NETWORK TECHNOLOGIES INCORPORATED
1275 Danner Dr Tel:330-562-7070
Aurora, OH 44202 Fax:330-562-1999
www.networktechinc.com

SERIMUX® Series

SERIMUX-S-x

SECURE SSH CONSOLE SERIAL SWITCH
Installation and Operation Manual

CE

TRADEMARK

SERIMUX and the NTI logo are registered trademarks of Network Technologies Inc in the U.S. and other countries. All other brand names and trademarks or registered trademarks are the property of their respective owners.

COPYRIGHT

This product contains software licensed under the GNU Public License version 2 and other open source licenses.
(http://www.gnu.org/copyleft/gpl.html)
You may obtain the complete open-source code free of charge from Network Technologies Inc (send email to tech-consult@ntigo.com) for more information.

CHANGES

The material in this guide is for information only and is subject to change without notice. Network Technologies Inc reserves the right to make changes in the product design without reservation and without notification to its users.

FIRMWARE VERSION

Current Firmware Version 2.13

Note: When upgrading the firmware from a version before 2.1 to version 2.1, follow the procedure outlined in the release notes to complete the firmware upgrade and take advantage of the feature added in version 2.1.

CE Statement

We, Network Technologies Inc, declare under our sole responsibility that the SERIMUX-S-4/8/16/24/32 are in conformity with European Standard EN55022.

Typographic Conventions

The table below offers examples of text format and the meaning when that format is used when the font varies from the standard font (Helvetica) used in this manual.

Typeface meaning	Font Configuration	Example
On-screen computer output	Courier New-(not bold)	C:>
What you type on the computer	**Courier New-bold**	C:>**edit text.bat**
Characters to be typed as instructed within the body of a paragraph	**Courier New-bold Surrounded by < >**	<**L**>
Place holder-description of other data to enter	*Helvetica-Italic*	*Hostname*

TABLE OF CONTENTS

TABLE OF FIGURES

APPENDICES

INTRODUCTION

The NTI SERIMUX-S-x SSH Console Serial Switch (SERIMUX) is a serial port switch that delivers secure management of up to 32 serial devices via the internet, TCP/IP network, or dial-up modem connections. It combines the advanced security of Secure Shell v2 with unlimited access to remote network management. The SERIMUX-S-x allows links (or connections) between multiple pairs of RS232 asynchronous serial ports. The SERIMUX-S-x (x=8,16,24,or 32) is available with up to 32 serial port connections.

The main purpose of the switch is to provide secure management of several serial devices from local or remote locations (using Ethernet or external modems). Devices include routers, DSU's, servers, switches or any other equipment allowing serial operation using RS232 interface. Users can work locally using a VT100 or ANSI serial console, a CPU with a terminal program (i.e. HyperTerminal)) or from remote locations via Ethernet connection (Web Interface, SSH, Telnet).

Each SERIMUX port has to be configured for serial communication (baud rate, parity, etc) within the specifications of the attached serial device, but the configurations of the two devices linked by the SERIMUX do not need to match. Various parameters (communication speed, hardware and/or software flow control, timeout, etc) can be selected for each SERIMUX port. Devices may be either locally connected or connected through attached modems.

Each SERIMUX port can be configured as either a host or user port. Serial hosts (such as servers, switches etc.) are connected to host ports, while serial user devices (such as a terminal or serial console) are connected to user ports. Up to five (5) concurrent connections can be made to the same host port.

The SERIMUX supports two operator levels: user and administrator. Users may login and connect to serial devices attached at host ports. The administrator and users with administrative privileges can see and/or modify various port or user parameters in addition to connecting to serial devices attached at host ports.

Option:

- **Dual AC Power Option**- includes a second power connector for a secondary AC power supply cable- to order, add a "DP" to the part number (i.e. SERIMUX-S-x**DP**)

Serial Interface Specifications

- Serial ports: 8,16,24 or 32 RJ45 RS232 serial port connections
- Console port: 1-RJ45 RS232 console port connector
- Data: asynchronous, 5, 6, 7, or 8 bits per character
- Parity: even, odd, or none
- Stop Bits: 1 or 2 bits
- Flow Control: Xon/Xoff, RTS/CTS, Both, or None
- Baud Rate: 50 bps to 115200 bps between ports
  - Two connecting ports can be at different baud rates

Network Interface

- Two 10/100 Base-T Ethernet ports with RJ45 Ethernet connector
- Supports both static and dynamic IP addresses

RJ45 Sensor Ports

- Two RJ45 modular jacks for connecting NTI temperature, humidity, temperature/humidity, and liquid detection sensors.

Protocols

- SSH V2, Telnet ,IPMI
- IPV4, IPV6
- TCP/IP, TFTP, DHCP, ICMP, UDP, ARP
- HTTP, HTTPS, SMTP, SNMP V1/V2c, Syslog, SMTP
- IPMI v2, RMCP
- Alerts are sent using email, and/or SNMP traps when any monitored environmental condition exceeds a user-specified range or a serial port is connected or disconnected.

Supported Web Browsers

Most modern web browsers should be supported. The following browsers have been tested:

- Microsoft Internet Explorer 6.0 or higher
- Mozilla FireFox 0.9.2 or higher
- Opera 9.0 or higher
- Google Chrome 3.0 or higher

Set your browser to always check if there is a newer version of the page than the version stored in cache. This action will ensure that it will display the most up-to-date information.

Definitions

device	equipment that can transmit and/or receive data using RS232 interface
host	serial device that performs a function or stores data to be controlled by a user
inactivity	when a port is not receiving data from the device connected to it
terminal program	a terminal emulation program- computer program that communicates via RS232 interface (i.e. HyperTerminal)
"dumb" terminal	serial terminal device or CPU terminal program that emulates a serial terminal
timeout	time period of inactivity after which a port will be disconnected (the inter-port connection will be broken)
baud rate	serial device or port receiver and transmitter speed; measured in "bps" (bits per second)
flow control	a method to temporarily stop and restart serial data transfer (flow). It can be - Hardware (out-band)- usually using the RTS and CTS physical handshaking signals; - Software (in-band)- using special characters, usually named Xon and Xoff, inserted in data being transferred; - Both

Materials

Materials Supplied with this kit:

SERIMUX-S-x

Administrator's Note

4-#10-32 X ¾" Pan Head Screws
4-#10-32 Cage Nuts

IEC Power cord (country specific) (x2 with Dual AC power option)
(6 feet of 22AWG 2-wire cable provided for models with DC power connectors)

5 Foot RJ45-to-RJ45 Cat5 Patch Cable

Rubber Feet

DB9F-RJ45F Serial Adapter

DB25F-RJ45F Console Adapter

Rack mount ears kit

DB25M-RJ45F-C Modem Adapter

DB25M-RJ45F-T Console Adapter

RJ45MF-RS232-CO
Serial Crossover Adapter

Materials Required but <u>not supplied:</u>

Serial cable with at least one RJ45 male end for connection to the Console Switch from each device to be connected. See Interconnection Cable Wiring Method on page 86 for cable pinout.

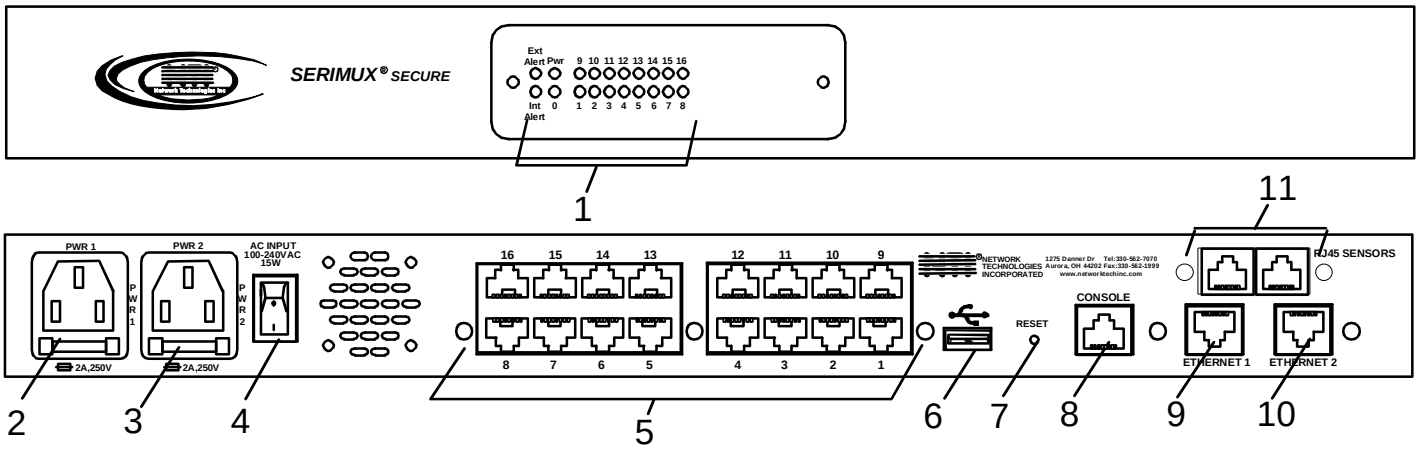
DEFAULT USER NAME AND PASSWORD

The default user name is **root** (lower case letters only).

The default password is **nti** (lower case letters only).

FEATURES AND FUNCTIONS

Front and Rear Views of SERIMUX-S-16DP



1. **STATUS LEDs**- LEDs will illuminate to indicate the SERIMUX is ON, activity on connected ports, or if there are alerts
2. **PWR1-** IEC Connector- for connection of AC power cord
3. **PWR2-** IEC Connector- for connection of second AC power cord for redundant power source (models with Dual AC Power option only)
4. **Power Switch**- for turning the SERIMUX ON or OFF
5. **Port connectors**- RJ45 female serial connectors- for connecting serial cables from serial devices or user terminals
6. **USB Devices**- USB Type A female connector- for connecting USB flash drive for various data storage options
7. **Reset button**- For power cycling the SERIMUX firmware without powering down the SERIMUX
8. **Console Port**- RJ45 female serial connector- for connecting serial cable from a terminal console
9. **Ethernet 1**- RJ45 female connector- for connection of CAT5 cable to Local Area Network (LAN) for WEB interface
10. **Ethernet 2**- RJ45 female connector- for redundant connection of CAT5 cable to Local Area Network (LAN) for WEB interface
11. **RJ45 Sensors**- RJ45 female connector- for connection of CAT5 cables to optional sensors

INSTALLATION

This NTI switch was designed to be mounted to a rack or to set on a desktop. It includes rack mount ears to make attachment to a rack easy, and rubber feet to be applied to the bottom of the case if it will instead sit on a flat surface. If this will sit on a flat surface, simply apply the rubber feet to the bottom of the case in each of the 4 corners.

To Mount to a Rack

1. Attach the ears to the switch using the #6-32x3/16" flat Phillips-head screws (6) provided as shown in the illustration below. The holes in the ears should line up with pre-threaded holes in the sides of the NTI switch. Tighten the screws securely.

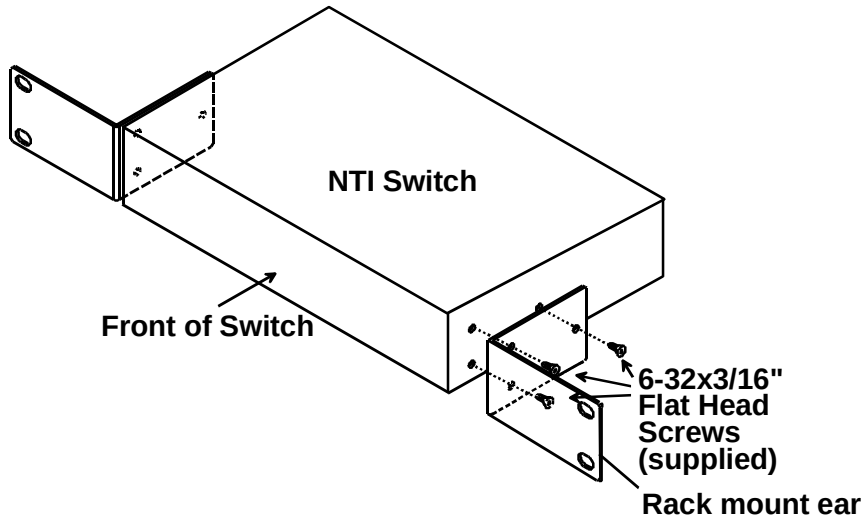


Figure 1- Secure rack mount ears to switch

2. Install 4 cage nuts (supplied) to the rack in locations that line up with the holes in the mounting ear on the NTI switch.

3. Secure the NTI switch to the rack using four #10-32X3/4" screws (supplied). Each screw should be of sufficient length to go completely through the NTI mounting ear, rack frame and fully engage all threads in the cage nut. Be sure to tighten all mounting screws securely.

4. Attach all cables securely to the switch and where necessary supply adequate means of strain relief for cables.

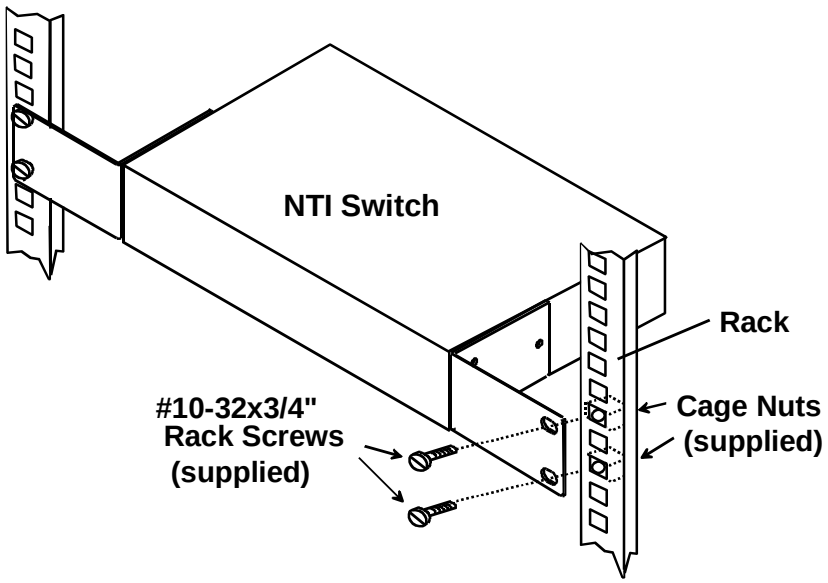


Figure 2- Secure switch to a rack

Cable Connections

1. Connect a serial console to the port labeled "CONSOLE" on the SERIMUX using a serial cable with an RJ45 male connector (Cat5 patch cable supplied). This will be the default administrator device. (Figure 3)

2. Connect each additional serial user device or host device to be connected by the SERIMUX to any remaining port (1-4/8/16/24/32) using a serial cable with an RJ45 male connector (see cable specification on page 86). It may be necessary to add one of the cable adapters (supplied) detailed in Appendix C (page 88) between the device port on the serial user device or host device and the RJ45 connector. An NTI RJ45MF-RS232-CO serial crossover adapter has been provided for connection of one DCE type device. More adapters can be purchased separately.

Note: There are two types of serial devices, data communication equipment (DCE)(i.e. modem) and data terminal equipment (DTE) (i.e. CPU), each having different connector pin assignments. The cable adapters (see Appendix C on page 88) make the proper connections.

3. Follow the "Initial Startup" instructions on page 10.

Rear View of SERIMUX-S-16DP

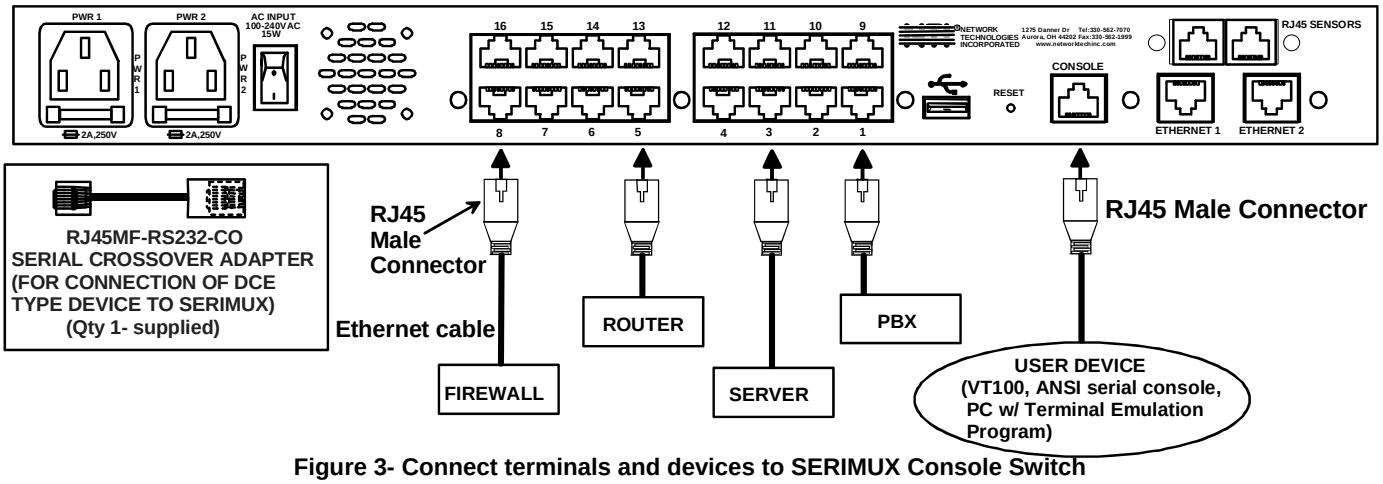


Figure 3- Connect terminals and devices to SERIMUX Console Switch

Connect to the Ethernet

If the Ethernet connection is made, the Web Interface (page 52) can be used. Up to two Ethernet connections to a Local Area Network (LAN) can be made using Cat5 cable with RJ45 connectors attached. Wiring between connectors should be straight through (pin 1 to pin 1, pin 2 to pin 2, etc.). Connect a Cat5 cable between the connector labeled "ETHERNET 1" and the LAN (see Figure 4). For a redundant connection, attach a second Cat5 cable between the connector labeled “ETHERNET 2” and the LAN.

Rear View of SERIMUX-S-16DP

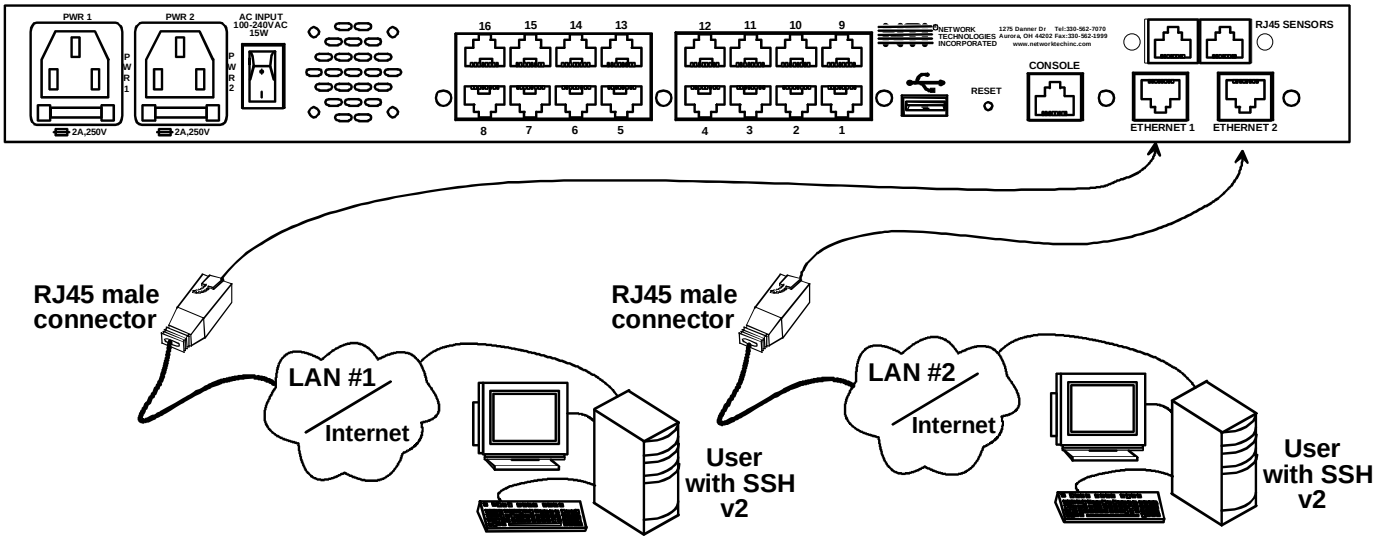


Figure 4- Connect the LAN to the SERIMUX

Dual Power Option

The SERIMUX-S-xDP has two IEC connectors on the rear, for connection to two separate power sources. If the power source connected to “PWR 1” fails, the SERIMUX will automatically and without interruption switch over to the power source connected to “PWR 2”.

Note: If only one power source is used, it should be connected to “PWR 1”.

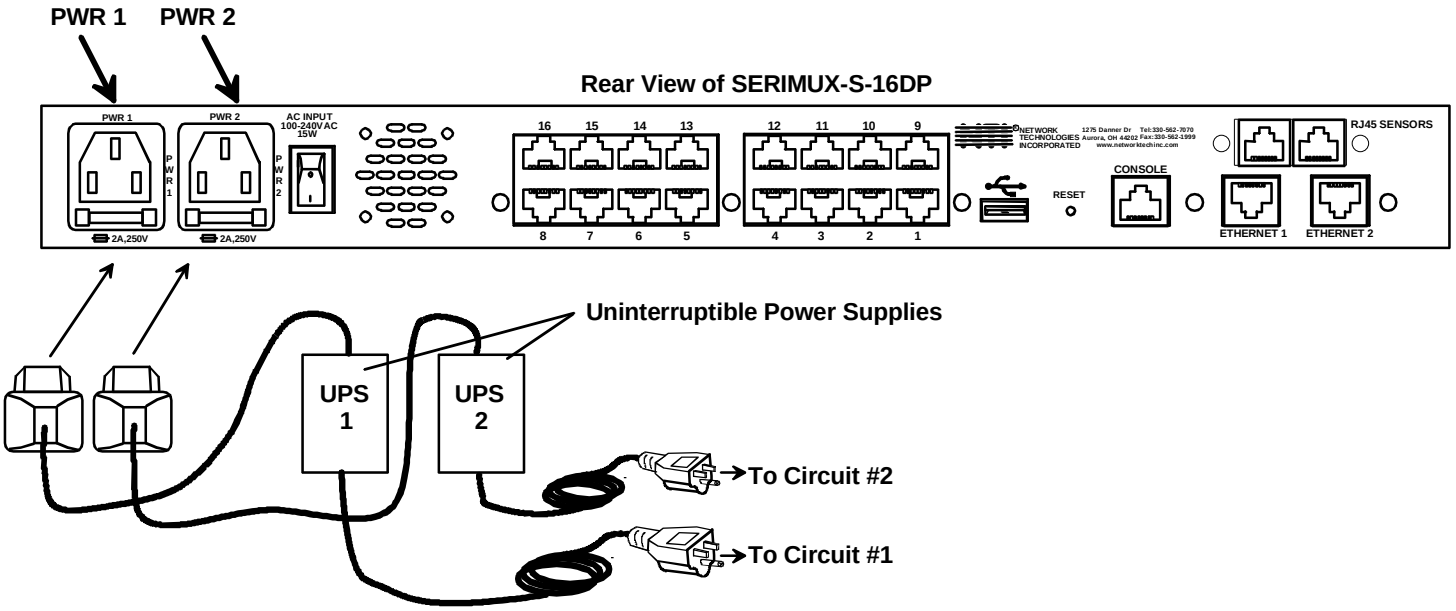


Figure 5- Power connections for SERIMUX with Dual Power option

Connect Sensors

The SERIMUX-S-x has two RJ45 connectors for attachment of up to two sensors to monitor environmental conditions. Sensors can be connected to measure temperature (ENVIROMUX-STS), temperature and humidity (ENVIROMUX-STHSB), temperature and wide range humidity (ENVIROMUX-STHS-99). A sensor can also be connected to detect liquids (ENVIROMUX-LDSx-y). All sensors are sold separately.

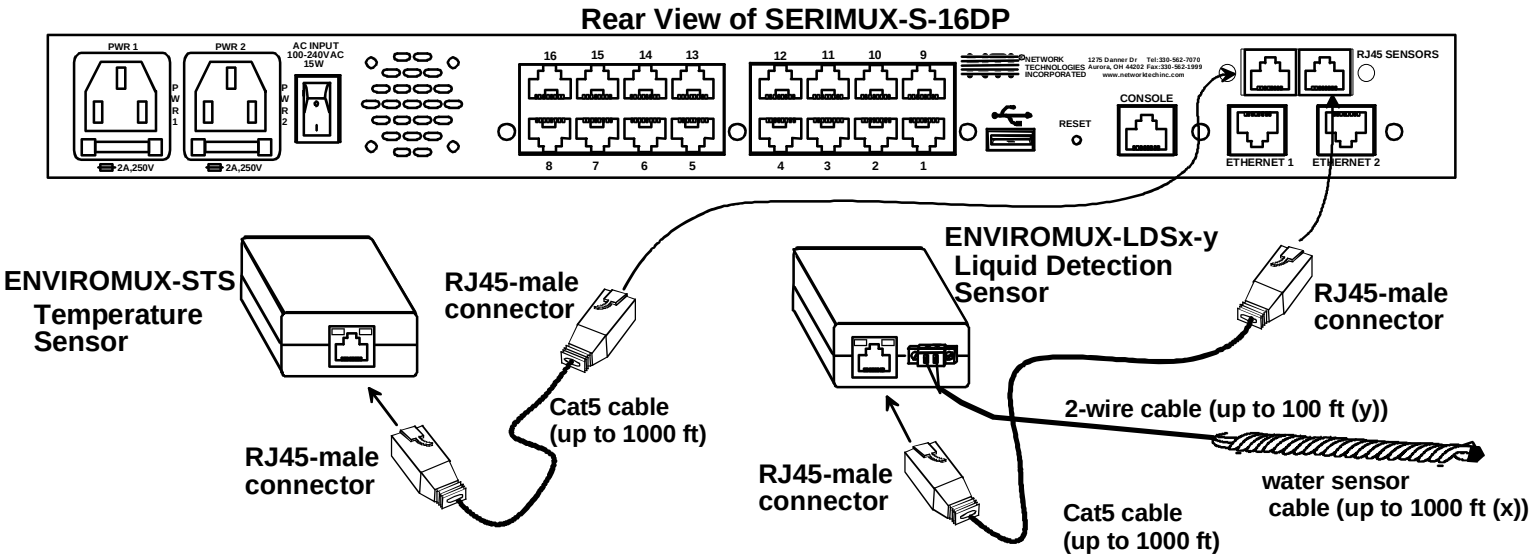


Figure 6- Connect sensors to the SERIMUX

INITIAL STARTUP

The following instruction will enable the user to quickly make port connections using a terminal connected to the "CONSOLE" port. For instruction to make quick connection using the Ethernet port and Web Interface, see page 52.

1. Make sure the SERIMUX is turned OFF.
2. Using the serial console device connected to the port labeled "CONSOLE", start the terminal program (e.g. Windows HyperTerminal or Putty) and configure it as follows:
   - direct connection (using the appropriate CPU local serial Com port)
   - 115200 bps
   - 8 bits
   - no parity
   - 1 stop bit
   - no flow control
   - ANSI or VT100 terminal mode.

3. Power ON the SERIMUX. Wait for the SERIMUX login prompt.

4. At "`login as:` " type <**`root`**> (all lowercase letters) and press <**`Enter`**>.

5. At "`password`" type <**`nti`**> (all lowercase letters) and press <**`Enter`**>.

Note: If the administrator password has been changed and is not known, contact NTI for instruction on resetting the SERIMUX to defaults.

6. A shell prompt will be displayed "`-sh-2.05b#` ". From this point you can either access the SERIMUX configuration menu, or access a submenu for either making a port connection or viewing the status of connected sensors.

A. **To access the configuration menu**:

Type <**`serimuxconfig`**> to open Serimux Secure Configuration Menu. (See Figure 7) Use menu structure to configure SERIMUX.

```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Thu Apr  8 13:22:40 2010 from 65.243.248.30
-sh-2.05b# serimuxconfig

------------------------------------------------------------------------
Welcome to NTI Serimux Secure configuration menu
Firmware Revision  :1.4
MAC Address(eth0)  :00:0c:82:04:00:02
IP Address(eth0)   :192.168.3.89
------------------------------------------------------------------------
   1. Serial Port Management
   2. Device Management
   3. Network Management
   4. Administration Settings
   5. User Management
   6. Administrative Info

e[x]it, [s]ave, a[p]ply, [h]elp, [Esc]
INPUT :
```

Figure 7- SERIMUX Secure configuration menu via serial connection

B. To make a connection with a host:

Type <**portmenu**> to open a submenu listing the “Port Connect Menu” and the “Sensor Monitor Menu”.

Figure 8- Submenu for Port Connect or Sensor Monitoring

Enter <**1**> +<**Enter**> to proceed to the port connection menu.

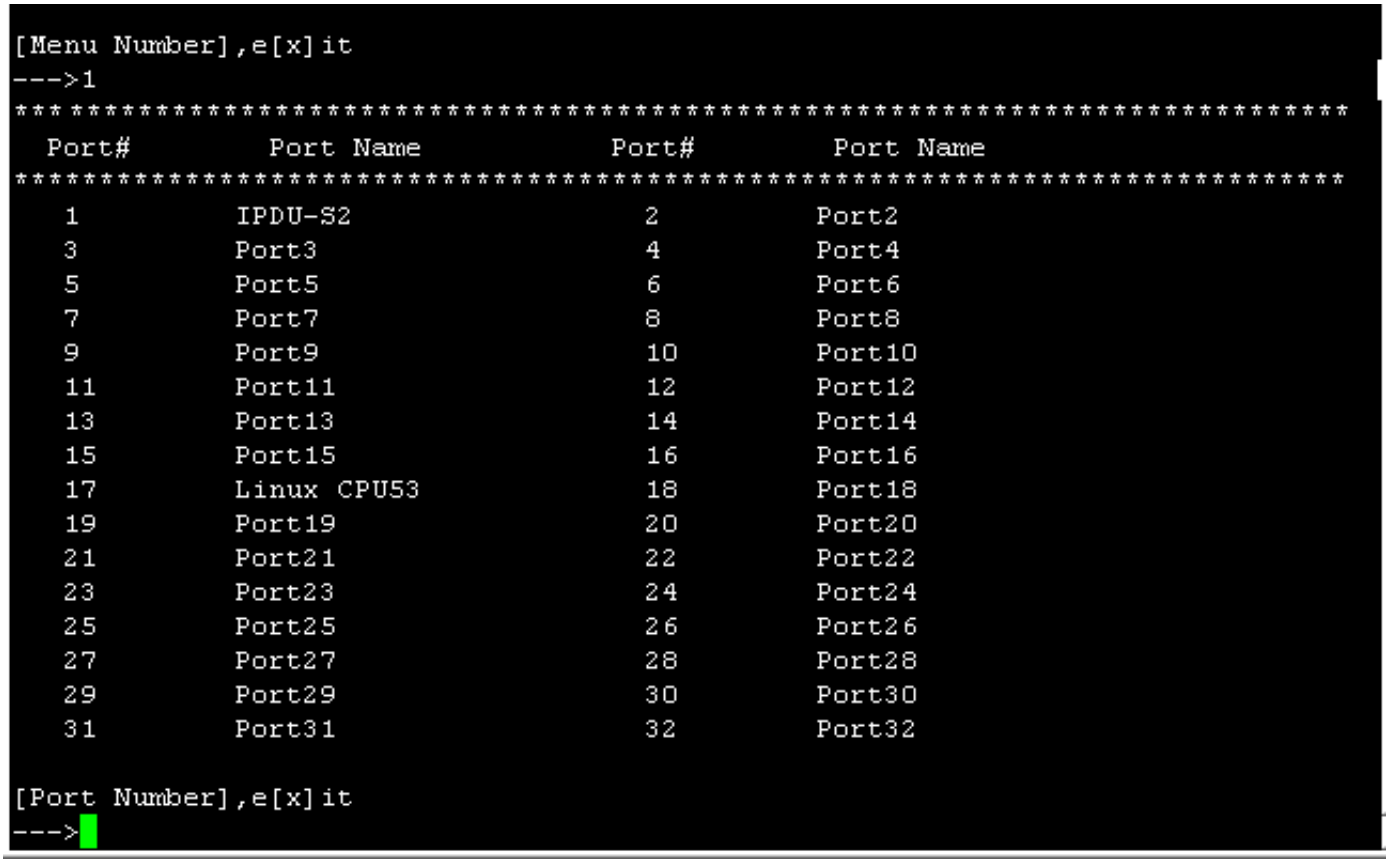


Figure 9- Port Connection menu

Then type a port number and press <**Enter**> to make a connection with a host. (See Figure 9)

Enter <**x**> to return to the previous menu.

Note: To connect to a host, the host must first be configured with the same communication settings as the port (default serial settings = 9600 baud, 8 bits, no parity, 1 stop bit, no flow control). If needed, see “Serial Settings” on page 18 to change the SERIMUX port serial settings.

C. To view sensor status:

Type <**portmenu**> to open a submenu listing the "Port Connect Menu" and the "Sensor Monitor Men" (see Figure 8).
Enter <**2**> +<**Enter**> to proceed to the Sensor List.

```
*********************************************************************************
Select Menu
*********************************************************************************
1) Port Connect Menu
2) Sensor Monitor menu

[Menu Number],e[x]it
--->2


Sensor list

No.  TYPE             DESCRIPTION             VALUE      STATUS
-------------------------------------------------------------------
1    Temperature      Internal Temp.          84.2       Normal
2    Internal Power   Internal Power Status   Open       Normal
3    Internal Fan     Internal Fan Speed       8675 rpm  Normal
4    Temp. Combo      Server Rack Temp        77.3       Normal
5    Humidity Combo   Server Rack Humidity    26         Normal
6    Water            Water                   Open       Normal
-------------------------------------------------------------------
[A]cknowledge Alert,[D]ismiss Alert,E[x]it
INPUT :
```

Figure 10- Sensor Monitoring

From the Sensor Monitor menu you will view a list of all sensors monitored by the SERIMUX. From here you will be able to view the current value being reported by the sensor and its alert status. If a sensor is reporting an alert, you can either press <a> to acknowledge the alert, or <d> to dismiss the alert.

If the sensor is in alert status, the user has the option to either **acknowledge** the alert or **dismiss** it. If the user acknowledges the alert, no additional alert messages will be sent during that alert status cycle. If the user dismisses the alert, another alert message will be sent once the "notify again after" time designated on the configuration page elapses.

Connect Direct to Serial Port from Command Line

To connect directly to a serial port from the command line, the SERIMUX must first be connected to the Ethernet (page 7).

Connect Via Telnet

To open a telnet session to a serial port, Issue the following command from the command line:

`telnet` <*Serimux-S hostname or IP address*> <*TCP port number*>

<*Serimux-S hostname*> is the hostname configured in the workstation where the telnet client will run (through /etc/hosts or DNS table). It can also be just the IP address of the SERIMUX.

<*TCP port number*> is the number assigned to the serial port. From the factory, 7001 corresponds to serial port 1, 7002 to serial port 2 and so forth.

The user will be prompted for username and password to connect to the port/device (unless the device has no security).

Connect Via SSH

To open an SSH session to a serial port, issue the following command from the command line:

`ssh -l` <*Username*> <*Serimux-S hostname or IP address*> **`-p`** <*Tcp port number*>

<*Username*> is the user configured to access that serial port (as defined in the list of users in the device configuration).

<*Serimux-S hostname*> is the hostname configured in the workstation where the telnet client will run (through /etc/hosts or DNS table). It can also be just the IP address of the SERIMUX.

<*TCP port number*> is the number assigned to the serial port. From the factory, 7001 corresponds to serial port 1, 7002 to serial port 2 and so forth.

The user will be prompted for a password to connect to the port/host.

Note: Up to five (5) concurrent connections can be made to the same host port.

USING THE SERIMUX CONSOLE SWITCH

The SERIMUX Console Switch is controlled using

- Serial Control- from a "dumb" terminal- locally-connected
  - through an external modem from a remote location
  - through a CPU connected to a "User" port
- Ethernet Connection (through a LAN or the Internet)
  - using the Web Interface
  - using Telnet or SSH client

Serial Control

The SERIMUX Console Switch can be easily configured using serial communications from either a locally-connected "dumb" terminal, from a terminal remotely connected through a modem, or from a CPU connected to a port configured as a "User" port. Using a keyboard-controlled menu, the user can make port connections or modify various parameters and options for each port.

Ethernet Connection

With an Ethernet connection to a LAN, the user can remotely control SERIMUX port configuration and connections. A user can connect through the Web Interface menus (see page 52) or using a Telnet or SSH client.

SERIAL CONTROL- ADMINISTRATOR

Using serial control, the SERIMUX supports 2 operator levels, administrator and user, each with separate password protection for security.

- The administrator logs in using an administrator password

administrator name : root (all lowercase letters)
administrator password : nti (all lowercase letters)

The administrator name cannot be changed.

To change the administrator password, see page 36.

- Users login using a password set by the administrator or a user with administrative privileges.

FYI: Users may be granted administrative access rights by any user with administrative access rights.

The administrator and any user with administrative rights can:

- view / modify port parameters;
- view / modify user parameters and user access rights to ports;
- disconnect ports, logout users etc.
- connect to devices on all host ports
- fully configure the SERIMUX except change the "root" password (only the "root" user can change the "root" password)

Users with only "user" rights can only connect to host ports they have access to as defined by the root user or a user with administrative access rights.

Throughout the SERIMUX Secure Configuration menu, the following guidelines apply:

Once changes are made, at the "`INPUT`" prompt;

- press <**s**>-<**Enter**> to save them for application to the system on the next reboot
- press <**p**>-<**Enter**> to save and apply changes immediately
- press <**Esc**> to exit the menu and step back one menu
- press <**x**>-<**Enter**> to exit the SERIMUX Secure configuration menu

If you press <**x**>-<**Enter**> without saving first, the message "`Do you want to save and apply configuration (y/n):`" will appear. Press <**y**> to save and apply, press <**n**> to exit without saving. If you press <**n**> or anything but <**y**>, you will receive the message "`Nothing applied`".

If you press <**x**>-<**Enter>** without having made any changes, the message "`Do you want to exit configuration menu(y/n):`" will appear. Press <**y**> to exit, or press <**n**> to be returned to the menu at which you were last. Pressing any other key will cause the message "`INVALID INPUT`" and return you to the current menu.

Press <**h**>-<**Enter**> for topic specific help.

Login as the administrator

1. From the user terminal connected to the “Console” port, open the terminal program (configured as described on page 10 under "Initial Startup").
2. Power ON the SERIMUX. Wait for the SERIMUX login prompt.

3. At “`login as:` “ type <**`root`**> (all lowercase letters) and press <**`Enter`**>. A prompt requesting a password will appear.

4. At “`password`” type <**`nti`**> (all lowercase letters) and press <**`Enter`**>.

Note: This will only access the SERIMUX if the administrator password has not yet been changed from "nti".

Note: If the administrator password has been changed and is not known, contact NTI for instruction on resetting the SERIMUX to the default password “nti”.

5. A shell prompt will be displayed **“**`-sh-2.05b#` “

To access the configuration menu:

Type <**`serimuxconfig`**> to open Serimux Secure Configuration Menu. (See Figure 7) Use the menus as described on the following pages to configure the SERIMUX.

