x> <x> <x> <enter>**<br>`SEND_COMMAND IR_1,"'XCH-3'"`<br>Transmits the IR code as 0-0-3-enter.<br>`SEND_COMMAND IR_1,"'XCH-34'"`<br>Transmits the IR code as 0-3-4-enter.<br>`SEND_COMMAND IR_1,"'XCH-343'"`<br>Transmits the IR code as 3-4-3-enter.<br>Mode 2 Example: **<x> <x> <x>**<br>`SEND_COMMAND IR_1,"'XCH-3'"`<br>Transmits the IR code as 0-0-3.<br>`SEND_COMMAND IR_1,"'XCH-34'"`<br>Transmits the IR code as 0-3-4.<br>`SEND_COMMAND IR_1,"'XCH-343'"`<br>Transmits the IR code as 3-4-3.<br>Mode 3 Example: **[[100][100]...] <x> <x>**<br>`SEND_COMMAND IR_1,"'XCH-3'"`<br>Transmits the IR code as 0-3.<br>`SEND_COMMAND IR_1,"'XCH-34'"`<br>Transmits the IR code as 3-4.<br>`SEND_COMMAND IR_1,"'XCH-343'"`<br>Transmits the IR code as 100-100-100-4-3.<br>Mode 4: Mode 4 sends the same sequences as the 'CH' command. Only use Mode 4 with channels 0 - 199.<br>Mode 5 Example: **<x><x><x><x><enter>**<br>`SEND_COMMAND IR_1,"'XCH-3'"`<br>Transmits the IR code as 0-0-0-3-enter.<br>`SEND_COMMAND IR_1,"'XCH-34'"`<br>Transmits the IR code as 0-0-3-4-enter.<br>`SEND_COMMAND IR_1,"'XCH-343'"`<br>Transmits the IR code as 0-3-4-3-enter.<br>`SEND_COMMAND IR_1,"'XCH-1343'"`<br>Transmits the IR code as 1-3-4-3-enter.<br>Mode 6 Example: **<x><x><x><x>**<br>`SEND_COMMAND IR_1,"'XCH-3'"`<br>Transmits the IR code as 0-0-0-3.<br>`SEND_COMMAND IR_1,"'XCH-34'"`<br>Transmits the IR code as 0-0-3-4.<br>`SEND_COMMAND IR_1,"'XCH-343'"`<br>Transmits the IR code as 0-3-4-3.<br>`SEND_COMMAND IR_1,"'XCH-1343'"`<br>Transmits the IR code as 1-3-4-3. |

# Input/Output SEND_COMMANDs

The I/O port is port 22 on the NX-series controllers and the MCP-108 Massio ControlPad.

The following SEND_COMMANDs program the I/O ports on the Integrated Controller.

**I/O SEND_COMMANDs**

| Command | Description |
|---|---|
| **GET DBT** | Get Debounce Time<br>Syntax:<br>`GET DBT <n>`<br>Variable:<br>n = the channel number of the I/O input port<br>Example:<br>`SEND_COMMAND 5001:22:0,'GET DBT 1'`<br>Retrieves the Debounce time channel 1 on the I/O port.<br>Response:<br>`DBT 1 50`<br>Responds with the channel number and the Debounce time in milliseconds (ms). |
| **SET DBT** | Set Debounce Time<br>Syntax:<br>`SET DBT <n><v>`<br>Variables:<br>n = the channel number of the I/O input port<br>v = Value 1-50 which sets the debounce time in increments of 5ms<br>Example:<br>`SEND_COMMAND 5001:22:0,'SET DBT 1 10'`<br>Sets channel 1 on the I/O port to 50ms Debounce time. |
| **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'.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'GET INPUT <channel>'"`<br>Variable:<br>channel = Input channel 1 - 8.<br>Example:<br>`SEND_COMMAND IO,"'GET INPUT 1'"`<br>Gets the I/O port's active state.<br>The system could respond with:<br>`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.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'SET INPUT <channel> <state>'"`<br>Variable:<br>channel = Input channel 1 - 8.<br>state = Active state HIGH or LOW (default).<br>Example:<br>`SEND_COMMAND IO,"'SET INPUT 1 HIGH'"`<br>Sets the I/O channel to detect a high state change, and disables output on the channel. |

## PoE SEND_COMMANDs

The NX-4200 has 4 ICSLAN ports, each of which feature Power-over-Ethernet (PoE). The ports are numbered 1-4. The following PoE SEND_COMMANDs program the ICSLAN ports on the controller.

**NOTE:** *Note: These commands are not compatible with Massio ControlPads.*

**PoE SEND_COMMANDs**

| Command | Description |
|---|---|
| **GET CLASS** | Retrieve the class type of the device connected via PoE. This command receives a COMMAND event of ’DISABLED’, ’NO DEVICE’, or ’CLASS x DEVICE’, with x being a value from 0 to 4.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'GET CLASS'"`<br>Example:<br>`SEND_COMMAND PoE_24,"'GET CLASS'"` |
| **GET CURRENT** | Retrieve the current of the device connected via PoE. This command receives a COMMAND event with the number in milliamps (mA).<br>Syntax:<br>`SEND_COMMAND <DEV>,"'GET CURRENT'"`<br>Example:<br>`SEND_COMMAND PoE_24,"'GET CURRENT'"` |
| **GET FAULT** | Retrieve the type of fault on the PoE port. This command receives a COMMAND event of ’DISABLED’, ’NONE’, ’UNDER-VOLTAGE / OVER-VOLTAGE’, ’CURRENT OVERLOAD’, ’LOAD DISCONNECT’, MAX POWER EXCEEDED,’ or ’POE NOT AVAILABLE’.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'GET FAULT'"`<br>Example:<br>`SEND_COMMAND PoE_24,"'GET FAULT'"` |
| **GET STATUS** | Retrieve the status of the PoE port. This command receives a COMMAND event of ’STATUS: NORMAL’ or, ’STATUS: FAULT’.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'GET STATUS'"`<br>Example:<br>`SEND_COMMAND PoE_24,"'GET STATUS'"` |
| **GET VOLTAGE** | Retrieve the current draw on the PoE port. This command receives a COMMAND event with the number in volts.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'GET VOLTAGE'"`<br>Example:<br>`SEND_COMMAND PoE_24,"'GET VOLTAGE'"` |
| **SET FAULT DETECT OFF** | Disables fault detection on the PoE port. Fault detection is turned on by default.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'SET FAULT DETECT OFF'"`<br>Example:<br>`SEND_COMMAND PoE_24,"'SET FAULT DETECT OFF'"` |
| **SET FAULT DETECT ON** | Enables fault detection on the PoE port. Fault detection is turned on by default.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'SET FAULT DETECT ON'"`<br>Example:<br>`SEND_COMMAND PoE_24,"'SET FAULT DETECT ON'"` |
| **SET POWER OFF** | Disables PoE to the port. PoE is turned on by default.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'SET POWER OFF'"`<br>Example:<br>`SEND_COMMAND PoE_24,"'SET POWER OFF'"` |
| **SET POWER ON** | Enables PoE to the port. PoE is turned on by default.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'SET POWER ON'"`<br>Example:<br>`SEND_COMMAND PoE_24,"'SET POWER ON'"` |

## AxLink SEND_COMMANDs

The following commands program the AxLink ports on the NX controller.

**NOTE:** *These commands are not compatible with Massio ControlPads.*

| AxLink SEND_COMMANDs | |
|---|---|
| **Command** | **Description** |
| **AXPWROFF** | Powers off the specified AxLink port.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'AXPWROFF <UPPER\|LOWER>'"`<br>Variable:<br>UPPER\|LOWER = Specifies the AxLink port on the controller<br>Example:<br>`SEND_COMMAND 5001:1:0,"'AXPWROFF UPPER'"`<br>Powers off the upper AxLink port on the controller. |
| **AXPWRON** | Powers on the specified AxLink port.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'AXPWRON <UPPER\|LOWER>'"`<br>Variable:<br>UPPER\|LOWER = Specifies the AxLink port on the controller<br>Example:<br>`SEND_COMMAND 5001:1:0,"'AXPWRON LOWER'"`<br>Powers on the lower AxLink port on the controller. |
| **GET AX FAULT** | Retrieve the AxLink port which currently has a fault.<br>Syntax:<br>`SEND_COMMAND <DEV>,"'GET AX FAULT'"`<br>Example:<br>`SEND_COMMAND 5001:1:0,"'GET AX FAULT'"`<br>Responds with the COMMAND event: 'AX FAULT: UPPER/LOWER' or 'NONE'. |

## Audit Log SEND_COMMANDs

The following command enables you to send an audit log from a device.

| Audit Log SEND_COMMANDs | |
|---|---|
| **Command** | **Description** |
| **LOG** | Sends Audit Logs to the Master for output via Syslog. The D:P:S of the sending device will be added to the audit log. It is the sender's responsibility to ensure that the log conforms to the standard format (i.e. contains event type, component, source if not the device itself, identity and outcome).<br>Syntax:<br>`SEND_COMMAND <DEV>,"'LOG, <log text>'"`<br>or<br>`SEND_COMMAND <DEV>,"'LOG,<severity>,<log text>'"`<br>Variable:<br>log text - the text of the log message<br>severity - 1=fatal, 2=error, 3=warning, 4=info, 5=debug<br>Example:<br>`SEND_COMMAND <DEV>,"'LOG, TEST LOG'"`<br>`SEND_COMMAND <DEV>,"'LOG, 4, TEST LOG'"` |

# Authentication

The NetLinx.axi file that ships with NetLinx Studio includes the following types/constants for authentication:

```
(*-------------------------------------------------------------------------------------------*)
(* Added v1.56 *)
(*-------------------------------------------------------------------------------------------*)
STRUCTURE LAST_LOGIN_INFO
{
    INTEGER failedLoginCount
    CHAR lastSuccessfulLoginDate[MAX_LAST_LOGIN_INFO_LENGTH]
    CHAR lastSuccessfulLoginIp[MAX_LAST_LOGIN_INFO_LENGTH]
    CHAR lastFaileLoginDate[MAX_LAST_LOGIN_INFO_LENGTH]
    CHAR lastFailedLoginIp[MAX_LAST_LOGIN_INFO_LENGTH]
}
```

## Library Calls

The NetLinx.axi file that ships with NetLinx Studio includes the following Authentication-specific library calls:

| NetLinx.axi - Library Calls | |
|---|---|
| **TLS_CLIENT_CLOSE** | Closes an open TLS communication port with a remote device. Typically, the remote host closes the connection and you do not need to send this command.<br>Syntax:<br>`integer TLS_CLIENT_CLOSE(LocalPort)`<br>Parameters:<br>• LocalPort - A user-defined (non-zero) integer value representing the local port on the client machine to use for this conversation. This local port number must be passed to TLS_CLIENT_OPEN to open the conversation.<br>Returns:<br>0 - Success<br>1 - Error<br>Example:<br>`TLS_CLIENT_CLOSE(5000)` |
| **TLS_CLIENT_OPEN** | Opens a port for TLS communication with a remote device.<br>Syntax:<br>`integer TLS_CLIENT_OPEN(LocalPort, hostname, port, mode)`<br>Parameters:<br>• LocalPort- A user-defined (non-zero) integer value representing the local port on the client machine to use for this conversation. This local port number must be passed to TLS_CLIENT_CLOSE to close the conversation.<br>• hostname - The host name or IP address of the remote host.<br>• port - The connecting port on the remote host, usually port 443 for standard HTTPS connections.<br>• mode - 0: TLS_VALIDATE_CERTIFICATE (perform certificate validation), 1: TLS_IGNORE_CERTIFICATE_ERRORS (connect to the remote site while ignoring certificate errors or mismatches)<br>Returns:<br>This function returns 0 is all parameters are accepted, or a positive value indicating the offending parameter if there is an error.<br>Example:<br>`TLS_CLIENT_OPEN(5000, '192.168.0.1', 443, 0)` |

| NetLinx.axi - Library Calls (Cont.) | |
|---|---|
| **VALIDATE_NETLINX_ACCOUNT** | This function validates the specified user name and password against the NetLinx Master Controller's internal user account database. For the account to be valid the user name must exist with the matching password and the specified user account must have been set up with ICSP Authorization.<br>Syntax:<br>`sinteger VALIDATE_NETLINX_ACCOUNT(CHAR username[], CHAR password[],LAST_LOGIN_INFO info)`<br>Parameters:<br>username - A character array containing the user name to validate.<br>password - A character array containing the password to validate.<br>info - A return structure of type LAST_LOGIN_INFO.<br>Returns:<br>The following values are returned from the call:<br>0 - Valid user account.<br>-1 - Username invalid<br>-2 - Password invalid<br>-3 - Invalid user account<br>-4 - No authorization (Username/password are not authorized)<br>-5 - Invalid parameter<br>-6 - User account matching name is locked out<br>-7 - User account matching name has expired |
| **VALIDATE_NETLINX_ACCOUNT_ WITH_PERMISSION** | This function validates the specified user name and password against the NetLinx Master Controller's internal user account database. For the account to be valid the user name must exist with the matching password and the specified user account must have been set up with ICSP Authorization. This command includes parameters for authorization and permission types.<br>Syntax:<br>`sinteger VALIDATE_NETLINX_ACCOUNT_WITH_PERMISSION(CHAR username[], CHAR password[],CHAR type[], CHAR permission[], LAST_LOGIN_INFO info)`<br>Parameters:<br>username - A character array containing the user name to validate.<br>password - A character array containing the password to validate.<br>type - The authorization type.<br>permission - The permission type. Valid permissions include: Configuration, Console, Diags, EncryptICSP, FTP, HTTP, ICSP, Terminal, AuditLog, User1, User2, User3, and User4<br>info - A return structure of type LAST_LOGIN_INFO<br>Returns:<br>The following values are returned from the call:<br>0 - Valid user account.<br>-1 - Username parameter is not a valid string<br>-2 - Password parameter is not a valid string<br>-3 - Invalid user account<br>-4 - No authorization (Username/password are not authorized and/or permission is not authorized)<br>-5 - Third argument is not a LAST_LOGIN_INFO structure<br>-6 - User account matching name is locked out<br>-7 - User account matching name has expired |

# Terminal (Program Port/Telnet) Commands

## Overview

There are two types of terminal communications available on NetLinx Integrated Controllers:

- **Program Port** - The "Program" port is a Type-B USB port located on the Master that allows terminal communication with the Master. This type of terminal communication requires that you are physically connected to the Master to access the configuration options and commands supported. Since this method of terminal communication requires physical proximity as well as a physical connection to the Master, it is the most secure form of terminal communication.

  For this reason, all Security Configuration options are only available via the Program port (and cannot be accessed via Telnet).
- **Telnet** - This type of terminal communication can be accessed remotely, via TCP/IP. It is a less secure form of terminal communication, since it does not require a physical connection to the Master to connect. Further, the Telnet interface exposes information to the network (which could be intercepted by an unauthorized network client).

