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

ENVIROMUX® Series

E-MINI-LXO

Mini Server Environment Monitoring System
Installation and Operation Manual

Front View of E-MINI-LXO

TRADEMARK

ENVIROMUX is a registered trademark of Network Technologies Inc in the U.S. and other countries.

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 2.6

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.

Note: Do not try to manually edit the downloaded configuration file and then restore it to the ENVIROMUX (page 39). The ENVIROMUX will quit working and you will have to return it to NTI to have default settings restored. Restoration of the default settings is not covered under the product warranty.

TABLE OF CONTENTS

TABLE OF FIGURES

INTRODUCTION

The E-MINI-LXO (ENVIROMUX) are Server Environment Monitoring Systems designed to monitor, from a remote location, the critical environmental conditions in cabinets and rooms containing servers, hubs, switches and other network components. Remote monitoring is provided via a 10/100BaseT Ethernet web interface, secure web interface, SSH, or Telnet. The input data is filtered, collected, analyzed and processed to allow the user to configure it to meet individual requirements. The user is able to specify parameters for all monitored signals. When a sensor exceeds the configured threshold, the unit will signal an alert. Alert methods include email, SMS, SNMP traps (MIBs), web-page alerts, and a visual indicator (red LED).

The E-MINI-LXO will monitor temperature, humidity, and detect the presence of water on a flat surface (such as the floor). The unit also has four sets of terminal block pairs for the connection of contact-closure sensors.

Features and Applications

- Monitor and manage server room environmental conditions over IP.
- Monitors and operates at temperatures from 32°F to 122°F (0ºC and 50ºC) and 20% to 90% relative humidity.
  - Optional Industrial version (E-MINI-LXO-**IND**) operates at 32 to 167°F (0 to 75°C).
- Sensors supported:
  - 2 temperature/humidity sensors
  - 5 digital input devices
- Operates and configures via HTTP web page.
- 4 remote users can access the system simultaneously.
- Supports SMS alert messages via GSM modem
- Supports SMTP protocol
- Supports SNMP V1, V2C and V3 protocols
- Supports Microsoft Internet Explorer 6.0 and higher, Firefox 2.0 and higher, Chrome, Safari 4.0 or higher, and Opera 9.0
- Sensor alerts and log messages are sent using email, Syslog, and SNMP traps when any monitored environmental condition exceeds a user-specified range.
- Sensor alerts, end of alerts, and log-ins are posted in message log, which is accessible through web interface.
- SNMP trap messages can be imported into Microsoft Excel
- Use in data centers, co-lo sites, web hosting facilities, telecom switching sites, POP sites, server closets, or any unmanned area that needs to be monitored.
- Security: HTTPS, SSHv2, SSLv3, IP Filtering, LDAPv3, AES 256-bit encryption, 3DES, Blowfish, RSA, EDH-RSA, Arcfour, SNMPv3, IPV6, SNTP support, 16-character username/password authentication, user account restricted access rights.
- Monitor (ping) up to 16 IP network devices.
  - Configure the timeout and number of retries to classify a device as unresponsive.
  - Alerts are sent if devices are not responding.
- Monitored sensors and devices can be individually named (up to 63 characters).
- Monitor environmental conditions.
  - Supports two sensors, including: temperature, humidity, up to 5 dry contacts or water detection sensors.
  - When a sensor goes out of range of a configurable threshold, the system will notify you via email, syslog, LEDs, web page, and network management (SNMP).
- Operates on a Linux system.
- Firmware upgradeable "in-field" through Ethernet port..
- Output relay for control of external device (contacts rated for up to 1A, 30VDC or 0.5A, 125VAC)
- Monitor up to 8 IP cameras

Options:

- The ENVIROMUX can be ordered with a DIN rail mounting bracket- Add “D” to the part number (i.e. E-MINI-LXO-**D**)
- The ENVIROMUX can be ordered with battery backup support and DC power monitoring installed, providing up to 2.3 hours of operation in the event of a power failure- to order, add “B” to the part number (i.e. E-MINI-LXO**B**)
- The ENVIROMUX can be ordered with a higher operating temperature range (32 to 167°F (0 to 75°C))- to order add “-IND” to the part number (i.e. . E-MINI-LXO-**IND**)

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 2.0 or higher
- Opera 9.0
- Google Chrome
- Safari 4.0 or higher for MAC and PC

MATERIALS

Materials supplied with this kit:

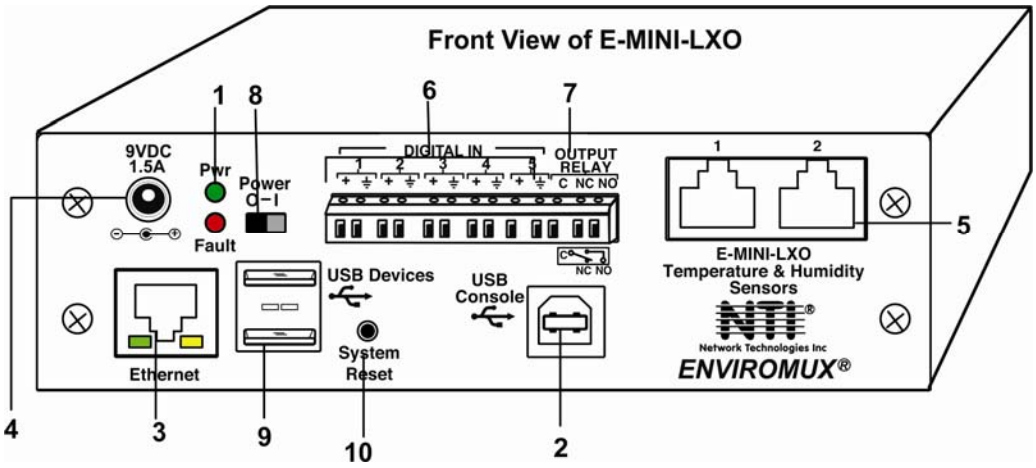
- NTI E-MINI-LXO Mini Server Environment Monitoring System
- 1- 120VAC or 240VAC at 50 or 60Hz-9VDC/1.5A AC Adapter (PS4074)
- 1- Line cord- country specific
- 1- USB2-AB-2M-5T 2 meter USB 2.0 male type A-male type-B transparent cable (CB4306)

Additional materials may need to be ordered;

CAT5/5e/6 (CATx) unshielded twisted-pair cable(s) terminated with RJ45 connectors wired straight thru- pin 1 to pin 1, etc. for Ethernet connection

Contact your nearest NTI distributor or NTI directly for all of your cable needs at 800-RGB-TECH (800-742-8324) in US & Canada or 330-562-7070 (Worldwide) or at our website at http://www.networktechinc.com and we will be happy to be of assistance.

CONNECTORS AND LEDS



#	LABEL	CONNECTOR/LED	DESCRIPTION
1	**Pwr**	Green LED	green — indicates device is powered
	Fault	Red LED	red — illuminates if a sensor goes out of range of a configurable threshold
2	**USB Console**	USB Type B female connector	For connection of terminal for control through Text Menu
3	**Ethernet**	RJ45 female connector	for connection to an Ethernet for remote multi-user control and monitoring • Yellow LED- indicates 100Base-T activity when illuminated, 10Base-T activity when dark • Green LED – illuminated when Ethernet link is present, strobing indicates activity on the Ethernet port
4	**9V 1.5A**	2.1x5.5mm Power Jack	for connection of power supply
5	**Temperature & Humidity Sensors**	RJ45 female connectors	for connection of optional E-T, E-RH, or E-TRH sensors (The left port is "#1", the right port is "#2" as listed in the Summary Page on Page 24.)
6	**DIGITAL IN**	Wire terminal block	For connecting dry-contact and liquid detection sensors
7	**OUTPUT RELAY**	Wire terminal block	For control of external devices (contacts rated up to 1A, 30VDC or 0.5A, 125VAC)
8	**Power**	Slide switch	For powering the ENVIROMUX On (I) and Off (O)
9	**USB Devices**	USB Type A female connectors	For connecting USB Flashdrive and USB Modem
10	**System Reset**	Push button	For manually rebooting the ENVIROMUX without power-cycling- a momentary press will activate

INSTALLATION

Mount the Unit

The E-MINI-LXO can either be placed on a solid surface, mounted to a wall, or mounted to an accessible surface within rack (Zero-RU). To mount to a wall or other surface, first remove the screws holding the mounting tabs to the rear of the box. Rotate the tabs such that they extend from the back of the box, and attach the tabs with the screws removed. Now the E-MINI-LXO can be secured to any convenient surface. Use appropriate hardware (not supplied) when mounting.

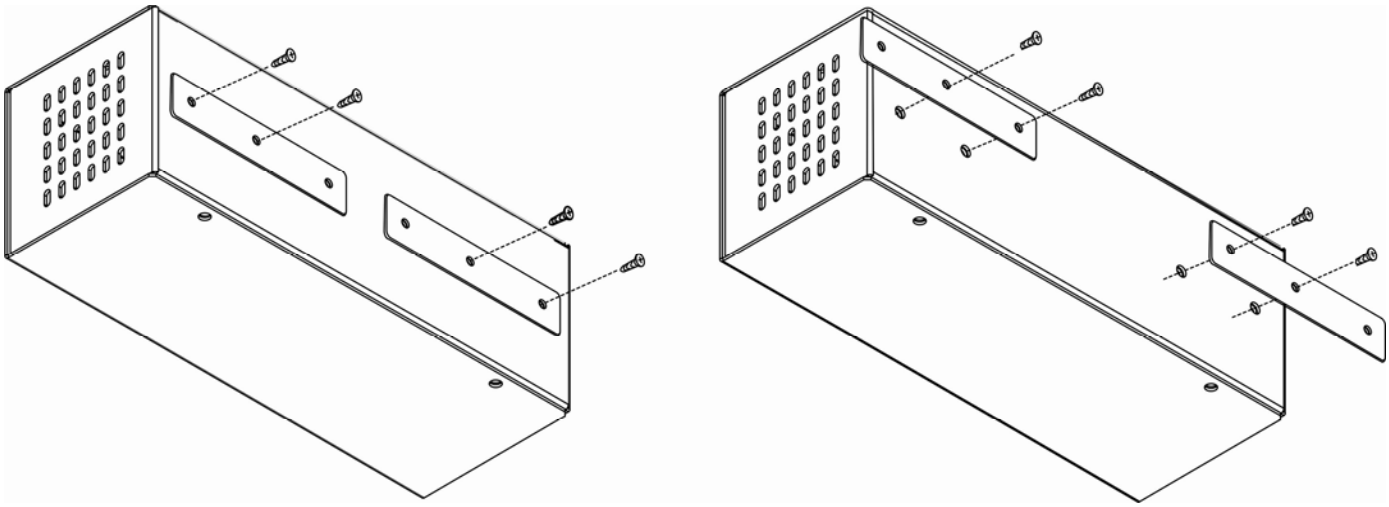


Figure 1- Rotate the tabs for Zero-RU mounting

DIN Rail Mounting

The E-MINI-LXO-D is for mounting to a DIN rails in a server rack. It is supplied with a DIN rail clip on the back. With the clip installed, it can be readily snapped to a DIN rail and easily removed. Press the top of the clip against the channel, rotate the E-MINI-LXO-D into position, and release the pressure. Reverse the procedure to remove it.

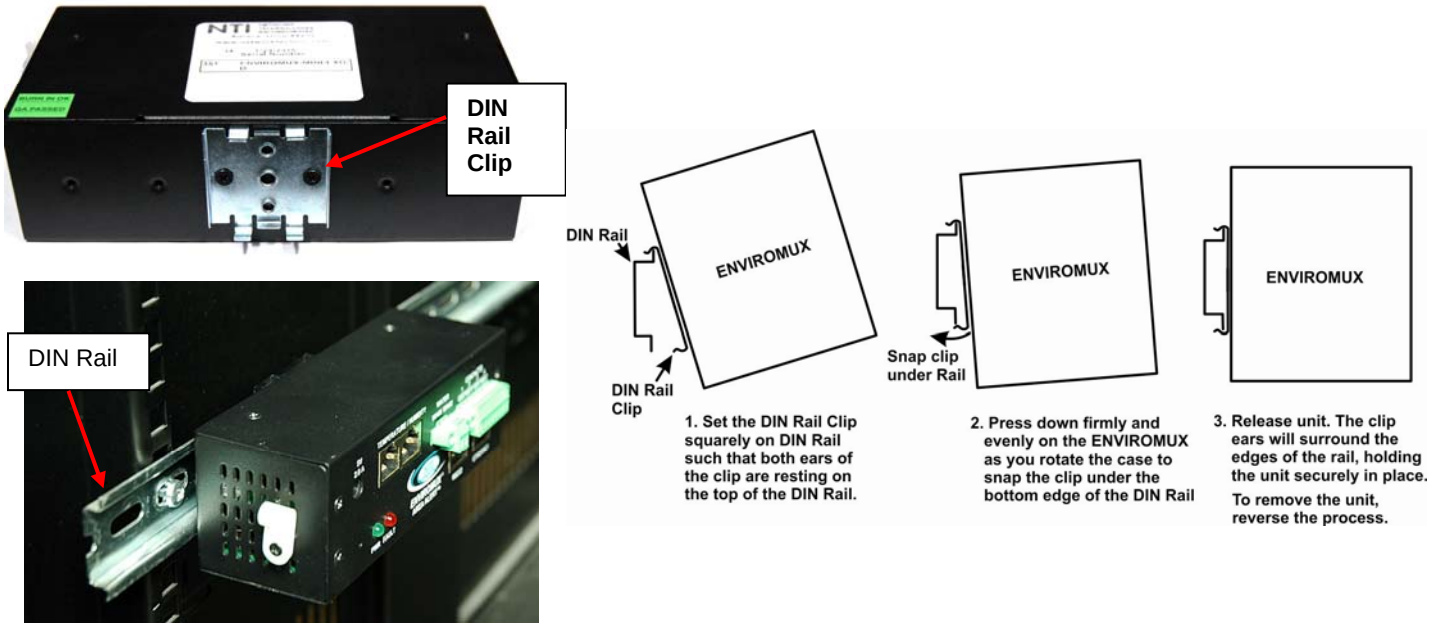


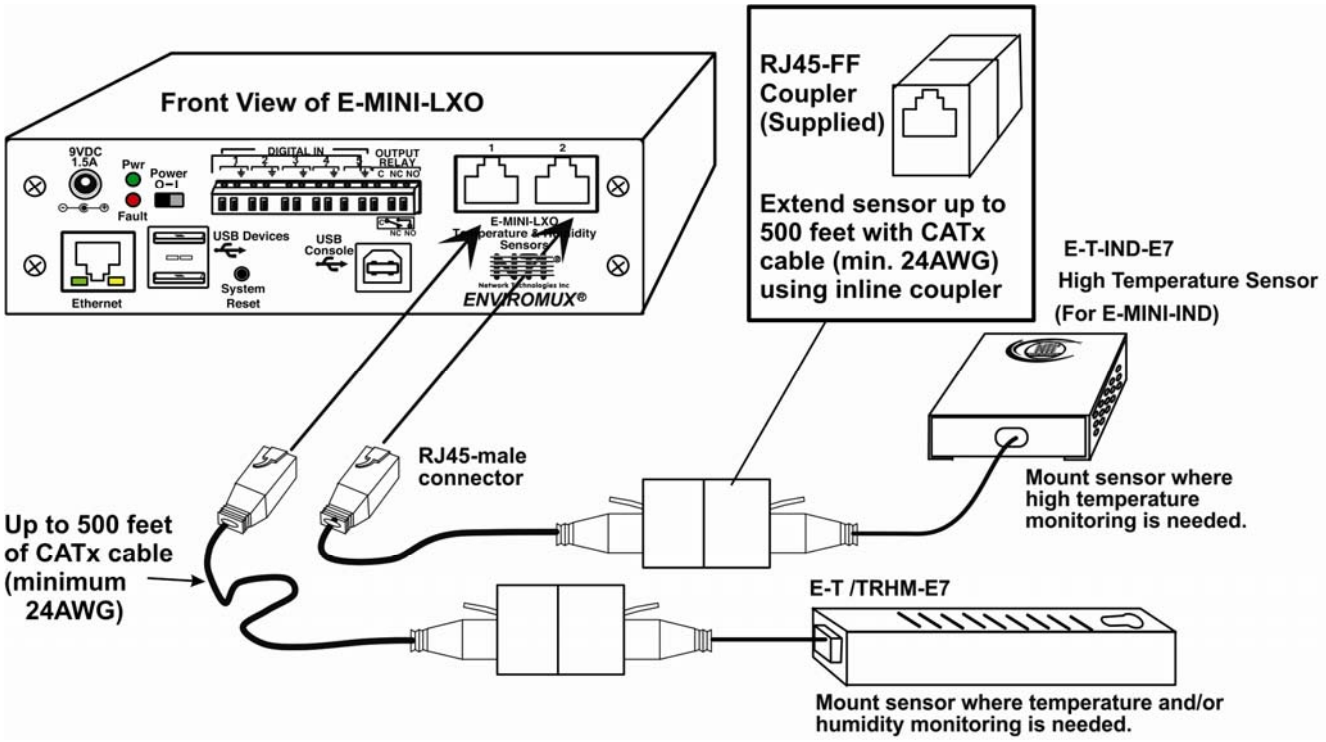
Figure 2- DIN Rail clip and unit mounted to a rail

Connect Sensors

Connect the desired sensors (sold separately) to the available ports on the ENVIROMUX. Plug the RJ45 connectors to either of the two RJ45 ports marked "TEMPERATURE/HUMIDITY". Mount the sensors according to their individual operating characteristics. Power-cycle the ENVIROMUX after sensors have been plugged-in.

Note: The maximum CAT5 cable length for attachment of temperature and humidity sensors in the E-MINI-LXO is 507 feet using minimum 24AWG cable (requires firmware version 2.0 or later).

Note: Mounting the temperature sensor in the path of a fan or on a heated surface may affect the accuracy of the sensor's readings.



Up to five dry-contact sensors can also be connected. Sensors with 16-26 AWG connection wires that operate on 5V at 10mA maximum current may be used. A contact resistance of 10kΩ or less will be interpreted by the ENVIROMUX as a closed contact. The maximum cable length for attachment of contact sensors is 1000 feet.

To install the dry-contact sensor(s) to "DIGITAL IN" terminals:

A. Attach the positive lead to a terminal corresponding to a "+" marking on the ENVIROMUX and the ground lead to the next terminal to the right that will correspond to a ⏚ marking on the ENVIROMUX. Tighten the set screw above each contact. Terminal sets are numbered 1-5.

B. Mount the sensors as desired.

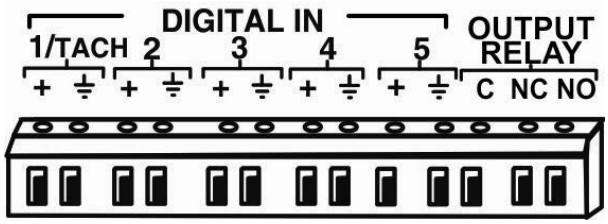


Figure 4- Terminal block for dry-contact sensors

Note: The terminal block is removable for easy sensor wire attachment if needed.

Optionally, connect the two-wire cable from a liquid detection sensor (E-LD shown below- sold separately) to a set of “DIGITAL IN” contacts.

The twisted orange sensing cable should be placed flat on the surface (usually the floor) where liquid detection is desired. If tape is required to hold the sensor in place, be sure to only apply tape to the ends, exposing as much of the sensor as possible. At least 5/8" of the sensor must be exposed for it to function. (See Figure 5)

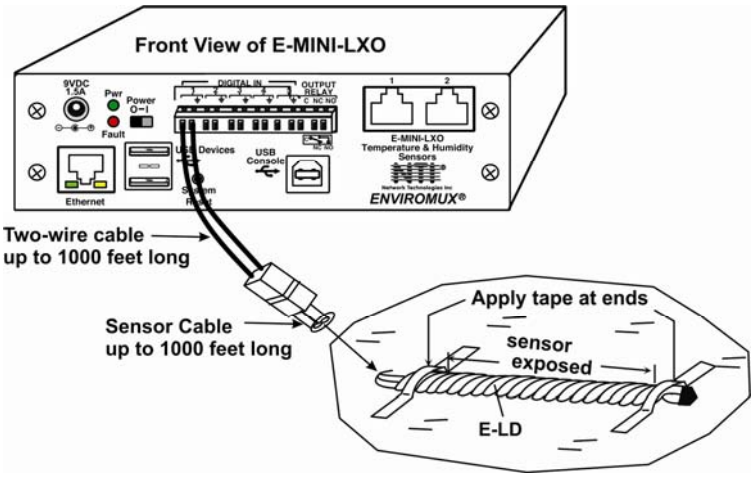


Figure 5- Secure liquid detection sensor with tape

To test the E-LD;

1. Configure the sensor (page 31). (Normal Status set to “Open”, Refresh Rate set to 5 seconds.)
2. Submerge at least inch of the exposed twisted orange wire (not the wrapped end) for up to 30 seconds. Do NOT use distilled water as water must be conductive.
3. Monitor the sensor (page 25) to see the sensor “Value” change from “Open” (dry) to “Closed” (wet).
4. Dry the exposed area of sensor and the sensor “Value” should change back to “Open” within 30 seconds.

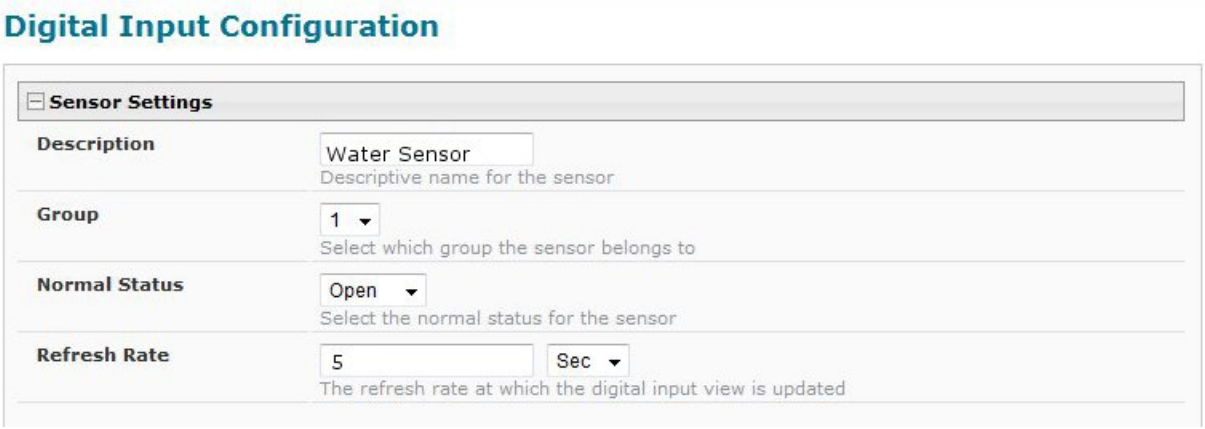


Figure 6- Portion of Water Sensor configuration page

Output Relay

An output relay is provided to control an external device with a rating of up to 1A, 30VDC or 0.5A, 125VAC. Three terminals are provided to enable a normally-open connection (using the N.O. and C terminals) or a normally-closed connection (using the N.C. and C terminals). Using the web interface, this relay can be set to change state (close the normally-open connection, or open the normally-closed connection) either manually (page 34) or as a result of an alert state from one or more of the connected sensors (page 27). The terminals for these connections will accept 16-26AWG wire.

Note: A recent design improvement resulted in a change to the pinout of the output relay in the E-MINI-LXO. Please be aware of the change and note which version yours is. The previous version is shown below.

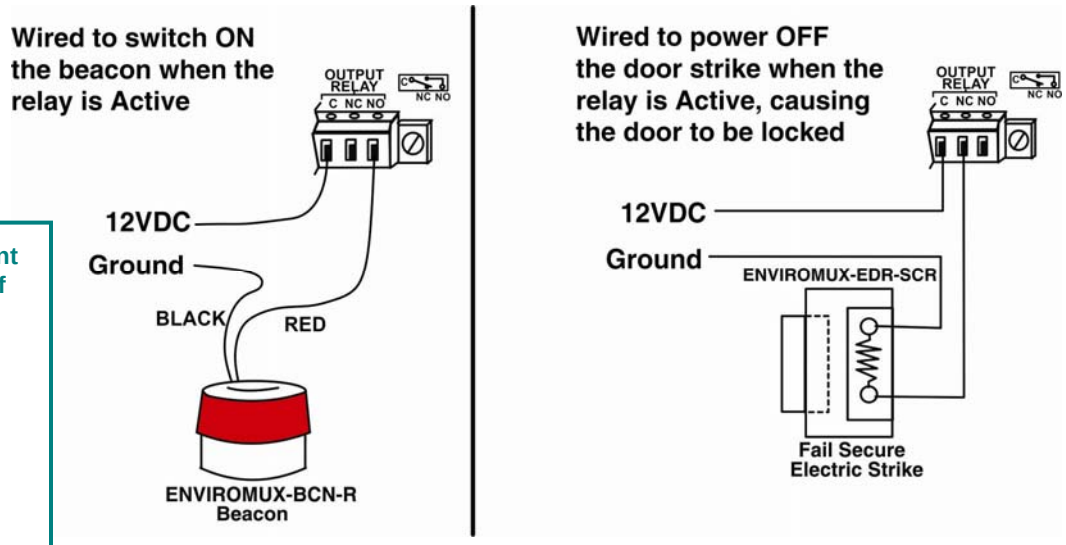


Figure 7- Output Relay Application Examples

Ethernet Connection

Connect a CAT5 patch cable (RJ45 connectors on each end wired pin 1 to pin 1, pin 2 to pin 2 etc) from the local Ethernet network connection to the connector on the ENVIROMUX marked "Ethernet".

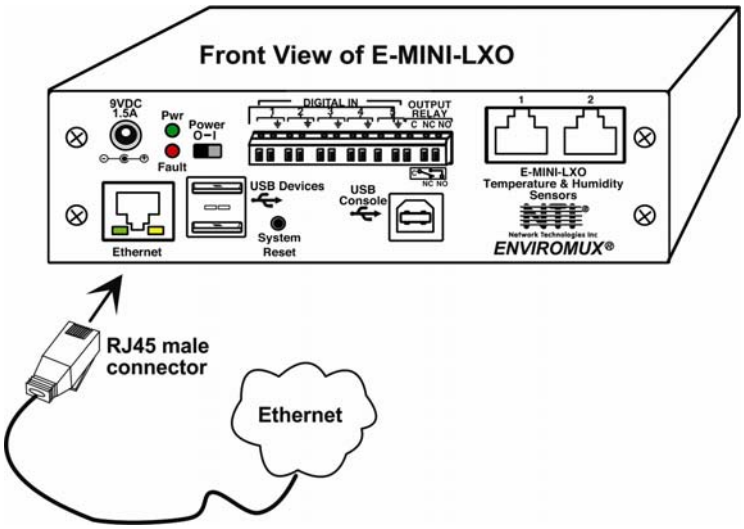


Figure 8- Connect E-MINI-LXO to the Ethernet

Note: A direct Ethernet connection can be made with a PC using a crossover cable. For the pinout of this cable, see page 110.

USB Console Port

Your ENVIROMUX includes a USB Type B connector labeled “USB Console”. If you connect a USB cable between the ENVIROMUX and your PC you will be able to control your ENVIROMUX serially from a terminal console using this connection.

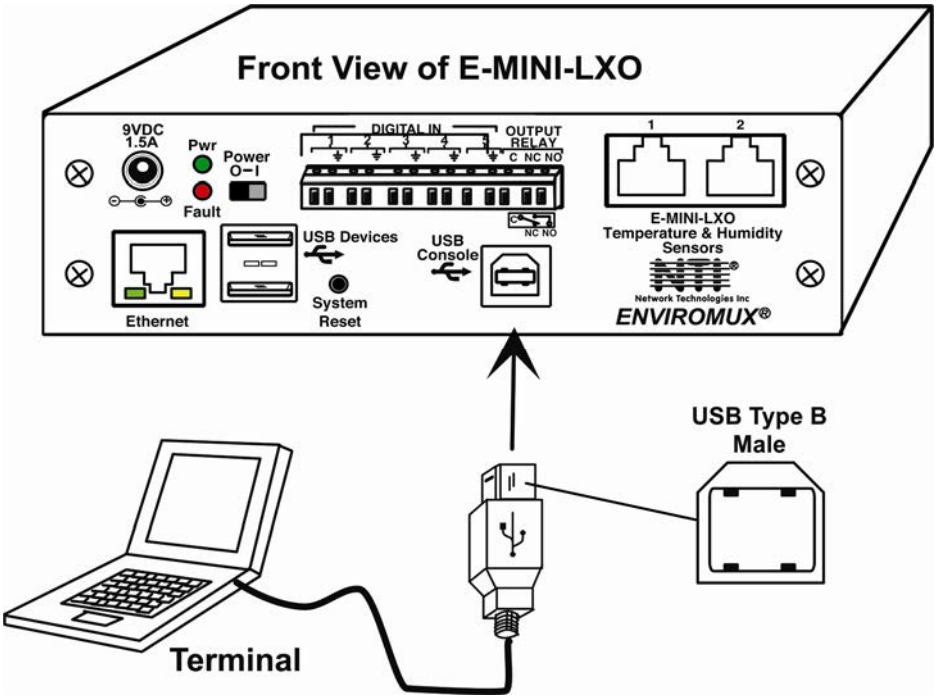


Figure 9- Connect terminal to USB Console port

Installing Drivers

You will only need to install drivers the first time the ENVIROMUX is connected to your PC with Windows XP, 2000, Vista, Windows 7 and Windows 8 (32 and 64 bit versions). (Drivers will automatically install when connected to a Windows 10 PC.) After the first time, when the ENVIROMUX is connected, your PC should recognize the ENVIROMUX and re-assign the COM port. Follow the steps below to install the drivers.

Note: When trying to load the USB driver to a Windows 8 PC, you will likely be stopped by an “unsigned driver” warning, even though the driver you are trying to load is actually a Microsoft driver from an earlier operating system. Follow the instruction on page 17 to disable this warning and be able to proceed with driver installation.

1. Make sure the USB cable is connected between the ENVIROMUX and your PC.

2. Power ON the ENVIROMUX. The PC will see the ENVIROMUX as “New Hardware” and create a virtual COM port to communicate with it.

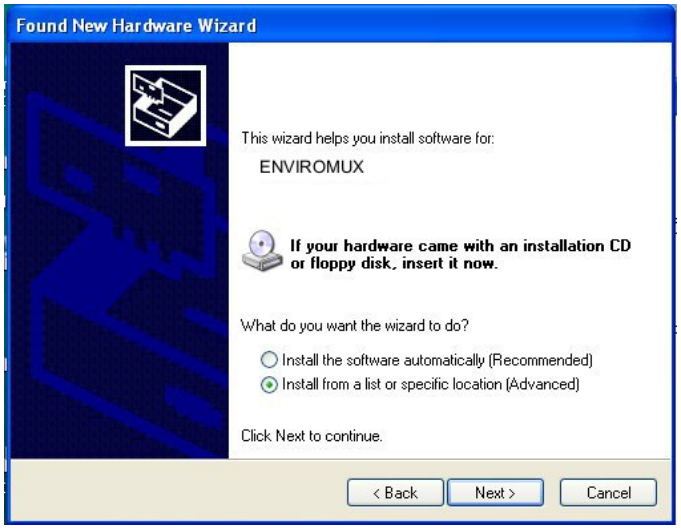
3. You will be prompted to load drivers. A driver file compatible with Windows XP, 2000, Vista, Windows 7 and Windows 8 (32 and 64 bit versions) can be found at http://www.networktechinc.com/environment-monitoring.html. Go to the firmware downloads page, download the USB-drivers.zip, and unzip it to your PC. Locate and select the file named “**`enviromux.inf`**” in a directory named **`“windows-drivers\32bit or \64bit”`** depending upon your operating system.

The .inf file will direct your PC to locate and install the file **`usbser.sys`** (already on your PC, comes with Windows). Installing the usbser.sys file should happen automatically. When finished, Windows will indicate installation is successful.

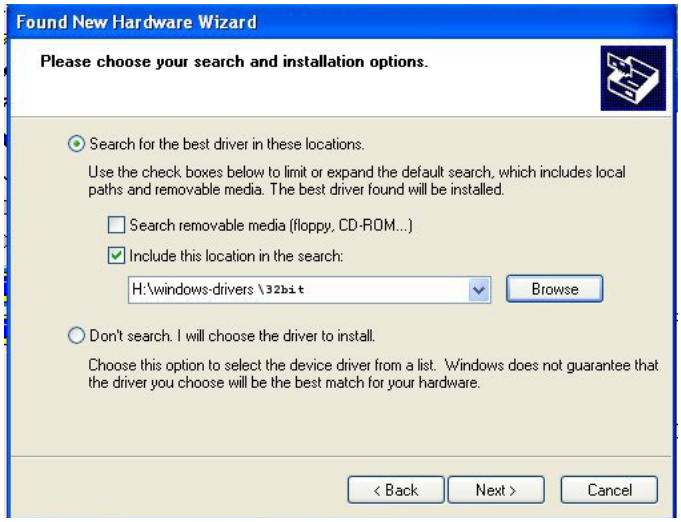
Windows XP-32 bit Installation

Your typical installation will include windows like the ones that follow. The images below are from a Windows XP SP2 32 bit installation.

A. Windows will want to check the internet for drivers. Choose "**No, not this time**" because the drivers are unique to the ENVIROMUX.



B. You can try to "**Install the software automatically**" but if windows doesn't check the CD, you will need to use "**Install from a list or specific location**" instead.



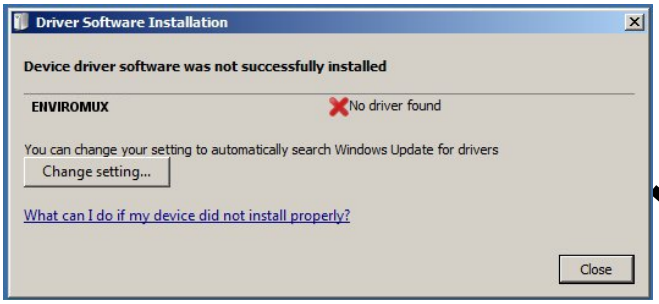
C. Let the New Hardware Wizard search for the driver, but direct it to the drive the Product Manual CD is in and the directory of either the 32 bit driver or the 64 bit driver.

Click “Next” and the Wizard will automatically install the proper driver.

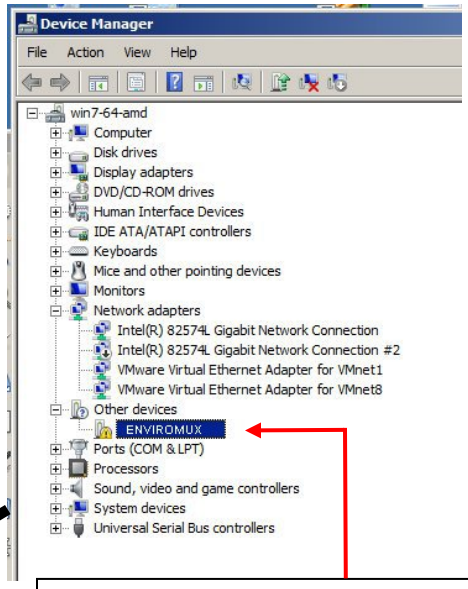
D. Once the driver is installed, you will get this screen and the ENVIROMUX USB Console Port will be ready to use.

Windows 7-64 bit Installation

A Windows 7 64 bit installation has a few extra steps. The images below are from a Windows 7, 64-bit installation.

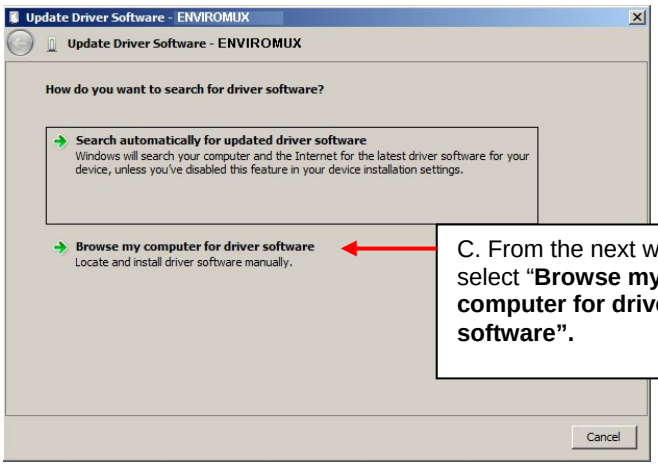


A. Upon ENVIROMUX power ON, the driver cannot be found. Press "**Close**".

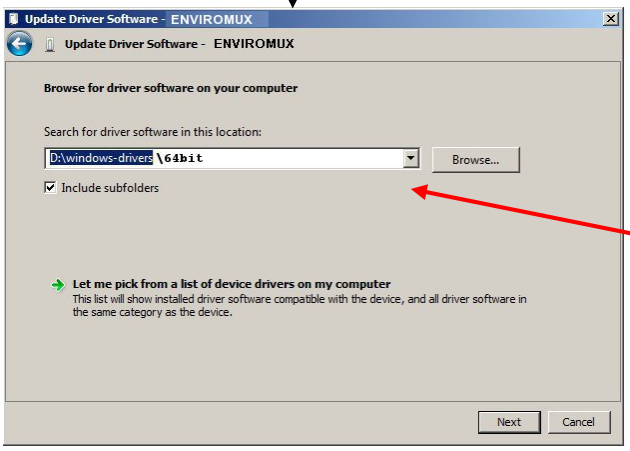


B. Open the Device Manager and select the ENVIROMUX in the device list. Right-click and open "Properties". Select "Update Driver Software".

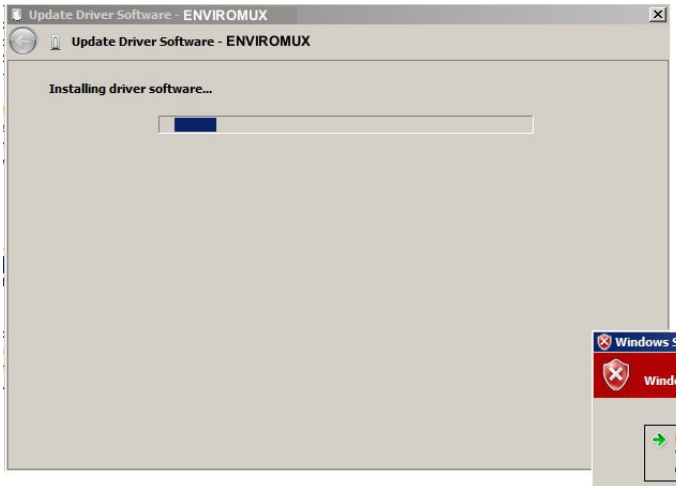
Tip: The Device Manager can be opened by right-clicking on "My Computer" on the desktop, selecting "Properties", and selecting "Device Manager".

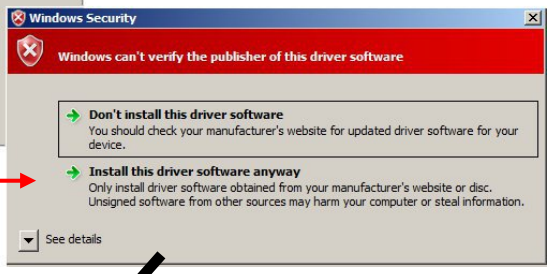


C. From the next window, select "**Browse my computer for driver software".**

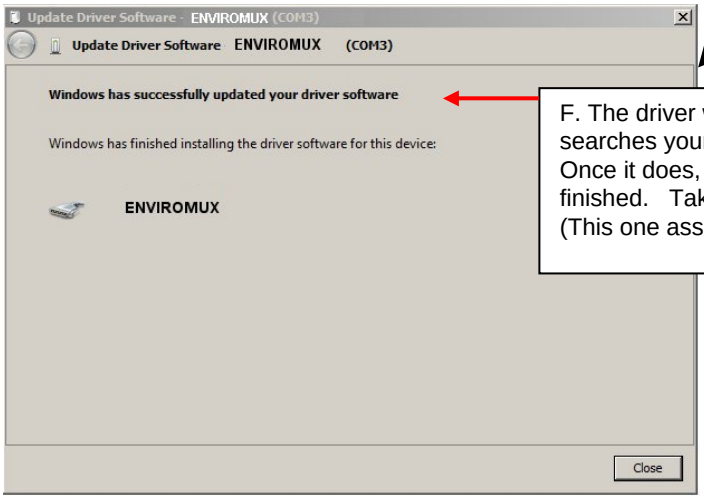


D. In the next window, enter the path to the .inf driver file (on the Product Manual CD). Press "Next".





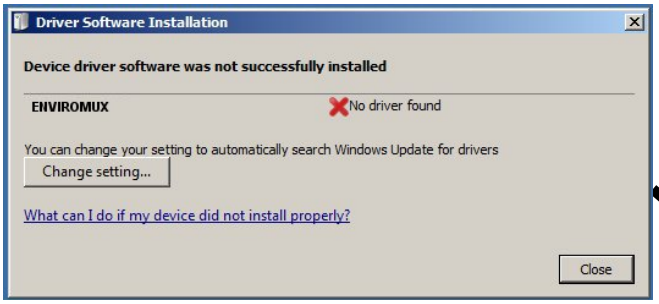
E. You will probably get this warning that Windows can't verify the publisher of the driver software. Select **"Install this driver software anyway. "**



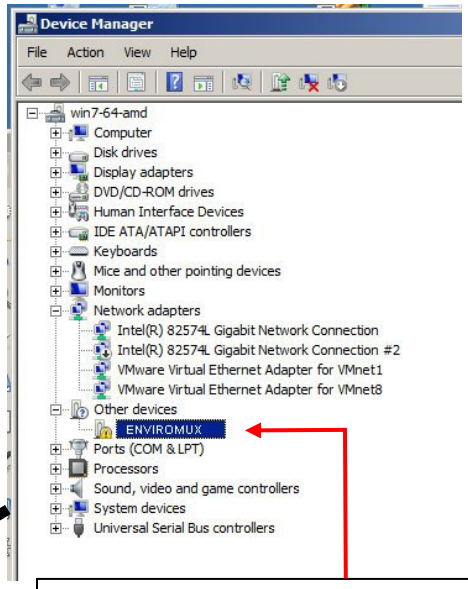
F. The driver will load. This might take a minute while it searches your computer for the `usbser.sys` file it needs. Once it does, you will get a window telling you Windows is finished. Take note of the COM port number it assigned. (This one assigned COM3.)

Windows 8-64 bit Installation

A Windows 8 64 bit installation has a few extra steps. The images below are from a Windows 8, 64-bit installation.

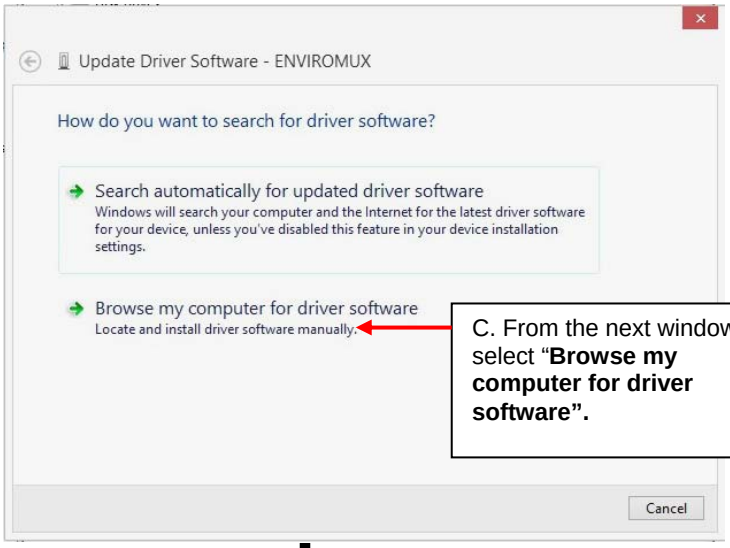


A. Upon ENVIROMUX power ON, the driver cannot be found. Press "**Close**".

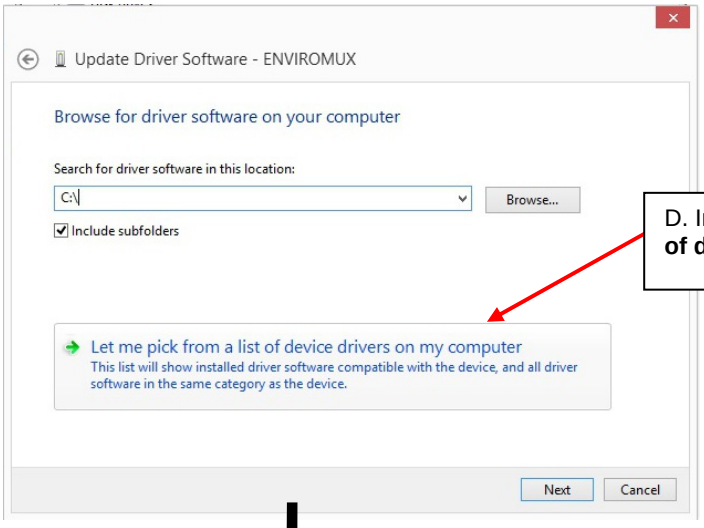


B. Open the Device Manager and select the ENVIROMUX in the device list. Right-click and open "Properties". Select "Update Driver Software".

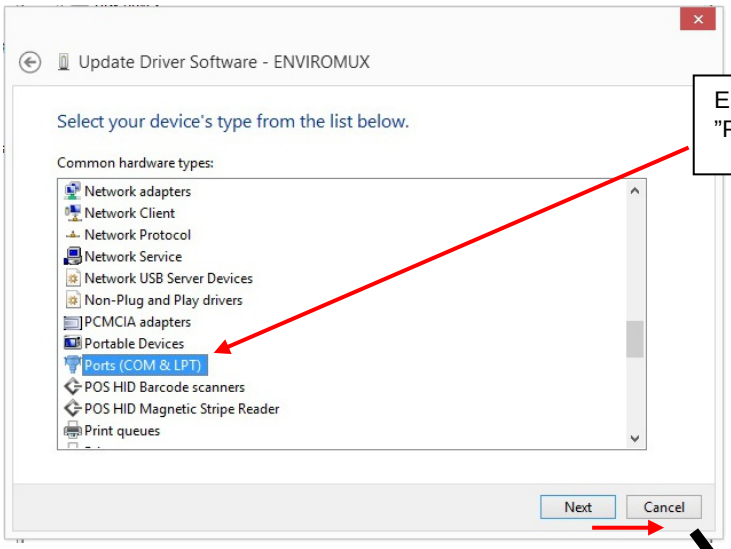
Tip: The Device Manager can be opened by right-clicking on "My Computer" on the desktop, selecting "Properties", and selecting "Device Manager".