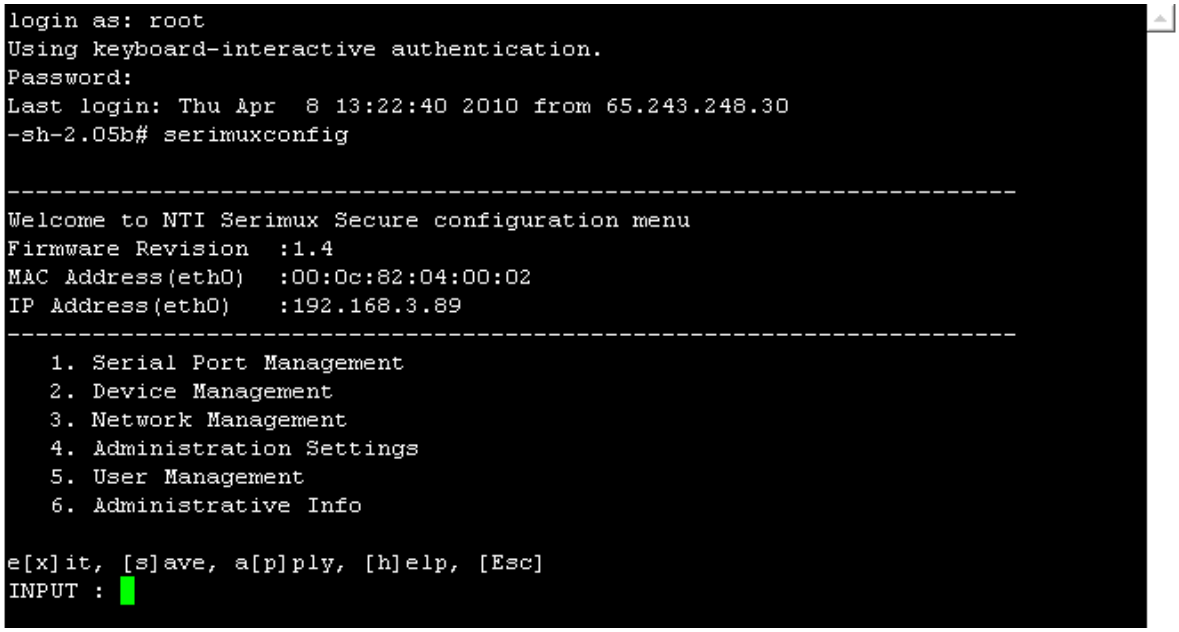


Figure 11- Serimux Secure Configuration menu

FYI: Only a user with administrative rights can access the configuration menu. Otherwise, a user will login directly to the Port Connect menu (Figure 10, page 12), with access to ports as defined by the administrator.

From the Serimux Secure Configuration menu, the following options are possible:

Function	Description	Keystroke
Port Management	Configure port settings	<1>-<Enter>
Device Management	Configure Sensor settings	<2>-<Enter>
Network Management	Configure Network settings	<3>-<Enter>
Administration Settings	Configure unit name, “root” password, security, and perform firmware update	<4>-<Enter>
User Management	Add, delete, and configure user settings; add, delete, setup access groups	<5>-<Enter>
Administrative Info	View syslog, firmware version, MAC addresses, network information	<6>-<Enter>
Exit	Exit connection with SERIMUX	<x>-<Enter>

From any submenu, press <**`Esc`**> to exit and back out to the previous menu. Press <**`x`**>-<**`Enter`**> to exit configuration menu.

Port Management

From the Configuration menu, press <**1**> to open the "Port Management" menu.

```
Port Management
------------------------------------------------------------------------

No.  Name             Mode    Serial-Setting        Esc Seq.Protocol Port
1    Web Server 1     Host    115200-8-1-None-None   ^z       ssh      7001
2    Web Server 2     Host    115200-8-1-None-None   ^z       ssh      7002
3    E-Mail Server    Host    115200-8-1-None-None   ^z       ssh      7003
4    Office Server    Host    115200-8-1-None-None   ^z       ssh      7004
5    DHCP Server      Host    9600-8-1-None-None     ^z       telnet   7005
6    DNS Server       Host    115200-8-1-None-None   ^z       ssh      7006
7    Backup Server    Host    115200-8-1-None-None   ^z       ssh      7007
8    T1 Router        Host    115200-8-1-None-None   ^z       ssh      7008
9    DSL Router       Host    115200-8-1-None-None   ^z       ssh      7009
10   T1 Firewall      Host    115200-8-1-None-None   ^z       ssh      7010
11   DSL Firewall     Host    115200-8-1-None-None   ^z       ssh      7011
12   Network Switch 1Host    115200-8-1-None-None   ^z       ssh      7012
13   Network Switch 2Host    115200-8-1-None-None   ^z       ssh      7013
14   Reserved         Host    9600-8-1-None-None     ^z       ssh      7014
15   Reserved         Host    9600-8-1-None-None     ^z       ssh      7015
16   Reserved         Host    9600-8-1-None-None     ^z       ssh      7016

SELECT PORT:
e[x]it, [s]ave, a[p]ply, [h]elp, [Esc],[O]common
INPUT :
```

Figure 12- Port Management- complete ports list

All ports, whether devices are connected to them or not, are listed in the Port Management menu. To make changes to a specific port's configuration, enter the port number and press <**Enter**>. A menu of Port Management settings will appear.

```
SELECT PORT:
e[x]it, [s]ave, a[p]ply, [h]elp, [Esc],[O]common
INPUT : 1

------------------------------------------------------------------------
Port Management->Port1
------------------------------------------------------------------------
   1. Port Setting
   2. Serial Setting
   3. Port Logging
   4. Modem Setting
   5. Authentication
   6. Event Notification
   7. Port Access List
   8. Port Disconnect
   9. Apply Common Settings

e[x]it, [s]ave, a[p]ply, [h]elp, [Esc]
INPUT :
```

Figure 13- Port Management selections for Port 1

To choose a category of settings to change, enter the number of the selection and press <**Enter**>.

Common Settings

Before making changes to settings for specific ports, it would be quicker to apply settings to the "common" port, by pressing <**o**> from the Port Management menu. This will open a menu (below) where the settings most common to the greatest number of ports can be configured. With these configured, changing port settings for specific ports will be quicker by making the selection of menu item 9-"Apply Common Settings" in the Port Management menu (page 24).

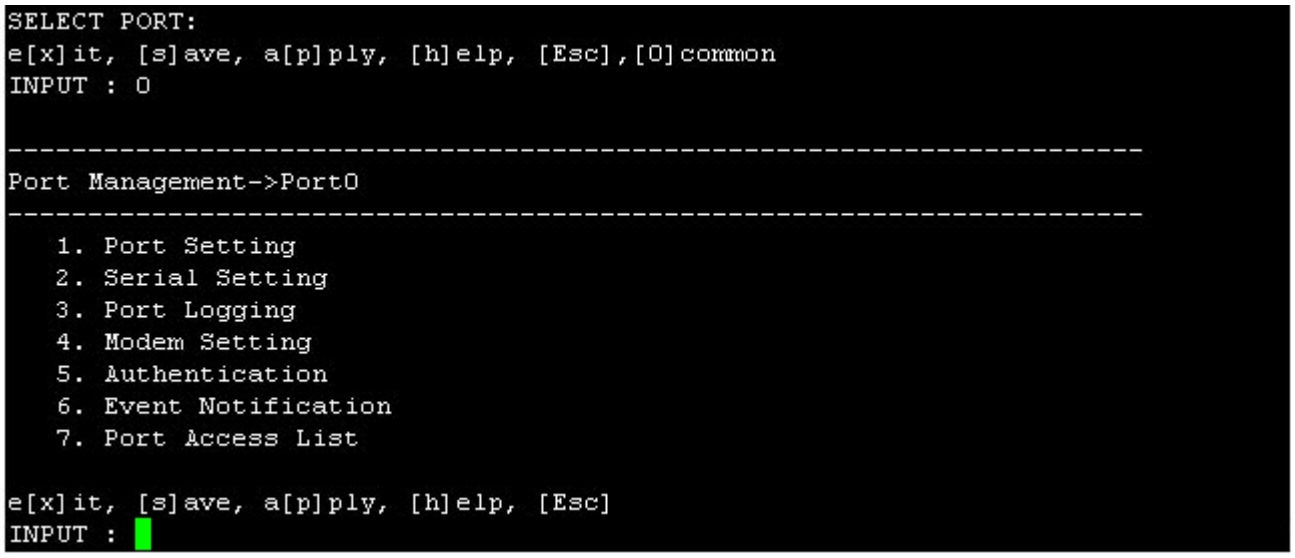


Figure 14- Port Management- configure common settings for most ports

Port Settings

From the Port Management menu, with Port x (any port) selected, press <**1**>-<**Enter**> to open the Port Setting menu.

Tip: Before configuring settings for Port 1-xx, configure common settings (top of page) and consider if applying them to the selected port will save time (see also page 24).

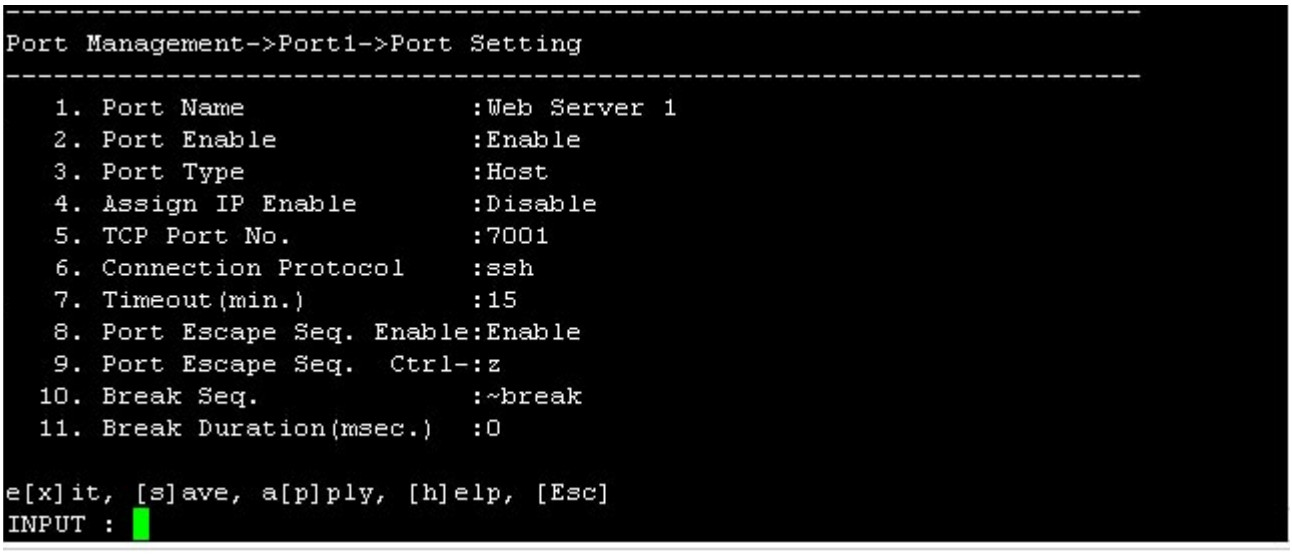


Figure 15- Port Management- port settings for Port 1

Setting	Valid Entries
Port Name	the name as it will appear in the port list- max. 50 characters.
Port Enable	Enable or Disable. If disabled, no user can connect to it.
Port Type	Host : for device connection User: for direct user connection Dial-in User: for connection via modem
Assign IP Enable	When enabled, an IP address can be specifically assigned to this port. Once enabled, the menu will refresh and an additional line will be added to assign the IP address to be used.
TCP Port No.	Assign number used for TCP communication **Be careful not to assign the same number used by another port, or the second port with a duplicate TCP port assignment will not work.**
Connection Protocol	Select: RawTCP for direct TCP connection Telnet is using a Telnet client (non-secure connection) SSH is using an SSH client (secure connection)
Timeout (minutes)	set time (in minutes) before a port connection that is idle will be automatically disconnected- range 0-999 minutes (0= disable)
Port Escape Seq. Enable	Enable or disable the function of using a port escape sequence
Port Escape Sequence	Keyboard key to use in conjunction with the <**Ctrl**> key for a port escape sequence. The default is <**z**>.
Break Sequence	Sequence of characters which will send a break signal – ie. <**Ctrl**>-<**break**>
Break Duration (msec.)	Duration for which the break signal will be applied-range=0-999

Press <**Esc**> to exit and back out to the previous menu.

Serial Settings

From the Port Management menu, with Port x (any port) selected, press <**2**>-<**Enter**> to open the Serial Setting menu.

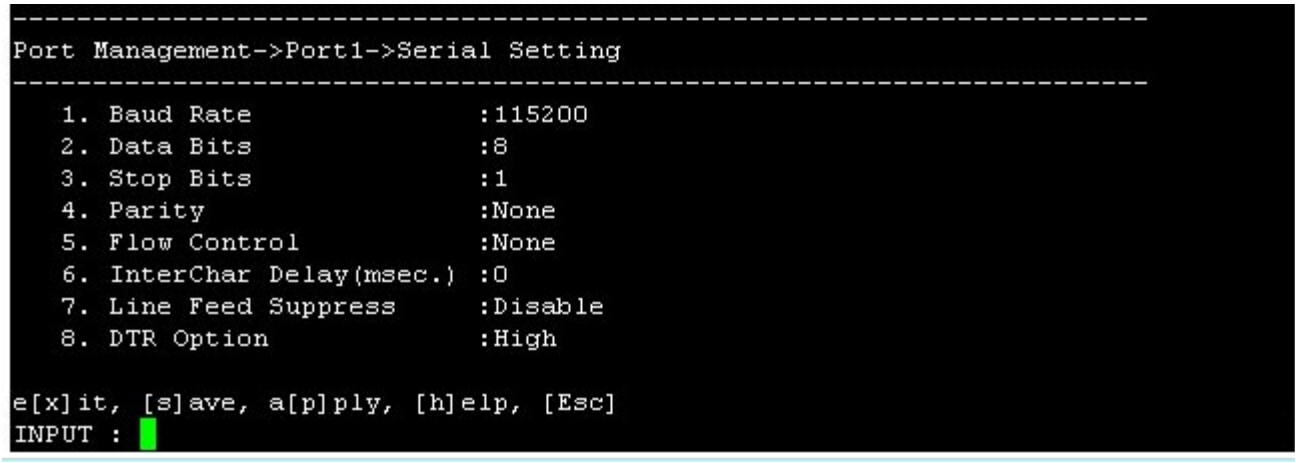


Figure 16- Port Management-serial settings for Port 1

Setting	Value
Baud Rate	50bps-115.2Kbps (default = 9600)
Data Bits	5, 6, 7, or 8 (default = 8)
Stop bits	1 or 2 (default = 1)
Parity	None, Even, or Odd (default = none)
Flow Control	Hardware, Software, Both, or None (default = none)
Inter Character Delay	0-999 ms
Line Feed Suppress	Enable or Disable
DTR Option	High or Low

Port Logging

From the Port Management menu, with Port x (any port) selected, press <**3**>-<**Enter**> to open the "Port Logging" menu. Port logging is used to record data received on the serial port.

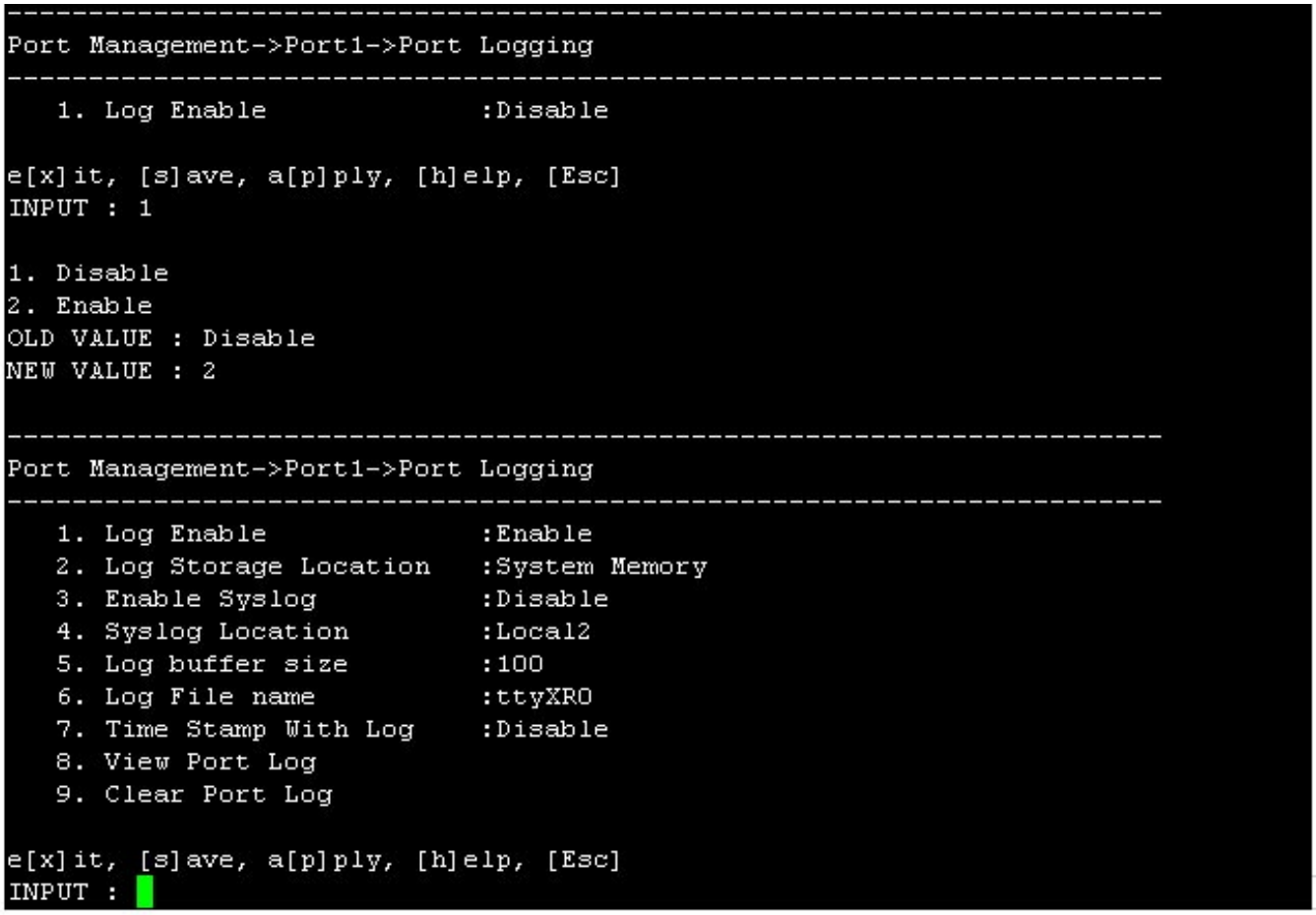


Figure 17- Port Management-port logging for Port 1

Only 1 menu item will be displayed, indicating that port logging is disabled. Press <**1**>-<**Enter**> to be prompted for a new value. Press <**2**>-<**Enter**> to enable port logging.

With port logging enabled, additional menu items will appear with the following setting options:

Setting	Value
Log Enable	Disable or Enable Logging feature for this port
Log Storage Location	System Memory (cannot change at this time)
Enable Syslog	Disable or Enable Syslog feature for port
Syslog Location	Local
Log Buffer Size	0-999 (K bytes)
Log File Name	up to 100 characters
Time Stamp With Log	Enable to have log entries include a timestamp

Press <**8**> to view any current entries in the port log.

Press <**9**> to delete any entries in the port log for that port.

Modem Setting

From the Port Management menu, with Port x (any port) selected, press <**4**>-<**Enter**> to open the “Modem Setting” menu.

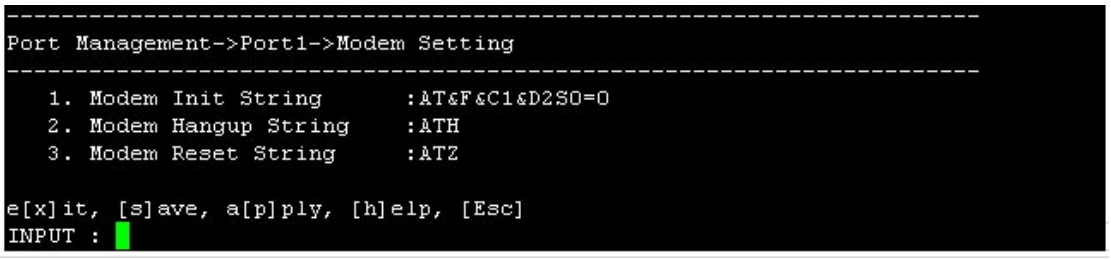


Figure 18- Port Management-modem setting for Port 1

If the port is set for a port type “Dial-In User” (see page 17), it will require a modem to be connected. Refer to your modem instructions for appropriate settings to be applied here.

Authentication

From the Port Management menu, with Port x (any port) selected, press <**5**>-<**Enter**> to open the ”Authentication” menu.

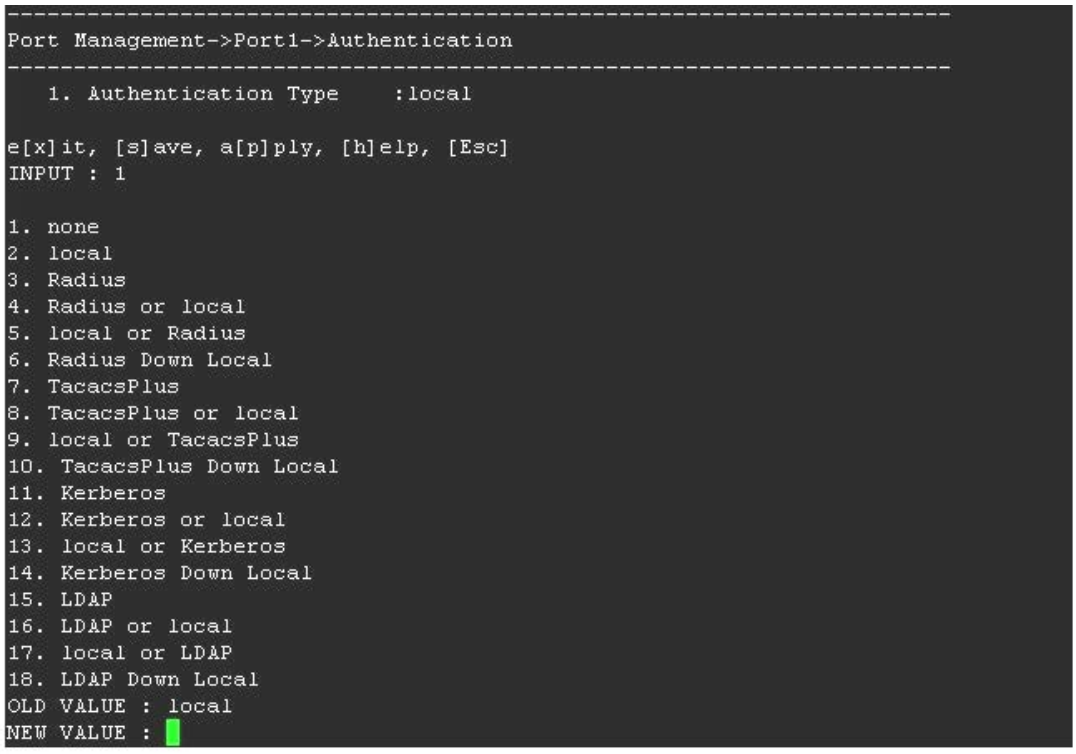


Figure 19- Port Management-authentication for Port 1

From the menu (showing “`1. Authentication Type`”), press <**1**>-<**Enter**> to open a list of authentication options.

To disable authentication for that port, enter <**1**> for “`none`”. If the Authentication Type is set to “none”, then a user will not be required to provide a username and password to access that port when connecting to it.

Authentication options that include Radius, TacacsPlus, Kerberos, and LDAP will require additional configuration when selected.

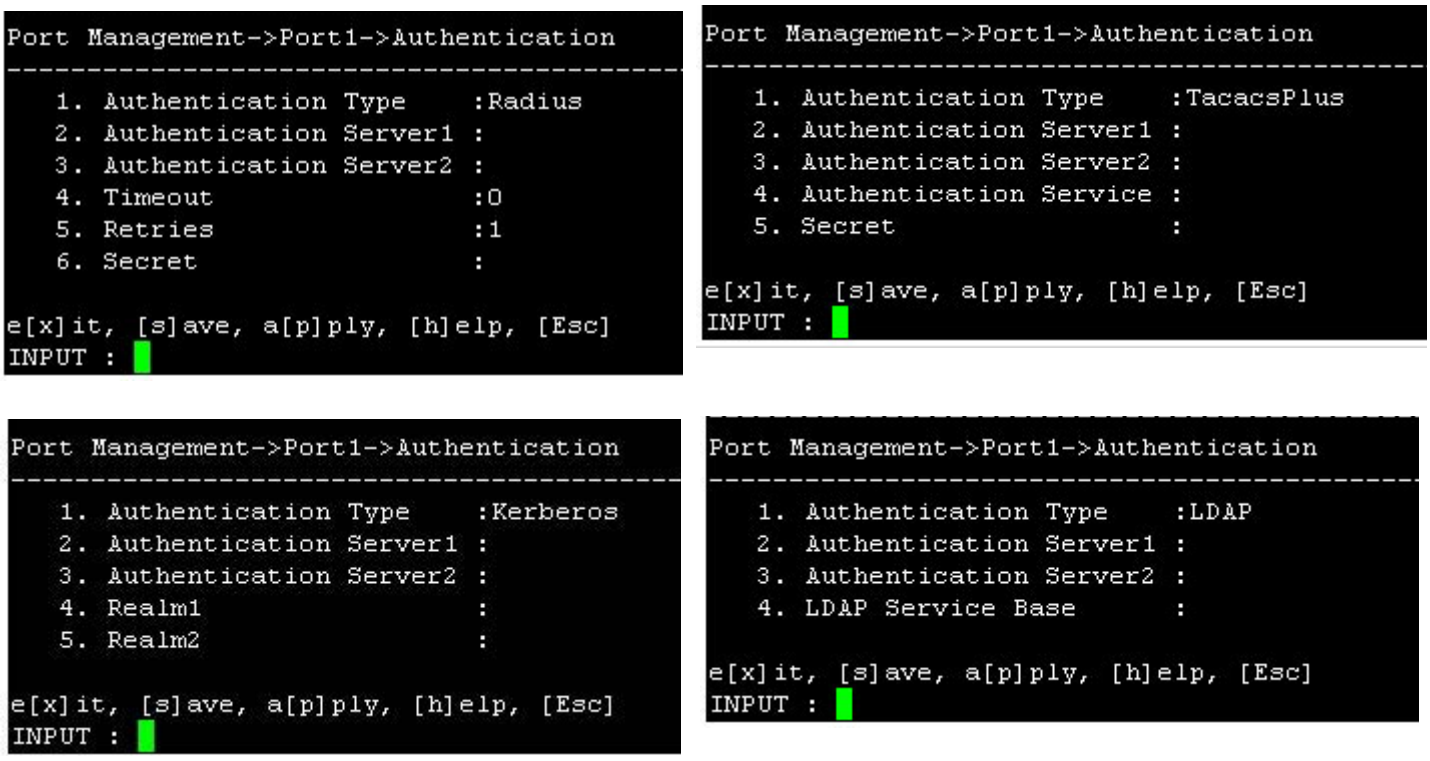


Figure 20- Authentication server configuration

Apply the appropriate authentication server IP addresses and additional configuration settings for your authentication method of choice.

Event Notification

From the Port Management menu, with Port x (any port) selected, press <**6**>-<**Enter**> to open the "Event Notification" menu.

From the Event Notification menu the user can configure what email address to send notice to when a port is disconnected from, and provide a separate email address (if desired) to send notice of connection. Either or both may also remain disabled (the default).

If the option is changed from "Disable" to "Enable", the menu will refresh and a setting will be provided to enter an email address to send notification to.

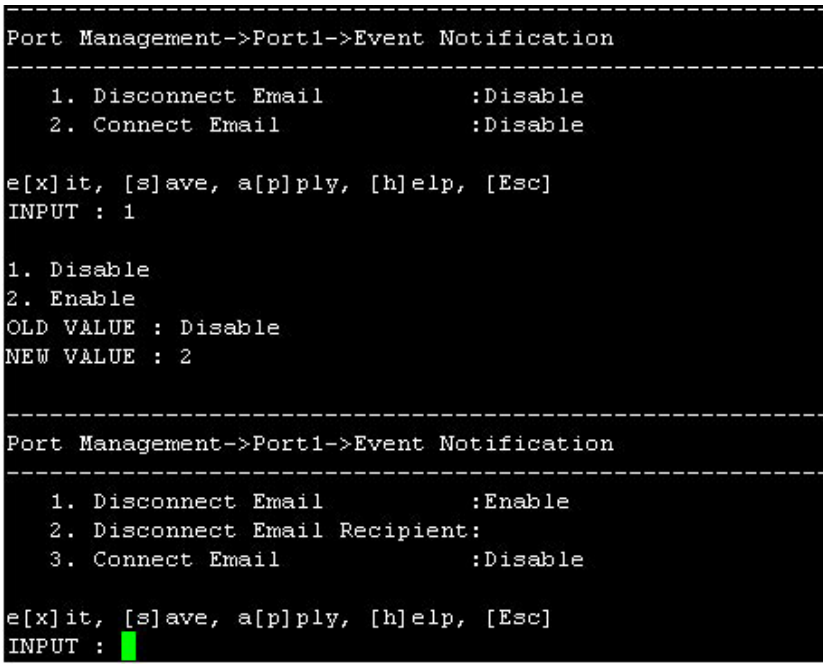


Figure 21- Port Management- event notification for Port 1

Port Access List

From the Port Management menu, with Port x (any port) selected, press <**7**>-<**Enter**> to open the "Port Access List".

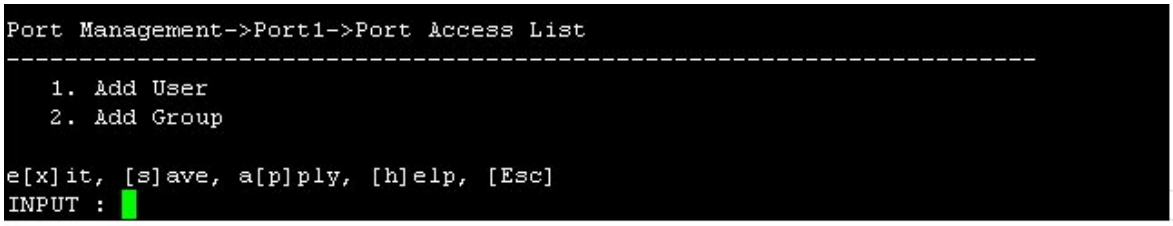


Figure 22- Port Management-port access list for Port 1

Each port can have individual user names and group names (pre-defined groups of users- see page 45) added to it that the connected device will recognize as valid users. These names are not limited to the user names that can access the SERIMUX menu. A user may connect to the SERIMUX using one name, and to a device with another. As long as the device recognizes the name and password provided, access will be granted.

Note: Users and Groups defined in the Port Access List will only effect user access when the port is configured as a "Host" port. When configured as a "User" port (page 17), all system users will have access to the SERIMUX through the port.

Press <**1**> to be provided a prompt to add a user name.

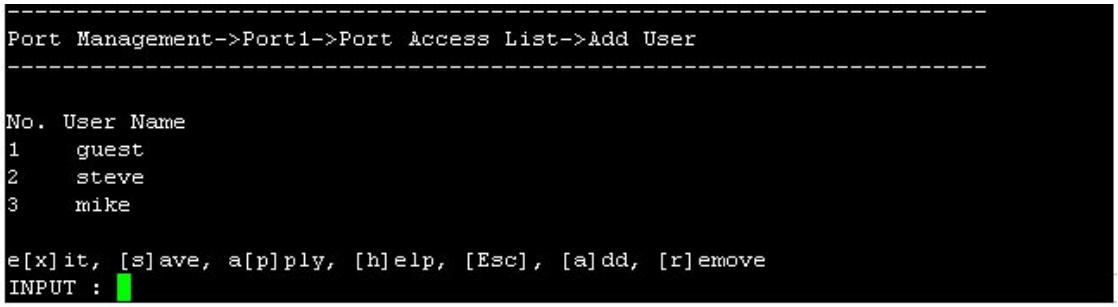


Figure 23- Port Management-add users to access list

Options "add" and "remove" have been added to your choices. Press <**a**> to be prompted to enter a name to add to the user list, or press <**r**> to be asked for the user number to remove from the list.

From the Port Access List menu (top of page), press <**2**>, then <**a**> (for add) to be shown the list of groups of users that have been formed (page 45) and may be assigned access to that port.

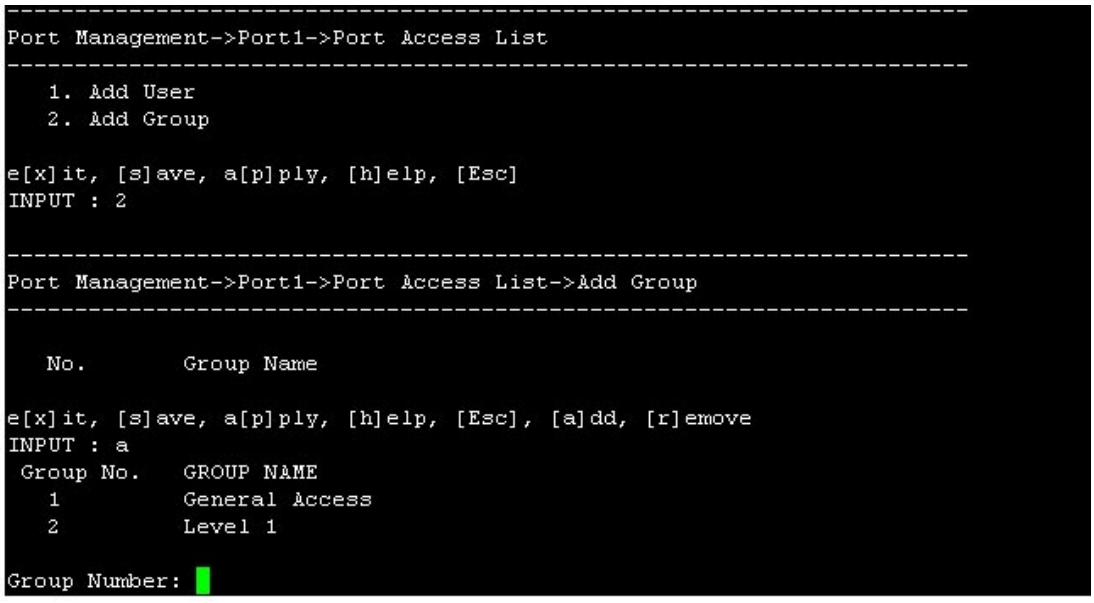


Figure 24- Port Management-add group to access list

To remove a group from the list, press <**2**> (from the Port Access List menu), then <**r**> (for remove). You will be prompted for the group number in the list to remove. Enter the group number and press <**Enter**> to remove it from the list.

```
------------------------------------------------------------------------
Port Management->Port1->Port Access List->Add Group
------------------------------------------------------------------------

   No.        Group Name
   1          General Access
   2          Level 1

e[x]it, [s]ave, a[p]ply, [h]elp, [Esc], [a]dd, [r]emove
INPUT : r
Remove Group No. :
```

Figure 25- Port Management- remove group from access list

Port Disconnect

From the Port Management menu, with Port x (any port) selected, press <**8**>-<**Enter**> to initiate disconnection of the port selected. You will be prompted "`Disconnect Port x (y/n)` ?" If <**y**> is entered, any connection made through port 1 will be disconnected. Press <**n**> or <**Esc**> to cancel the command.

```
Port Management->Port1
------------------------------------------------------------------------
   1. Port Setting
   2. Serial Setting
   3. Port Logging
   4. Modem Setting
   5. Authentication
   6. Event Notification
   7. Port Access List
   8. Port Disconnect
   9. Apply Common Settings

e[x]it, [s]ave, a[p]ply, [h]elp, [Esc]
INPUT : 8
 Disconnect Port 1 (y/n) ?
```

Figure 26- Port Management- disconnect Port 1

Apply Common Settings

To quickly apply settings to a port that are commonly used by many other ports, the "Apply Common Setting" option is provided. Once common settings are configured (page 17), this feature will help to save time in configuring a port for use.

From the Port Management menu, with Port x (any port) selected, press <**9**>-<**Enter**> to apply common settings to the selected port. You will be prompted "`Apply common port settings to port no. x(y/n)?`" If <**y**> is entered, the settings configured under "Common Settings" will be applied to the port. Press <**n**> or <**Esc**> to cancel the command.

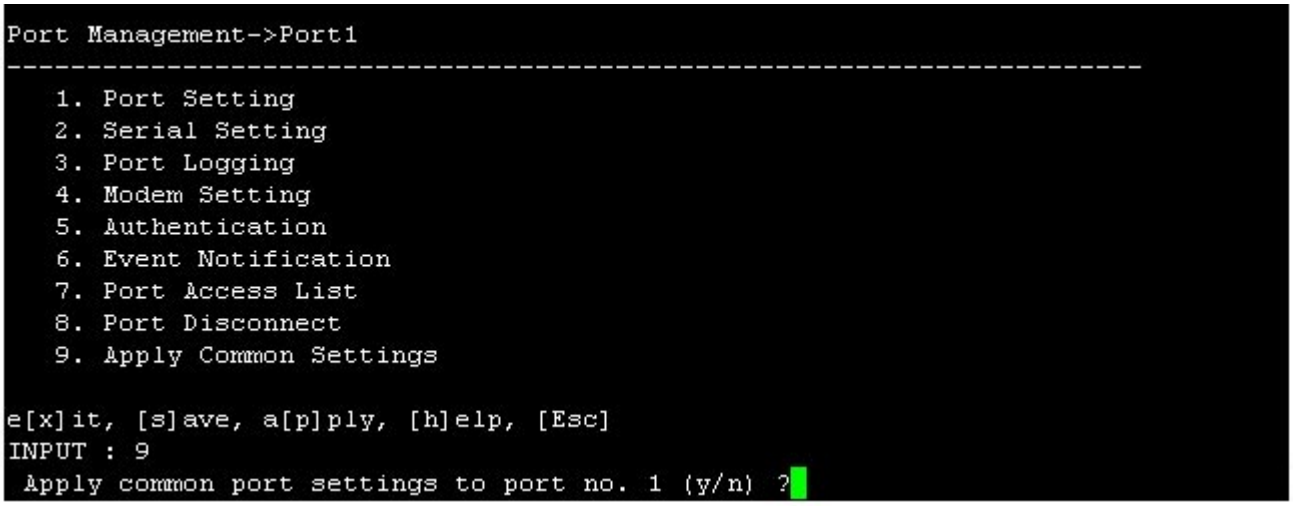


Figure 27- Port Management- apply common settings to Port 1

Using LDAP Server

To use Generic LDAP/Open LDAP server you can use the procedure below.

Note: Microsoft Active Directory is not compatible with the SERIMUX

1. In **Port Management** (page 16) select a Port you want to provide LDAP access for.
2. Change **Authentication Type** (page 20) to one of "LDAP" or "LDAP or local", "local or LDAP", "LDAP Down local"
3. Add **Service Base** DN (page 21) for your Users directory structure.

   Example "ou=people,DC=test,DC=example,DC=com"
4. Add your Users with the same username as in LDAP in the "**Port Access List**" section of Port Configuration (page 22). All users should have the same base DN. Please note that this user should already be added in **User Management -> System Users** (page 44).

LDAP authentication will work for the selected ports according to your Authentication Type now.

To use Radius authentication please refer to page 84. When using Radius, users are auto added to the Port List if authentication succeeds and does not require manual addition.

Device Management

From the Configuration menu, press <**2**> to open the Device Management menu. The Device Management menu lists each of the sensors that are being monitored by the SERIMUX. The menu lists (left to right) the sensor number, the RJ45 connector it is attached to (0 means it is an internal sensor), the type of sensor connected, and the user defined descriptions applied to the sensor.

```
------------------------------------------------------------------------
Device Management
------------------------------------------------------------------------
No.   RJ45 Conn.      Type                      Description
1     0               Temperature               Internal Temp.
2     0               Internal Power            Internal Power Status
3     0               Internal Fan              Internal Fan Speed
4     1               Temp. Combo               Server Rack Temp
5     1               Humidity Combo            Server Rack Humidity
6     2               Panic Button              Undefined

e[x]it, [s]ave, a[p]ply, [h]elp, [Esc]
INPUT :
```

Figure 28- Device Management menu

From this menu sensors can be added, removed, and have their settings configured. RS485 sensors that are connected will be automatically sensed and listed under "Type" at the connector they are attached to. Contact sensors must be manually connected.