**NOTE:** *It is recommended that you make initial configurations as well as subsequent changes via the WebConsole. Refer to the On-Board WebConsole User Interface section on page 35.*

Refer to the *Terminal Commands* section on page 106 for a listing of all commands available in a terminal session.

Note that all commands in the table are available for both Program Port and Telnet sessions, with two exceptions: "Help Security" and "Resetadminpassword". These commands are only available via a Program Port connection.

## Establishing a Terminal Connection via the Program Port

To establish a terminal session via the Program Port, the USB port on your PC must be physically connected to the Program port on the NetLinx Master.

## Establishing a Terminal Connection via Telnet

1. In your Windows task bar, select **Start > Run** to open the Run dialog.
2. Type **cmd** in the *Open* field and click **OK** to open an instance of the Windows command interpreter (cmd.exe).
3. In the CMD (command), type "**telnet**" followed by a space and the Master’s IP address info.

   Example:

   ```
   >telnet XXX.XXX.XXX.XXX
   ```
4. Press *Enter*.
   - Unless Telnet security is enabled, a session will begin with a welcome banner:

     ```
     Welcome to NetLinx vX.XX.XXX, AMX LLC
     >
     ```
   - If Telnet security is enabled, type in the word **login** to be prompted for a Username and Password before gaining access to the Master.
5. Enter your username to be prompted for a password.
   - If the password is correct, you will see the welcome banner.
   - 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 you to try again.

     If after 5 prompts, the login information is not entered correctly, the following message will be displayed and the connection closed:

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

- To restrict access to the Master via terminal connection, enable Telnet/SSH on the Master via the Telnet/SSH option on the Security page - see the *Security Options Menu* section on page 126 for details). With Configuration Security enabled, a valid user with Configuration Security access will have to login before being able to execute Telnet commands. If security is not enabled, these commands are available to all.
- If a connection is opened, but a valid username / password combination is not entered (i.e. just sitting at a login prompt), the connection will be closed after one minute.

# Terminal Commands

The Terminal commands listed in the following table can be sent directly to the Master via either a Program Port or a Telnet terminal session (with the exception of the "*Help Security*" and "*Resetadminpassword*" commands, which are only available to a Program Port (RS232) connection.

In your terminal program, type "**Help**" or a question mark ("**?**") and <**Enter**> to access the Help Menu, and display the Program port commands described below:

**Terminal Commands**

| Command | Description |
|---|---|
| **----- Help ----- <D:P:S>** | (Extended diag messages are OFF)<br>`<D:P:S>`: Device:Port:System. If omitted, assumes Master. |
| **? or Help** | Displays this list of commands. |
| **ADD AUDIT SERVER [D:P:P]** | Adds a remote syslog server for audit messages.<br>- D: IP address or host name of the remote server<br>- P: Port number<br>- P: Protocol (UDP, TCP, or RELP)<br>Example:<br>`>ADD AUDIT SERVER REMOTESVR:514:UDP` |
| **AUTO LOCATE (ENABLE\|DISABLE\|STATUS)** | Enables/Disables/queries the auto locate feature on the Master.<br>Auto locate adds additional broadcast information for use by AMX Touch Panel devices configured in *Auto connect* mode. |
| **BOOT STATUS** | Returns the current boot state of the master.<br>Response is either "Boot in progress." or "Boot complete." |
| **CHANGE PASSWORD** | Change your password (requires login). |
| **CLEAR AUDIT** | Removes all locally-stored audit records.<br>See the *SHOW AUDIT LOG* command on page 117. |
| **CLEAR HTTPS REDIRECT** | Clears the HTTPS redirect flag.<br>See the *SET HTTPS REDIRECT* command on page 113. |
| **CLEAR MAX BUFFERS** | Reset the max buffers high-water counters to zero. |
| **CLEAR PERSISTENT VARS** | Clear out the persistent/non-volatile variable values without having to download a new NetLinx program. |
| **CPU USAGE** | Diagnostic tool to calculate a running average of the current CPU usage of the Master. |
| **DATE** | Displays the current date and day of the week.<br>Example:<br>`>DATE`<br>`10/31/2004 Wed` |
| **DATE/TIME ON\|OFF** | ENABLES/DISABLES the addition of a date time stamp to the terminal logs displayed via "`msg on`"<br>DATE/TIME is Off by default at the start of each Terminal/Telnet session. |
| **DEVICE DEBUG** | Turns the device side traffic debug messages on or off. |
| **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.<br>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.<br>When `DEVICE_HOLDOFF` is ON, you must use `ONLINE` events to trigger device startup `SEND_COMMAND`s.<br>By default, `DEVICE_HOLDOFF` is OFF to maintain compatibility with Axcess systems where devices are initialized in `DEFINE_START`.<br>**NOTE:** *This command sets the state of the device holdoff. The GET DEVICE HOLDOFF command reveals whether the state is On or Off (see page 107).*<br>Example:<br>`>Device Holdoff ON`<br>`Device Holdoff Set.` |
| **DEVICE STATUS <D:P:S>** | Displays a list of all active (on) channels for the specified D:P:S. |
| **DIPSWITCH** | Displays the current state of the Master's hardware dip switches. |
| **DISK FREE** | Displays the total bytes of free space available on the Master.<br>Example:<br>`>DISK FREE`<br>`The disk has 2441216 bytes of free space.` |

### Terminal Commands (Cont.)

| Command | Description |
|---|---|
| **DNS LIST <D:P:S>** | Displays the DNS configuration of a specific device including:<br>• Domain suffix·<br>• Configured DNS IP Information<br>Example:<br>`>DNS LIST [0:1:0]`<br>`  Domain suffix:amx.com`<br>`    The following DNS IPs are configured`<br>`    Entry 1-192.168.20.5`<br>`    Entry 2-12.18.110.8`<br>`    Entry 3-12.18.110.7` |
| **DOT1X (ENABLE\|DISABLE\|STATUS)** | Enables/disables wired 802.1x security or displays its current settings.<br>Syntax:<br>`DOT1X[status\|enable\|disable]` |
| **ECHO ON\|OFF** | Enables/Disables echo (display) of typed characters. |
| **EXPORT (CONFIG\|CLONE) TO USB (FRONT\|BACK)** | Exports a Master's configuration (config) or entire clone to USB media connected to the front or back of the Master.<br>Syntax:<br>`EXPORT [CONFIG\|CLONE] TO USB [FRONT\|BACK]`<br>The copy format of the configuration export includes:<br>• Auto-locate enable/disable<br>• Clock Manager settings<br>• Device Holdoff setting<br>• ICSP TCP timeout<br>• IP Device Discovery enable/disable<br>• LDAP settings<br>• Master-to-Master route mode<br>• Message log length<br>• Message thresholds for threads<br>• NDP enable/disable<br>• Queue sizes for threads<br>• Security configuration including the system, group, and user level settings<br>• Security profile<br>• Server port enable/disable for FTP, HTTP, HTTPS, ICSP, SSH, Telnet<br>• Server port numbers for FTP, HTTP, HTTPS, ICSP, SSH, Telnet<br>• SSL certificate parameters<br>• Startup log enable/disable<br>• UDP broadcast rate<br>• Zeroconfig enable/disable<br>The clone format of the configuration export includes all of the items from the copy format plus the following:<br>• DNS server names<br>• Domain name<br>• Duet memory allocation<br>• Hostname<br>• System number<br>• URL list<br>• NetLinx code<br>• Java code (Duet modules, XDD modules)<br>• All user files and folders, (includes .IRL files)<br>**NOTE:** *See IMPORT CONFIG.* |
| **EXPORT AUDIT to USB (FRONT\|BACK)** | Exports all locally stored audit files to USB media connected to the front or back of the Master.<br>Syntax:<br>`EXPORT AUDIT TO USB [FRONT\|BACK]` |
| **GET AUDIT STATUS** | Displays the log daemon status and the percentage of free disk space. |
| **GET DEVICE HOLDOFF** | Displays the state of the Master’s device holdoff setting.<br>**NOTE:** *This command reveals the state of the device holdoff set using the DEVICE HOLDOFF ON\|OFF command (see page 106).*<br>Example:<br>`>GET DEVICE HOLDOFF`<br>`  Device Holdoff is off.` |

| Terminal Commands (Cont.) | |
|---|---|
| **Command** | **Description** |
| **GET DEVICE TRAFFIC** | Gets diagnostic information about device side traffic.<br>Example:<br>`>get device traffic` |
| **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 ICSLAN** | Displays the current ICSLAN port settings. See the *Using the ICSLAN Network* section on page 122 for more information.<br>Example:<br>`>get icslan`<br>`   ICSLan Network: 198.18.0.0`<br>`   ICSLan Hostname: ICSLAN`<br>`   ICSLan Master IPv4 Address: 198.18.0.1`<br>`   ICSLan Master IPv6 Address: fe80::260:9fff:fe98:bd9e`<br>`   ICSLan DHCP Server is enabled`<br>`   ICSLan Dns Server is 198.18.0.1`<br>*Note: See SET ICSLAN*. |
| **GET IP <D:P:S>** | Displays the IP configuration of a device.<br>If you enter GET IP without the D:P:S variable, the Master displays its D:P:S, Host Name, Type (*DHCP* or *Static*), IP Address, Subnet Mask, Gateway IP, and MAC Address.<br>Example:<br>`>GET IP [0:1:50]`<br>`  IP Settings for 0:1:50`<br>`     HostName    MLK-INSTRUCTOR`<br>`     Type        DHCP`<br>`     IP Address  192.168.21.101`<br>`     Subnet Mask 255.255.255.0`<br>`     Gateway IP  192.168.21.2`<br>`     MAC Address 00:60:9f:90:0d:39` |
| **GET LEASES** | Displays the leases on the ICSLAN port. |
| **GET PLATFORM INFO** | Retrieves information about a Master connected via USB port. The command returns the master type, host name, system number, IPv4 address, IPv6 address, MAC address, and serial number in a single response.<br>Example:<br>`>get platform info`<br>`DESC=NX-3200;HOST=AMXM98BFB0;SYS=1;IP4=192.168.224.68;IP6=fe80::260:`<br>`9fff:fe98:bfb0;MAC=00:60:9f:98:bf:b0;SN='654321',0,0,0,0,0,0,0,0,0` |
| **HELP SECURITY** | Displays security related commands.<br>**NOTE:** *This command is only available to Program Port terminal sessions. It is not available to Telnet sessions (see the Overview* section on page 105*).*<br>Example:<br>`>HELP SECURITY`<br>`>logout   Logout and close secure session`<br>`>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. |
| **IMPORT CONFIG** | Installs a previously exported config or clone file. The command searches the USB media for config and clone .tar files and allows you to select which file to import. See *EXPORT (CONFIG\|CLONE) TO USB (FRONT\|BACK)*. |
| **IMPORT IRL** | Loads an IRL file from USB media onto the masters flash file system. The command searches the USB media for .irl files and allows you to select which IRL file to import. |
| **IMPORT KIT** | Installs a KIT file from USB media. The command searches the USB media for .kit files and allows you to select which KIT file to import. |
| **IMPORT TKN** | Installs a NetLinx token file from USB media. The command searches the USB media for .tkn files and allows you to select which .tkn file to import.<br>**NOTE:** *NOTE: This command does not install the zipped token file and its associated duet files. This command only works with the base token file (PROG.tkn).* |
| **IP STATUS** | Provides information about the current NetLinx IP Connections.<br>Example:<br>`>IP STATUS`<br>` NetLinx IP Connections`<br>` No active IP connections` |

| Terminal Commands (Cont.) | |
|---|---|
| **Command** | **Description** |
| **IPDD** | Provides information about the IP Device Discovery setting.<br>Example:<br>`>IPDD`<br>`IP Device Discovery has been ***ENABLED***.` |
| **JAVA SECURITY** | Provides information about the Java Security Manager setting.<br>Example:<br>`>JAVA SECURITY DISABLE`<br>`Java Security Manager has been ***DISABLED***. Reboot required.` |
| **LIST AUDIT FILES** | Displays the file names of all locally stored audit files. |
| **LIST AUDIT SERVERS** | Lists all remote syslog servers that receive audit messages. |
| **LOG FORMAT** | Sets the format of log messages for specific devices.<br>Example:<br>`>log format`<br>`Format Logging for which log device:`<br>`0) ALL (changes will apply to all devices)`<br>`1) BUFFER`<br>`2) STARTUP`<br>`3) SESSION`<br>`4) USB`<br>`5) CONSOLE`<br>`Enter selection or press return to exit without changes: 3`<br>`Setting Log format for SESSION`<br>`Print user-friendly date/timestamps in logs? (Y/N): Y  Y`<br>`Print Day of Week in logs? (Y/N): N`<br>`Print Clock Tick (ms since start) in logs? (Y/N): N`<br>`Print Thread IDs in logs? (Y/N): Y  Y`<br>`Log format for BUFFER: (ticks) log`<br>`Log format for STARTUP: timestamp (ticks) [threadId] (severity) log`<br>`Log format for SESSION: timestamp [threadId] log`<br>`Log format for USB: timestamp day (ticks) log`<br>`Log format for CONSOLE: timestamp (ticks) [threadId] (severity) log` |
| **MAIL RESET** | Resets the mail service. |
| **MAIL STATUS** | Displays the status of the configured mail server. |
| **MANAGE FIRMWARE** | Telnet interface to load previous and factory firmware versions for both master (device 0) and Integrated Device (device 5001)<br>Example:<br>`>manage firmware`<br>`Devices`<br>`-------`<br>`0 - Master`<br>`5001`<br>`Select device or press return to cancel:0`<br>`Current Version:  1.2.259`<br>`Previous Version: 1.2.258`<br>`Factory Version:  1.2.250`<br>`To install a firmware version:`<br>`Enter P (Previous), F (Factory) or press return to cancel:` |
| **MEM** | Displays the largest free block of the Master's memory.<br>Example:<br>`>MEM`<br>`The largest free block of memory is 11442776 bytes.` |