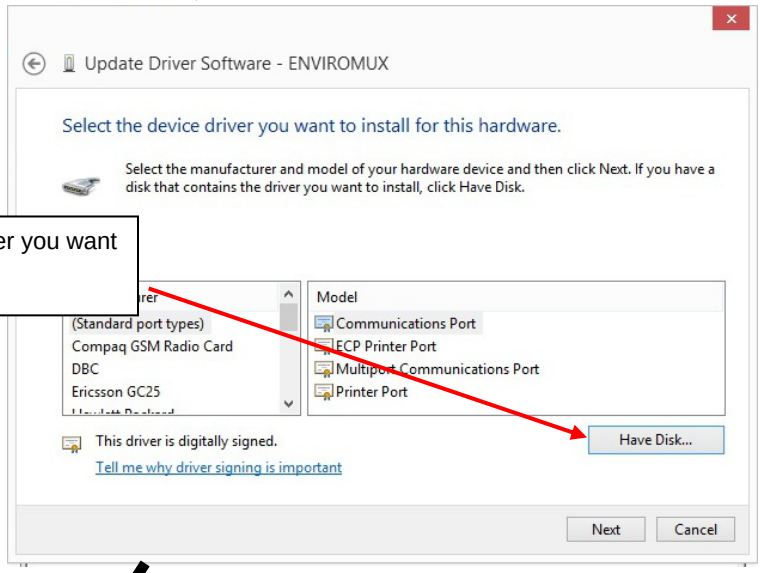
C. From the next window, select "**Browse my computer for driver software".**



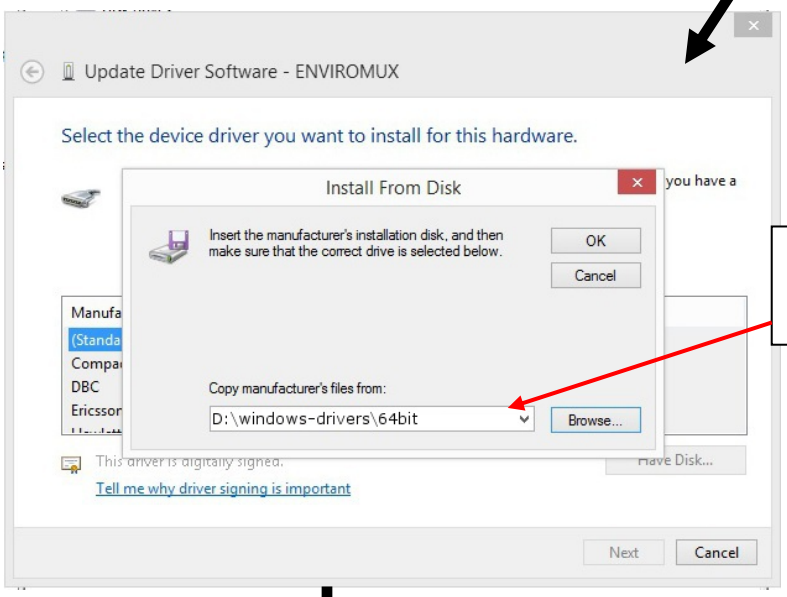
D. In the next window, select "**Let me pick from a list of device drivers on my computer"**. Press "Next".



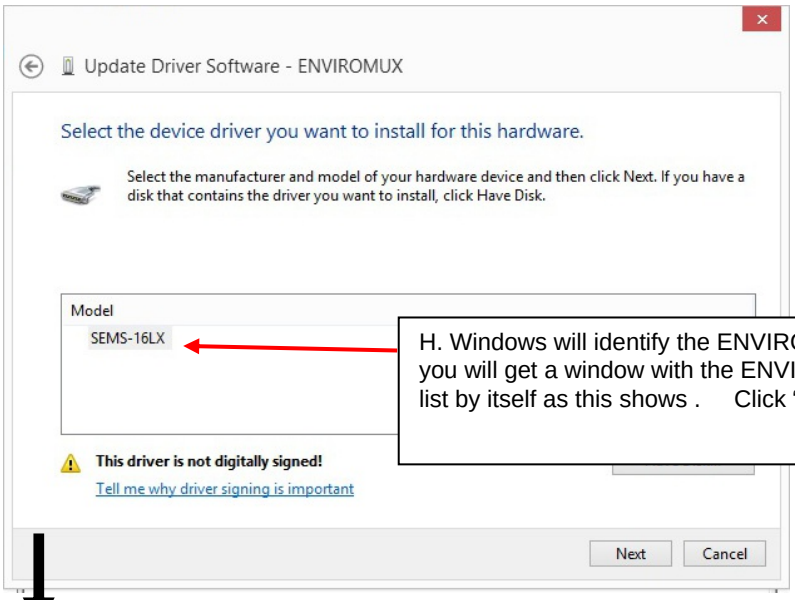
E. From the list of hardware types that comes up, select "Ports (COM&LPT)" and click "Next"



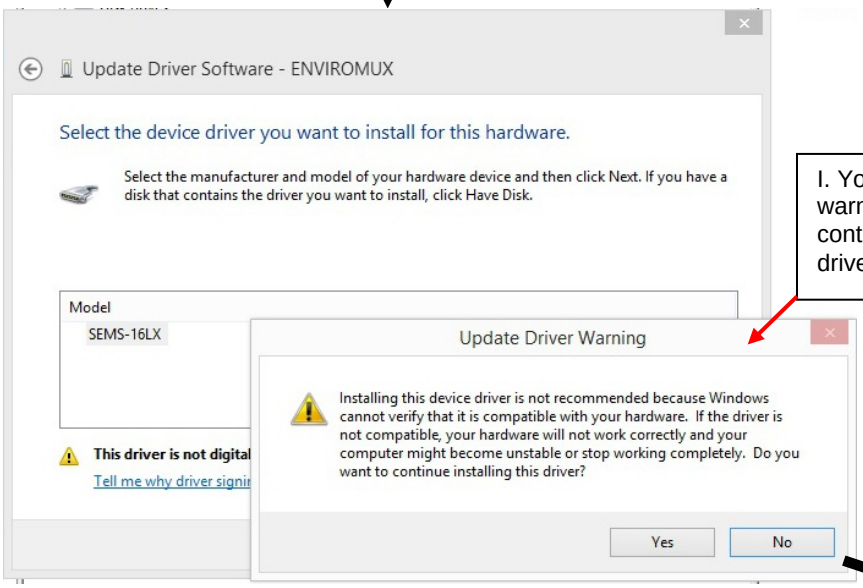
F. From the next window, asking what model driver you want to install, just click on "**Have Disk**"



G. In the next window, click "Browse" to the location of the .inf file on the CD in the CD ROM drive." and click "OK".

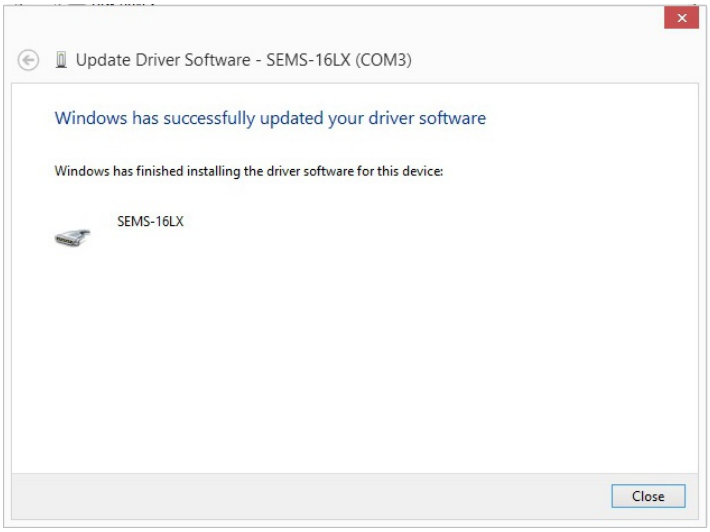


H. Windows will identify the ENVIROMUX. Once it does, you will get a window with the ENVIROMUX, probably in a list by itself as this shows . Click "Next".



I. You will probably get an "**Update Driver Warning**" warning you not to install the driver, asking if you want to continue. Click "Yes". (Remember, this is a Microsoft driver, not foreign)

J. You may even get a second warning. Double-click **"Install this driver software anyway"**



K. The driver will load. This might take a minute while it searches your computer for the `usbser.sys` file it needs. Once it does, you will get a window telling you Windows is finished. Take note of the COM port number it assigned. (This one assigned COM3.)

4. During the installation, your PC will assign a COM port number to the USB port attached to the ENVIROMUX. You will need to identify the COM port number assigned. This information can be viewed in your Device Manager list (below) if you didn't take note of it during installation.

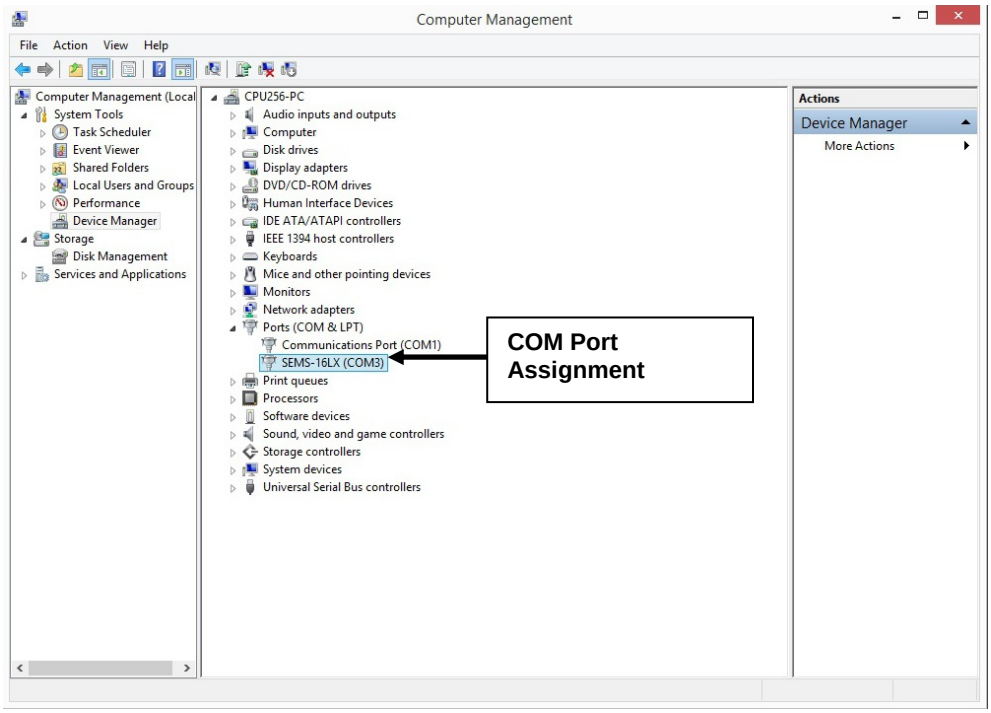


Figure 10- COM port assigned to ENVIROMUX

Using the USB Console Port

The virtual COM port will be used to enable serial control over the ENVIROMUX (see Operation Via Text Menu on page 66). When you open a terminal program be sure to use the correct COM port (see Figure 10 and Figure 11).

Figure 11- Configure COM port in HyperTerminal

Installing an Unsigned Driver in Windows 8 (x64)

When trying to load the USB driver into a Windows 8 PC in order to use the USB Console port on an NTI product, you may encounter a window that prevents it because it is an “unsigned driver”, in spite of the fact it is actually a Microsoft driver from an earlier operating system.

The steps to enable the installation of the USB driver on Windows 8 are as follows:

1. Hold the Shift key and press Power –> Restart from the Power menu.

Now the system will restart and might take some minutes to show up the boot menu. Wait for It patiently.
After some time you will be prompted with a menu with the following options.

```
1. Continue
2. Troubleshoot
3. Turn off
```

2. Choose “Troubleshoot”

Then the following menu appears:

```
Refresh your PC
Reset your PC
Advanced Options
```

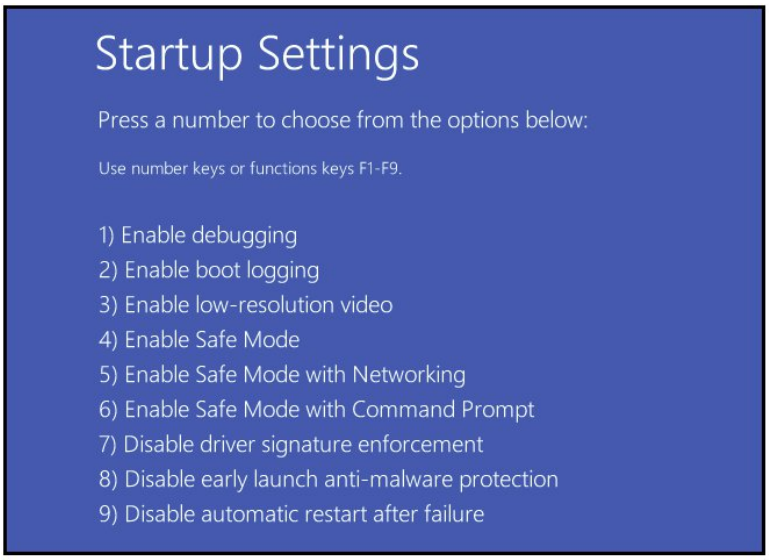
3. Choose “Advanced Options”

Then the following menu appears:

```
System Restore
System Image Recovery
Startup Repair
Command Prompt
Startup settings
```

4. Choose “Startup Settings”, then Click Restart.

Now the computer will restart and the boot menu appears with a “Startup Settings” list.



5. Choose “Disable Driver Signature Enforcement” from the boot menu (press F7).

Now Windows will start and you can follow the instructions on page 8 for the installation of the USB driver.

Connect the Power

Note: Sensors should be connected before supplying power to the ENVIROMUX.

1. Connect the AC adapter to the connection marked "PWR" on the ENVIROMUX and plug it into an outlet.

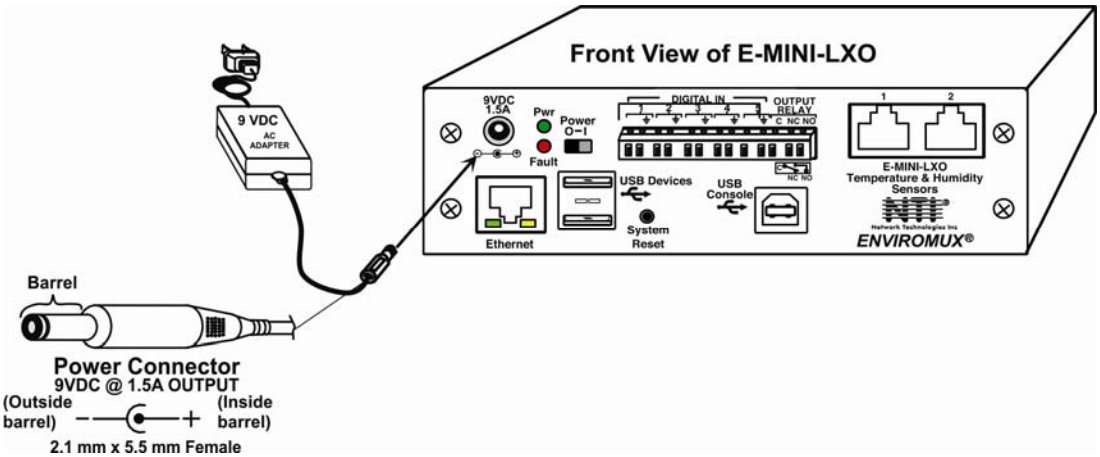


Figure 12- Connect the AC adapter and power-up

2. Use the NTI Discovery Tool (page 22) to configure network settings.

Front Panel LEDs Indicate Status

With proper connections made, the ENVIROMUX is now ready to power ON. With the power cord attached and plugged into an AC outlet, the “Power” green LED should be illuminated on the front of the ENVIROMUX. The red “Fault” LED will illuminate when power is first applied and while the ENVIROMUX boots up (for up to 60 seconds). Once the red LED goes OFF, the ENVIROMUX is ready for use. After a completed boot-up, the red LED will only illuminate when one of the connected sensors is in alert.

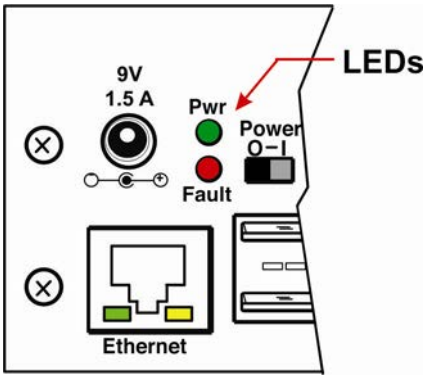


Figure 13- LEDs on front of ENVIROMUX

Connect a Modem

A USB GSM modem may be connected (E-3GU-4) to use to send SMS alert messages to a contact's cell phone. The E-3GU-4 modem will connect to the ENVIROMUX at the "USB Devices" port (either USB Type A connector, it doesn't matter which one) . The remaining USB Type A connector on the ENVIROMUX is available for the connection of a USB Flash Drive for data logging (page 64).

The phone number to be called for each user is configured under "User Configuration-Contact Settings" (page 46).

Note: A Mini SIM card (not included) must be installed in the modem for the modem to send messages. Make sure the SIM card is for GSM communication (not CDMA) and that it is not locked (some SIM cards are "locked" to search for a specific IMEI number of the phone to operate).

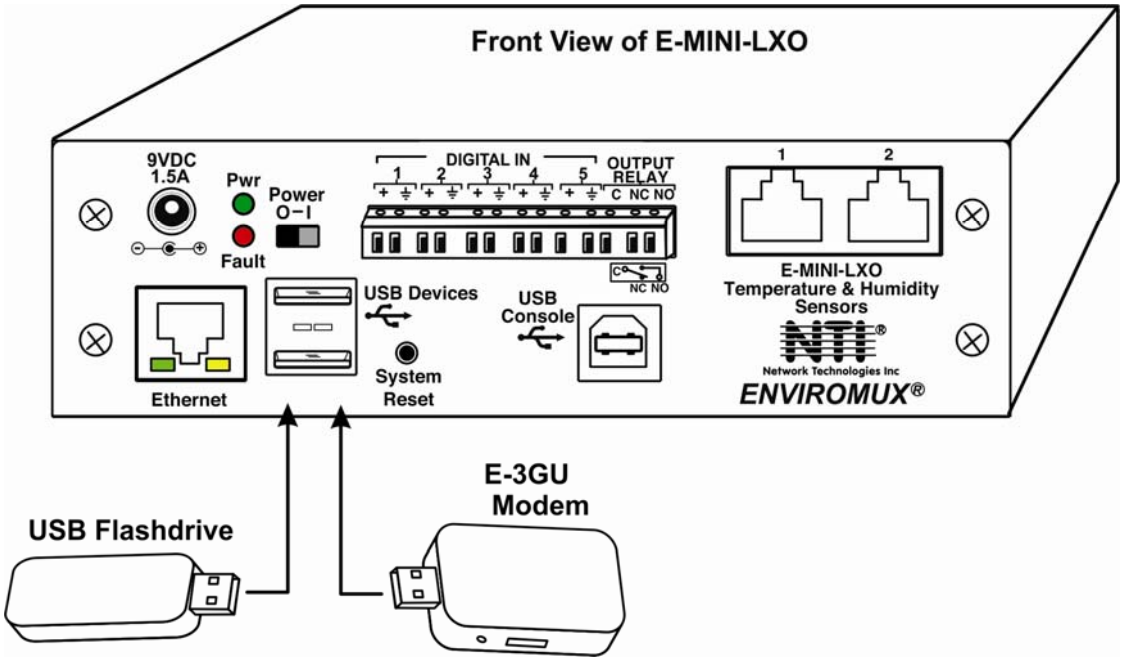


Figure 14- Connect a Modem

Cell phone Mini SIM card for GSM modem

A SIM card or *Subscriber Identity Module* is a portable memory chip used in some models of cellular telephones. It can be thought of as a mini hard disk that automatically activates the phone (or in this case the GSM modem) into which it is inserted.

SIM cards are available in two standard sizes. The first is the size of a credit card (85.60 mm 53.98 mm x 0.76 mm). The newer, more popular miniature-version has a width of 25 mm, a height of 15 mm, and a thickness of 0.76 mm.

Some cellular service providers use Mini SIM cards. Verify with your service provider that their Mini SIM card will work with GSM / 3G GSM modems before making a purchase.

Note: The E-3GU-4 will send SMS messages only. No access to the ENVIROMUX is possible through the modem.

OVERVIEW

Administration

The ENVIROMUX can be administered in any one of the following ways:

- Using Telnet or SSH protocol via the Ethernet Port.
- Using a terminal program via the USB Console Port
- Using the web interface (HTTP/HTTPS protocol) via the Ethernet Port.

The following administrative controls are available in the ENVIROMUX, thru the menu.

- View or modify the administrator & user parameters (passwords, sensor alert subscriptions, admin access, etc.)
- View or modify the network parameters (e.g. IP Address, Gateways, DNS, etc.)
- View and clear system event logs
- Clear, import, export and restore configuration parameters
- Firmware upgrades for the ENVIROMUX (over Ethernet)
- View or modify sensor, and IP device configurations

General Functions

Sensor Alerts

A high and low threshold limit can be set for each temperature or humidity sensor. When a sensor takes a reading that is outside a threshold, an alert notification is generated. The user can specify the frequency of alert notifications to match his or her schedule. Also, there will be some hysteresis involved with alert notifications. This means if a sensor's readings are moving in and out of the threshold boundaries within a configurable period of time, additional alert notifications will not be sent. After an alert is activated, it remains persistent even if the condition of the sensors returns back to normal, until the user acknowledges or dismisses that alert. The user has the option to set the unit to auto-clear the alert if the sensor's status returns to normal, and the user can be notified if the condition goes back to normal. Alert notifications will be provided through four main methods: visible notification via one of the user interfaces (red "Fault" LED on front panel, alert on webpage, alert in text menu), emails, syslog message and/or SNMP traps.

IP Monitoring & Alerts

Individual IP addresses can be monitored. The ENVIROMUX will ping each address, and if a response is received, the IP address status is considered to be "OK"'. If no response, the user will have the option to configure the ENVIROMUX for an alert will be logged and sent. The user can configure the timeout for a response and the number of retries before signaling an alert. The ENVIROMUX can also be configured to monitor the IP addresses of the network switches and routers to which these devices are connected, so as to determine if the problem is due to a lack of response from the device or a network failure. Alert notifications will be provided through four main methods: visible notification via one of the user interfaces (red "Fault" LED on front panel, alert on webpage, alert in text menu), emails, syslog messages, SMS messages and/or SNMP traps.

Event Log

The ENVIROMUX maintains an event log. The event log includes power-ON, system, and alert notifications, as well as user login/logout, and user alert handling. The maximum number of log entries is 1000, and these entries are sorted in chronological order. The log can be viewed at any time through the web interface or text menu, and can be saved as a text file. Log entries can be removed individually or all at once.

Data Log

The ENVIROMUX maintains a data log. The data log includes readings taken from sensors, IP devices, and connected accessories being monitored. The maximum number of log entries is 1000, and these entries are sorted in chronological order. The log can be viewed at any time through the web interface or text menu, and can be saved as a text file. Log entries can be removed individually or all at once.

Email

The ENVIROMUX can access an SMTP server to send outgoing email. Outgoing email would contain pre-formatted alert notifications. SMTP server information can be configured using one of the interfaces. Email addresses can be configured through web pages or text menu. Each user (up to 15) can have their own email address. For assistance in setting up Email, see page 111.

The email messages sent by the ENVIROMUX have a fixed format. Alert emails contain 6 fields and will have a configurable title. The title is configurable for each sensor, device, or IP address. The title is the "email subject" in all configuration pages. A sample message is shown below:

```
ENTERPRISE: Enterprise name here
LOCATION: Danner Drive
CONTACT: John Smith
DESCRIPTION: Undefined #5
TYPE: Humidity
MESSAGE: Sensor value exceeded thresholds
```

SNMP

The ENVIROMUX can send alerts as SNMP traps when a sensor or IP device enters/leaves alert mode and for all log events. Using an SNMP MIB browser, a user can monitor all sensor statuses and system IP settings.

The destination for SNMP traps can be configured for each user.

Note: The SNMP MIB file (mini-lx-v1-xx.mib), for use with an SNMP MIB browser or SNMP trap receiver, can be found at http://www.networktechinc.com/download/d-environment-monitoring.html. Click on the link to open the file, then save the file to your hard drive to use with the SNMP MIB browser or SNMP trap receiver.

GSM Modem

An external GSM modem can be connected to allow the system to send alert notifications via SMS messages. When a sensor crosses a threshold or IP device become inactive, an alert notification can be formatted to SMS message (see page 29) and the modem can transmit the message to all users that subscribe to the applicable sensor group.

Security

User Settings

In order to configure and operate the ENVIROMUX, each user must login with a unique username and password. The Administrator can configure each user's settings as User or Administrator. An Administrator has access to all configurations and controls. A user can monitor sensors, accessories, and IP devices. A user can edit his/her own account. Users cannot configure the sensor settings.

IP Filtering

The ENVIROMUX allows the administrator to block access to the device from certain IP addresses. The ENVIROMUX can accept or drop requests based on the IP filter settings. IP Filtering provides an additional mechanism for securing the ENVIROMUX. Access to the ENVIROMUX network services (SNMP, HTTP(S), SSH, Telnet) can be controlled by allowing or disallowing connections from various IP addresses, subnets, or networks.

Secure Connections

The ENVIROMUX supports secure connections using SSHv2 and HTTPS.

Authentications

The ENVIROMUX supports local authentication with up to 16 character usernames and passwords, and it also supports LDAPv3.

Encryption

The ENVIROMUX supports 256-bit AES encryption.

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-environment-monitoring.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 (version 6 or later) to operate. Here is a link to the web page from which it can be downloaded.

Note: The computer using the Device Discovery Tool and the NTI Device must be connected to the same subnet 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.

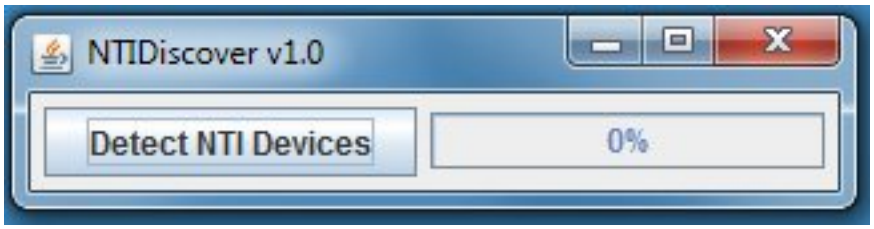


Figure 15- Device Discovery Tool

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.

How to Use the Device Discovery Tool

<u>To Change a Device's Settings</u>, within the row of the device whose settings you wish to change, type in a new setting and click on the **Enter** key, or the **Submit** button on that row. If the tool discovers more than one device, the settings for all devices can be changed and you can click on the **Submit All** button to submit all changes at once.

<u>To Refresh the list of devices</u>, click on the **Refresh** button.

<u>To Blink the LEDs of the unit</u>, click on the **Blink LED** button **(This feature is not supported on all products.)** The **Blink LED** button will change to a "**Blinking…."** button. The LEDs of the unit will blink until the **Blinking…** button is clicked on, or the NTI Device Discovery Application is closed. The LEDs will automatically cease blinking after 2 hours.

<u>To Stop the LEDs of the unit from blinking</u>, click on the **Blinking…** button. The **Blinking….** button will change to a **Blink LED** button.

OPERATION VIA WEB INTERFACE

A user may monitor and configure the settings of the ENVIROMUX and any sensor connected to it using the Web Interface via any web browser (see page 2 for supported web browsers). To access the Web Interface, connect the ENVIROMUX to the Ethernet (page 7). Use the Device Discovery Tool (page 22) to setup the network settings. Then, to access the web interface controls, the user must log in.

By default, the ENVIROMUX is configured to dynamically assign network settings received from a DHCP server on the network it is connected to. (This can be changed to a static IP address to manually enter these settings in the Network Settings on page 41.) The ENVIROMUX will search for a DHCP server to automatically assign its IP address each time the unit is powered up. If the ENVIROMUX does not find a DHCP server, the address entered into the static IP address field (page 41 -default address shown below) will be used. If a DHCP server on the network has assigned the IP address, use the Device Discovery Tool to identify the IP address to enter when logging in to the ENVIROMUX.

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

Log In and Enter Password

To access the web interface, type the current IP address into the address bar of the web browser. (The default IP address is shown below):

http://192.168.1.23

Note: If "Allow HTTP Access" (page 41) is not checked to be enabled (disabled by default) , only an SSL-encrypted connection will be possible. The software will automatically redirect to an HTTPS (secure) connection. The user will likely see a warning about the SSL certificate and a prompt to accept the certificate. The ENVIROMUX uses a self-signed NTI certificate. Accept the NTI certificate.

A log in prompt requiring a username and password will appear:

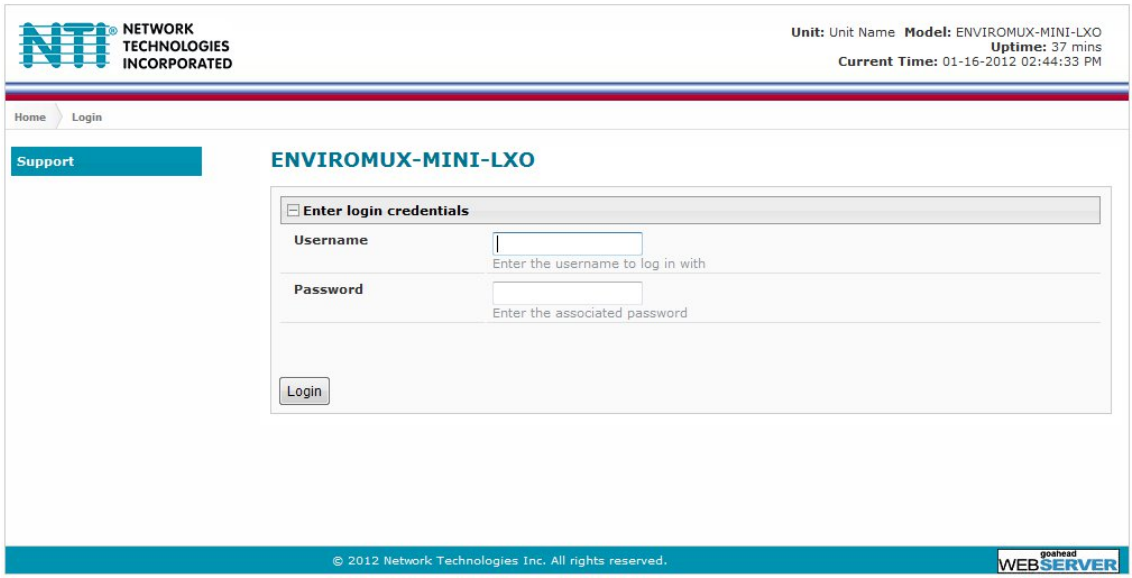


Figure 16- Login prompt to access web interface

Username = root

Password = nti

(lower case letters only)

Note: usernames and passwords are case sensitive

With a successful log in, the “Summary” page with a menu at left will appear on the screen:

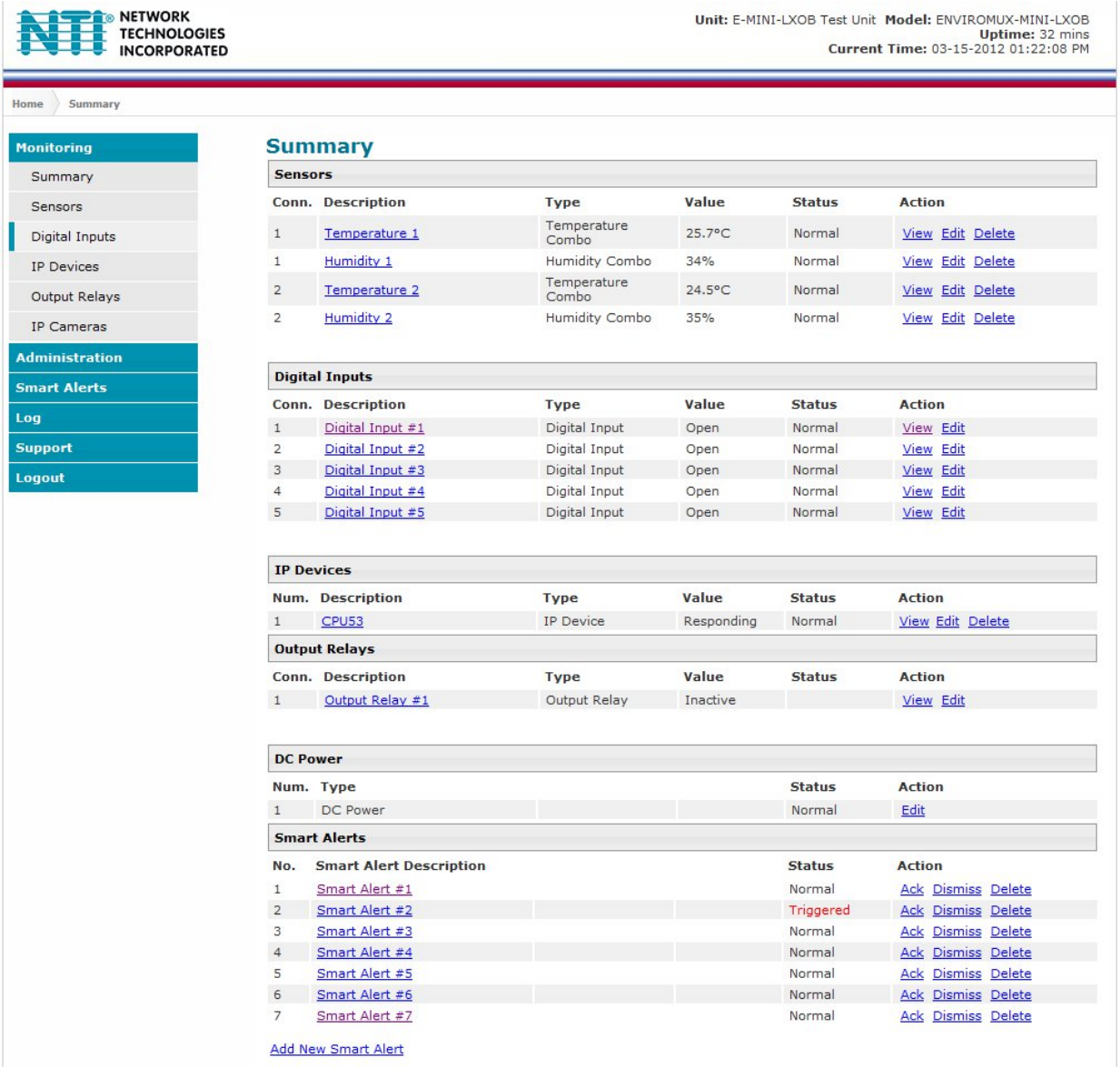


Figure 17- Summary page

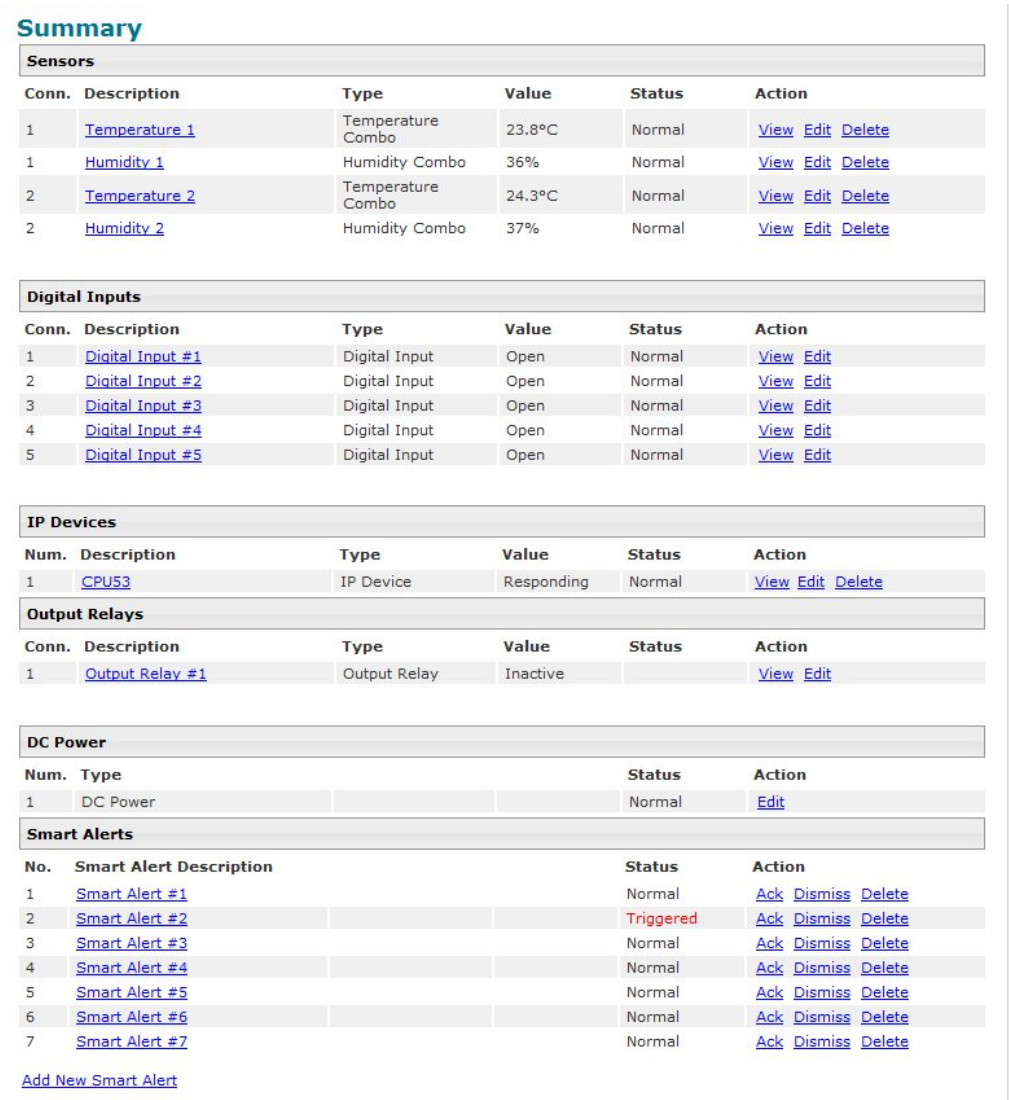
From this initial page, the user can use the menu to the left to manage all the functions of the ENVIROMUX.

Function	Description
MONITORING	Monitor the sensors, accessories, and IP devices of the ENVIROMUX (next page)
ADMINISTRATION	**Configure all system, network, multi-user access, and security settings as well as upgrade firmware (page 38)**
SMART ALERTS	View and configure the Events used for Smart Alerts and the Smart Alerts themselves (page 55)
LOG	View and configure the Event and Data Logs (page 62)
SUPPORT	Links for downloading a manual, the MIB file, or firmware upgrades
LOGOUT	Log the user out of the ENVIROMUX web interface

Monitoring

Under Monitoring, there are links to view the status of all sensors and IP Devices being monitored by the ENVIROMUX.

Link	Description
Summary	Lists all items being monitored, including their description, type, value, and status
Sensors	Provides a link to view the status of only the Sensors and a link to add them (page 27)
Digital Inputs	Provides a link to view the status of any sensors connected to the CONTACT terminals (1-5) a link to view or edit their configuration (page 27)
IP Devices	Provides a link to view the status of only the IP Devices and a link to add them (page 32)
Output Relay	Provides a link to view the status of the output relay and a link to edit the configuration (page 34)
IP Cameras	Displays an image from up to 8 webcams with links to connect to each (page 36)
DC Power	Provides status of the external DC power supply (page 37) (only applicable on models with battery-backup feature)
Smart Alerts	Displays the status of each Smart Alert configuration (page 55) and provided link to respond when triggered



Summary

Sensors

Conn.	Description	Type	Value	Status	Action
1	Temperature 1	Temperature Combo	23.8°C	Normal	View Edit Delete
1	Humidity 1	Humidity Combo	36%	Normal	View Edit Delete
2	Temperature 2	Temperature Combo	24.3°C	Normal	View Edit Delete
2	Humidity 2	Humidity Combo	37%	Normal	View Edit Delete

Digital Inputs

Conn.	Description	Type	Value	Status	Action
1	Digital Input #1	Digital Input	Open	Normal	View Edit
2	Digital Input #2	Digital Input	Open	Normal	View Edit
3	Digital Input #3	Digital Input	Open	Normal	View Edit
4	Digital Input #4	Digital Input	Open	Normal	View Edit
5	Digital Input #5	Digital Input	Open	Normal	View Edit

IP Devices

Num.	Description	Type	Value	Status	Action
1	CPU53	IP Device	Responding	Normal	View Edit Delete

Output Relays

Conn.	Description	Type	Value	Status	Action
1	Output Relay #1	Output Relay	Inactive		View Edit

DC Power

Num.	Type	Status	Action
1	DC Power	Normal	Edit

Smart Alerts

No.	Smart Alert Description	Status	Action
1	Smart Alert #1	Normal	Ack Dismiss Delete
2	Smart Alert #2	Triggered	Ack Dismiss Delete
3	Smart Alert #3	Normal	Ack Dismiss Delete
4	Smart Alert #4	Normal	Ack Dismiss Delete
5	Smart Alert #5	Normal	Ack Dismiss Delete
6	Smart Alert #6	Normal	Ack Dismiss Delete
7	Smart Alert #7	Normal	Ack Dismiss Delete

Add New Smart Alert

Figure 18- Summary page and the Monitoring menu

From the Summary page, the user can view the status of all sensors and the IP Devices being monitored by the ENVIROMUX. Each item listed has a link that when selected will open the status page for that item.

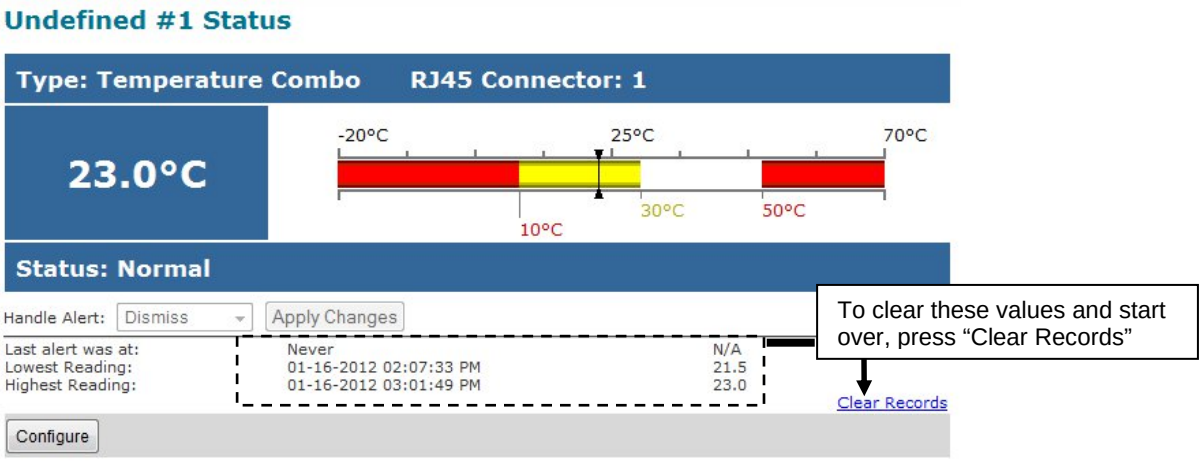


Figure 19- Status page for a temperature sensor

If the temperature 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 (page 28) elapses.

After selecting **acknowledge** or **dismiss**, click **Apply Changes**.

The administrative user can open the sensor configuration page by clicking on the **Configure** button at the bottom of the sensor status page (above) or by clicking on **Edit** from the Summary page. From the sensor configuration page the user can apply settings to control how or if alert messages are sent in the event the sensor is in alert status, threshold settings, and data logging settings.

Configure Sensors

The Sensor Configuration page is broken into three sections; Sensor Settings, Alert Settings and Data Logging. To explode the window to see settings for a section, click on the section heading (Figure 20).

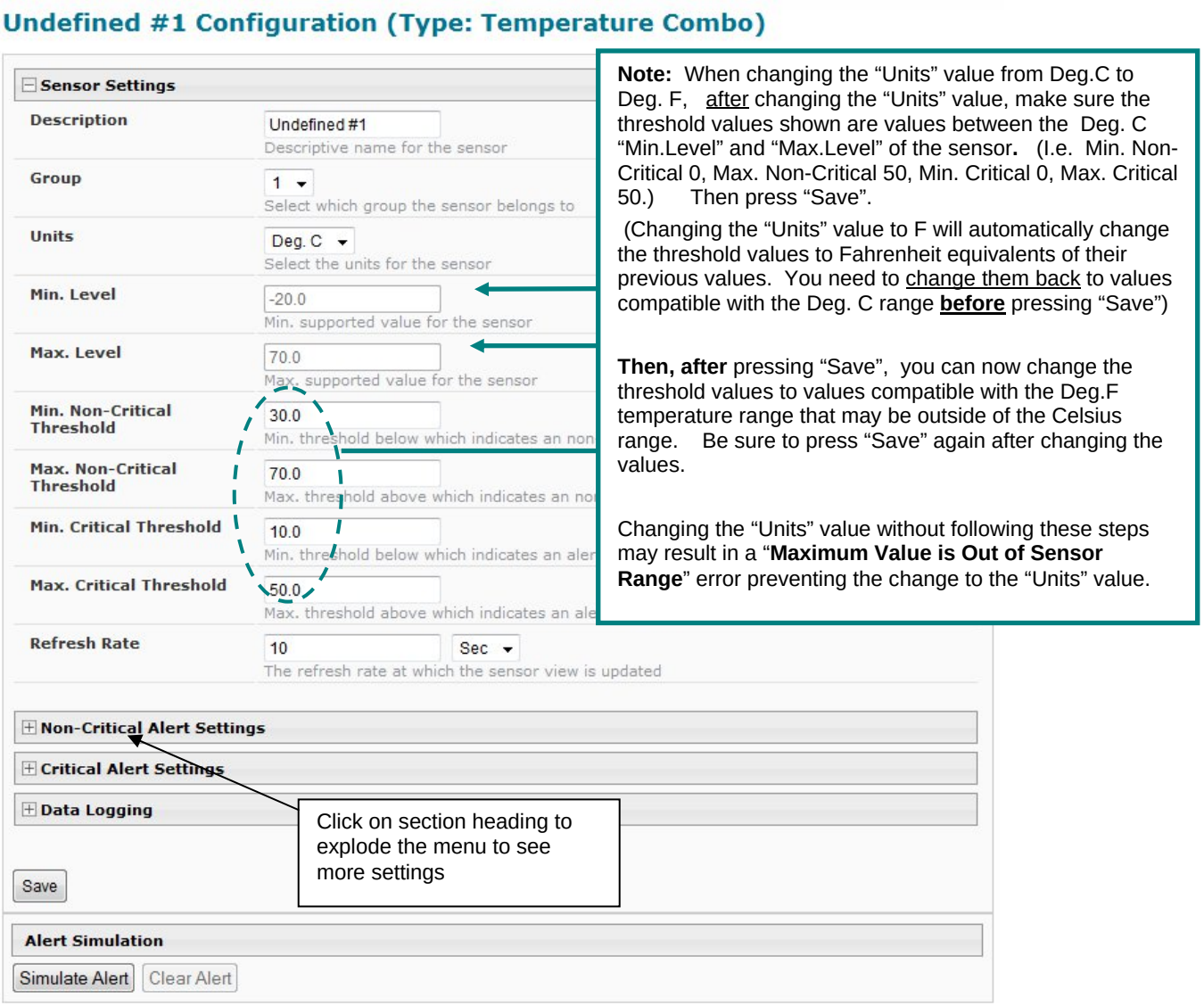


Figure 20- Sensor Configuration page

Threshold Settings

A sensor designed for connection to the RJ45 ports often has a range of reporting values (for example E-T has a range of 32°-104°F). Two levels of threshold values for each end of that range can be configured (above) to initiate two different alert messages, depending upon the severity of the alert. These levels are identified as "Non-critical" and "Critical". Use these variations in alert communication as needed to inform users of the severity of sensor reading changes. Each level of alert has its own configuration for how or if the user will be alerted as to a sensor's status (see Figure 21).