Add a Contact Sensor

To add a contact sensor, the sensor must first be connected to an available port on the SERIMUX. Press <**a**> at the cursor and be asked which RJ45 connector the sensor is to be assigned to. If only 1 connector has not been assigned, then only 1 connector will be made available for assignment. If no connectors are available, you will receive the response "**`All RJ45 Connectors are in use.`**"

With an available connector chosen, select the contact sensor type and press **`<Enter>.`**

Connector 1 is in use.

The only available connector

Select sensor type

```
------------------------------------------------------------------------
Device Management
------------------------------------------------------------------------
No.   RJ45 Conn.      Type                      Description
1     0               Temperature               Internal Temp.
2     0               Internal Power            Internal Power Status
3     0               Internal Fan              Internal Fan Speed
4     1               Temp. Combo               Server Rack Temp
5     1               Humidity Combo            Server Rack Humidity

e[x]it, [s]ave, a[p]ply, [h]elp, [Esc]
INPUT : a
No.    RJ45 Conn.
2. RJ45 Connector 2
SELECT CONNECTOR:2
No.   .          Sensor Type
1.    Water
2.    Smoke
3.    Vibration
4.    Motion
5.    Glass Break
6.    Door
7.    Keypad
8.    Panic Button
9.    Key Station
10.    Dry Contact
SELECT TYPE:
```

Figure 29- Adding a sensor

Remove a Sensor

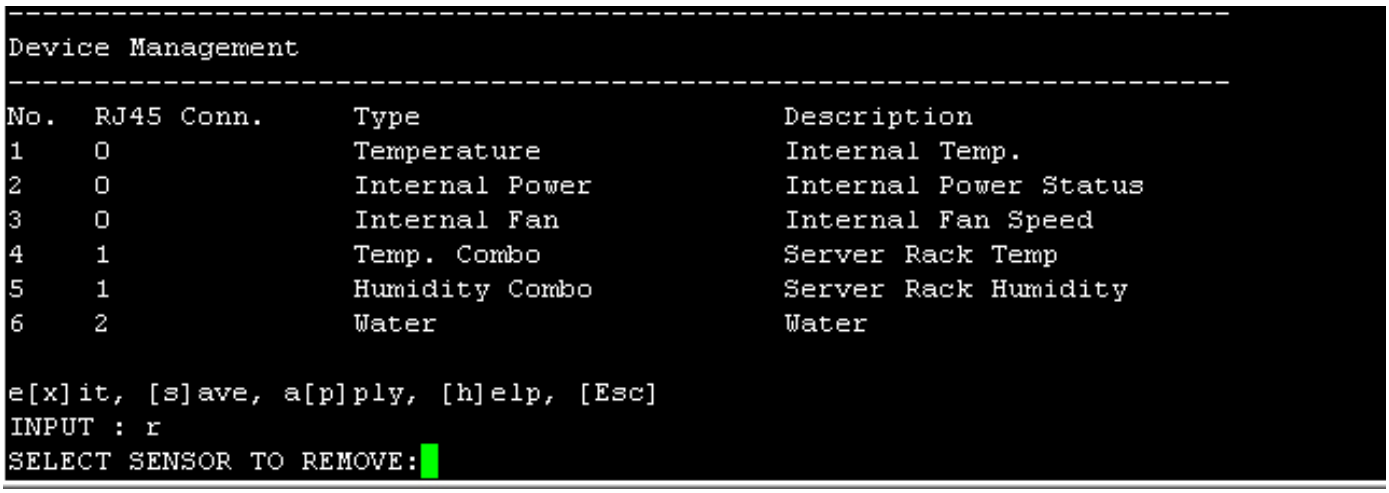


Figure 30- Remove a Sensor

To remove a sensor, press <**r**> at the cursor to be asked to "**SELECT SENSOR TO REMOVE:"** . Enter the connector number and press <**Enter**>. Unplug the sensor from the SERIMUX.

Note: If the sensor is an RS485 type sensor (page 61) and remains connected to the SERIMUX, the sensor will be immediately auto-discovered by the SERIMUX and added back to the sensor list with the description "Undefined".

Configure a Sensor

To configure the settings for a sensor, from the Device Management menu enter the sensor number (listed under "No." in the image above) at the cursor and press <**Enter**>. A list of sensor setting topics will be presented to choose from.

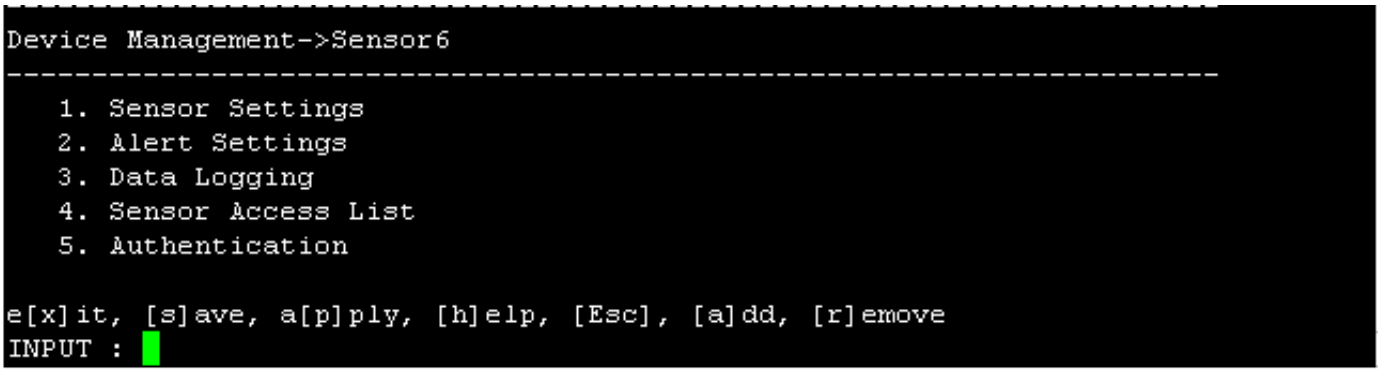


Figure 31- Sensor configuration topics

Category	Description
Sensor Settings	Menu options allow the user to change the description and various sensing criteria depending upon the type of sensor selected
Alert Settings	A sensor can be configured to notify a user via e-mail alerts or SNMP traps (v1,v2c); alerts are always logged to Syslog messages.
Data Logging	Options to enable and configure data logging settings
Sensor Access List	Select which users (local users only) and which groups will have access to sensor readings
Authentication	Choose between Local or none. None means the sensor can be viewed by any user. Local means the sensor can be viewed by only the users/groups in the sensor access list.

Sensor Settings

The options that can be configured under “Sensor Settings” will vary depending on the type of sensor selected. As you can see in Figure 32 and Figure 33, the criteria can vary considerably.

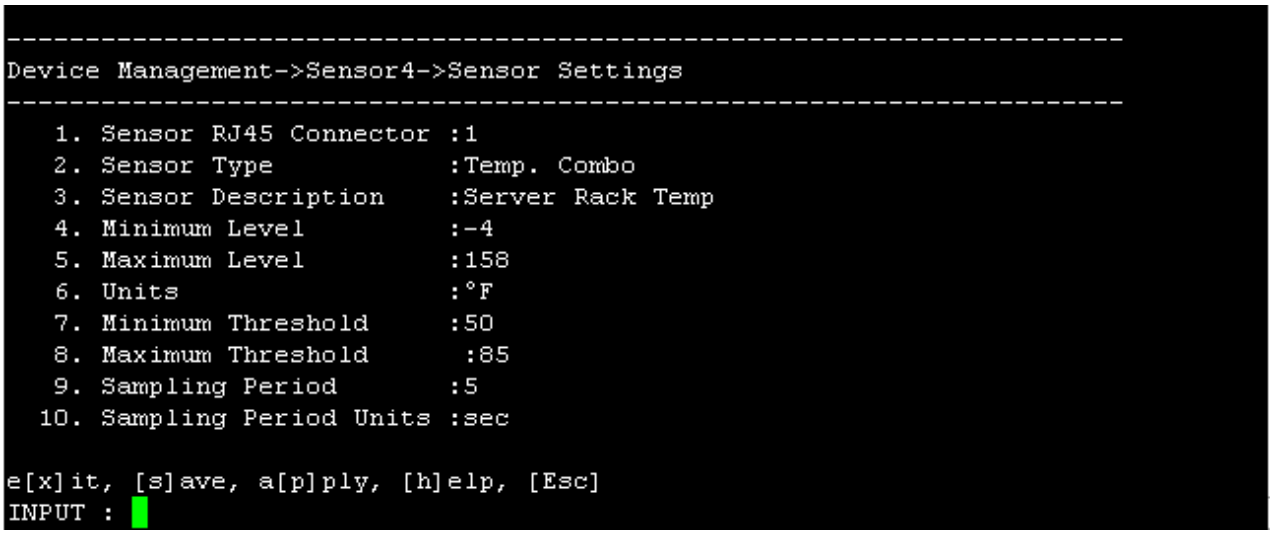


Figure 32- Sensor settings for temperature sensor

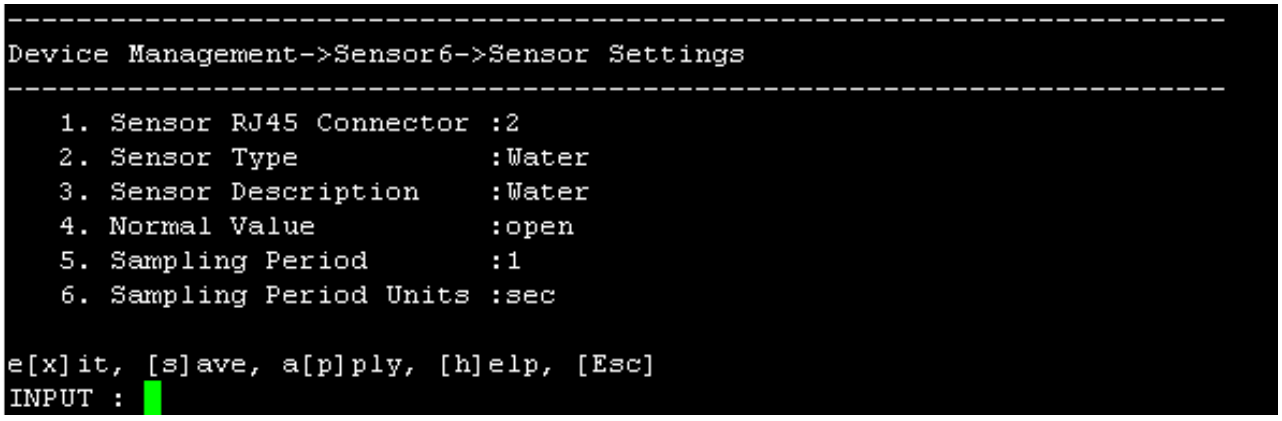


Figure 33- Sensor settings for water sensor

Field	Description
Sensor RJ45 Conn.	Value cannot be changed
Sensor Type	Value cannot be changed
Sensor Description	Each sensor can be given a unique description. Descriptions can be from 1-80 characters in length and include most characters. They cannot contain a backslash (\ ) or quotation mark ("). Descriptions will be used in e-mail alerts in the DESCRIPTION field.
Normal Value	(only for contact sensors) value in non-alert state is either “Open” or “Closed”
Minimum Level	The minimum value the sensor can report- default values are applied automatically (changing them is not recommended)
Maximum Level	The maximum value the sensor can report- default values are applied automatically (changing them is not recommended)
Units	(only for Temperature sensors) This lets the operator choose between Celsius and Fahrenheit as the temperature measurement unit.
Minimum Threshold	The minimum acceptable value to be measured before switching the sensor to alert status
Maximum Threshold	The maximum acceptable value to be measured before switching the sensor to alert status
Sampling Period	Determines how often the displayed sensor value is refreshed. A numeric value (1-999) should be entered
Sampling Period Units	A measurement unit for the sampling period should be entered (seconds or minutes)

For more on sensor settings, see page 65. Be sure to save changes before exiting.

Alert Settings

Under Alert Settings, the sensor can be configured to send alert messages or not. If enabled, various criteria for alert messages can be defined.

Figure 34- Sensor alert settings

Field	Description
Disable Alert	Yes or No If NO, no alert messages will be sent when the sensor is in alert status
Alert Delay	an amount of time the sensor must be in an alert condition before an alert is sent. This provides some protection against false alarms. The Alert Delay value can be set for 0-999 (seconds or minutes).
Alert Delay Units	Seconds or minutes
Notify Again After	Specifies the amount of time before an alert message is repeated. The repeated alert can be set to occur from 1-999 (seconds, minutes, or hours).
Notify Again Units	seconds, minutes, or hours.
Notify when return to normal	The user can also be notified when the sensor readings have returned to the normal range by enabling this feature for a sensor.
Auto Acknowledge alert on condition clear	Enable this to have alert notifications in the summary page return to normal state automatically when sensor readings return to normal.
Email Alert Enable	Choose whether or not alert messages should be sent via email
Email Recipient	Enter a valid email address that alert messages should be sent to regarding this sensor.
SNMP Notification	Choose whether or not alert messages should be sent via SNMP
Notification Address	Enter a valid SNMP address that alert messages should be sent to regarding this sensor.

Be sure to save changes before exiting.

Data Logging

Under Data Logging, the sensor can be configured to record readings reported by the sensor and to record syslog messages of alert events.

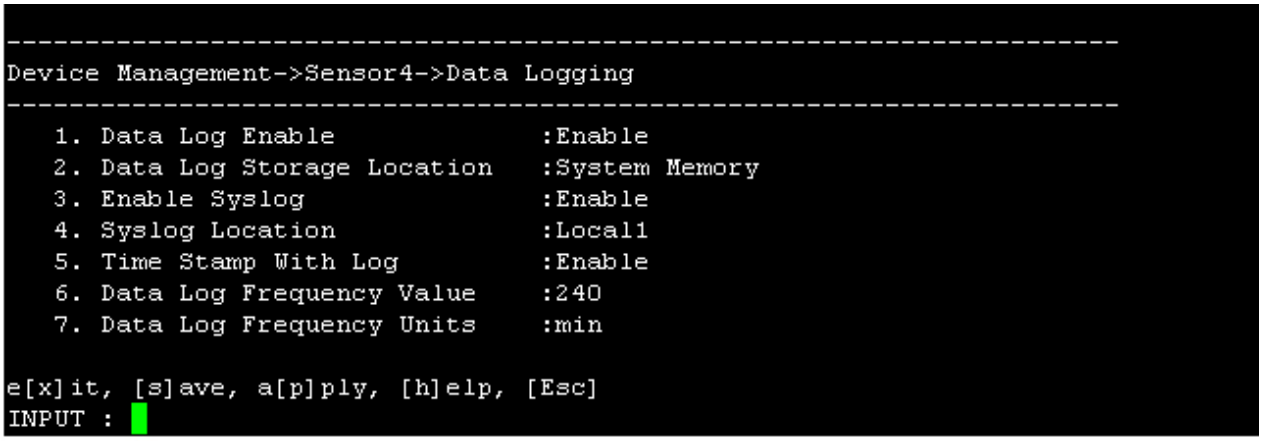


Figure 35- Sensor Data Logging

Field	Description
Data Log Enable	Enable or Disable If disabled, data log readings from the sensor will not be recorded
Data Log Storage Loc.	The only location they can be stored at this time is in system memory.
Enable Syslog	The recording of alert message via syslog from the sensor can be enabled or disabled.
Syslog Location	Syslog messages can be recorded in locations “Local1” through “Local6”. (See Syslog configuration- page 75- for more on this)
Time Stamp With Log	Determine whether a time stamp should be included with each syslog record.
Data Log Frequency Value	a value to determine how frequently data log entries should be recorded. The value can be set for 0-999 (seconds or minutes.)
Data Log Frequency Units	seconds or minutes

Be sure to save changes before exiting.

Sensor Access List

Use the Sensor Access List to define who will have access to sensor readings.

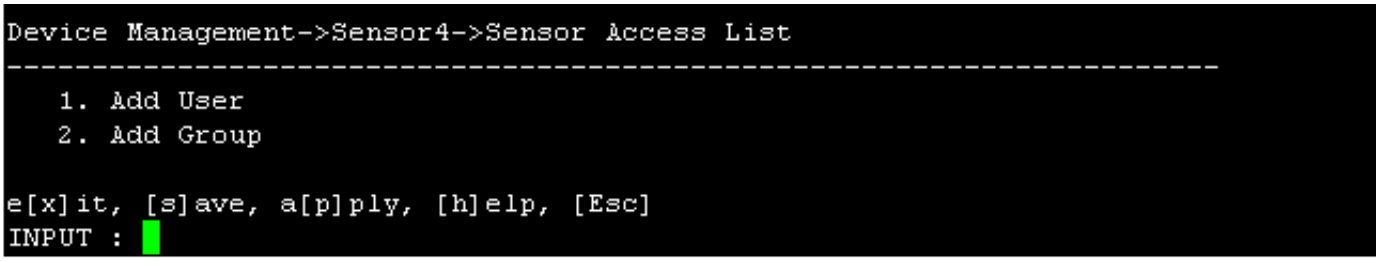


Figure 36- Sensor Access List

Add User: Add users that will have access to sensor readings when sensor authentication is set to “Local”. Usernames added must be valid users with access to the SERIMUX as defined under “System Users” (page 44).

Add Group: Add group names as defined under “Access Groups” (page 45) to quickly define who will have access to sensor readings when Sensor Authentication is set to “Local”.

Sensor Authentication

Sensor Authentication Type: Choose between Local or none. None means the sensor can be viewed by any user. Local means the sensor can be viewed by only the users/groups in the sensor access list (page 29).

Figure 37- Sensor user authentication

Note: Only local authentication is supported for sensors.

Network Management

From the Configuration menu, press <**3**> to open the Network Management menu. The Network Management menu provides selections to open configuration menus for the “Ethernet 1” and “Ethernet 2” ports on the SERIMUX as well as web server configuration and TCP keepalive settings. .

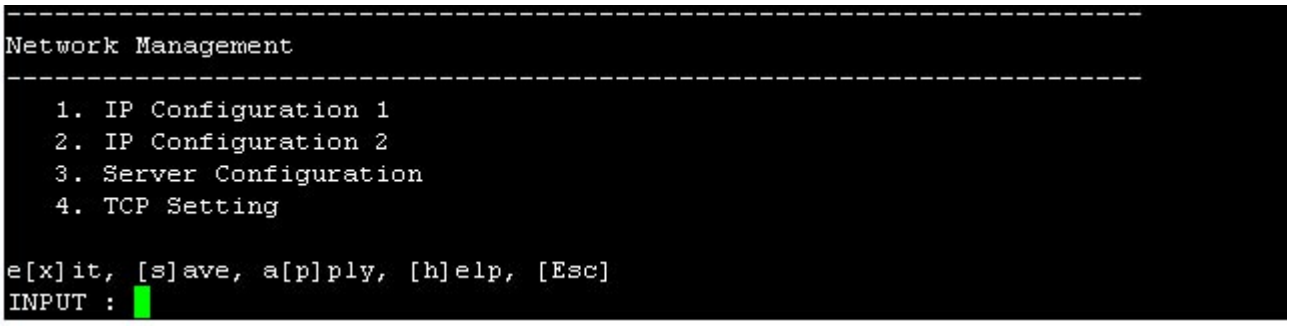


Figure 38-Network Management menu

IP Configuration

The IP Configuration 1 and 2 menus are used to configure the Ethernet ports and enable the SERIMUX to connect to the local LAN or Internet. Only one connection is necessary, but two can be configured for remote SERIMUX access redundancy.

From the Network Management menu, either press <**1**>-<**Enter**> or <**2**>-<**Enter**> to open configuration menus for Ethernet port 1 or 2 (respectively).

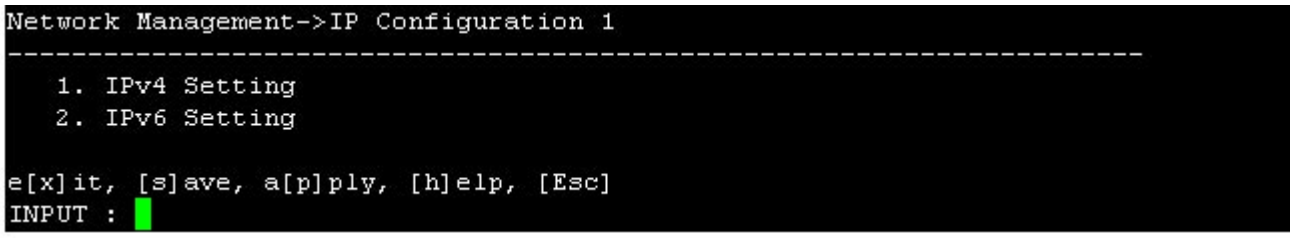


Figure 39- Network Management-IP Configuration

Press **<1>-<Enter>** to open configuration menu for IPv4 Settings or press **<2>-<Enter>** to open configuration menu for IPv6 settings.

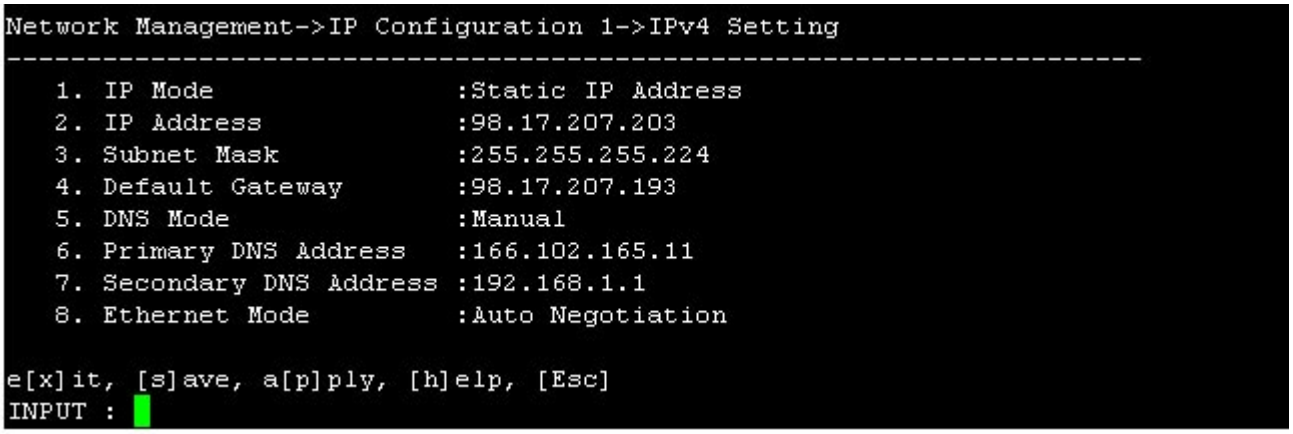


Figure 40- Network Management-IPv4 settings

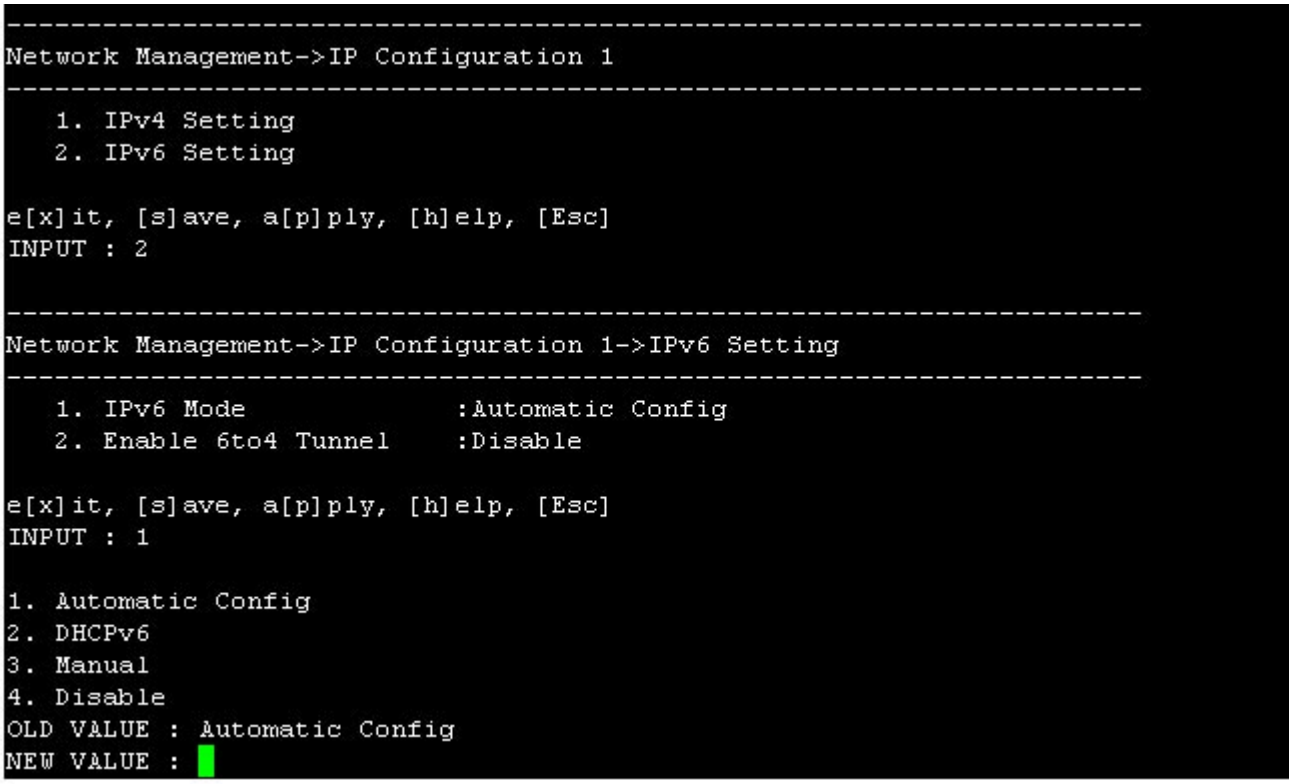


Figure 41- Network Management- IPv6 settings

Be sure to apply valid information in the fields provided.

Default Settings include:

- IP address: 192.168.1.91
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

The Ethernet Mode in the IPv4 settings can be set for :

- 100 Base T Full Duplex
- 100 Base T Half Duplex
- 10 Base T Full Duplex
- 10 Base T Half Duplex
- Auto Negotiation (default setting)- to allow the SERIMUX to select what will work best for your connection.

When configuring IPv6 settings, if the mode is set at “Manual”, additional menu items will appear to apply the IP Address and Gateway settings.

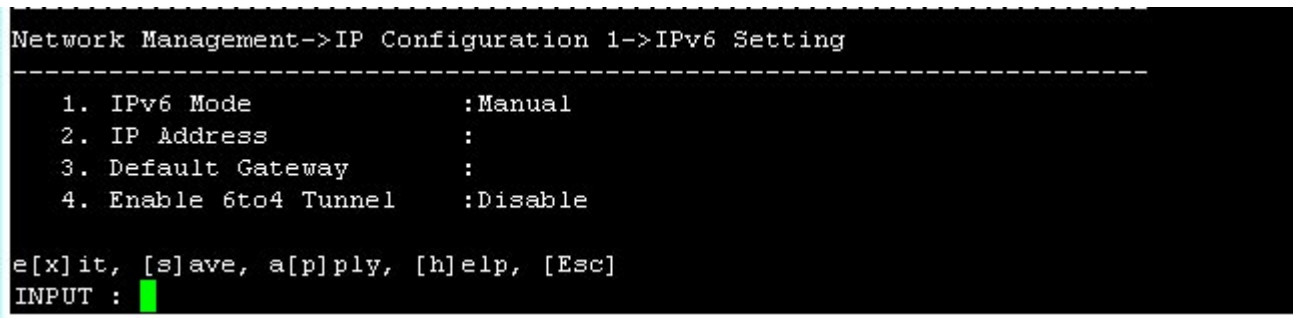


Figure 42- Network Management-IPv6 manual IP assignment

Server Configuration

The Server Configuration section is provided to apply settings for Web Server connection and behavior as well as the SMTP server for e-mail functions.

From the Network Management menu, press <**3**>-<**Enter**> to open Server Configuration menus.

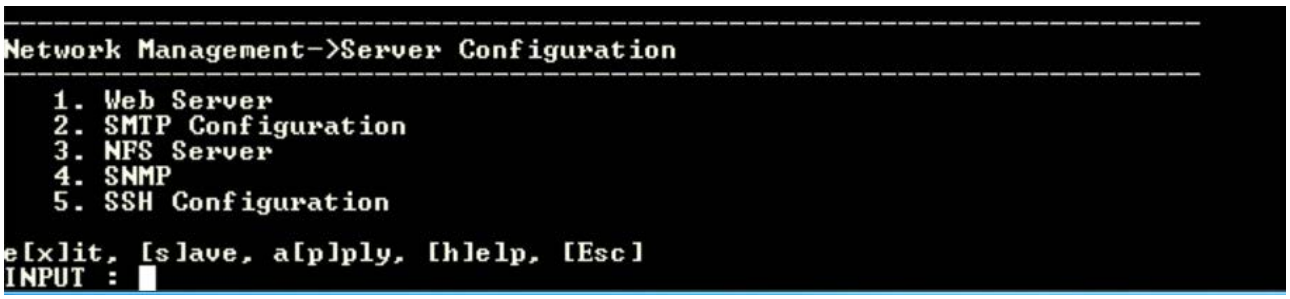


Figure 43-Network Management- Server Configuration

From the Server Configuration menu, press <**1**>, <**2**>, <**3**> or <**4**> -<**Enter**> to open the Web Server, SMTP server, NFS server, SNMP or SSH configuration menus. (See the table on page 35 for configuration values.)

Figure 44- Network Management- Web Server settings

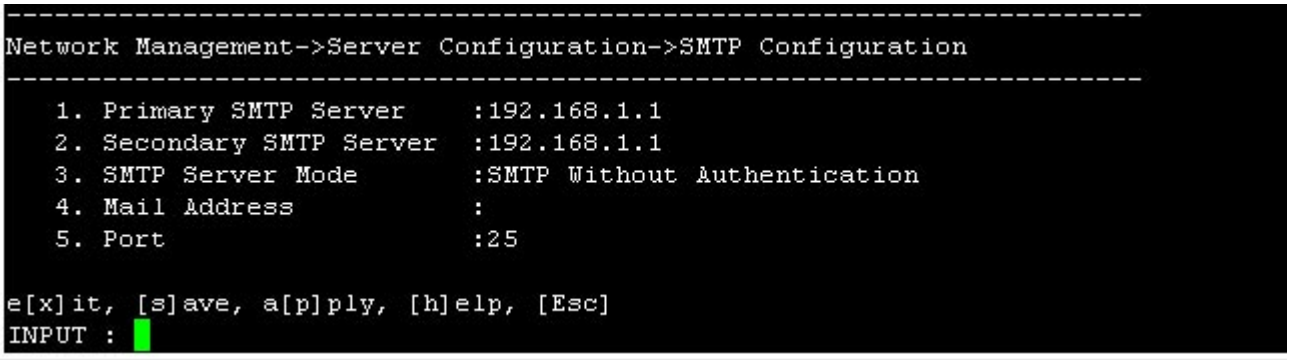


Figure 45- Network Management- SMTP server settings

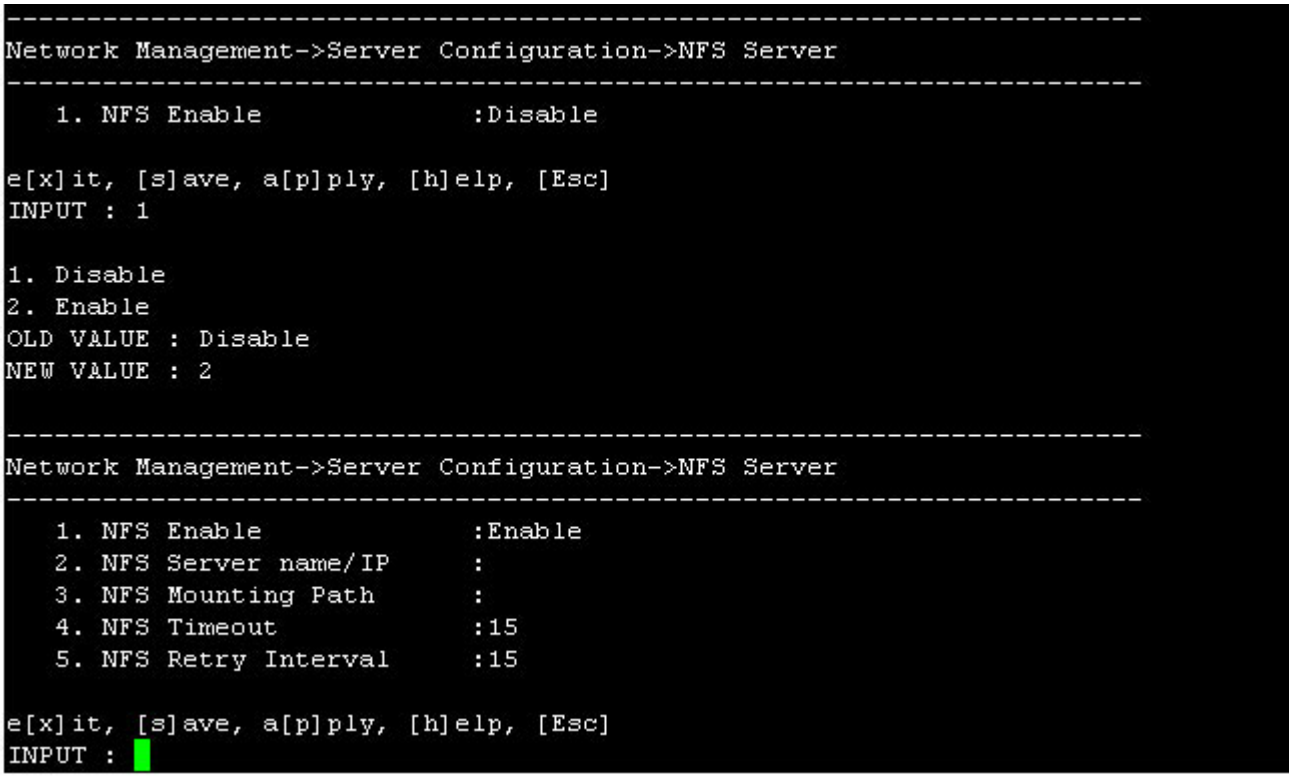


Figure 46- Network Management- NFS server configuration

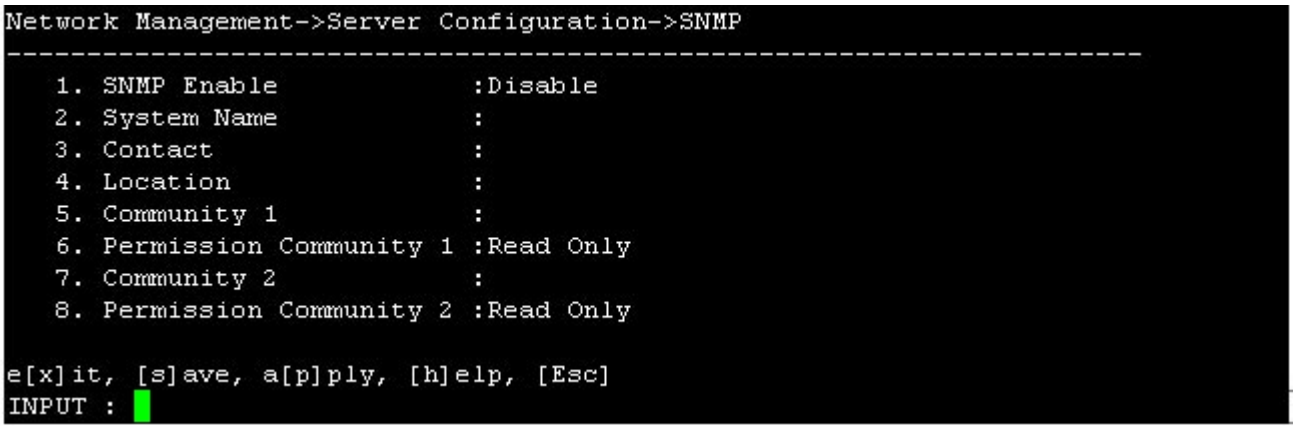


Figure 47- Network Management-SNMP configuration

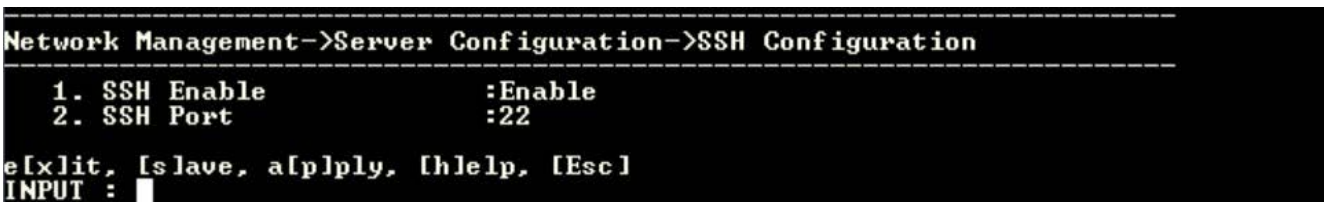


Figure 48- Network Management- SSH configuration

See table on page 35 for configuration values.

Server Configuration Settings:

Setting	Value
Web Server	
Web Page Refresh Rate (sec)	0-999 seconds
Login Timeout (minutes)	0-999 minutes
Authentication Type	Many including local, Radius, Tacacs, TacacsPlus, Kerberos, LDAP, or combinations
HTTP Port	0-65535
HTTPS Port	0-65535
HTTP Enable	Enable or Disable (Disable forces all users to login via SSH)
SMTP Configuration	
Primary SMTP Server	Apply valid IP address
Secondary SMTP Server	Apply valid IP address
SMTP Server Mode	SMTP with or without authentication required
Mail Address	e-mail address assigned to the SERIMUX to use for sending messages
Port	Port on which the SERIMUX will communicate with SMTP server (default =25)
NFS Configuration	
NFS Enable	The default is disabled. Enable to expand the page and apply configuration settings for an NFS server, mounting path, timeout period, and retry interval.
SNMP Configuration	
SNMP Enable	Enable or Disable
System Name	Up to 50 characters
Contact	Up to 50 characters
Location	Up to 50 characters
Community 1	Name– example “private”
Permission Community 1	Read only / read-write
Community 2	Name – example “public”
Permission Community 2	Read only / read-write
SSH Configuration	
SSH Enable	Enable or Disable
Port	Port on which the SERIMUX will communicate via SSH (default =22)

SNMP

The SERIMUX can send alerts as SNMP traps for all port connect/disconnect events. Using an SNMP MIB browser, a user can monitor all settings. The SNMP agent supports both SNMPv1 and SNMPv2.

Note: The SNMP MIB file (serimuxsec.mib), for use with an SNMP MIB browser, can be found at http://www.networktechinc.com/download/d-srvsw-term-ssh.html . Click on the link to open the file, then save the file to your hard drive to use with the SNMP MIB browser.

TCP Setting

Settings are provided to apply values for TCP keepalive parameters. A **keepalive** is a message sent by one device to another (remote or local) to check that the link between the two is operating.

From the Network Management menu, press <**4**>-<**Enter**> to open the “TCP Setting” menu.

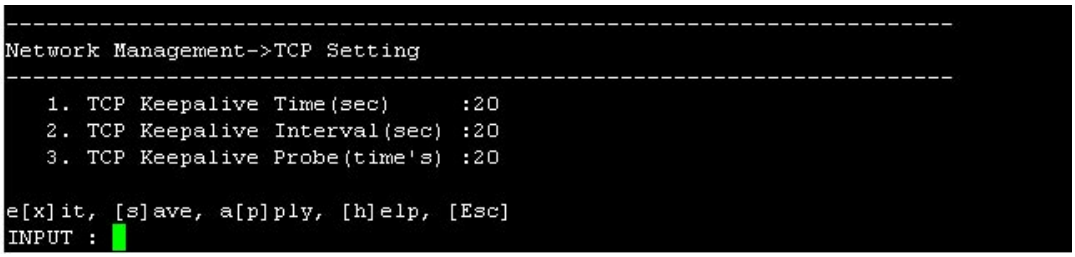


Figure 49- Network Management-TCP settings

Keepalive time is the duration between two keepalive transmissions in idle condition. TCP keepalive period is configurable and by default is set to 20 minutes. The range of acceptable values is 0-999 minutes.