**Terminal Commands (Cont.)**

| Command | Description |
|---|---|
| **MSG ON\|OFF** | Enables/Disables extended diagnostic messages.<br>• MSG On [error\|warning\|info\|debug] sets the terminal program to display log messages generated by the Master. The level of log printed to the terminal window depends both on the level used when sending the message and the output level selected with "msg on."<br>For example if log output is enabled via "msg on warning" then logs produced at levels AMX_ERROR and AMX_WARNING will be displayed, but not logs produced at levels AMX_INFO or AMX_DEBUG.<br>The order of severity from highest to lowest is ERROR, WARNING, INFO, DEBUG.<br>If no severity is supplied with "msg on", the default setting is WARNING.<br>• MSG OFF disables the display.<br>Example:<br>`> MSG ON`<br>`  Extended diagnostic information messages turned on.`<br>`> MSG OFF`<br>`  Extended diagnostic information messages turned off.` |
| **MSG STATS** | Calculates incoming and outgoing messages over a time interval. |
| **NDP** | Provides information about the NetLinx Discovery Protocol (NDP) setting.<br>Example:<br>`>NDP`<br>`NDP beacon is ***ENABLED***.` |
| **NETLINX LOG LEVEL** | Configure the current setting for the NetLinx AMX_LOG facility.<br>Example:<br>`>netlinx log level`<br>`NetLinx Log Level is WARNING`<br>`  Set NetLinx Log level to :`<br>`    1) ERROR`<br>`    2) WARNING`<br>`    3) INFO`<br>`    4) DEBUG`<br>`      Enter selection or press return to keep current level:`<br>`>3`<br>`NetLinx Log Level set to INFO` |
| **OFF [D:P:S or NAME,CHAN]** | Turns off a specified channel on a device. The device can be on any system that the Master you are connected to is able to 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.<br>Syntax:<br>`OFF[name,channel]`<br>-or-<br>`OFF[D:P:S,channel]`<br>Example:<br>`>OFF[5001:7:4,1]`<br>` Sending Off[5001:7:4,1]` |
| **ON [D:P:S or NAME,CHAN]** | Turns on a specified channel on a device. The device can be on any system that the Master you are connected to is able to 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.<br>Syntax:<br>`ON[name,channel]`<br>-or-<br>`ON[D:P:S,channel]`<br>Example:<br>`>ON[5001:7:4,1]`<br>` Sending On[5001:7:4,1]` |

**Terminal Commands (Cont.)**

| Command | Description |
|---|---|
| **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 that the Master you are connected to is able to 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.<br>• Mode is exited by ++ ESC ESC.<br>• Display Format is set by ++ ESC n<br>Where n =<br>**A**, format = ASCII<br>**D**, format = Decimal<br>**H** = Hex<br>**NOTE:** *Refer to the ESC Pass Codes* section on page 122 *for detailed descriptions of the supported pass codes.*<br>Example:<br>`>pass[5001:7:4]`<br>` Entering pass mode.` |
| **PHYSICAL STATUS** | Retrieve the current LED states. |
| **PING [ADDRESS]** | Pings an address (IP or URL), to test network connectivity to and confirms the presence of another networked device. The syntax is just like the PING application in Windows or Linux.<br>Example:<br>`>ping 192.168.29.209`<br>` 192.168.29.209 is alive.` |
| **PROGRAM (ENABLE\|DISABLE\|STATUS)** | Enable/disable the NetLinx program or display the status of the current program execution setting. The PROGRAM command performs the same function as flipping dip switch 1 on the rear panel of the Master. The setting persists until it is manually changed. If the software setting is disabled OR dip switch 1 is "on" then the NetLinx program is disabled. The default setting is enabled.<br>Syntax:<br>`PROGRAM [status\|enable\|disable]` |
| **PROGRAM INFO** | Displays a list of program files and modules residing on the Master.<br>Example:<br>`>PROGRAM INFO`<br>` -- Program Name Info`<br>` -- Module Count = 1`<br>`      1   Name is i!-PCLinkPowerPointTest`<br><br>` -- File Names = 2`<br>`      1 = C:\Program Files\AMX Applications\i!-PCLinkPowerPoint`<br>`      2 = C:\Program Files\Common Files\AMXShare\AXIs\NetLinx.axi`<br>`      2 = Name is MDLPP`<br><br>` -- File Names = 2`<br>`      1 C:\AppDev\i!-PCLink-PowerPoint\i!-PCLinkPowerPointMod.axs`<br>`      2 C:\Program files\Common Files\AMXShare\AXIs\NetLinx.axi` |
| **PULSE [D:P:S or NAME,CHAN]** | Pulses a specified 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.<br>Example:<br>`>PULSE[50001:8:50,1]`<br>`Sending Pulse[50001:8:50,1]` |
| **PWD** | Displays the name of the current directory.<br>Example:<br>`pwd`<br>`      The current directory is doc:` |
| **REBOOT** | Reboots the Master or specified device. Options for rebooting the Master are cold, soft, and warm. The reboot command with no parameter executes as "reboot cold".<br>Example (Rebooting device):<br>`>REBOOT [0:1:0]`<br>` Rebooting...`<br>Example (Rebooting Master):<br>`>reboot cold`<br>Reboots the Master and restarts the entire operating system.<br>`>reboot warm`<br>`>reboot soft`<br>Reboots the Master but only starts the AMX NetLinx application firmware. |

**Terminal Commands (Cont.)**

| Command | Description |
|---|---|
| **REMOVE AUDIT SERVER [D:P:P]** | Removes a remote syslog server for audit messages.<br>- D: IP address or host name of the remote server<br>- P: Port number<br>- P: Protocol (UDP, TCP, or RELP)<br>Example:<br>`>REMOVE AUDIT SERVER REMOTESVR:514:UDP` |
| **RENEW DHCP** | Renews/Releases the current DHCP lease for the Master.<br>**NOTE:** *The Master must be rebooted to acquire a new DHCP lease.*<br>Example:<br>`>RENEW DHCP` |
| **REPORT FIRMWARE** | Calculates and displays checksums for stored firmware installation files. |
| **REPORT NETLINX** | Calculates and displays a checksum for the currently installed NetLinx code. |
| **RESETADMINPASSWORD** | This command resets the administrator password. The password is set to one of the following passwords depending on the Password Complexity setting:<br>• Low - password<br>• Medium - Amx1234!<br>• High - Amx1234!PasSword<br>**NOTE:** *This command is only available to Program Port terminal sessions. It is not available to Telnet sessions (see the Overview* section on page 105*).* |
| **RESET FACTORY** | Resets the Master to factory default state including removal of all security settings, removal of all user files, resetting to DHCP, and loading an empty NetLinx program. The Master will be effectively in an out-of-box state. |
| **ROUTE MODE DIRECT\|NORMAL** | Sets the Master-to-Master route mode:<br>• Normal mode - allows a Master to communicate with any Master accessible via the routing tables (shown with the `SHOW ROUTE` command - see page 120). This includes a directly-connected Master (route metric =1) and indirectly connected Masters (route metric greater than 1, but less than 16).<br>• Direct mode - allows communication only with Masters that are directly connected (route metric = 1). Indirectly connected Masters cannot be communicated within this mode.<br>Examples:<br>`>ROUTE MODE DIRECT`<br>`  Route Mode "Direct" Set`<br>`>ROUTE MODE NORMAL`<br>`  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 that 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.<br>The data of the string is entered with the following NetLinx string syntax:<br>`SEND_COMMAND 1:1:1,"'This is a test',13,10"`<br>`SEND_COMMAND RS232_1,"'This is a test',13,10"` |
| **SEND_LEVEL <D:P:S>, <LEVEL ID>,<LEVEL VALUE>** | Allows the user to set a level on a device via the Master's Telnet/program port interface. |
| **SEND_STRING D:P:S or NAME,STRING** | Sends a string to a specified device. The device can be on any system that the Master you are connected to can reach.<br>You can specify the device number, port, and system; or the name of the device defined in the `DEFINE_DEVICE` section of the Program.<br>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.<br>**NOTE:** *This command will not update clocks on devices connected to another Master (in Master-to-Master systems).*<br>Example:<br>`>SET DATE`<br>`  Enter Date: (mm/dd//yyyy) ->` |
| **SET DEVICE REBOOT** | Sets the fault response to an NI device side failure.<br>Example:<br>`>SET DEVICE REBOOT` |

<table>
<tr><th colspan="2">Terminal Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>SET DNS &lt;D:P:S&gt;</b></td><td>Sets up the DNS configuration of a device. This command 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.<br>Entering N (no) cancels the operation.<br><b>NOTE:</b> <i>The device must be rebooted to enable new settings.</i><br>Example:
<pre>
>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
</pre></td></tr>
<tr><td><b>SET DUET MEMORY</b></td><td>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.<br>Valid values are:<br>• 2 - 8 for 32MB systems<br>• 2 - 36 for 64MB systems.<br>This setting does not take effect until the next reboot.<br><b>NOTE:</b> <i>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.</i></td></tr>
<tr><td><b>SET FTP PORT</b></td><td>Enables/Disables the Master’s IP port listened to for FTP connections.<br><b>NOTE:</b> <i>The Master must be rebooted to enable new settings.</i><br>Example:
<pre>
>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.
</pre></td></tr>
<tr><td><b>SET HTTP PORT</b></td><td>Sets the Master’s IP port listened to for HTTP connections.<br><b>NOTE:</b> <i>The Master must be rebooted to enable new settings.</i><br>Example:
<pre>
>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 affect.
</pre></td></tr>
<tr><td><b>SET HTTPS PORT</b></td><td>Sets the Master’s IP port listened to for HTTPS connections.<br><b>NOTE:</b> <i>The Master must be rebooted to enable new settings.</i><br>Example:
<pre>
>SET HTTPS PORT
 Current HTTPS port number = 443
 Enter new HTTPS port number (Usually 443) (0=disable HTTPS):
</pre>
Once you enter a value and press the ENTER key, you get the following message:
<pre>
 Setting HTTPS port number to
 New HTTPS port number set, reboot the Master for the change to take affect.
</pre></td></tr>
<tr><td><b>SET HTTPS REDIRECT</b></td><td>Sets the HTTPS redirect flag. All HTTP requests will be redirected to HTTPS.<br>See the <i>CLEAR HTTPS REDIRECT</i> command on page 106.</td></tr>
</table>

| Terminal Commands (Cont.) | |
|---|---|
| **Command** | **Description** |
| **SET ICSLAN** | Sets the ICSLAN port settings.<br>Example:<br>`>set icslan`<br>`    --- Enter New Values or just hit Enter to keep current settings`<br>`    Enter ICSLan Host Name:    ICSLAN`<br>`    Enter ICSLan Network octet 1:    198`<br>`    Enter ICSLan Network octet 2:    18`<br>`    Disable DHCP Server? (Y):`<br>See the *Using the ICSLAN Network* section on page 122 for more information. |
| **SET ICSP PORT** | Sets the Master's IP port listened to for ICSP connections.<br>**NOTE:** *The Master must be rebooted to enable new settings.*<br>Example:<br>`>SET ICSP PORT`<br>`  Current ICSP port number = 1319`<br>`  Enter new ICSP port number (Usually 1319)`<br>`  (0=disable ICSP):`<br>Once you enter a value and press the ENTER key, you get the following message:<br>`   Setting ICSP port number to`<br>`   New ICSP port number set, reboot the Master for the change to`<br>`   take affect.` |
| **SET ICSP TCP TIMEOUT** | Sets the timeout period for ICSP and i!-Web Control TCP connections.<br>**NOTE:** *The new timeout value is immediately (no reboot required).*<br>Example:<br>`>SET ICSP TCP TIMEOUT`<br><br>`This will set the timeout for TCP connections for both ICSP and i!-Web`<br>`Control.When no communication has been detected for the specified number of`<br>`seconds, the socket connection is closed.ICSP and i!-Web Control have built-in`<br>`timeouts and reducing the TCP timeout below these will cause undesirable`<br>`results. The default value is 45 seconds.`<br><br>`The current ICSP TCP timeout is 45 seconds`<br>`Enter new timeout (in seconds):`<br>Once you enter a value and press the ENTER key, you get the following message:<br>`New timeout value set (in affect immediately).` |
| **SET IP <D:P:S>** | Sets the IP configuration of a specified device.<br>Enter a Host Name, Type (DHCP or Fixed), IP Address, Subnet Mask, and Gateway IP Address.<br>**NOTE:** *For NetLinx Central Controllers, the "Host Name" can only consist of alphanumeric characters.*<br>• Enter Y (yes) to approve/store the information into the Master.<br>• Enter N (no) to cancel the operation.<br>**NOTE:** *The Device must be rebooted to enable new settings.*<br>Example:<br>`>SET IP [0:1:0]`<br>` --- Enter New Values or just hit Enter to keep current settings ---`<br><br>` Enter Host Name:    MLK-INSTRUCTOR`<br>` Enter IP type. Type D for DHCP or S for Static IP and then Enter: DHCP`<br>` Enter Gateway IP:   192.168.21.2`<br><br>` You have entered: Host Name   MLK-INSTRUCTOR`<br>`                   Type        DHCP`<br>`                   Gateway IP  192.168.21.2`<br>` Is this correct? Type Y or N and Enter -> y`<br>` Settings written. Device must be rebooted to enable new settings.` |
| **SET LOCKOUT** | Sets the number of failed logins on a user account before the user account is locked.<br>Example:<br>`>SET LOCKOUT 10` |

**Terminal Commands (Cont.)**

| Command | Description |
|---|---|
| **SET LOG COUNT** | Sets the number of entries allowed in the message log.<br>**NOTE:** *The Master must be rebooted to enable new settings.*<br>Example:<br>`>SET LOG COUNT`<br>`  Current log count = 1000`<br>`  Enter new log count (between 50-10000):`<br>Once you enter a value and press the ENTER key, you get the following message:<br>`  Setting log count to`<br>`  New log count set, reboot the Master for the change to take affect.` |
| **SET NOTIFY THROTTLE** | Sets the Master-to-Master notification throttle level.<br>Example:<br>`>SET NOTIFY THROTTLE`<br>`  Current notification throttle level = 5`<br>`  Enter the master-to-master notification throttle level between 1 (low) and 10 (high):`<br>`  Notification throttle set to 5`<br>`  The system must be rebooted for the setting to take effect.` |
| **SET QUEUE SIZE** | Provides the capability to modify maximum message queue sizes for various threads.<br>Example:<br>`set queue size`<br>This will set the maximum message queue sizes for several threads.<br>Use caution when adjusting these values.<br>Set Queue Size Menu:<br>1. Interpreter (factory default=2000, currently=600)<br>2. Notification Manager (factory default=2000, currently=200)<br>3. Connection Manager (factory default=2000, currently=500)<br>4. Route Manager (factory default=400, currently=200)<br>5. Device Manager (factory default=500, currently=500)<br>6. Diagnostic Manager (factory default=500, currently=500)<br>7. TCP Transmit Threads (factory default=600, currently=200)<br>8. IP Connection Manager (factory default=800, currently=500)<br>9. Message Dispatcher (factory default=1000, currently=500)<br>10. Axlink Transmit (factory default=800, currently=200)<br>11. ICSP 232 Transmit (factory default=500, currently=500)<br>12. UDP Transmit (factory default=500, currently=500)<br>13. NX Device (factory default=500, currently=500)<br>Enter choice or press ESC. |
| **SET SNMP** | Sets SNMP read and write community strings. This command invokes the SET SNMP sub-menu:<br>`>SET SNMP`<br>`--- Enter New Values or just hit Enter to keep current settings`<br>`SNMP Enabled (Y or N)? N  y`<br>`Enter System Description:     NetLinx VxWorks SNMPv1/v2c Agent`<br>`Enter System Contact:         AMX LLC`<br>`Enter System Location:        Richardson, TX USA`<br>`Enter Read community string:  public`<br>`Enter Write community string: private`<br>You have entered:<br>`Description = NetLinx VxWorks SNMPv1/v2c Agent`<br>`Contact = AMX LLC`<br>`Location = Richardson, TX USA`<br>`Read Community = public`<br>`Write Community = private`<br>`Is this correct? Type Y or N and Enter->`<br>**NOTE:** *The "System Description", "System Contact" and "System Location" are the values that will be published for the Master via SNMP. The system must be rebooted once the new values are entered.* |