Non-Critical Alert Settings

Disable Alerts	☑ Disable alert notifications for this sensor
Alert Delay	30 Sec Duration the sensor must be out of thresholds before alert is generated
Notify Again Time	30 Min Time after which alert notifications will be sent again
Notify on return to normal	☑ Send a notification when this sensor returns to normal status
Enable Syslog Alerts	☐ Send alerts for this sensor via syslog
Enable SNMP Traps	☐ Send alerts for this sensor via SNMP traps
Enable E-mail Alerts	☐ Send alerts for this sensor via e-mail
E-mail Subject	Subject of e-mails sent for alerts
Enable SMS Alerts	☐ Send alerts for this sensor via SMS
Associated Output Relay	None Name of the output relay that can be controlled by this sensor
Output Relay status on alert	Active Status of the output relay when going to alert
Output Relay status on return from alert	Active Status of the output relay when returning from alert

Critical Alert Settings

Disable Alerts	☐ Disable alert notifications for this sensor
Alert Delay	30 Sec Duration the sensor must be out of thresholds before alert is generated
Notify Again Time	30 Min Time after which alert notifications will be sent again
Notify on return to normal	☑ Send a notification when this sensor returns to normal status
Auto acknowledge	☐ Automatically acknowledge alert when sensor returns to normal status
Enable Syslog Alerts	☐ Send alerts for this sensor via syslog
Enable SNMP Traps	☐ Send alerts for this sensor via SNMP traps
Enable E-mail Alerts	☑ Send alerts for this sensor via e-mail
E-mail Subject	Subject of e-mails sent for alerts
Attach IP camera capture to e-mail	☐ Bench Camera Attach captured image from selected IP camera to alert e-mail
Enable SMS Alerts	☐ Send alerts for this sensor via SMS
Associated Output Relay	None Name of the output relay that can be controlled by this sensor
Output Relay status on alert	Inactive Status of the output relay when going to alert
Output Relay status on return from alert	Inactive Status of the output relay when returning from alert

Data Logging

Figure 21- Sensor Configuration- exploded view of additional settings

Sensor Settings	Description
Description	The description of the sensor that will be viewed in the Summary page and in the body of alert messages
Group	Assign the sensor to any group 1 -8 (see also page 44)
Units	This lets the operator choose between Celsius and Fahrenheit as the temperature measurement unit. **SEE NOTE-PAGE 27- regarding changing this value**
Min. Level	Displays the minimum value that this sensor will report
Max. Level	Displays the maximum value that this sensor will report
Minimum Non-Critical - 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 non-critical 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, and error message will be shown.
Maximum Non-Critical 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 non-critical 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, and error message will be shown.
Minimum Critical 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, ➢ lower than the assigned Maximum Threshold value, and ➢ lower than the Minimum Non-Critical Threshold value. If values out of the range are entered, and error message will be shown.
Maximum Critical 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, ➢ higher than the assigned Minimum Threshold value, and ➢ higher than the Maximum Non-Critical Threshold value. If values out of the range are entered, and error message will be shown.
Refresh Rate	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.
Alert Settings (Applies to Critical and Non-Critical Alerts except where noted)	
Disable Alerts	Place a checkmark in the box to prevent alerts from being sent when this sensor's status changes
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.
Notify Again Time	Enter the amount of time in seconds, minutes, or hours (1-999) before an alert message will be repeated
Notify on Return to Normal	The user can also be notified when the sensor readings have returned to the normal range by selecting the "***Notify when return to normal***" box for a sensor.
Auto Acknowledge	Place a checkmark in this box to have alert notifications in the summary page return to normal state automatically when sensor readings return to normal. **Note**: The Non-Critical alert settings do not have this option. Instead, non-critical alert notifications are always auto-acknowledged when sensor readings return to normal
Enable Syslog Alerts	Place a checkmark in this box to have alert notifications sent via Syslog messages
Enable SNMP traps	Place a checkmark in this box to have alert notifications sent via SNMP traps (v2c)
Enable Email Alerts	Place a checkmark in this box to have alert notifications sent via Email
Email Subject	Enter the subject to be viewed when an email alert message is received

Alert Settings (Applies to Critical and Non-Critical Alerts except where noted)	
Attach IP Camera capture to email	Associate a sensor with a IP camera. Select an IP camera from the drop-down box. An image will be captured and sent with the alert message when an alert is sent via e-mail. IP cameras that are monitored by the ENVIROMUX (page 36) will be available for this purpose. ***Note: To be able to send IP camera captures as e-mail attachments, viewer security (in your camera's configuration) needs to be disabled. Consult your IP camera manual to see if this feature is present and for instructions on how to do this.***
Enable SMS Alerts	Place a checkmark in this box to have alert notifications sent via SMS messages (requires a modem)
Associated Output Relay	Associate the sensor with the operation of the output relay, or not ***Note: Only one sensor should be associated with the Output Relay at a time. Contradicting commands from two or more sensors will result in the output relay responding to the state directed by the last command received.***
Output Relay Status on Alert	State the output relay will be in when sensor goes to an alert
Output Relay Status on Return from Alert	State the output relay will be in when sensor is no longer in alert
Data Logging	
Add to data log	This is a check-box that lets the user decide if the data sampled should be recorded in the Data Log.
Logging Period	Enter the time period between logged measurements

Be sure to press the **Save** button to save the configuration settings.

Note: If the Output Relay is associated with a sensor, and configured to change state when a sensor crosses threshold into alert, it will change state even if the alerts are disabled.

More about Groups

Groups are used to create a common relationship between sensors, IP devices, etc. and their alert messages. Each item being monitored is assigned to one group of 8 possible. Users (a maximum number of 16 including the root user) can receive alert messages from items in one or more groups (see user configuration on page 44).

Test Alerts

With all the configuration settings completed, each sensor and how the ENVIROMUX will react to an alert condition can be tested. Press the **Simulate Alert** button at the bottom of the configuration page to test each of the notification methods configured. To cancel the simulation, press the **Clear** button.

Note: A simulated alert will test all settings including any delay that has been configured (i.e. if a 2 minute delay is configured, it will delay sending the email for 2 minutes)

To perform a test, the ENVIROMUX must be properly setup for a user to receive alert messages. Use the chart below to make sure the ENVIROMUX is setup properly.

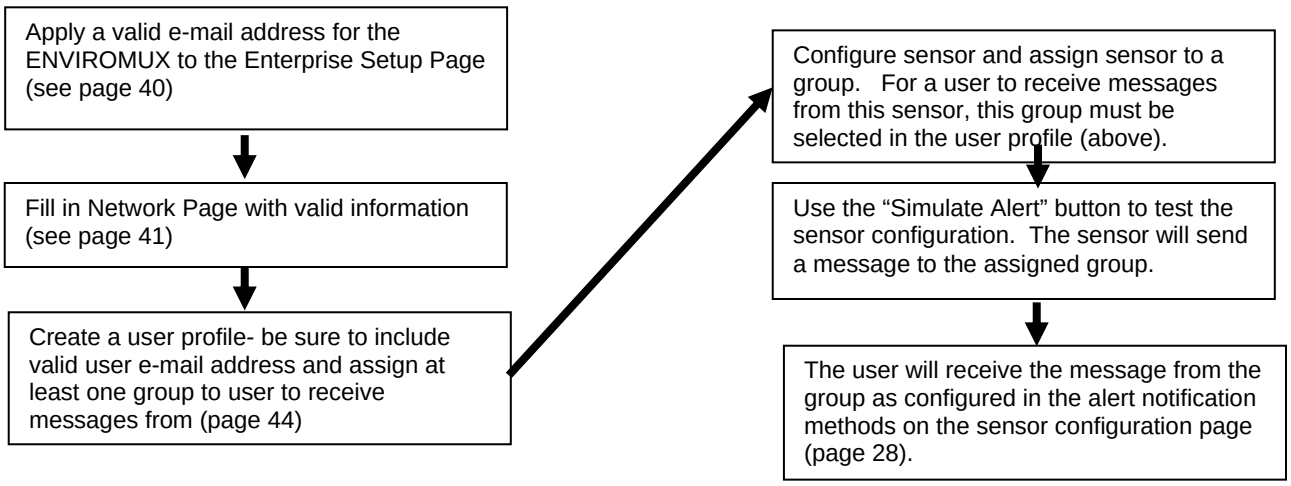


Figure 22- Chart to setup alert notification

Configure Digital Inputs

The configuration page for digital inputs is almost the same as that for temperature and humidity sensors, with a few differences. Instead of threshold and minimum/maximum levels settings, digital inputs (water sensors and contact sensors) are either open contact or closed contact sensors. Therefore, the field "Normal Status" is provided to select the status of the sensor when it is not in an alert state. Select between **Open** contacts, or **Close** contacts for the normal status of the sensor. (Water sensors are open contact when not in alert state.)

Alert settings and data logging features are the same as those described on page 29.

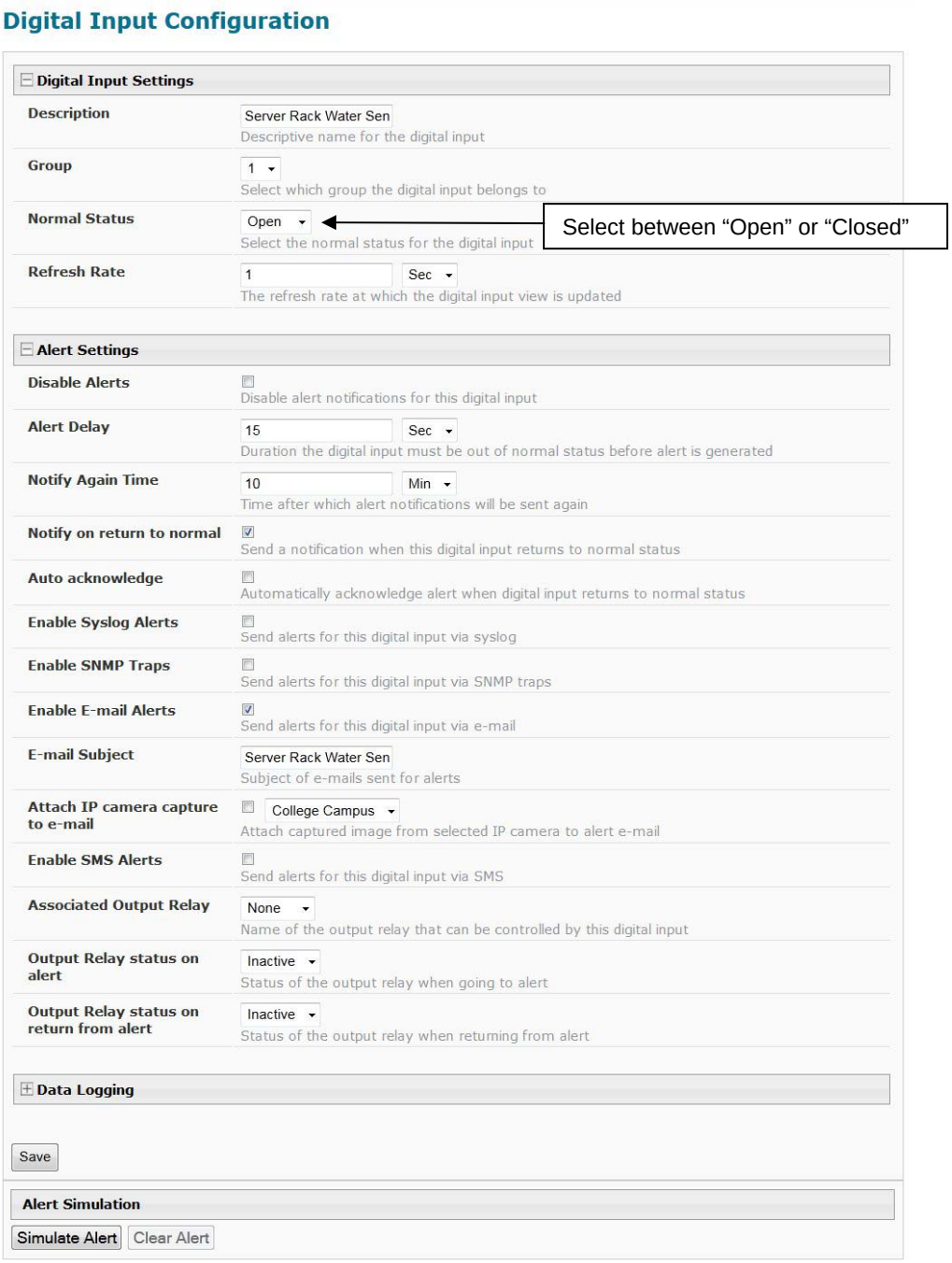


Figure 23- Sensor Configuration for Digital Inputs

Monitor IP Devices

IP devices such as servers, routers, cameras, etc. can be monitored to make sure network connections are open to them. In order to monitor an IP Device the devices must be added to the list of IP Devices being monitored. From the **Monitoring** section of the menu, click on **IP Devices.** A page listing IP Devices being monitored will open, with a link to add IP Devices. Click on **Add New IP Device**.

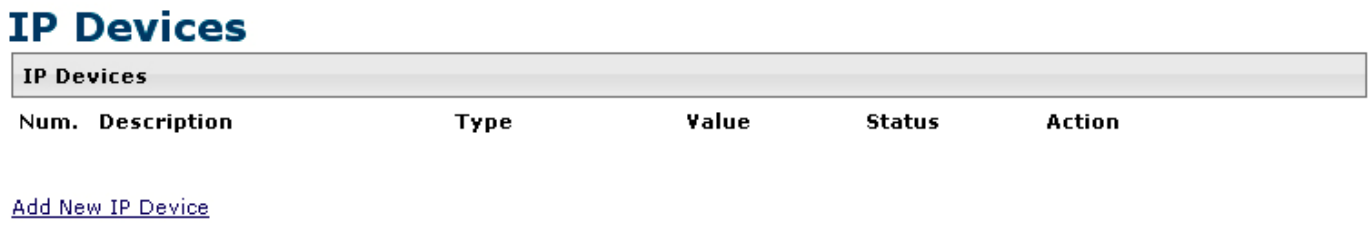


Figure 24- IP Devices listing-none monitored yet

The page shown below will open. Enter a description for the new IP Device and the IP Address of the device.

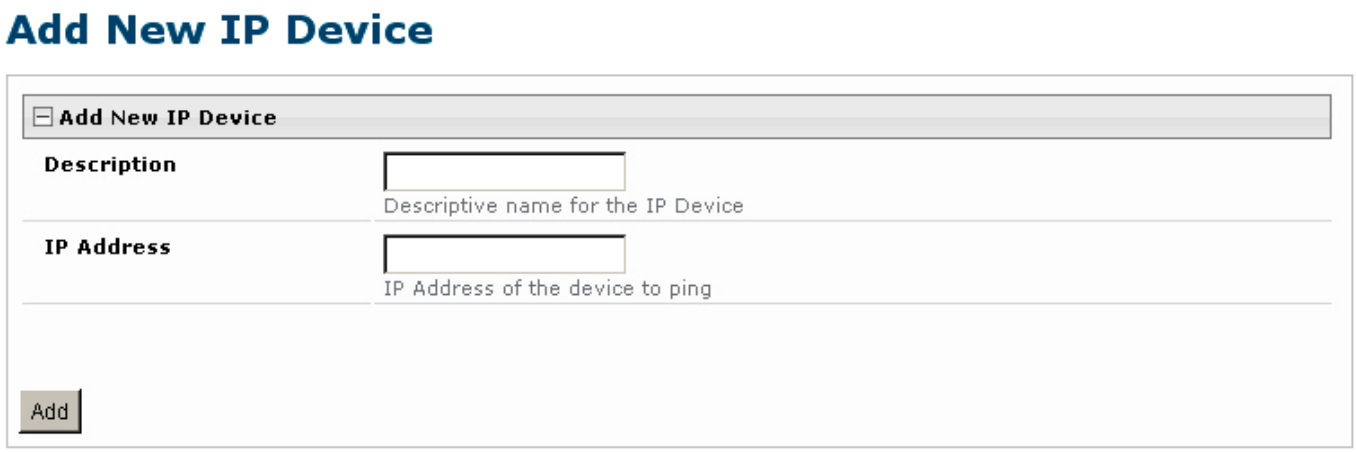


Figure 25- Add New IP Device page

With the address entered in the block, click on the "**Add**" button.

The IP Device Configuration page will immediately open. Here you can configure the ENVIROMUX to ping the IP Device as often as desired and to react to a lack of response by sending alert messages.

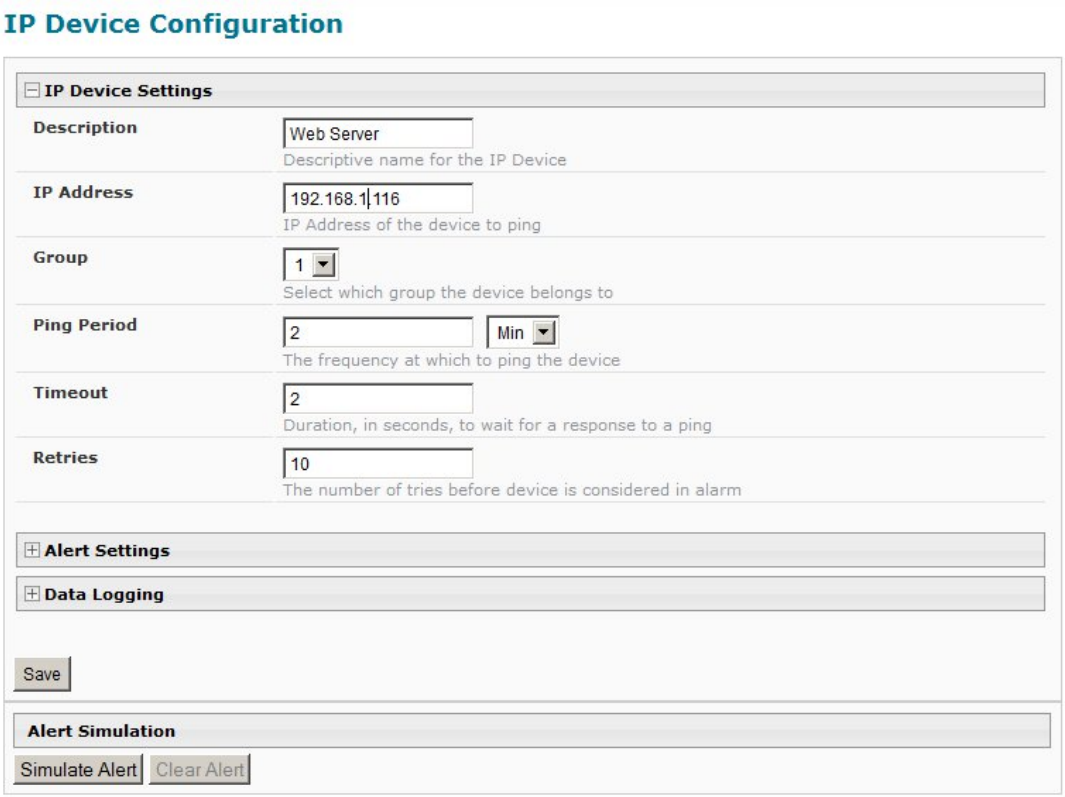


Figure 26- IP Device Configuration page

IP Device Settings	Description
Description	The description of the IP Device that will be viewed in the Summary page and in the body of alert messages
IP Address	The IP address of the IP Device
Group	Assign the IP Device to any group 1 -8
Ping Period	Enter the frequency in minutes or seconds that the ENVIROMUX should ping the IP Device
Timeout	Enter the length of time in seconds to wait for a response to a ping before considering the attempt a failure
Retries	Enter the number of times the ENVIROMUX should ping a non-responsive IP device before changing its status from normal to alarm and sending an alert

The alert settings and data logging are the same as for sensor configuration, described on page 29.

As an example, let's assume the three configurable values are set as follows:

Ping Period = 10 sec Timeout = 2 sec Retries = 5

The device being monitored will be pinged every 10 seconds and it should respond within 2 seconds.

If the device fails to respond within the 2 second timeout, the retry will occur immediately and wait two more seconds. This will repeat for as many retries as you have configured. In this case, 5 tries. With 5 failures, the status will change to alert.

With a couple of IP devices having been configured for monitoring, the IP Device list will provide links to them for viewing their status, editing their configuration, or deleting them from the list.

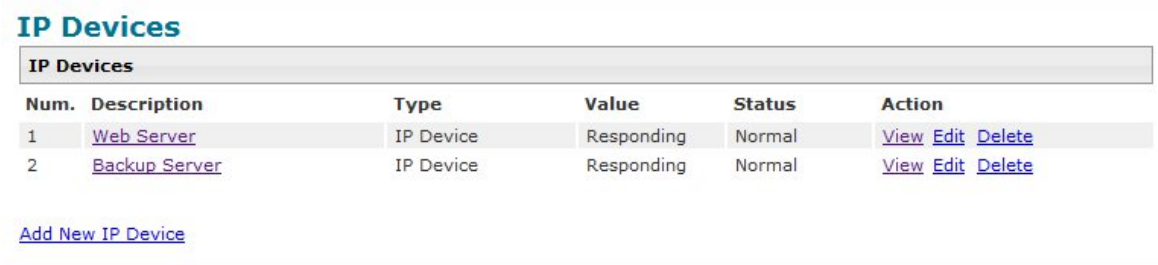


Figure 27- IP Device list with new devices added

To view the graphic image showing the status of an IP address, click on the IP Device description or click **View**. From the IP Device status page, the user can view the current status, either dismiss or acknowledge an alert, or open the IP Device configuration page (if the user has administrative privileges). If you have found the device to be in an alert state and have either dismissed or acknowledged it, be sure to click the **Apply Changes** button.

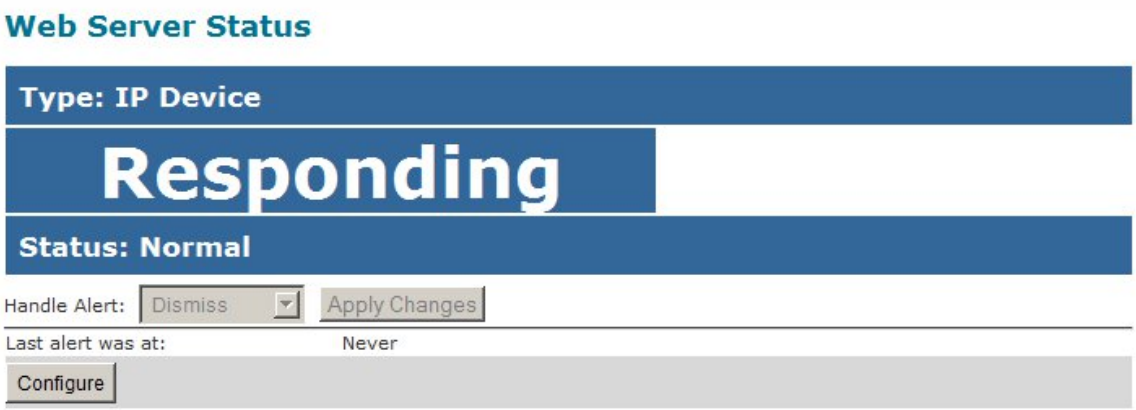


Figure 28- IP Device Status page

Monitor Output Relay

An output relay is provided to control an external device with a rating of up to 1A, 30VDC or 0.5A, 125VAC. The relay state is monitored to be either inactive (relay is at rest; contacts as indicated by product markings) or active (relay is energized; contacts are opposite that of product markings). The status of the relay can be changed either manually through the web interface, or as a result of an alert (page 27).

Figure 29- Output Relay Status

To set the state of the relay manually, from the relay status page (Figure 29), select the arrow next to “Set Output” to drop down the window and select either “Deactivate” or “Activate”. Then click the “Apply Changes” button.

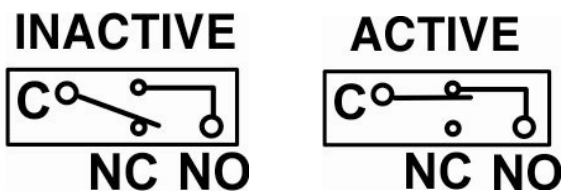
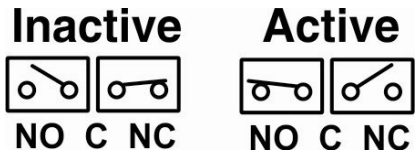


Figure 30- Output Relay Contact State

Note: A recent design improvement resulted in a change to the pinout of the output relay in the E-MINI-LXO. Please be aware of the change and note which version yours is. The previous version is shown below.



To change settings for the output relay and whether or not a state change should generate an alert message, click the "Configure" button.

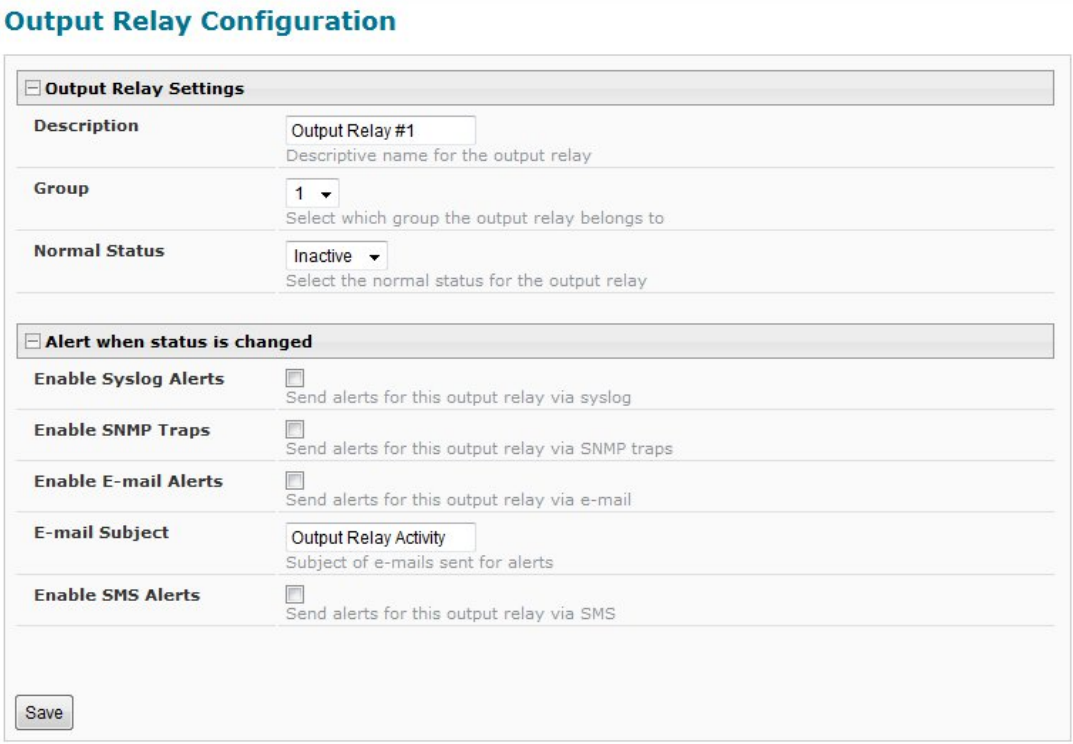


Figure 31- Configure Output Relay

From the configuration page, the user can apply a description of the relay that will be used on the summary page and in any alert messages sent, if so configured.

To have messages sent to specific members, select the monitoring group the relay will belong to.

Choose the Normal Status for the relay, between Inactive or Active. When the status changes from what is defined as "normal", an alert will be sent if so configured.

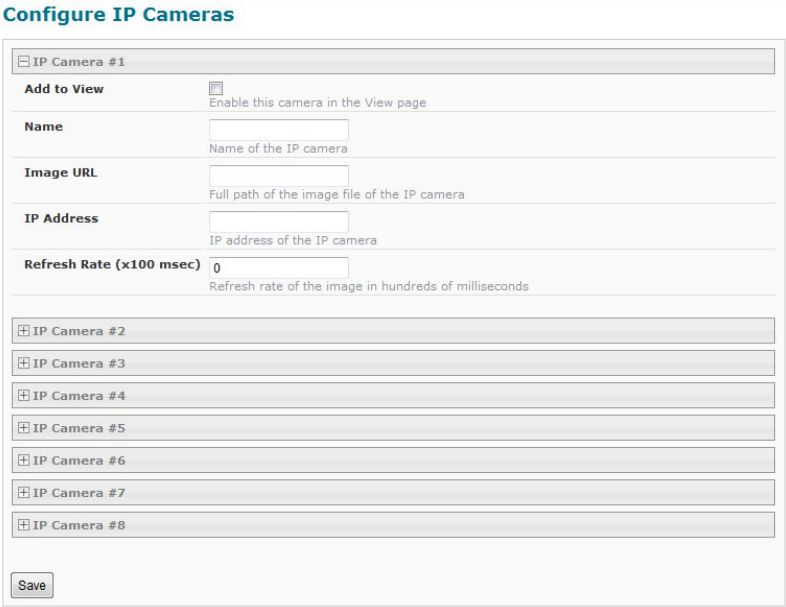
When the relay is an alert state, the ENVIROMUX can be configured to send an email, syslog and SMS alerts, as well as an SNMP trap to the users subscribing to alerts in the selected group. Place a checkmark in the box for those features you wish to enable.

If email alerts is enabled, enter an e-mail subject line that will get the attention of the recipient(s).

Monitor IP Cameras

The IP Cameras page displays the video snapshots of up to 8 monitored IP cameras. ENVIROMUX will display the video from specified IP addresses and provide images at 320 x 240 resolution. To configure the IP cameras to be monitored, click on the "Configure IP Cameras" link.

Figure 32- IP Camera Monitoring



Place a name, the URL or IP address of the link, and the full path including name of the image taken by the camera in the blocks provided, click the "Add to view" checkbox, and click SAVE at the bottom of the page. Then click on **Monitoring->IP Cameras** to see the images taken by those cameras. The images can be set to be refreshed every 100 msec (.1 second) up to 99,900 msec (almost 100 seconds). The user can click on any image and be connected to the site defined by the URL or IP Address.

Figure 33- Configure IP Cameras

The images from IP cameras can also be associated with alert messages. When configured (page 27), an image from a IP camera can be taken and sent along with a sensor alert message via email.

Note: To be able to send IP camera captures as e-mail attachments, viewer security (in your camera's configuration) needs to be disabled. Consult your IP camera manual to see if this feature is present and for instructions on how to do this.

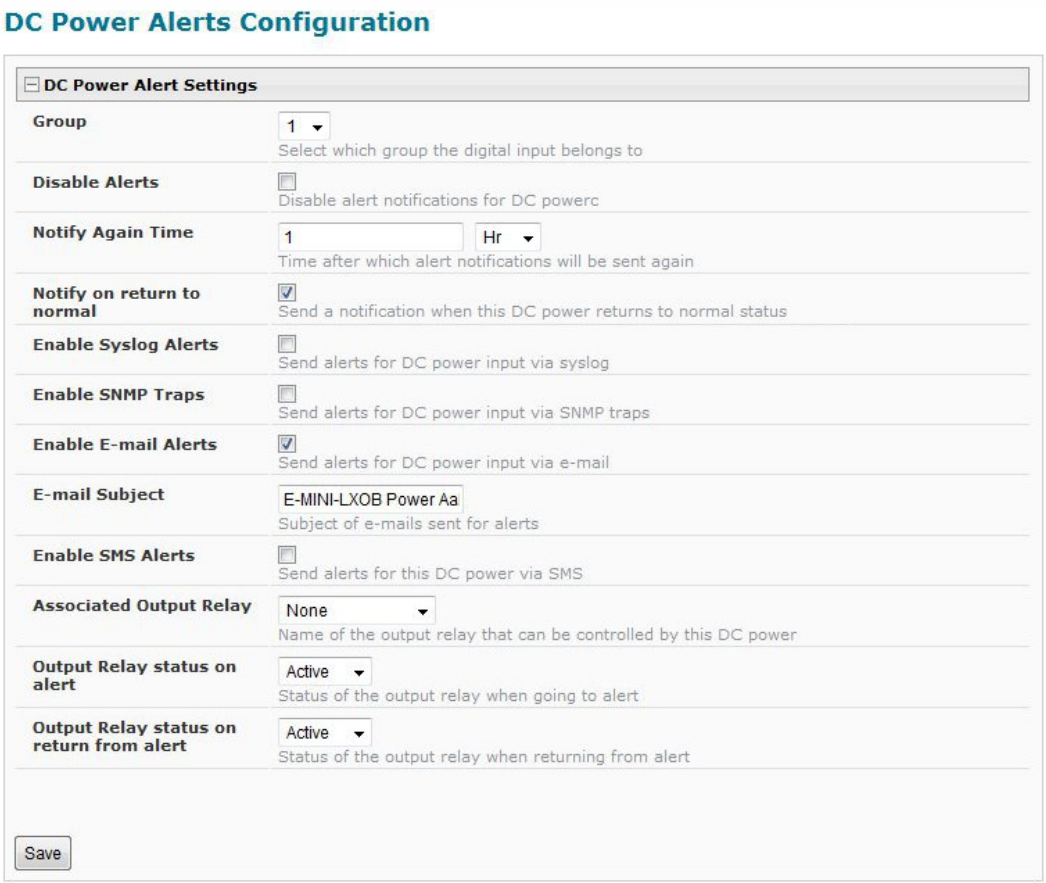
DC Power

On the Summary Page (under Monitoring), the status of the DC power supply can be found (only applicable for models with battery backup). The ENVIROMUX will monitor the power coming into the ENVIROMUX and can be configured to send an alert in the event that power supply fails. Click on "Edit" to configure how the ENVIROMUX should respond.

DC Power

Num.	Type			Status	Action
1	DC Power			Normal	Edit

Figure 34- Excerpt from the Summary Page showing DC Power monitoring



DC Power Alerts Configuration

DC Power Alert Settings

Group	1 Select which group the digital input belongs to
Disable Alerts	☐ Disable alert notifications for DC powerc
Notify Again Time	1 Hr Time after which alert notifications will be sent again
Notify on return to normal	☑ Send a notification when this DC power returns to normal status
Enable Syslog Alerts	☐ Send alerts for DC power input via syslog
Enable SNMP Traps	☐ Send alerts for DC power input via SNMP traps
Enable E-mail Alerts	☑ Send alerts for DC power input via e-mail
E-mail Subject	E-MINI-LXOB Power Aa Subject of e-mails sent for alerts
Enable SMS Alerts	☐ Send alerts for this DC power via SMS
Associated Output Relay	None Name of the output relay that can be controlled by this DC power
Output Relay status on alert	Active Status of the output relay when going to alert
Output Relay status on return from alert	Active Status of the output relay when returning from alert

Save

Figure 35- DC Power Alert Configuration

Many of the same options that apply to sensor alerts (page 27) can be configured for DC Power alerts. The battery backup will keep the ENVIROMUX on line for up to 2.3 hours in the event of a power failure.

Administration

From the Administration section there are several sub sections for configuring the ENVIROMUX:

System	Fields for applying time zone, date, time, NTP server, and backup and restore configuration settings
Enterprise	Fields for assigning the unit name, address, contact person, the ENVIROMUX e-mail address, and phone number of a contact person
Network	Fields for providing all the network settings the ENVIROMUX including IP address, DNS, SMTP and SNMP settings
Users	Fields for assigning users, access privileges, passwords, contact settings, and schedule settings
Security	Fields for setting authentication method and IP Filtering
System Information	For viewing ENVIROMUX system information
Firmware	For updating the firmware of the ENVIROMUX when improved software becomes available.
Reboot	Enables user to reboot the ENVIROMUX using the web interface

System Configuration

The System Configuration section is where all the settings necessary for proper time reporting within alert messages and log records are configured. To view the System Configuration page, click on **System** from the **Administration** section of the menu.

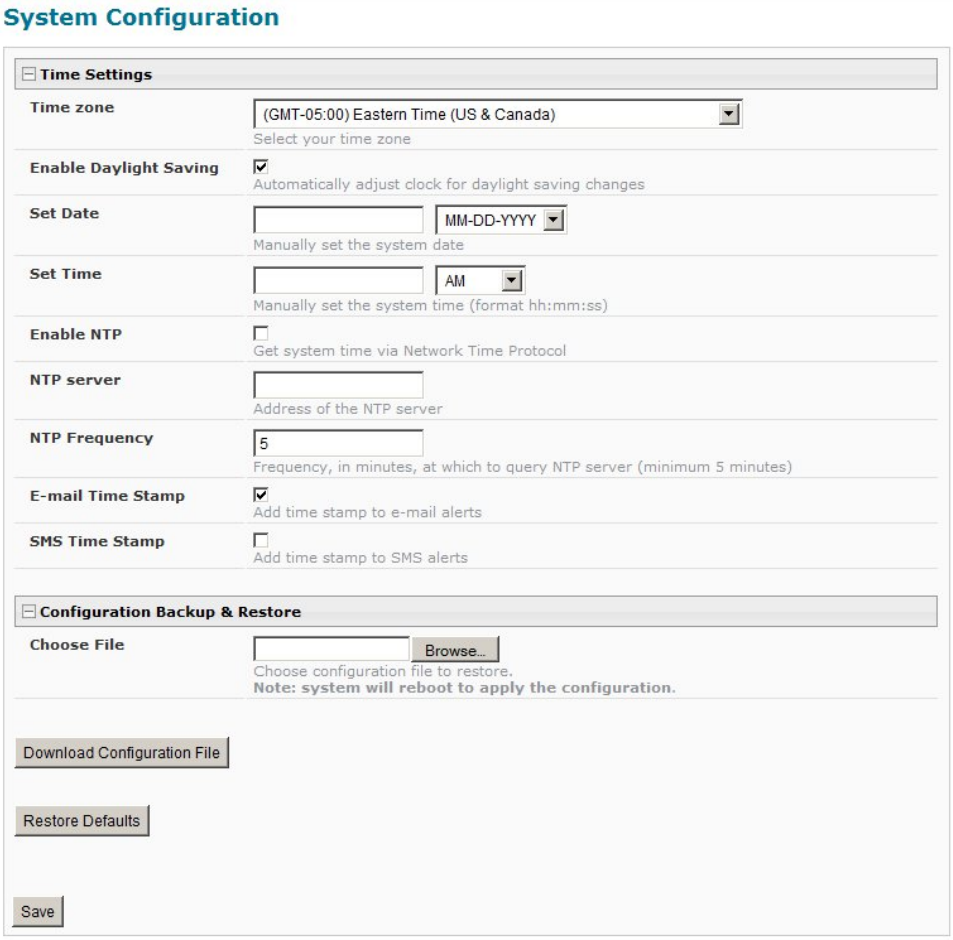


Figure 36- System Configuration page

The Date and Time of the ENVIROMUX can be either manually setup to use an onboard clock or set to be synchronized with an NTP server. The configuration of the ENVIROMUX can also be easily backed up to a file on your PC and restored from that file as needed.

Time Settings	Description
Time Zone	Enter the appropriate time zone
Enable Daylight Saving	Apply a checkmark to have the time change according to Daylight Saving Time rules
Set Date	Enter the system date in MM-DD-YYYY format
Set Time	Enter the system time of day in hh:mm:ss format
Enable NTP	Place a checkmark to enable the ENVIROMUX to automatically sync up with a time server via NTP
NTP server	If the NTP is enabled, enter the Domain Name or IP address of the NTP server
NTP Frequency	Enter the frequency (in minutes) for the ENVIROMUX to query the NTP server (minimum is 5 minutes)
E-mail Time Stamp	Place a checkmark to have the ENVIROMUX apply a time of day stamp in the alert message sent via email
SMS Time Stamp	Place a checkmark to have the ENVIROMUX apply a time of day stamp in the alert message sent via SMS
Configuration Backup & Restore	
Choose file	Browse for a saved configuration file to be restored to the ENVIROMUX. Upon selection, the ENVIROMUX will restore the configuration settings and reboot. Allow 1 minute before trying to reconnect and log in again. ***Note: The IP address will be set to the IP address in the file and may be different***
Download Configuration File	Click this button to save the configuration of the ENVIROMUX to a location on your PC. This file can be restored using the "Choose file" field in the event you wish to return the ENVIROMUX to a former state. **SEE NOTE BELOW**
Restore Defaults	Click this button to restore the ENVIROMUX to the configuration settings it had upon receipt from the factory. **Be careful!** This will erase all user configuration settings. Upon restoration, the ENVIROMUX will reboot. Allow 1 minute before trying to reconnect and log in again. **Confirmation is required**.

Note: If "Restore Defaults" is used, the IP address will also be restored to its default address of 192.168.1.23 with a login name "root" and password "nti". To restore the root password to "nti" without having to restore all default settings, contact NTI for assistance.

To identify the IP address of the ENVIROMUX without restoring defaults, use the Discovery Tool (page 22).

Click on **Save** when finished with Time Setting changes.

Default settings can also be restored through the serial interface via text menu (page 85).

Note: Do not try to manually edit the downloaded configuration file and then restore it to the ENVIROMUX. The ENVIROMUX will quit working and you will have to return it to NTI to have default settings restored. Factory restoration of the default settings is not covered under the product warranty.

Enterprise Configuration

The Enterprise Configuration page is used to enter basic company information to be applied to the body of alerts. To view the Enterprise Configuration, click on **Enterprise** from the **Administration** section of the menu. Enter in the blocks your unit name, location, the contact person that alert e-mails should refer to, the phone number to reach them, and the e-mail address assigned to the ENVIROMUX.

If a GSM modem is properly installed (page 19), the "Modem Status" found in the GSM Modem Status section will indicate "Connected" and the IMEI number for the modem will be indicated. Once the modem makes connection with the cell tower, "Connected" will change to "Ready" (as seen below).

Note: It may take several minutes for the GSM modem to be detected by the ENVIROMUX.

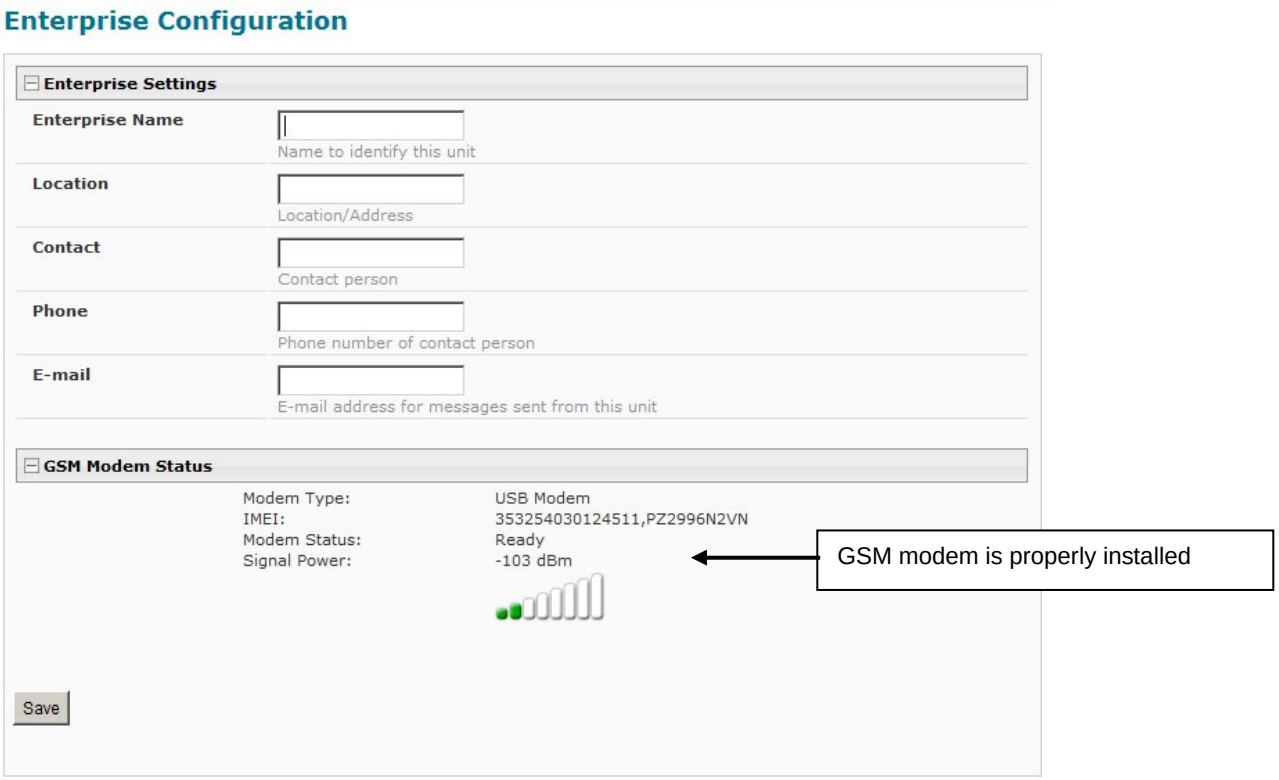


Figure 37- Enterprise Configuration- Modem Status "Ready"

If no modem is installed, the modem type will be "Not Available" and the status will be "Not Connected".

Figure 38- No Modem Installed

Network Configuration

From the Network Setup page the administrator can either choose to have the IP address and DNS information filled in automatically by the DHCP server (the default setting), or manually fill in the fields (use a static address). Settings can be entered for either the IPv4 or IPv6 protocols. To view the Network Configuration page, click on **Network** from the **Administration** section of the menu.

Note: If you select "DHCP", make sure a DHCP server is running on the network the ENVIROMUX is connected to.

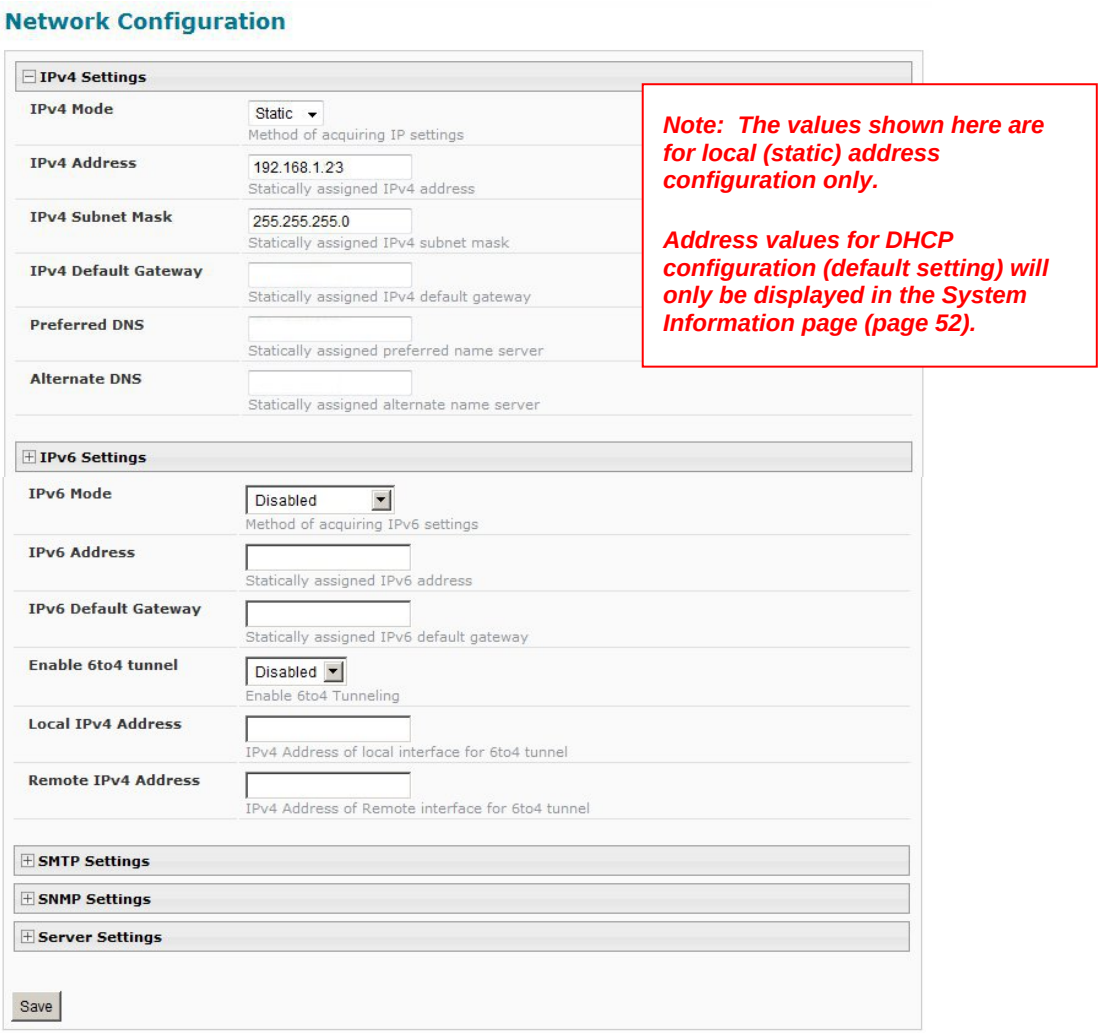


Figure 39- Network Configuration page

IPv4 Settings	Description
Mode	Select between Static (manual) , or DHCP (automatic IP and DNS) settings (default)
IP Address	Enter a valid IP address (default address shown above)
Subnet Mask	Enter a valid subnet mask (default value shown above)
Default Gateway	Enter a valid gateway (default gateway shown above)
Preferred DNS	Enter a preferred domain name server address
Alternate DNS	Enter an alternate domain name server address

Enter IPv6 settings as applicable.