Keepalive Interval is the duration between two successive keepalive retransmissions, if acknowledgement to the previous keepalive transmission is not received. The default value is 20 minutes, and the range of acceptable values is 0-999 minutes.

Keepalive Probe is the number of retransmissions to be carried out before declaring that remote end is not available. The default value is 3, and the range of acceptable values is 0-999.

Administration Settings

From the Configuration menu, press <**4**>-<**Enter**> to open the "Administration Settings" menu. The Administration Settings menu provides selections to configure the SERIMUX name, root password, date and time, security, and syslog. It also includes a selection for performing firmware updates.

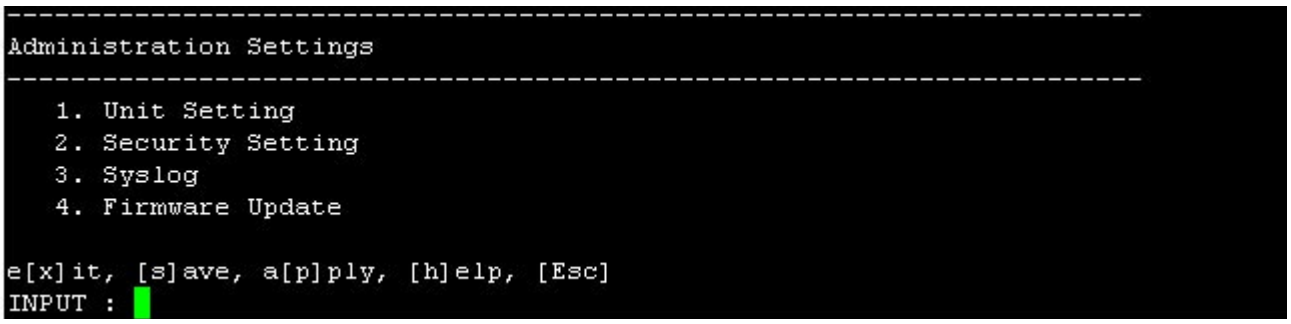


Figure 50- Administration Settings

Unit Settings

The Unit Setting menu has fields for setting up the name for the SERIMUX, the password for user "root", and the system date and time settings.

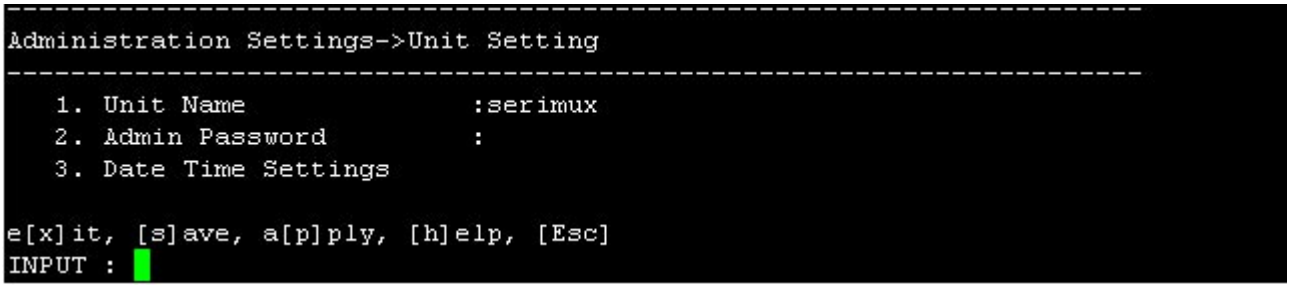


Figure 51- Administration Settings-Unit Settings

From the "Administration Settings" menu, press <**1**>-<**Enter**> to select "Unit Settings". Configure as desired:

Setting	Description	Value
Unit Name	Name for the SERIMUX	Maximum of 50 Characters- Alphabetical or Numeric
Root Password	Password for user "root" **This menu selection is only accessible if user "root" is logged in**	Maximum of 50 Characters- Alphabetical or Numeric- **Case Sensitive** (default is "**nti**")
Date and Time Settings	Apply current date and time-or enable NTP server	Valid date format mm/dd/yy / Enable NTP

FYI- The SERIMUX complies with the new U.S.-Daylight Saving Time rules (passed in 2005).

Unit Setting->Change Admin Password

From "Unit Setting", press <**2**>-<**Enter**> to select "Admin Password". The administrator can change the default Admin password for user "root" from "**nti**" to a new password.

Type the desired password (maximum 50 ASCII characters- case sensitive) and press <**Enter**>
Retype the new password exactly as it was just typed and press <**Enter**> .

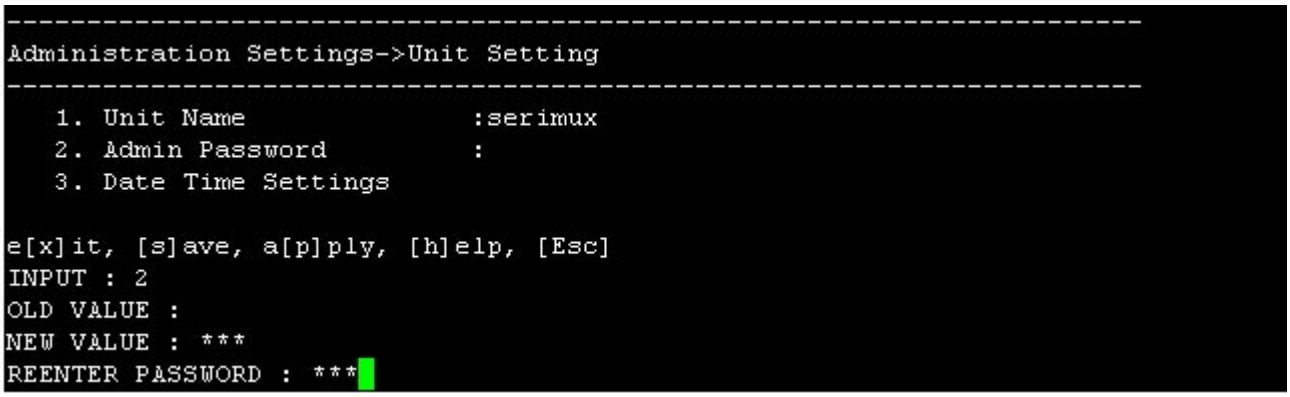


Figure 52-Unit Settings-change password

Be sure to press "**Save**" to have the change take effect after the next reboot of the SERIMUX, or "**Save & Apply**" to have the change take effect immediately.

NOTE: The password entered will be case sensitive so be sure to note what characters are upper or lower case if any are alphabetical. The password characters are displayed as '*' (asterisk) characters while entering them.

Unit Settings->Date Time Settings

The Date and Time of the SERIMUX can be either manually setup to use an onboard clock or set to be synchronized with an NTP server. From "Unit Setting", press <**3**>-<**Enter**> to select "Date Time Settings".

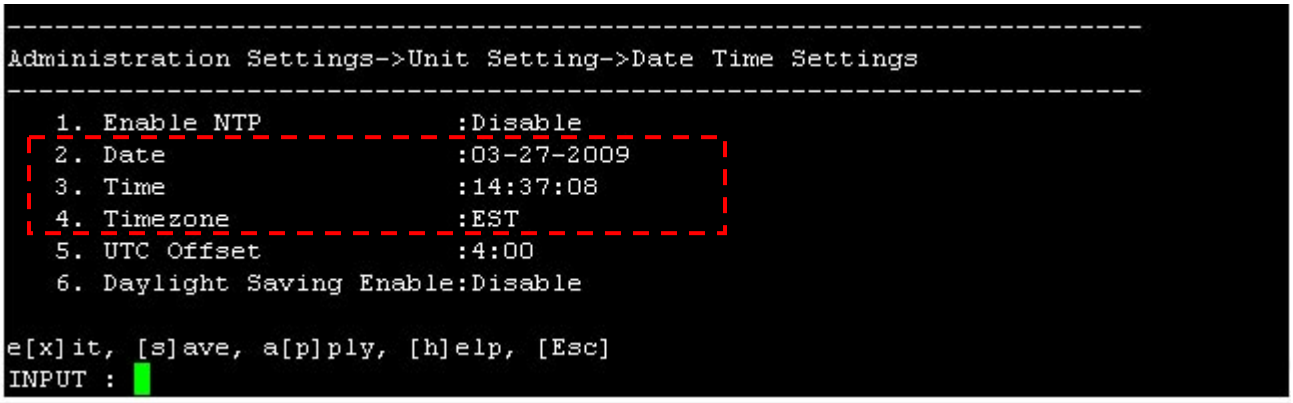


Figure 53- Unit Settings-manual date and time

To set the SERIMUX date and time manually, set the "Enable NTP" value to "Disable". Enter values for:

- date in mm-dd-yyyy format
- time in 24 hour format hh:mm:ss
- time zone for the location of the SERIMUX

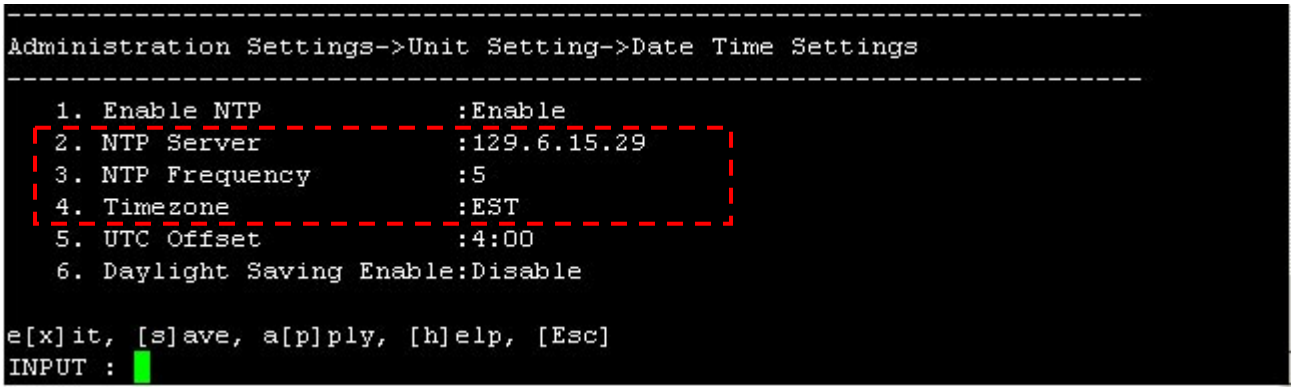


Figure 54-Unit Settings-NTP Server settings

To synchronize the SERIMUX with an NTP Server, set the "Enable NTP" value to "Enable". Enter values for:

- IP address of the NTP Server
- Frequency (how often, in hours (0-99), the SERIMUX will query the NTP Server)
- time zone for the location of the SERIMUX

UTC Offset

The UTC offset is the offset in hours from GMT (if you are located in GMT, the value is "00.00"). The UTC offset value is hh.mm (hours.minutes). If you are behind GMT, the value will be negative (i.e. "-02.00"). If you are ahead of GMT, the value will be positive (i.e. "+02.00" or "02.00").

Daylight Savings Enable

In order to have the time change in accordance with Daylight Saving Time rules, set the value of "Daylight Saving Enable" to "Enable" and select the appropriate time zone in the "Daylight Time zone" box. Also be sure to apply proper Start Date/Time and End Date/Time values to defiine Daylight Saving Time begins and ends.

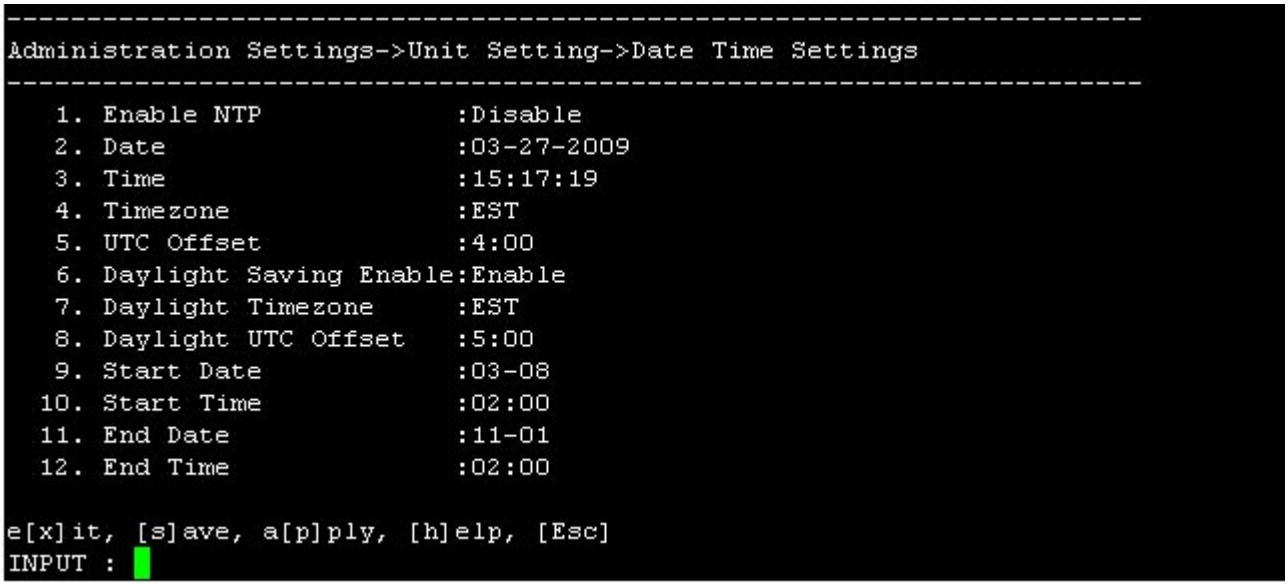


Figure 55- Unit Settings-Daylight Savings

Security Settings

Security settings enable the administrator to configure the CLI (Command Line Interpreter) authentication type to be used to connect with serial devices through the web interface or through the SERIMUX shell. Choose from various common CLI authentication methods.

From this menu you can also Enable or Disable Telnet access for logging in.

From the “Administration Settings” menu, press <**2**>-<**Enter**> to select “Security Setting”.

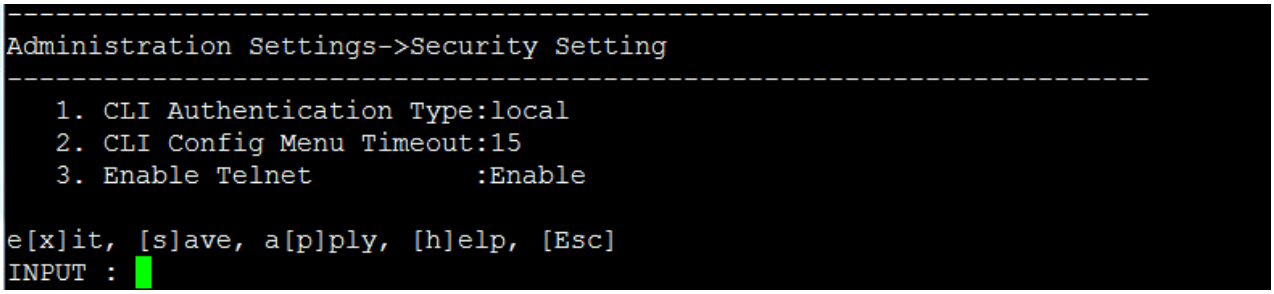


Figure 56- Administration Settings-Security Setting

Press <**1**>-<**Enter**> to open a list of CLI Authentication options.

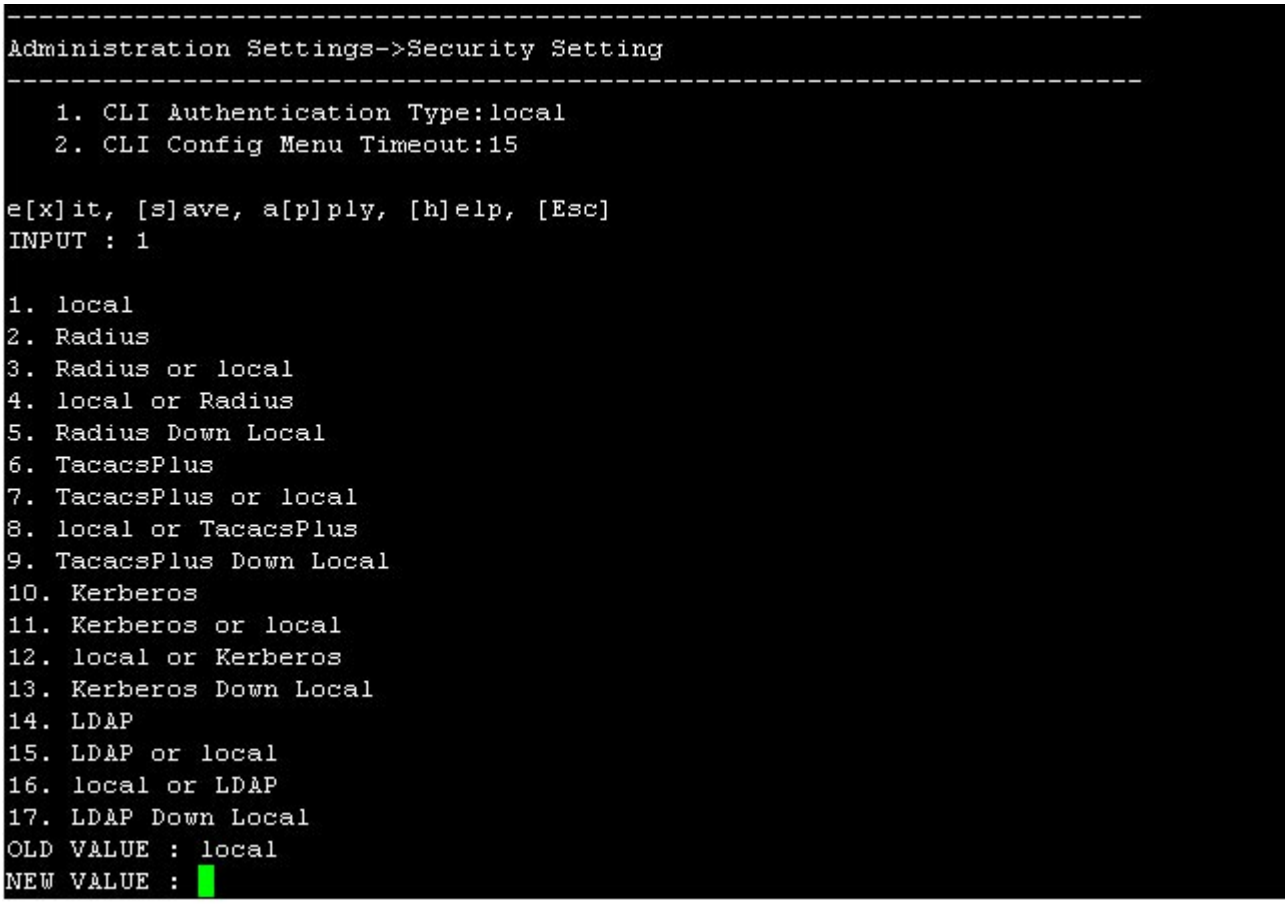


Figure 57- Administration Settings-CLI Authentication Types

Authentication options that include Radius, TacacsPlus, Kerberos, and LDAP will require additional configuration when selected.

Note: In order to access ports or the configuration menu through the web or the shell, all users must be added to the system (page 44) irrespective of the authentication type. Users connecting with devices directly (page 13) will only be restricted access by port authentication (page 20) and by the user access limitations of the device itself.

Configuration options for CLI authentication are the same as those shown under Port authentication (page 21), except that an additional option for setting the CLI Config menu timeout is present.

The CLI Config Menu Timeout is the time period (in minutes) before an idle user will be automatically exited from the configuration menu and returned to their point of connection when logging into the SERIMUX. The valid entry for this time period is 0-99 minutes. A value of 0 disables the timeout. If a user connects to the Configuration menu automatically at login, then they will need to login again to reconnect to the Configuration menu in the event of a timeout.

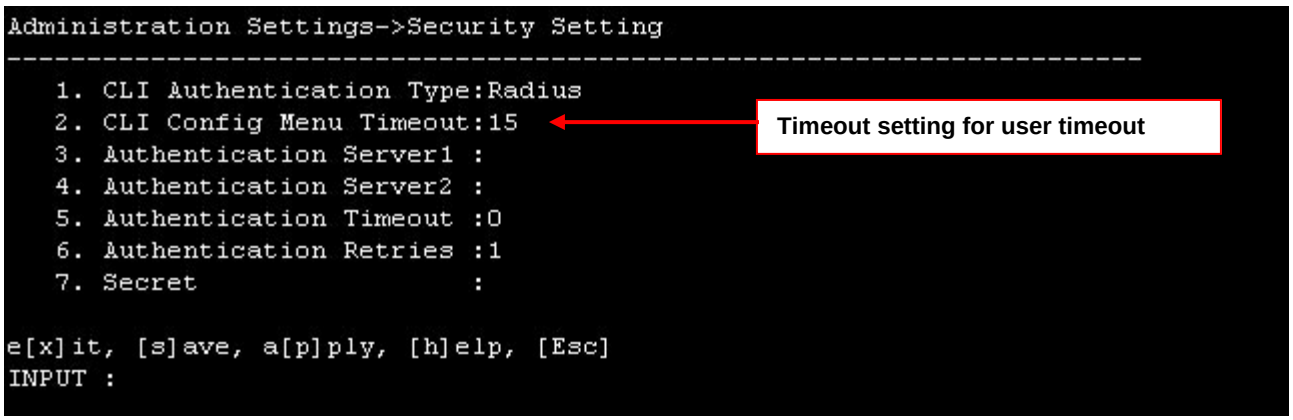


Figure 58- Administration Settings-Security-CLI Authentication

If the CLI Config Menu Timeout is changed while other users are already logged in, the change will not effect those users until their next login.

Suggestion: Users that are configured to have admin rights should be configured to either open to the Port Connect Menu or to the Config Menu, not to the shell. When the configured time period for the CLI timeout expires, administrative users will not be logged out if they open to the shell. They can quickly reenter the Config Menu by typing <serimuxconfig> at the shell prompt.

Syslog

The Syslog menu contains the settings that effect the location, size, name, and destination when downloaded of the System Log. The System Log displays a listing of all user that have logged in and out of the SERIMUX, providing the date and time of their login and logout. It also displays when configuration changes are made. From the Syslog menu, log records can be deleted to make room for more.

From the "Administration Settings" menu, press <**3**>-<**Enter**> to select "Syslog".

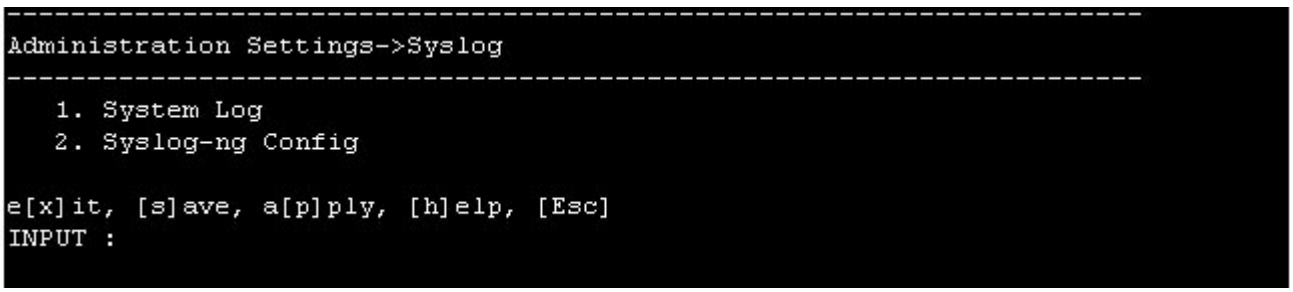


Figure 59- Administrative Settings-Syslog

Press <**1**>-<**Enter**> to open the menu for System Log settings, or <**2**>-<**Enter**> to open the Syslog-ng Configuration menu.

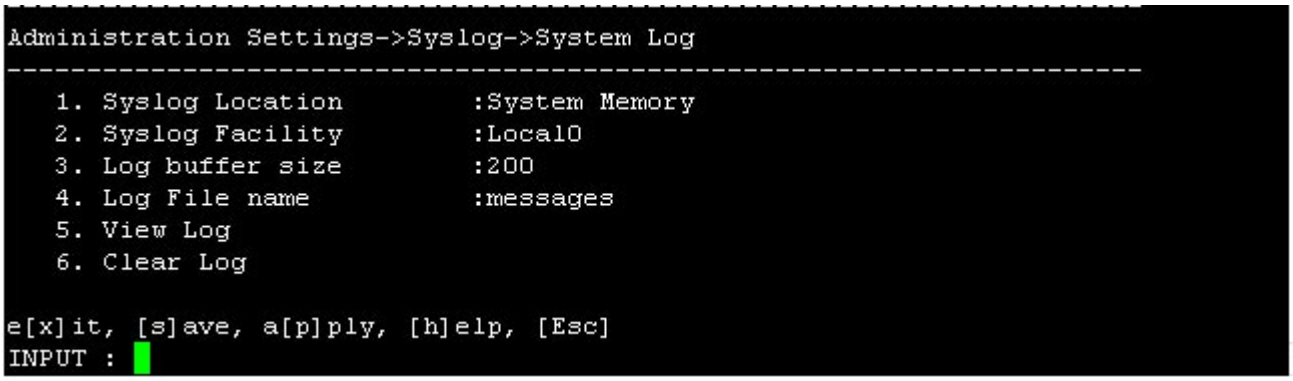


Figure 60- Administration Settings-System Log settings

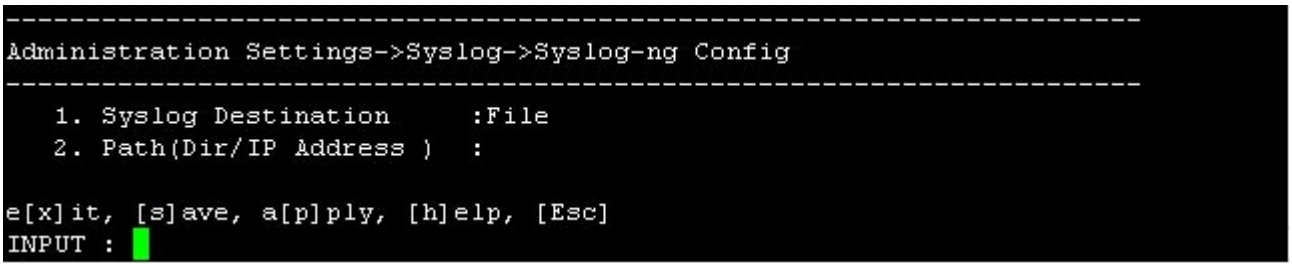


Figure 61- Administration Settings-Syslog-ng Configuration

Setting	Value
System Log Settings	
Syslog Location	System Memory (no options as of this printing)
Syslog Facility	Local0 (no options as of this printing)
Log Buffer Size	0-999 K bytes
Log File name	1-100 characters
View System Log	None- view accumulated system logs
Clear System Log	delete system logs
Syslog-ng Config	
Syslog Destination	File / TCP / UDP
Path	drive and directory (when destination is File), or IP address (when destination is TCP or UDP)

To store Syslog data in locations other than on the SERIMUX, configure the Syslog-ng Config settings for writing it to a flash drive, NFS, or sending it to a remote location via TCP or UDP.

Example: For remote location via TCP or UDP,

1. select the file destination (i.e. UDP).
2. enter the IP address of the remote machine

Syslog info will now be sent to the remote machine.

Note: The syslog will be cleared completely and immediately and will not be retrievable when "Clear System Log" is selected, so be sure that is what you want to do.

Firmware Update

The Firmware Update menu is used to introduce firmware files that provide the architecture of the user interface. Occasionally new features or changes to existing features will be introduced and new firmware with these changes will be made available on the NTI website (http://www.networktechinc.com/srvsw-term-ssh.html). Once a user has downloaded the required file for firmware upgrade, this page will be used to upload them to the SERIMUX.

From the "Administration Settings" menu, press <**4**>-<**Enter**> to select "Firmware Update".

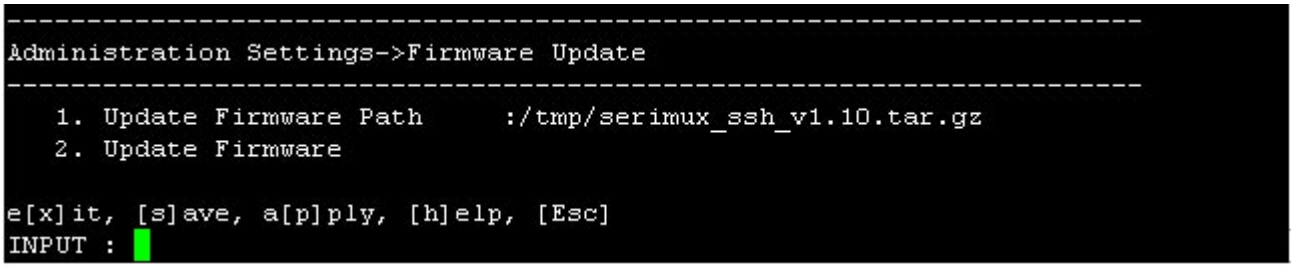


Figure 62- Administration Settings-Firmware Update

To update the firmware:

1. Download the firmware file from the NTI website to either a USB Flash Drive, to your tftp server, or to an NFS drive. Be sure to take note of the location on your CPU as to where it will be.

2. Press <**1**>-<**Enter**> to select "Update Firmware Path". You will be prompted to provide the path to the firmware file. The file name will be in the format ***serimux_ssh_vx_xx.tar.gz*** (where x_xx is the version number).

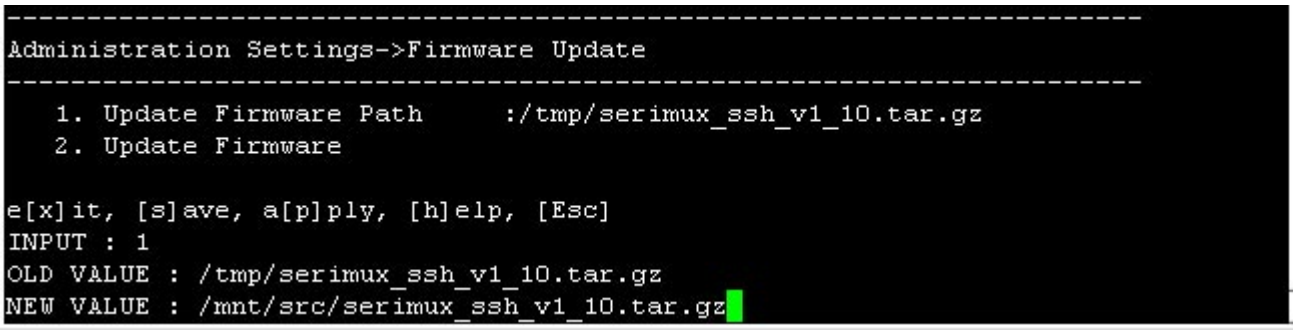


Figure 63- Change path from tftp source to flash drive

The update firmware path when the firmware file is on a USB flash drive (attached to the SERIMUX and with the USB flash drive mounted as described below) will be:

/mnt/src/*serimux_ssh_vx_xx.tar.gz*

Mount the USB flash drive

Before the USB flash drive can be used, it must be mounted to the SERIMUX system. At the shell prompt (before opening the Config Menu), enter the following command:

mount –t vfat /dev/sda1 /mnt/src

serimuxconfig (This will open the SERIMUX Configuration menu-proceed with update)

The update firmware path, when using a tftp server will be:

/tmp/*serimux_ssh_vx_xx.tar.gz*

When using a tftp server, before using the Update Firmware command, run the following commands from the shell prompt:

cd /tmp

tftp -r serimux_ssh_v1_10.tar.gz -g <tftp-server-ip>

(i.e. tftp -r serimux_ssh_v1_10.tar.gz -g 192.168.3.151)

serimuxconfig (This will open the SERIMUX Configuration menu-proceed with update)

3. Press <**2**>-<**Enter**> to select "Update Firmware". You will be prompted for a <**y**> for yes or <**n**> for no to confirm that this is the action you want.

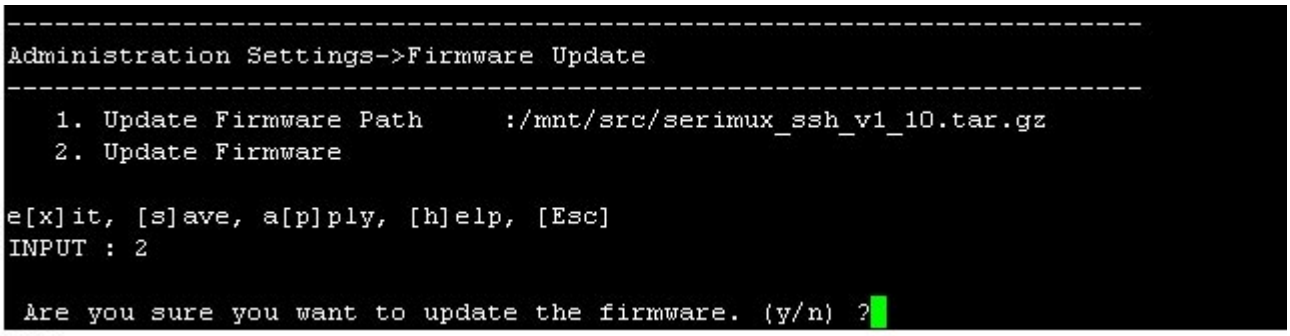


Figure 64- Firmware update- confirm to perform update

When the update is complete, you will see the message "`Firmware Update done.`"

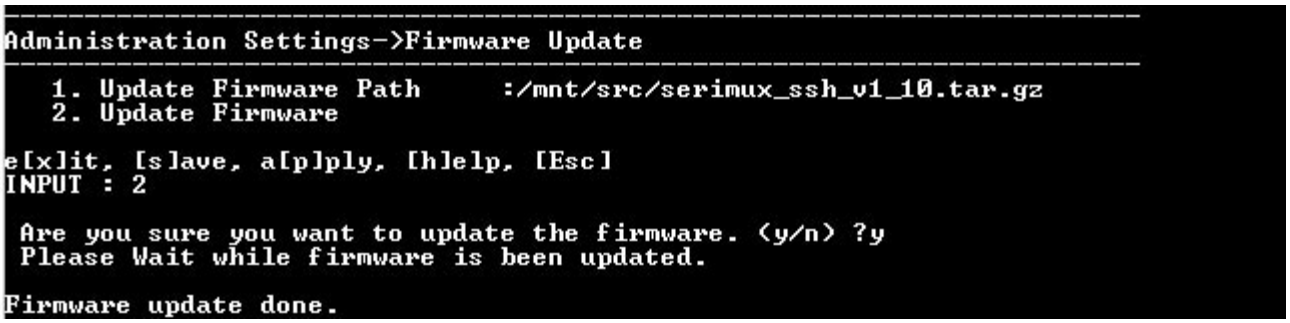


Figure 65- Firmware update- Completed

4. Press <**x**>-<**Enter**> to exit the configuration menu. You will be prompted for a <**y**> for yes or <**n**> for no to confirm that you want to exit the menu. Press <**y**>--<**Enter**>.

5. Type <**reboot**> to reboot the SERIMUX and have the new firmware take effect.

User Management

From the Configuration menu, press <**5**>-<**Enter**> to open the "User Management" menu. The User Management menu provides selections to configure user access to the SERIMUX configuration menus and to the devices attached to the SERIMUX. Users can be assigned to specific groups, and group names can be assigned to make port management easier.

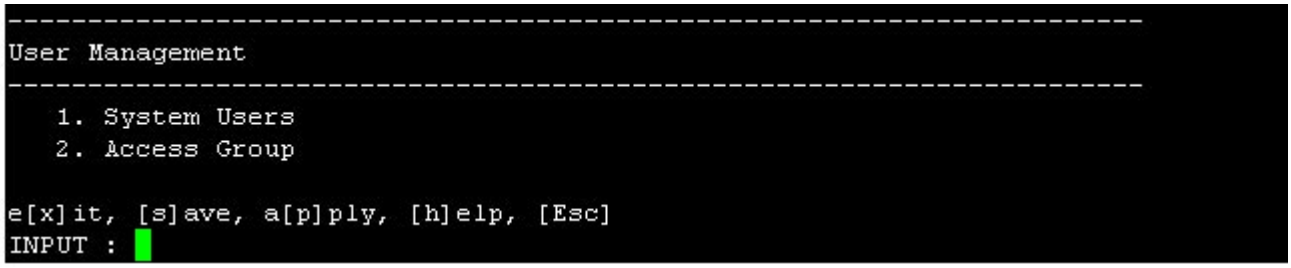


Figure 66- User Management menu

System Users

The System Users list is a list of all assigned user names. From the User Management menu, press <**1**>-<**Enter**> to open the "System Users" list. Users can be added, selected for editing, or deleted. The list indicates

- the user names,
- the user access location to open with each login via SSH, Telnet, or serial port,
- the access rights that have been assigned to the user.

Operators that are assigned "User" access privileges can only enter at the Port Connect menu, while operators assigned "Admin" access privileges can open into the Shell, the Config Menu, or the Port Connect Menu.

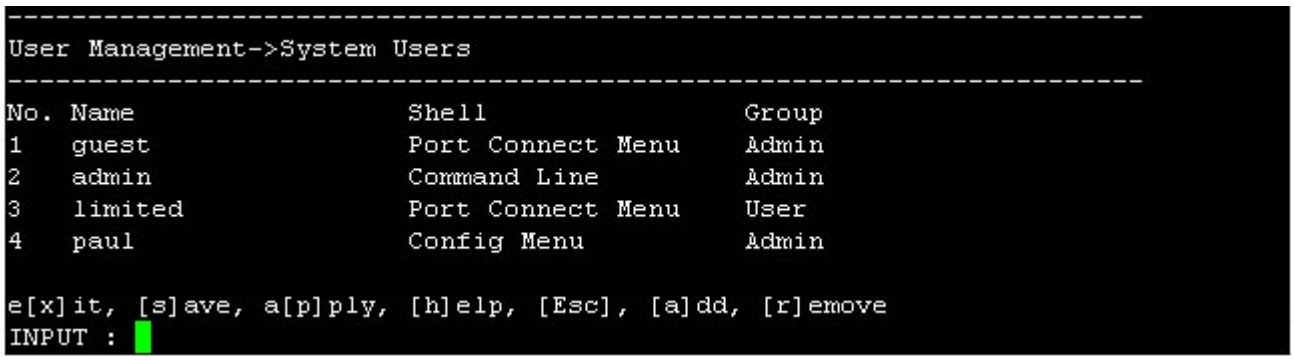


Figure 67- User Management- System Users

To make changes to a user configuration, press the index number of the user and press <**Enter**>.

Figure 68- User Management-Configure User

User configuration has the following options:

Setting	Valid Entry
User Name	Up to 50 alphabetical or numeric characters
Group	- Admin - assign administrative rights - User- assign limited user rights.
Shell	- Command line- SERIMUX will open a command line interface when user logs in - Config menu- SERIMUX will open configuration menu when user logs in - Port connect menu- SERIMUX will open port connection menu when user logs in
Password	Enter a password for the selected user to use at log in All passwords can be changed except the "root" password. A user must be logged in as "root" to change the password for user "root", and it can only be changed from the "Unit Settings" menu (page 36).

If a change is made to the user name, group, or shell, the password for that user must also be provided (whether it is a new password or an existing password). Otherwise the user will automatically be assigned the default password of "nti" by the SERIMUX to login the next time.

Access Group

The Access Group list displays each of the groups of users that have been assigned in the SERIMUX. From the User Management menu, press <**2**>-<**Enter**> to display the "Access Group" list.

Access Groups provide a quick means by which to define who will have access to specific ports on the SERIMUX. Each port can be configured for access by individual users and by Access Groups (page 22). Assigning users to Access Groups will save port configuration time.