**Terminal Commands (Cont.)**

| Command | Description |
|---|---|
| **SET SSH PORT** | Sets the Master’s IP port listened to for SSH connections.<br>**NOTE:** *The Master must be rebooted to enable new settings.*<br>Example:<br>`>SET SSH PORT`<br>`  Current SSH port number = 22`<br>`  Enter new SSH port number (Usually 22) (0=disable SSH):`<br>Once you enter a value and press the ENTER key, you get the following message:<br>`Setting SSH port number to 22`<br>`New SSH port number set, reboot the Master for   the change to take effect.` |
| **SET SYSTEM NUMBER** | Sets the system number for this Master.<br>**NOTE:** *The Master must be rebooted to enable new settings.*<br>Example:<br>`>set system number`<br>`Current System number = 1`<br>`Enter new System number : 2`<br>`Setting System number to 2`<br>New System number set, reboot the master for the change to take effect. |
| **SET TELNET PORT** | Sets the Master’s IP port listened to for Telnet connections.<br>**NOTE:** *The Master must be rebooted to enable new settings.*<br>Example:<br>`>SET TELNET PORT`<br>` Current telnet port number = 23`<br>` Enter new telnet port number (Usually 23)`<br>` (0=disable Telnet):`<br>Once you enter a value and press the ENTER key, you get the following message:<br>`Setting telnet port number to 23`<br>`New telnet port number set, reboot the Master for the change to take effect.` |
| **SET THRESHOLD** | Sets the Master's internal message thresholds.<br>This command will set the thresholds of when particular tasks are pended. The threshold is the number of messages queued before a task is pended.<br>*Use extreme caution when adjusting these values.*<br>**NOTE:** *The Master must be rebooted to enable new settings.*<br>Example:<br>`>SET THRESHOLD`<br><br>`-- This will set the thresholds of when particular tasks are pended. The threshold is the number of messages queued before a task is pended.--`<br>`--Use extreme caution when adjusting these values.--`<br>`  Current Interpreter Threshold = 2000`<br>`  Enter new Interpreter Threshold (Between 1 and 2000)(Default=10):`<br>Once you enter a value and press the ENTER key, you get the following message:<br>`  Current Lontalk Threshold = 50`<br>`  Enter new Lontalk Threshold (Between 1 and 2000)`<br>`   (Default=50):50`<br>`  Current IP Threshold = 600`<br>`  Enter new IP Threshold (Between 1 and 2000)`<br>`  (Default=200): 600`<br>`  Setting Thresholds to: Interpreter 2000`<br>`                         Lontalk     50`<br>`                         IP          600`<br>`New thresholds set, reboot the Master for the changes to take effect.` |
| **SET TIME** | Sets the current time. 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.<br>**NOTE:** *This will not update clocks on devices connected to another Master (in Master-to-Master systems).*<br>Example:<br>`>SET TIME`<br>` Enter Date: (hh:mm:ss) ->` |
| **SET TIMELINE LOOPCNT** | Sets the Master's timeline/event max loopcount. |

**Terminal Commands (Cont.)**

| Command | Description |
|---|---|
| **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.<br>Example:<br>`>SET UPD BC RATE`<br>` Current broadcast message rate is 5 seconds between messages.`<br>`  Enter broadcast message rate in seconds between messages`<br>`  (off=0; default=5) (valid values 0-300):`<br>Once you enter a value and press the ENTER key, you get the following message:<br>`Setting broadcast message rate to 300 seconds between messages`<br>`New broadcast message rate set.` |
| **SET URL <D:P:S>** | Sets the initiated connection list URLs of a device. Enter the URL address and port number of another Master or device (that will be added to the URL list).<br>• Enter Y (yes) to approve/store the new addresses in the Master.<br>• Enter N (no) to cancel the operation.<br>Example:<br>`>SET URL [0:1:0]`<br>`     No URLs in the URL connection list`<br>` Type A and Enter to Add a URL or Enter to exit.`<br>`> a`<br><br>` Enter URL -> 192.168.21.200`<br>` Enter Port or hit Enter to accept default (1319) ->`<br>` Enter Type (Enter for permanent or T for temporary) ->`<br>`     URL Added successfully.` |
| **SHOW AUDIT [FILENAME]** | Displays the current day's audit record. Optionally, you can specify a file name to display previous audit logs. |
| **SHOW AUDIT LOG** | Displays the User Account Access Audit Log.<br>Example:<br>`SHOW AUDIT LOG`<br>`08-24-2009 06:54:04 <TERMINAL> administrator TERMINAL LOGIN_SUCCESS`<br>`08-24-2009 07:05:30 <TERMINAL> administrator TERMINAL LOGIN_SUCCESS`<br>`09-04-2009 09:21:09 <TERMINAL> administrator TERMINAL LOGIN_SUCCESS`<br>`09-04-2009 09:25:49 192.168.220.171 administrator HTTPS LOGIN_SUCCESS`<br>`09-04-2009 09:35:55 192.168.220.171 administrator HTTPS LOGOUT`<br>`09-08-2009 06:07:46 192.168.220.171 administrator SSH LOGIN_SUCCESS`<br>`09-08-2009 06:07:55 192.168.220.171 administrator SSH LOGOUT`<br>`09-08-2009 07:44:29 192.168.220.171 administrator HTTPS LOGIN_FAIL`<br>`09-08-2009 07:44:44 192.168.220.171 administrator HTTPS LOGIN_SUCCESS`<br>`09-08-2009 07:45:25 192.168.220.171 administrator HTTPS LOGOUT`<br>Each record displays:<br>• Date and time of access,<br>• Connection source consisting of either <TERMINAL> or the IP address of the user,<br>• Account username,<br>• Access transport mechanism (TERMINAL, HTTP, HTTPS, TELNET, SSH)<br>• Activity (LOGIN_SUCCESS, LOGIN_FAIL, LOGOUT).<br>**NOTE:** *Records older than 90 days will be automatically purged.*<br>The entire database of audit records can be purged manually from Telnet/SSH/terminal session using the "`CLEAR AUDIT LOG`" command (see page 106). |

<table>
<tr><th colspan="2">Terminal Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>SHOW BUFFERS</b></td><td>Displays a list of various message queues and the number of buffers in each queue<br>Example:
<pre>
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
Java Router         0
            ----   ----   ----
Total          0    0     0 GrandTotal 0
</pre>
<b>NOTE:</b> <i>See the SHOW MAX BUFFERS</i> section on page 119.</td></tr>
<tr><td><b>SHOW COMBINE</b></td><td>Displays a list of devices, levels, and channels that are currently combined.<br>Example:
<pre>
> 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])
</pre></td></tr>
<tr><td><b>SHOW DEVICE &lt;D:P:S&gt;</b></td><td>Displays a list of devices present on the bus, with their device attributes.<br>Example:
<pre>
>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
</pre></td></tr>
<tr><td><b>SHOW HTTPS REDIRECT</b></td><td>Displays the status of the HTTPS redirect flag.<br>See the <i>SET HTTPS REDIRECT</i> command on page 113.</td></tr>
</table>

## Terminal 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 [filename]
SHOW LOG ALL
```

- [start] specifies message to begin the display.
- 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
```

To display only the startup log, use the SHOW START LOG command (see page 120).

**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 the *SHOW BUFFERS* section on page 118.

**SHOW MEM**

Displays the memory usage for all memory types.

<table>
<thead>
<tr><th colspan="2">Terminal Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Description</th></tr>
</thead>
<tbody>
<tr>
<td><strong>SHOW NOTIFY</strong></td>
<td>

Displays the Notify Device List (Master-Master). This is a list of devices (up to 1000) that other systems have requested input from and the types of information needed.

**NOTE:** *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
```

</td>
</tr>
<tr>
<td><strong>SHOW REMOTE</strong></td>
<td>

Displays the Remote Device List (Master-Master). This is 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
```

</td>
</tr>
<tr>
<td><strong>SHOW ROUTE</strong></td>
<td>

Displays information about how this NetLinx Master is connected to other NetLinx Masters (routing information).

Example:

```
 >SHOW ROUTE
    Route Data:

    System Route  Metric  PhyAddress
    --------------------------------
   -> 50     50     0      AxLink
```

</td>
</tr>
<tr>
<td><strong>SHOW START LOG &lt;START&gt;</strong></td>
<td>

Displays the startup log (see START LOG below).

&lt;START&gt; specifies the message to begin the display.

'ALL' will display all startup log messages.

**NOTE:** *This command is identical in implementation to the SHOW LOG command (see page 119), except that it executes the startup log.*

</td>
</tr>
</tbody>
</table>

<table>
<tr><th colspan="2">Terminal Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Description</th></tr>
<tr><td><b>SHOW SYSTEM <S></b></td><td>Displays 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 <code>DEFINE_DEVICE</code> 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. <code>SHOW SYSTEM 2001</code>).<br>The systems listed are in numerical order.<br>Example:
<pre>
>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
</pre></td></tr>
<tr><td><b>SHOW TCP</b></td><td>Displays a list of active TCP/IP connections.<br>Example:
<pre>
>SHOW TCP
 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)
</pre></td></tr>
<tr><td><b>SHOW WATCHDOG</b></td><td>Displays the Watchdog Manager monitors.</td></tr>
<tr><td><b>START LOG (ON|OFF)</b></td><td>Enables and disables the collection of startup log messages. Once enabled, the first x number of logs will be retained at startup for subsequent review via the <i>SHOW START LOG <START></i> command. Use <i>SET LOG COUNT</i> (page 115) to set the number of log message that are retained.</td></tr>
<tr><td><b>TIME</b></td><td>Displays the current time on the Master.<br>Example:
<pre>
>TIME
 13:42:04
</pre></td></tr>
<tr><td><b>TOD ADJUSTMENTS</b></td><td>Displays the number of times the Linux system clock needed to be updated. The Linux system clock is compared to the hardware clock chip every hour, and if different, the Linux clock is updated with the correct time.</td></tr>
<tr><td><b>URL LIST <D:P:S></b></td><td>Displays the list of URL addresses programmed in the Master (or another system if specified).<br>Example:
<pre>
>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
</pre></td></tr>
<tr><td><b>USB LOG [front|back]<br>[enable|disable]</b></td><td>Directs the Master logs to a USB flash media file. The log files are named with the current date and time.<br>Syntax:
<pre>
USB LOG [front|back] [enable|disable]
</pre>
<b>NOTE:</b> <i>For safe removal of the USB drive, you must issue the command to disable USB LOG. Failure to do so may result in a message indicating "A fatal error has been detected by the Java Runtime Environment" if the Master is actively writing a log file to the USB device.</i></td></tr>
<tr><td><b>ZEROCONF<br>[ENABLE|DISABLE|STATUS]</b></td><td>Enable, disable or view the new Zeroconf client in the Master. When Zeroconf is enabled (default) the Master's web interface will be registered via Zeroconf and can be viewed through a Zeroconf browser plug-in such as Bonjour for IE.</td></tr>
</table>

## 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.<br>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.<br>Any ASCII characters received by the device will be displayed by their ASCII symbol.<br>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.<br>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.<br>Any characters received by the device will be displayed with a \ followed by two hex characters to indicate the characters hex value. |

## Using the ICSLAN Network

The default IP address for the ICSLAN network is 198.18.0.1 with a subnet mask of 255.255.0.0.

It is important that the ICSLAN and LAN subnets do not overlap. If the LAN port is configured such that its address space overlaps with the ICSLAN network, the ICSLAN network will be DISABLED.

### DHCP Server

The ICSLAN port has a built-in DHCP server. This DHCP server is enabled by default and will serve IP addresses to any connected devices set to DHCP mode.

The DHCP server can be disabled from telnet with the command:

```
SET ICSLAN
```

The DHCP address range is fixed. The server will provide addresses in the range x.x.0.2 through x.x.63.255.

Devices using static IP addresses on the ICSLAN network should be set within the reserved static IP address range of x.x.64.1 to x.x.255.255.

### Opening LAN and ICSLAN Sockets from Code

When opening sockets from NetLinx or Java code there is no mechanism to indicate which network to use. The controller will open the socket on whichever network has an IP subnet that matches the address provided in the command to open the socket. There is no indication which network was used, only whether the socket was created successfully.

# Accessing the Security Configuration Options

**Security configuration options are only available to Program Port connections** (see the *Overview* section on page 105).

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
set password complexity         Sets the password complexity: low, medium, high.
set password min age [age]      Sets the password min age.
set password max age [age]      Sets the password max age.
set password history [count]    Sets the number of historical passwords to compare against.
set lockout                     Set the password lockout settings
setup security                  Access the security setup menus
set security preset [level]     Set the security preset
```

**NOTE:** *The 'help security' and 'setup security' functions are only available via a direct Program Port connection. They are not available to Telnet sessions.*

**NOTE:** *You can set the security preset levels to low, medium, or high.*

2. Type **setup security** to access the *Setup 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 Device
 8) Edit device
 9) Delete device
 10) Show list of authorized devices
 11) Add role
 12) Edit role
 13) Delete role
 14) Show list of authorized roles
 15) Set Inactivity Timeout (minutes)
 16) Display Inactivity Timeout (minutes)
 17) Enter LDAP security information
 18) Test connection to the LDAP server
 19) Test an LDAP user
 20) Display LDAP security information
 21) Show active sessions/logins
 22) Backup Database
 23) Restore Database from backup
 24) Reset Database
 25) Display Database
Or <ENTER> to return to previous menu

Security Setup ->
```

3. The Setup 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** - **25**) at the prompt and press <Enter>.

Each option in the Setup Security menu displays a sub-menu specific to that option. The following subsections describe using each of the Setup Security menu options.