For descriptions of SMTP, SNMP, and Server Settings, see page 43. .

The Network Configuration page is broken into four sections; IP Settings, SMTP Settings, SNMP Settings, and Server Settings. To explode the window to see settings for a section, click on the section heading.

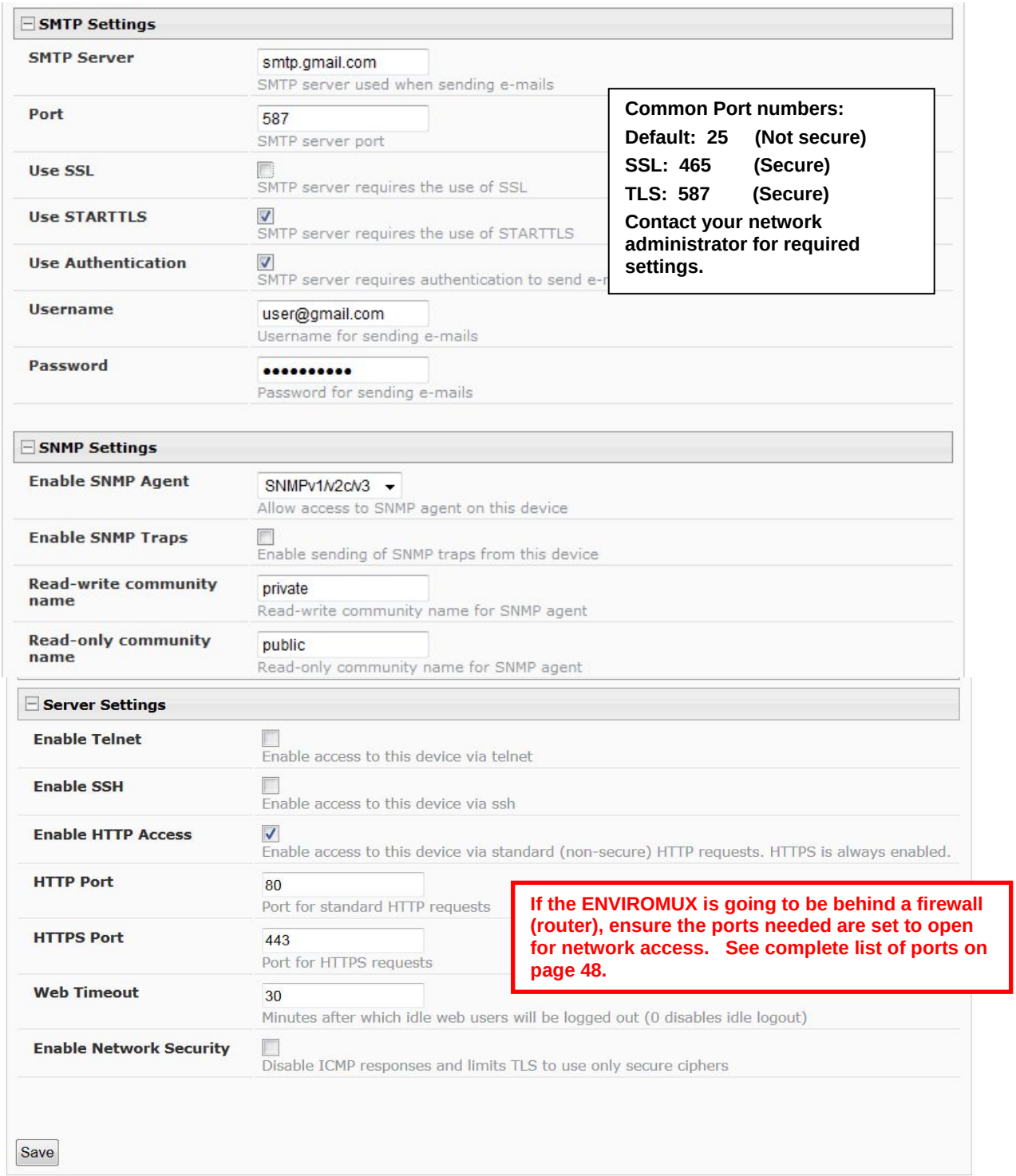


Figure 40- Network Configuration- more settings

More Network Settings (see Figure 40)

SMTP Settings	Description
SMTP Server	Enter a valid SMTP server name (e.g. yourcompany.com)
Port	Enter a valid port number (default port is 25, for SSL most use 465, for STARTTLS most use 587)
Use SSL	Place a checkmark in the box if the SMTP server supports SSL
Use STARTLS	Place a checkmark in the box if the SMTP server supports TLS
Use Authentication	Place a checkmark in the box if the SMTP server requires authentication to send email
Username	Enter a valid username to be used by the ENVIROMUX to send emails
Password	Enter a valid password assigned to the ENVIROMUX username
SNMP Settings	
Enable SNMP agent	Place a checkmark in the box to enable access to the SNMP agent
Enable SNMP traps	Place a checkmark in the box to allow SNMP traps to be sent
Read-write community name	Enter applicable name (commonly used- "private") **Not applicable as of this printing**
Read-only community name	Enter applicable name (commonly used- "public")
Server Settings	
Enable Telnet	Place a checkmark in the box to enable access to the ENVIROMUX via Telnet **The default is disabled.**
Enable SSH	Place a checkmark in the box to enable access to the ENVIROMUX via SSH
Enabe HTTP access	Place a checkmark in the box to enable access to the ENVIROMUX via standard (non-secure) HTTP requests. **Don't disable until you read the first two notes below.**
HTTP Port	Port to be used for standard HTTP requests
HTTPS Port	Port to be used for HTTPS requests
Web Timeout	Number of minutes after which idle web uses will be logged-out (enter 0 to disable this feature)
Enable Network Security	Place a checkmark in the box to disable ICMP responses and limit TLS to only secure ciphers.

Note: When using only a secure access configuration ("Enable HTTP Access" is NOT checked), if you intend to connect to the ENVIROMUX from a location outside the local area network, make sure the firewall on the local area network is configured to allow traffic through the port assigned to HTTPS requests.

Note: If you are installing the ENVIROMUX with a public IP address and intend to use only a secure access configuration, you will need to create an x.509 certificate (page 124) and load it into the ENVIROMUX and any PC that will be required to access the ENVIROMUX.

If the administrator chooses to have the IP and DNS information filled in automatically via DHCP, the SMTP server and port number still need to be entered for email alerts to work. If the SMTP server requires a password in order for users to send emails, the network administrator must first assign a user name and password to the ENVIROMUX.

Note: The SMTP server port number is shown in Figure 40 as "25". This is a common port number assigned, but not necessarily the port number assigned to your SMTP server. For SMTP servers that support SSL, the common port number is 465, and for those that support TLS, the common port number is 587.

The administrator may assign a different HTTP Server Port than is used by most servers (80).

Note: If the port number is changed and forgotten, to determine what it has been changed to connect the ENVIROMUX for control using the text menu (page 66) and review the Miscellaneous Service Settings (page 89).

Read-Only Community Name

The SNMP Read-only community name enables a user to retrieve "read-only" information from the ENVIROMUX using the SNMP browser and MIB file. This name must be present in the ENVIROMUX and in the proper field in the SNMP browser.

Read-Write Community Name

(not applicable as of this printing)

The SNMP Read-Write community name enables a user to read information from the ENVIROMUX and to modify settings on the ENVIROMUX using the SNMP browser and MIB file. This name must be present in the ENVIROMUX and in the proper field in the SNMP browser.

User Configuration

The Users page is a list of all configured users of the ENVIROMUX. A maximum of 15 users (other than root) can be configured.

From this page the user can choose to add more users, go to the user configuration page to edit a user's access to the ENVIROMUX, or delete a user from the list. To view the Users page, click on **Users** from the **Administration** section of the menu.

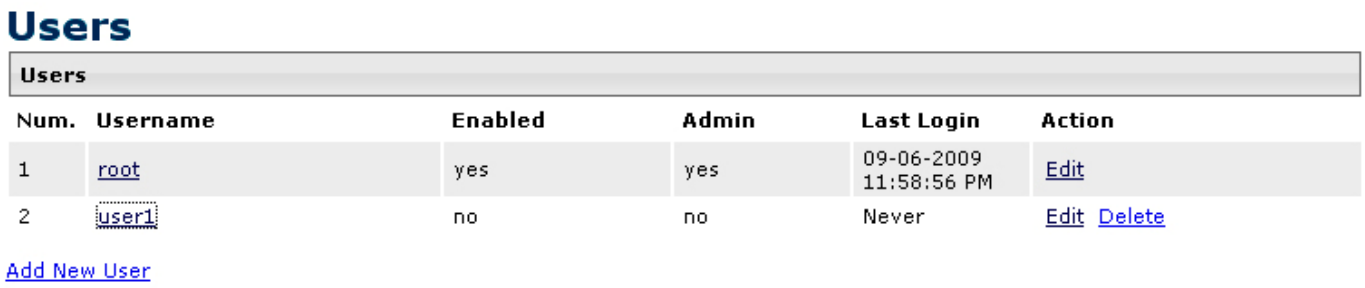


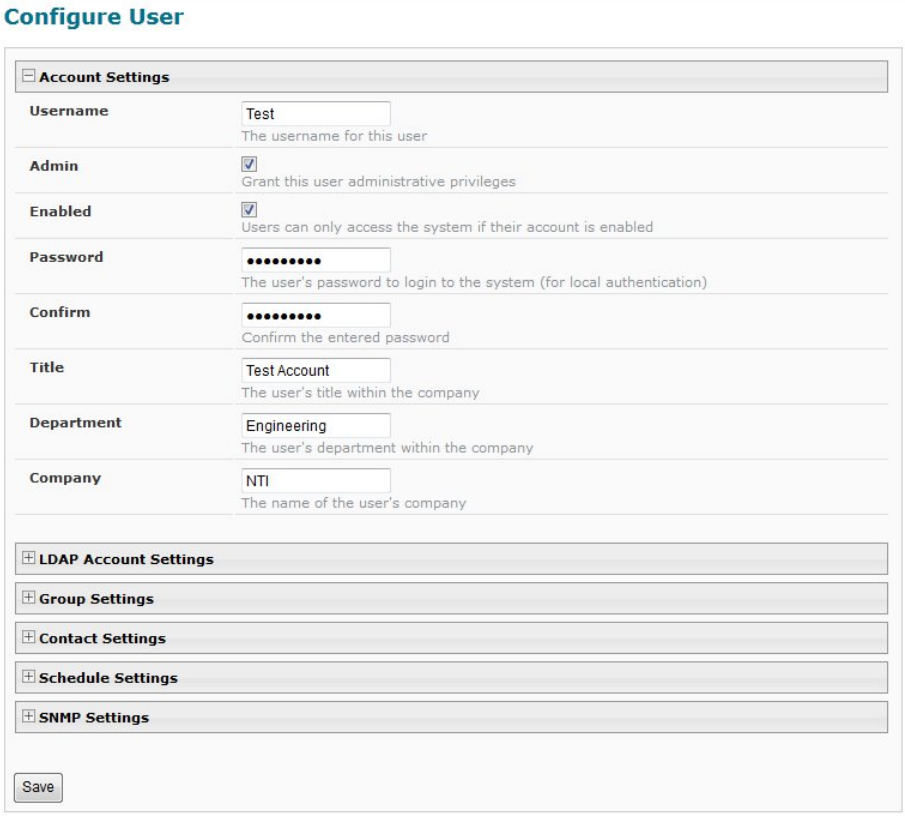
Figure 41- Users page

To add a user, click on the "Add New User" link.

To edit a user's configuration, either click on the listed username, or on the "Edit" link.

To delete a user and their configuration, click on "Delete" link.

When adding a new user, the Configure User page will open with the username "user*x*" assigned, where x = the next consecutive number (up to 15) based on the quantity of users in the list (other than the root user). You can either leave the name as "userx", or change it to what you would like to see listed. With the name assigned, fill in the remaining information as needed.



If the password for user "root" is changed from "nti", and you lose or forget what it is, you will need to return the ENVIROMUX to NTI to have default settings restored. Contact NTI for an RMA to return the ENVIROMUX.

Figure 42- Configure Users page

LDAP Account Settings

Common Name (for LDAP)	Test Account The Common Name for the user in an Active Directory
Organizational Unit (for LDAP)	Eng,BldgC The Organizational Unit the user belongs to in an Active Directory

Group Settings

Group 1	☐ User receives notifications for Group 1
Group 2	☐ User receives notifications for Group 2
Group 3	☐ User receives notifications for Group 3
Group 4	☐ User receives notifications for Group 4
Group 5	☐ User receives notifications for Group 5
Group 6	☐ User receives notifications for Group 6
Group 7	☐ User receives notifications for Group 7
Group 8	☐ User receives notifications for Group 8

Contact Settings

E-mail Alerts	☐ User receives alerts via e-mail
E-mail Address	E-mail address for the user
Syslog Alerts	☐ User receives alerts via syslog
SNMP Traps	☐ User receives alerts via SNMP traps
Syslog/SNMP IP Address	IP address where syslog messages/SNMP traps are sent for this user
SMS Alerts	☐ User receives alerts via SMS
SMS Number	Phone number where SMS messagess are sent for this user

Schedule Settings

Schedule Type	Always active Configure the user's schedule type
Start Day	Sun First day of the week when the user active
End Day	Sun Last day of the week when the user active
Start Hour	00:00 Starting hour for the user's daily schedule
End Hour	00:00 Ending hour for the user's daily schedule

Figure 43- Configure User- more options

Account Settings	Description
Username	Enter the desired username for this user
Admin	Place a checkmark here if this user should have administrative privileges
Enabled	Place a checkmark here to enable this user to access the ENVIROMUX
Password	Enter a password that a user must use to login to the system **A password must be assigned for the user's login to be valid** **Passwords must be at least 1 keyboard character.**
Confirm	Re-enter a password that a user must use to login to the system
Title	Enter information as applicable
Department	Enter information as applicable
Company	Enter information as applicable
LDAP Account Settings	
Common Name (for LDAP)	"Common Name" assigned in the LDAP server account in an Active Directory. Often a name assigned that is different than the Username. If this is the same as the Username in the "Account Settings" (above), this can be left blank.
Organizational Unit (for LDAP)	Enter the Organizational Unit the user belongs to in an Active Directory Format is <ou,ou,etc> (like example in Figure 43)
Group Settings	
Group 1-8	Place a checkmark if the user should receive messages from sensors, accessories, or IP devices in Group 1, 2, 3… thru 8 (see also pages 29 and 33 for group assignments)
Contact Settings	
Email alerts	Place a checkmark if the user should receive messages via email
Email address	Enter a valid email address if this user should receive email alert messages **Tip:** The user can receive alert messages to their cell phone (SMS) by entering the cell carrier's email address here (i.e. 1234567890@vtext.com for Verizon) in the absence of a modem.
Syslog alerts	Place a checkmark if the user should receive alerts via syslog messages
SNMP traps	Place a checkmark if the user should receive alerts via SNMP traps
Syslog/SNMP IP address	Enter a valid syslog/SNMP IP address for the user to receive syslog/SNMP messages
SMS Alerts	Place a checkmark if the user should receive alerts via SMS messages (requires a modem)
SMS Number	Enter a phone number to call to alert the user via SMS message **Note:** Use all numbers for this entry (i.e. for international numbers, enter 00 (EU), or 011 (US), not a plus (+) sign)
Schedule Settings	
Schedule Type	**Always active**- user will receive messages at all hours of each day **Active during defined times**- user will only receive alert messages during times as outlined below
Start Day	First day of the week the user should begin receiving messages
End Day	Last day of the week the user should receive messages
Start Hour	First hour of the day the user should begin receiving messages
End Hour	Last hour of the day the user should receive messages

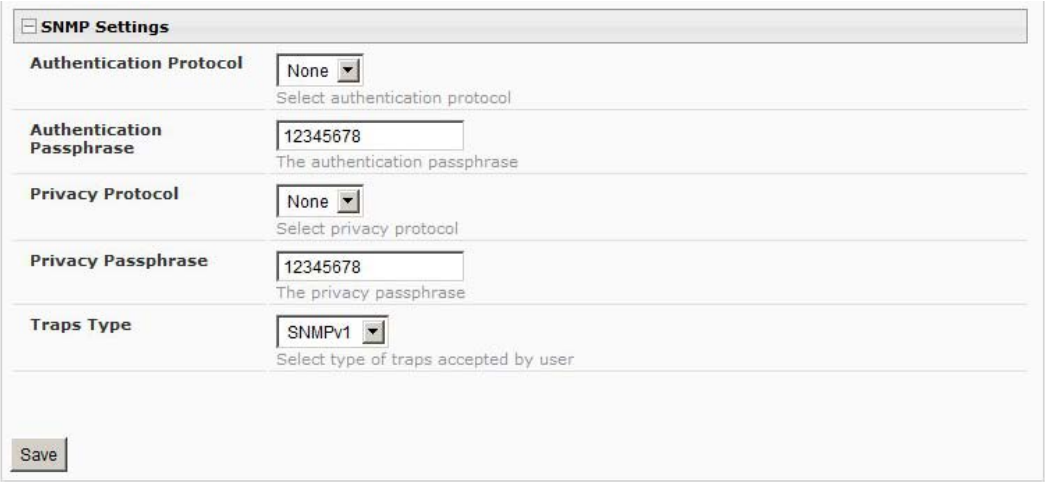


Figure 44- Configure User- SNMP Settings

SNMP Settings	
Authentication Protocol	Choose between MD5 or SHA to require authentication, or none to disable it
Authentication Passphrase	Assign the passphrase to be used to enable the receipt of SNMP v3 messages
Privacy Protocol	Choose between DES or AES to encrypt SNMP readings or traps or none to disable encryption. If encryption is enabled, then the Authentication Protocol must also be set at “MD5” or “SHA”.
Privacy Passphrase	Assign the passphrase to be used to open and read readings or alert messages received via SNMP v3
Traps Type	Choose between SNMPv1, SNMPv2C, or SNMPv3

After changing any settings in the user profile, press “Apply”.

More about User Privileges

The root user (or any user with administrator rights) can change the root password and configure how the root user will receive alert messages. Users with administrative rights can change all configuration settings except for the root user name.

Users with user rights can only see the current readings of monitored items and change their own passwords.

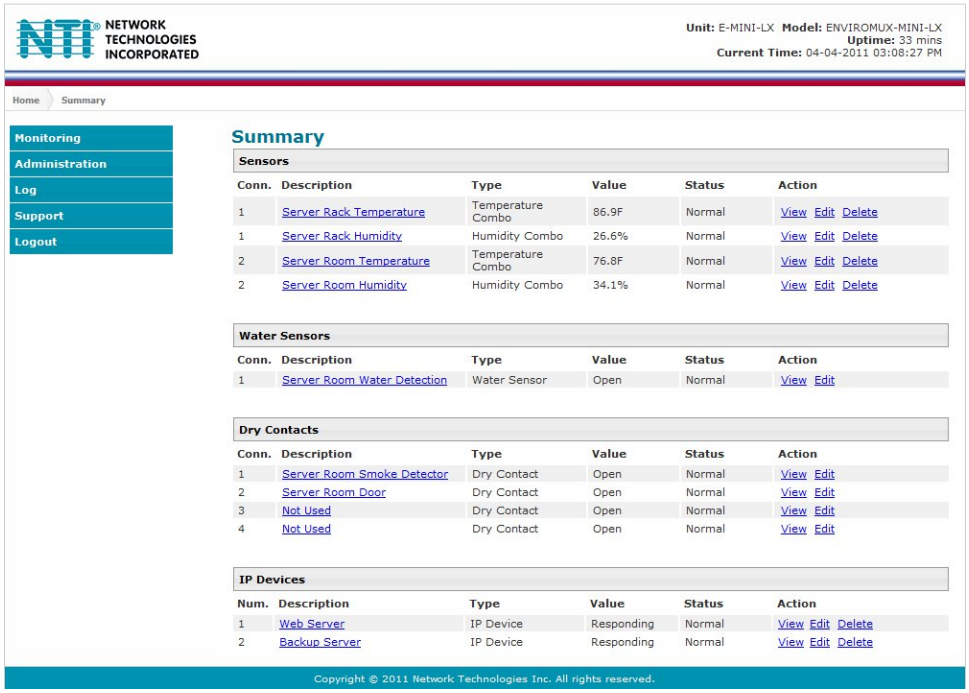


Figure 45-Summary page for User without Admin privileges

Security

Security in the ENVIROMUX can be managed one of two ways; through the local settings (passwords assigned in user settings on page 46) or through an LDAP server. If security is configured to use LDAP mode, then the passwords for users must be those found on a configured LDAP server. To view the Security Configuration page, select **Security** in the **Administration** section of the menu.

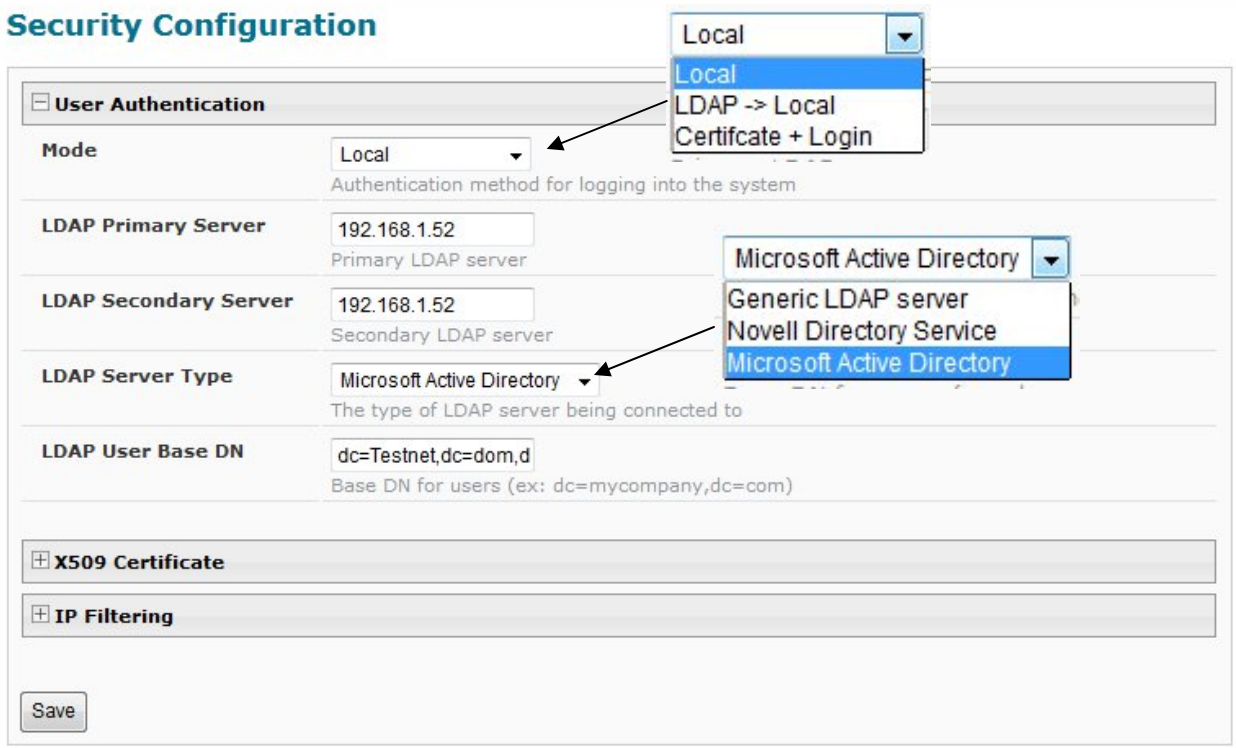


Figure 46- Security Configuration page

When in LDAP mode, Usernames (and Common name, if different from Username) on the LDAP server must match those in the user settings of the ENVIROMUX (page 44) or access will be denied.

Note: When in LDAP mode, if the LDAP server is not responding, local authentication will be tried.

User Authentication	
Mode	Select Local to use authentication based on passwords in the ENVIROMUX user configuration Select LDAP to use authentication based on passwords in an LDAP server Select "Certificate+Login" when authentication requires the connecting PC to hold a valid certificate
LDAP Primary Server	Enter Hostname or IP address of Primary LDAP Server
LDAP Secondary Server	Enter Hostname or IP address of Secondary LDAP Server (optional)
LDAP Server Type	Choose from drop down list: Generic LDAP server Novell Directory service Microsoft Active Directory
LDAP User Base DN	Enter the Base DN for users (ex: dc=mycompany,dc=com)

Even though LDAP authentication is being used, each user must also have a local account within the ENVIROMUX. User permission level is established by the local account (page 44).

X509 Certificate

The ENVIROMUX 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 ENVIROMUX. The Server certificate and key must be combined in a single file ("PEM" format). For instruction to create your own certificate, see page 124.

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 Client Authentication

In addition to Local and LDAP client authentication, X509 client authentication is also available. In order to use X509 client certificate authentication, select "**Certificate + Login**" for the mode setting (Figure 46). X509 client certificate authentication requires the user to present client certification (this happens behind the scenes when you enter the https IP address, before you are presented with a "Login" screen). For this to work:

1. A client certificate signed by a Certifying Authority (CA) must be loaded into the user's browser.
2. Use "**Choose File**" and browse to the CA certificate (file with ".crt" extension) and select it.
3. Click on the "**Upload CA certificate**" button and load the CA certificate to the ENVIROMUX.

Note: The user will need to login after the X509 client certificate is validated.

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

Whether you are just loading your own Server Certificate, or also using client authentication, **reboot the ENVIROMUX for this certificate to take effect.**

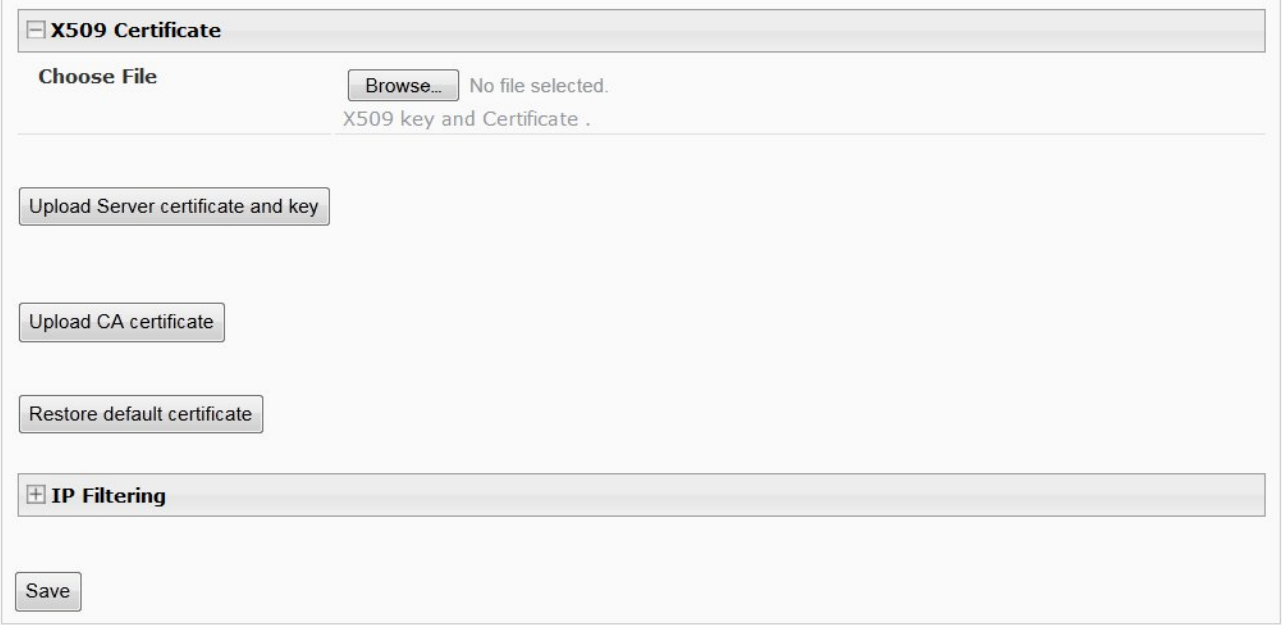


Figure 47- Security Configuration-x509 Certificate

Note: HTTP access can be enabled/disabled from web page under Administration -> Network -> Server Settings -> Enable HTTP (page 43). Do not disable http access until you verify certificate verification works properly for https connection. HTTP connection will allow you to change any settings if a wrong certificate is uploaded. Once HTTPS client certificate validation is verified to be working properly, disable HTTP access for security.

IP Filtering

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

Up to 16 IP Filtering rules can be defined to protect the ENVIROMUX 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.

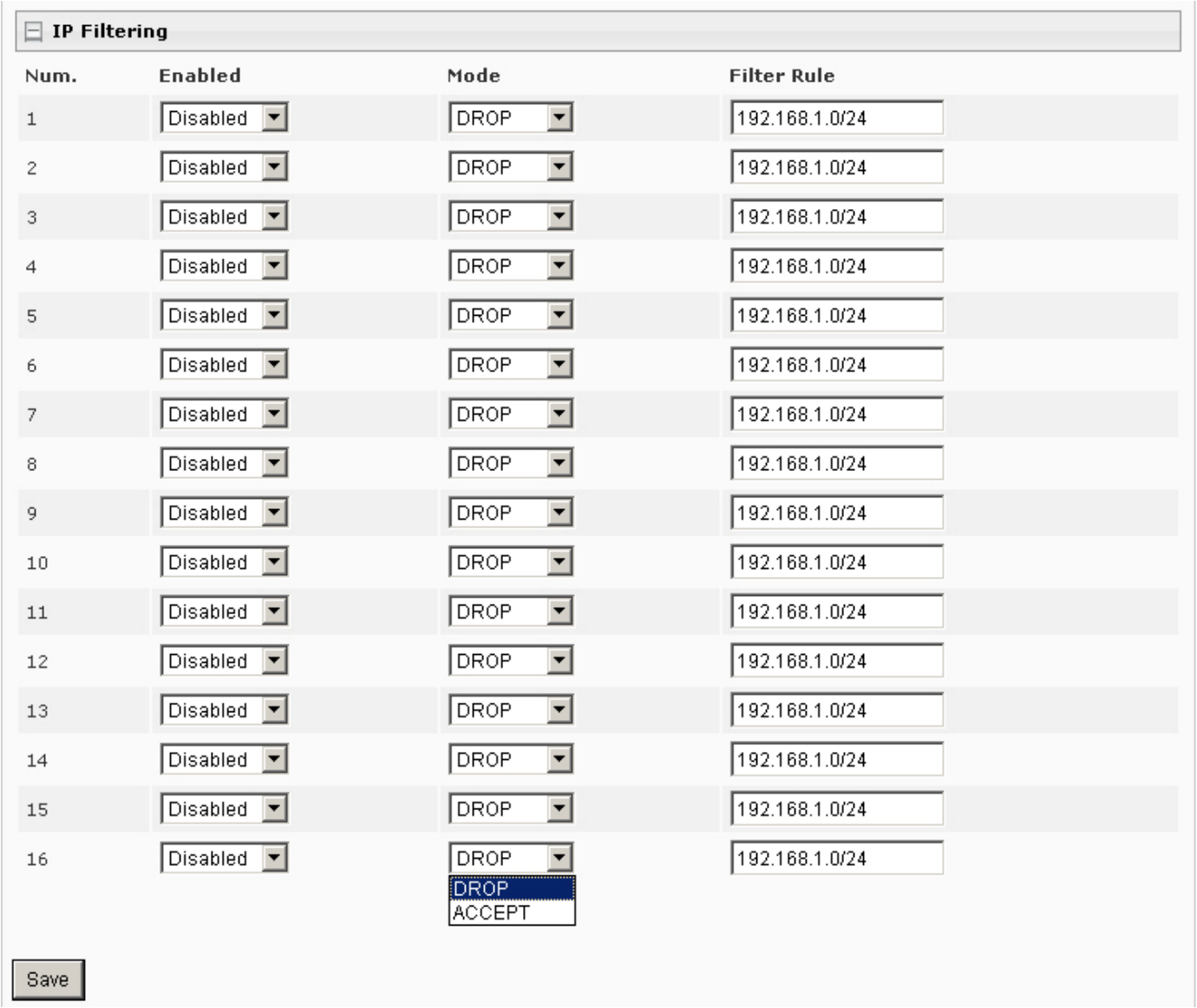


Figure 48- Security Configuration- IP Filtering Rules

More on IP Filtering

The most common approach is to only allow “white-listed” 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:

1	Enabled	ACCEPT	192.168.1.100

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

16	Enabled	DROP	0.0.0.0/0

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).

System Information

The system information page displays the model name of the ENVIROMUX, the firmware version in the ENVIROMUX, the MAC address of the Ethernet port, the IP mode, and the network configuration. To view the System Information, select **System Information** in the **Administration** section of the main menu.

System Information

System Information

Product:	ENVIROMUX-MINI-LX Mini Server Environment Monitoring System
Revision:	1.0
Build Date:	09-27-2011 01:21:22 PM
MAC Address:	00:0C:82:0B:00:03
IP Mode:	Static
IP Address:	192.168.3.85
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.3.3
Primary DNS:	166.102.165.11
Secondary DNS:	166.102.165.13
SNMPv3 Engine ID:	0x80001F8803000C820B0003

Figure 49- System Information page

Update Firmware

The Update Firmware page is used to change the firmware of the ENVIROMUX. 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/download/d-environment-monitoring.html). To view the Update Firmware page, select **Firmware** in the **Administration** section of the main menu. Once a user has downloaded the required file for firmware upgrade, this page will be used to upload it to the ENVIROMUX.

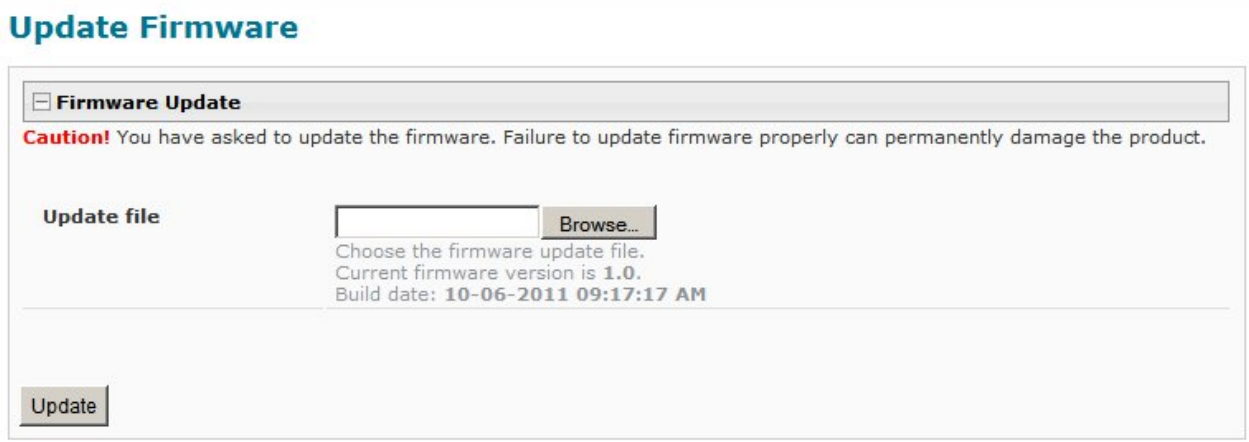


Figure 50- Update Firmware page

1. Download the most current firmware file from http://www.networktechinc.com/download/d-environment-monitoring.html to a location on your PC.
2. Click on the "Browse" button and locate and select the firmware file for the ENVIROMUX (***E-MINI-lxo-vx-x.bin, for example***).
3. Click on the "Update" button to perform the firmware update. The firmware update process will take approximately 5 minutes while the ENVIROMUX installs the firmware. Once the update file has been installed, the unit will automatically reboot and the login screen will appear.

Reboot the System

The ENVIROMUX can be remotely rebooted by anyone with administrative privileges. To view the Reboot System page, select **Reboot** in the **Administration** section of the main menu. Click the **Reboot Now** button to cause the ENVIROMUX to reboot. This will disconnect any user and shut down all activity.

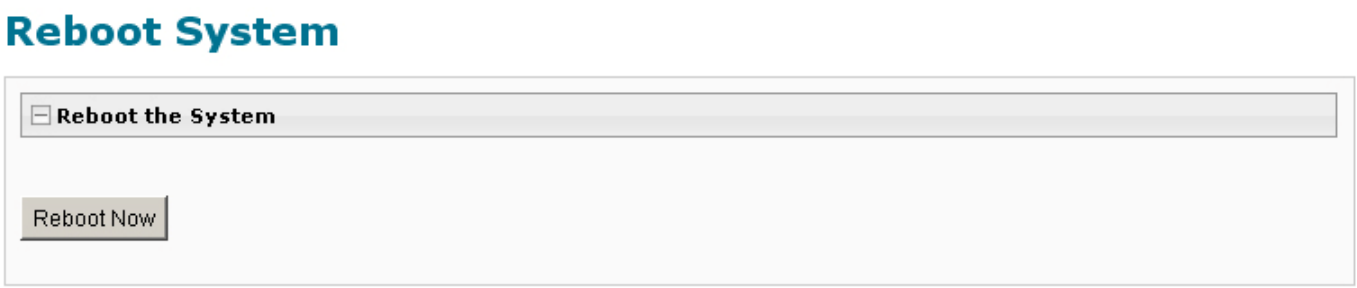


Figure 51- Reboot System page

The message "System is rebooting, please wait..... " will appear and after approximately 45 seconds the login screen will appear. Log in to resume activity.

Figure 52- System is rebooting

Smart Alerts

Smart Alerts enable the ENVIROMUX to contact users when specially configured circumstances exist for defined sensors. Smart Alerts will respond to 1 or more alert conditions independent of the alert configurations for each sensor configured on page 27.

Assorted conditions can produce configurable events that can then be used in numerous scenarios to produce Smart Alert messages that are sent to users.

To begin, Events must be defined and configured. Events are sensor conditions to be notified of. Events logged based on the sensor configurations described on page 27 will be managed separately from events logged by these pre-defined Events. Sensor configuration for these Events will have no impact on the general configuration of your sensors. Pre-defined Events provide more control over what you want to be notified of.

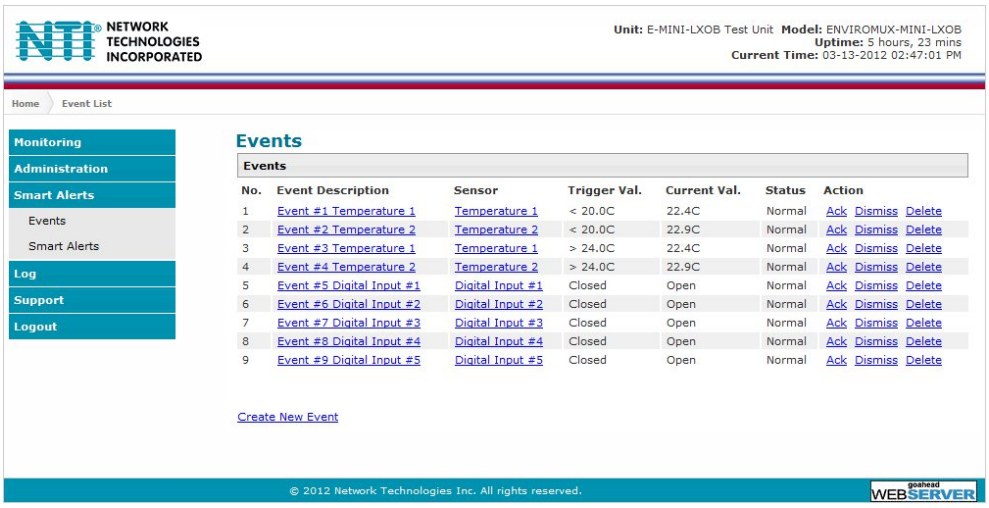


Figure 53- Events used for Smart Alerts

From the side menu, select “Smart Alerts”, and “Events”. On the Events page, click on “Create New Event”.

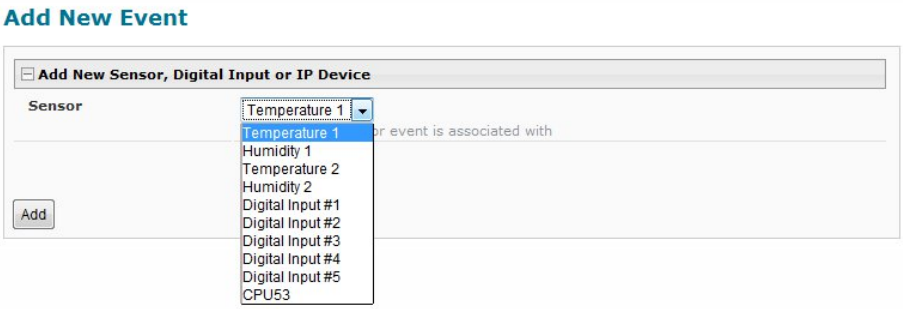


Figure 54- Sensor to be used for a predefined event

You will be prompted to select which connected sensor to associate the event with. Which sensor’s data do you want to trigger this event? Once selected, click “Add”.

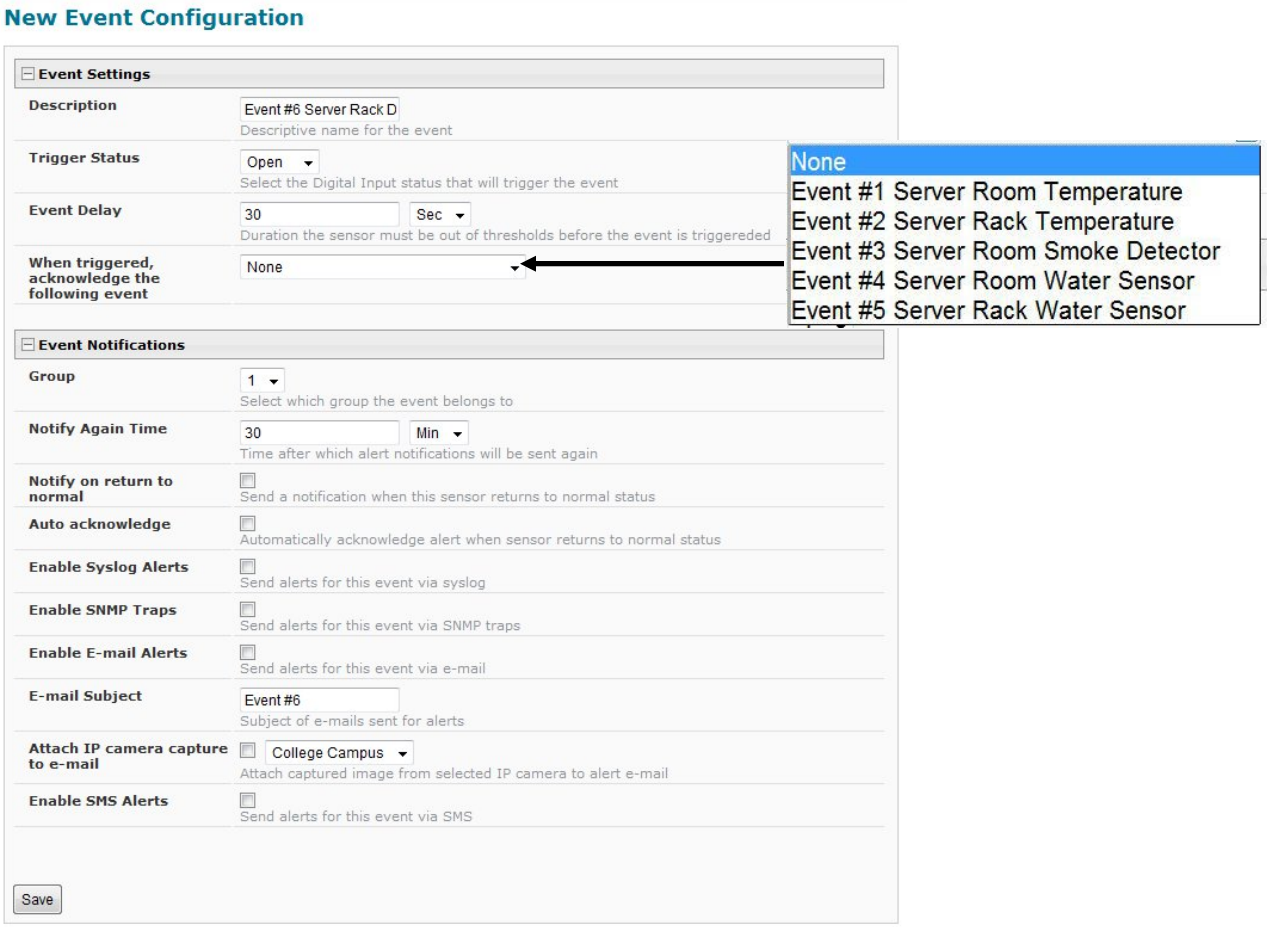


Figure 55- Configuration options for new event

Depending upon the type of sensor chosen, various event settings can be configured that will cause an event to be logged.

In the example above, if the temperature sensor sees a temperature greater than 75.0 degrees C for more than 30 seconds, and event will be logged.

Event Notifications can then be configured to be sent, with the options described in the following table.

Event Settings	
Description	The description of the sensor that will be viewed in the Summary page and in the body of alert messages
Threshold (for RJ45 sensors)	The threshold value of the measured unit that will trigger an event ***Note: The trigger value can be a value that is considered a sensor's "normal" state, or its "alert" state.***
Threshold Type	The type of variation from the threshold value that indicates a condition (greater than or less than)
Trigger Status (for digital inputs)	The condition of the sensor that indicates a triggered state (open or closed)
Event Delay	The amount of time the event must be triggered before an event is logged. This provides some protection against false alarms. The Event Delay value can be set for 0-999 seconds or minutes.
When triggered, acknowledge the following event	Selecting an event for this field gives the option to cancel notice of another separate event (acknowledge) when current event is triggered
Event Notification Settings	
Group	Assign the Event to any group 1 -8 (see also page 44)
Notify Again Time	Enter the amount of time in seconds, minutes, or hours (1-999) before an alert message will be repeated
Notify on Return to Normal	The user can also be notified when the Event has returned to a non-triggered state by selecting the "***Notify when return to normal***" box for an Event.