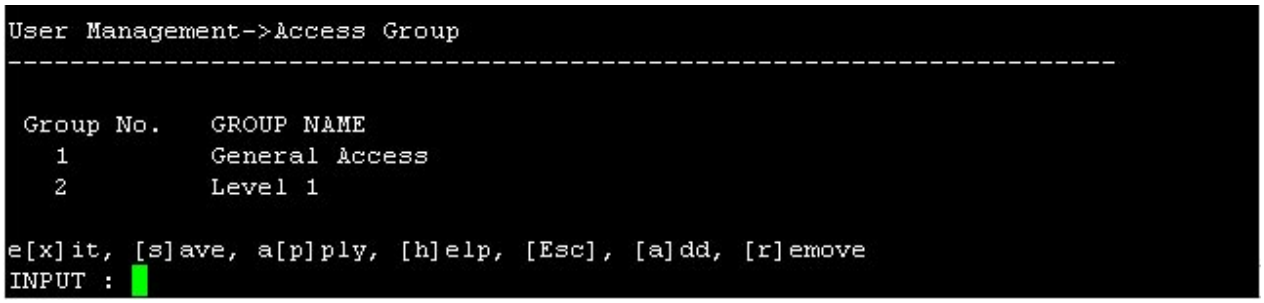


Figure 69- User Management-Access Groups

To add a group name, press <**a**>-<**Enter**> , type a group name (maximum 50 characters), and press <**Enter**>.

To remove a group name, press <**r**>-<**Enter**>, type the group number, and press <**Enter**>.

To edit the user names in a group, type the group No. and press <**Enter**>. The users assigned to that group will be listed.

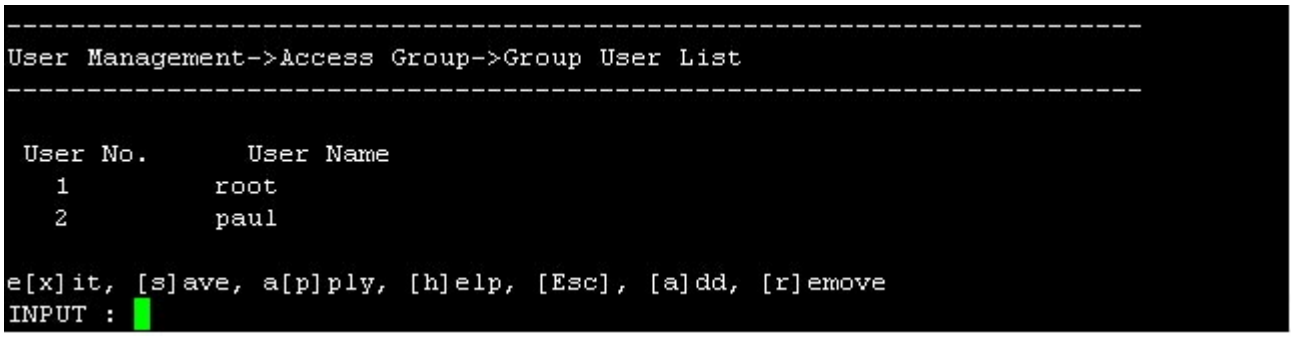


Figure 70- User Management- Group User List

From this list the user can add or remove users assigned to the group. Names typed when added will be applied whether they are names in the System Users list or not. Names are of authorized device users, not necessarily authorized SERIMUX users.

Administrative Info

From the Configuration menu, press <**6**>-<**Enter**> to open the "Administrative Info" menu. The Administrative Info menu provides selections to view pieces of information quickly that are useful to review the settings and status of the SERIMUX. The administrator can view the System Log to review user access and changes to the SERIMUX, network, Ethernet, and system settings, and review the status of each of the SERIMUX ports.

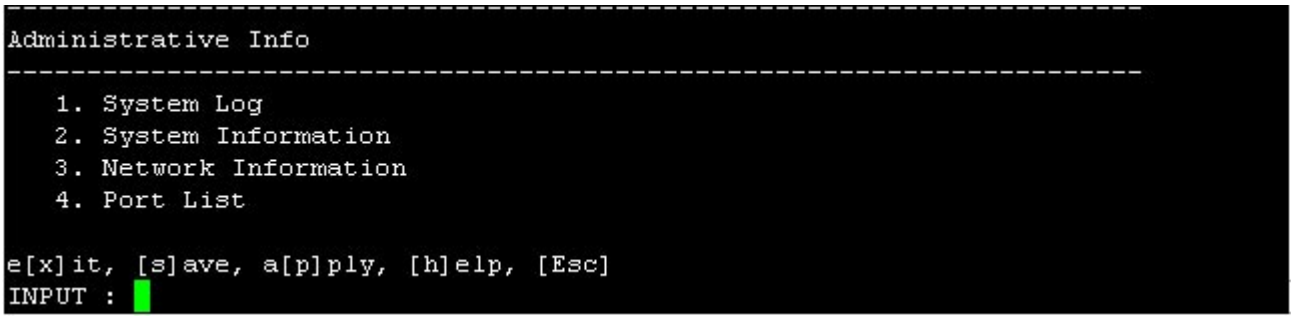


Figure 71- Administrative Info menu

System Log

The system log will display a listing of all user access to the SERIMUX, providing the date and time of their login and logout, and when any configuration changes have been made. From the Administrative Info menu, press <**1**>-<**Enter**> to display the "System Log".

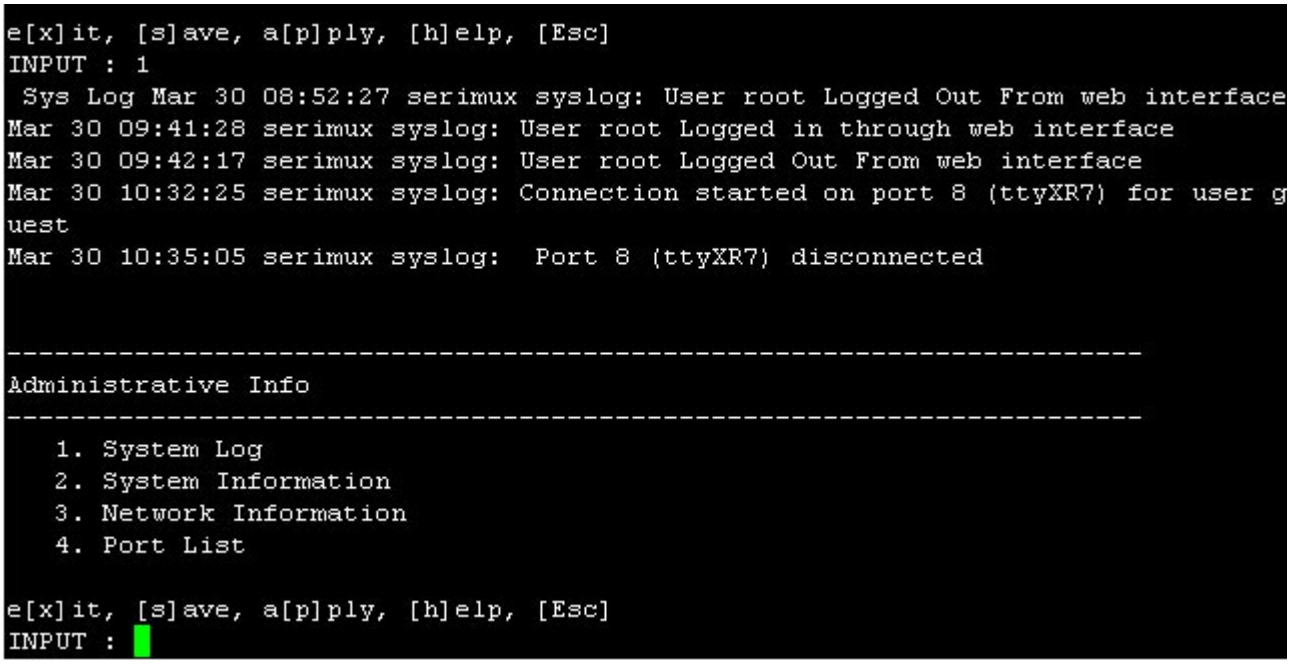


Figure 72- Administrative Info-System Log

Once the System Log is displayed, the SERIMUX will return the user to the Administrative Info menu.

System Information

The System Information list displays the model name of the SERIMUX, the firmware version in the SERIMUX, the MAC addresses of the Ethernet ports, the date in the system, and syslog status. From the Administrative Info menu, press <**2**>-<**Enter**> to display the "System Information" list.

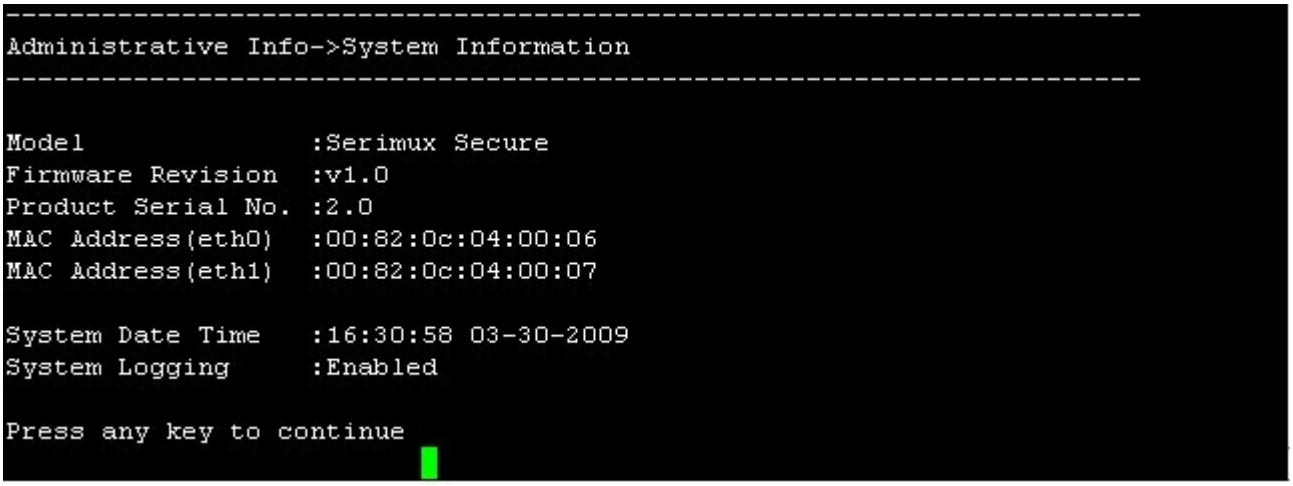


Figure 73- Administrative Info-System Information

Once the System Information is displayed, with the press of any key the SERIMUX will return the user to the Administrative Info menu.

Network Information

The Network Information list displays all of the current network settings for the Ethernet ports on the SERIMUX. Settings include IP mode, IP address, netmask, gateway, and DNS addresses. From the Administrative Info menu, press <**3**>-<**Enter**> to display the "Network Information" list. To edit these settings, see "Network Management" on page 31.

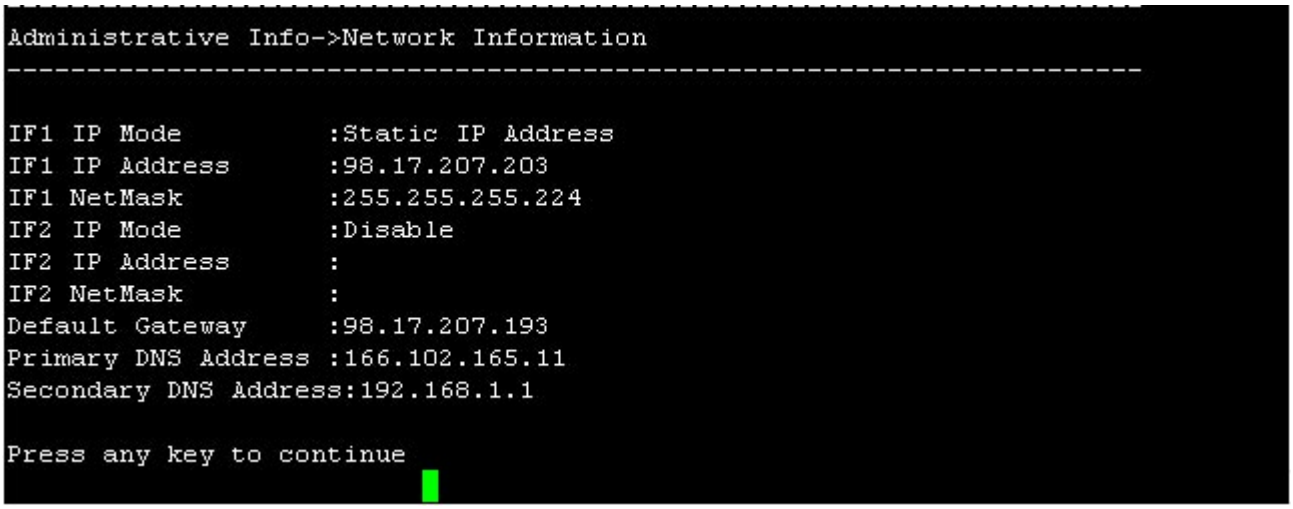


Figure 74- Administrative Info-Network Information

Once the Network Information is displayed, with the press of any key the SERIMUX will return the user to the Administrative Info menu.

Port List

The port list displays the status of device ports on the SERIMUX. It provides a quick overview of names of all users and hosts connected, the port serial settings, port escape sequence, protocol, and port numbers.

From the Administrative Info menu, press <**4**>-<**Enter**> to display the "Port List".

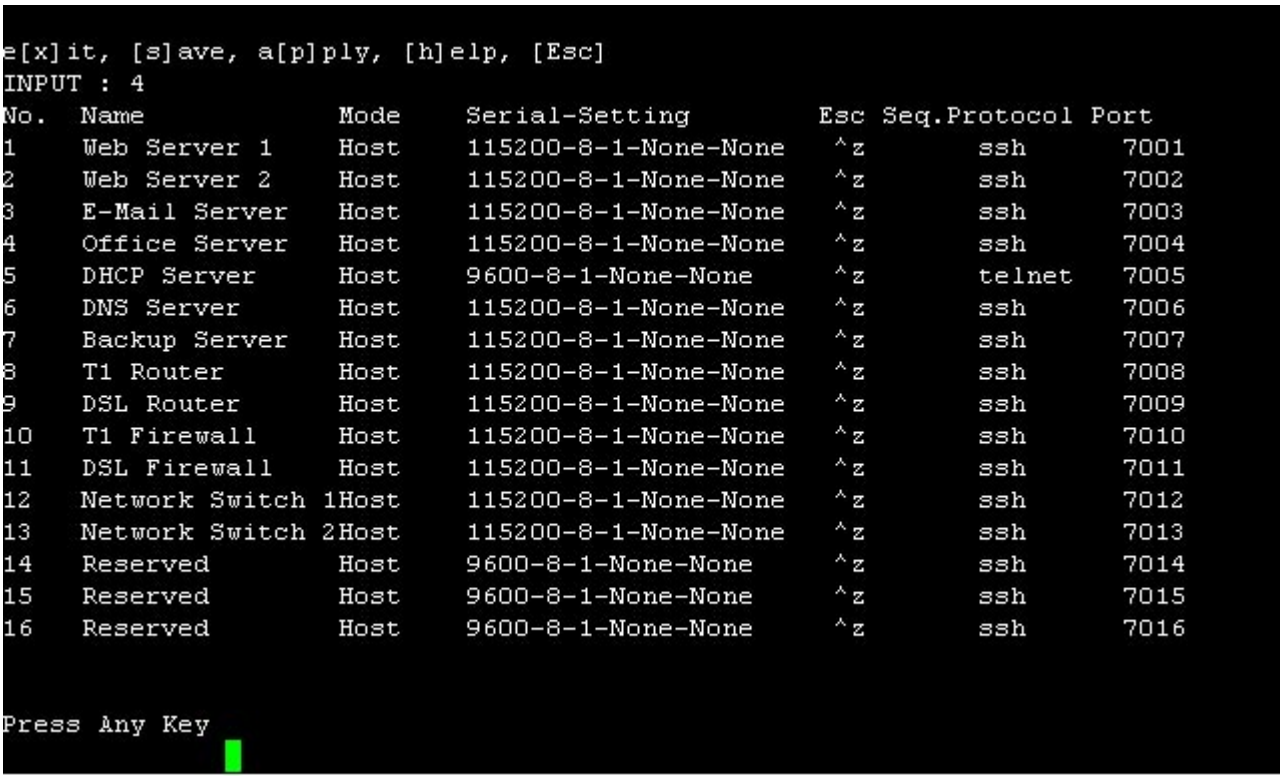


Figure 75- Administrative Info-Port List

Once the Port List is displayed, with the press of any key the SERIMUX will return the user to the Administrative Info menu.

Reboot

The SERIMUX can be rebooted from the shell prompt, either before entering the Config or Port Connect menus, or after exiting them.

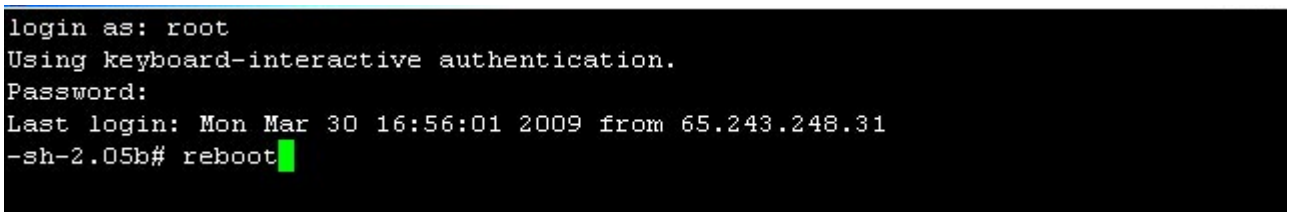


Figure 76- Reboot the SERIMUX from the shell

SERIAL CONTROL-USERS

Operators with “User” rights can connect only to accessible ports as defined by the administrator. A list of those ports will be displayed with a successful login.

To login, using a serial terminal or an emulator (e.g. Windows HyperTerminal or Putty),

1. connect the terminal to the SERIMUX at an accessible user port (users may have limited access through specific “user” ports, as opposed to all ports configured as “user” ports) and press the <**Spacebar**> or <**Enter**> key.
2. type a valid user name (assigned by the administrator) and press <**Enter**>.
3. type a valid password (assigned by the administrator) and press <**Enter**>.

Note: User names and passwords are case sensitive. It is important to know what characters must be capitalized and what characters must not.

After login, the User may connect to an allowed host port.

User Initial Selection Menu

After successful login, a menu will be displayed where you can choose between viewing the Port Connect Menu or the Sensor Monitor menu.

Figure 77- Initial menu for users

Press <**1**> to proceed to the Port Connect Menu where you will see a listing of accessible host ports, or press <**2**> to proceed to a listing of connected sensors and their current readings.

Figure 78- A user with limited host port access

From the Port Connect Menu the user can perform the following functions:

Function	Keystroke
Connect to host	<xx>-<**Enter**> (where xx is the port number)
Logout	<**X**>-<Enter> , then <Y> to confirm

FYI: The port index numbers are 1 and 2-digit decimal numbers. If the wrong number is entered, press the <Esc> key to remove it. Simply enter the correct number. The <Enter> key validates the command; <Esc> cancels it.

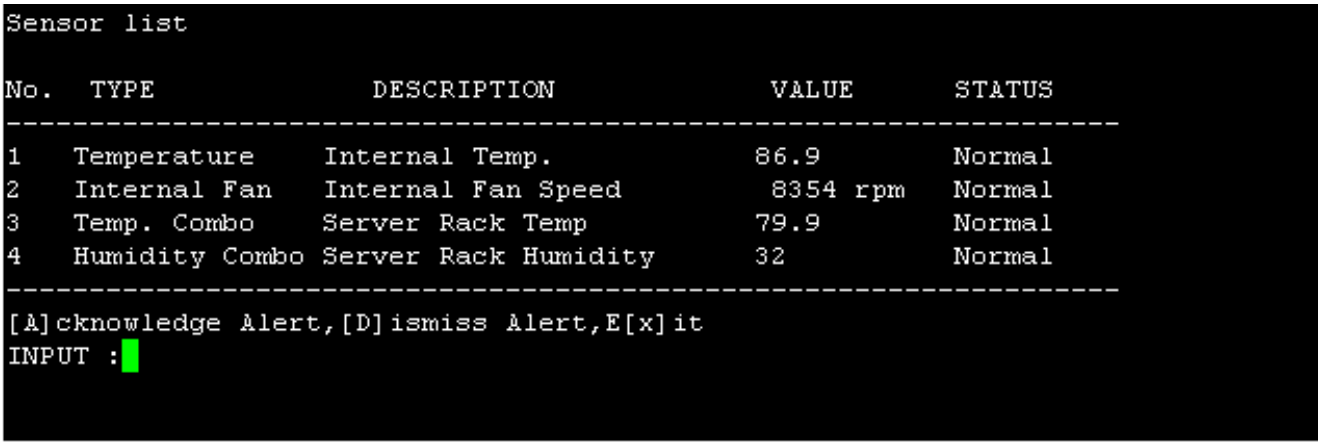


Figure 79- Sensor list with current readings

From the Sensor Monitor menu (or "Sensor List"), each of the sensor readings can be viewed. If a sensor is reporting an alert, you can either press <a> to acknowledge the alert, or <d> to dismiss the alert.

If the sensor is in alert status, the user has the option to either **acknowledge** the alert or **dismiss** it. If the user acknowledges the alert, no additional alert messages will be sent during that alert status cycle. If the user dismisses the alert, another alert message will be sent once the "notify again after" time designated on the configuration page elapses.

Note: If local authentication is enabled (page 21), then only the sensors you have been given access to will be presented for viewing.

DEVICE DISCOVERY TOOL

In order to easily locate NTI Devices on a network, the NTI Device Discovery Tool may be used. The Discover Tool can be downloaded from http://www.networktechinc.com/download/d-srvsw-term-ssh.html, unzipped and saved to a location on your PC. To open it just double-click on the file **`NTIdiscover.jar`** . This will open the NTI Device Discovery Tool.

Note: The Device Discovery Tool requires the Java Runtime Environment (install Java 6 or 7, NOT Java 8) to operate. Java can be downloaded from http://java.com/en/download/manual.jsp .

Note: The computer using the Device Discovery Tool and the NTI Device must be connected to the same physical network in order for the Device Discovery Tool to work. If no devices are found, the message "No Devices Found" will be displayed.

Tip: If your Windows program asks which program to open the `NTIDiscover.jar` file with, select the Java program.

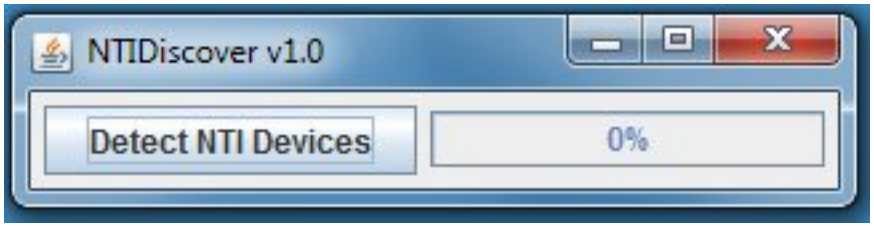


Figure 80- Device Discovery Tool

Click on the "**Detect NTI Devices**" button to start the discovery process. After a short time, the tool will display all NTI devices on your network, along with their network settings.

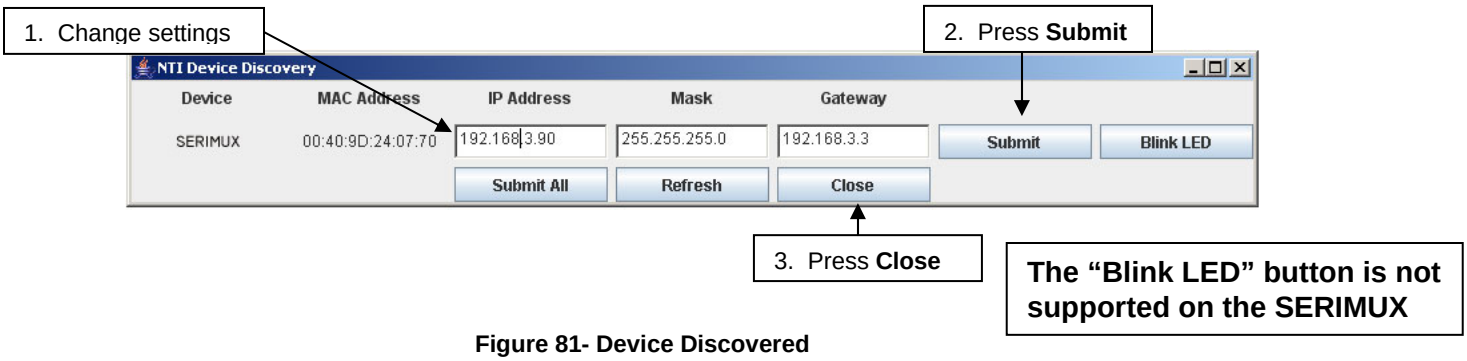


Figure 81- Device Discovered

How to Use the Device Discovery Tool

Note: If more than one device is discovered by the tool, the following instruction only applies to the SERIMUX.

To temporarily change the network settings for a SERIMUX,

1. type in new settings in the boxes provided (see below)
2. press the **`Enter`** key or the **`Submit`** button.
3. press the **`Close`** button to close the Discovery Tool.

Use your browser to access the SERIMUX as described on page 52.

Note: Be sure to go to the IP Configuration page (page 67) and permanently change the settings as desired. The settings changed by the Discovery Tool are temporary. If the SERIMUX is power cycled, rebooted, or the Reset button is pressed (page 85), the SERIMUX will return to the last settings saved on the IP Configuration page.

WEB INTERFACE

A user may control the connections of the SERIMUX using a Web Interface via any web browser (see page 2 for web supported browsers) provided the Ethernet is connected. With the SERIMUX connected to a LAN through an Ethernet cable, a user can access the web interface controls inside the SERIMUX.

FYI: To quickly locate a SERIMUX on the LAN and edit the IP address settings, use the Device Discovery Tool (page 51).

To access the web interface, type the current IP address into the address bar of the web browser.
Address http://192.168.1.91

Note: If the "HTTP Enable" (page 68) is set for as "Disable", only an SSL-encrypted connection (below) will be possible. The default setting is "Enable".

To open a SSL-encrypted connection, type:
Address https://192.168.1.91

If the SERIMUX did not have a valid custom certificate, you will be prompted with a warning for default NTI certificate. Click **"Proceed anyway"** to continue.

A "Login Page" will appear.

Figure 82- Web interface Login page

Enter the Password

Type in the default user name and password. To change the password, see page 71.

User Name = root (lower case letters only)
Password = nti (lower case letters only)

Note: The browser must be configured to accept cookies in order for the user to successfully make use of the web interface.

Note: If the administrator password has been changed and is not known, contact NTI for instruction on resetting the SERIMUX to defaults.

With the acceptance of a valid user name and password, the main menu will be displayed with a complete ports list.
As described on the following pages, each link on the main menu will enable different areas of control for the SERIMUX.

Menu Overview

The SERIMUX menu may be navigated using the left mouse button. The list below summarizes the function of each topic in the menu for quick reference.

Connect Port- Click to return to the Ports List, a listing of all Host ports. Click any port to make a connection to that port.

Port Management- Click to display the following three Port Management topics:
- Port Configuration- Click to display the port list. Click on any port to display the list of configurable port settings for that port.
- Common Port Configuration- Click to display a list of configurable port settings that can quickly be copied to any other port. These settings are used for quickly configuring any port with the most common settings used,
- Copy Paste Port- Used to copy port settings from one port to another. Click to display a list of settings that can be copied from any existing port and a list of the ports those settings can be copied to.

Sensor Management- Click to display the following three Sensor Management topics:
- Sensor Summary- Click to display the sensor list. Click on any sensor to display the detailed status of a sensor.
- Sensor Configuration- Click to display the sensor list and add or remove sensors as desired. Click on any sensor to display a list of configurable settings for sensor operation and alert notification.
- View Data Log- Click to display all log entries as reported by each sensor configured to store data logs.

Network Management - Click to display the following three Network Management topics:
- IP Configuration- Click to display a list of configurable IP settings for “Ethernet 1” and “Ethernet 2”
- Server Configuration- Click to display configurable settings for the Web Server, SMTP Server, SNMP, and NFS.
- TCP Settings- Click to display settings for configuring TCP settings

Administrative Settings- Click to display the following four Administrative topics:
- Unit Settings- Click to display configurable settings for the unit name, administrator password, and system date and time
- Security Settings- Click to display configurable settings for CLI authentication type and CLI menu timeout period
  - x509 Certificates- Upload alternate SSL certificates
- Syslog- Click to display a configuration page for the system log to control the log size, log filename, where it is saved, and to remove all or part of the logs content.
- Firmware Update- Click to be provided with a block to supply the name and path, or browse for a firmware file to be applied to the SERIMUX and a button labeled “Update” to initiate a firmware update using that file.

User Management- Click to display the following two User Management topics:
- System Users- Click to display the list of users. From this screen you can click on a user to change user settings, delete users, or add a new user.
- Access Groups- Click to display the list of named access groups. Groups names can be added. Under user settings, each user is assigned to group. Under Port Configuration, ports are configured for which user groups have access to them.

Administrative Information- Click to display the following four Administrative Information topics:
- System Log- Click to display a window detailing the login, logout and timeout dates and times for each user that has accessed the SERIMUX.
- System Information- Click to display the Firmware version, MAC addresses of the Ethernet ports, and system log status.
- Network Information- Click to display all the current network settings for the SERIMUX
- Port List- Click to display all the ports on the SERIMUX and the status of each.

Logout- Click to open a window prompting you to logout from the SERIMUX.

Support- Click to display the following two Support topics:
- Manual- Click to be taken to the web location of the manual for the SERIMUX
- Downloads- Click to be taken to the web location of the firmware download available for the SERIMUX.

Reboot- Click to open a window prompting you to click a button if you wish to reboot the SERIMUX. If Reboot is used, you will be automatically logged out and need to log in to resume operation.

Main Menu and Port List

The first screen displayed in the Web Interface after a valid login shows the main menu on the left side and a complete port list on the right.

The Port List details, from left to right:

- **Port No.** -the physical port number on the rear of the SERIMUX
- **Name**- the name assigned to the port
- **Mode**- what connection purpose the port is configured for (Host, User, or Dial-in User)
- **Serial Settings**-the serial communication settings for that port
- **Port Escape Seq**.- the keyboard key sequence used to exit a connection to the port
- **Protocol**- the communication protocol of the port
- **TCP Port No**.- the TCP port number assigned to the port
- **Status**- the current status of the port ("None" for not in use, or "Connected" to indicate it is in use)

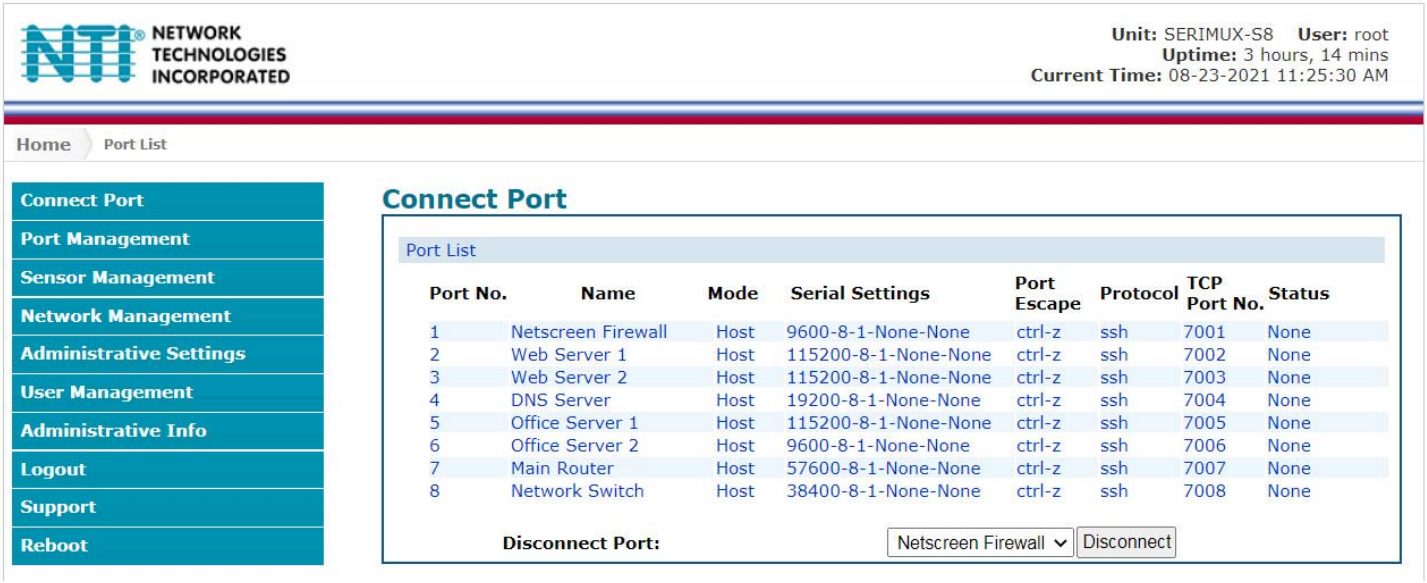


Figure 83- Connect Port/Port List Page

Port Management

Port Configuration

The Port Configuration page is used to setup all of the criteria necessary to communicate between the user and host devices.

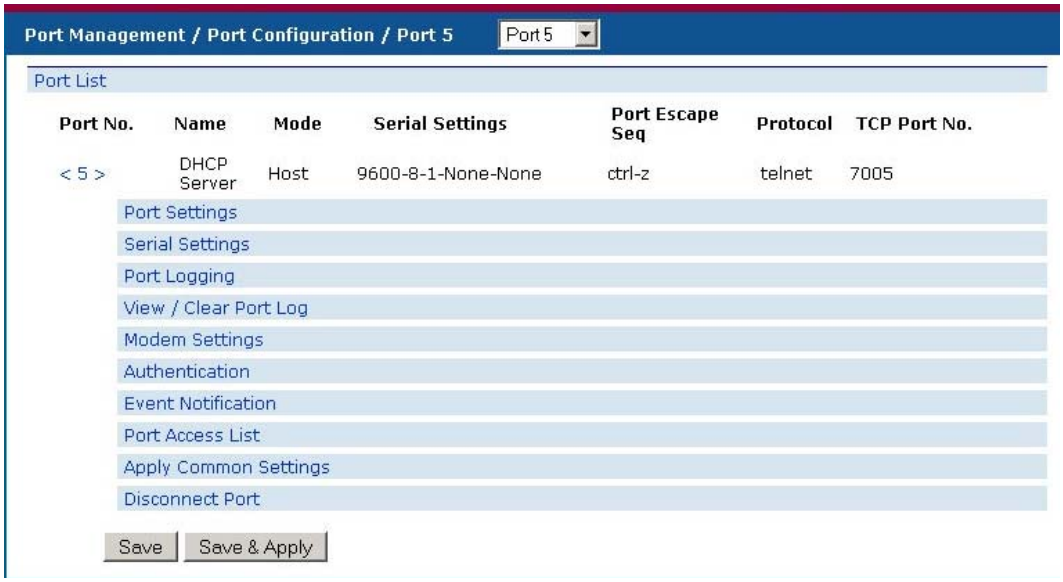


Figure 84- Port Configuration page

Under "Port Management" in the main menu, select "Port Configuration" to display a ports list. Click on a port to display the current configuration settings for the selected port and the configurable setting categories.

Setting	Description
Port Settings	Various settings for port identification, type, and connection methods
Serial Settings	Define the serial settings for serial connections to communicate
Port Logging	Define characteristics of port logs and storage method
View/Clear Port Log	View log for current port and clear data if desired
Modem Settings	Apply settings required for connection to a modem
Authentication	Select authentication method for port
Event Notification	Configure to send e-mail upon connection and/or disconnection at port and/or to send SNMP message
Port Access List	Determine which users and/or groups of users have port access
Apply Common Settings	Apply settings configured under "common settings" (page 59) to port
Disconnect Port	Disconnect port from use at any time

Port Configuration->Port Settings

Setting	Description
Port Name	This is the name of the port as it will appear in the port list. Up to 50 characters may be used.
Port Enable	If this is set to disabled, no one will be able to connect to the port, either as a user, or with a device
Port Type	A port can be either defined as a: - Host port for serial device connection - User port for direct user plug in - Dial-in user such that a modem will be connected and a remote user can connect through a modem
Assign IP Enable	With this enabled, an IP address can be specifically assigned to this port. Once enabled, an additional configuration block will appear to assign the IP address to be used.

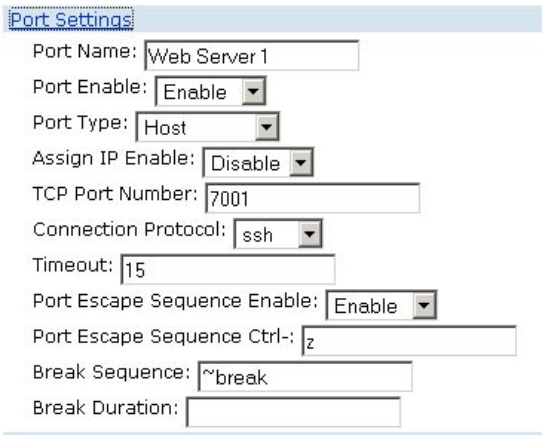


Figure 85- Port Settings

Port Settings (Cont'd)

Setting	Description
TCP Port Number	Assign number used for TCP communication **Be careful not to assign the same number used by another port, or the second port with a duplicate TCP port assignment will not work.**
Connection Protocol	Select: RawTCP for direct TCP connection Telnet is using a Telnet client (non-secure connection) SSH is using an SSH client (secure connection)
Timeout	Set time (in minutes) before an connection that is idle will be automatically disconnected- range 0-999 minutes (0 = disabled)
Port Escape Sequence Enable	Enable or disable the function of using a port escape sequence
Port Escape Sequence Ctrl	Keyboard key to use in conjunction with the <**Ctrl**> key for a port escape sequence
Break Sequence	Sequence of characters which will send a break signal – ie. <**Ctrl**>-<**break**>
Break Duration	Duration for which the break signal will be applied-range=0-999
Multiple Connection	Enable or Disable to allow access to the same port from more than one device simultaneously. .

Port Configuration->Serial Settings

Setting	Value
Baud Rate	50bps-115.2Kbps
Data Bits	5, 6, 7, or 8
Stop bits	1 or 2
Parity	None, Even, or Odd
Flow Control	Hardware, Software, Both, or None
Inter Character Delay	0-999 ms
Line Feed Suppress	Enable to suppress the line feed
DTR Option	High or low

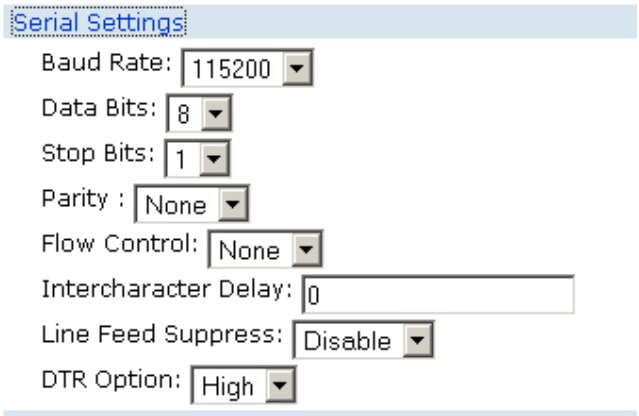


Figure 86- Serial Settings

Port Configuration->Port Logging

Setting	Value
Log Enable	Disable or Enable Logging feature for this port
Log Storage Location	System Memory (cannot change at this time)
Enable Syslog	Disable or Enable Syslog feature for port
Syslog Location	Local2 (cannot change at this time)
Log Buffer Size	0-999 K bytes
Log File Name	Up to 100 characters
Time Stamp With Log	Enable to have log entries include a timestamp

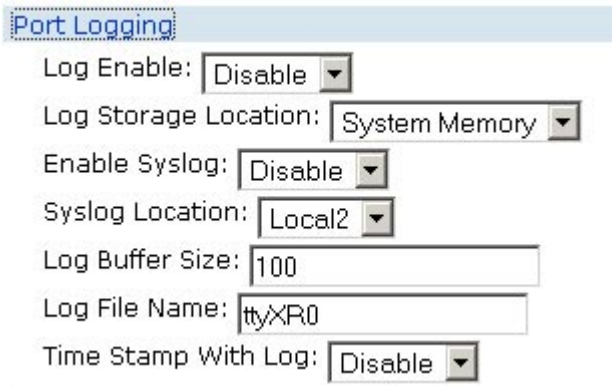


Figure 87- Port Logging settings

Port Configuration->View Port Log

Select to view log records for selected port. The viewing window will display up to 1K bytes of records. To view the next 1K bytes, press the "**Next>>"** button. The SERIMUX will record all data passing through the port.