**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.*

## Setup Security Menu

The following table lists the options in the Setup Security menu:

| Setup Security Menu | |
|---|---|
| **Command** | **Description** |
| `1) Set system security options for NetLinx Master`<br>See the *Security Options Menu* section on page 126 for descriptions of each menu item. | This selection will bring up the Security Options Menu that allows you to change the security options for the NetLinx Master. These are "global" options that enable rights given to users and groups.<br>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.<br>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 name for the User you are adding. The user name must be a unique alpha-numeric string (4 - 20 characters).<br>**NOTE:** *User and Role names are case sensitive.*<br>After the user has been added, you will be taken to the *Edit User* menu to setup the new user’s privileges (see page 127). |
| `4) Edit user` | This selection will prompt you select a user whose properties you want to edit. Once you have selected the user you want to edit, you will access the *Edit User* menu so you can edit the user's privileges (see page 127). |
| `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 that are currently enrolled. |
| `7) Add device` | This selection will prompt you for a name for the device you are adding. The device name must be a unique alpha-numeric string (4 - 20 characters).<br>After the device has been added, you will be taken to the *Edit device* menu to setup the new users right (see page 128). |
| `8) Edit device` | This selection will prompt you select a device whose properties you want to edit. Once you have selected the device you want to edit, it will take you to the Edit Device Menu so you can edit the device’s rights (see page 128). |
| `9) Delete device` | This selection will prompt you select a device to delete. A device can only be deleted if there are no users assigned to that device. |
| `10) Show list of authorized devices` | This selection displays a list of devices that are currently enrolled. |
| `11) Add role` | This selection will prompt you for a name for the role you are adding. The role name must be a unique alpha-numeric string (4 - 20 characters).<br>**NOTE:** *User and Role names are case sensitive.*<br>After the role has been added, you will be taken to the *Edit Role* menu to setup the new users rights (see page 128). |
| `12) Edit role` | This selection will prompt you select a role whose properties you want to edit. Once you have selected the role you want to edit, it will take you to the Edit Role Menu so you can edit the role’s rights (see page 128). |
| `13) Delete role` | This selection will prompt you select a role to delete. A role can only be deleted if there are no users assigned to that role. |
| `14) Show list of authorized roles` | This selection displays a list of roles that are currently defined. |
| `15) Set Inactivity Timeout (minutes)` | This selection allows you to set a period of inactive time that must elapse before the Master can log out a user. You can set a timeout in the range of 1 to 60 minutes. The timeout applies to Program Port, Telnet, SSH, HTTP, and HTTPS sessions. |
| `16) Display Inactivity Timeout (minutes)` | This selection displays the time set for the inactivity timeout. |
| `17) Enter LDAP security information` | This selection prompts you to specify the LDAP URI. Once the URI is entered and enter is pressed, a prompt for the next LDAP parameter will be displayed, and so on until all LDAP parameters are entered.<br>**NOTE:** *Options 3 - 14 (Add user, Edit user, Delete user, Show the list of authorized users, Add device, Edit device, Delete device, Show list of authorized devices, Add role, Edit role, Delete role, Show list of authorized roles) on the Security Setup menu are disabled when LDAP is enabled.* |

| Setup Security Menu (Cont.) | |
|---|---|
| **Command** | **Description** |
| `18) Test connection to the LDAP server` | This selection prompts you for a user name and password to access an LDAP server. |
| `19) Test an LDAP user` | This selection attempts to access the LDAP server with a user name and password you provide. |
| `20) Display LDAP security information` | This selection displays the current LDAP server information. |
| `21) Show active sessions/logins` | This selection displays the users and administrators that are currently logged into the Master. |
| `22) Backup Database` | This selection creates a backup of the current local database. |
| `23) Restore Database from backup` | This selection restores the local database from the most recent backup. |
| `24) Reset Database` | 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.<br>This function is only visible to administrators. |
| `25) Display Database` | 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.<br>This function is only visible to administrators. |

## Enabling LDAP via the Program Port

1. Type setup security to access the Setup 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 device
 8) Edit device
 9) Delete device
 10) Show list of authorized devices
 11) Add role
 12) Edit role
 13) Delete role
 14) Show list of authorized roles
 15) Set Inactivity Timeout (minutes)
 16) Display Inactivity Timeout (minutes)
 17) Enter LDAP security information
 18) Test connection to the LDAP server
 19) Test an LDAP user
 20) Display LDAP security information
 21) Show active sessions/logins
 22) Backup Database
 23) Restore Database from backup
 24) Reset Database
 25) Display Database
 Or <ENTER> to return to previous menu

 Security Setup ->
```

2. To enable LDAP, enter **1** and press **Enter**. The following will be output to the screen:

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

3. To proceed, enter **y** and press **enter**. The following menu displays:

```
Select to change current security option
 1) Audit Log................................. Disabled
 2) Banner Disply............................. Disabled
 3) Inactivity Timeout........................ Disabled
 4) Failed Login Lockout...................... Disabled
 5) OCSP...................................... Disabled
 6) Password Expiration....................... Disabled
 7) Usb....................................... Enabled
 8) Auth on server port (telnet, ftp)......... Enabled
 9) Auth on ICSP Lan ......................... Disabled
10) Encryption on ICSP Lan ................... Disabled
11) Auth on ICSP-ICSLan ...................... Disabled
12) Encryption on ICSP-ICSLan ................ Disabled
13) HTTP Service.............................. Enabled
14) HTTPS Service............................. Enabled
15) Telnet Service............................ Enabled
16) SSH Service............................... Enabled
17) FTP Service............................... Enabled
18) SFTP Service.............................. Enabled
19) ICSP on WAN............................... Enabled
20) ICSP on ICSLan............................ Enabled
21) General Configuration Security............ Disabled
22) LDAP Security............................. Enabled
Or <ENTER> to return to previous menu
```

4. To enable LDAP Security, enter **21** and press **Enter**. The same menu will be sent to the screen with LDAP Security set to Enabled. Press enter to return to the Security Setup menu.
5. When back to the Security Setup menu, enter **17** and press **Enter**.

   A prompt to enter the LDAP URI will be displayed. Once you enter the URI is entered and press enter, a prompt for the next LDAP parameter appears.

   Continue entering the LDAP server parameters until all parameters are entered. The Security Setup menu displays again.
6. To test the connection to the server enter **18** and press **Enter**.

   This test performs a bind to the BIND DN using the Search Password entered. If the bind is successful, "**Connection successful**" appears on the screen. If the server could not be reached or the bind is unsuccessful, "**Could not connect to server**" appears on the screen.
7. Press **Enter** to return to the main menu.

**NOTE:** *Options 3 - 14 (Add user, Edit user, Delete user, Show the list of authorized users, Add device, Edit device, Delete device, Show list of authorized devices, Add role, Edit role, Delete role, Show list of authorized roles) on the Security Setup menu are disabled when LDAP is enabled.*

## Security Options Menu

Select "**Set system security options for NetLinx Master**" (option **1**) from the Setup Security Menu to access the *Security Options* menu, described in the following table:

**Security Options Menu**

| Command | Description |
|---|---|
| `1) Audit Log` | This selection enables/disables remote syslog. |
| `2) Banner Display` | This selection enables/disables banner messages. |
| `3) Inactivity Timeout` | This selection enables/disables whether the Master logs out a user after a defined period of inactivity. |
| `4) Failed Login Lockout` | This selection enables/disables whether the Master places a lock on a user account after a set number of failed logins. |
| `5) OCSP` | This selection enables/disables usage of the Online Certificate Status Protocol (OCSP) to validate received certificates before trusting the sending site. |
| `6) Password Expiration` | This selection enables/disables whether the Master forces a user to change its password after a set period of time. |
| `7) USB` | This selection enables/disables all Type-A USB connectors on the Master. |
| `8) Auth on server port (Telnet, FTP)` | This selection enables/disables whether the Master requires user name and password authentication on Telnet, Program, and HTTP/HTTPS ports. |
| `9) Auth on ICSP LAN` | This selection enables/disables whether the Master requires user name and password authentication on devices connected to the LAN ports on the Master. |
| `10) Encryption on ICSP LAN` | This selection enables/disables whether there is encryption on the LAN ports on the Master. |

| Security Options Menu (Cont.) | |
|---|---|
| **Command** | **Description** |
| `11) Auth on ICSP-ICSLAN` | This selection enables/disables whether the Master requires user name and password authentication on devices connected to the ICSLAN ports on the Master. |
| `12) Encryption on ICSP-ICSLAN` | This selection enables/disables whether there is encryption on the ICSLAN ports on the Master. |
| `13) HTTP Service` | This selection enables/disables HTTP access to the Master. |
| `14) HTTPS Service` | This selection enables/disables HTTPS access to the Master. |
| `15) Telnet Service` | This selection enables/disables Telnet access to the Master. |
| `16) SSH Service` | This selection enables/disables SSH access to the Master. |
| `17) FTP Service` | This selection enables/disables FTP access to the Master. |
| `18) SFTP Service` | This selection enables/disables SFTP access to the Master. |
| `19) ICSP on WAN` | This selection enables/disables ICSP on WAN ports. |
| `20) ICSP on ICSLAN` | This selection enables/disables ICSP on ICSLAN ports. |
| `21) General Configuration Security` | This selection enables/disables general configuration including access to WebControl for RMS and RPM Configuration and the following parameters:<br>• Auto-locate enable/disable<br>• Device Holdoff setting<br>• Duet memory allocation<br>• ICSP TCP timeout<br>• Master-to-master route mode<br>• Message log length<br>• Message thresholds for threads<br>• Queue sizes for threads<br>• UDP broadcast rate |
| `22) LDAP Security` | This selection enables/disables LDAP Security. Refer to *Appendix A: LDAP Implementation Details* on page 127 for details on LDAP Implementation. |

## Edit User Menu

The Edit User Menu is accessed whenever you enter the **Add user**, or **Edit user** selections from the Setup Security menu. The Edit User Menu options are described in the following table:

| Edit User Menu | |
|---|---|
| **Command** | **Description** |
| `1) Generate New Password` | This selection creates a new password for the user. Once the new password is entered, the user must use the new password from that point forward, or change the password. |
| `2) Rename User` | This selection enables you to change the user's name. |
| `3) Require Password Change On Next Login` | This selection enables you to toggle whether the user will be required to change its password the next time the user logs in to the Master. When this option is enabled, the words "already set" appear next to the option in the Edit menu. |
| `4) Change Role Membership` | This selection enables you to assign or remove a role from the user. Active roles for the user are marked with an asterisk (*). |
| `5) Display Role Membership` | This selection will display any roles assigned to the user. |
| `6) Lock/Unlock User` | This selection enables you to lock the user's account. When locked, the option changes to Unlock User. Select the option again to unlock the user's account. |

## Edit Device Menu

The Edit Device Menu is accessed whenever you enter the **Add device**, or **Edit device** selections from the Setup Security menu. The Edit Device Menu options are described in the following table:

| Edit Device Menu | |
|---|---|
| **Command** | **Description** |
| `1) Generate Device Password` | This selection prompts you to enter the new password (twice) for the user. Once you enter the new password, you must use the new password from that point forward. |
| `2) Change Role Membership` | This selection enables you to assign or remove a role from the device. Active roles for the device are marked with an asterisk (*). |
| `3) Display Role Membership` | This selection will display any roles assigned to the device. |
| `4) Lock/Unlock Device` | This selection enables you to lock the device's account. When locked, the option changes to Unlock Device. Select the option again to unlock the device's account. |
| `5) Rename` | This selection enables you to change the device's name. |

## Edit Role Menu

The Edit Role Menu is accessed whenever you enter the **Add role**, or **Edit role** selections from the Setup Security menu. The Edit Role Menu options are described in the following table:

| Edit Role Menu | |
|---|---|
| **Command** | **Description** |
| `1) Display Access Rights` | This selection will display the current Access Rights assigned to the role. |
| `2) Change Access Rights` | This selection will display any current directory associations assigned to the role, and then will prompt you to select the directory association you want to delete. |
| `3) Disable/Enable Role` | This selection allows you to disable the role so it cannot be assigned to a user or device. When disabled, the option changes to Enable Role. Select the option again to enable the role. |
| `4) Rename` | This selection enables you to change the role's name. |

## Access Rights Menu

The Access Rights Menu is accessed whenever you select **Change Access Rights** (option **2**) from the Edit Role menu. Active access rights for the role are marked with an asterisk (*). The options in this menu is described in the following table:

| Access Rights Menu | |
|---|---|
| **Option** | **Description** |
| `1) View Audit Log` | Select to allow the role to view and configure the audit log. |
| `2) Configuration Security` | Select to allow the role to modify general configuration including access to WebControl for RMS and RPM Configuration and the following parameters:<br>• Auto-locate enable/disable<br>• Device Holdoff setting<br>• Duet memory allocation<br>• ICSP TCP timeout<br>• Master-to-master route mode<br>• Message log length<br>• Message thresholds for threads<br>• Queue sizes for threads<br>• UDP broadcast rate<br>**NOTE:** *This permission also includes the right to reboot the Master after the configuration change. It does not include the right to reboot the Master outside of this context or to reboot any other devices.*<br>**NOTE:** *This permission is not required to view the information, only to change it.* |
| `3) Device Configuration` | Select to allow the role to modify the configuration of NetLinx and 3rd party devices including the following:<br>• System number<br>• Device number<br>• Duet/XDD module binding options<br>• IP Device Discovery enable/disable<br>• NDP enable/disable<br>• NetLinx device control/emulation<br>• URL list<br>• Integrated device settings<br>• Switcher device settings (DVX or DGX)<br>• Reboot<br>**NOTE:** *This permission is not required to view the information, only to change it.* |
| `4) Network Configuration` | Select to allow the role to modify network configuration including the following:<br>• Clock Manager settings<br>• DHCP/Static setting (Gateway IPv4 address, IPv4 address, IPv4 subnet mask (if static selected))<br>• DNS server addresses<br>• Domain name<br>• Hostname<br>• zeroconfig enable/disable<br>**NOTE:** *This permission also includes the right to reboot the Master after the configuration change. It does not include the right to reboot the Master outside of this context or to reboot any other devices.*<br>**NOTE:** *This permission is not required to view the information, only to change it.* |
| `5) Telnet/SSH` | Select to allow the role to have Telnet and SSH access. |
| `6) FTP/SFTP Access` | Select to allow the role to have FTP and SFTP access. |
| `7) HTTP` | Select to allow the role to have HTTP and HTTPS access. |
| `8) Program Port/RS232` | Select to allow the role to have terminal access via the Program Port. |

**Access Rights Menu (Cont.)**

| Option | Description |
|---|---|
| `9) Security Control` | Select to allow the role to view and configure security including the following:<br>- Security settings<br>- Certificate policy (trusted CAs, etc.) and management (upload, delete)<br>- LDAP server settings<br>- Role settings<br>**NOTE:** *This permission also includes the right to reboot the Master after the configuration change. It does not include the right to reboot the Master outside of this context or to reboot any other devices.*<br>**NOTE:** *This permission is not required to view the information, only to change it.* |
| `10) Software Update` | Select to allow the role to update firmware and software.<br>**NOTE:** *This permission also includes the right to reboot the Master after the update. It does not include the right to reboot the Master outside of this context or to reboot any other devices.* |
| `11) User Management` | Select to allow the role to view, create, modify, lock, and remove user accounts.<br>**NOTE:** *A user has the ability to change its own password, regardless of whether it has the User Management permission.* |
| `12-15) User Access 1-4` | Select to allow the role access generic access permissions. These privileges are to be used by NetLinx programs. |
| `16) TPAdmin` | Select to allow the Master to access a touch panel's settings page. |
| `17) Remote UI` | Select to allow the Master to access Web controls for remote user interfaces, such as Virtual Touch Panel or Virtual Keypad. |

### Adding a Role

1. Type **11** and **<Enter>** at the Security Setup prompt (at the bottom of the Main Security Menu) to add a new role. A sample session response is:

```
The following groups are currently defined:
   All_Permissions
   Studio
   User
Enter name of new role:
```

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 Edit Group menu.

## 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
Role:                   All_Permissions
Directory Association: /*

Account 2:              User Name: NetLinx
Password:               password
Role:                   Studio
Directory Association: none

Role 1:                Group: All_Permissions
Rights:                 All
Directory Association: /*

Role 2:                Role: Studio
Rights:                 Device Management, Firmware Update, Network Management, Security Control
Directory Association: /*

Security Options:       USB enabled
                        Auth on server port (telnet, ftp) enabled
                        HTTP/HTTPS Services enabled
                        Telnet/SSH Services enabled
                        FTP/SFTP Services enabled
                        ICSP on WAN/ICSLAN enabled
                        All other options disabled
```

## Telnet Diagnostics Commands

The following Telnet Diagnostics Commands provide visibility to remote Masters, in order to determine the current state of operations, and are provided as diagnostic/troubleshooting tools.