Event Notification Settings (Continued)	
Auto Acknowledge	Place a checkmark in this box to have alert notifications in the summary page return to normal state automatically when an Event is no longer being triggered.
Enable Syslog Alerts	Place a checkmark in this box to have alert notifications sent via Syslog messages
Enable SNMP traps	Place a checkmark in this box to have alert notifications sent via SNMP traps (v2c)
Enable Email Alerts	Place a checkmark in this box to have alert notifications sent via Email
Email Subject	Enter the subject to be viewed when an email alert message is received
Attach IP Camera capture to email	Associate an Event with an IP camera. Select an IP camera from the drop-down box. An image will be captured and sent with the alert message when an alert is sent via e-mail. IP cameras that are monitored by the ENVIROMUX (page 36) will be available for this purpose. ***Note: To be able to send IP camera captures as e-mail attachments, viewer security (in your camera's configuration) needs to be disabled. Consult your IP camera manual to see if this feature is present and for instructions on how to do this.***
Enable SMS Alerts	Place a checkmark in this box to have alert notifications sent via SMS messages (requires a modem)

After all options are selected, click the "Save" button. This Event will now be added to the Events page (Figure 53). Up to 50 events can be defined. Events can be configured to trigger alerts by themselves, and/or be used in combination with other events to trigger Smart Alerts.

With Events defined, Smart Alerts (up to 20) can be configured to use Event combinations to send alert messages.

Figure 56- Smart Alert summary page

From the side menu, select "Smart Alerts", and "Smart Alerts" again. On the Smart Alerts page, click on "Add New Smart Alert". A new numbered Smart Alert will be added to the summary page (above). To configure the Smart Alert, click on it.

A menu will open with many options to choose to make the best use of the information provided by the events.

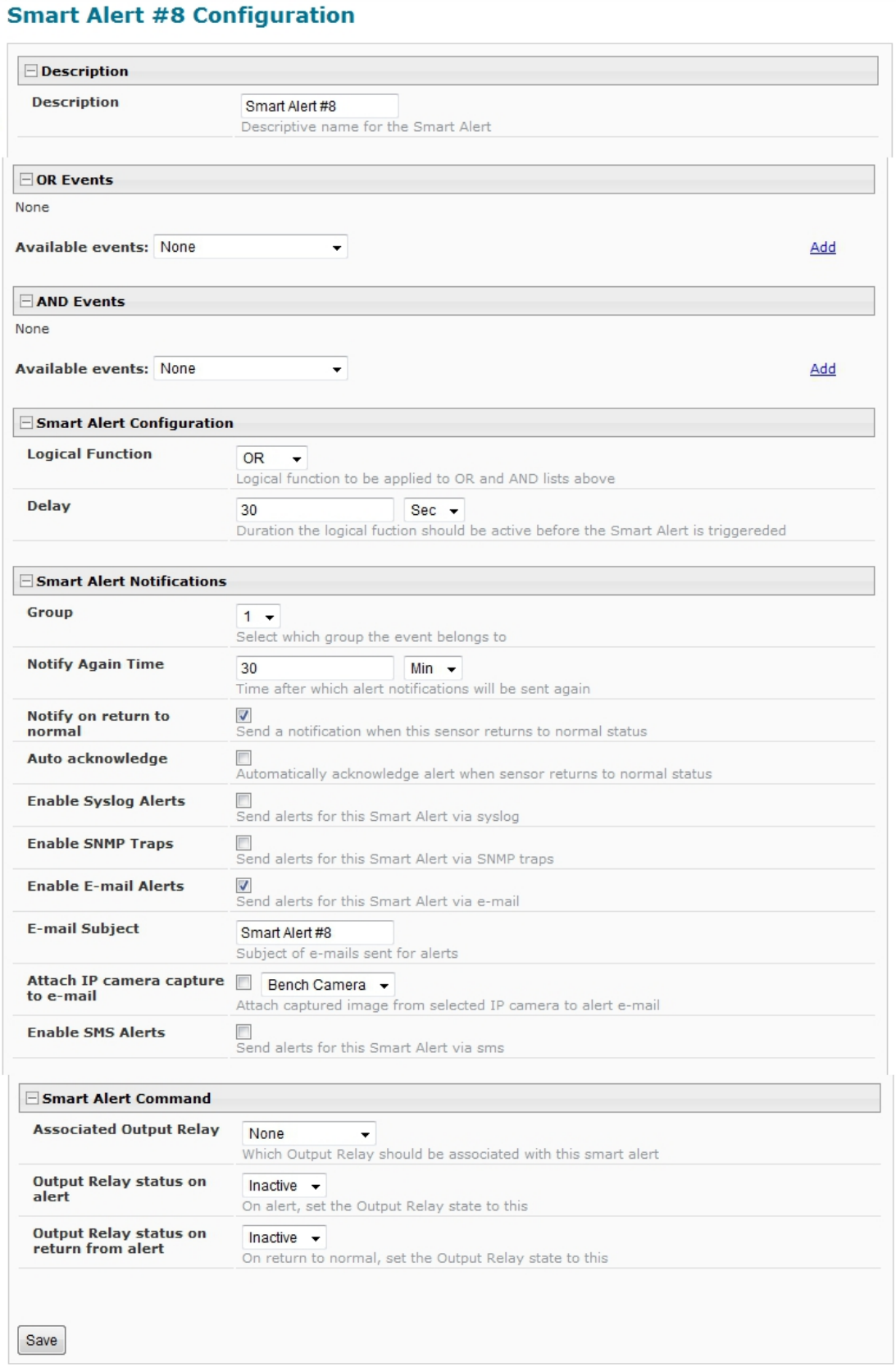


Figure 57- Smart Alert configuration

DESCRIPTION	
Description	Use the default description provided or enter the description you want to see on notifications received.
OR Events	
Available Events	Select from the predefined available Events (Figure 53) to have OR logic applied to a triggered Event
AND Events	
Available Events	Select from the predefined available Events (Figure 53) to have AND logic applied to a triggered Event
Smart Alert Configuration	
Logical Function	Logical function to be applied to the output of the logical status of the OR and AND lists to determine when a Smart Alert should be generated. Options include OR, AND, XOR, NOR and NAND
Delay	The amount of time the Smart Alert Event status must be in an alert condition before a Smart Alert message is triggered. This provides some protection against false alarms. The Delay value can be set for 0-999 seconds or minutes.
Smart Alert Notifications	
Group	Assign the Smart Alert to any group 1 -8 (see also page 44)
Notify Again Time	Enter the amount of time in seconds, minutes, or hours (1-999) before an alert message will be repeated
Notify on Return to Normal	The user can also be notified when the Smart Alert conditions have returned to the normal (non-triggered state) by selecting the "***Notify when return to normal***" box.
Auto Acknowledge	Place a checkmark in this box to have alert notifications in the summary page return to normal state automatically when Smart Alert conditions return to normal.
Enable Syslog Alerts	Place a checkmark in this box to have alert notifications sent via Syslog messages
Enable SNMP traps	Place a checkmark in this box to have alert notifications sent via SNMP traps (v2c)
Enable Email Alerts	Place a checkmark in this box to have alert notifications sent via Email
Email Subject	Enter the subject to be viewed when an email alert message is received
Attach IP Camera capture to email	Associate a Smart Alert with an IP camera. Select an IP camera from the drop-down box. An image will be captured and sent with the alert message when an alert is sent via e-mail. IP cameras that are monitored by the ENVIROMUX (page 36) will be available for this purpose. ***Note: To be able to send IP camera captures as e-mail attachments, viewer security (in your camera's configuration) needs to be disabled. Consult your IP camera manual to see if this feature is present and for instructions on how to do this.***
Enable SMS Alerts	Place a checkmark in this box to have alert notifications sent via SMS messages (requires a modem)
Smart Alert Command	
Associated Output Relay	Associate the Smart Alert with the operation of the output relay, or not ***Note: Only one sensor or Smart Alert should be associated with the Output Relay at a time. Contradicting commands from two or more sensors or Smart Alerts will result in the output relay responding to the state directed by the last command received.***
Output Relay Status on Alert	State the output relay will be in when a Smart Alert is triggered
Output Relay Status on Return from Alert	State the output relay will be in when a Smart Alert is no longer being triggered

More on Logical Functions

Using Logical Functions, you can select how to use or not use the reported state of an Event. You can combine the information from multiple Events to achieve an end result.

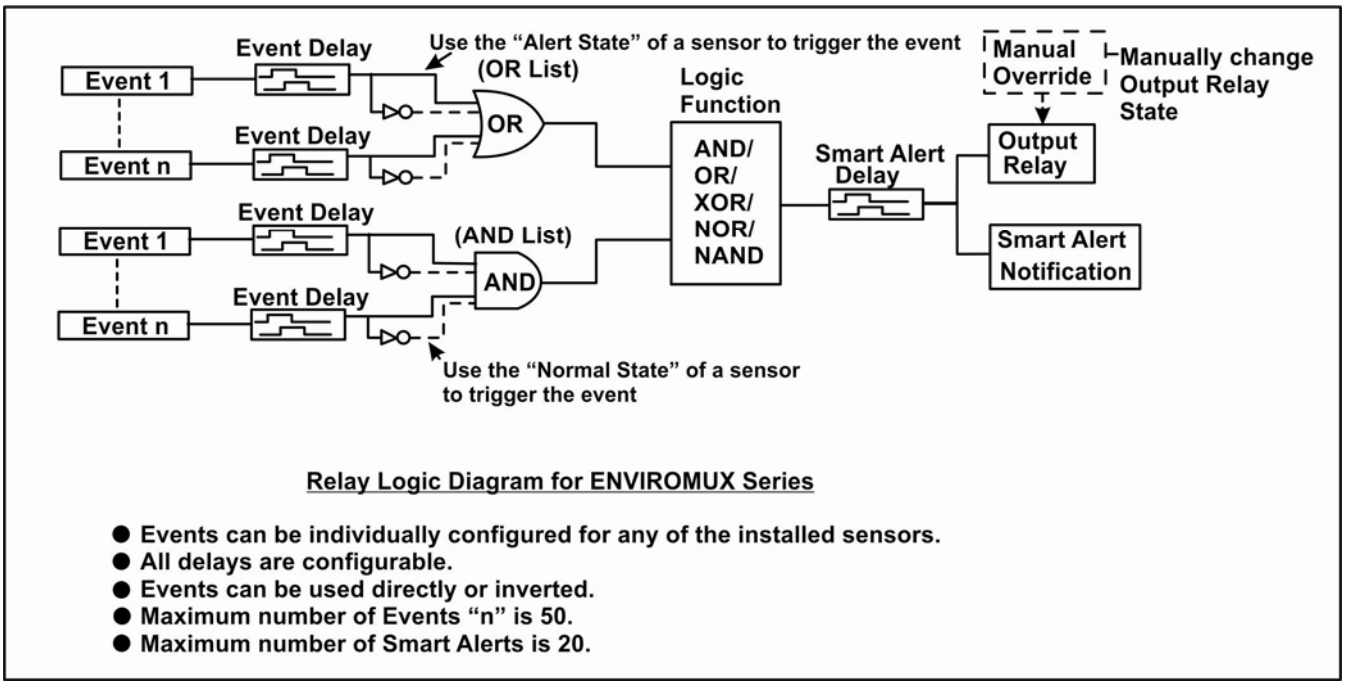


Figure 58- Event Logical Function Diagram

Smart Alert Rules:

- Any configured Event can be applied to either the OR Events list or the AND Events list, or both lists.
- Events can be configured to be triggered by a sensor or monitored device in alert state or in normal state.
- Each list will generate an output value, the value to either send an alert (1), or not (0).

  - If **any** Event in the OR list is triggered, the output value of the OR list will be 1.

  - **All** Events in the AND list must be triggered for the output value of the AND list to be 1.

The Logical Function combines the two values to determine if a Smart Alert should be sent, as detailed in the table below:

OR List	AND List	Logical Function	Smart Alert Generated
0	0	OR	No
1	0		Yes
0	1		Yes
1	1		Yes
0	0	XOR	No
1	0		Yes
0	1		Yes
1	1		No
0	0	AND	No
1	0		No
0	1		No
1	1		Yes

OR List	AND List	Logical Function	Smart Alert Generated
0	0	NOR	Yes
1	0		No
0	1		No
1	1		No
0	0	NAND	Yes
1	0		Yes
0	1		Yes
1	1		No

Example: If the OR list value is at 0, and AND list value is at 0, when the Logical Function is set to OR a Smart Alert will NOT be generated.

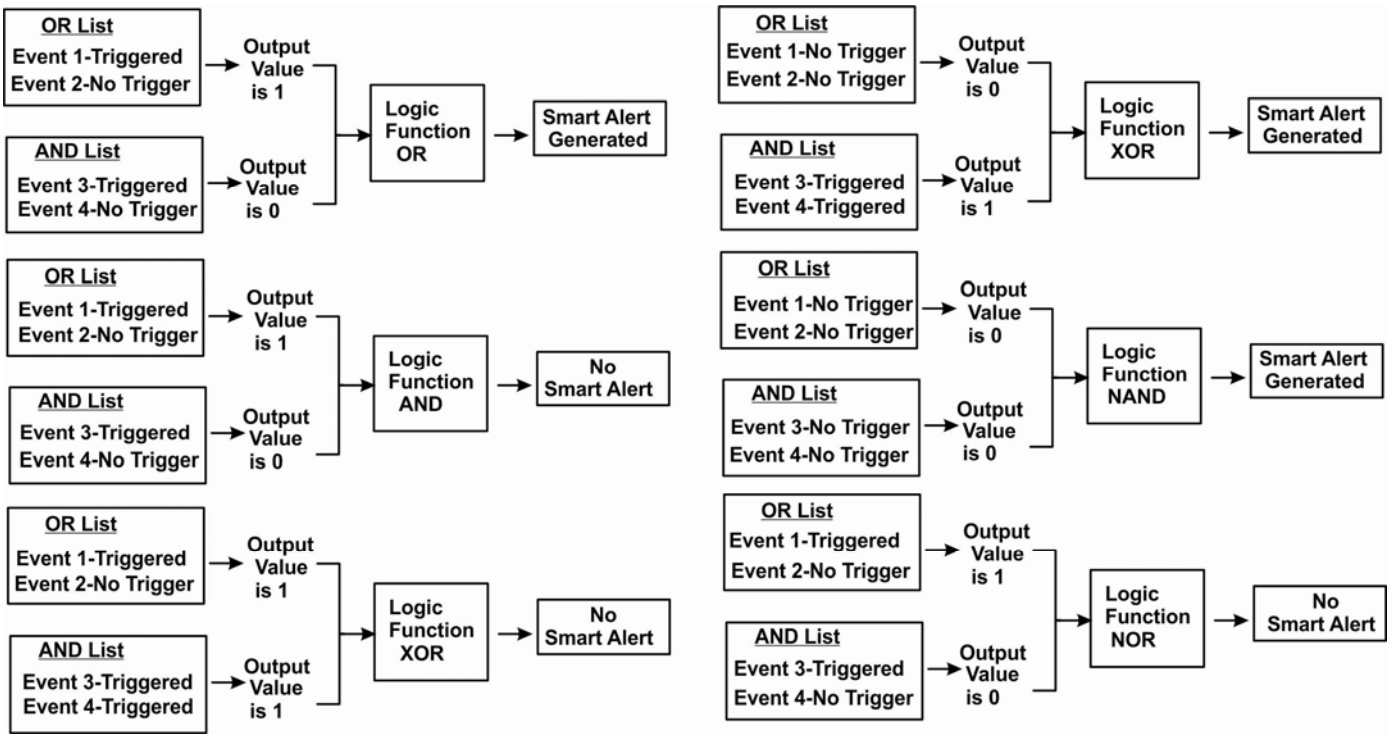
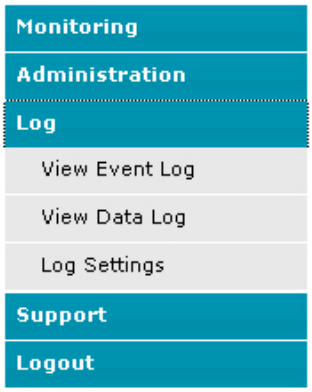


Figure 59- Examples of Smart Alert conditions

Log

From the Log section there are three sub sections for configuring the ENVIROMUX:



View Event Log	View a log listing the date and time of events such as startups, shut downs, user logins
View Data Log	View data readings from sensors and IP addresses
Log Settings	Configure how the logs are sent to users, how they handle reaching capacity, which users will be notified that it has reached capacity, and how they will be notified

View Event Log

The Event Log provides the administrative user with a listing of many events that occur within the ENVIROMUX. The event log will record the date and time of:

- each ENVIROMUX startup,
- each user login and logout time,
- any time an unknown user tries to login,
- sensor and IP device alerts
- an alert handled by a user

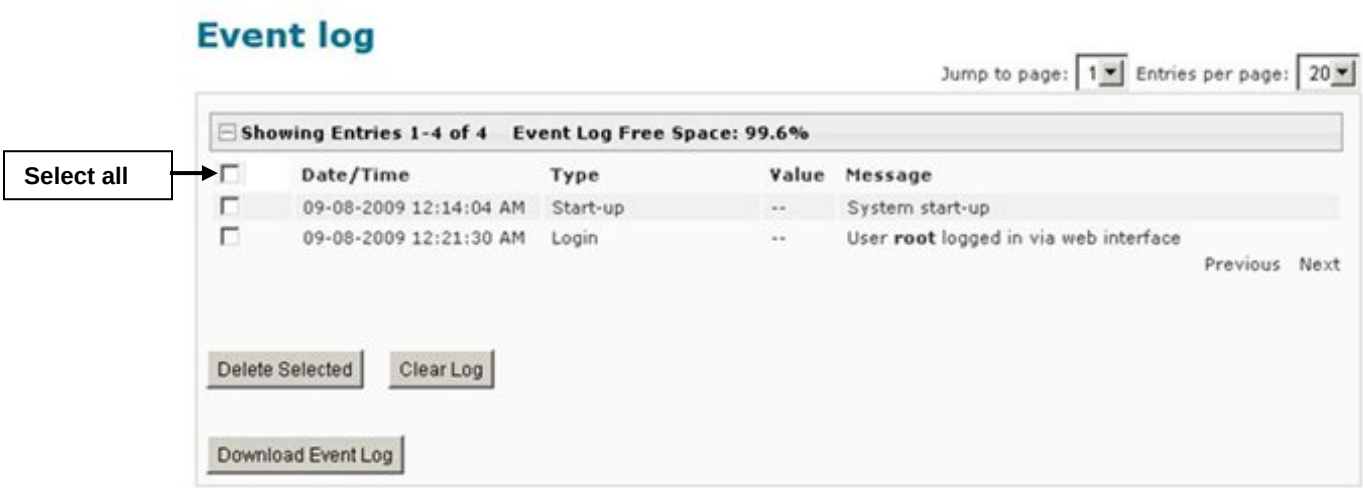


Figure 60- Event Log page

From the Event Log page the administrative user can view the logs, select specific logs to be deleted or press **Clear Log** to delete them all. The number of entries per page can be changed for the user's reading preference. Navigating between pages is as easy as clicking **Previous** or **Next** buttons, or jumping to a specific page if you know where the log entry you are interested in is listed.

To clear only specific log entries, place a checkmark in each line item to be deleted, and press **Delete Selected**. To select all entries at once, place a checkmark in the uppermost box. Before deleting, the user may want to save the log for future reference and to make space for more logs by downloading the event log to a file on a PC. Press **Download Event Log** to save the log file before clearing it.

View Data Log

The Data Log provides the administrative user with a listing of all the readings taken by the ENVIROMUX pertaining to the sensors and IP Devices being monitored. The event log will record the date and time of each reading.

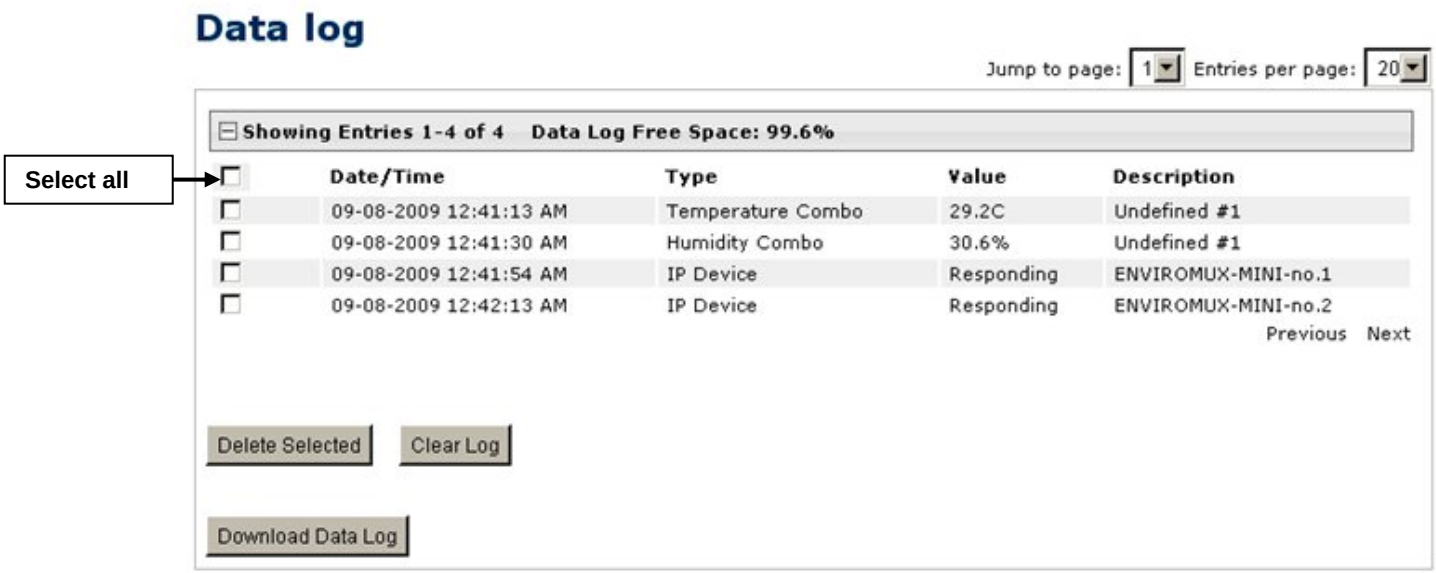


Figure 61- Data Log page

From the Data Log page the administrative user can view the logs, select specific logs to be deleted or press **Clear Log** to delete them all. The number of entries per page can be changed for the user's reading preference. Navigating between pages is as easy as clicking **Previous** or **Next** buttons, or jumping to a specific page if you know where the log entry you are interested in is listed.

To clear only specific log entries, place a checkmark in each line item to be deleted, and press **Delete Selected**. To select all entries at once, place a checkmark in the uppermost box. Before deleting, the user may want to save the log for future reference and to make space for more logs by downloading the event log to a file on a PC. Press **Download Data Log** to save the log file before clearing it.

Log Settings

The Log Settings page (Figure 62) provides settings for how the ENVIROMUX will react when its Data and Event logs reach capacity.

The Event Log settings include a logging level that can be configured to log different amounts of information:

- Error : shows only system errors (like sending e-mail failures or SMS)
- Alerts: shows recorded system errors and alert messages
- Info: In addition to all of the above, the log will show less relevant information: user login/logout for example

Each log can be assigned to a group and any user that receives messages from that group can be notified when capacity is being reached.

The log can be set to either :

- Discontinue- stop logging information
- Clear and restart- delete all log entries and restart with new entries
- Wrap- continue logging but delete the oldest entries so new ones can be recorded

The Data and/or Event log can be set to send alerts to users via email, syslog, and/or SNMP traps once it has reached 90% of capacity, allowing them time to react.

The Data log can also be set to send log entries via email, syslog, or SNMP traps to users in addition to the entries it records internally. Enable Remote Logging for email, syslog, of SNMP as desired.

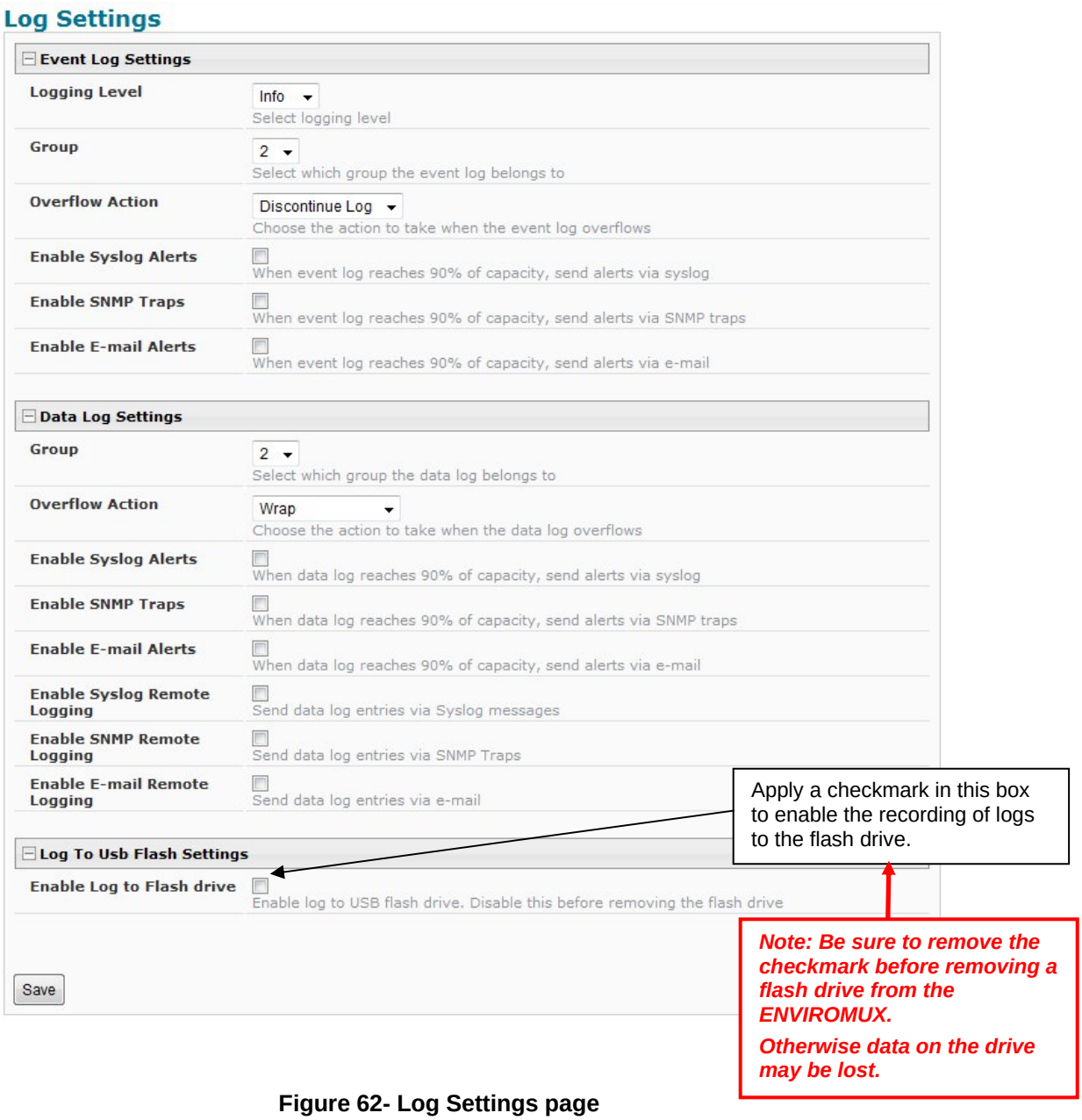


Figure 62- Log Settings page

Log to USB Flash Settings

Event and Data log messages are automatically sent to users as configured above in addition to being recorded in the logs. The logs can also be downloaded as a tab-delimited plain text file. If a USB flash drive is present, logs will also be recorded on the flash drive to make them portable provided the feature is enabled.

The number of logs that can be recorded depends on the capacity of the flash drive installed. To begin recording to the flash drive, place a checkmark in the “Enable Log to Flash drive” box. Be sure to remove the checkmark before removing the flash drive from the ENVIROMUX or the data on the drive may be lost.

Support

The Support section of the menu includes two links, Manual and Downloads.

The Manual link will open the pdf manual for the ENVIROMUX on the NTI website. You must have Adobe Reader installed on your PC to open this.

The Downloads link will take you to the Firmware Downloads page for the ENVIROMUX on the NTI website. All versions of firmware and MIB files for the ENVIROMUX will be found there, available for immediate download to your PC.

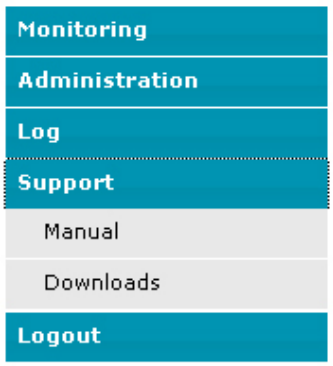


Figure 63- Support

Logout

To logout of the ENVIROMUX user interface, click on the “Logout” section in the menu. A gray menu label will drop down. Click on the gray label to be immediately logged out. The login screen will appear, at which you can close your browser or log back in.

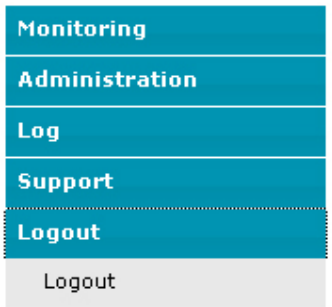


Figure 64- Logout

OPERATION VIA TEXT MENU- ENVIROMUX

The ENVIROMUX can be controlled through a text menu using a terminal program (e.g. HyperTerminal) connected to the USB Console Port (page 8), or using the Telnet or the SSH protocol provided a connection has been made to the Ethernet Port (page 7). Either of these methods will work to access the ENVIROMUX text menu. The text menu can be used to control all functions of the ENVIROMUX as an alternative to the Web Interface (page 23).

Connect to ENVIROMUX from a Terminal Program

The following instruction will enable the user to quickly make connections using a terminal connected to the "USB CONSOLE" port after the drivers have been loaded (page 8). For instruction to make quick connection using the Ethernet port and Web Interface, see page 23.

Note: Drivers must first be installed on the PC (page 8) before the terminal program and USB CONSOLE port can be used.

1. Make sure the ENVIROMUX is powered ON.
2. Using the serial console device connected to the port labeled "USB CONSOLE", start the terminal program (e.g. Windows HyperTerminal) 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
    - VT100 terminal mode.
3. Press <**Enter**> and a login prompt will appear- "**minilxo login:" ,** type <**root**> (all lowercase letters) and press <Enter>.
4. At "Username: " type <**root**> (all lowercase letters) and press <**Enter**>.
5. At "Password" type <**nti**> (all lowercase letters) and press <**Enter**>.

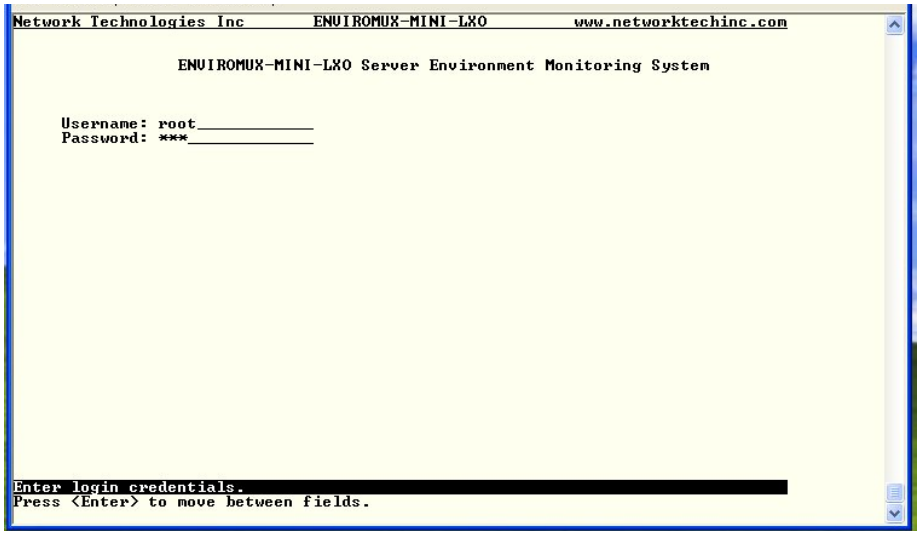


Figure 65- Text Menu Login screen

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

Note: Only the user "root" can access the text menu when connected through the "USB CONSOLE" port.

Connect to ENVIROMUX from Command Line

To access the Text Menu from the command line, the ENVIROMUX must first be connected to the Ethernet (page 7).

Connect Via Telnet

Note: Telnet must be enabled for a connection via Telnet to be possible (page 42)

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

`telnet` *<ENVIROMUX hostname or IP address>*

<ENVIROMUX 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 ENVIROMUX (default is 192.168.1.23).

The user will be prompted for username and password to connect to the ENVIROMUX.

Connect Via SSH

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

`ssh -l` *<Username> <ENVIROMUX hostname or IP address>*

<Username> is any user configured to access the ENVIROMUX (as defined in the list of users (page 44).

<ENVIROMUX hostname> is the hostname configured in the workstation where the SSH client will run (through /etc/hosts or DNS table). It can also be just the IP address of the ENVIROMUX (default is 192.168.1.23).

The user will be prompted for a password to connect to the ENVIROMUX.

The main menu of the Text Menu will be displayed whether you are connecting via USB Console,Telnet, or SSH.

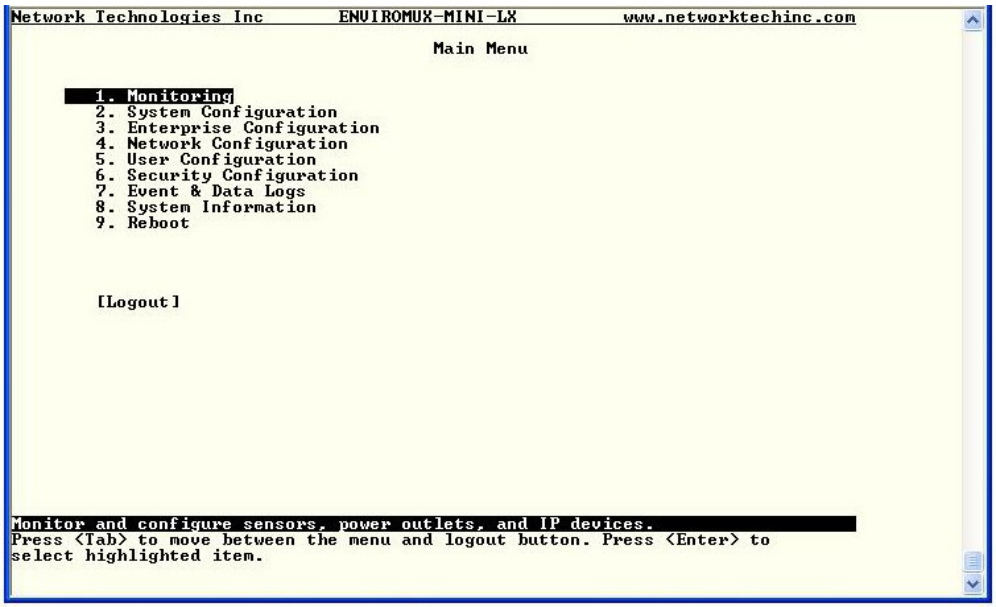


Figure 66- Text Menu- Administrator Main Menu

If you are a user with only user privileges (no administrative privileges), the text menu will have more limited options.

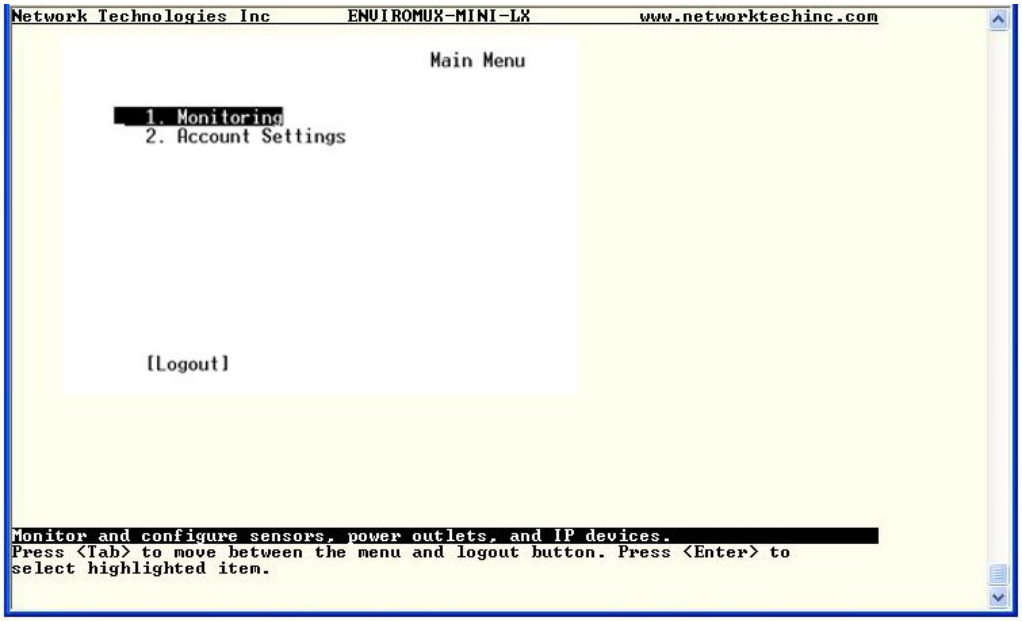


Figure 67- Text Menu- User Main Menu

For more on the Text Menu options for non-administrative users, see page 102.

Using the Text Menu

Text Menu Navigation

- To move up and down the numbered menu items or toggle through field options, use the arrow keys.
- To jump from menu item to another quickly, press the numbered key above the QWERTY keys (**the numberpad number keys are not used**).
- To move from menu list to action key (such as “Logout” in Figure 67 above), press <**Tab**>.
- To exit an action or menu, press <**Esc**>.
- To select a highlighted item or move to another field in a configuration page, press <**Enter**>.
- Be sure to Tab to “**Save**” and press <**Enter**> when configuration changes are made.
- To return from “Save” back to a field on the configuration page, press <**Tab**>.

The Administrators Main Menu is broken into 9 categories:

Function	Description
Monitoring	Monitor and configure the sensors, accessories and IP devices
System Configuration	Set the ENVIROMUX time settings or reset the unit to factory default settings
Enterprise Configuration	Configure system settings
Network Configuration	Configure network settings
User Configuration	Configure user access settings
Security Configuration	Configure security settings
Event and Data Logs	View and configure the Event and Data Logs (page 98)
System Information	View system and network settings
Reboot	Enables the user to reboot the ENVIROMUX

Monitoring

The Monitoring menu lists choices for viewing the status of items monitored by the ENVIROMUX as well as for configuring how they are monitored and how or if alert messages will be sent.

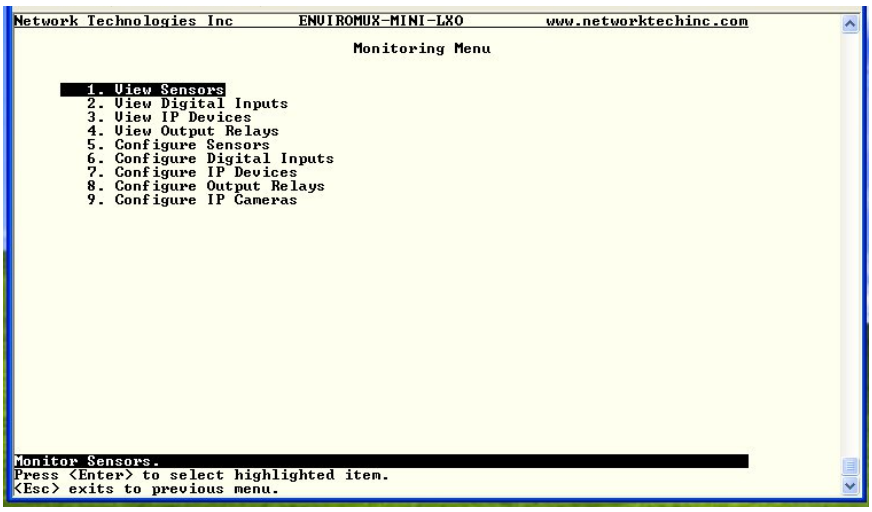


Figure 68- Text Menu-Monitoring Menu

View Sensors

The View Sensors selection will show the present status of each analog sensor connected to the ENVIROMUX.

The current value being reported by the sensor and the state (whether Normal or Alert) will be shown. If the sensor is in alert status, pressing the <**Enter**> key would provide the option to either **acknowledge** the alert or **dismiss** it.

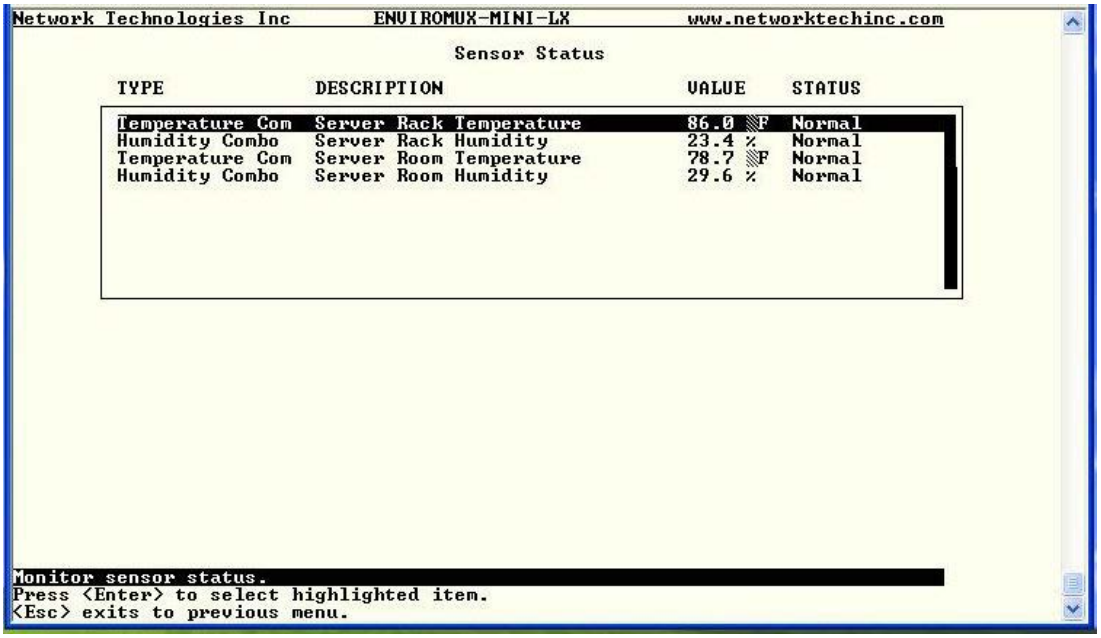


Figure 69- Text Menu-Sensor Status

View Digital Inputs

The View Digital Inputs selection will show the present status of each dry contact sensor connected to the ENVIROMUX.

The current value being reported by the sensor and the state (whether Normal or Alert) will be shown. If the sensor is in alert status, pressing the <**Enter**> key would provide the option to either **acknowledge** the alert or **dismiss** it.

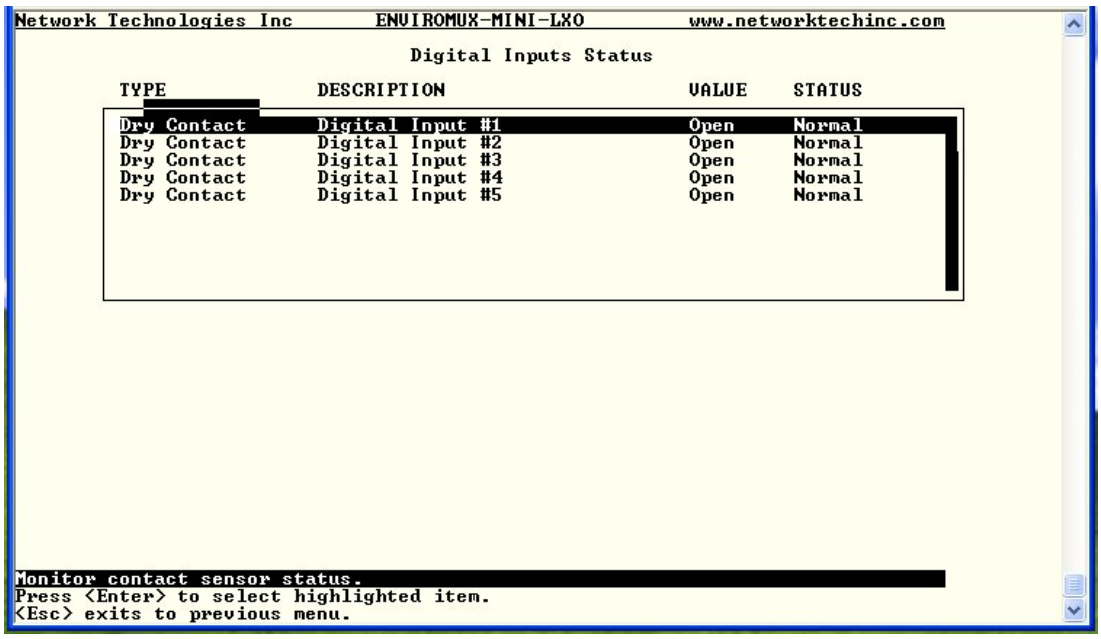


Figure 70- Text Menu- Digital Input Status

View IP Devices

The View IP Devices selection will show the present status of each IP Device monitored by the ENVIROMUX.

The current value being reported by the IP Device and the state (whether Normal or Alert) will be shown. If the IP Device is in alert status, pressing the <**Enter**> key would provide the option to either **acknowledge** the alert or **dismiss** it.

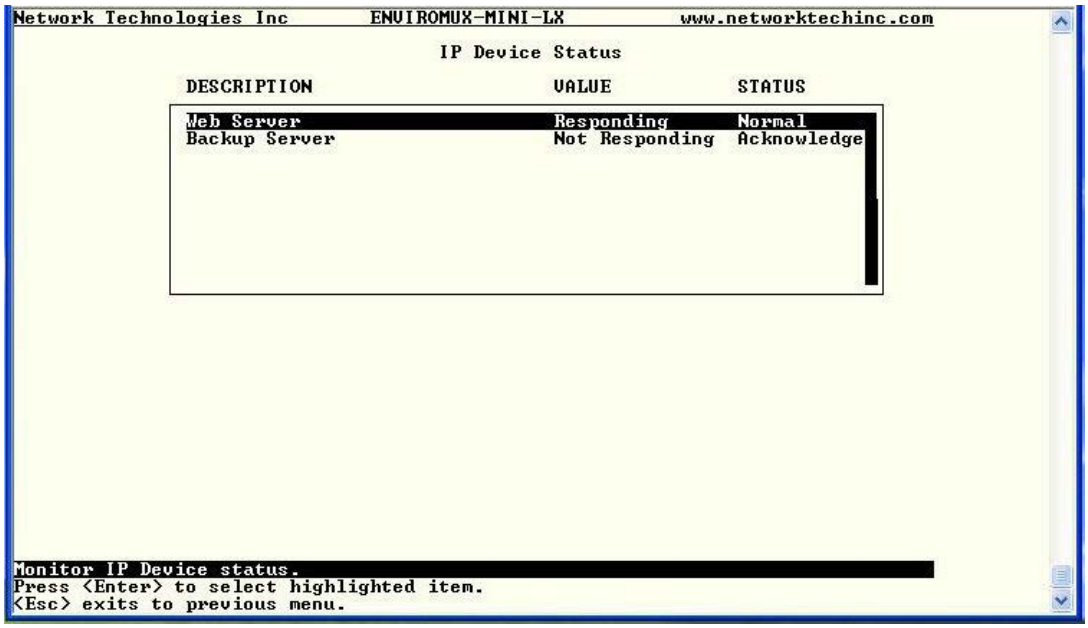


Figure 71- Text Menu-View IP Devices

View Output Relay

The View Output Relay selection will show the present state of the Output Relay on the ENVIROMUX. To manually change its state, press <**Enter**> and select between Inactive and Active.