Press "**Clear Log**" to erase all records. If records are allowed to accumulate in the buffer, when the buffer reaches 100% of its set capacity (0-999 K bytes), the first 10% of records will drop off to make room for new records.

Figure 88- View or Clear Port Log

Port Configuration->Modem Settings

If the port is set for a port type "Dial-In User, it will require a modem to be connected. Refer to your modem instructions for appropriate settings to be applied here.

Figure 89- Modem settings

Port Configuration->Authentication

The authentication type required for communication through this port can be chosen from a drop-down list.

If no authentication method is desired, disable authentication by selecting "none". With "none" selected, a user will immediately connect to a port when that port is selected in the port list.

Authentication options that include Radius, TacacsPlus, Kerberos, and LDAP will require additional configuration when selected. Apply the appropriate authentication server IP addresses and additional configuration settings for your authentication method of choice.

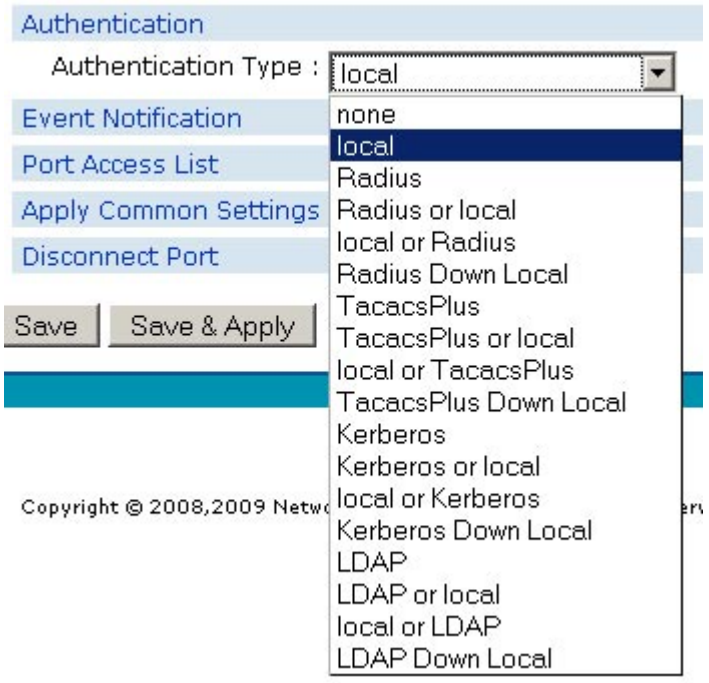


Figure 90- Authentication method options

Port Configuration->Event Notification

If desired, an e-mail and/or SNMP message can be sent each time a port is connected to, and / or disconnected from. The recipient's can be the same for each event, or different. Simply enter valid e-mail addresses and SNMP addresses and make sure the SERIMUX web server is properly configured to send e-mails (page 68).

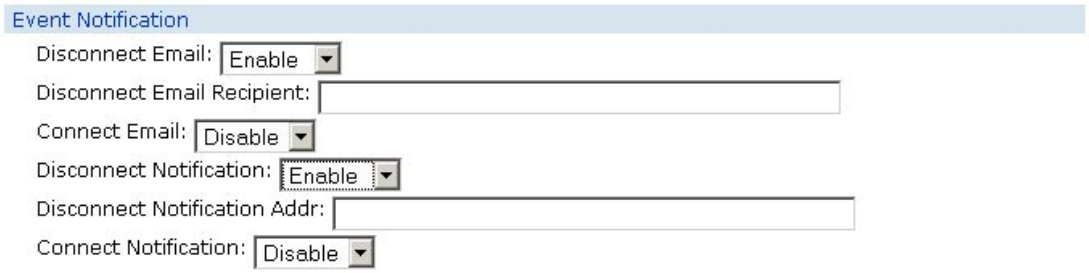


Figure 91- Port event notifications

Port Configuration->Port Access List

Through the Port Access List, control which users will have access to the port. The list can be quickly edited to include users listed individually, or in groups. With Access Groups properly defined (see page 79), quickly add users to the Port Access List.

To add a user, enter a valid user name in the box to the left of the "**Add User Name**" button, and press the button. The screen will refresh to indicate the added user.

To add an access group, enter a valid access group name in the box to the left of the "**Add Group**" button, and press the button. The screen will refresh to indicate the added group.

If a user needs to be removed from the list, select the check-box to the left of the user name and press "**Delete Checked User Names**". The screen will refresh to indicate the user has been removed.

If a group needs to be removed from the list, select the check-box to the left of the group's name and press "**Delete Checked Group Names**". The screen will refresh to indicate the group has been removed.

Figure 92- Port Access List

Port Configuration->Apply Common Settings

Press the button "**Apply Common Settings for Port x**" if the common settings configured on page 59 are applicable to this port.

Figure 93- Apply common settings to port

Note: Settings previously configured will be overwritten with the settings specified in the "Common Port Configuration".

Port Configuration->Disconnect Port

To quickly disconnect any communication through a port in use, press the "**Disconnect Port**" button.

Figure 94- Disconnect Port button

With the selections made in the Port Configuration page (and on any other pages throughout the Web Interface), press "**Save**" to save the changes without immediately applying them. The changes will be made the next time the SERIMUX is booted. To apply the changes immediately, press "**Save & Apply**".

Common Port Configuration Page

The Common Port Configuration Page is used to setup all of the common criteria necessary to communicate between the user and host devices. Once setup, the user needs only to select "Apply Common Settings" from the Port Configuration page (above) for a selected port to quickly apply these settings. This will help the user to save considerable time in configuring the SERIMUX.

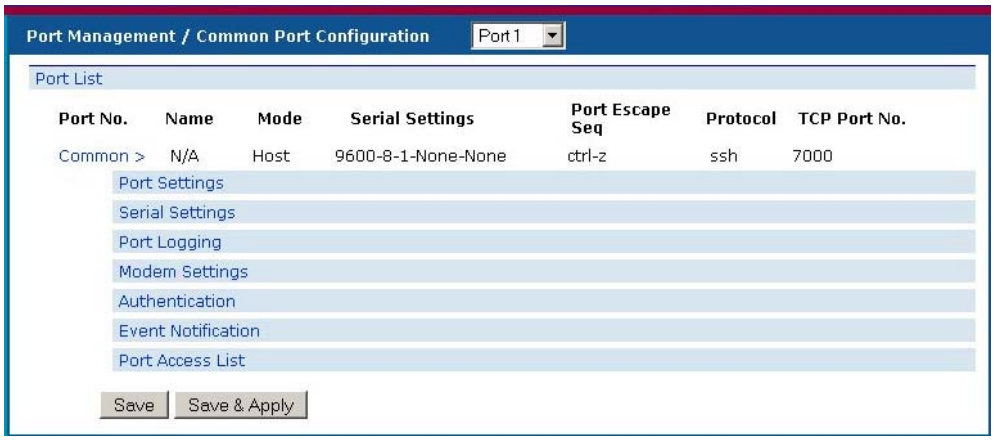


Figure 95- Common Port Configuration page

Under "Port Management" in the main menu, select "Common Port Configuration". A list of configurable settings will be displayed. Configure settings that are considered to be commonly used by the ports on your SERIMUX. For a description and instruction on the various settings, see "Port Configuration" on page 55.

Copy Paste Port

The Copy Paste Port page is provided in the event the settings in the Common Port Configuration aren't what you need but the settings of another port are. This provides yet another way to save time in configuring the SERIMUX.

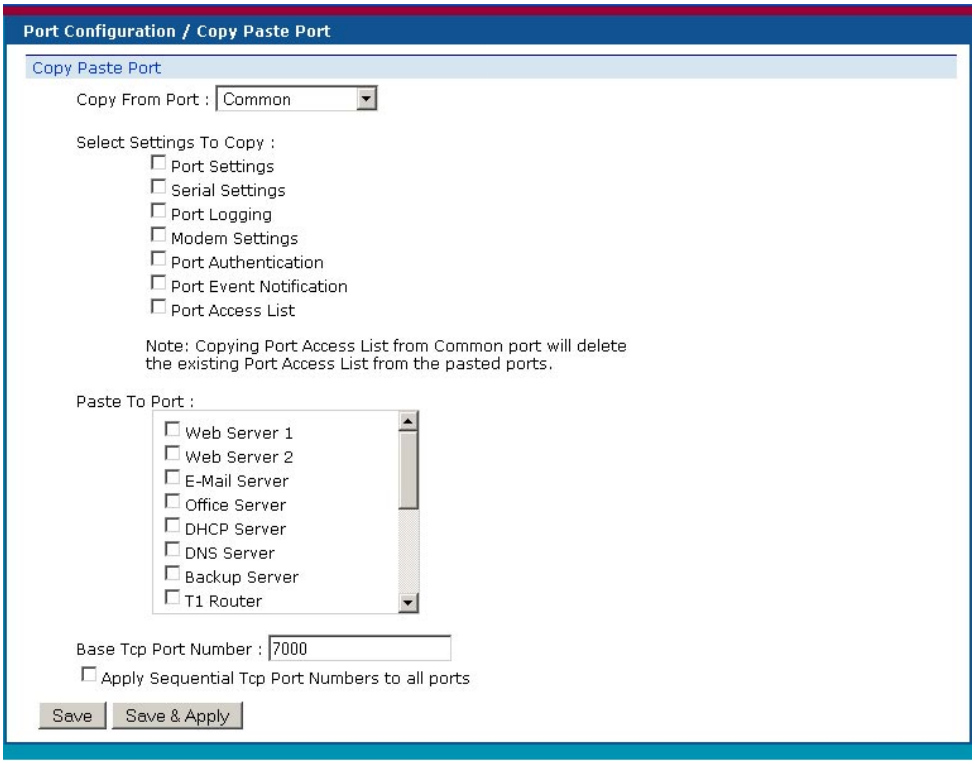


Figure 96- Copy Paste Port page

Under "Port Management" in the main menu, select "Copy Paste Port". The user can copy all or specific settings from any port and paste them to as many other ports as desired. Once the source port ("Copy From Port") is selected, and the categories to copy are selected, select which ports the settings are to be applied (pasted) to.

Base TCP Port

This selection enables the user to configure TCP port numbers to be assigned to each serial port. When "Apply Sequential Tcp Port Numbers to all ports" is selected, each serial port is assigned the TCP port number in sequential order following the "Base" port number (i.e. if the Base TCP Port Number is 7000, then port 1 will be 7001, port 2 will be 7002, etc).

With the selections made, press "**Save**" to save the changes without immediately applying them. The changes will be made the next time the SERIMUX is booted. To apply the changes immediately, press "**Save & Apply**".

Note: If TCP port numbers have already been assigned to ports, the previously assigned TCP port numbers will be overwritten with new port numbers in order of their physical port number connection on the SERIMUX.

Sensor Management

Sensor Management provides the ability to monitor internal sensors (temperature, fan speed, and the power supply (only in units with dual power supplies)) as well as add external sensors. External sensors connect through RJ45 connectors to the ports on the SERIMUX labeled “RJ45 Sensors”.

Internal Sensors

SERIMUX has three on-board sensors, which are permanently present:
- one temperature sensor
- one fans speed sensor
- one dual power sensor (only present in models with dual power supply option)

Internal sensors are monitored and fully configurable just as External Sensors are (see page 64).

Internal sensors are always shown in the Summary Page and cannot be removed.

External Sensors

The External Sensors are those that connect through RJ45 connectors. There are two types of external sensors supported by the RJ45 connectors: **RS485 Sensors** and **Contact Sensors**.

RS485 Sensors

The following types of RS485 sensors are supported:
- Temperature Sensor (ENVIROMUX-STS)
- Humidity Sensor (ENVIROMUX-SHS)
- Combined Temperature + Humidity Sensor (ENVIROMUX-STHS)

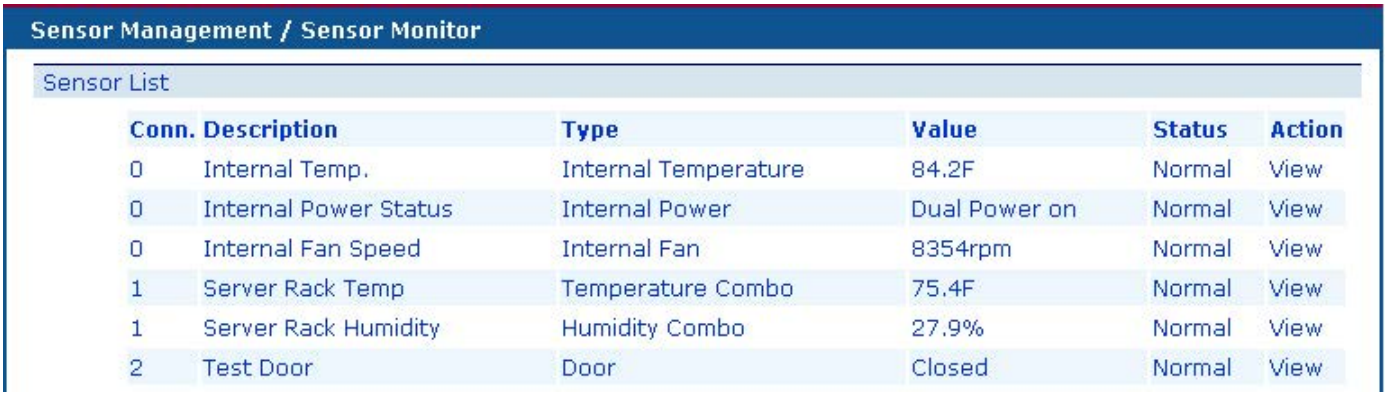
RS485 Sensor Management

The RS485 sensors are detected and identified by type automatically when they are connected to the RJ45 connector. The newly detected sensor will appear in the Summary Page. A web page will be created for the sensor and the default description issued to the sensor by SERIMUX will be "***Undefined"***.

If a **double-function sensor** is detected (ENVIROMUX-STHS), it will be displayed as two sensors, each one with a single function. For example a Temperature/Humidity sensor will appear as separate sensors (Temperature sensor and a Humidity sensor) both with the same number connector. The default description of both sensors will be ***Undefined***. A double-function sensor will be listed as a “Combo” type (i.e. “Temperature Combo” as seen in Figure 97)

Sensor Summary

The Sensor Summary page lists each of the sensors that are connected to and monitored by the SERIMUX. This page provides the current status of each sensor.



Conn.	Description	Type	Value	Status	Action
0	Internal Temp.	Internal Temperature	84.2F	Normal	View
0	Internal Power Status	Internal Power	Dual Power on	Normal	View
0	Internal Fan Speed	Internal Fan	8354rpm	Normal	View
1	Server Rack Temp	Temperature Combo	75.4F	Normal	View
1	Server Rack Humidity	Humidity Combo	27.9%	Normal	View
2	Test Door	Door	Closed	Normal	View

Figure 97- Sensor Summary page

The user can see the sensor measurements by clicking on the sensor's name in the Summary page. A web page will be displayed for the selected sensor, showing the type of sensor, the name, value of the reading (if it is an analog value it will be also displayed graphically), the threshold settings (in red) and the current reading (in green) of a selected sensor. It also shows the time, date, and measurement taken of the most recent alert and statistics (last alert, lowest reading, highest reading). Lowest and highest readings are indicated only for RS485 sensors.

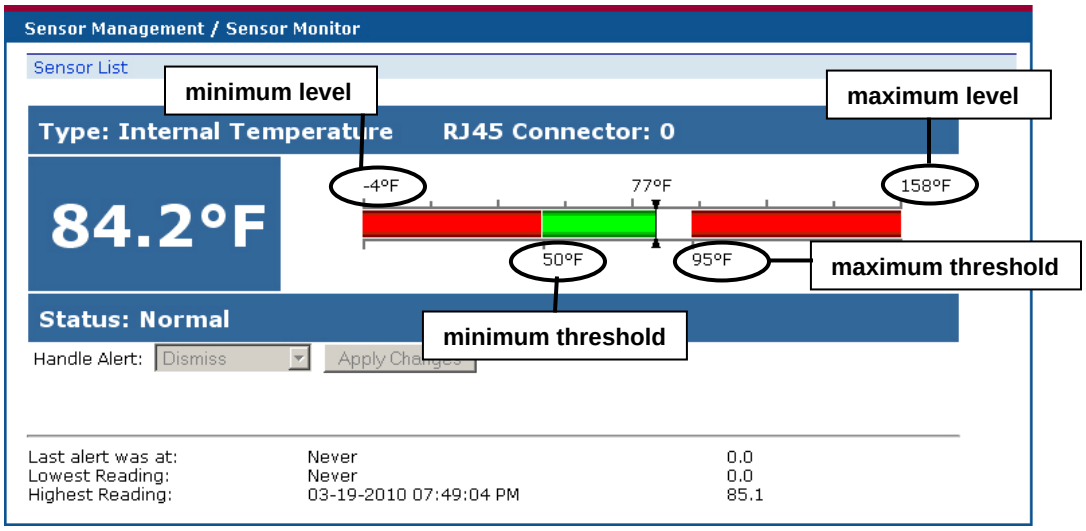


Figure 98- Sensor status details

If the sensor is in alert status, the user has the option to either **acknowledge** the alert or **dismiss** it. If the user acknowledges the alert, no additional alert messages will be sent during that alert status cycle. If the user dismisses the alert, another alert message will be sent once the "notify again after" time designated on the configuration page elapses.

To configure the sensing and alert notification parameters of a sensor, go to the Sensor Configuration page and click on the sensor to open the Common Sensor Configuration page for that sensor.

If the sensor is removed or communication lost for any reason (example: cable disconnected) the unit will detect this and show the sensor in "Non Responding" status. Question marks (???) will replace the name in the Summary Page. In this way the user will know the sensor has a problem or as been accidentally disconnected. If the user wants to remove a sensor (including a sensor now replaced by question marks) from the list, it must be done manually using the **Remove** button on the Sensor Configuration page.

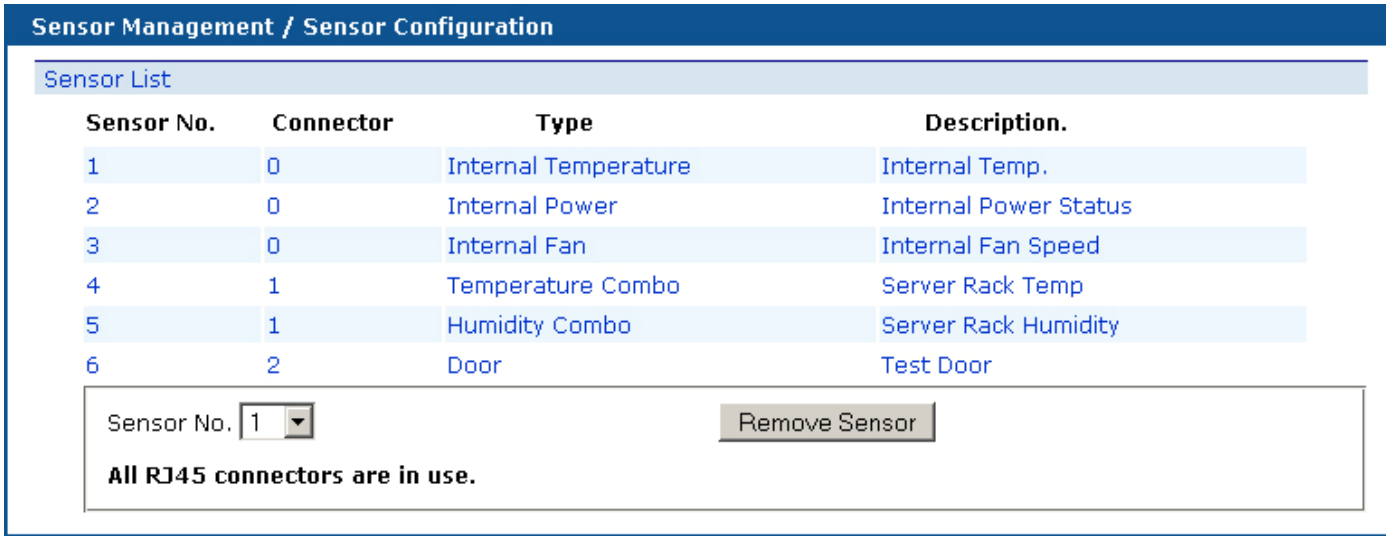


Figure 99- Sensor Configuration page

Adding a Sensor

If both of the "RJ45 Sensor" connectors on the SERIMUX are not in use by RS485 type sensors (these would be automatically sensed and added to the Summary Page), then a contact sensor can be added.

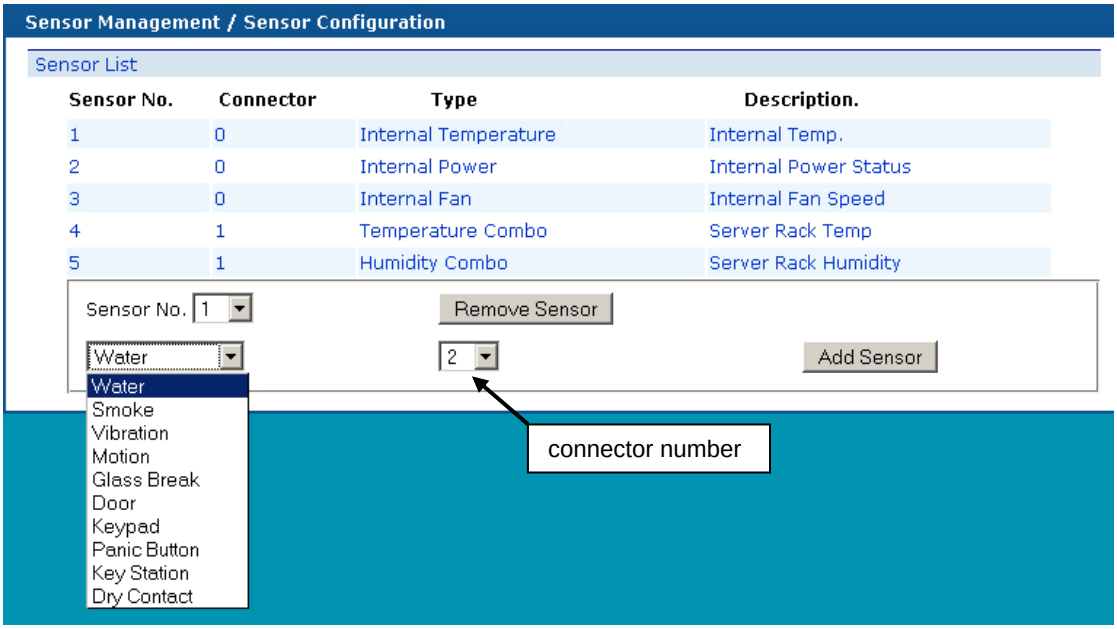


Figure 100-Add a sensor

The names of several contact sensor types (i.e. water, smoke, vibration, etc) have been pre-assigned and can be selected (see Figure 100) or the type "Dry Contact" can be selected. Make sure the connector number shown is the connector used by the new sensor. The right-hand connector is "1", and the left-hand connector is "2" (as viewed from the rear of the SERIMUX).

If the sensor is not connected at the time it is added to the Sensor List, the sensor status page will report it as "Open".

Use the schematic below to wire the contact sensor to an RJ45 plug.

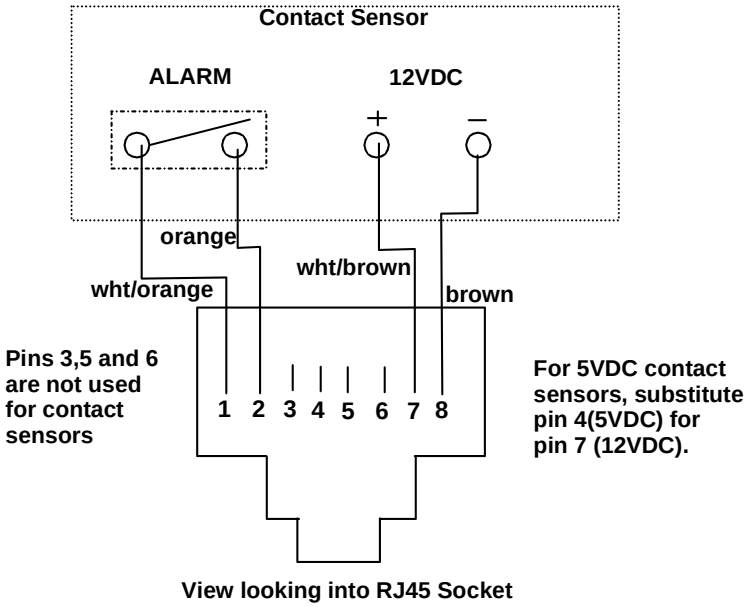


Figure 101- Wiring method for contact sensor

Configure a Sensor

Many parameters can be defined to determine how or if a sensor reports data to the user. To configure those parameters, click on a sensor listed on the Sensor Configuration page to open the Common Sensor Configuration page for that sensor.

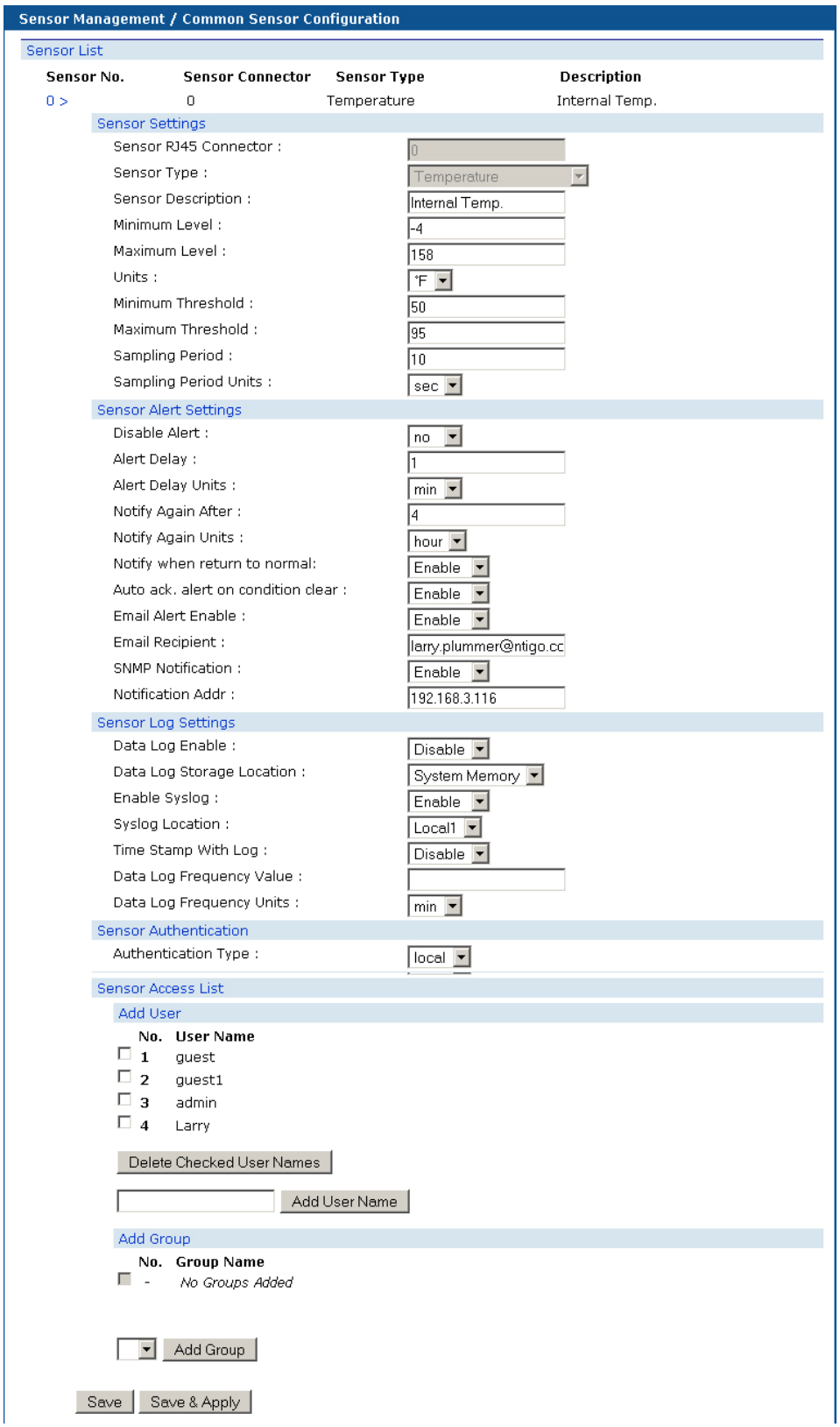


Figure 102- Common Sensor Configuration page

Sensor Settings

Sensor Description: Each sensor can be given a unique description. Descriptions can be from 1-80 characters in length and include most characters. They cannot contain a backslash (\ ) or quotation mark ("). Descriptions will be used in e-mail alerts in the DESCRIPTION field.

Within this section the alerts regarding this sensor can be disabled.

Note: if the user wants to disable alerts for a sensor after the sensor is already in alert status, the user must either acknowledge or dismiss the alert first.

Minimum Level: This shows the minimum value supported by the sensor. It is factory configured for each type of sensor but can be changed. Changing this value is **not** recommended.

Maximum Level: This shows the maximum value supported by the sensor. It is factory configured for each type of sensor but can be changed. Changing this value is **not** recommended.

Units: (only for Temperature sensors) This lets the operator choose between Celsius and Fahrenheit as the temperature measurement unit.

Minimum Threshold: The user must define the lowest acceptable value for the sensors. If the sensor measures a value below this threshold, the sensor will move to alert status. The assigned value should be within the range defined by Minimum Level and Maximum Level and lower than the assigned Maximum Threshold value. If values out of the range are entered, they will be automatically adjusted to be within range.

Maximum Threshold: The user must define the highest acceptable value for the sensors. If the sensor measures a value above this threshold, the sensor will move to alert status. The assigned value should be within the range defined by Minimum Level and Maximum Level and higher than the assigned Minimum Threshold value. If values out of the range are entered, they will be automatically adjusted to be within range.

Sampling Period: Determines how often the displayed sensor value is refreshed on the Sensor page. A numeric value and a measurement unit (minimum 1 seconds, maximum 999 minutes) should be entered.

Note: Regardless of the sampling period SERIMUX will read the sensor every second and will send an alert as needed based on the configured values. An extended sampling period will not delay an alert response from SERIMUX. The shorter the sampling period, the more traffic that will be seen on the network.

Sensor Alert Settings

A sensor can be configured to notify a user via e-mail alerts or SNMP traps (v1,v2c); alerts are always logged to Syslog messages. Alerts are also indicated in the WEB interface and via Telnet menu.

Disable Alert: Set to Yes or No depending on whether alert messages should be sent regarding this sensor

Alert Delay: The alert delay is an amount of time the sensor must be in an alert condition before an alert is sent. This provides some protection against false alarms. The Alert Delay value can be set for 0-999 seconds or minutes.

Example:
The maximum threshold of a temperature sensor is 90 F, and the temperature of the monitored area is fluctuating between 88 and 91 degrees:

Reading # (taken 1/ second)	Value	Action (with delay set @ 3 seconds
1	88F	
2	89F	
3	90F	Ignored
4	89F	
5	90F	Ignored
6	89F	
7	90F	Ignored
8	90F	Ignored
9	90F	Alert sent
10	89F	

The sensor is in an alert condition in Reading 3 but is back within the acceptable range in Reading 4. At Reading 5, the sensor is in an alert condition again. Without the Alert Delay set, alerts will be sent for both Reading 3 and Reading 5. If the Alert Delay had been set to 3 seconds, an alert would only be sent if the sensor had made three consecutive readings in an alert condition (since readings are made every second). In this case, an alert will not be sent until Reading 9.

Notify Again: Specifies the amount of time before an alert message is repeated. The repeated alert can be set to occur from 1-999 seconds, minutes, or hours.

Notify when return to normal: The user can also be notified when the sensor readings have returned to the normal range by enabling the "***Notify when return to normal***" feature for a sensor.

Automatically acknowledge alert when condition clears: Enable this to have alert notifications in the summary page return to normal state automatically when sensor readings return to normal.

Email Alert Enable: Choose whether or not alert messages should be sent via email

Email Recipient: Enter a valid email address that alert messages should be sent to regarding this sensor.

SNMP Notification: Choose whether or not alert messages should be sent via SNMP

Notification Address: Enter a valid SNMP address that alert messages should be sent to regarding this sensor.

Sensor Log Settings

Data Log Enable: The recording of data log readings from each sensor can be enabled or disabled.

Data Log Storage Location: The only location they can be stored at this time is in system memory.

Enable Syslog: The recording of alert message via syslog from each sensor can be enabled or disabled.

Syslog Location: Syslog messages can be recorded in locations “Local1” through “Local6”. (See Syslog configuration- page 75- for more on this)

Time Stamp with Log: Determine whether a time stamp should be included with each syslog record.

Data Log Frequency: Enter a value to determine how frequently data log entries should be recorded. The value can be set for 0-999 seconds or minutes.

Sensor Authentication

Sensor Authentication Type: Choose between Local or none. None means the sensor can be viewed by any user. Local means the sensor can be viewed by only the users/groups in the sensor access list.

Sensor Access List

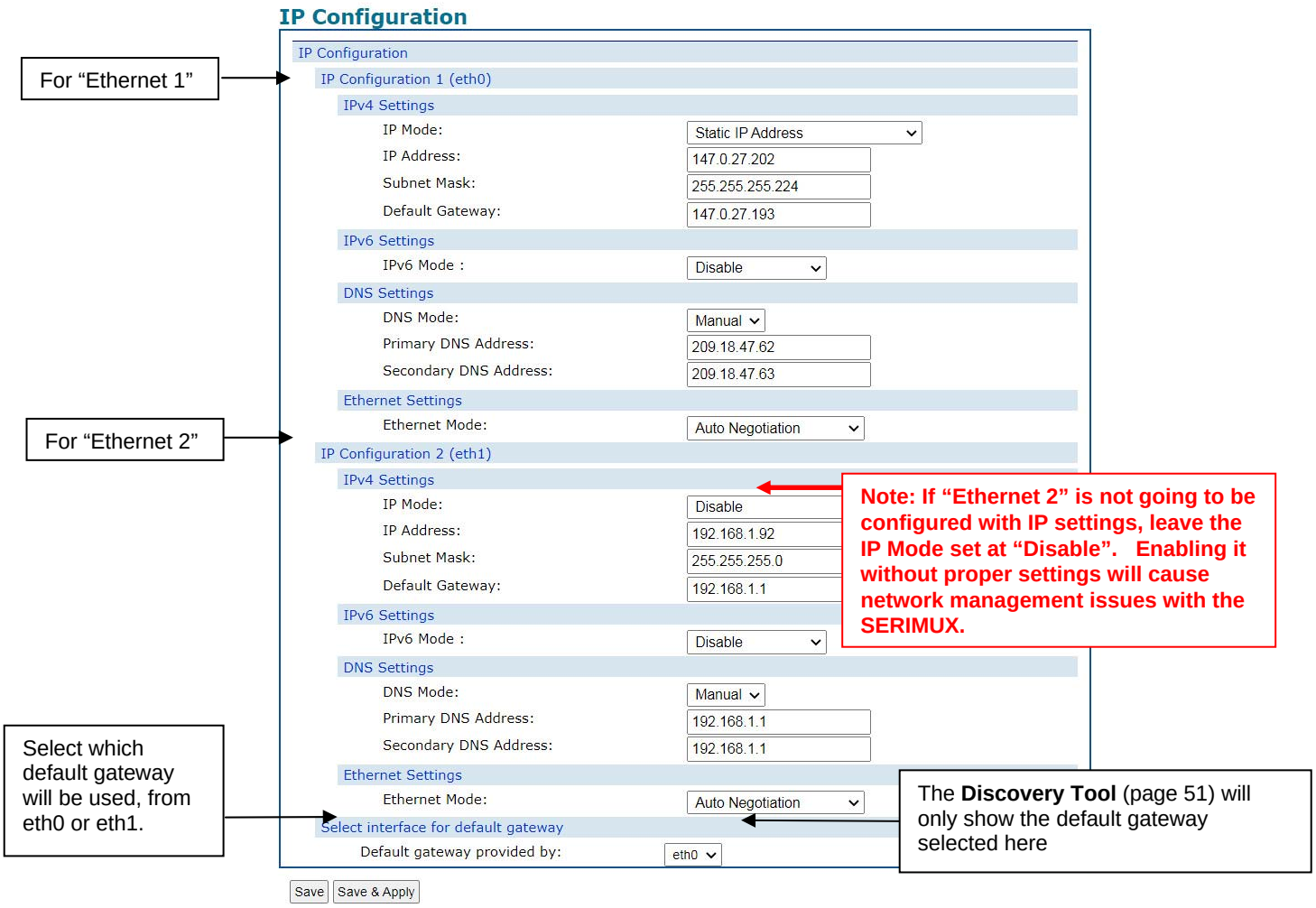
Add User: Add users that will have access to sensor readings when sensor authentication is set to “Local”.
Usernames added must be valid users with access to the SERIMUX as defined under “System Users” (page 77).

Add Group: Add group names as defined under “Access Groups” (page 79) to quickly define who will have access to sensor readings when Sensor Authentication is set to “Local”.

Network Management

IP Configuration

The IP Configuration page is where the settings are applied to enable the SERIMUX to connect to the local LAN or Internet. Only one connection is necessary, but two can be configured for remote SERIMUX access redundancy.



Under “Network Management” in the main menu, select “IP Configuration”. This page is in two sections. Settings for IP Configuration 1 will effect communication at the “Ethernet 1” port and settings for IP Configuration 2 will effect communication at the “Ethernet 2” port. Be sure to apply valid information in the blocks provided.

Be sure to either leave the factory selection of Default Gateway as "eth0" (for Ethernet 1) or change it to "eth1" (for Ethernet 2). This will be the gateway used to access the SERIMUX from other subnets.

Factory Default Settings include:

- IP address: 192.168.1.91
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

The Ethernet Mode can be set for :

- 100 Base T Full Duplex
- 100 Base T Half Duplex
- 10 Base T Full Duplex
- 10 Base T Half Duplex
- Auto Negotiation (default setting)- to allow the SERIMUX to select what will work best for your connection.

Server Configuration

The Server Configuration page is where the settings are applied to enable the SERIMUX to send e-mail and SNMP messages to users and to establish behavioral characteristics for the web interface.

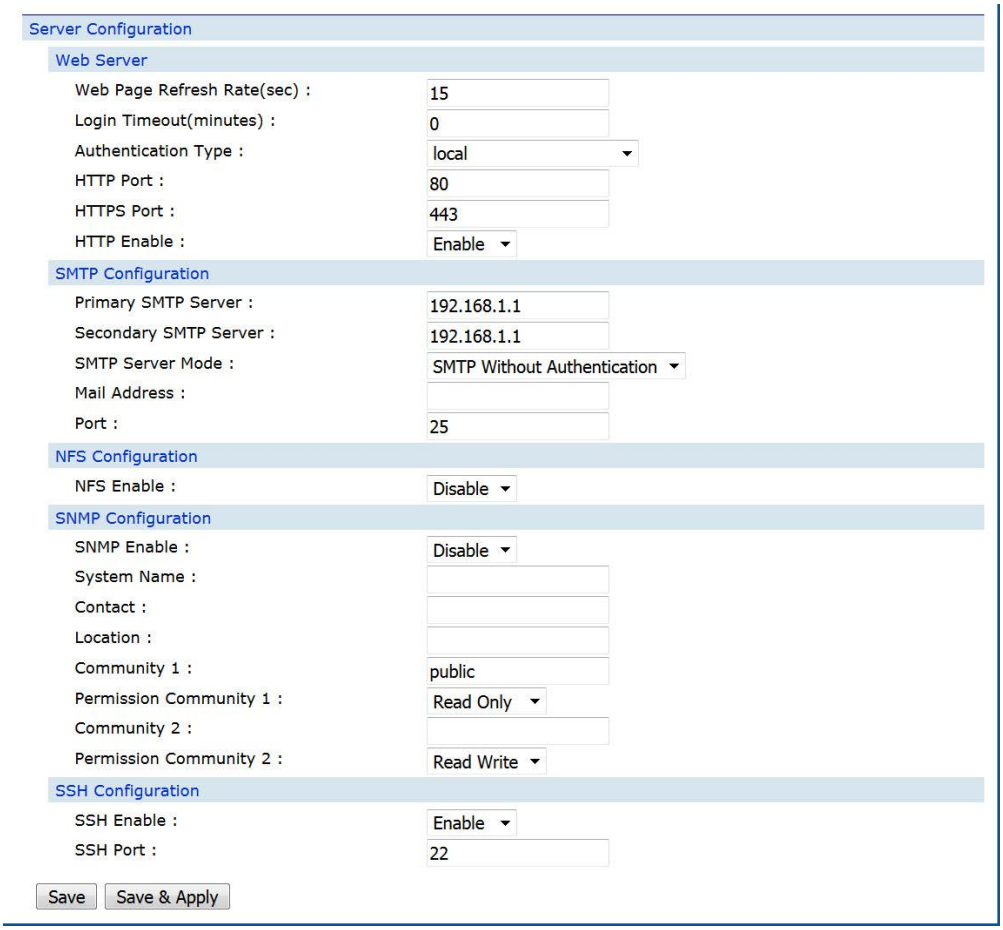


Figure 104- Server Configuration Page

Under “Network Management” in the main menu, select “Server Configuration”. Blocks are provided to apply criteria for the Web Server connection and behavior as well as information to specify the e-mail server and the e-mail address of the SERIMUX. Be sure to apply valid information in the blocks provided.