While these commands are available for any user to execute, their output is interpretable primarily by an AMX Technical Support Engineer.

**Telnet Diagnostics Commands**

| Command | Description |
|---|---|
| **PHYSICAL STATUS** | This command reports the current state of the Master's Status, Output and Input LEDs, in order to troubleshoot a remote Master. For example, if PHYSICAL STATUS indicates that the Input LED always shows '1' (or ON), it could indicate that the Master is being hammered by incoming events. |
| **MSG STATS** | This command collects messages statistics for the Interpreter over a 10 second period by calculating the number of event messages that have been processed. This can be useful as a debugging/diagnostics tool to determine if the NetLinx Interpreter is running and how many messages it's processing. |

## Logging Out of a Terminal Session

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

## 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.

# Appendix A: LDAP Implementation Details

## Overview

The process of verifying credentials and obtaining user authorization is designed to support most organizations requirements for 'least privilege'. The account used to search LDAP to provide user objects for authentication never needs access to user information. Authorization lookups are performed as the authenticated user and as such, no elevated permission is required.

## Changes to LDAP Implementation (v1.4.x)

There are numerous changes to LDAP configuration when you upgrade your Master’s firmware to version 1.4.x or higher. Upgrading from version 1.3.x to 1.4.x may require you to make changes to the configuration on your LDAP server.

- When a remote directory service is enabled, the Master maps a user’s group memberships in the LDAP database to a locally-defined Role. A Role is a set of privileges or permissions assigned to one or more users. See the *Security - Roles* section on page 48 for more information.
- The common name of the LDAP group on the LDAP server must match the name of the Role assigned to the user on the Master.
- ICSP permission is granted for Device-type users, and only when the user is granted the Firmware/Software Update permission. See the *Role Permissions* section on page 49 for more information.
- Device authentication is no longer checked against the remote LDAP server. All device authentication is performed locally.
- Several changes to Active Directory and OpenLDAP configurations. See the *Active Directory/OpenLDAP Setup* section below for more details.

### Active Directory/OpenLDAP Setup

Unix Identity Module on Active Directory or OpenLDAP must use posixAccount for user and group memberships. For OpenLDAP, you can add posixAccount to each entry that requires SSH/SFTP authentication. inetOrgPerson will continue to work for FTP/HTTP/HTTPS/Program Port authentication.

When adding posixAccount to an existing entry, you may be asked for a uidNumber. This number must be unique for each user, however, the actual value does not matter to the NX-controller. When creating the attributes, consider the following rules:

- uidNumber must be unique (often enforced by the server.)
- homeDirectory can be anything (typically it is */home/<cn>*, but you can also use */bin/false* or */opt/amx/user.*)

The following table provides sample LDIF files:

| Sample LDIF Files | |
|---|---|
| *Example*:<br>**dn**: cn=admin,dc=smith,dc=local<br>**objectClass**: simpleSecurityObject<br>**objectClass**: organizationalRole<br>**cn**: admin<br>**description**: LDAP administrator | *Example*:<br>**dn**: ou=users,dc=smith,dc=local<br>**objectClass**: organizationalUnit<br>**objectClass**: top<br>**ou**: users |
| *Example*:<br>**dn**: uid=olUser,ou=users,dc=smith,dc=local<br>**cn**: user<br>**uid**: olUser<br>**objectClass**: posixAccount<br>**objectClass**: inetOrgPerson<br>**objectClass**: top<br>**uidNumber**: 5001<br>**gidNumber**: 5001<br>**homeDirectory**: /home/olUser<br>**sn**: olUser | *Example*:<br>**dn**: uid=olAdmin,ou=users,dc=smith,dc=local<br>**cn**: olAdmin<br>**uid**: olAdmin<br>**objectClass**: posixAccount<br>**objectClass**: inetOrgPerson<br>**objectClass**: top<br>**uidNumber**: 5000<br>**homeDirectory**: /home/olAdmin<br>**sn**: admin<br>**gidNumber**: 5000 |

## Assumptions and Prerequisites

Assumptions made about the LDAP implementation or environment in which the AMX client will participate include:

1. Must support simple authentication (for example, NetLinx Masters do not support *Kerberos* or *SASL*).
2. The account setup for a bind DN must have search capability along with the necessary permissions to read the 'uid', 'cn', 'member' and 'objectclass' attributes.
3. When a search is performed to find a DN with the specified user ID, a search must return one and only one object if the user exists. No object will be returned if an account does not exist for that user ID.
4. An account is considered valid if a user can authenticate/bind. No other attributes are considered during the authentication process.
5. AMX LDAP implementation supports both encrypted and un-encrypted connections using SSL.
6. When a person authenticates, that account must have access to all the attributes defined by RFC 2798 with the following exception:

   User passwords are not necessarily accessible for anything except to perform a bind to the directory (for example, this attribute may not be directly available to the user).
7. The bind DN must have the ability to search for group membership. (This ability is similar to RMS requirements.)
8. When a person authenticates, that account must have access to "cn" attributes for all groups of which it is a member.
9. Group membership for users is defined by the Role assigned to the user. Use *GroupOfNames* as the objectClass for group mapping. *GroupOfUniqueNames* is not supported due to ambiguities associated with implementations which use unique IDs appended to membership DNs.
10. When performing searches for group membership, no restrictions exist which would the restrict returning the full list of objects for which the user is a member with the possible exception of reasonable response timeouts. AMX LDAP implementation does not support paged search results.
11. AMX LDAP implementation does not support following referrals.

**IMPORTANT:** *For the NX-series Masters to work with LDAP over SSL (LDAPS), you must upload a CA server certificate in .pem format to the Master's FTP server. The certificate's file name must be "ldap_ad.pem". You can attach the file to your NetLinx Studio project and upload the file to the ../8021x directory (the default directory for .pem files.) Once the file is uploaded, you must reboot the Master for the certificate file to be read and employed by the system. LDAPS requires Master Firmware version 1.3.78 or greater.*

# Example - Setting Up User's Access Rights

To give AMX equipment users access rights to the Master, group memberships for administrators and users are defined by the *Role Name* setting when establishing Roles (see the *Security - Roles* section on page 48 for more information.) Two records need to be created in the database:

- One that represents users with administrative privileges (Program Port Access, FTP Access, HTTP Access, Telnet Access, General and Network Configuration, Firmware Updates, and Security Control). The factory default settings include an *administrator* user which includes all administrative privileges.
- Another that represents users with user privileges. The factory default settings include a *netlinx* user which includes Device Management, Firmware Update, Network Management, and Security Control privileges.

**NOTE:** *You can create as many groups as necessary according to your policies, but you should create at least two groups to separate administrators from other users.*

**IMPORTANT:** *The common name of the LDAP group on the server must match the name of the Role assigned to the user on the Master.*

## Administrator Access Example

| Administrator Access | |
|---|---|
| **LDAP Server Configuration** | **Master Configuration** |
| *Example*:<br>**dn**: cn=administrator,ou=groups,ou=Dallas, dc=example,dc=com<br>**objectClass**: groupOfNames<br>**objectClass**: top<br>**cn**: All_Permissions<br>**member**: uid=DallasAdminUser1,ou=people, ou=Dallas,dc=example,dc=com<br>**member**: uid=ICSPUser,ou=people, ou=Dallas,dc=example,dc=com | On the *Role Security Details* page, create a Role with the Administrator groupOfNames cn, or use the existing administrator role.<br>*Example*:<br>**Role Name**: All_Permissions |

## User Access Example

| User Access | |
|---|---|
| **LDAP Server Configuration** | **Master Configuration** |
| *Example*:<br>**dn**: cn=master01User,ou=groups, ou=Dallas,dc=example,dc=com<br>**objectClass**: groupOfNames<br>**objectClass**: top<br>**cn**: Studio<br>**member**: uid=DallasUser1,ou=people, ou=Dallas,dc=example,dc=com<br>**member**: uid=DallasUser2,ou=people, ou=Dallas,dc=example,dc=com | On the *Role Security Details* page, create a Role with a name which matches the groupOfNames cn.<br>*Example*:<br>**Role Name**: Studio |

**NOTE:** *If the DN of a user is in both the administrator groupOfNames and the user groupOfNames, the administrative privileges take precedence over user privileges.*

# Appendix B: Certificates

## Overview

In any security scenario, it is important that the private key is protected. If the private key is compromised, the entire security chain breaks down and is subject to decryption by outside parties. The following table lists certificates supported by NX Masters:

**Supported Certificates**

| **Certificate Type** | **Format** | **Function** |
|---|---|---|
| Trusted CA | PEM | A list of trusted Certificate Authorities (CAs) for verifying secure connections include Secure-ICSP (ICSPS), TLS_CLIENT_OPEN, Audit Log, and LDAPS. For Secure ICSP connections, this only works when the NX Master is used as a client (contains an entry in the URL list). An audit log trusted CA must be specified when configuring remote logging. The primary usage for Trusted CAs is to enable validation of remote sites based on the site certificate. |
| CRL (Certificate Revocation List) | PEM | A list of compromised certificates that should no longer be trusted. The primary usage of CRLs is to prevent a secure connection to a remote site. Since CAs must be loaded manually, this type should be rarely needed for a well-defined system that does not connect to random sites. |
| Device Certificate and Private Key | PEM | A certificate and private key (must be generated together) used in Secure ICSPS connections. The primary use of custom device certificates and private keys is to conform to unique site-specific certificate/security policies.<br>**NOTE:** *These must be added in pairs to work. The key has no use without the public certificate, and vice versa.* |
| NetLinx/SSH Private Key | SSH-Private Key | A private key (generated by SSH-keygen) to connect to a remote system using passwordless/PKI authorization. This is NOT an X.509 certificate, but the X.509-like/ SSH custom form used by most SSH client/servers. The primary reason for SSH private key usage is to connect to a remote server without a plain-text password in the NetLinx program. |
| 802.1x Certificate | PEM | Used by the upstream switch/RADIUS server for network authorization. |
| Audit Log Certificate and Private Key | PEM | A certificate and private key used for authorization on the Remote Syslog server. This certificate is used only when the audit log is sending data to a remote server. The primary reason for audit log certificates is to encrypt the logging connection to the Remote Syslog server.<br>**NOTE:** *These must be added in pairs to work. The key has no use without the public certificate, and vice versa.* |
| HTTPS KeyStore | JKS (Java KeyStore/ Keytool) | The default HTTPS store is auto-generated at the first boot. A user KeyStore should include the private key, the device certificate as well as the signer's certificate. The primary reason for updating the HTTPS KeyStore is to prevent the security exception warning when connecting to the NX over HTTPS. |
| Duet TrustStore | JKS (Java KeyStore/ Keytool) | The Duet TrustStore is the default shipped with Java. If additional CAs are required, they should be added to the original. A user-provided Duet TrustStore is NOT in addition to a system TrustStore. The primary reason for doing this is to add a self-signed/internally signed CA for a server to enable HTTPS connections to RMS. |

**NOTE:** *Existing secure sites coming from 1.4 using LDAPS should continue to work for user authentication. However, in NetLinx Studio, the Certificate Manager may show an LDAP CA as an 802.1x certificate. This is due to previous versions of Studio sending .pem files to the 8021x directory. It is recommended that the LDAP CA be removed from the 802.1x type, and re-sent to the NX as a Trusted CA type.*

**NOTE:** *Existing installations that used basic FTP and installed the LDAP CA in user/certs will NOT show up in the Certificate Manager. However, auth will still be available for most access.*

**NOTE:** *For LDAPS connections, specifically FTP/SSH, the CA must be in the Trusted CA store otherwise the NX will authorize, but FTP/ SSH will fail. This is not required for instances where the Controller authorizes the activity (HTTP, ICSP).*

## Creating an HTTPS KeyStore

Java Keytool is a key and certificate management utility provided by the Java SDK. Java Keytool allows users to manage their own public and private key pairs and certificates and to cache certificates. Java Keytool stores the keys and certificates in a KeyStore. By default, the Java KeyStore is implemented as a file. To create an HTTPS KeyStore, you are required to install Java SDK on the host system. You do not create certificates on the NX Master. Certificates are created on a PC then transferred to an NX Master via NetLinx Studio.

The following steps are required to create an HTTPS KeyStore.

### Step 1: Create the private key

Use the following commands to create the private key:

```
keytool -genkeypair -keyalg RSA \
-validity 365 -keystore amxcert -keysize 2048 \
-storepass amxcertpassword -keypass amxcertpassword \
-dname CN=hostname,OU=Harman,O=Amx,L=Richardson,S=Tx,C=US
```

### Step 2: Generate a CSR request

Use the following command to generate a CSR request:

```
keytool -certreq -keystore amxcert -file master.csr -storepass amxcertpassword
```

### Step 3: Send the *master.csr* file to the CA to have it signed.

**IMPORTANT:** *Typically, this step is performed by the CA service. Normally, you will NOT perform this step unless you acting as the CA.*

This process will vary with each registrar. If signing locally, the command should look similar to the following line:

```
openssl x509 -req -in master.csr -CA CA.crt -CAkey CA.key -CAserial ./CA.srl -out master.crt -days 10240
```

### Step 4: Import the newly signed certificate into the KeyStore

Use the following commands to import the newly signed certificate into the KeyStore:

```
keytool -keystore amxcert -alias CA -import  -file CA.crt -trustcacerts
keytool -keystore amxcert -import  -file master.crt -trustcacerts
```

### Step 5: Upload amxcert to the NX as HTTPS KeyStore and reboot the NX

When connecting to HTTPS, the certificate information should reflect the new certificate information.