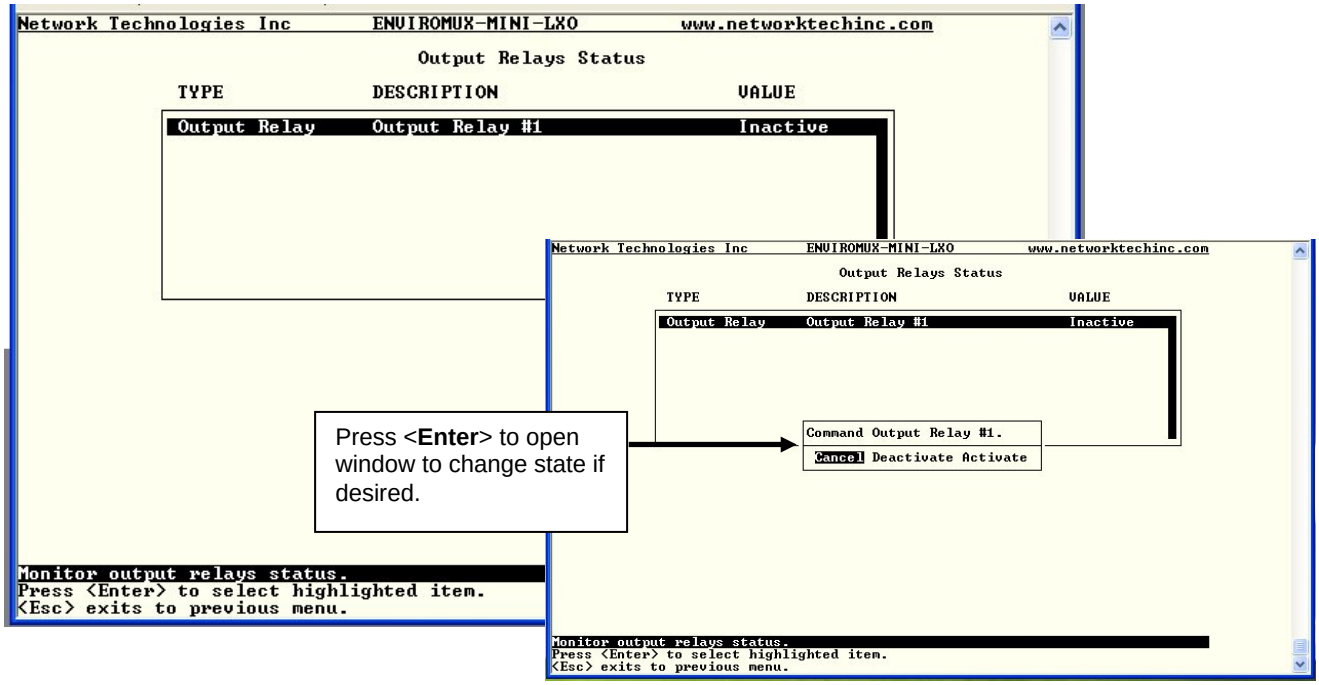


Figure 72- Text Menu- View Output Relay Status

Configure Sensors

The Configure Sensors menu lists the temperature and humidity sensors connected to the ENVIROMUX. Press <**Enter**> to open the configuration menu for the selected sensor.

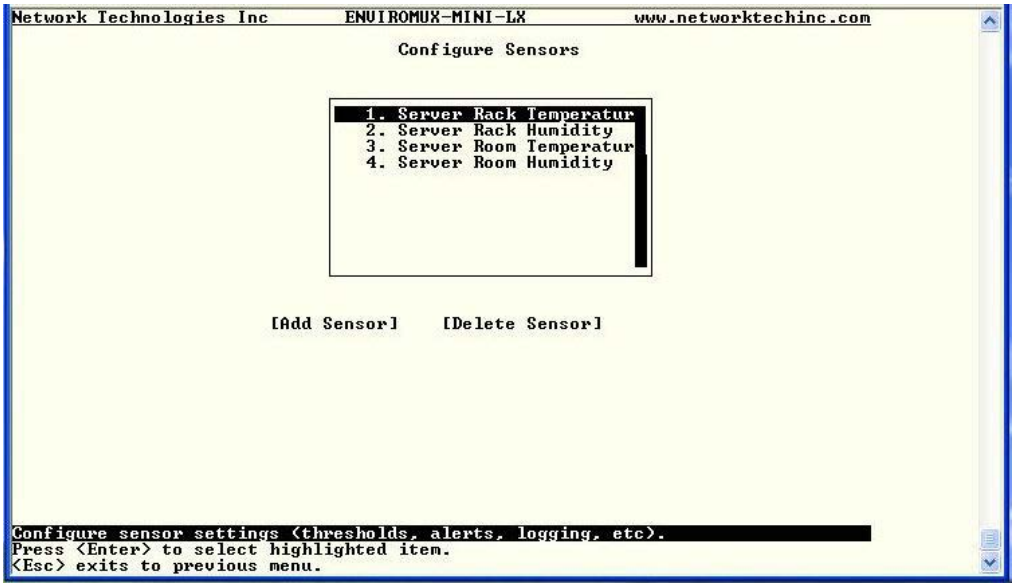


Figure 73- Text Menu-Configure Sensors list

The configuration menu for the sensor includes options to enter the Sensor Settings, Non-Critical Alert Settings, Critical Alert Settings, and Data Logging.

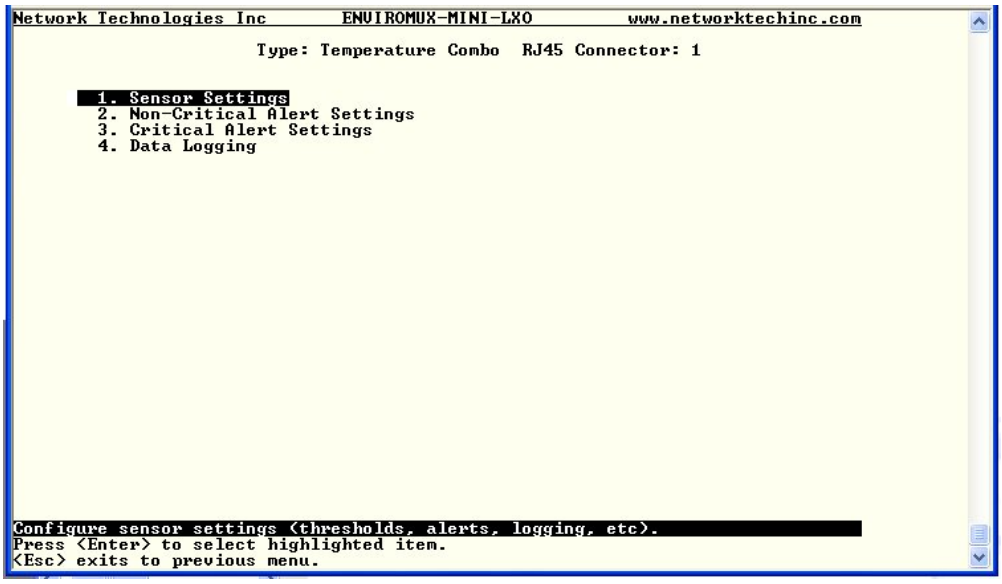


Figure 74- Text Menu-Configuration Menu for Sensor

From the Sensor Settings menu enter the Description for the sensor and select which sensor group the sensor should belong to (1 or 2).

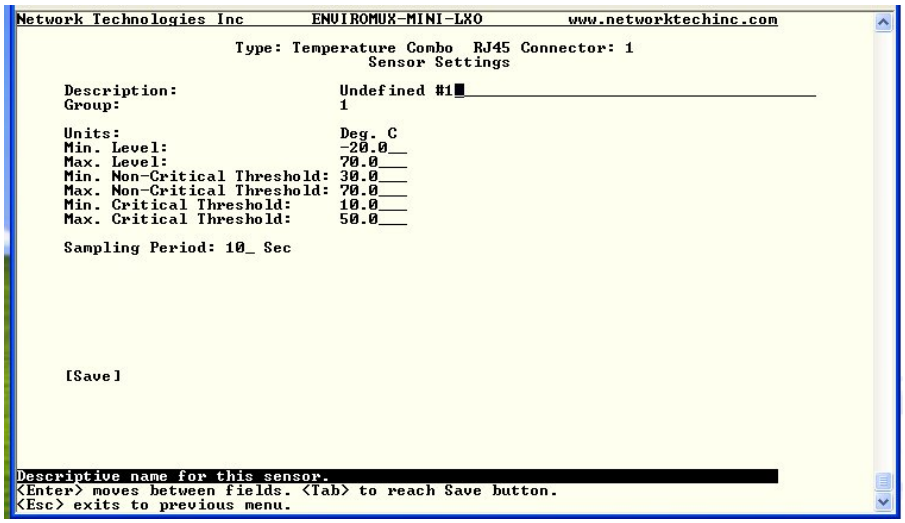
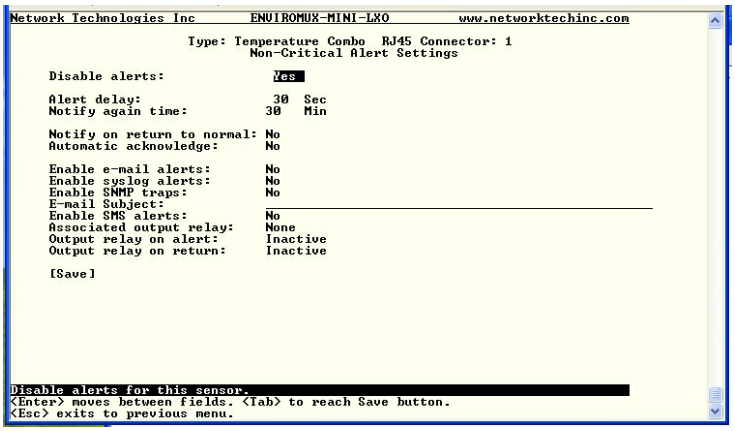


Figure 75- Text Menu-Sensor Settings

Sensor Settings	Description
Description	The description of the sensor that will be viewed in the Summary page and in the body of alert messages
Group	Assign the sensor to a group (1 -8) (see also page 92)
Units	This lets the operator choose between Celsius and Fahrenheit as the temperature measurement unit.
Min. Level	Displays the minimum value that this sensor will report
Max. Level	Displays the maximum value that this sensor will report
Minimum Non-Critical -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 non-critical 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, and error message will be shown.
Maximum Non-Critical 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 non-critical 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, and error message will be shown.
Minimum Critical 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, ➢ lower than the assigned Maximum Threshold value, and ➢ lower than the Minimum Non-Critical Threshold value. If values out of the range are entered, and error message will be shown.
Maximum Critical 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, ➢ higher than the assigned Minimum Threshold value, and ➢ higher than the Maximum Non-Critical Threshold value. If values out of the range are entered, and error message will be shown.
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.

Press <**Tab**> to highlight **Save** and press <**Enter**> to save before pressing <**Esc**> to exit.

From the Non-Critical or Critical Alert Settings menu, the user can enable/disable alert messages to be sent when the sensor is in an alert state and configure when and how alert messages are sent. Additionally, from the Critical Alert Settings menu, the user can configure the ENVIROMUX to capture a snapshot from an IP camera and attach the image to the alert message sent via email.



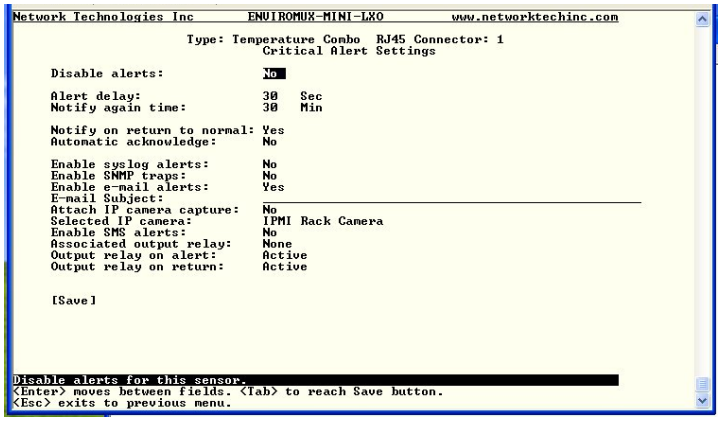


Figure 76- Text Menu-Non-Critical and Critical Alert Settings

Alert Settings	
Disable alerts	Change to “Yes” to prevent alerts from being sent when this sensor’s status changes
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.
Notify Again Time	Enter the amount of time in seconds, minutes, or hours (1-999) before an alert message will be repeated
Notify on Return to Normal	The user can also be notified when the sensor readings have returned to the normal range by changing to “Yes” for "***Notify on return to normal***" for a sensor.
Auto Acknowledge	Change to “Yes” to have alert notifications in the summary page return to normal state automatically when sensor readings return to normal.
Enable Email Alerts	Change to “Yes” to have alert notifications sent via Email
Enable Syslog Alerts	Change to “Yes” to have alert notifications sent via Syslog messages
Enable SNMP traps	Change to “Yes” to have alert notifications sent via SNMP traps (v2c)
Enable SMS Alerts	Change to “Yes” to have alert notifications sent via SMS (requires GSM modem)
Email Subject	Enter the subject to be viewed when an email alert message is received
Attach IP camera capture	Change to “Yes” to enable a snapshot to be taken from an IP camera and attached to the alert message (for critical alert messages only.)
Selected IP camera	Select which IP camera to take a snapshot from to be attached to an alert message (for critical alert messages only)
Associated output relay	Choose which output relay to change state when sensor is in alert
Output relay on alert	Choose the state the output relay should be in when the sensor is in alert
Output relay on return	Choose the state the output relay should be in when the sensor returns to normal

Press <**Tab**> to highlight **Save** and press <**Enter**> to save before pressing <**Esc**> to exit.

From the Data Logging menu for the sensor, the user can decide if the data sampled should be recorded in the Data Log and how frequently.

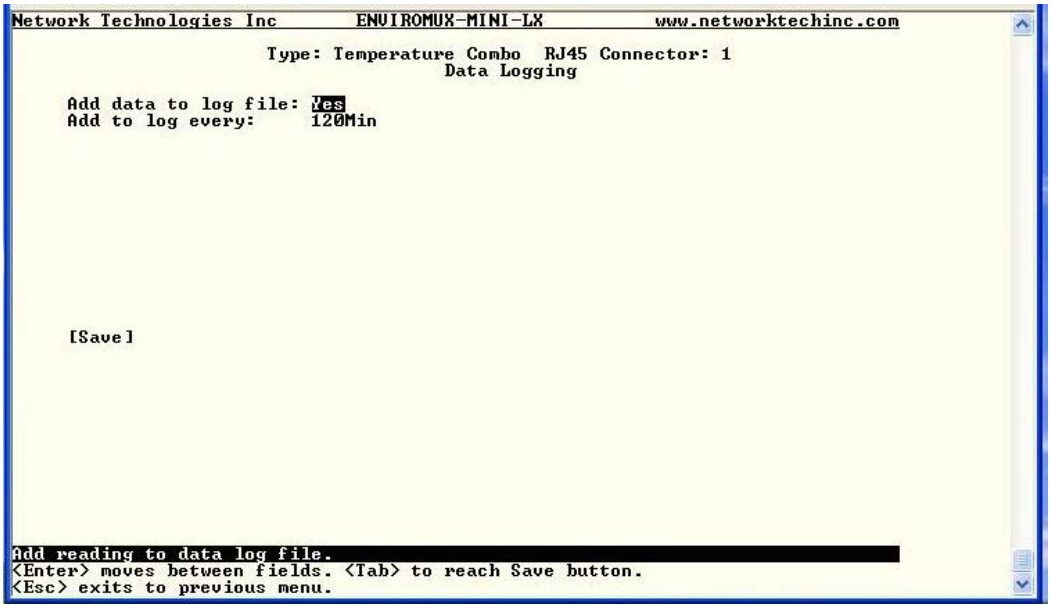


Figure 77- Text Menu-Sensor Data Logging

Configure Digital Inputs

The Configure Digital Input Sensors menu lists the contact sensors connected to the ENVIROMUX. Press <**Enter**> to open the configuration menu for the selected contact sensor. (The Water Sensor menu contains the same options as the contact sensor menus.) The configuration menu for the Digital Inputs includes options to enter the Digital Input Settings, Alert Settings, and Data Logging.

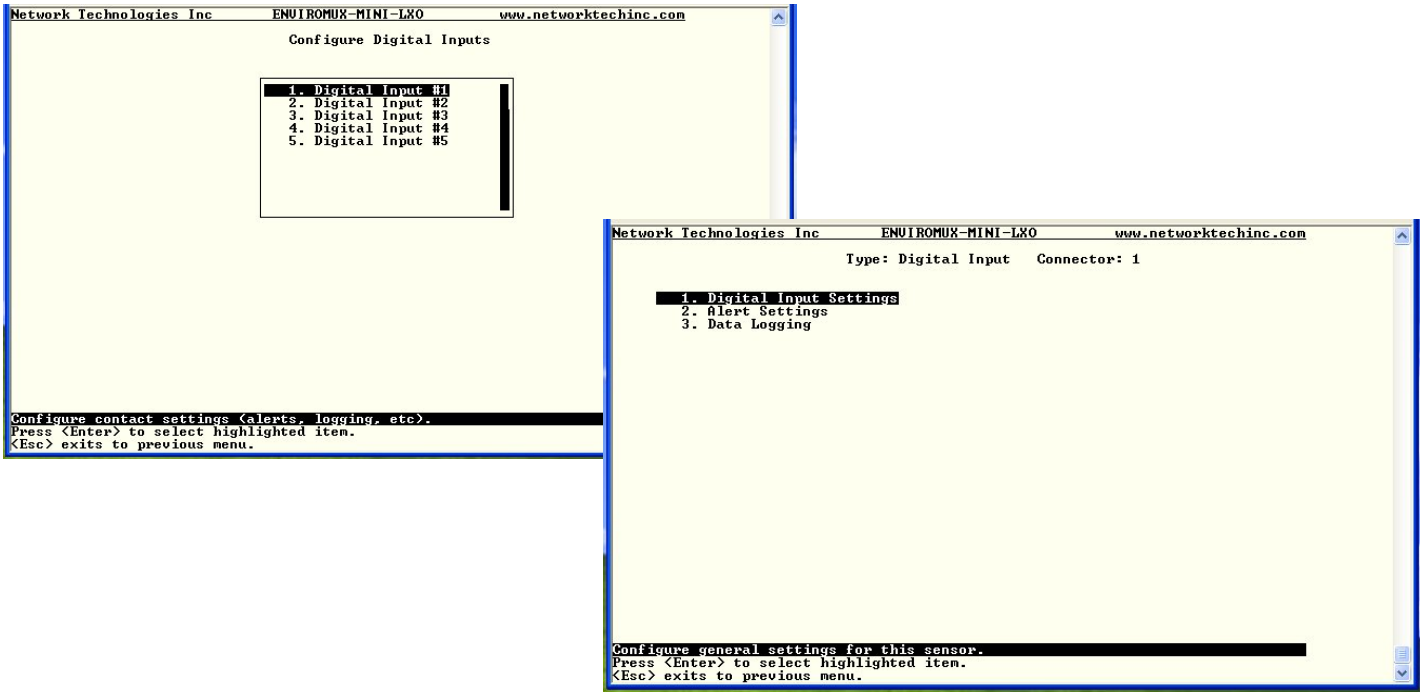


Figure 78- Configure Digital Input Sensors

Water sensors and contact sensors are each configured much like the temperature and humidity sensors previously described. Only the Sensor Settings menu (below) is different. Alert settings and data logging menus are as seen in Figure 76 and Figure 77.

Instead of threshold and minimum/maximum levels settings, water sensors and contact sensors are either open contact or closed contact sensors. Therefore, the field "**Normal Status**" is provided to select the status of the sensor when it is not in an alert state. Select between **Open** contacts, or **Close** contacts for the normal status of the sensor. (Water sensors are open contact when not in an alert state.)

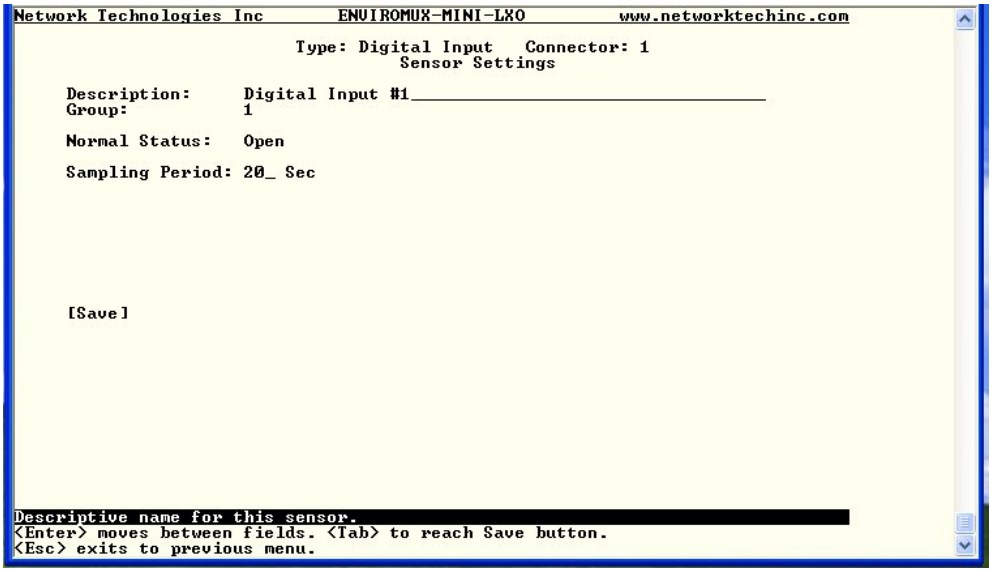


Figure 79- Digital Input Sensor Settings Menu

From the Alert Settings menu, the user can enable/disable alert messages to be sent when the sensor is in an alert state and configure when and how alert messages are sent.

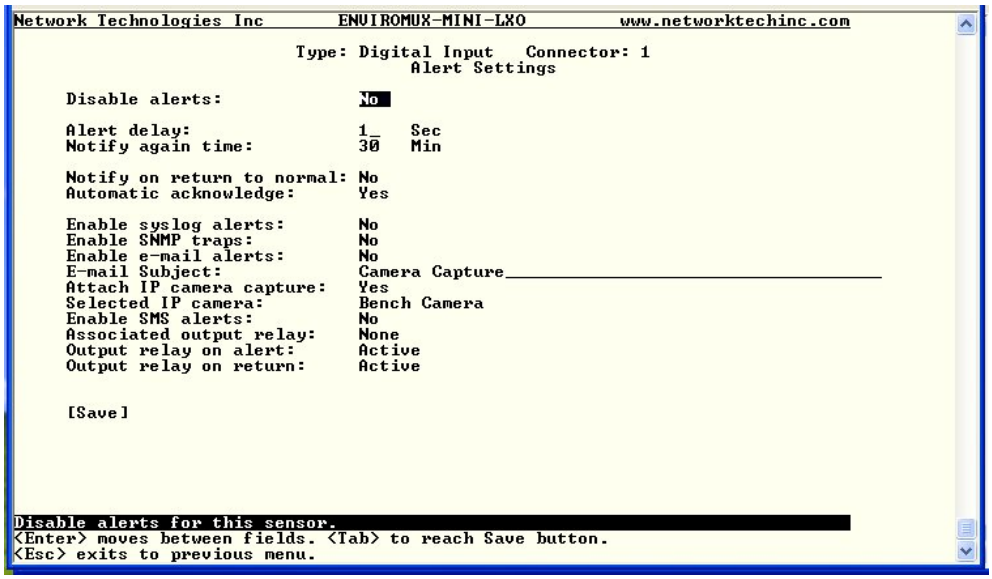


Figure 80- Digital Input Alert Settings

Alert Settings	
Disable alerts	Change to “Yes” to prevent alerts from being sent when this sensor’s status changes
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.
Notify Again Time	Enter the amount of time in seconds, minutes, or hours (1-999) before an alert message will be repeated
Notify on Return to Normal	The user can also be notified when the sensor readings have returned to the normal range by changing to “Yes” for "***Notify on return to normal***" for a sensor.
Auto Acknowledge	Change to “Yes” to have alert notifications in the summary page return to normal state automatically when sensor readings return to normal.
Enable Syslog Alerts	Change to “Yes” to have alert notifications sent via Syslog messages
Enable SNMP traps	Change to “Yes” to have alert notifications sent via SNMP traps (v2c)
Enable Email Alerts	Change to “Yes” to have alert notifications sent via Email
Email Subject	Enter the subject to be viewed when an email alert message is received
Attach IP camera capture	Change to “Yes” to enable a snapshot to be taken from an IP camera and attached to the alert message (for critical alert messages only.)
Selected IP camera	Select which IP camera to take a snapshot from to be attached to an alert message (for critical alert messages only)
Enable SMS Alerts	Change to “Yes” to have alert notifications sent via SMS (requires GSM modem)
Associated output relay	Choose which output relay to change state when sensor is in alert
Output relay on alert	Choose the state the output relay should be in when the sensor is in alert
Output relay on return	Choose the state the output relay should be in when the sensor returns to normal

Press <**Tab**> to highlight **Save** and press <**Enter**> to save before pressing <**Esc**> to exit.

From the Data Logging menu for the Digital Input sensor, the user can decide if the data sampled should be recorded in the Data Log and how frequently.

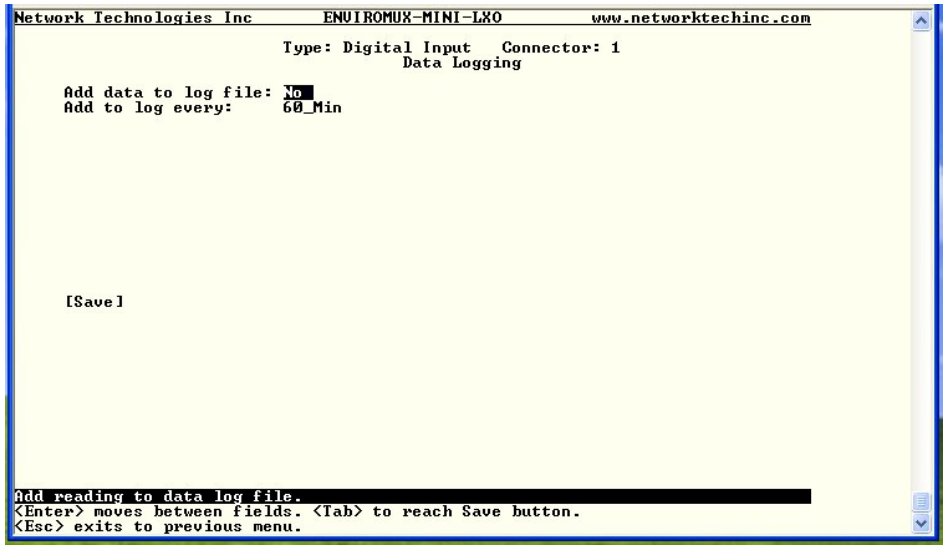


Figure 81- Data Logging for Digital Input Sensors

Configure IP Devices

The Configure IP Devices menu lists the IP Devices monitored by the ENVIROMUX. Press <**Enter**> to open the configuration menu for the selected IP Device.

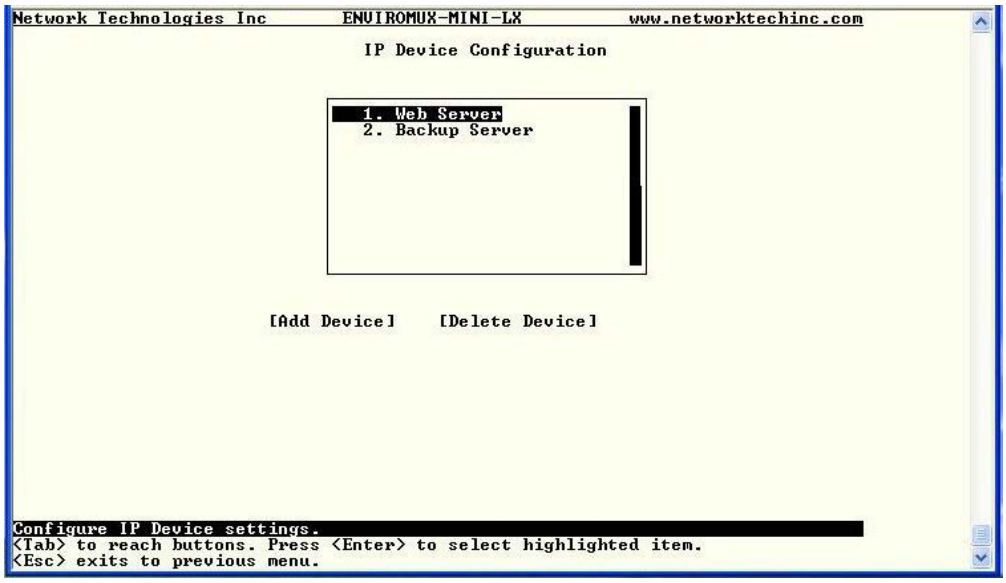


Figure 82- Text Menu-Configure IP Devices List

The configuration menu for the IP Device includes options to enter the IP Device Settings, Alert Settings, and Data Logging.

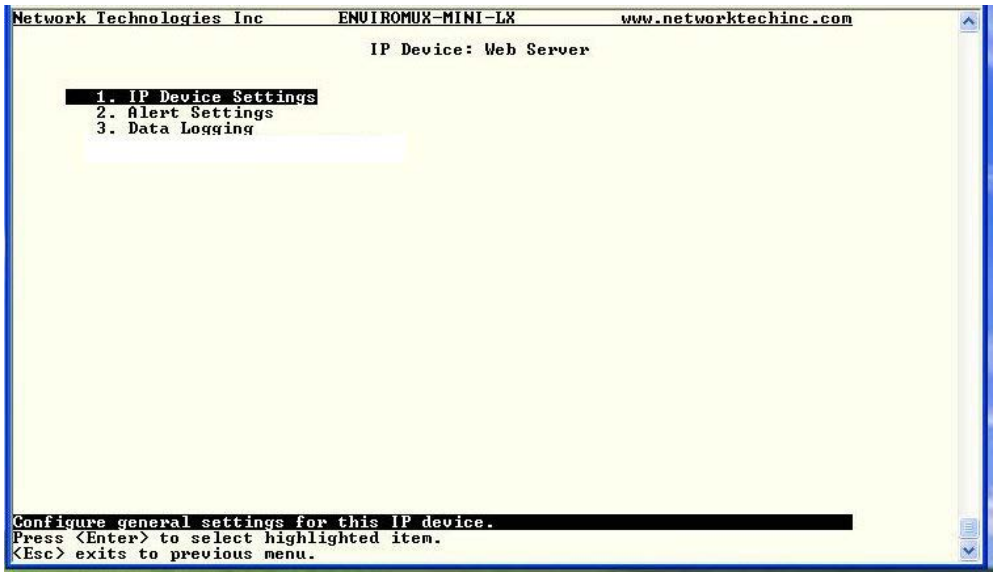


Figure 83- Text menu-Configuration Menu for IP Devices

From the IP Device Settings menu, the user can enter the name and address of the IP Device, assign a sensor group, and define how the IP Device will be monitored.

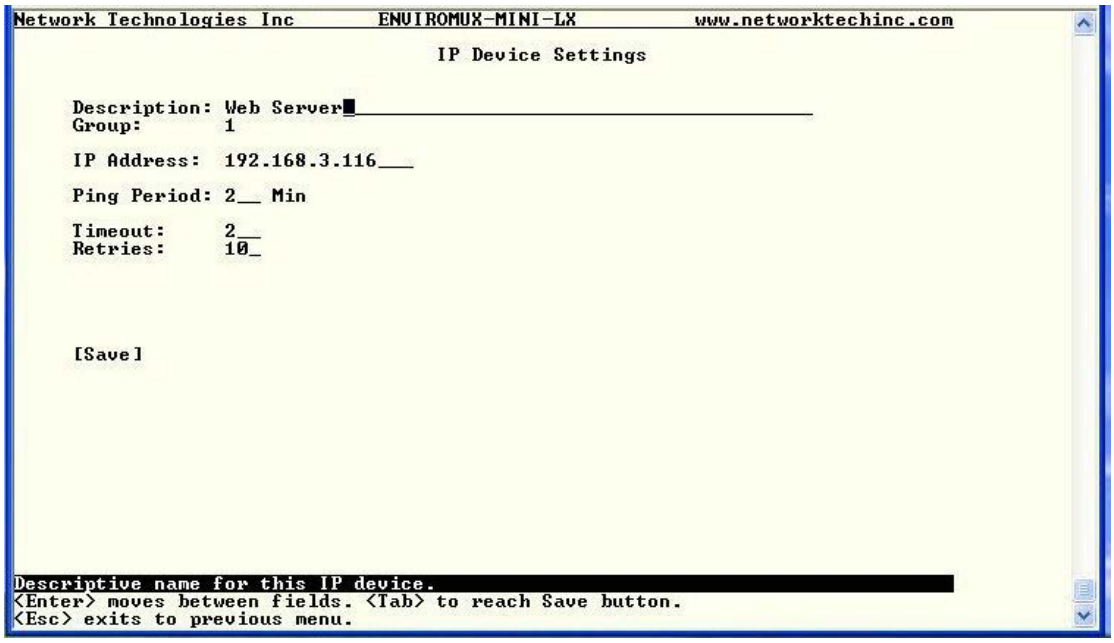


Figure 84-Text Menu-IP Device Settings

IP Device Settings	Description
Description	The description of the IP Device that will be viewed in the Summary page and in the body of alert messages
Group	Assign the IP device to a group (1 -8)
IP Address	The IP address of the IP Device
Ping Period	Enter the frequency in minutes or seconds that the ENVIROMUX should ping the IP Device
Timeout	Enter the length of time in seconds to wait for a response to a ping before considering the attempt a failure
Retries	Enter the number of times the ENVIROMUX should ping a non-responsive IP device before changing its status from normal to alarm and sending an alert

Press <**Tab**> to highlight **Save** and press <**Enter**> to save before pressing <**Esc**> to exit.

From the Alert Settings menu, the user can enable/disable alert messages to be sent when the IP Device is not responding and configure when and how alert messages are sent.

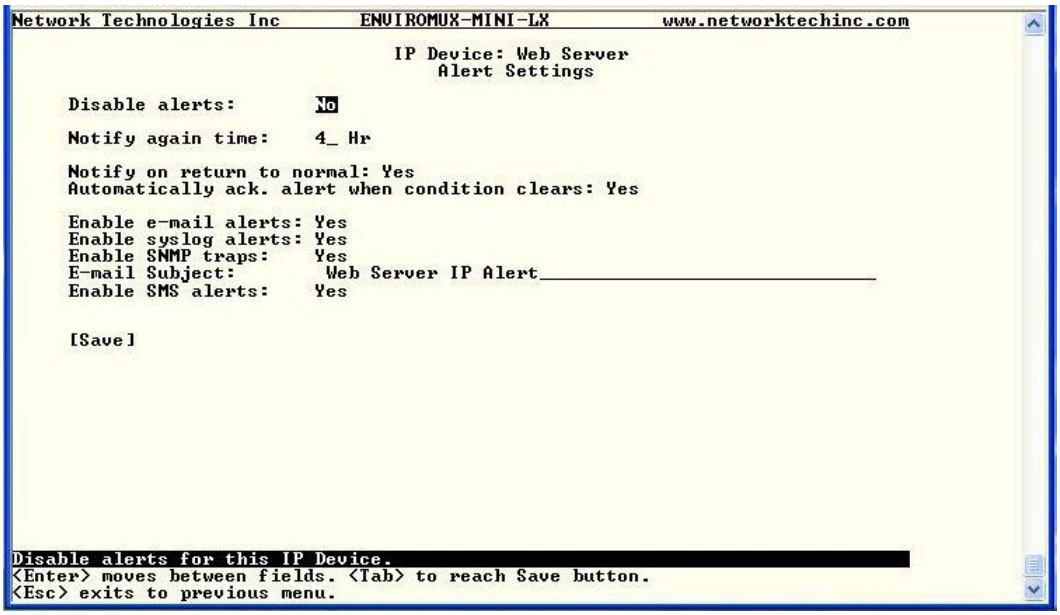


Figure 85- Text Menu-IP Device Alert Settings

Alert Settings	Description
Disable alerts	Change to “Yes” to prevent alerts from being sent when this IP Device’s status changes
Alert Delay	The alert delay is an amount of time the IP Device 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.
Notify Again Time	Enter the amount of time in seconds, minutes, or hours (1-999) before an alert message will be repeated
Notify on Return to Normal	The user can also be notified when the IP Device’s state has returned to the normal by changing to “Yes” for "***Notify on return to normal***" for a sensor.
Auto Acknowledge	Change to “Yes” to have alert notifications in the summary page return to normal state automatically when sensor readings return to normal.
Enable Email Alerts	Change to “Yes” to have alert notifications sent via Email
Enable Syslog Alerts	Change to “Yes” to have alert notifications sent via Syslog messages
Enable SNMP traps	Change to “Yes” to have alert notifications sent via SNMP traps (v2c)
Enable SMS Alerts	Change to “Yes” to have alert notifications sent via SMS (requires GSM modem)
Email Subject	Enter the subject to be viewed when an email alert message is received

Press <**Tab**> to highlight **Save** and press <**Enter**> to save before pressing <**Esc**> to exit.

From the Data Logging menu for the IP Device, the user can decide if the data sampled should be recorded in the Data Log and how frequently.

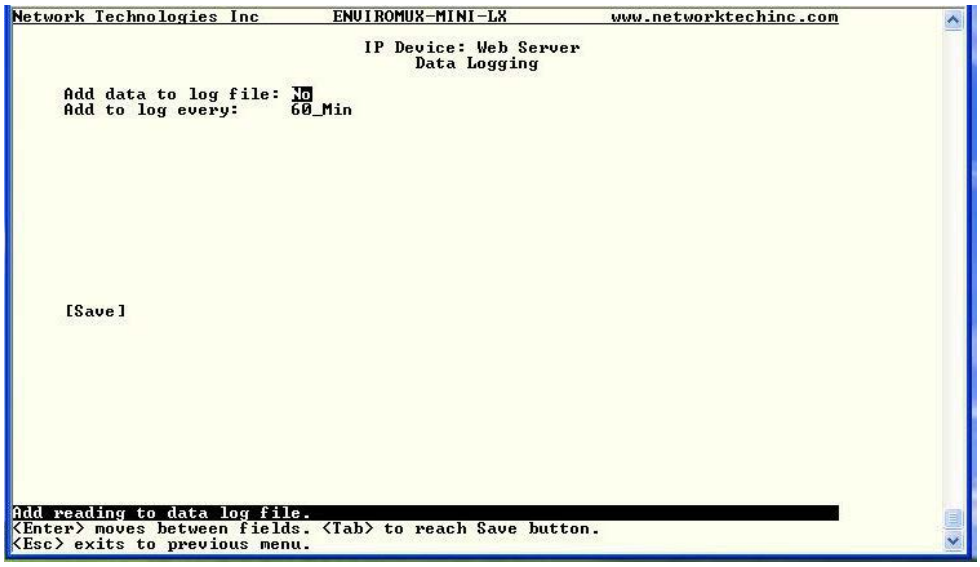


Figure 86- Text Menu-IP Device Data Logging

Configure Output Relay

From the Monitoring menu, the user can select to configure the Output Relay. You will first be presented with the Output Relays list (only one in this product). Press <Enter> to be given a choice of configuring Output Relay Settings or Alert Settings to associate with the relay state.

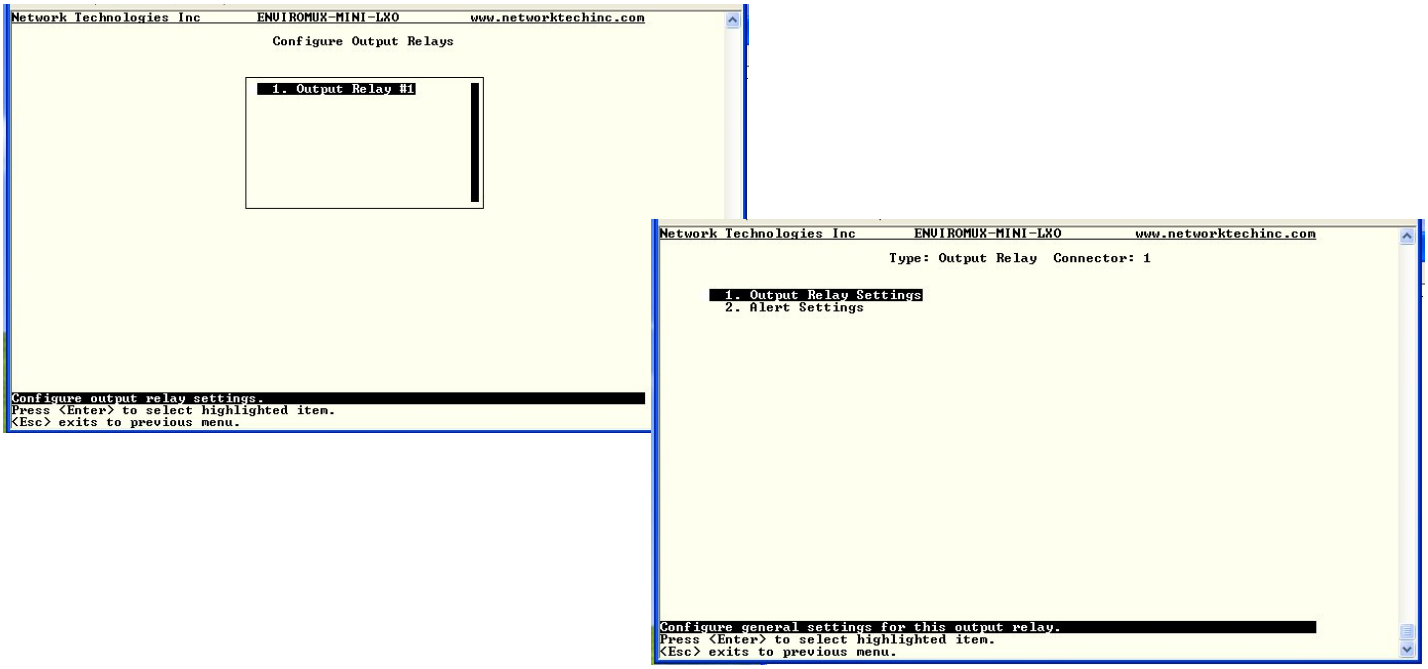


Figure 87- Text Menu- Select Configure Output Relay

Select the Output Relay Settings to access a menu where the description of the Output Relay can be defined. This definition will be presented in the View Output Relays list as well as in the description field when viewing the list through the WEB interface (page 24).

The group this relay will be associated with can be defined here to determine who will receive alerts generated by the relay state change, if any.

The “Normal Status” of the relay is defined here which determines what the ENVIROMUX will consider a normal versus alert condition for the relay.

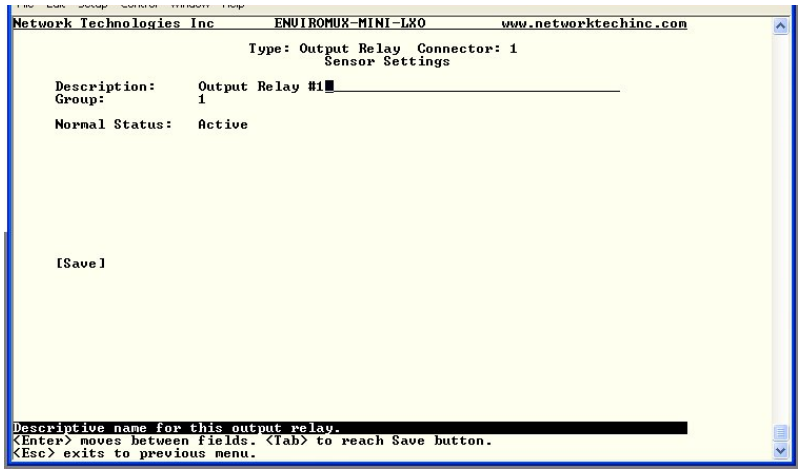


Figure 88- Text Menu- Output Relay Settings

Select the Alert Settings to access a menu for enabling alert messages that can be sent when the relay changes from its “Normal” state.

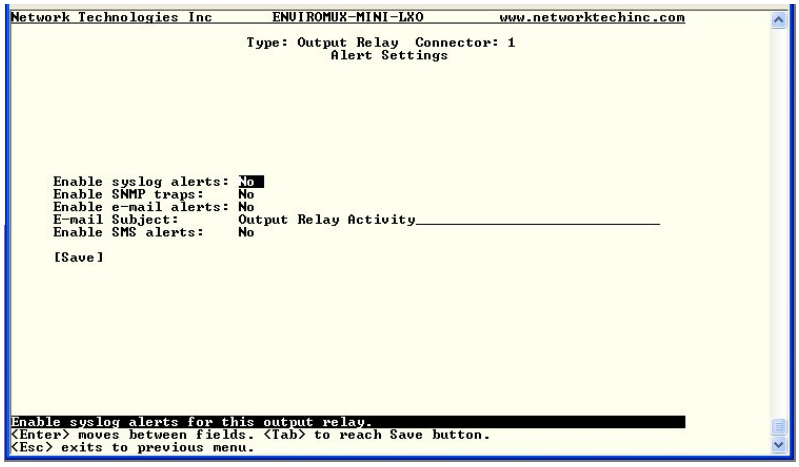


Figure 89- Text Menu- Output Relay Alert Settings

Configure IP Cameras

From the Monitoring menu, the user can select to configure IP Cameras. You will first be presented with the IP Cameras list (up to 8 can be configured). Select an IP Camera in the list and press <Enter> to open the IP Camera Settings menu.

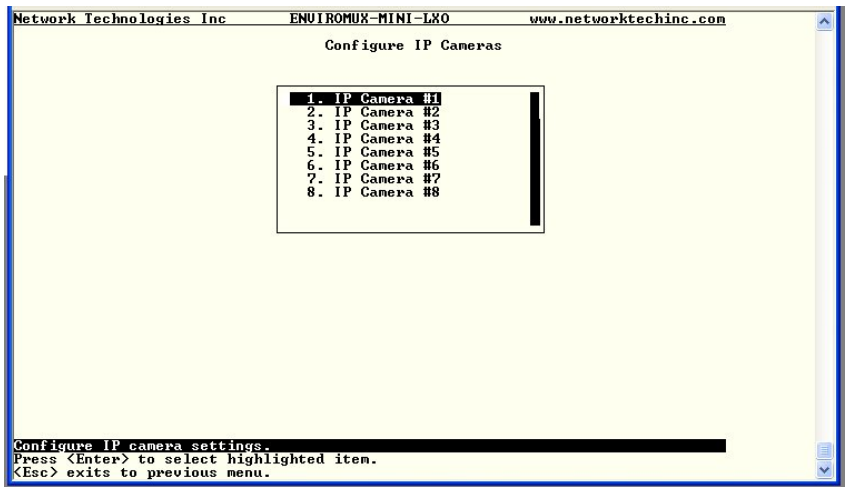


Figure 90- Text Menu- IP Camera List for Configuration

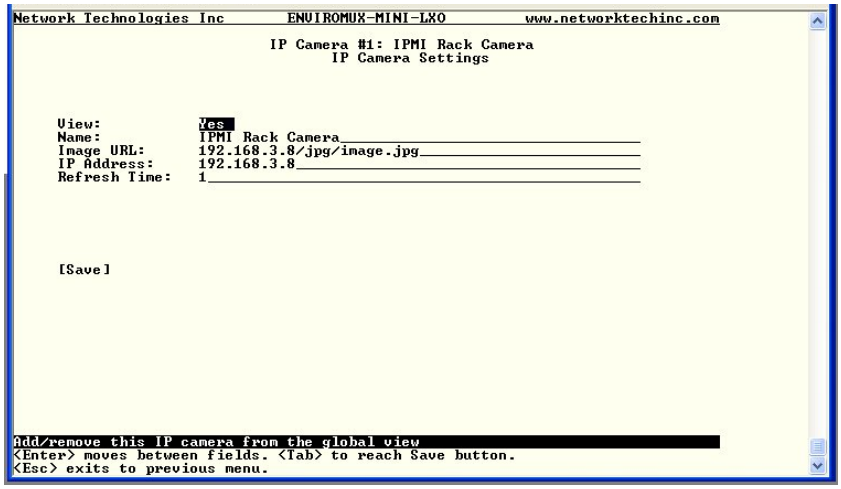


Figure 91- Text Menu- IP Camera Settings

Camera Settings	Description
View	Change to "Yes" to enable images from the IP Camera to appear in the view when selecting the IP Cameras from the Monitoring menu in the WEB interface (page 25).
Name	Characters entered will appear in any listing of the IP camera selection.
Image URL	Enter the full path to the image file captured by the IP camera under "Image URL".
IP Address	the IP address for the IP camera.
Refresh Time	Enter a refresh time period in increments of 100 msec (milliseconds). That is, a value of 1 = 100 msec, 5 = 500 msec , 10 = 1000 msec (or 1 second). The images can be set to be refreshed every 100 msec (.1 second) up to 99,900 msec (almost 100 seconds).