Setting	Value
Web Server	
Web Page Refresh Rate (sec)	0-999 seconds
Login Timeout (minutes)	0-999 minutes
Authentication Type	Many including local, Radius, Tacacs, TacacsPlus, Kerberos, LDAP, or combinations
HTTP Port	0-65535
HTTPS Port	0-65535
HTTP Enable	Enable or Disable (Disable forces all users to login via SSH)
SMTP Configuration	
Primary SMTP Server	Apply valid IP address
Secondary SMTP Server	Apply valid IP address
SMTP Server Mode	SMTP with or without authentication required
Mail Address	e-mail address assigned to the SERIMUX to use for sending messages
Port	Port on which the SERIMUX will communicate with SMTP server
NFS Configuration	
NFS Enable	Default is disable. Enable to expand the page and apply configuration settings for an NFS server, mounting path, timeout period, and retry interval. See Figure 105.

Setting	Value
SNMP Configuration	
SNMP Enable	Enable or Disable
System Name	Up to 50 characters
Contact	Up to 50 characters
Location	Up to 50 characters
Community 1	Name– example “private” (up to 50 characters)
Permission Community 1	Read only / read-write
Community 2	Name – example “public” (up to 50 characters)
Permission Community 2	Read only / read-write
SSH Configuration	
SSH Enable	Enable or Disable
Port	Port on which the SERIMUX will communicate via SSH (default =22)

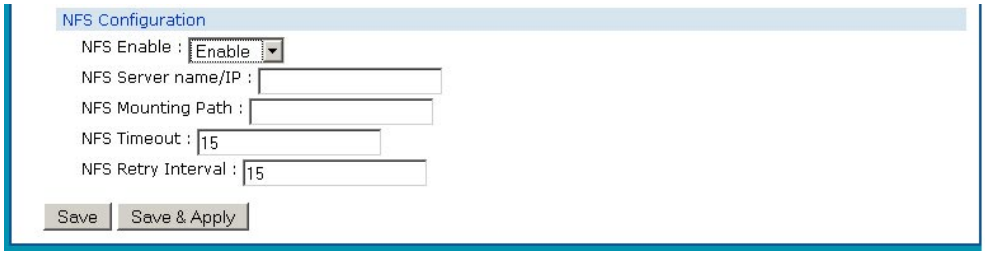


Figure 105- NFS Configuration settings

SNMP

The SERIMUX can send alerts as SNMP traps for all port connect/disconnect events. Using an SNMP MIB browser, a user can monitor all settings. The SNMP agent supports both SNMPv1 and SNMPv2.

Note: The SNMP MIB file (serimuxsec.mib), for use with an SNMP MIB browser, can be found at http://www.networktechinc.com/download/d-srvsw-term-ssh.html . Click on the link to open the file; then save the file to your hard drive to use with the SNMP MIB browser.

TCP Settings

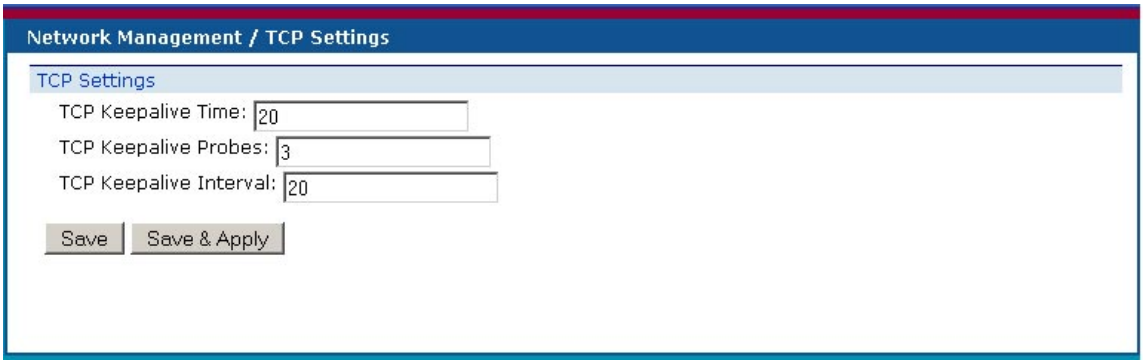


Figure 106- TCP Settings page

Under “Network Management” in the main menu, select “TCP Settings”. Settings are provided to apply values for TCP keepalive parameters. A **keepalive** is a message sent by one device to another to check that the link between the two is operating.

Keepalive time is the duration between two keepalive transmissions in idle condition. TCP keepalive period is configurable and by default is set to 20 minutes. The range of acceptable values is 0-999 minutes.

Keepalive Probes is the number of retransmissions to be carried out before declaring that remote end is not available. The default value is 3, and the range of acceptable values is 0-999.

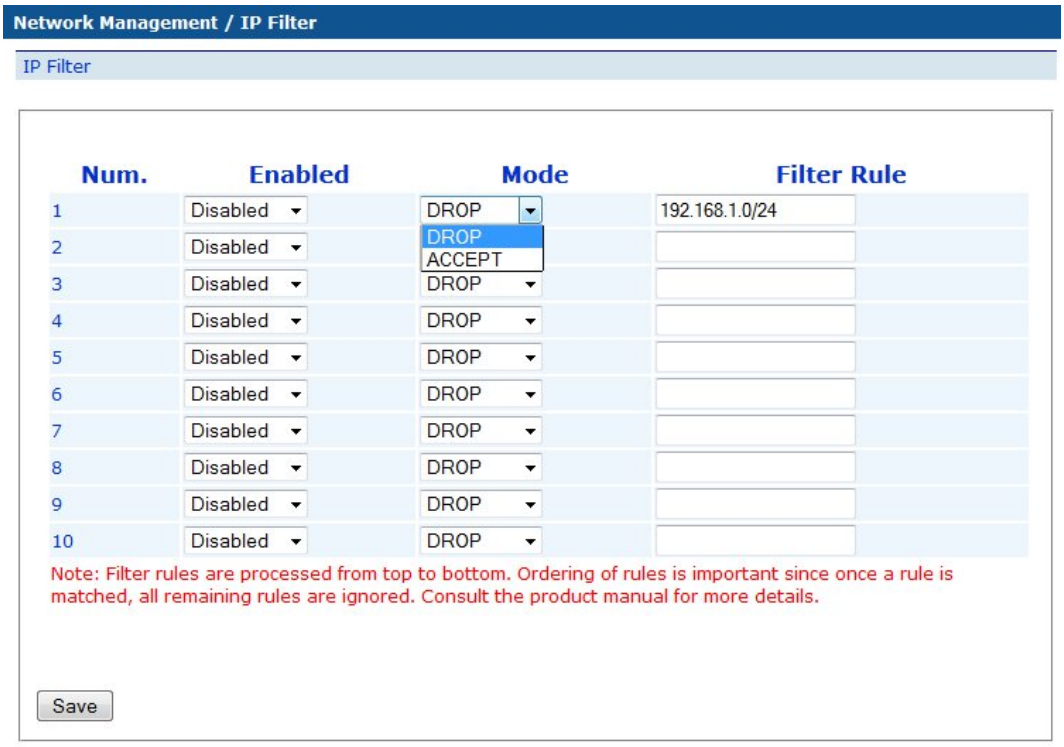
Keepalive Interval is the duration between two successive keepalive retransmissions, if acknowledgement to the previous keepalive transmission is not received. The default value is 20 minutes, and the range of acceptable values is 0-999 minutes.

IP Filters

Included in the Network Management options is IP Filtering. IP Filtering provides an additional mechanism for securing the SERIMUX. Access to the SERIMUX network services (SNMP, HTTP(S), SSH, Telnet) can be controlled by allowing or disallowing connections from various IP addresses, subnets, or networks.

Up to 10 IP Filtering rules can be defined to protect the SERIMUX from unwanted access from intruders. Each rule can be set as Enabled or Disabled. Rules can be set to explicitly drop attempts to connect, or to accept them.

Be sure to press **Save** after changes are made.



More on IP Filtering

The most common approach is to only allow “whitelisted” IP addresses, subnets, or networks to access the device while blocking all others. The IP Filters are processed sequentially from top to bottom, so it is important to place the most precise rules at the top of the list and the most generic rules at the bottom of the list.

As an example, assume we wish to block all connections except those which come from the IP address 192.168.1.100. To allow connections from 192.168.1.100, we need to configure and enable an ACCEPT rule at the top of the list:

Then, to block all other IP addresses from connecting to the SERIMUX, we add a rule to drop all other connections.

If the preceding “drop all connections” rule was placed in position one, no connections at all would be allowed to the unit. Remember: rules are processed from top to bottom. As soon as a rule matches, the processing stops and the matching rule is executed.

To match a particular IP address, simply enter in the desired IP address (e.g. 192.168.1.100).

To match a subnet, enter in the subnet with the associated mask (e.g. 192.168.1.0/24).

To match all IP address, specify a mask of 0 (e.g. 0.0.0.0/0).

Administrative Settings

Unit Settings

The Unit Settings page provides fields for setting up the name, administrative password, and system date and time settings.

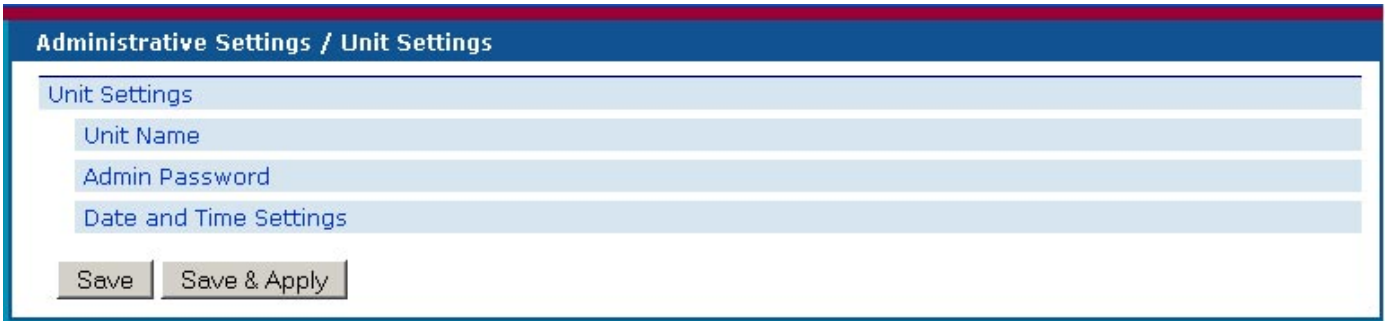


Figure 107- Unit Settings page

Under "Administrative Settings" in the main menu, select "Unit Settings". Fields are provided as described below:

Setting	Description	Value
Unit Name	Name for the SERIMUX	Maximum of 50 Characters- Alphabetical or Numeric
Root Password	Password for user "root" **This menu selection is only accessible if user "root" is logged in**	Maximum of 50 Characters- Alphabetical or Numeric- **Case Sensitive** (default is "**nti**")
Date and Time Settings	Apply current date and time-or enable NTP server	Valid date format mm/dd/yy / Enable NTP

FYI- The SERIMUX complies with the new U.S.-Daylight Saving Time rules (passed in 2005).

Unit Settings->Admin Password

Under "Unit Settings", select "Admin Password". On this page the administrator can change the default password for user "root" from "**nti**" to a new password. Enter the desired password (maximum 50 ASCII characters- case sensitive) in the block "Admin Password". Once entered, re-enter the new password in the "Confirm Password Change" block provided.

Be sure to press "**Save**" to have the change take effect after the next reboot of the SERIMUX, or "**Save & Apply**" to have the change take effect immediately.

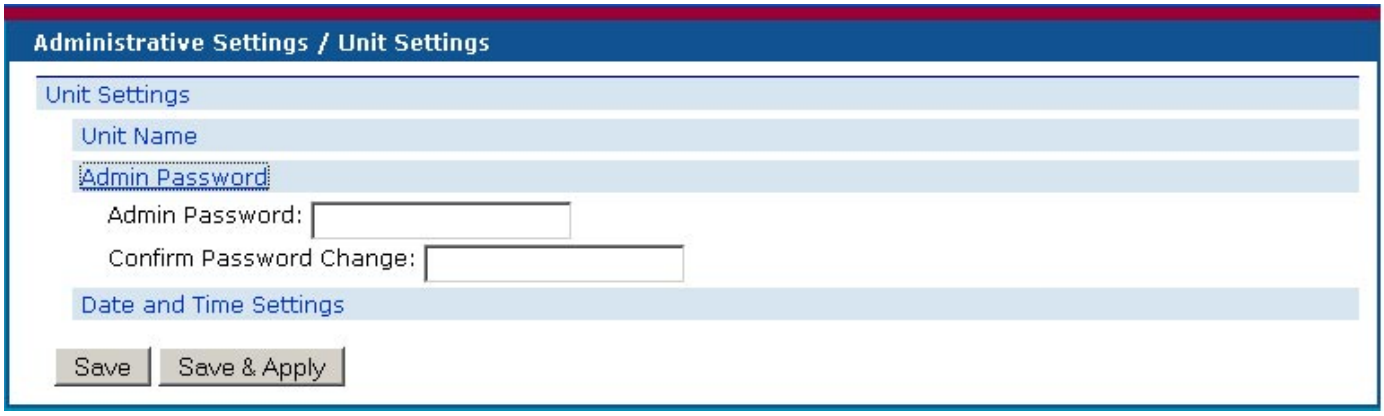


Figure 108- Change password for user "root"

Note: The password entered will be case sensitive so be sure to note what characters are upper or lower case if any are alphabetical. The password characters are displayed as '*' (asterisk) characters while entering them.

Note: If the administrator password is not known, contact NTI for instruction on resetting the SERIMUX to defaults.

Unit Settings->Date and Time Settings

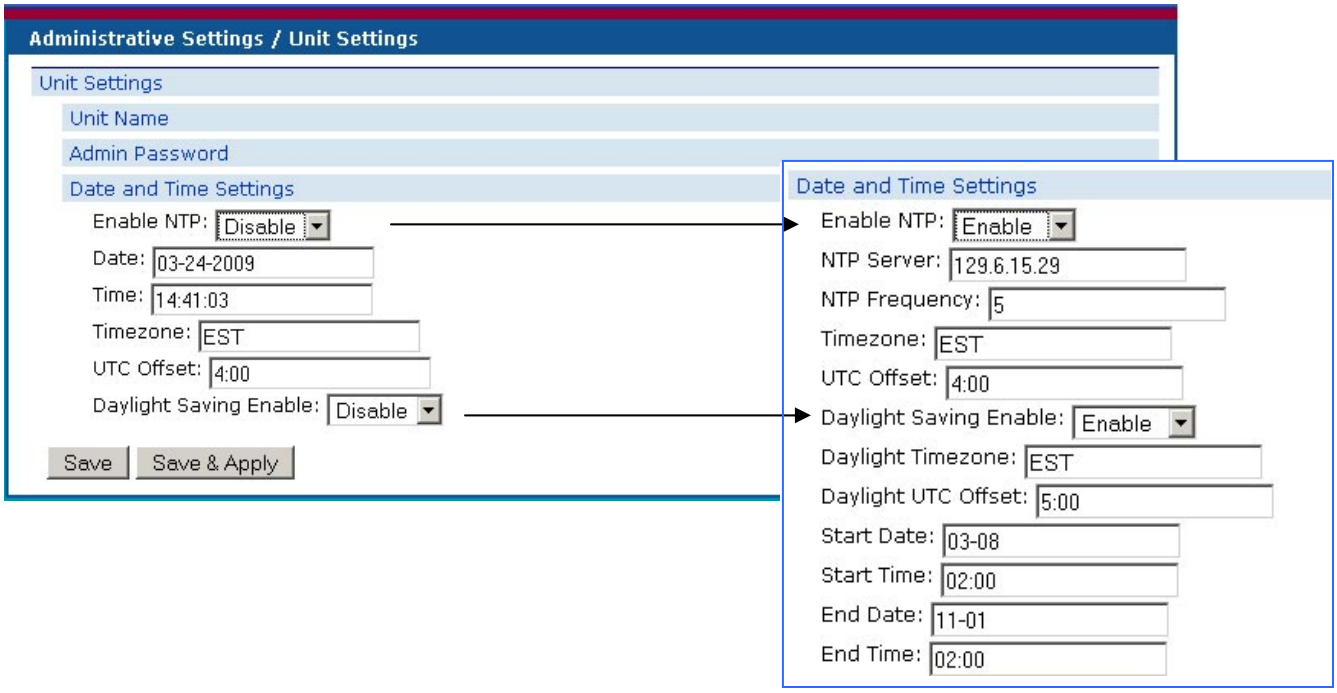


Figure 109- Unit Settings page, date and time

The Date and Time of the SERIMUX (**Administrative Settings->Unit Settings->Date & Time Settings**) can be either manually setup to use an onboard clock or set to be synchronized with an NTP server.

To synchronize it, change the "Enable NTP" value from "Disable" to "Enable". Enter appropriate values for

- IP address of the NTP Server
- Frequency (how often, in hours (0-99), the SERIMUX will query the NTP Server)
- time zone for the location of the SERIMUX.

To set it manually, set the "Enable NTP" value to "Disable". Enter the

- date in mm/dd/yyyy format
- time in 24 hour format hh:mm:ss .
- time zone for the location of the SERIMUX
- the UTC offset from GMT (if you are located in GMT, the value is "00.00")

The UTC offset value is hh.mm (hours.minutes). If you are behind GMT, the value will be negative (i.e. "-02.00"). If you are ahead of GMT, the value will be positive (i.e. "+02.00" or "02.00").

In order to have the time change in accordance Daylight Saving Time rules, set the value of "Daylight Saving Enable" to "Enable". and select the appropriate time zone in the "Daylight Time zone" box. Also be sure to apply proper Start Date/Time and End Date/Time values for when Daylight Saving Time begins and ends.

Be sure to press "**Save**" to have the changes take effect after the next reboot of the SERIMUX, or "**Save & Apply**" to have the change take effect immediately.

Security Settings

The Security Settings page enables the administrator to configure the CLI (Command Line Interpreter) authentication type to be used to connect with serial devices. Choose from many common CLI authentication methods.

To have the option to use Telnet to login, change the Disable to Enable. Be sure to click "**Save"** or "**Save & Apply"**.

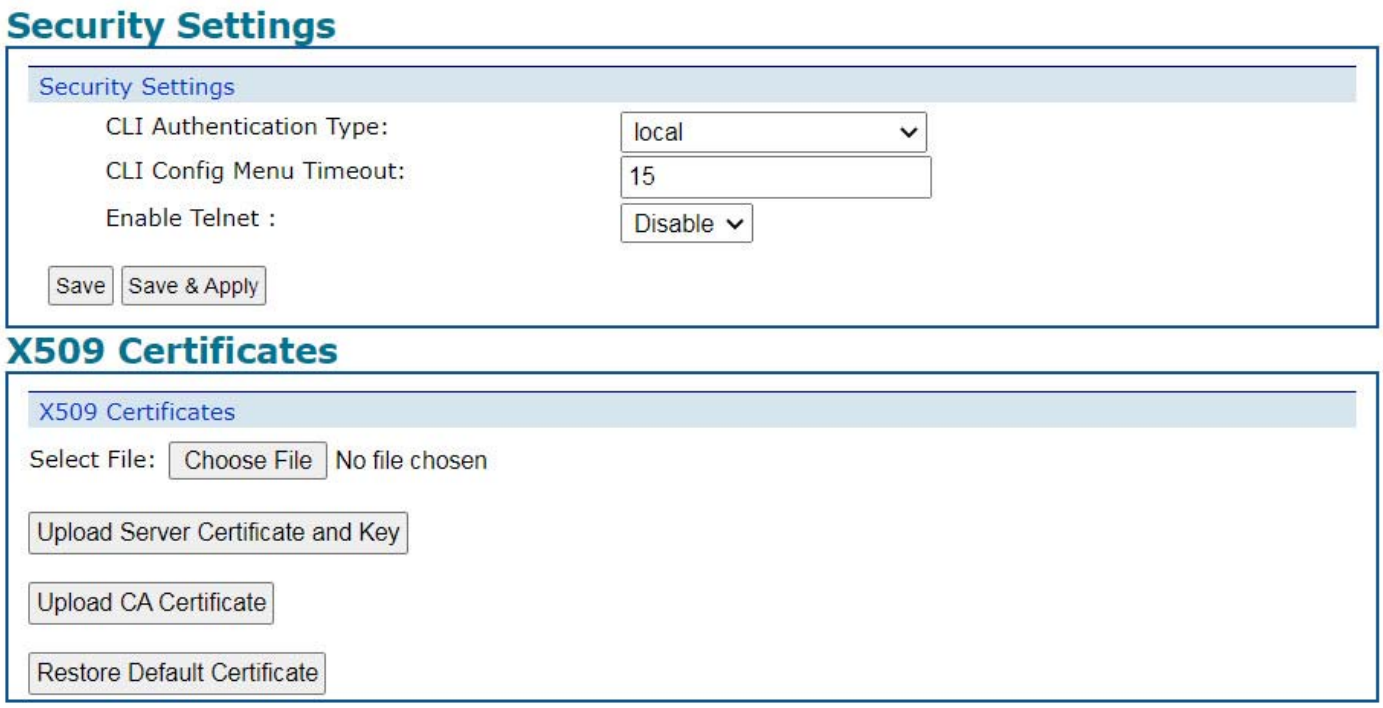
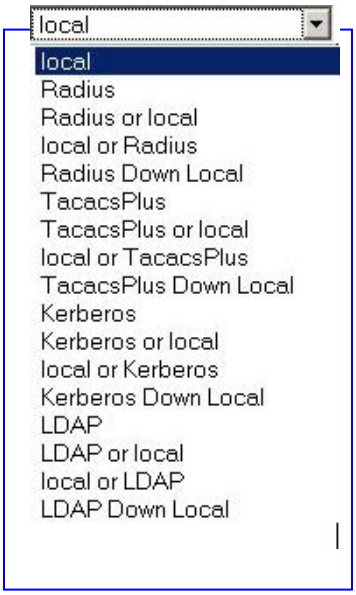


Figure 110- Security Settings page

Under “Administrative Settings” in the main menu, select “Security Settings”. Click on the arrow to open a drop-down box listing various CLI authentication types (below), and select one. Then apply a timeout value (in minutes) from 0-99. A value of 0 disables the timeout.



X509 Certificate

The SERIMUX is designed to be configurable with secure access to the web interface controls. The SERIMUX is pre-loaded with a generic X509 Server Certificate. If you wish to provide your own X509 Server certificate, the Server certificate must be uploaded to the SERIMUX. The Server certificate and key must be combined in a single file ("PEM" format). For instruction to create your own certificate, see "How to Create x509 Certificate" for more information.

.

Browse to the Server certificate file and select it. Then load using the button "**Upload Server Certificate and key**".

Note: The key used should not be password protected.

X509 Certificate Authority

A Certificate Authority (CA) needs to be used to sign the server certificate described above. This Certificate Authority can be created as a self-signed certificate in "CRT" format. It can also be given to you by an external Certificate Authority in "CRT" or "PEM" format.

For https to work properly, you must load the certificate of your CA onto the SERIMUX. Use the "**Browse"** button to browse to the file containing the CA certificate (which may also contain an intermediate certificate) and select it. Then click on the "**Upload CA certificate**" button. Please see "How to Create x509 Certificate" for more information.

Please reboot the device after uploading a certificate for the changes to take effect.

The "**Restore default certificate**" button will restore the unit's default self-signed certificates if needed.

Syslog

The Syslog page contains the settings that effect the location, size, name, and destination when downloaded of the System Log. The System log displays a listing of all users that have logged in and out of the SERIMUX, providing the date and time of their login and logout. It also displays when configuration changes are made. From the Syslog page, log records can be deleted to make room for more.

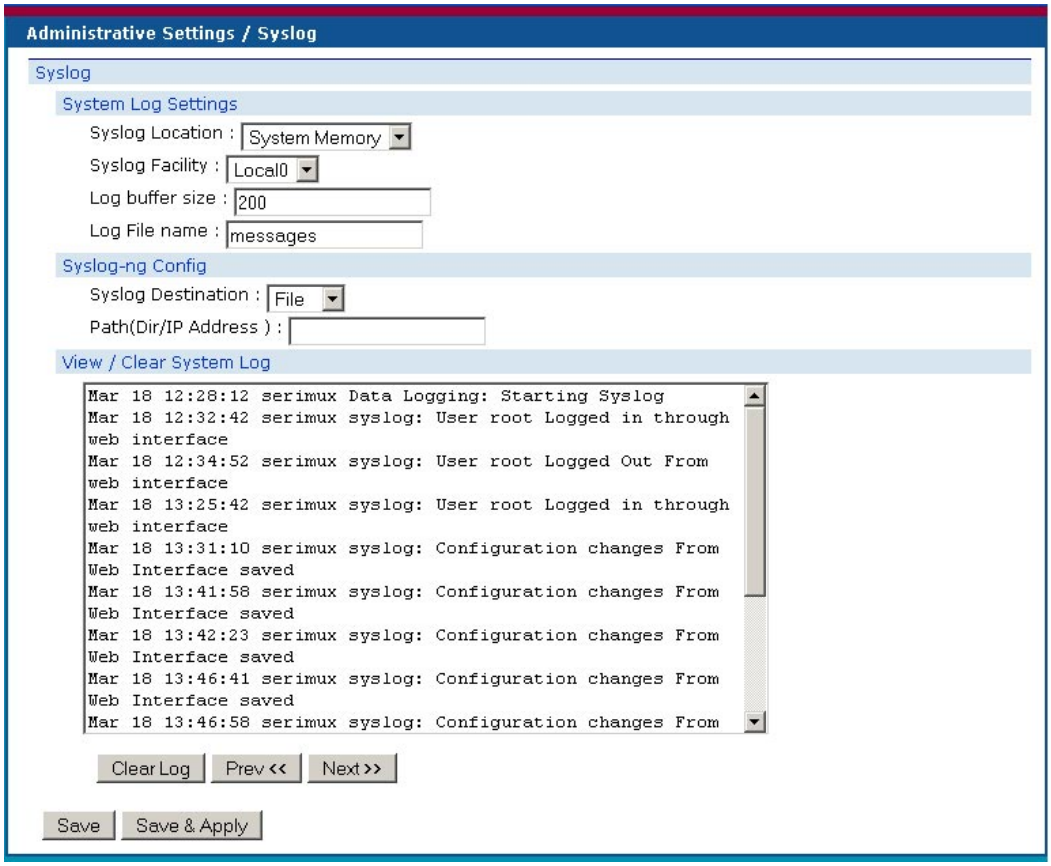


Figure 111- Syslog page

Under “Administrative Settings” in the main menu, select “Syslog”.

Setting	Value
System Log Settings	
Syslog Location	System Memory (no options as of this printing)
Syslog Facility	Local0 (no options as of this printing)
Log Buffer Size	0-999 K bytes
Log File name	1-100 characters
View System Log	None- view accumulated system logs
Clear System Log	delete system logs
Syslog-ng Config	
Syslog Destination	File / TCP / UDP
Path	drive and directory (when destination is File), or IP address (when destination is TCP or UDP)
View / Clear System Log	**None- view accumulated system logs and clear them if desired**

A list displaying up to 1K bytes of log records is displayed (use the scroll bar to see all of them). Press the “**Next>>”** button to display the next 1K byte of log records. The System Log can be viewed and cleared from this page.

To store syslog data in locations other than on the SERIMUX, configure the Syslog-ng Config settings for writing it to a flash drive, NFS, or sending it to a remote location via TCP or UDP.

Press “**Clear Log**” to delete the complete syslog record.

Note: The syslog will be cleared completely and immediately and will not be retrievable when “Clear Log” is pressed, so be sure that is what you want to do.

When changes are complete, press “**Save & Apply**” to make them take effect immediately in the SERIMUX.

Firmware Update

The Firmware Update page is used to introduce firmware files that provide the architecture of the user interface. Occasionally new features or changes to existing features will be introduced and new firmware with these changes will be made available on the NTI website (http://www.networktechinc.com/srvsw-term-ssh.html). Once a user has downloaded the required file for firmware upgrade, this page will be used to upload them to the SERIMUX.

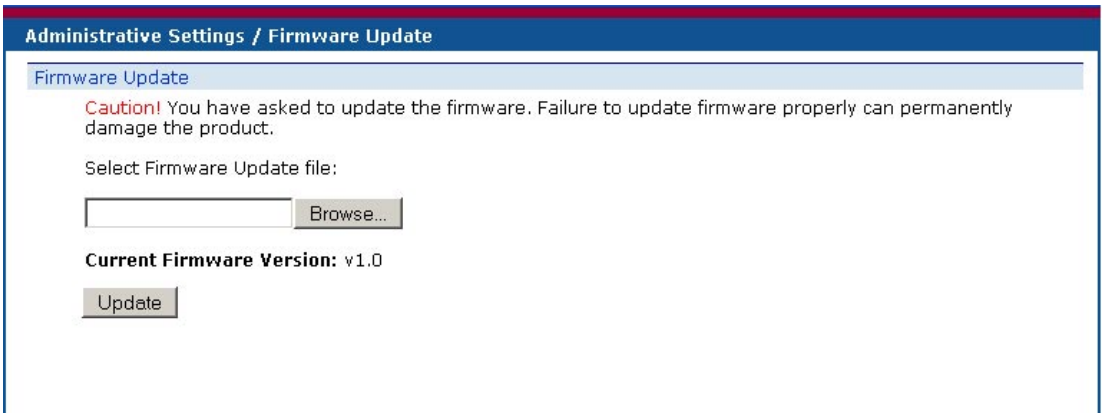


Figure 112- Firmware Update page

Under "Administrative Settings" in the main menu, select "Firmware Update". Click on the "Browse" button and locate and select the firmware file for the SERIMUX (***serimux_ssh_vx_xx.tar.gz***).

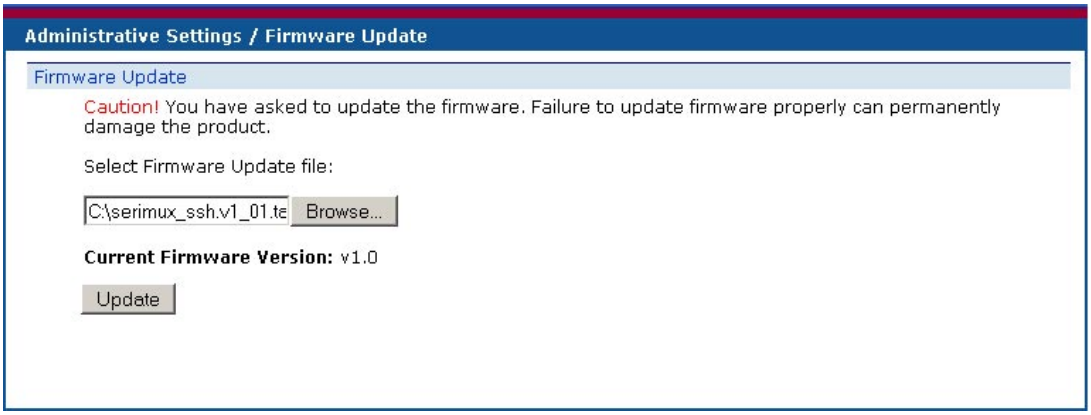


Figure 113- Firmware Update- file selected

Click on the "Update" button to perform the firmware update. The firmware will take between 60 and 90 seconds to update. Once the update file has been applied to the SERIMUX, and message "Status = Firmware update done!" will be displayed.

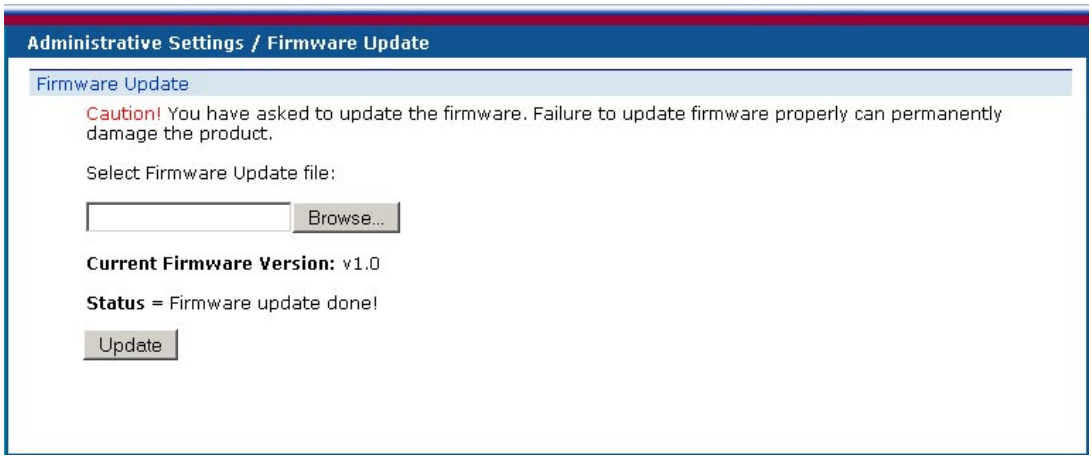


Figure 114- Firmware update done

To see the effects of the new firmware file the SERIMUX must be rebooted using either of three methods:

- use the “Reboot” feature in the main menu (see page 82)
- power cycle the SERIMUX
- press the “Reset” button on the rear of the SERIMUX (see page 85)

The SERIMUX will continue to operate normally using the previous firmware until it has been rebooted.

After rebooting (approximately 45 seconds), refresh the browser screen and log back in to the SERIMUX to resume operation. Any user names, passwords, and all configuration settings will remain in place and in effect.

If the wrong file is submitted to the SERIMUX to perform the firmware upgrade, the message “Status = Firmware update failed!”. Double-check that the file in the selection block is the correct SERIMUX firmware file in the format ***serimux_ssh_vx_xx.tar.gz***.

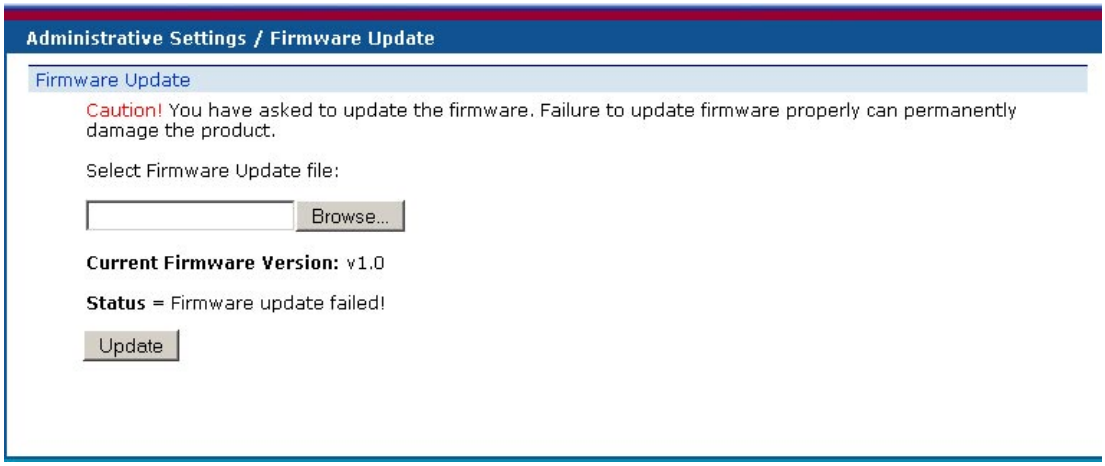


Figure 115- Firmware update failure

User Management

System Users

The System Users page displays a list of assigned user names. From this page users can be added, deleted, or selected for editing.

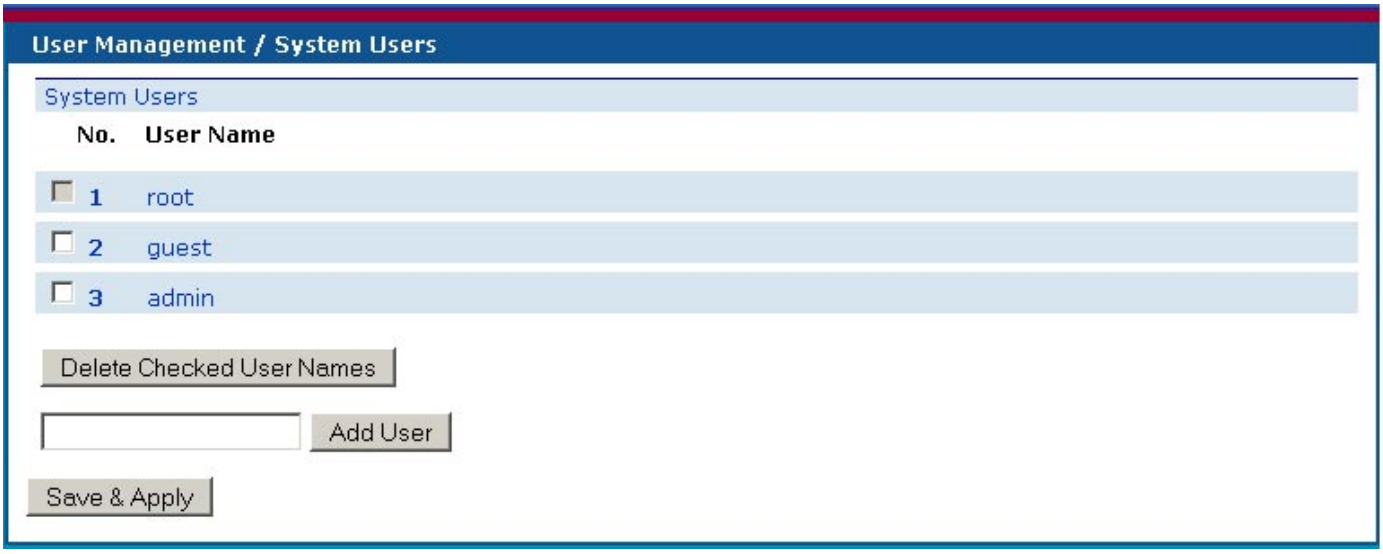


Figure 116- System User page

Under “User Management” in the main menu, select “System Users”.

To delete a user, or several users, click with the mouse to place a check mark in the check boxes to the left of the user number(s). (The user “root” cannot be deleted.) Then click on “Delete Checked User names”.

To add a user, enter the name desired for the new user (maximum 50 characters) and press “Add User”. The page will expand to include configuration criteria for the user.