# Creating & Installing Self-Signed HTTPS KeyStore

A self-signed KeyStore is simply a certificate signed by itself.

## Generating a Self-Signed KeyStore

Use the following command to generate a self-signed KeyStore:

```
 keytool -genkey -keyalg RSA -validity 365 -keystore amxcert -keysize 2048 \
         -storepass amxcertpassword -keypass amxcertpassword \
         -dname CN=hostname,OU=Harman,O=Amx,L=Richardson,S=Tx,C=US
```

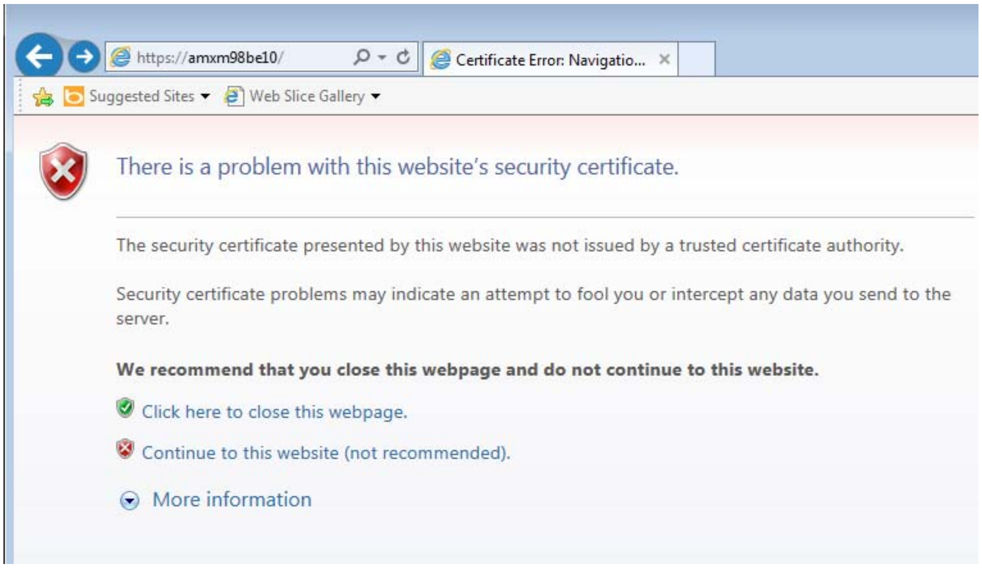
**NOTE:** *The hostname should either be the IP, or the DNS hostname.*

**NOTE:** *Keystore, storepass, and keypass are all fixed values and must not be changed.*

## Installing a Self-Signed KeyStore

Perform these steps to install a self-signed HTTPS KeyStore:

1. Transfer the certificate to the NX Master and reboot the Master.
2. Navigate to *https://hostname*. You should see the unknown certificate authority message (FIG. 61).



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

**We recommend that you close this webpage and do not continue to this website.**

Click here to close this webpage.

Continue to this website (not recommended).

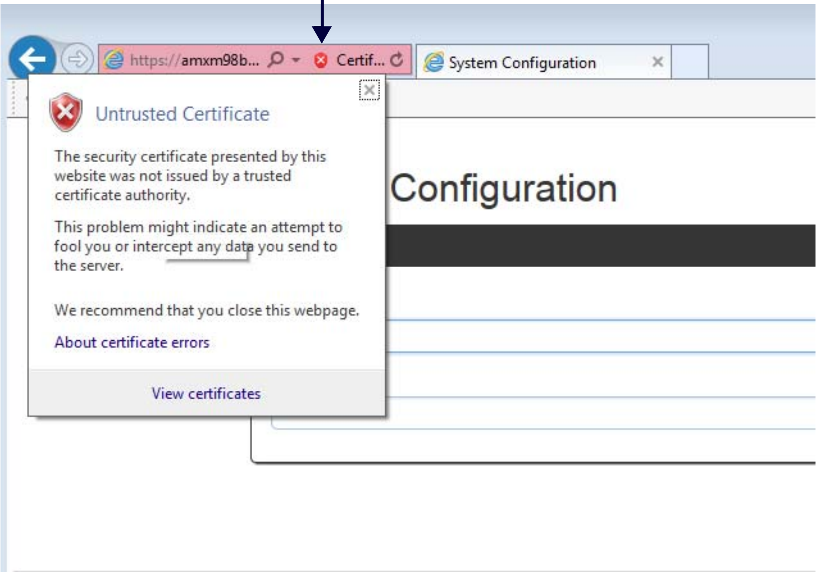
More information

**FIG. 61** Unknown Certificate Authority Message

3. Click **Continue to this website**.

4. When the website appears, click the red X in the address bar (FIG. 62). An Untrusted Certificate pop-up message will appear.

Click to access pop-up screen



Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

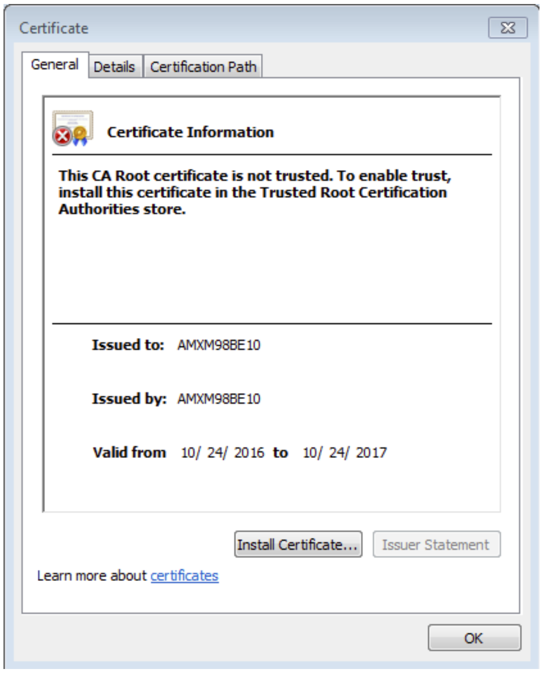
This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

FIG. 62 Untrusted Certificate pop-up message

5. Click **View Certificates** in the pop-up. The certificate information for the self-signed certificate on the NX appears (FIG. 63).



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: AMXM98BE10

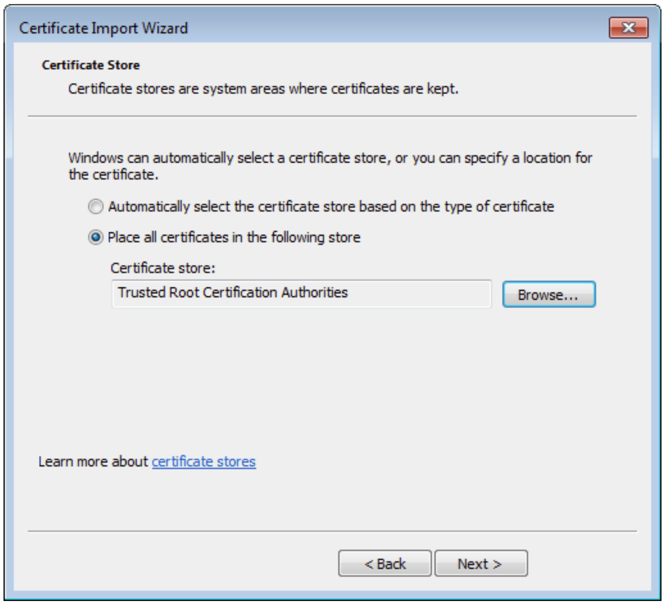
Issued by: AMXM98BE10

Valid from 10/ 24/ 2016 to 10/ 24/ 2017

Learn more about certificates

FIG. 63 Certificate dialog

6. Click **Install Certificate**. The Certificate Import Wizard opens. Click **Next** to access the Certificate Store page (FIG. 64).



Certificate Import Wizard

**Certificate Store**

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

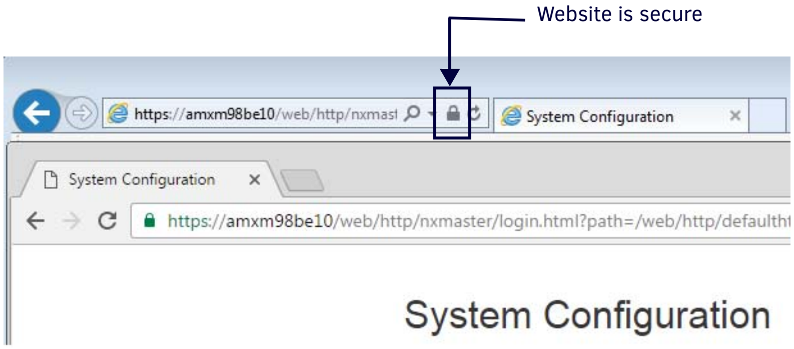
Certificate store:

Trusted Root Certification Authorities

Learn more about certificate stores

**FIG. 64** Certificate Import Wizard - Certificate Store

7. Select **Place all certificates in the following store**, and click **Browse**. Select **Trusted Root Certification Authorities** from the list that appears, and click **OK**.
8. Click **Next**, then verify the information is correct before clicking **Finish**. The certificate is installed.
9. Restart the browser or open a new browser, and navigate to the hostname of the Master. You should see a secure lock symbol in the address bar (FIG. 65).



Website is secure

https://amxm98be10/web/http/nxmast

https://amxm98be10/web/http/nxmaster/login.html?path=/web/http/defaultht

**FIG. 65** Secure Website

## Creating/Updating the Duet TrustStore

The Duet TrustStore is the trusted CA repository for the Duet/Java environment. The default TLS factory in Java references the Duet TrustStore to verify certificates of remote servers. Additional CAs can be installed to the Duet TrustStore to connect to servers signed with a private/internal certificate or signed by a CA not trusted by the default JVM installation. The following instructions describe how to update the Duet TrustStore. Updating the Duet TrustStore requires that a Java JDK/Keytool is installed on the host system.

The default password for the TrustStore is *changeit*. You can change the password, but it is not necessary to do so. The primary reason for making changes to the Duet TrustStore is so you can connect to an RMS server with a self-signed/internal signed certificate via HTTPS.

Before updating the Duet TrustStore, you must download the Duet TrustStore via the Certificate Manager in NetLinx Studio. See the *NetLinx Studio Instruction Manual* or the consult the NetLinx Studio online help for more information.

Using the Keytool, enter the following:

```
keytool -import -v -trustcacerts -alias myCa -file myCA.crt  -keystore cacerts -keypass changeit
```

- cacerts is the name of the Duet TrustStore downloaded from the NX
- myCa is a unique alias for the CA
- myCA.crt is the certificate for the CA

## Acquiring/Installing Public Certificates

TLS connections to remote servers may require certificates to be uploaded to the NX Master if certificate validation is used. The connections also requires accurate date/time information. Perform the following steps to connect to google.com via TLS_CLIENT_OPEN with certificate validation (This procedure provides instructions for Internet Explorer.)

1. Enter *https://www.google.com* in the address bar of the web browser.
2. Click the lock on the right hand side of the address bar (FIG. 66).

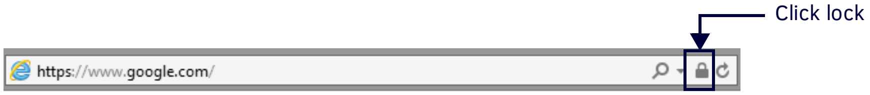
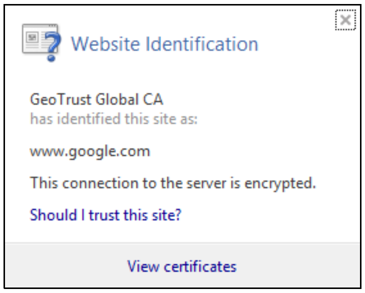


**FIG. 66** Click lock in address bar

3. The Website Identification pop-up opens (FIG. 67). Click **View Certificates**.



Website Identification

GeoTrust Global CA
has identified this site as:

www.google.com

This connection to the server is encrypted.

Should I trust this site?

View certificates

**FIG. 67** Website Identification pop-up

4. The Certificate dialog opens. Select the **Certification Path** tab.
5. Perform the following steps for every certificate in the path above the site to which you connected (in this case, Google Internet Authority G2 and GeoTrust Global CA):
   - Click **View Certificate**.
   - Select the **Details** tab.
   - Click **Copy to File**.
   - Click **Next**.
   - Select **Base-64 encoded X.509 (.cer)**.
   - Choose a file name. It should be similar to the subject name of the certificate. In the first case, choose *google.internet.auth.g2.cer.*
   - Click **OK**.
   - Repeat for each certificate
   - Upload each certificate as a Trusted CA.

# Appendix C: SMTP Support

## Overview

NetLinx Integrated Controllers (Masters) have built-in support for transmission or email via an SMTP server. NetLinx Master support includes the configuration of a single outbound SMTP server and the subsequent transmission of individual emails via the configured server.

## SMTP Server Configuration

The SMTP Server is configured by specifying a set of server properties. SMTP server properties once set are persistent on the master until they are reset to a different value. SMTP server properties include the server IP address or URL, the SMTP IP port number for connecting to the server, any username and password that is required for connecting with the server, the "from" address that will be associated with all outgoing messages and finally a flag indicating if the server must support TLS authentication security in order to establish a connection. Properties are set and read using two built-in NetLinx functions:

```
SMTP_SERVER_CONFIG_SET(CONSTANT CHAR cfgName[], CONSTANT CHAR cfgValue[])
```

Sets a server configuration parameter.   These configuration settings are general mail server settings and thus apply to all emails. Settings are saved to the configuration database & thus are static upon reboot.

*cfgName* is the server property name that is being set. Acceptable values are

- *ADDRESS* - SMTP server name, such as "mail.amx.com". The maximum number of characters allowed for email destination is 127.
- *PORT* - SMTP server port, such as "25" or "0". 0 means "use the best default port" which would imply using 25 which is the SMTP well-known port.
- *USERNAME* - User name to offer for authentication. If user name length is set to 0, authentication is not attempted.
- *PASSWORD* - Password to offer for authentication. If password length is set to 0, authentication is still attempted but simply uses a zero-length password.
- *FROM* - Mail address to populate to the 'Mail-From:' field in outgoing emails.
- *REQUIRE_TLS* - SMTP server must support TLS in order to establish a connection. Valid values are 'TRUE' or 'FALSE'

*cfgValue* is the value to associate for a setting property.

```
char[] SMTP_SERVER_CONFIG_GET (CONSTANT CHAR cfgName[])
```

Queries a server configuration property. Returns the config property value.