System Configuration

Under System Configuration (from the Main Menu), select “Time Settings” to enter the time of day, time zone, enable daylight saving time, or NTP server settings. Also, select “Restore Settings to Defaults” to clear all configuration and user settings and restore the ENVIROMUX to settings as received from the factory.

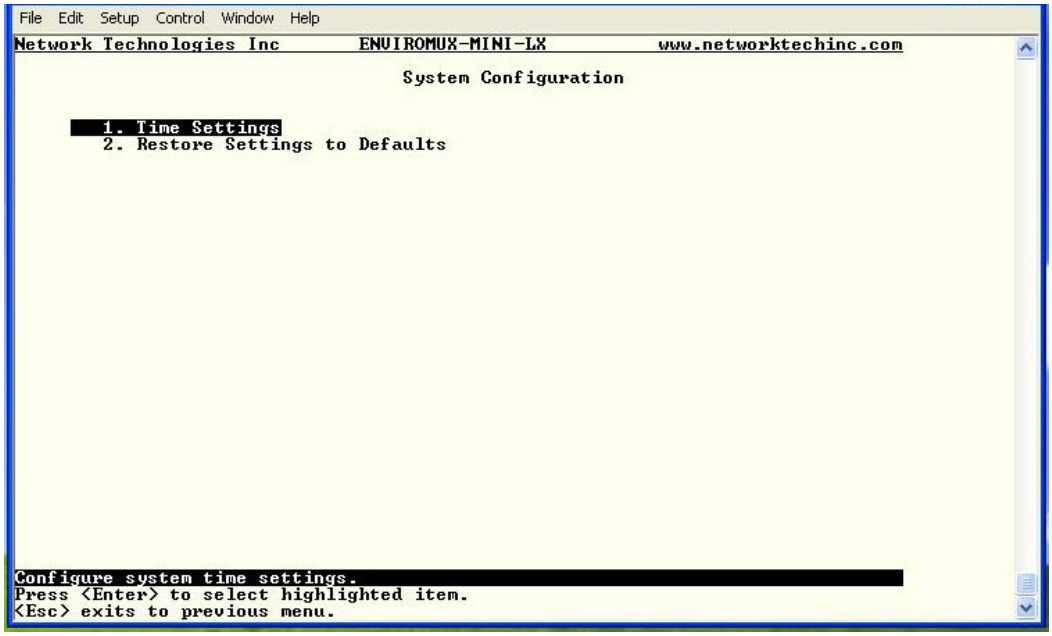


Figure 92- Text Menu- System Configuration

Time Settings

On the Time Settings menu, the user can designate what time zone the unit is associated with, set the date and time manually or configure the ENVIROMUX to get this information from an NTP server.

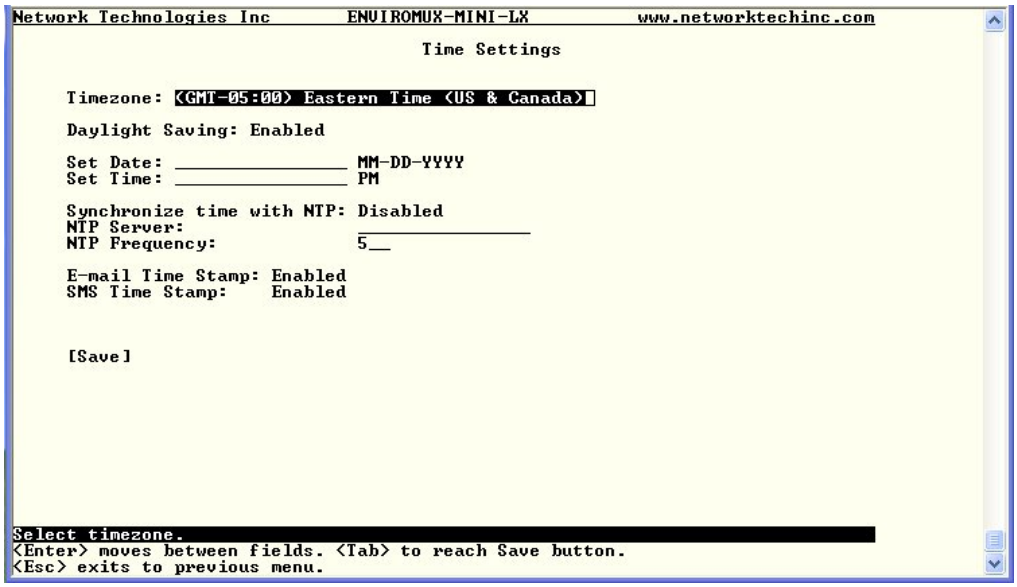


Figure 93- Text Menu-Time Settings menu

Time Settings	Description
Time Zone	Enter the appropriate time zone
Enable Daylight Saving	Change to “Yes” to have the time change in accordance Daylight Saving Time rules
Set Date	Enter the system date in MM-DD-YYYY format
Set Time	Enter the system time of day in hh:mm:ss format
Enable NTP	Change to “Enabled” to allow the ENVIROMUX to automatically sync up with a time server via NTP
NTP server	If the NTP is enabled, enter the Domain Name or IP address of the NTP server
NTP Frequency	Enter the frequency (in minutes) for the ENVIROMUX to query the NTP server (minimum is 5 minutes)
E-mail Time Stamp	Change to “Enabled” to allow the ENVIROMUX to automatically apply a time stamp to e-mail messages sent to users
SMS Time Stamp	Change to “Enabled” to allow the ENVIROMUX to automatically apply a time stamp to SMS messages sent to users

Press <**Tab**> to highlight **Save** and press <**Enter**> to save before pressing <**Esc**> to exit.

Restore Default Settings

Select this option to restore the ENVIROMUX to the configuration settings it had upon receipt from the factory. **Be careful!** This will erase all user configuration settings. Upon restoration, the ENVIROMUX will reboot. Allow 1 minute before trying to reconnect and log in again.

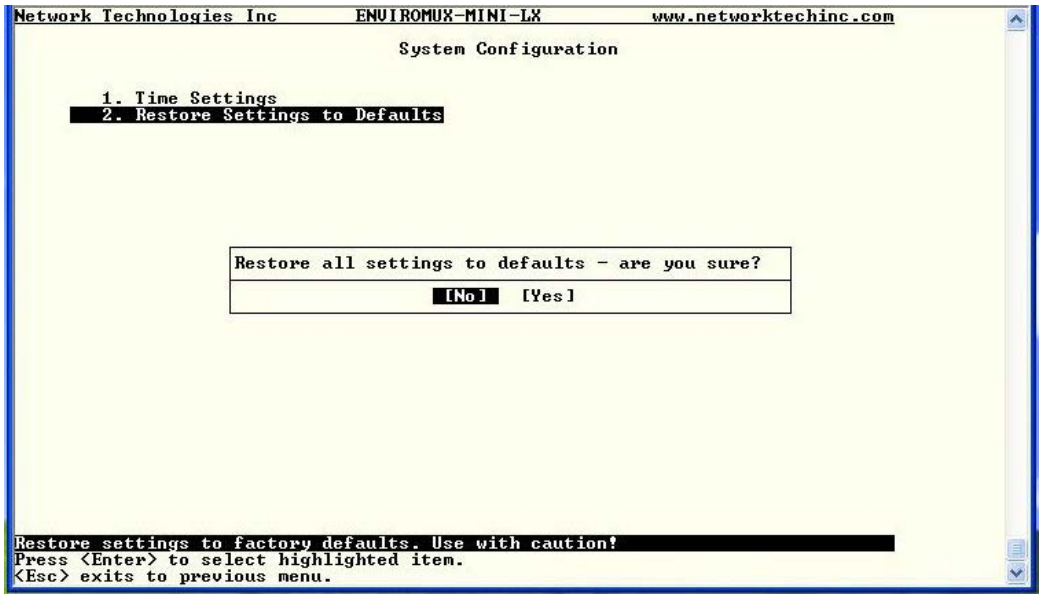


Figure 94- Text Menu-Restore Default Settings

Note: If “Restore Defaults” is used, the IP address will also be restored to its default address of 192.168.1.23 with a login name “root” and password “nti”. To restore the root password to “nti” without having to restore all default settings, contact NTI for assistance.

To identify the IP address of the ENVIROMUX without restoring defaults, use the Discovery Tool (page 22).

Default settings can also be restored using the web interface (page 39).

Enterprise Configuration

Under Enterprise Configuration (from the Main Menu), enter the unit name, location, the contact person emails should refer to and their phone number, and the email address of the ENVIROMUX to be used for outgoing alert messages.

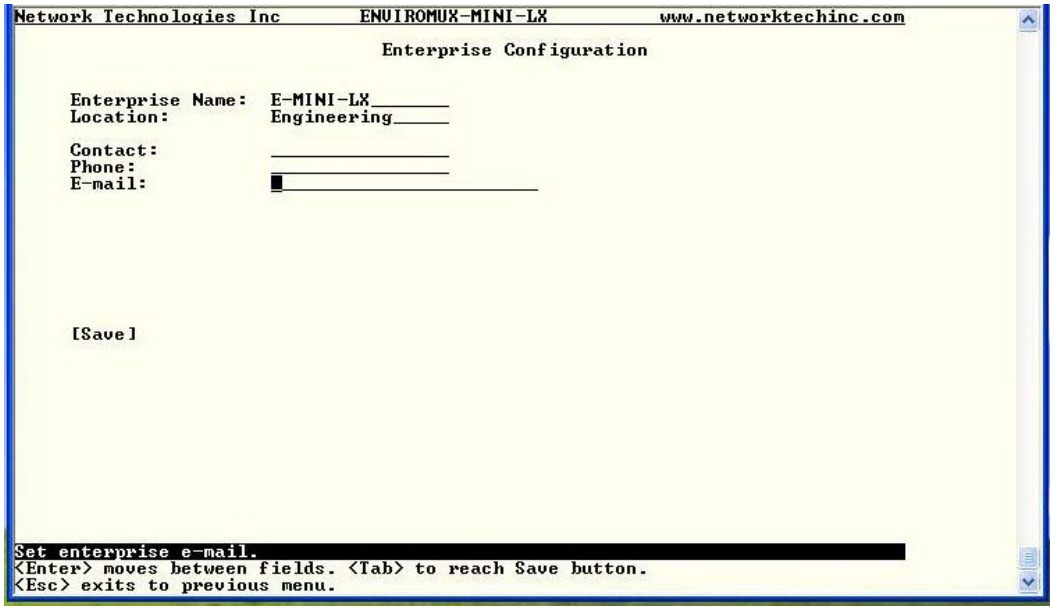


Figure 95- Text Menu-Enterprise Configuration

Network Configuration

The Network Configuration menu (from the Main Menu) includes submenus for applying IPv4 and IPv6 Settings, SMTP server settings, SNMP settings, and miscellaneous settings to enable services for SSH, Telnet, HTTP, HTTPS and Web Timeout.

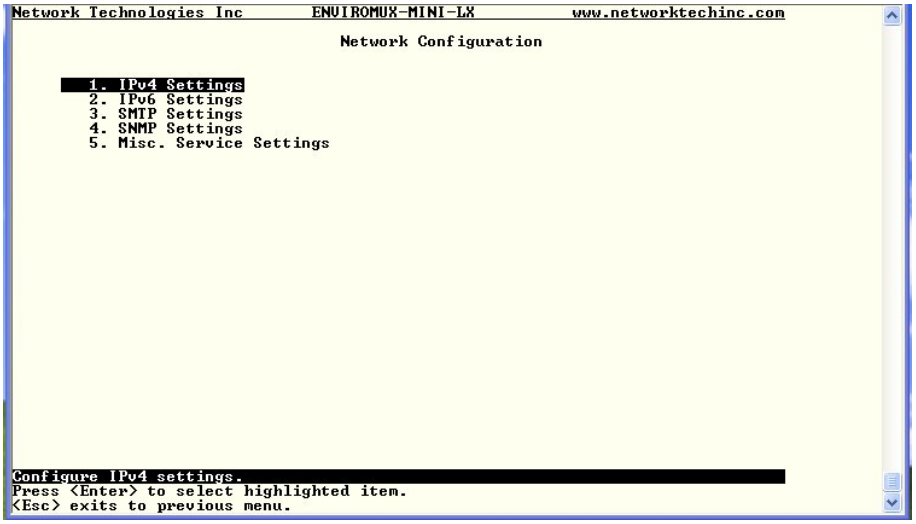


Figure 96- Text Menu-Network Configuration

IPv4 Settings

The IP Settings menu contains the network connection settings for the ENVIROMUX.

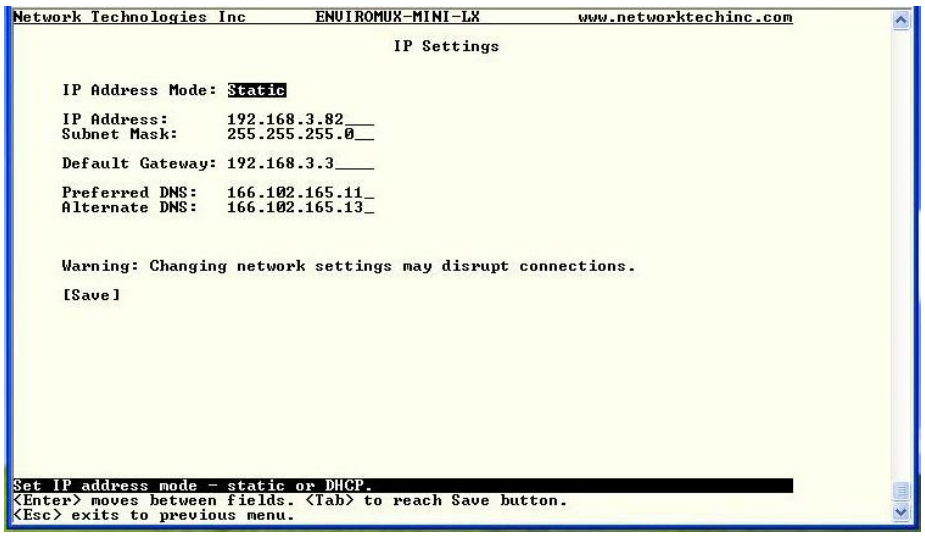


Figure 97- Text Menu-IPv4 Settings Menu

IP Settings	Description
Mode	Select between Static (manual) , or DHCP (automatic IP and DNS) settings
IP Address	Enter a valid IPv4 address (default value is 192.168.1.23)
Subnet Mask	Enter a valid subnet mask (default value is 255.255.255.0)
Default Gateway	Enter a valid gateway (default gateway value is 192.168.1.1)
Preferred DNS	Enter a preferred domain name server address
Alternate DNS	Enter an alternate domain name server address

If the administrator chooses to have the DNS and IP address information filled in automatically via DHCP, the SMTP server and port number still need to be entered for email alerts to work. If the SMTP server requires a password in order for users to send emails, the network administrator must first assign a user name and password to the ENVIROMUX.

Press <**Tab**> to highlight **Save** and press <**Enter**> to save before pressing <**Esc**> to exit.

IPv6 Settings

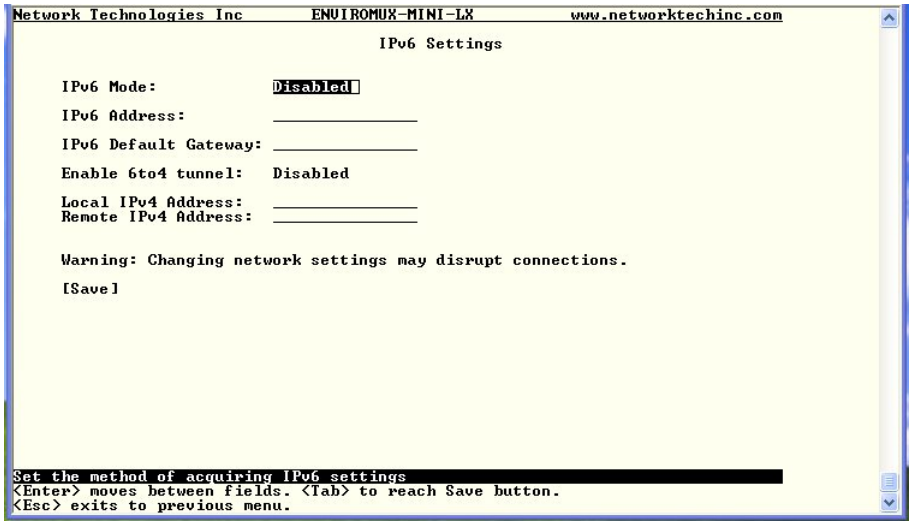
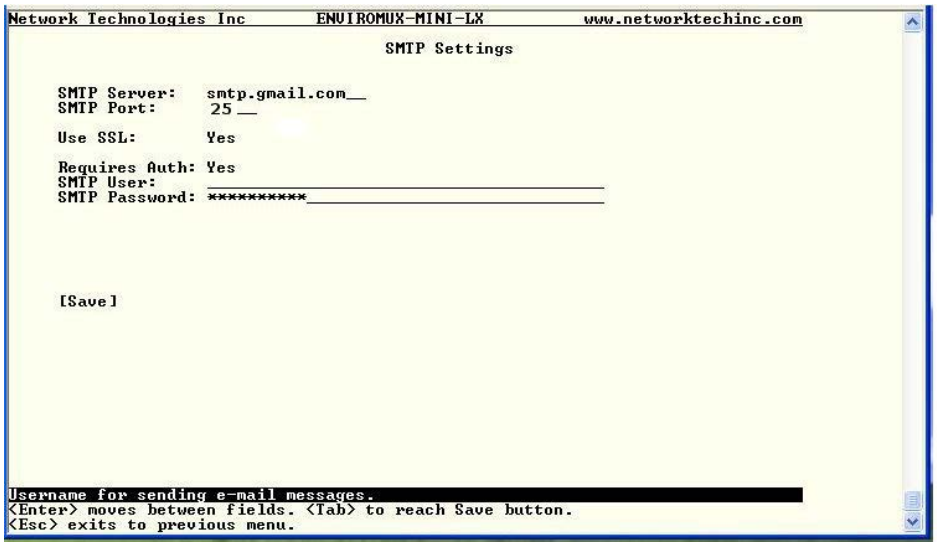


Figure 98- Text Menu-IPv6 Settings Menu

If IPv6 protocol will be used, change the mode to “Enabled” and apply valid in addresses for the IPv6 address and gateway. To use a 6to4 tunnel, change “Disabled” to “Enabled” and apply valid local and remote addresses.

SMTP Settings

The SMTP Settings menu contains the SMTP server settings for the ENVIROMUX.



Note: The SMTP server port number is shown in Figure 99 as "25". This is a common port number assigned, but not necessarily the port number assigned to your SMTP server. For SMTP servers that support SSL, the common port number is 465.

Figure 99- Text Menu-SMTP Server Settings

SMTP Settings	Description
SMTP Server	Enter a valid SMTP server name (e.g. yourcompany.com)
Port	Enter a valid port number (default port is 25)
Use SSL	Change to “Yes” if the SMTP server supports SSL
Requires Authentication	Change to “Yes” if the SMTP server requires authentication to send email
SMTP User	Enter a valid username to be used by the ENVIROMUX to send emails
SMTP Password	Enter a valid password assigned to the ENVIROMUX username

SNMP Settings

The SNMP Settings menu contains the SNMP server settings for the ENVIROMUX.

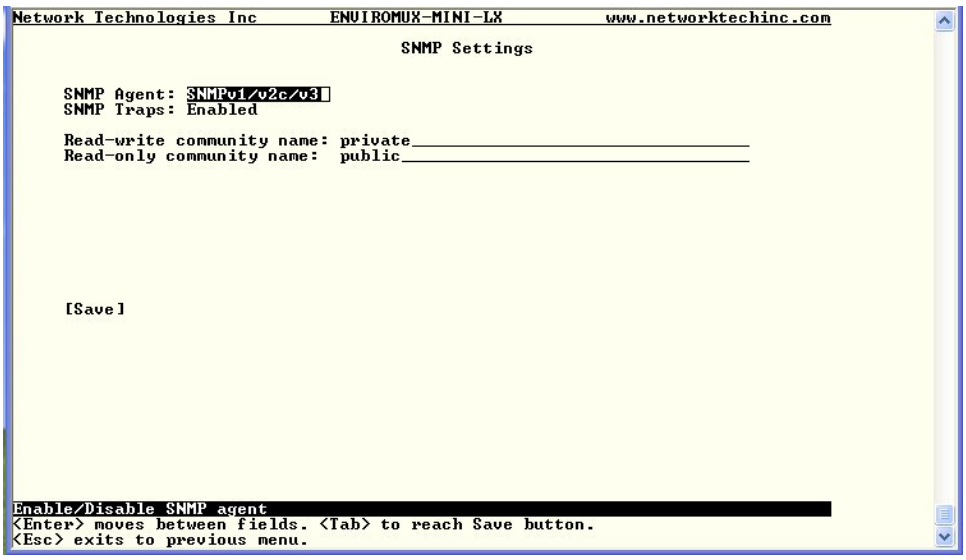


Figure 100- Text Menu-SNMP Server Settings

SNMP Settings	
Enable SNMP agent	Choose between v1/v2c, v3 , and v1/v2c/v3 SNMP agent version settings
Enable SNMP traps	Change to “Enabled” to enable SNMP traps to be sent
Read-write community name	Enter applicable name (commonly used- “private”) **(not applicable as of this printing)**
Read-only community name	Enter applicable name (commonly used- “public”)

Read-Only Community Name

The SNMP Read-only community name enables a user to retrieve "read-only" information from the ENVIROMUX using the SNMP browser and MIB file. This name must be present in the ENVIROMUX and in the proper field in the SNMP browser.

Read-Write Community Name

(not applicable as of this printing)

The SNMP Read-Write community name enables a user to read information from the ENVIROMUX and to modify settings on the ENVIROMUX using the SNMP browser and MIB file. This name must be present in the

ENVIROMUX and in the proper field in the SNMP browser.

Miscellaneous Service Settings

The Misc. Service Settings menu contains selections to configure services running on the ENVIROMUX.

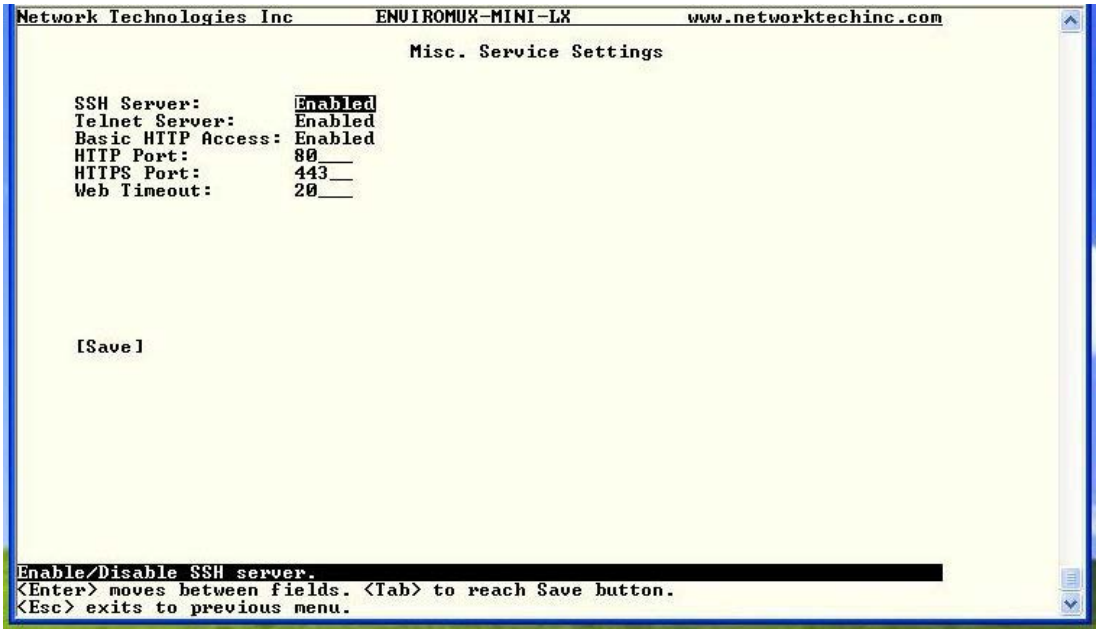


Figure 101- Text Menu-Misc. Service Settings menu

Server Settings	
Enable SSH	Enable this to allow access to the ENVIROMUX via SSH
Enable Telnet	Enable this to allow access to the ENVIROMUX via Telnet **The default setting is Disabled.**
Enabe HTTP access	Enable this to allow access to the ENVIROMUX via standard (non-secure) HTTP requests
HTTP Port	Port to be used for standard HTTP requests
HTTPS Port	Port to be used for HTTPS requests
Web Timeout	Number of minutes after which idle web uses will be logged-out (enter 0 to disable this feature)

The administrator may assign a different HTTP Server Port than is used by most servers (80).

User Configuration

The User Configuration menu lists all configured user names of the ENVIROMUX. A maximum of 15 users (other than root) can be configured. From this screen the administrative user can add users, go to the user configuration page to edit a user's access to the ENVIROMUX, or delete a user from the list.

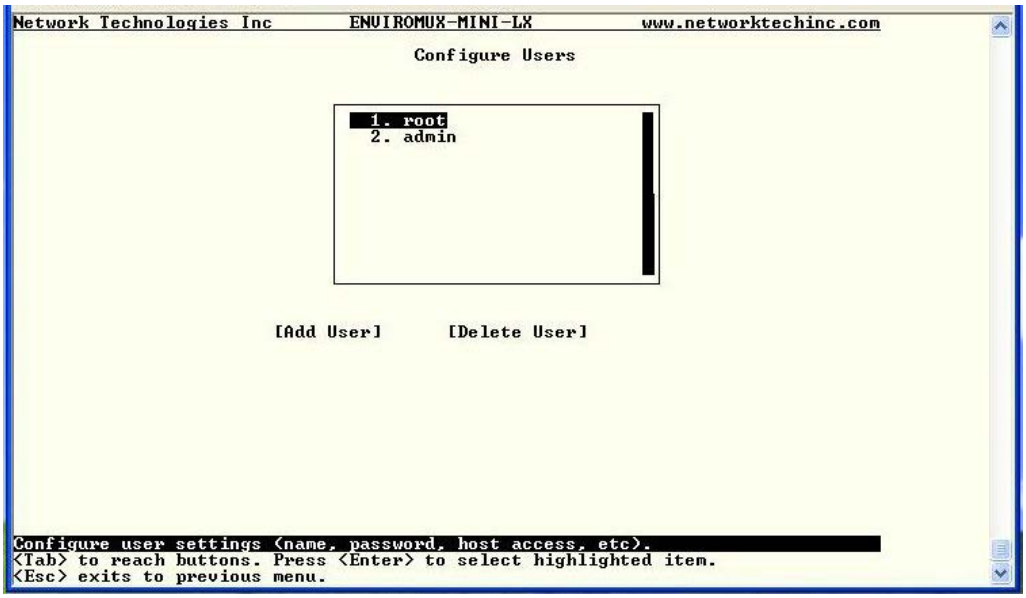


Figure 102- Text Menu-User Configuration

To add a user, Tab to "Add User" and press <**Enter**>.

To edit a user's configuration, select the listed username and press <**Enter**>

To delete a user and their configuration, select a listed username, Tab to "Delete User", and press <**Enter**>. You will be prompted for confirmation before deleting the user and configuration.

When adding a new user, you will be prompted to confirm the addition of the user. At that point, the Configure User menu will open a user settings list with the username "user*x*" assigned, where x = the next consecutive number (up to 15) based on the quantity of users in the list (other than the root user).

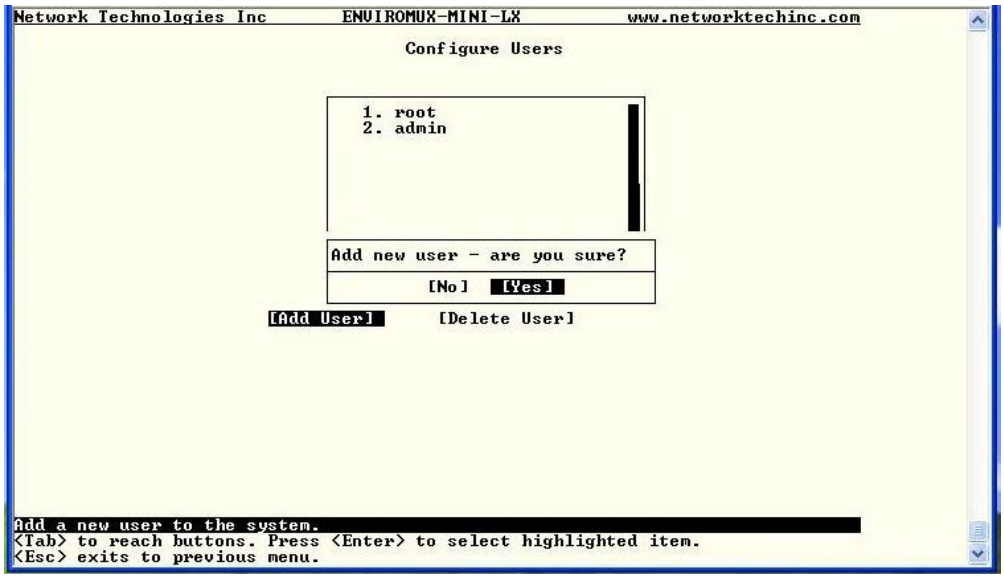


Figure 103- Text Menu-Confirm to add new user

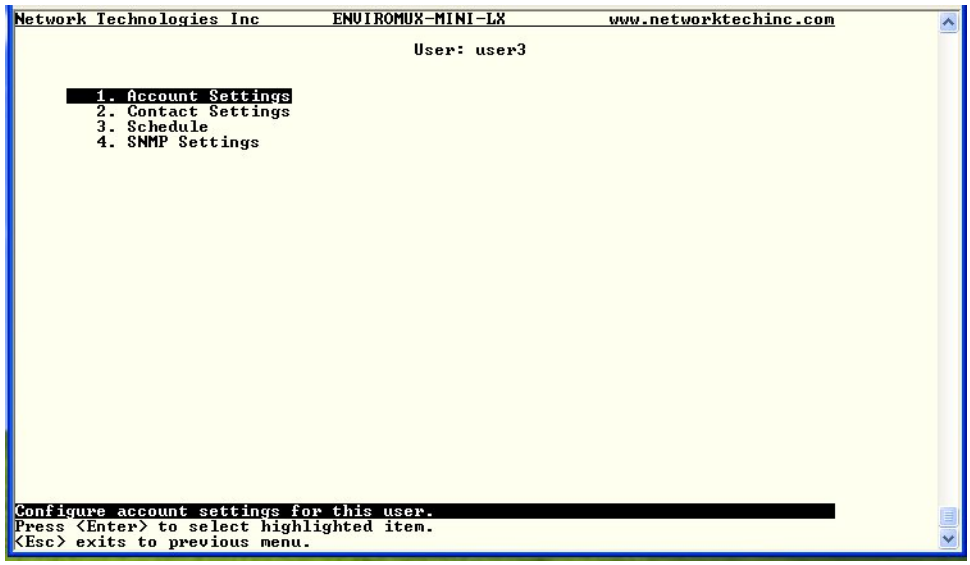


Figure 104- Text Menu-Configuration List for User

User Account Settings

Select "Account Settings" from the list and press <**Enter**>. A menu with the account settings for that specific user will open where you can either leave the name as "userx", or change it. With the name assigned, fill in the remaining information as needed.

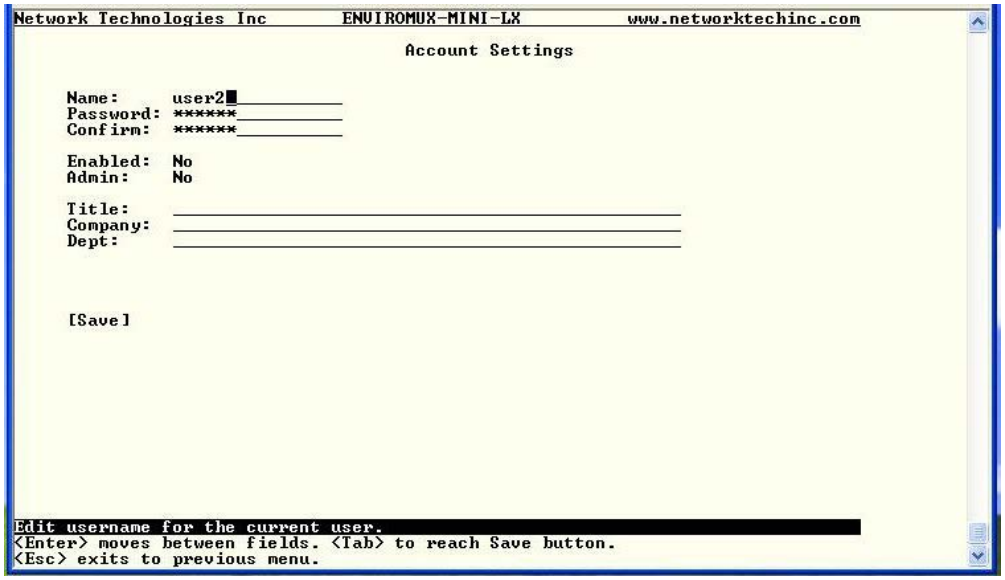


Figure 105- Text Menu-User Account Settings

Account Settings	Description
Username	Enter the desired username for this user
Password	Enter a password that a user must use to login to the system **A password must be assigned for the user's login to be valid** **Passwords must be at least 1 keyboard character.**
Confirm	Re-enter a password that a user must use to login to the system

Account Settings	Description
Enabled	Change to “Yes” to enable this user to access the ENVIROMUX
Admin	Change to “Yes” if this user should have administrative privileges
Title	Enter information as applicable (optional)
Department	Enter information as applicable (optional)
Company	Enter information as applicable (optional)

More about User Privileges

The root user (or any user with administrator rights) can change the root password and configure how the root user will receive alert messages. Users with administrative rights can change all configuration settings except for the root user name.

User Contact Settings

Select “Contact Settings” from the list and press <**Enter**>. A menu with the contact settings for that specific user will open.

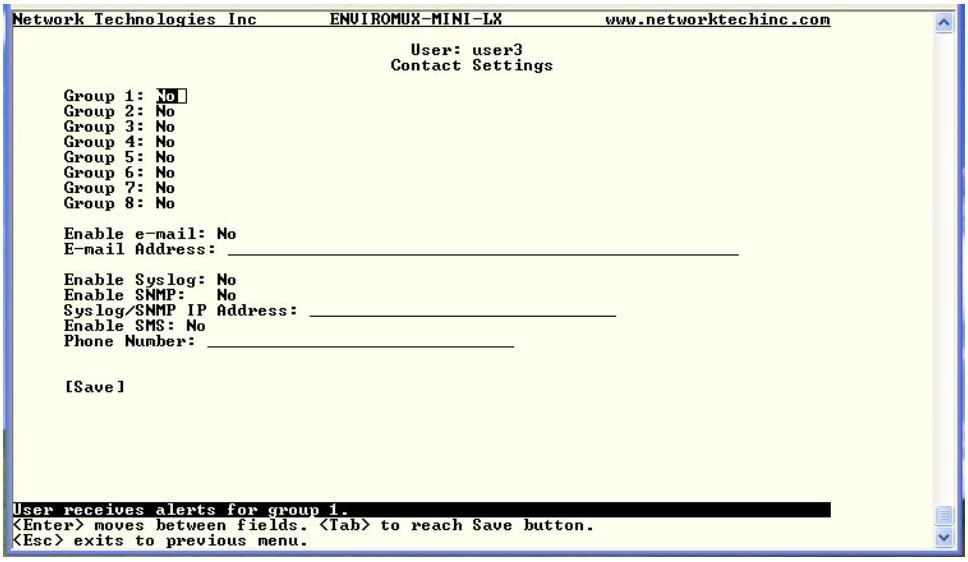


Figure 106- Text Menu-User Contact Settings

Contact Settings	
Group 1	Change to “Yes” if the user should receive messages from sensors, IP devices and accessories in Group 1
Group 2	Change to “Yes” if the user should receive messages from sensors, IP devices and accessories in Group 2
Enable Email	Change to “Yes” if the user should receive messages via email
Email address	Enter a valid email address if the user should receive email alert messages
Syslog alerts	Change to “Yes” if the user should receive alerts via syslog messages
SNMP traps	Change to “Yes” if the user should receive alerts via SNMP traps
Syslog/SNMP IP address	Enter a valid syslog/SNMP IP address for the user to receive syslog/SNMP messages
SMS	Change to “Yes” if the user should receive alerts via SMS messages
Phone Number	Enter a valid phone number for the user to receive SMS messages

Press <**Tab**> to highlight **Save** and press <**Enter**> to save before pressing <**Esc**> to exit.

User Activity Schedule

Select “Schedule” from the list and press <**Enter**>. A menu with the user activity settings for that specific user will open.

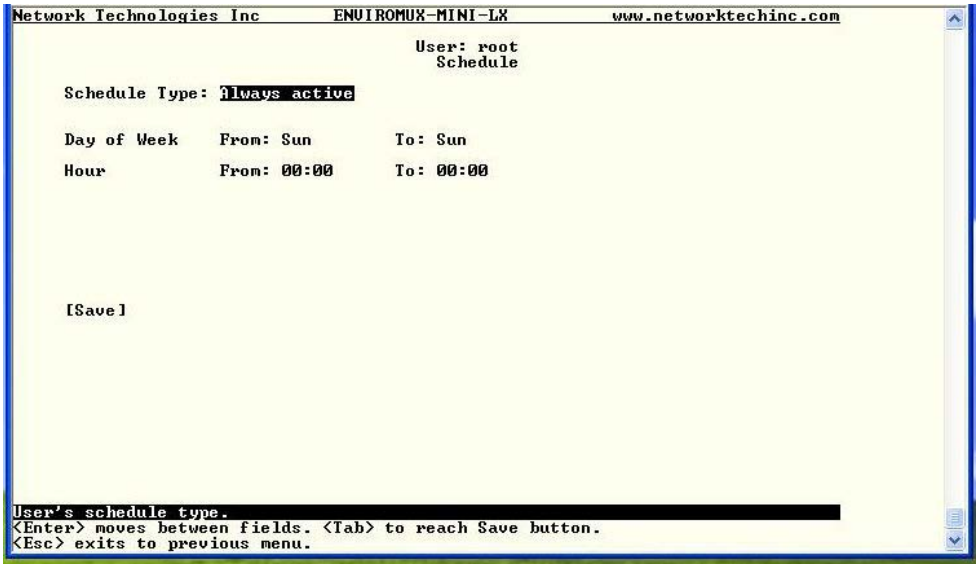


Figure 107- Text Menu-User Activity Schedule

Schedule Settings	
Schedule Type	**Always active**- user will receive messages at all hours of each day **Active during defined times**- user will only receive alert messages during times as outlined below
Day of Week-From:	First day of the week the user should begin receiving messages
Day of Week-To:	Last day of the week the user should receive messages
Hour From:	First hour of the day the user should begin receiving messages
Hour To:	Last hour of the day the user should receive messages

User SNMP Settings

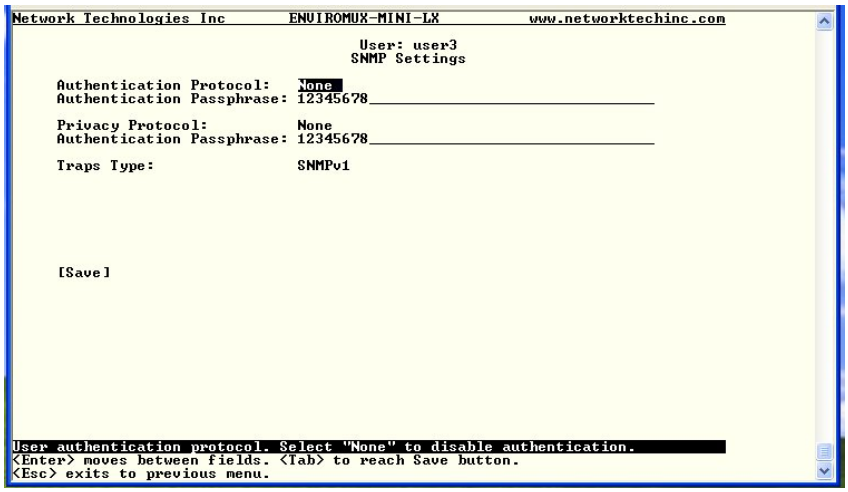


Figure 108-Text Menu- SNMP User Settings

Security settings can be configured within each user configuration if the SNMP protocol has been selected for use (page 89).

Settings	
Authentication Protocol	Choose between MD5 or SHA to require authentication, or none to disable it. This only needs to be changed from “none” if SNMPv3 is used.
Privacy Protocol	Choose between DES or AES to encrypt SNMP readings or traps or none to disable encryption. If encryption is enabled, then the Authentication Protocol must also be set at “MD5” or “SHA”.
Authentication Passphrase	Assign the passphrase to be used to enable the receipt of SNMP messages. This only needs to be changed from “none” if SNMPv3 is used.
Privacy Passphrase	Assign the passphrase to be used to open and read readings or alert messages received via SNMPv3
Traps Type	Choose which format traps should be received in, SNMP v1, v2c, or v3

After changing any settings in the user profile, press “Apply”.

Security Configuration

The Security Configuration menu provides two submenus for setting local versus LDAP authentication methods and for applying IP filtering rules to prevent unwanted access to the ENVIROMUX.

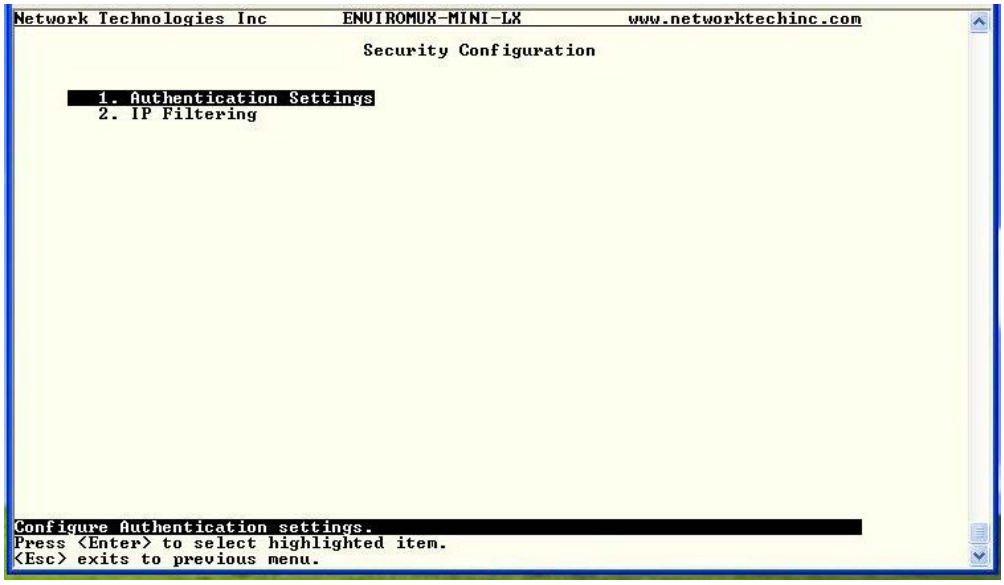


Figure 109- Text Menu-Security Configuration

Authentication Settings

Security in the ENVIROMUX can be managed one of two ways; through the local settings (passwords assigned in user settings on page 91) or through an LDAP server. If security is configured to use LDAP mode, then the passwords for users must be those found on a configured LDAP server.

Select "Authentication Settings" from the list and press <**Enter**>. A menu providing an option to either user Local authentication or LDAP mode. When in LDAP mode, usernames on the LDAP server must match those in the user settings of the ENVIROMUX or access will be denied.

Note: When the root user logs with the ENVIROMUX in LDAP mode, if the LDAP server is not responding, local authentication will be tried.

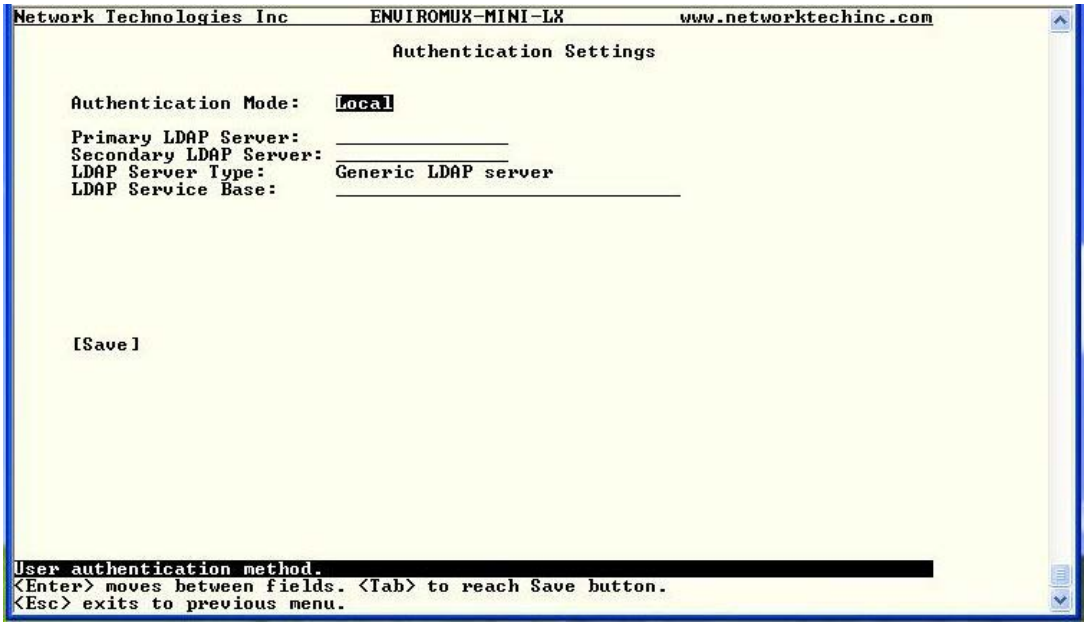


Figure 110- Text Menu-Authentication Settings

User Authentication	
Mode	Select Local to use authentication based on passwords in the ENVIROMUX user configuration Select LDAP to use authentication based on passwords in an LDAP server
Primary LDAP Server	Enter Hostname or IP address of Primary LDAP Server
Secondary LDAP Server	Enter Hostname or IP address of Secondary LDAP Server (optional)
LDAP Server Type	Tab to choose from the following: Generic LDAP server Novell Directory server Microsoft Active Directory
LDAP Service Base	Enter the Base DN for users (ex: ou=People,dc=mycompany,dc=com)

Even though LDAP authentication is being used, each user must also have a local account. User permission level is established by the local account.