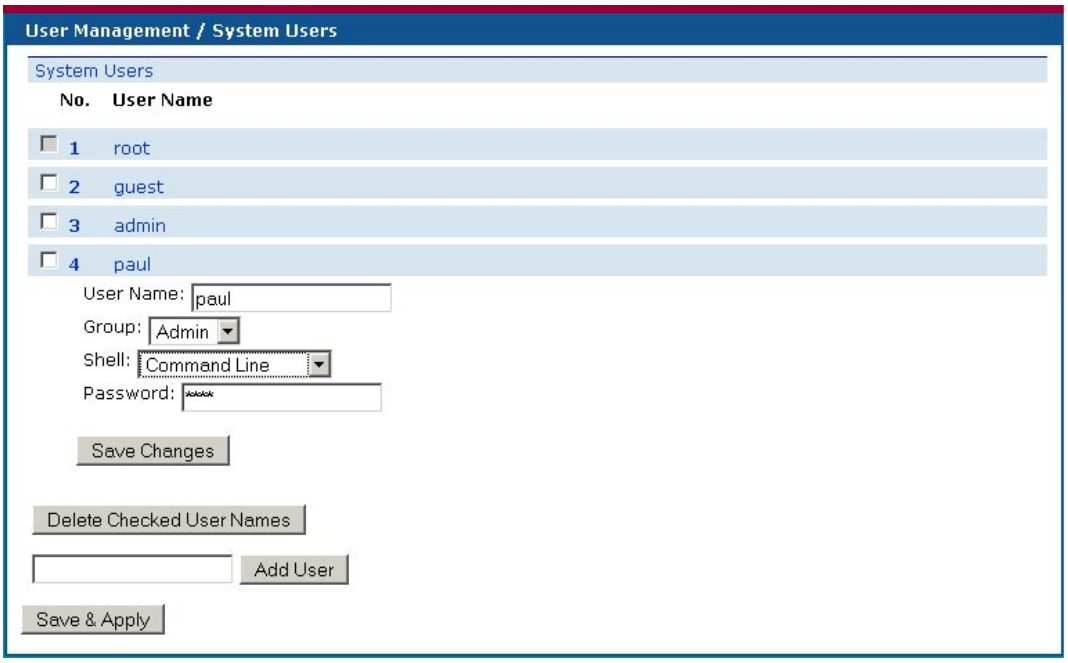


Figure 117- User configuration

Users have the following parameters to be configured:

Name: Names can be changed as desired (up to 50 alphabetical or numeric characters).

Group: Each operator must be defined as either a “Admin” type operator with full administrative rights, or as a “User” type operator with only the ability to access ports as defined under Port Configuration (page 55).

Shell: The Shell parameter defines where the operator will be directed to when they login to the SERIMUX through Telnet or SSH. Choices for “Admin” operators include:

- Command line- SERIMUX will open a command line interface
- Config menu- SERIMUX will open configuration menu
- Port Connect menu- SERIMUX will open Port Connect menu

Operators defined as “Users” can only make connections to ports, so their only option will be to login to the Port Connect menu.

Password: Enter a password for the selected user to use at log in (up to 50 alphabetical or numeric characters- case sensitive)

All passwords can be changed except the “root” password. A user must be logged in as “root” to change the password for user “root”, and it can only be changed from the “Unit Settings” menu (page 71).

If a change is made to the user name, group, or shell, the password for that user must also be provided (whether it is a new password or an existing password). Otherwise the user will be assigned the default password of “nti” to login the next time.

If a user logs in to a port and that user is not yet registered in the SERIMUX, the SERIMUX will check the RADIUS server registered users and if the username and password are registered in the RADIUS server, they will be added to the SERIMUX registered users as well.

Note: Irrespective of the Authentication type selected (page 68), all users of the SERIMUX must be added to the system users list in order to have access to the SERIMUX.

Note: Users auto roll when the 50 user limit is reached (the oldest user is auto removed and the new user is added)

Access Groups

The Access Groups page lists the assigned access group names. Access groups are used to provide a quick method of defining which users have accesses to devices. Once access group names are assigned, users are specified to be included in those groups. With properly defined groups, connected devices can be configured (see "port access list" -page 55) as to which access groups have access. Assigning users to Access Groups will save port configuration time.

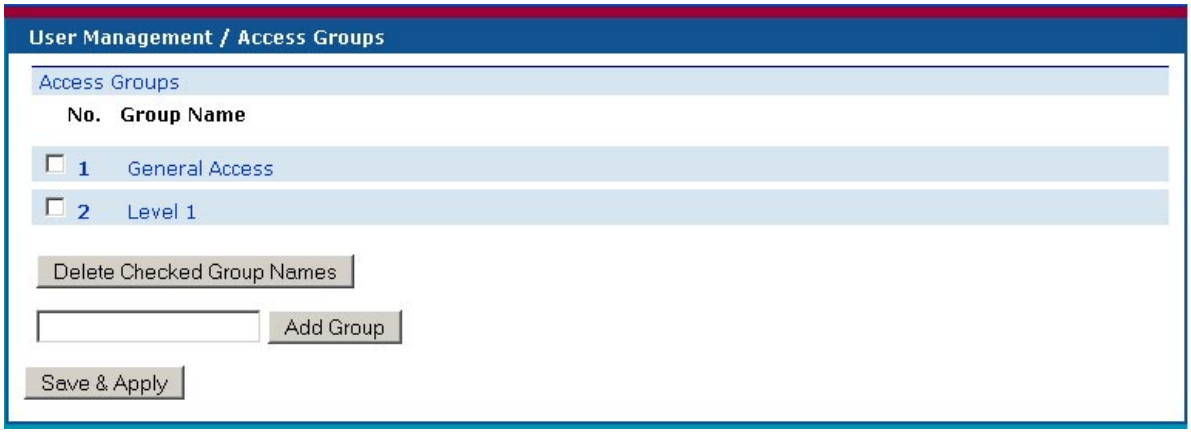


Figure 118- Access Groups page

Under "User Management" in the main menu, select "Access Groups". To add a group, enter the name desired for the new group (maximum 50 characters) and press "**Add Group**". The group name will be added to the list. To define what users are in the group, click on the group name to expand the page.

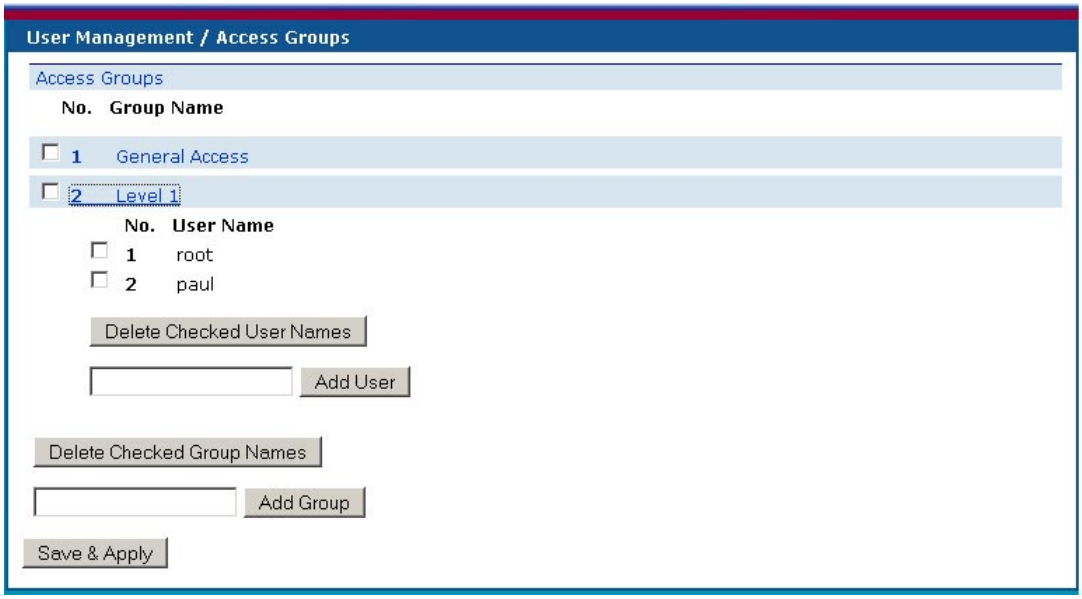


Figure 119- Edit user names listed in Access Group

To add users to a group, type in a valid User Name and press "**Add User**". The page will refresh and the User Name will be added.

To delete users from a group, click on the check boxes for the users to be deleted, and press "**Delete Checked User Names**". The page will refresh with an updated list of User Names.

To delete groups from the Access Groups list, click on the check boxes for the Access Groups to be deleted, and press "**Delete Checked Group Names**". The page will refresh with an updated list of Access Groups.

When changes are complete, press "**Save & Apply**" to make them take effect immediately in the SERIMUX.

Administrative Information

System Log

The System Log page displays a listing of all user access to the SERIMUX, providing the date and time of their login and logout. It also displays when configuration changes are made.

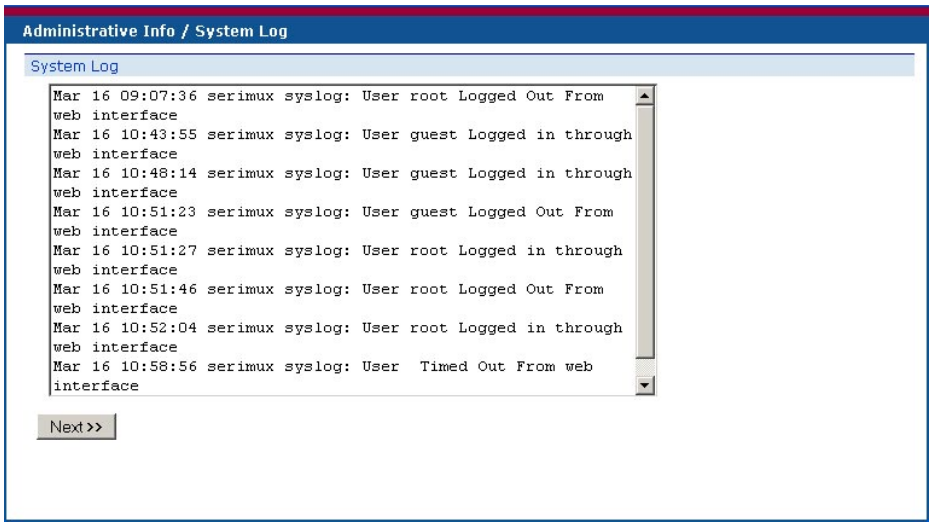


Figure 120- System Log displayed

Under "Administrative Information" in the main menu, select "System Log". A list displaying up to 1K bytes of log records will be displayed (use the scroll bar to see all of them). Press the "**Next>>"** button to display the next 1K bytes of log records. The System Log can only be viewed from this page. To clear the log, see the "Administrative Settings-Syslog" page (page 74).

System Information

The system information page displays the model name of the SERIMUX, the firmware version in the SERIMUX, the MAC addresses of the Ethernet ports, the date in the system, and syslog status. To view the System information, under "Administrative Information" in the main menu, select "System Information".

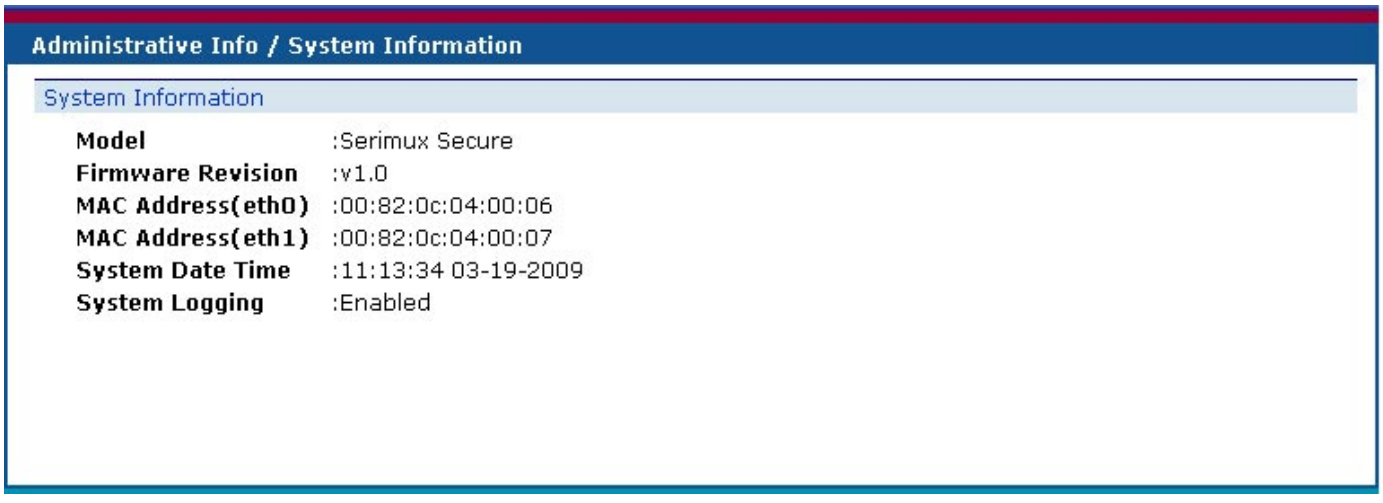


Figure 121- System Information page

Network Information

The Network Information page displays all of the current network settings for the Ethernet ports on the SERIMUX. Settings include IP mode, IP address, netmask, Default gateway, and DNS addresses. To view the network settings, under “Administrative Information” in the main menu, select “Network Information”. To edit these settings, see “Network Management” on page 67.

The Default Gateway will be the gateway selected as the "Default gateway" under "IP Configuration" on page 67. The SERIMUX will use only one gateway.

If "Ethernet 2" is disabled, the IP Address, Mode will not be shown for it (as below).

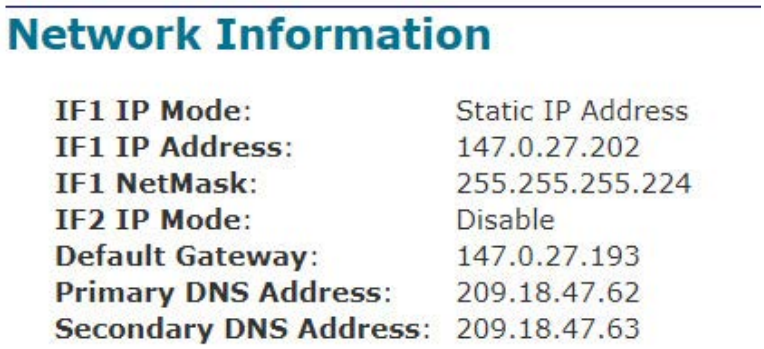


Figure 122- Network Information page

Support

From the SERIMUX web interface the user can quickly access the NTI website where a pdf copy of this manual and a link to the SERIMUX firmware download page can be found.

The “Support Menu” includes two links;

“Manual”- leads to the NTI SERIMUX web page where you can download a pdf copy of the Owner’s manual

“Downloads”- leads to the SERIMUX web page containing downloads for SERIMUX firmware updates (see page 76)

Note: As of this publication, the current and only available firmware is version 1.0, so the links lead to the SERIMUX Website where other links can be found for instruction or general information regarding the SERIMUX.

Figure 123- Support Links

Reboot

The Reboot page enables the user with administrative rights to easily reboot the SERIMUX as needed.

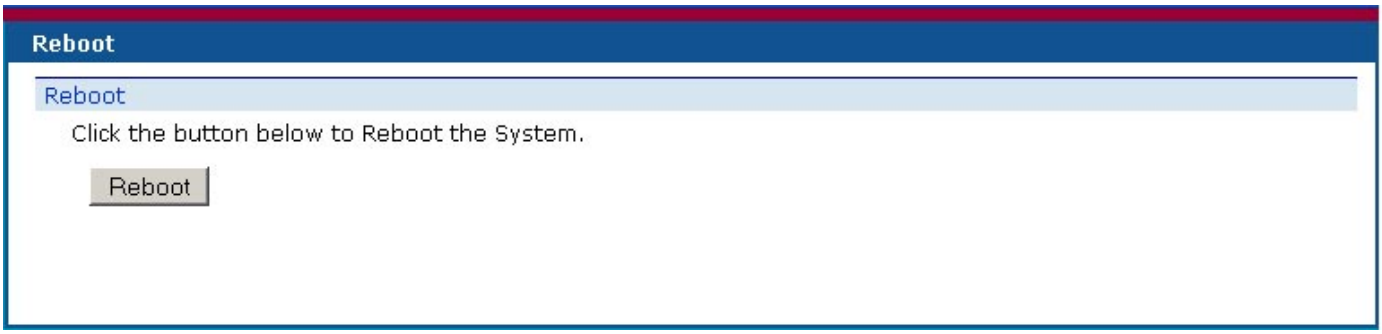


Figure 124- Reboot page

To use the Reboot page, select "Reboot" from the main menu. Press "**Reboot**" button to force the SERIMUX to log all users out and power cycle its processor. Any changes that were in cue from pressing the "**Save**" button (on another page) without pressing "**Save and Apply**" will be made to the entire system. All users will need to log back in to resume operation.

Note: If other users were making changes when Reboot is being used, and their changes were not saved, those changes will be lost.

A reboot will take approximately 45 seconds to occur. Refresh your browser and log back in to the SERIMUX as desired.

Logout

When a user is finished accessing the SERIMUX WEB interface, it is recommended that the user click on the "Logout " link in the side menu. If the "Logout" link isn't used, the web interface can be accessed by anyone that sits down to the desk where it is logged in until SERIMUX automatically logs the user out. The automatic logout, by default, will occur after 15 minutes of access time.

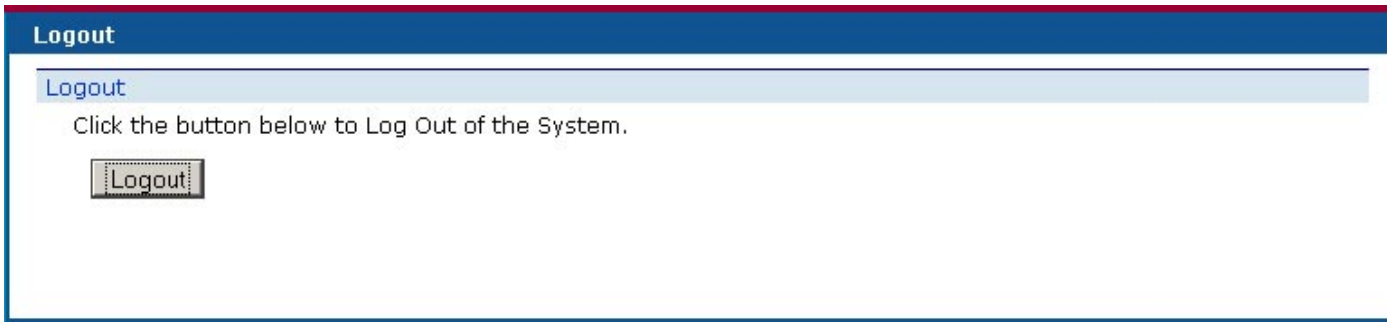


Figure 125- Logout screen

TELNET OR SSH CONNECTION

The SERIMUX shell, configuration menu and port connection menu can be accessed using a Telnet or SSH client. Connect to the SERIMUX using a standard port configuration (23 for Telnet, 22 for SSH) and login as either the "root" user or any system user (page 77). Menus as described under Serial Control (page 15) enable the operator with administrative rights to configure the SERIMUX, and operators with user rights to access ports as defined by the administrator.

FYI: From the shell prompt, IPMItool commands are also supported.

The user may connect to SERIMUX using a Telnet client like HyperTerminal or SSH client like Putty. Before these can be used, two conditions must be met:

1. A computer running a Telnet client must first be able to connected to SERIMUX through the ETHERNET port (see "Connect to the Ethernet" on page 7).
2. An SERIMUX Ethernet port must be configured for connection. This can be done through RS232 (page 10) and then using the Config Menu or using the web interface (page 67).

The Telnet or SSH menus and behavior are identical to controlling the SERIMUX using a connected terminal with RS232.

Telnet via HyperTerminal

Open HyperTerminal and configure the connection to use TCP/IP. Enter the IP address of SERIMUX (default is 192.168.1.91) and port number 23 (see Figure 126).

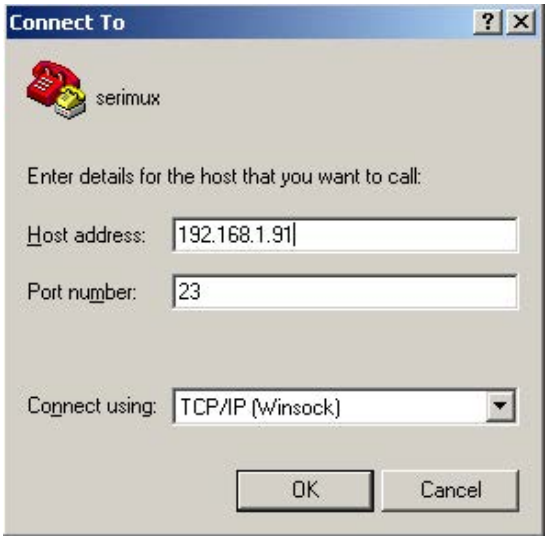


Figure 126- Telnet connection via HyperTerminal

Telnet via Command Prompt

At a command prompt (DOS window), type the following command to connect to ENVIROMUX:

C:\>*telnet 192.168.1.91 23* (or substitute current IP address)

Press **<Enter>** and continue as described on page 10.

RADIUS CONFIGURATION

Please follow the steps below to set up radius authentication for SERIMUX Ports.

1. Setup your user on your radius server. If you are using a service like Freeradius, you can add a user (using an entry similar to below) to the "users" file usually located in `/etc/raddb/` .

Please note the tab character preceding the second line. Restart the service and move to step 2 to setup SERIMUX.

root Cleartext-Password := "nti"

Service-Type = Login-User

2. Go to **User Management -> System Users** (page 78) and add the radius user with same username to SERIMUX. We recommend you set the same password that is in the radius server for this local user. This is required for local verification of allowed users.

3. Go to individual Port configuration in **Port Management' -> Port Configuration -> Click on desired Port** (page 55). In Authentication section (page 57) select one of "Radius", "Radius or local" (Radius server will be tried first. Upon failure local user will be tried), "local or Radius", "Radius Down local" (Local users will be tried only if Radius server cannot be reached). Enter the radius server settings and include radius secret as set in your server.

4. Go to **Port Access List** section (page 58) and add the users you wish to be able to access this port and click '**Save & Apply'**.

Now the SERIMUX will contact your radius server for authentication as set for any port logins.

If a user logs in to a port and that user is not yet registered in the SERIMUX, the SERIMUX will check the RADIUS server registered users and if the username and password are registered in the RADIUS server, they will be added to the SERIMUX registered users as well.

Note: If your radius service requires a Vendor ID (i.e. Microsoft Network Policy Server), the NTI Vendor ID for Radius is 3699.

RESET BUTTON

The "RESET" button on the back of the SERIMUX may be used for power cycling the SERIMUX processor without actually power cycling the rest of the SERIMUX.

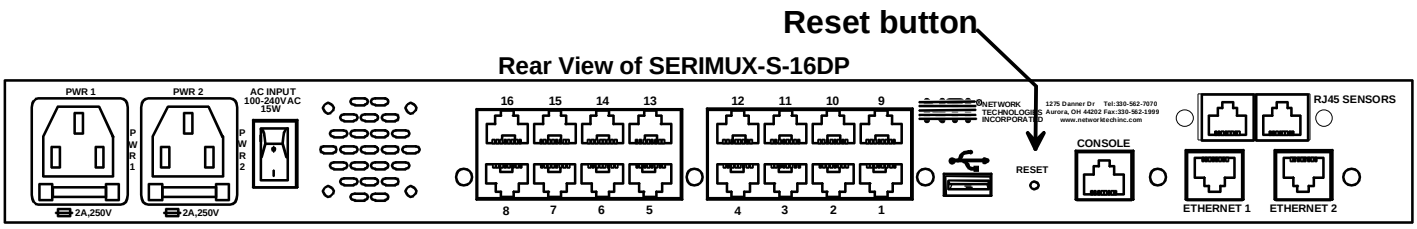


Figure 127- Location of RESET button

CHANGE CONSOLE PORT BAUD RATE

The administrator may desire to change the baud rate of the console port from its default baud rate of 115200. Use the following instruction to make that change.

1. Connect the console port of the unit to the serial port of any terminal or PC and open a terminal window. Configure it as follows:
    - direct connection (using the appropriate CPU local serial Com port)
    - 115200 bps
    - 8 bits
    - no parity
    - 1 stop bit
    - no flow control
    - ANSI or VT100 terminal mode.

2. Power ON the SERIMUX.

3. When prompted in the terminal window for "`press any key`" press a key before the prompt times out. A bootloader prompt "`serimux>`" will appear.

4. Type <**`run set_baud>`** and press <**`Enter`**>.

5. Enter the desired baud rate (any standard baud rate from 50 kbps to 115200 kbps) and press <**`Enter`**>.

6. Change the terminal or PC serial port baud rate to the baud rate entered in step 5.

7. Click back in the terminal window and press <**`Enter`**>.

8. To get to a login prompt, power cycle the SERIMUX or type the command <**`reset>`** on bootloader prompt and press <**`Enter`**>.

9. Allow the SERIMUX to boot up as normal.

INTERCONNECTION CABLE WIRING METHOD

The cable connecting the terminals and devices to the SERIMUX must be terminated with RJ45 connectors and must be wired according to the EIA/TIA 568 B industry standard. Wiring is as per the table and drawing below.

Pin	Wire Color	Pair	Function
1	White/Orange	2	T
2	Orange	2	R
3	White/Green	3	T
4	Blue	1	R
5	White/Blue	1	T
6	Green	3	R
7	White/Brown	4	T
8	Brown	4	R

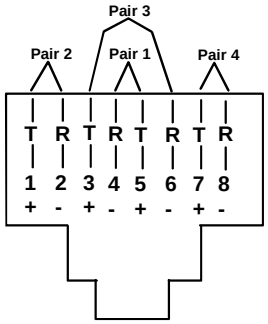


Figure 128- View looking into RJ45 female

TROUBLESHOOTING

If the Console Switch is not working properly, consider the suggestions below to see if a solution can be found.

Problem	Cause	Solution
No Front Panel LEDs are illuminated	No power to SERIMUX	Check all power connections
SERIMUX is not working properly	• Poor Connections • Port not configured correctly • Ports not initialized	• Verify that all cables are securely connected • Verify that the port configuration matches that of the device connected • Power-up the CPUs first, then the SERIMUX
Cannot Connect to port/device	• Port settings not correct • Wrong cable adapter used • Connections are loose	• Verify proper communication settings • Verify that adapter is one specified in Appendix C. • Verify that all cable connections are secure
SERIMUX will not accept username or password	Usernames and passwords are case sensitive	Verify characters used and enter again.
Cannot access Web Interface applet	SERIMUX is not compatible with some versions of Java 6 and not compatible with Java 8 at all	Install Java 6 or Java 7.
Cannot access shell from a port	Port is configured as host port	Configure port as user port (page 55).

If the passwords or other important parameters are not available, the SERIMUX Console Switch can be re-initialized to the default settings- contact NTI.

Caution: During initialization, the customer modified parameter values will be replaced with the factory default values; all ports will be placed in buffer mode; all passwords will be erased.

If the suggestions above have been tried and the NTI Console Switch is still not functioning properly, a solution to the problem may be found on our website at http://www.networktechinc.com in our FAQ (Frequently Asked Questions) section, or, please call us directly at **(800) 742-8324 (800-RGB-TECH)** in the US & Canada or **(330) 562-7070** (Worldwide) and we'll be happy to assist in any way we can.

Appendix A - SERIMUX Port Characteristics

Every port is defined through the following parameters:

Description	Acceptable Value	Default Value
Number	1-8/16/24/32	Same (not changeable)
Name	Up to 50 characters	“Port00” to “Port32”
Type	User or Host	Host
Baud rate– Console port	50-115200	115200
Baud rate – except Console port	50-115200	9600
Data bits per character – Console port	8	8
Data bits per character – except Console port	5,6,7,8	8
Stop bits	1, 2	1
Parity	No parity, even, odd	No parity
Flow control	Xon / Xoff (or in-band, or software), RTS/CTS (or out-band or hardware), Both, None	None
Inter-character delay	1-60 milliseconds, none	None
break duration (added to 1 character transmission time)	No break transmitted, 1-999 milliseconds	No break transmitted
Port escape sequence	ASCII characters	z
Connection timeout	0-99 minutes, (0=never)	15 minutes
DTR output upon disconnect	Low or high	High
Modem Reset string	Up to 41 characters	ATZ
Modem Initialization string	Up to 41 characters	AT&F&C1&D2S0=0
Modem Disconnect string	Up to 41 characters	ATH

Appendix B-SERIMUX User and Administrator Characteristics

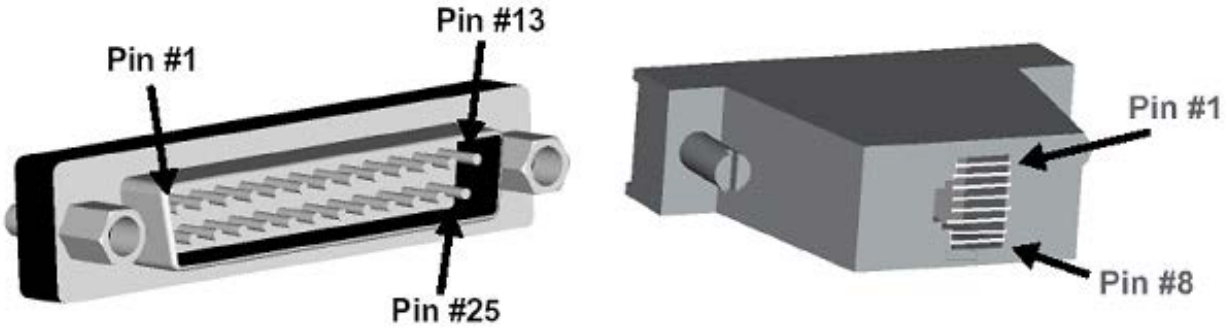
The users and the administrator are defined through the following parameters:

Description	Acceptable Value	Default Value
Users:		
User name	Up to 50 characters – case sensitive	None (must provide name)
User password	Up to 50 characters – case sensitive	“” (empty string)
Position at Login	Port Connect,Config menu, Shell	Port Connect
Group	Admin or User	User
Administrator:		
Administrator name	“root” – case sensitive	Same (not changeable)
Administrator password	Up to 50 characters – case sensitive	“nti”
Login timeout	0-999 minutes (0=never)	15 minutes

Appendix C- Cable Adapters

Four cable adapters are included with the SERIMUX with RJ45 connectors (to purchase more please contact NTI at **(800) 742-8324 (800-RGB-TECH)** or **(330) 562-7070**). The following illustrations show cable adapter pin outs.

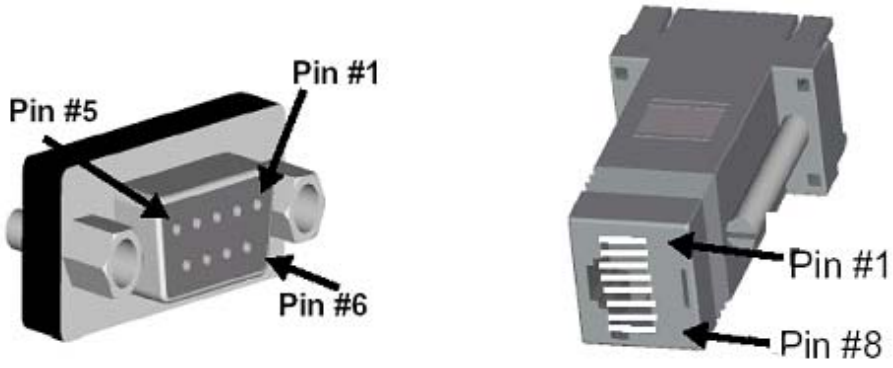
DB-25 Male Console Adapter (NTI P/N DB25M-RJ45F-T)



DB-25 Male to RJ45 Connector Pin Assignments

RJ45	Signal		DB-25M	Signal
1	CTS	Connected to	4	RTS
2	DSR	Connected to	20	DTR
5	DCD			
3	RxD	Connected to	2	TxD
4	GND	Connected to	7	GND
6	TxD	Connected to	3	RxD
7	DTR	Connected to	6	DCD
			8	DSR
8	RTS	Connected to	5	CTS

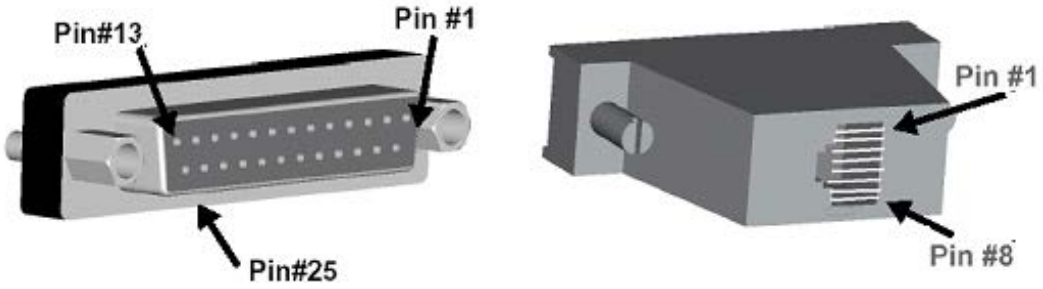
DB-9 Female Console Adapter (NTI P/N DB9F-RJ45F)



DB-9 Female to RJ45 Pin Assignments

RJ45	Signal		DB-9F	Signal
1	CTS	Connected to	7	RTS
2	DSR	Connected to	4	DTR
5	DCD			
3	RxD	Connected to	3	TxD
4	GND	Connected to	5	GND
6	TxD	Connected to	2	RxD
7	DTR	Connected to	1	DCD
			6	DSR
8	RTS	Connected to	8	CTS

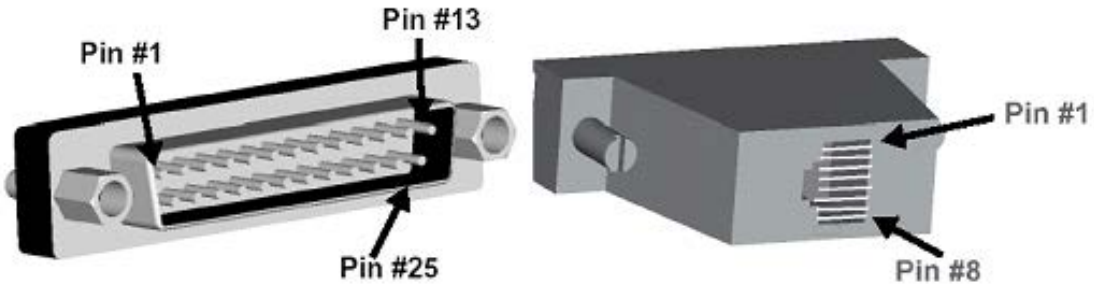
DB-25 Female Console Adapter (NTI P/N DB25F-RJ45F)



DB-25 Female to RJ45 Pin Assignments

RJ45	Signal		DB-25F	Signal
1	CTS	Connected to	4	RTS
2	DSR	Connected to	20	DTR
5	DCD			
3	RxD	Connected to	2	TxD
4	GND	Connected to	7	GND
6	TxD	Connected to	3	RxD
7	DTR	Connected to	6	DCD
			8	DSR
8	RTS	Connected to	5	CTS

DB-25 Male Modem Adapter (NTI P/N DB25M-RJ45F-C)



DB-25 Male Modem to RJ45 Pin Assignment

RJ45	Signal		DB-25M	Signal
1	CTS	Connected to	5	CTS
2	DSR	Connected to	6	DSR
3	RxD	Connected to	3	RxD
4	GND	Connected to	7	GND
5	DCD	Connected to	8	DCD
6	TxD	Connected to	2	TxD
7	DTR	Connected to	20	DTR
8	RTS	Connected to	4	RTS

Appendix D- Common Commands from Shell Command Line

To use the commands in this table, the user "root" must be logged in to the SERIMUX shell as described in page 10.

Command to Enter	Purpose
`serimuxconfig`	Open Configuration Menu
`portmenu`	Open Port Connect menu
`facdefault`	Restore Factory Default **Be Careful! This command restores all factory default settings, deleting any configuration settings that have been setup by the user.**
`serconfsave flash`	Configuration Save (Store the configuration to flash) This will store your current configuration to on-board flash memory. This would be good to use once all initial configuration of the SERIMUX is complete.
`serconfrestore`	Configuration Restore (Restore configuration from flash) This will restore your configuration from on-board flash memory, overwriting any configuration settings you presently have.

Note: If the command "serconfrestore" is used without first having previously saved a configuration using "serconfsave flash", then factory default settings will be restored instead (same result provided by using "facdefault" command)

Appendix E- SERIMUX-S-x Default Paths

Path	Purpose
`/var/log/messages`	System Log
`/var/run/databuf/ttyXRxx.data`	Port data buffering
`/mnt/nfs`	Mount for NFS
`/mnt/src`	Mount for USB
`/usr1/conf.tar.gz`	SERIMUX Complete Configuration file (password is encrypted)

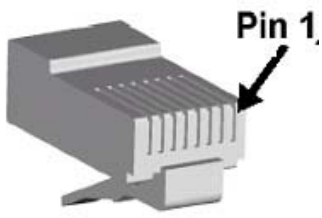
Appendix F- SERIMUX-S-x Default Network Settings

Setting	Purpose
192.168.1.91	IP address
255.255.255.0	Subnet Mask
192.168.1.1	Default Gateway

Ethernet Pinouts

The SERIMUX with RJ45 (8P8C) connectors uses a standard Ethernet connector that is a shielded and compliant with AT&T 258 specifications.

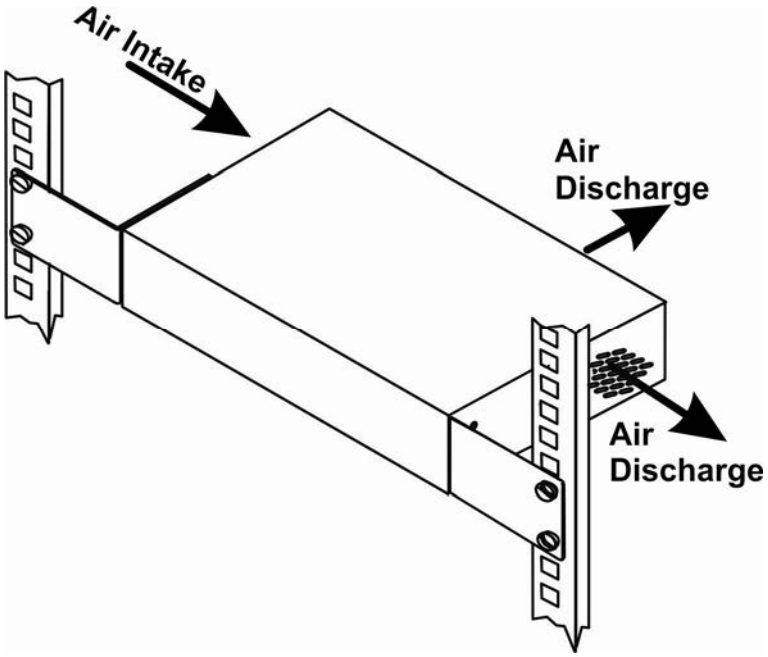
Pin	Description
1	Tx+
2	Tx-
3	Rx+
4	NC
5	NC
6	Rx-
7	NC
8	NC



SPECIFICATIONS

Description	Specification
Connectors	RJ45 Female DTE configuration via RS232
Operating temperature	32°F - 100°F (0°C - 38°C) (17-90% non-condensing RH)
Storage temperature	-20°F - 140°F (-30°C - 60°C). (17-90% non-condensing RH)
Airflow Direction	Cooling fan intake from the left, air output to the right and to the rear (see below)
Power requirements AC models	100-240VAC, 50 or 60Hz
Size (In.) WxDxH 8,16 port	16.2x9x1.75 without rack ears mounted 19x9x1.75 with rack ears mounted
Size (In.) WxDxH 24 and 32 port	17x10.1x1.75 without rack ears mounted 19x10.1x1.75 with rack ears mounted

To provide for proper cooling of the SERIMUX, please be sure not to block the air passage openings.



INDEX

WARRANTY INFORMATION

The warranty period on this product (parts and labor) is two (2) years from the date of purchase. Please contact Network Technologies Inc at **(800) 742-8324** (800-RGB-TECH) or **(330) 562-7070** or visit our website at http://www.networktechinc.com for information regarding repairs and/or returns. A return authorization number is required for all repairs/returns.

Man107 Rev 7/11/23