*cfgName* is the server property name that is being retrieved. Acceptable values are a subset of the settable properties (username & password query are disabled as a security precaution). No return value

- *ADDRESS* - SMTP server name, such as "mail.amx.com". The maximum number of characters allowed for email destination is 127.
- *PORT* - SMTP server port, such as "25" or "0". 0 means "use the best default port" which would imply using 25 which is the SMTP well-known port.
- *FROM* - Mail address populated to the 'Mail-From:' field in outgoing emails.
- *REQUIRE_TLS* - SMTP server must support TLS in order to establish a connection. Valid values are 'TRUE' or 'FALSE'

The **NetLinx .axi** file has the following built in constants to ease configuration:

```
CHAR SMTP_ADDRESS[] = 'ADDRESS';
CHAR SMTP_PORT_NUMBER[] = 'PORT';
CHAR SMTP_USERNAME[] = 'USERNAME';
CHAR SMTP_PASSWORD[] = 'PASSWORD';
CHAR SMTP_REQUIRE_TLS[] = 'REQUIRE_TLS';
CHAR SMTP_FROM[] = 'FROM';
CHAR NULL_STR[] = '';
CHAR SMTP_TLS_TRUE[] = 'TRUE';
CHAR SMTP_TLS_FALSE[] = 'FALSE';
```

Example server configuration:

```
SMTP_SERVER_CONFIG_SET(SMTP_ADDRESS,'mail.mymailserver.com')
SMTP_SERVER_CONFIG_SET(SMTP_PORT_NUMBER,'25')
SMTP_SERVER_CONFIG_SET(SMTP_USERNAME,'myAccountUsername')
SMTP_SERVER_CONFIG_SET(SMTP_PASSWORD,'myAccountPassword')
SMTP_SERVER_CONFIG_SET(SMTP_REQUIRE_TLS, SMTP_TLS_TRUE)
SMTP_SERVER_CONFIG_SET(SMTP_FROM,'John Doe')
```

## Sending Mail

Sending mail is accomplished with the use of the Master's built-in Mail Service. An outbound mail is handed to the Mail Service via the following built-in NetLinx function:

```
sinteger SMTP_SEND (DEV responseDPS, CONSTANT CHAR toAddress[], CONSTANT CHAR mailSubject[], CONSTANT
CHAR mailBody[], CONSTANT CHAR textAttachment[])
```

where:

- *responseDPS* - The DPS address to return asynchronous send status. Ex. 0:3:0
- *toAddress* - The email address of destination. Ex. john.doe@amx.com.

  Note that the NetLinx mail service supports up to eight recipient address (semi-colon delimited). These are "To" addresses only (not "Cc" or "Bcc" addresses.)

  The maximum number of characters allowed for email destination is 127.
- *mailSubject* - The email subject line.
- *mailBody* - The email body text.
- *textAttachment* - A text filename to attach to the email (optional argument). Filenames must be 256 characters or less, and file size must be under 65536 bytes. When no attachment is included textAttachment should be set to NULL_STR.

SMTP_SEND returns a signed integer.

- If the return value is negative (<0) that is an indication there was a failure in handing the message off to the mail service, most likely due to an invalid argument supplied to the SMTP_SEND call.
- If the return value is positive (>0) then the value is the index associated with the mail being sent.
- Mail sends are asynchronous to the normal processing of the NetLinx application.
- When SMTP_SEND is called and the mail is posted to the internal Mail Service, the NetLinx application will continue executing the code following the SMTP_SEND.
- The failed send status will be returned via an ONERROR DATA_EVENT for the *responseDPS* specified in the SMTP_SEND call with DATA.NUMBER set to the error code and DATA.TEXT set to the mail identifier returned from the SMTP_SEND call.

Example SMTP_SEND:

```
DEFINE_DEVICE
MAIL_SERVICE=0:3:0

DEFINE_VARIABLE
SINTEGER MAIL_IDX


…
MAIL_IDX = SMTP_SEND(MAIL_SERVICE,'jdoe@somemail.com','Mail Subj','Mail Body', NULL_STR)
IF (MAIL_IDX < 0)
{
     // FAILED TO SEND MAIL
}
…
DATA_EVEN [MAIL_SERVICE]
{
     ONERROR:
     {
          // AN ERROR OCCURRED
          LOG_ERROR("MAIL SEND FAILURE - IDX=',DATA.TEXT,' ERROR=',ITOA(DATA.NUMBER))
     }
}
```

The possible error codes are:

```
MALFORMED DATA = 1;
NOT ENOUGH MEMORY = 2;
SERVER UNREACHABLE = 3;
AUTHENTICATION FAILURE = 4;
SMTP PROTOCOL ERROR = 5;
```

# Appendix D: Clock Manager NetLinx Programming API

## Types/Constants

The NetLinx.axi file that ships with NetLinx Studio includes the following types/constants:

```
(*-----------------------------------------------------------------------------*)
(* Added v1.28, Clock Manager Time Offset Structure *)
(*-----------------------------------------------------------------------------*)
STRUCTURE CLKMGR_TIMEOFFSET_STRUCT
{
  INTEGER     HOURS;
  INTEGER     MINUTES;
  INTEGER     SECONDS;
}

(*-----------------------------------------------------------------------------*)
(* Added v1.28, Clock Manager Time Server Entry Structure *)
(*-----------------------------------------------------------------------------*)
STRUCTURE CLKMGR_TIMESERVER_STRUCT
{
  CHAR     IS_SELECTED;               (* TRUE/FALSE *)
  CHAR     IS_USER_DEFINED;           (* TRUE/FALSE *)
  CHAR     IP_ADDRESS_STRING[48];     (* Allow enough room for IPv6 in the future *)
  CHAR     URL_STRING[32];            (* Example: time.organization.net *)
  CHAR     LOCATION_STRING[32];       (* Example: Boulder, Colorado, US *)
}

(* Added v1.28, Clock Manager *)
INTEGER CLKMGR_MODE_NETWORK    = $01; (* Used to enable Clock Manager Functionality *)
INTEGER CLKMGR_MODE_STANDALONE = $02; (* Use a free-running clock - legacy behavior.*)
```

## Library Calls

The NetLinx.axi file that ships with NetLinx Studio includes the following Clock Manager-specific library calls:

| NetLinx.axi - Library Calls | |
|---|---|
| **CLKMGR_IS_NETWORK_SOURCED()** | Returns FALSE/0 or TRUE/1 (default = FALSE/0) |
| **CLKMGR_SET_CLK_SOURCE (CONSTANT INTEGER MODE)** | Can be set to CLKMGR_MODE_NETWORK or CLK-MGR_MODE_STANDALONE. |
| **CLKMGR_IS_DAYLIGHTSAVINGS_ON()** | Returns FALSE/0 or TRUE/1 (default = FALSE/0). |
| **CLKMGR_SET_DAYLIGHTSAVINGS_MODE (CONSTANT INTEGER ONOFF)** | Can be set to ON/TRUE or OFF/FALSE. |
| **CLKMGR_GET_TIMEZONE()** | Returns Timezone as a string in the format: UTC[+\|-]HH:MM |
| **CLKMGR_SET_TIMEZONE (CONSTANT CHAR TIMEZONE[])** | Input string must have the correct format: UTC[+\|-]HH:MM |
| **CLKMGR_GET_RESYNC_PERIOD()** | Returns the Clock Manager's re-sync period in minutes (default = 60). This setting has no effect if the Clock Manager mode is set to STANDALONE. |
| **CLKMGR_SET_RESYNC_PERIOD (CONSTANT INTEGER PERIOD)** | Sets the re-sync period to the specified minute value. The upper bound is 480 minutes (i.e., 8 hours). |
| **CLKMGR_GET_DAYLIGHTSAVINGS_OFFSET (CLKMGR_TIMEOFFSET_STRUCT T)** | Populates the TIMEOFFSET structure with the current Daylight Savings Offset configured. The function returns a negative SLONG value if it encounters an error. |
| **CLKMGR_SET_DAYLIGHTSAVINGS_OFFSET (CONSTANT CLKMGR_TIMEOFFSET_STRUCT T)** | Sets the Daylight Savings Offset to the specified value. |
| **CLKMGR_GET_ACTIVE_TIMESERVER (CLKMGR_TIMESERVER_STRUCT T)** | Populates the TIMESERVER structure with the currently active time server's data. The function returns a negative SLONG value if it encounters an error. |
| **CLKMGR_SET_ACTIVE_TIMESERVER (CONSTANT CHAR IP[])** | Sets the time server entry that has the matching IP-ADDRESS to the IP parameter as the active time server entry. |

| NetLinx.axi - Library Calls (Cont.) | |
|---|---|
| **CLKMGR_GET_TIMESERVERS (CLKMGR_TIMESERVER_STRUCT T[])** | Populates the currently configured time server entries from the Clock Manager into the specified TIMESERVER array.<br>The function returns a negative SLONG value if it encounters an error, otherwise the return value is set to the number of records populated into the CLK-MGR_-TIMESERVER_STRUCT array. |
| **CLKMGR_ADD_USERDEFINED_TIMESERVER (CONSTANT CHAR IP[], CONSTANT CHAR URL[], CONSTANT CHAR LOCATION[])** | Adds a user-defined time server entry. |
| **CLKMGR_DELETE_USERDEFINED_ TIMESERVER(CONSTANT CHAR IP[])** | Deletes the user-defined entry that has its IP-ADDRESS matching the parameter. |
| **CLKMGR_GET_START_ DAYLIGHTSAVINGS_RULE()** | Gets a string representation of when Daylight Savings is supposed to START.<br>The Fixed-Date rules have the form:<br>"fixed:DAY,MONTH,HH:MM:SS"<br>with all fields as numeric except for the word "fixed".<br>The Occurrence-Of-Day rules have the form:<br>"occurence:OCCURENCE,DAY-OF-WEEK,MONTH,HH:MM:SS"<br>with all fields as numeric except for the word "occurence".<br>• OCCURANCE range = 1-5<br>’5’ indicates the 'LAST' occurrence of a particular day of the month.<br>• DAY-OF-WEEK translates as:<br>1=Sunday<br>2=Monday<br>3=Tuesday<br>4=Wednsday<br>5=Thursday<br>6=Friday<br>7=Saturday<br>Examples:<br>"fixed:5,10,16:00:00" = October 5, at 4:00PM).<br>"occurence:5,1,10,02:00:00" = last Sunday in October, at 2:00AM). |
| **CLKMGR_SET_START_DAYLIGHTSAVINGS_RULE (CONSTANT CHAR RECORD[])** | Sets the START Daylight Savings rule to the specified string which *must* be in either the Fixed-Date format or the Occurence-Of-Day format. The function returns a negative SLONG value if it encounters an error.<br>The Fixed-Date rules have the form:<br>"fixed:DAY,MONTH,HH:MM:SS"<br>with all fields as numeric except for the word "fixed".<br>The Occurrence-Of-Day rules have the form:<br>"occurence:OCCURENCE,DAY-OF-WEEK,MONTH,HH:MM:SS"<br>with all fields as numeric except for the word "occurence".<br>• OCCURANCE range = 1-5<br>’5’ indicates the 'LAST' occurrence of a particular day of the month.<br>• DAY-OF-WEEK translates as:<br>1=Sunday<br>2=Monday<br>3=Tuesday<br>4=Wednsday<br>5=Thursday<br>6=Friday<br>7=Saturday<br>Examples:<br>"fixed:5,10,16:00:00" = October 5, at 4:00PM).<br>"occurence:5,1,10,02:00:00" = last Sunday in October, at 2:00AM). |

| NetLinx.axi - Library Calls (Cont.) | |
|---|---|
| **CLKMGR_GET_END_DAYLIGHTSAVINGS_RULE()** | Gets a string representation of when Daylight Savings is supposed to END.<br>The Fixed-Date rules have the form:<br>"fixed:DAY,MONTH,HH:MM:SS"<br>with all fields as numeric except for the word "fixed".<br>The Occurrence-Of-Day rules have the form:<br>"occurence:OCCURENCE,DAY-OF-WEEK,MONTH,HH:MM:SS"<br>with all fields as numeric except for the word "occurence".<br>• OCCURANCE range = 1-5<br>’5’ indicates the 'LAST' occurrence of a particular day of the month.<br>• DAY-OF-WEEK translates as:<br>1=Sunday<br>2=Monday<br>3=Tuesday<br>4=Wednsday<br>5=Thursday<br>6=Friday<br>7=Saturday<br>Examples:<br>"fixed:5,10,16:00:00" = October 5, at 4:00PM).<br>"occurence:5,1,10,02:00:00" = last Sunday in October, at 2:00AM). |
| **CLKMGR_SET_END_DAYLIGHTSAVINGS_RULE (CONSTANT CHAR RECORD[])** | Sets the END Daylight Savings rule to the specified string which MUST be in either the Fixed-Date format or the Occurence-Of-Day format. The function returns a negative SLONG value if it encounters an error.<br>The Fixed-Date rules have the form:<br>"fixed:DAY,MONTH,HH:MM:SS"<br>with all fields as numeric except for the word "fixed".<br>The Occurrence-Of-Day rules have the form:<br>"occurence:OCCURENCE,DAY-OF-WEEK,MONTH,HH:MM:SS"<br>with all fields as numeric except for the word "occurence".<br>• OCCURANCE range = 1-5<br>’5’ indicates the 'LAST' occurrence of a particular day of the month.<br>• DAY-OF-WEEK translates as:<br>1=Sunday<br>2=Monday<br>3=Tuesday<br>4=Wednsday<br>5=Thursday<br>6=Friday<br>7=Saturday<br>Examples:<br>"fixed:5,10,16:00:00" = October 5, at 4:00PM).<br>"occurence:5,1,10,02:00:00" = last Sunday in October, at 2:00AM). |

AMX does not assume responsibility for errors or omissions. AMX also reserves the right to alter specifications without prior notice at any time.
The AMX Warranty and Return Policy and related documents can be viewed/downloaded at www.amx.com.

**3000 RESEARCH DRIVE, RICHARDSON, TX 75082 AMX.com | 800.222.0193 | 469.624.8000 | +1.469.624.7400 | fax 469.624.7153**
**AMX (UK) LTD, AMX by HARMAN - Unit C, Auster Road, Clifton Moor, York, YO30 4GD United Kingdom • +44 1904-343-100 • www.amx.com/eu/**

Last Revised:
11/11/2016