Press <**Tab**> to highlight **Save** and press <**Enter**> to save before pressing <**Esc**> to exit.

IP Filtering

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

Up to 16 IP Filtering rules can be defined to protect the ENVIROMUX 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.

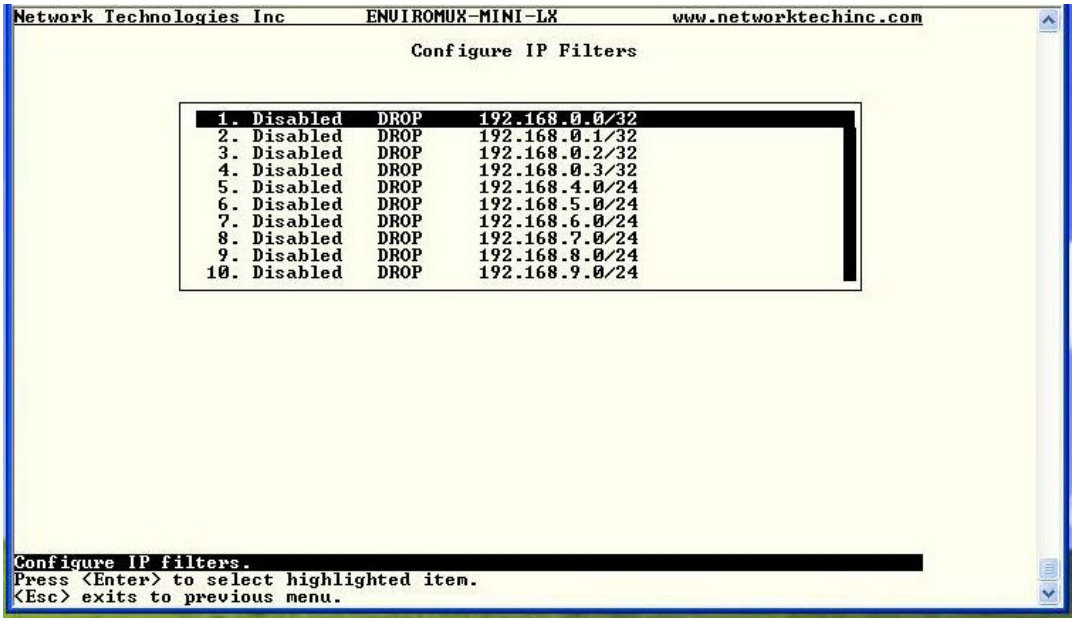


Figure 111- Text Menu-IP Filtering

To configure an IP Filter, select an IP Filter rule from the list and press <**Enter**>.

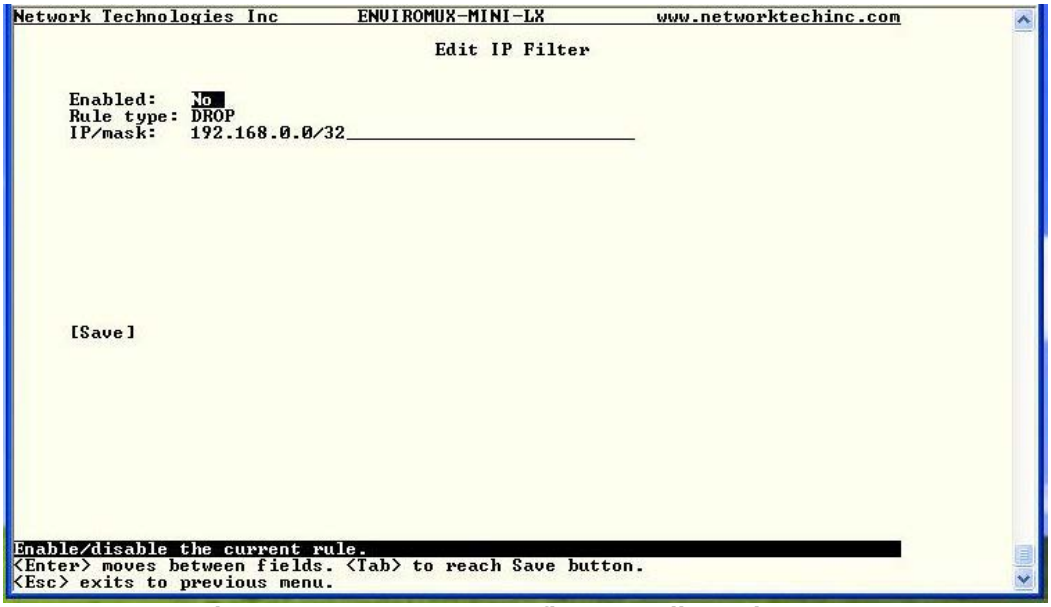


Figure 112- Text Menu-Configure IP Filter rule

The most common approach is to only allow “white-listed” 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:

(Rule 1)

```
Enabled: Yes
Rule type: ACCEPT
IP/mask:   192.168.1.100
```

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

(Rule 16)

```
Enabled: Yes
Rule type: DROP
IP/mask:   0.0.0.0/0
```

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).

Press <**Tab**> to highlight **Save** and press <**Enter**> to save before pressing <**Esc**> to exit.

Event and Data Logs

Under the Event and Data Logs menu find 4 submenus for viewing a log record of the events monitored by the ENVIROMUX and configuring how the ENVIROMUX will handle reaching the capacity of those logs.

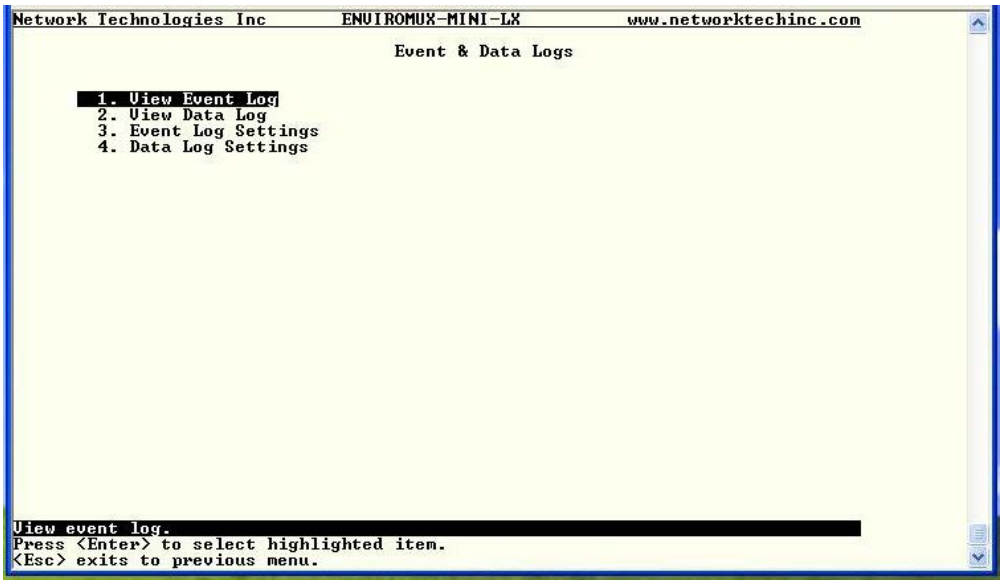


Figure 113- Text Menu-Event & Data Logs

View Event Log

The Event Log provides the administrative user with a listing of many events that occur within the ENVIROMUX. The event log will record the date and time of:

- each ENVIROMUX startup,
- each user login and logout time,
- any time an unknown user tries to login,
- sensor and IP device alerts
- an alert handled by a user

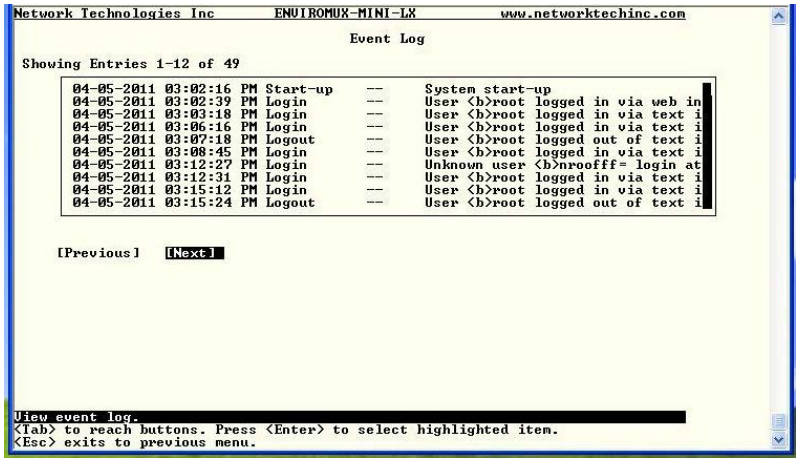


Figure 114- Text Menu-View Event Log

From the Event Log the administrative user can view the logs. In order to clear specific logs, download log entries, or clear the entire log, use the Web Interface (see page 62). To navigate between pages of logs, pres <**Tab**> to move between **Previous** and **Next** and press <**Enter**>.

View Data Log

The Data Log provides the administrative user with a listing of all the readings taken by the ENVIROMUX pertaining to the sensors and IP Devices being monitored. The data log will record the date and time of each reading.

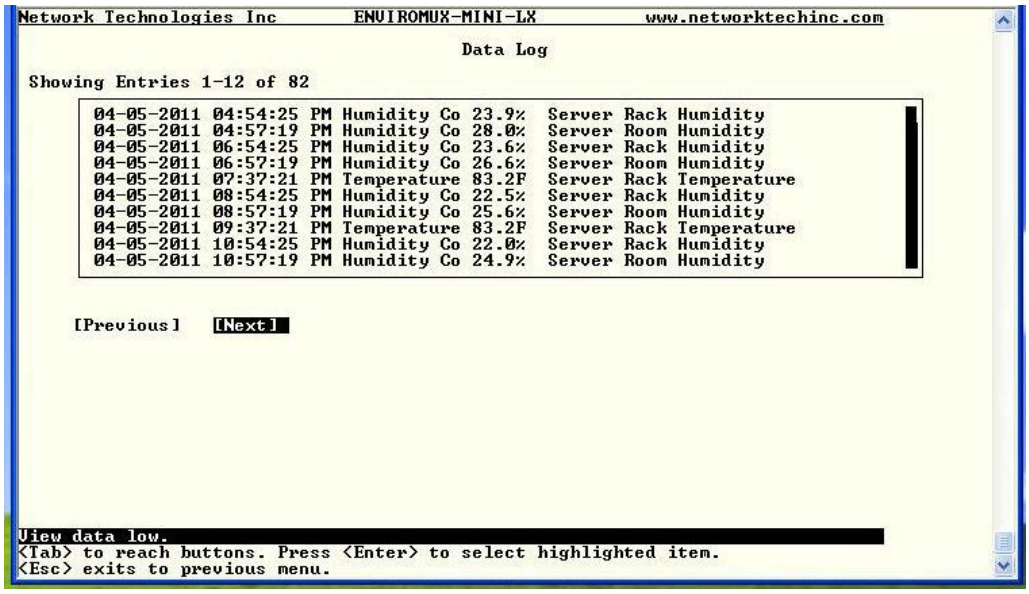


Figure 115- Text Menu-View Data Log

From the Data Log the administrative user can view the logs. In order to clear specific logs, download log entries, or clear the entire log, use the Web Interface (see page 63). To navigate between pages of logs, pres <**Tab**> to move between **Previous** and **Next** and press <**Enter**>.

Log Settings Menus

The Log Settings menus (Figure 116 and Figure 117) provide settings for how the ENVIROMUX will react when its Data and Event logs reach capacity.

The Event Log settings include a logging level that can be configured to log different amounts of information:

- Error : shows only system errors (like sending email failures or SMS)
- Alerts: shows recorded system errors and alert messages
- Info: In addition to all of the above, the log will show less relevant information: user login/logout for example

Each log can be assigned to a group and any user that receives messages from that group can be notified when capacity is being reached.

As a capacity overflow action the log can be set to either :

- Discontinue- stop logging information
- Clear and restart- delete all log entries and restart with new entries
- Wrap- continue logging but delete the oldest entries and new ones are recorded

The Data and/or Event log can be set to sent alerts to users via email, syslog, and/or SNMP traps once it has reached 90% of capacity, allowing them time to react.

The Data log can also be set to send log entries via email, syslog, or SNMP traps to users in addition to the entries it records internally. Enable Remote Logging for email, syslog, of SNMP as desired.

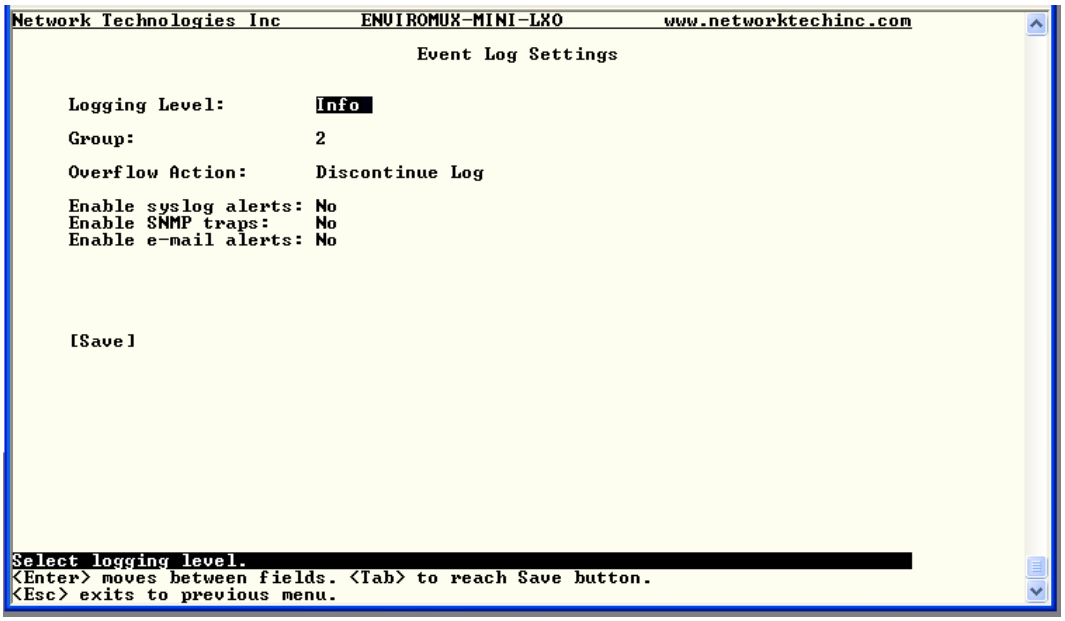


Figure 116- Text Menu-Event Log Settings

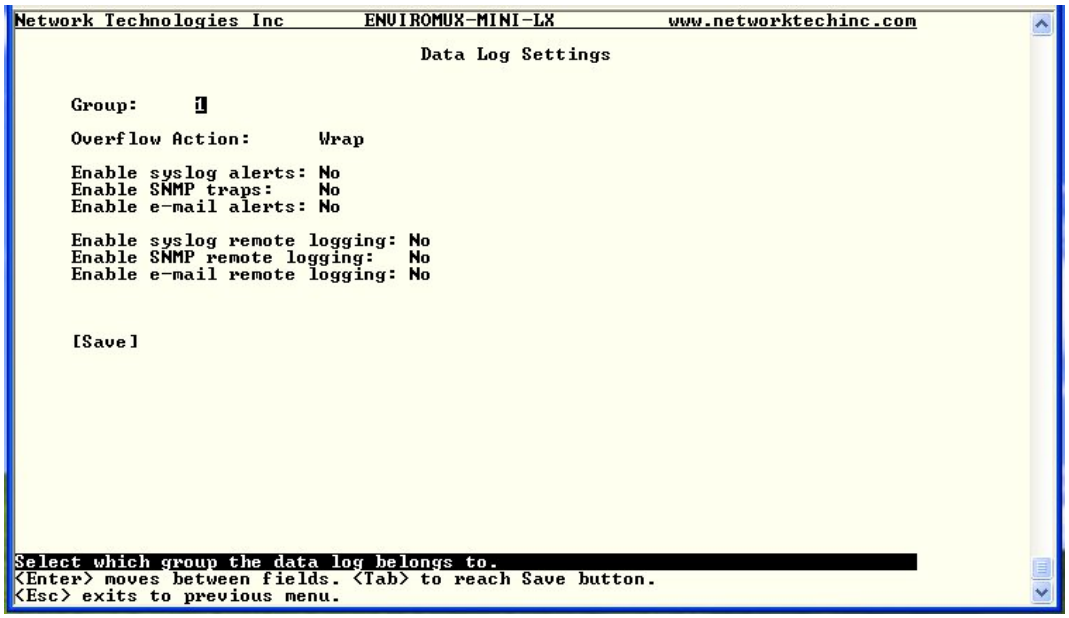


Figure 117-Text Menu-Data Log Settings

System Information

The System Information page lists current firmware, time, and network settings for the ENVIROMUX. It also lists the ENVIROMUX MAC address.

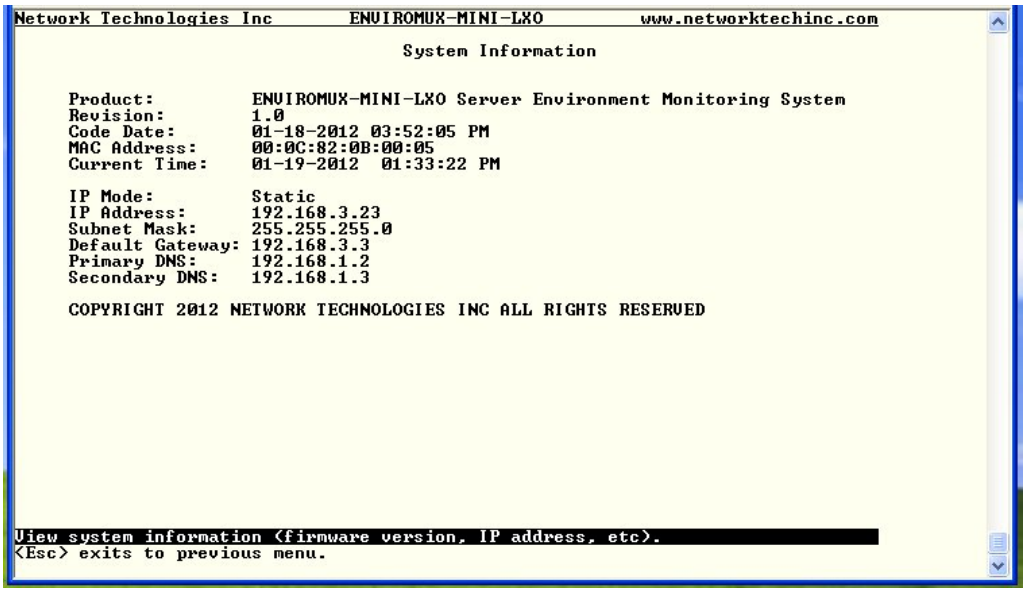


Figure 118-Text Menu-System Information

Reboot

From the Main Menu the administrative user can initiate a reboot of the ENVIROMUX. By highlighting "Reboot" and pressing <**Enter**> (or <**9**> and <**Enter**>), you will be prompted to confirm that you want to reboot the ENVIROMUX. Press <Enter> to cancel, or press the <**Tab**> or either <**arrow**> key to highlight "Yes" and <**Enter**> to reboot. The ENVIROMUX will reboot and a new connection must be initiated to reconnect, login, and resume operation.

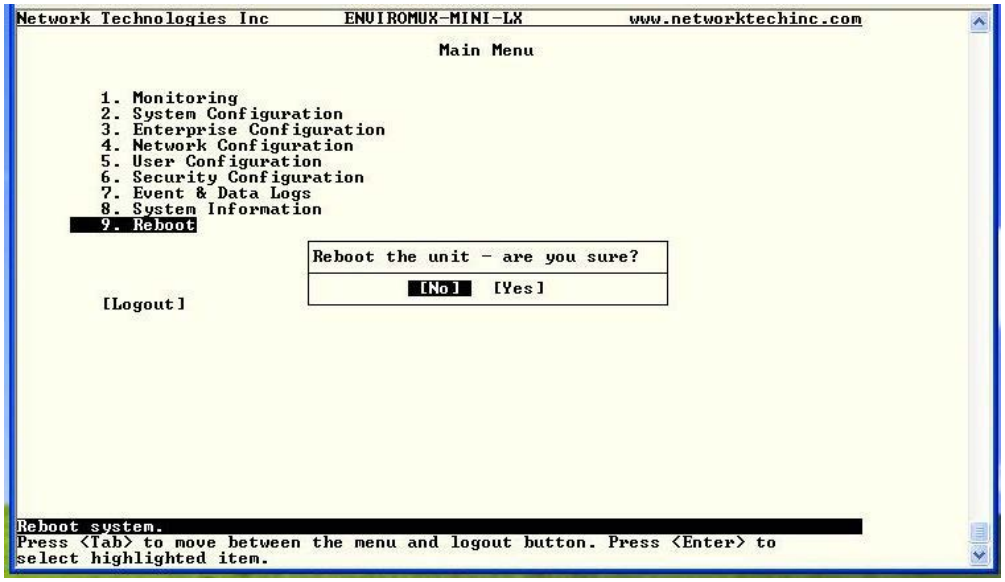


Figure 119- Text Menu-Reboot the ENVIROMUX

Text Menu for Non-Administrative Users

Users without administrative privileges are able to view sensors and IP Devices and edit their own account settings.

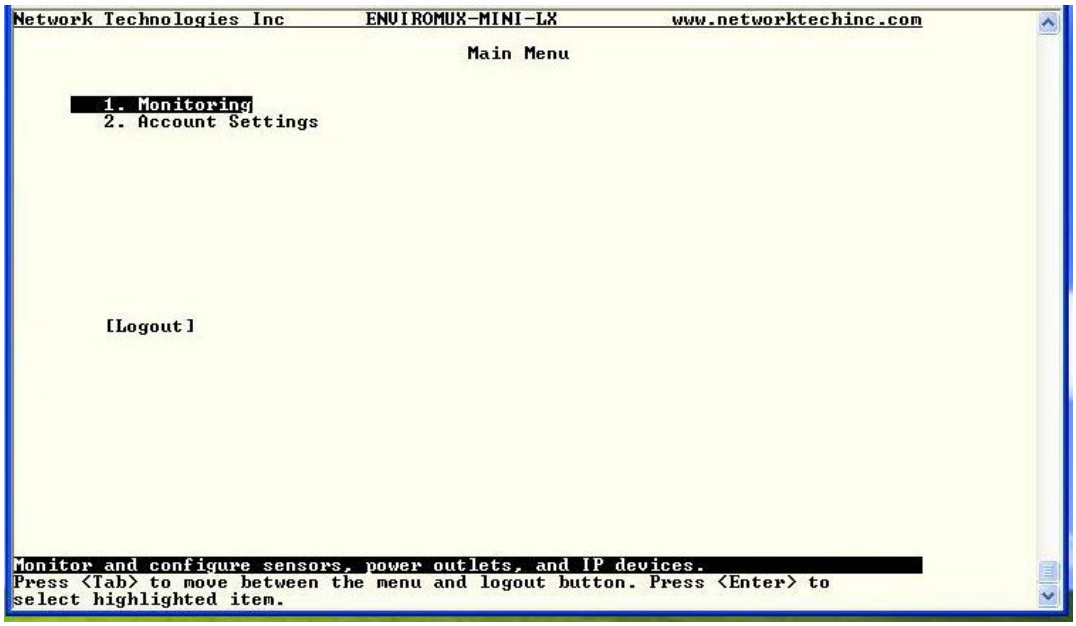


Figure 120- Text Menu-User Main Menu

Monitoring

The Monitoring menu lists 4 options for viewing the status of the items monitored by the ENVIROMUX.

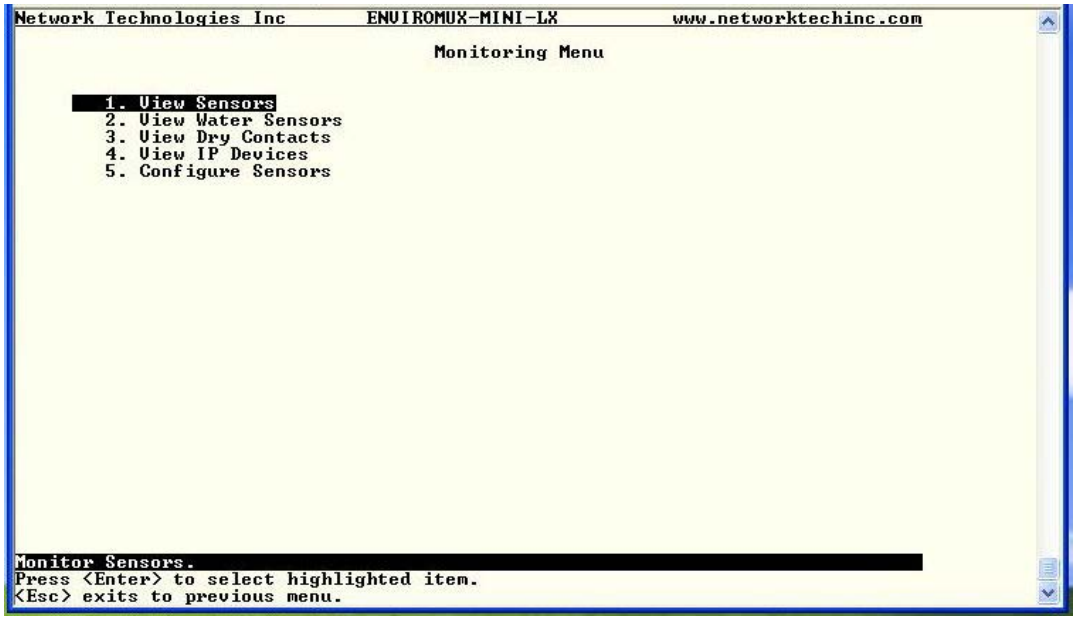


Figure 121-Text Menu-User Monitoring Menu

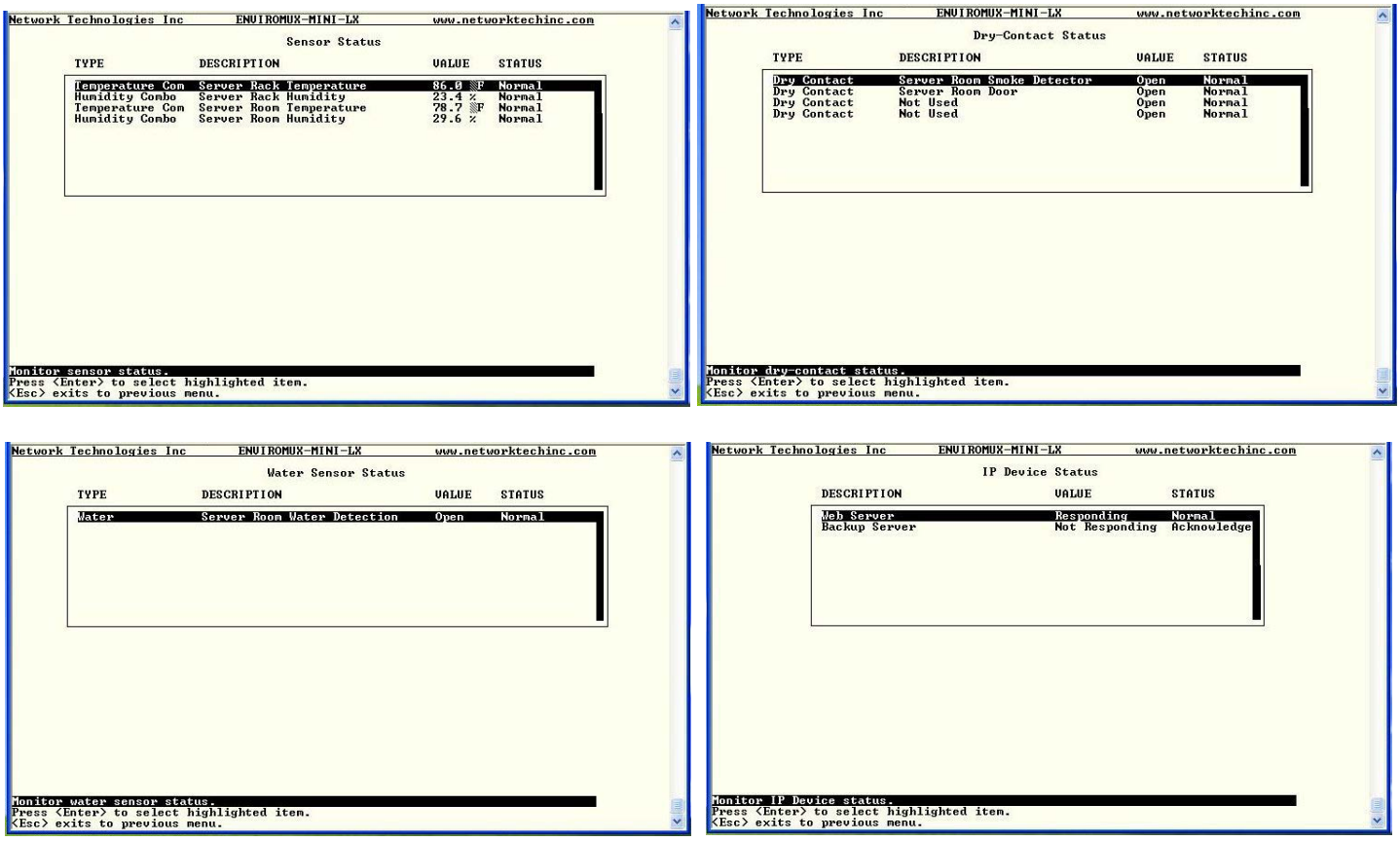


Figure 122- Text Menu-User accessible status menus

If a monitored item is in alert status, the non-administrative user can enter a response to it. By pressing the <**Enter**> key with the sensor selected, the user will have 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 (one example on page 28) elapses.

User Accessible Settings

The User without administrative privileges has access to setting for their own account.

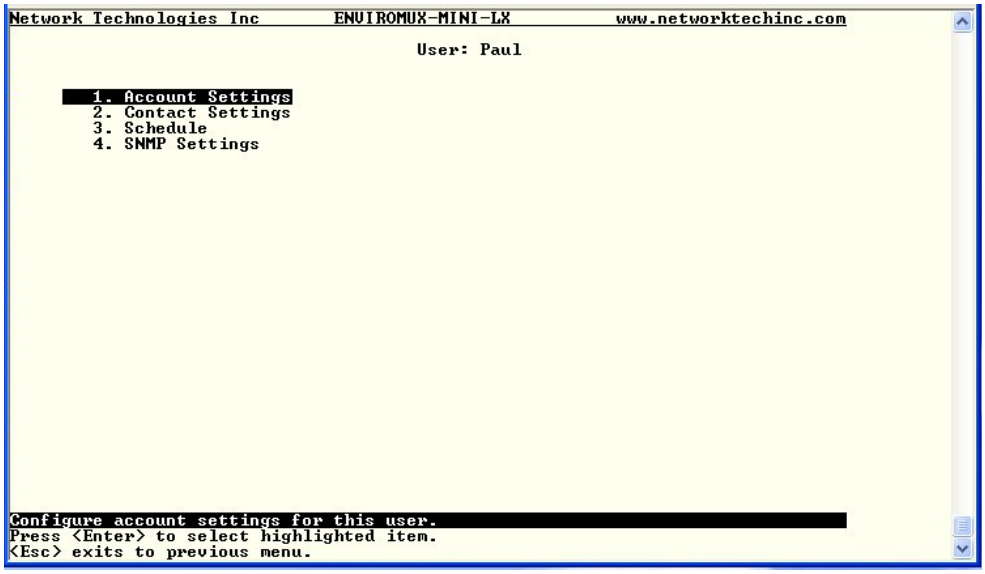


Figure 123- Text Menu-User Accessible Settings

Account Settings

Under Account Settings, the non-administrative user can edit their password, title, company, or department settings. Other settings are only accessible to the administrative user.

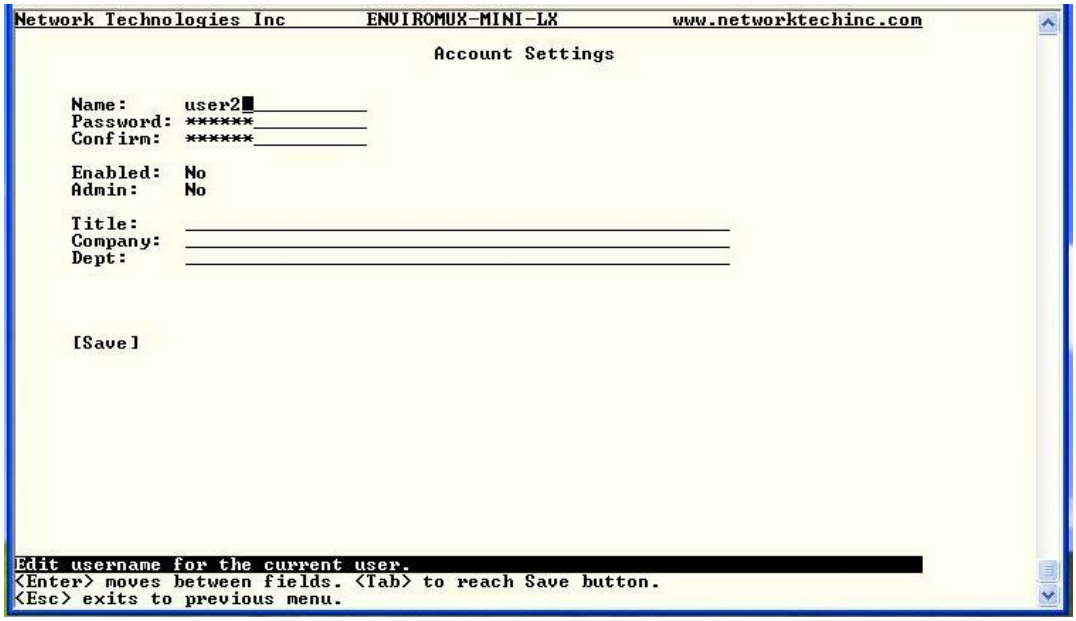


Figure 124- Text Menu-User Account Settings

Contact Settings

Under Contact Settings, the non-administrative user can decide which sensor group messages they will receive and how.

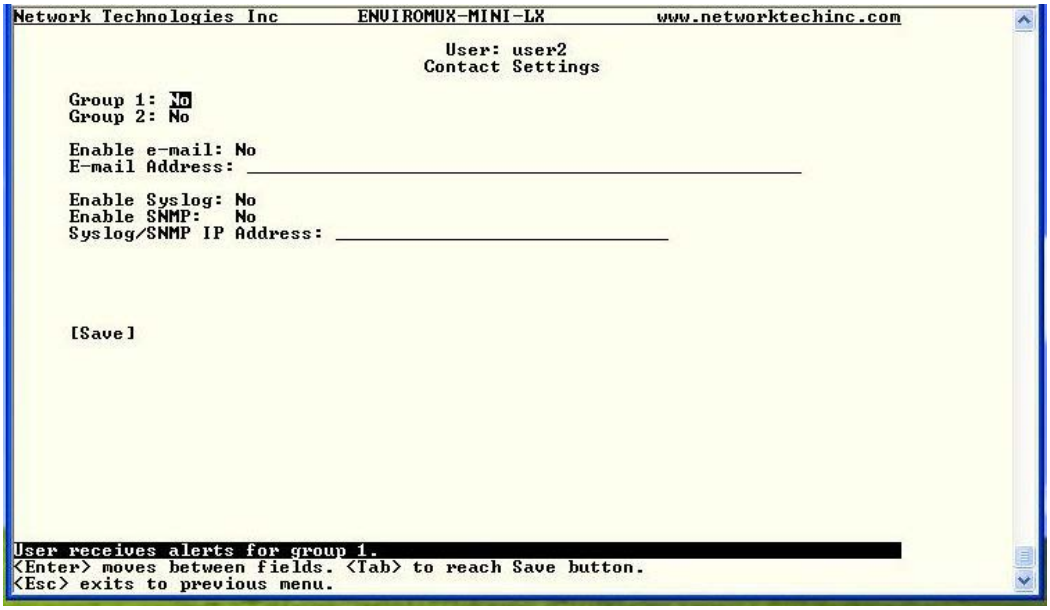


Figure 125- Text Menu-User Contact Settings

Contact Settings	
Group x	Change to “Yes” to receive messages from sensors, IP devices and accessories in any Group that sensors have been assigned to
Enable Email	Change to “Yes” to receive messages via email
Email address	Enter a valid email address to receive email alert messages
Syslog alerts	Change to “Yes” to receive alerts via syslog messages
SNMP traps	Change to “Yes” to receive alerts via SNMP traps
Syslog/SNMP IP address	Enter a valid syslog/SNMP IP address to receive syslog/SNMP messages

Press <**Tab**> to highlight **Save** and press <**Enter**> to save before pressing <**Esc**> to exit.

Schedule

Under Schedule, the non-administrative user can edit their activity schedule to control when messages should be sent to them.

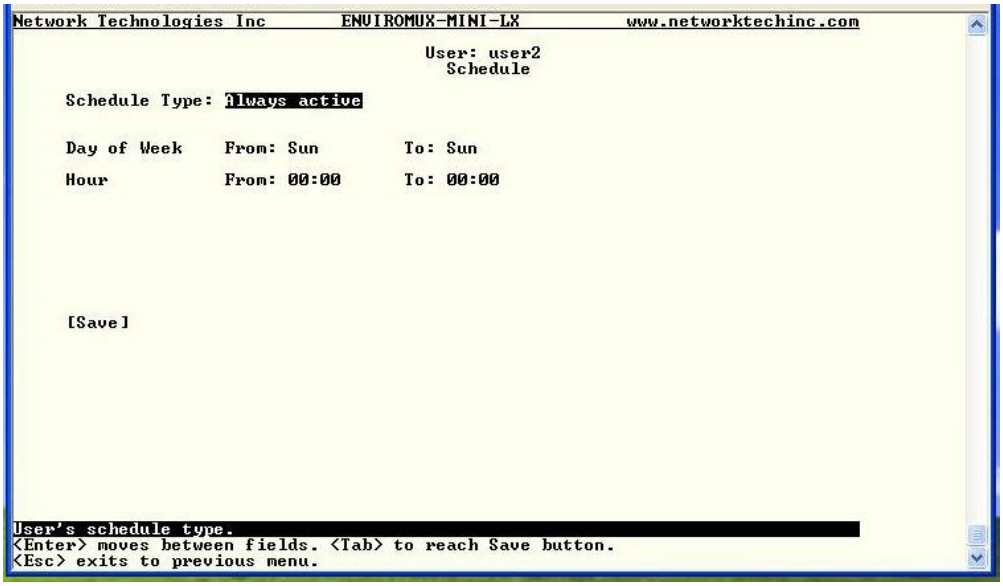


Figure 126- Text Menu-User Activity Schedule

Schedule Settings	
Schedule Type	**Always active**- user will receive messages at all hours of each day **Active during defined times**- user will only receive alert messages during times as outlined below
Day of Week-From:	First day of the week the user should begin receiving messages
Day of Week-To:	Last day of the week the user should receive messages
Hour From:	First hour of the day the user should begin receiving messages
Hour To:	Last hour of the day the user should receive messages

Press <**Tab**> to highlight **Save** and press <**Enter**> to save before pressing <**Esc**> to exit.

SNMP Settings

Under SNMP Settings, the non-administrative user can edit the settings required to receive SNMP messages.

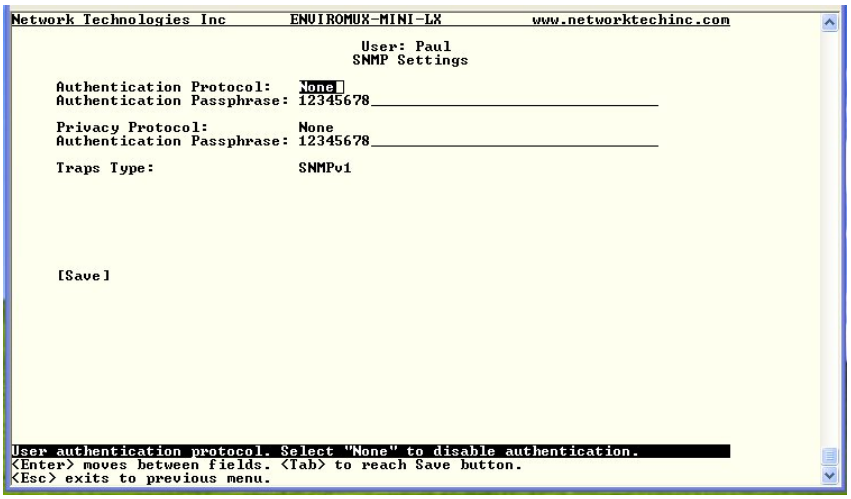


Figure 127- Text Menu-User SNMP Settings

Security settings can be configured within each user configuration if the SNMP protocol has been selected for use (page 89).

Settings	
Authentication Protocol	Choose between MD5 or SHA to require authentication, or none to disable it
Privacy Protocol	Choose between DES or AES to encrypt SNMP readings or traps or none to disable encryption. If encryption is enabled, then the Authentication Protocol must also be set at “MD5” or “SHA”
Authentication Passphrase	Assign the passphrase to be used to enable the receipt of SNMP messages
Privacy Passphrase	Assign the passphrase to be used to open and read readings or alert messages received via SNMP

After changing any settings in the user profile, press “Apply”.

If any changes are made to the user’s SNMP Settings, the ENVIROMUX must be rebooted (page 54) before they will take effect. If other users’ settings need to be changed, the reboot can be done after all users’ settings are complete.

SYSTEM RESET BUTTON

A System Reset push-button is on the front-panel and is recessed from the panel to prevent accidental use of the button. Pressing the System Reset button will cause the ENVIROMUX to restart, just as if it were power-cycled. A momentary press of the System Reset push-button will activate this function. The reset button can be used at any time.

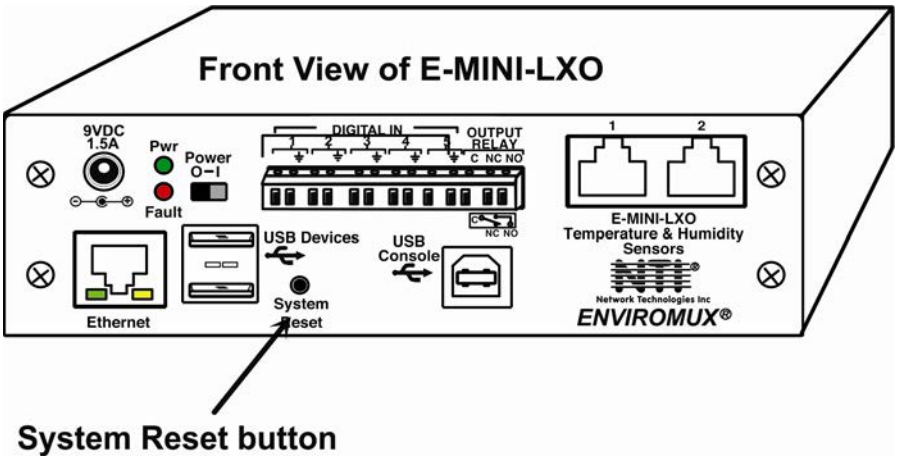


Figure 128- Location of Reset buttons

USB PORTS

The ENVIROMUX are each equipped with a USB Type A female ports for connection of a USB flash drive and a GSM modem (page 19) for receiving alert messages via SMS. The ports are compatible with USB 2.0 Full Speed flash drives. When enabled (page 64) and with the USB flash drive connected, the Event and Data Logs will be written to a text file on the flash drive in addition to the memory in the ENVIROMUX. When a modem is connected (page 19), it will automatically be sensed by the ENVIROMUX (page 40).

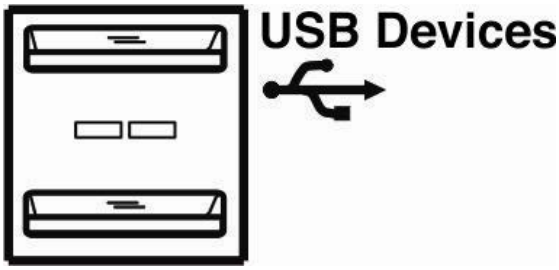


Figure 129- USB Flash Drive and GSM modem ports

MOBILE SUMMARY PAGE

The user can login to the ENVIROMUX through the browser on a smart phone or similar device to view a Summary Page for the sensor status (below). To login, type the current IP address of the ENVIROMUX into the address bar of the browser (default IP address used in the example below):

http://192.168.1.23/

Note: The ENVIROMUX must have a public accessible IP address for this to work or your browsing device must connected to the same local network as the ENVIROMUX.

Note: If the HTTP Server Port number is changed (page** Error! Bookmark not defined.**) from port 80 (default), then the port number will need to be added to the IP address (i.e. if the port number is changed to 95, then the IP address would be http://192.168.1.23:95)

A log in prompt requiring a username and password will appear:

Username = root

Password = nti

(lower case letters only)

Note: usernames and passwords are case sensitive

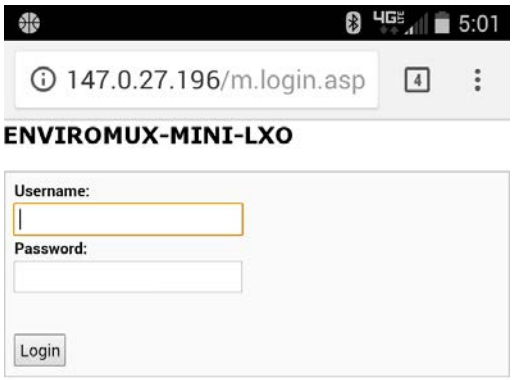


Figure 130- Mobile Login page

With a successful login, a screen similar to the following will appear. This is the only information that can be accessed through the interface. Select "**Refresh**" to refresh the information on the display. Select "**Log out**" when you are finished viewing the information. For access to the complete web interface, select "**Full Version**".

Note: The display will refresh automatically every 15 seconds

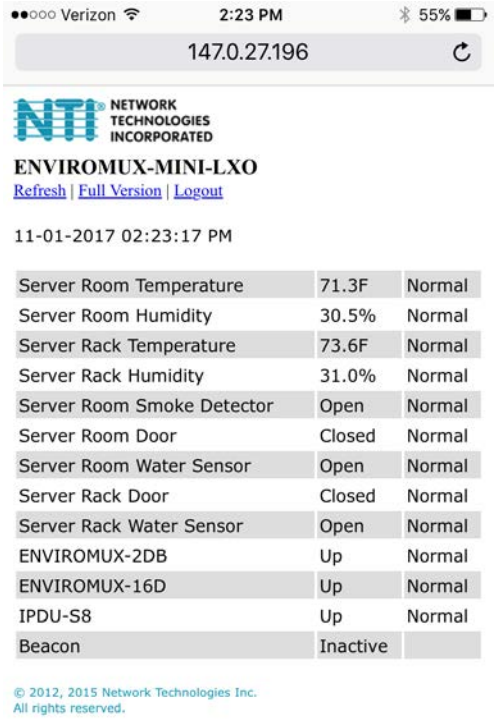


Figure 131- Mobile Summary page

PORT ASSIGNMENTS

Here are the default ports used by the ENVIROMUX:

- 80 HTTP
- 443 HTTPS
- 22 SSH
- 23 Telnet
- 161 SNMP (machine configuration & sensor data)
- 162 SNMP (traps)
- 514 SYSLOG

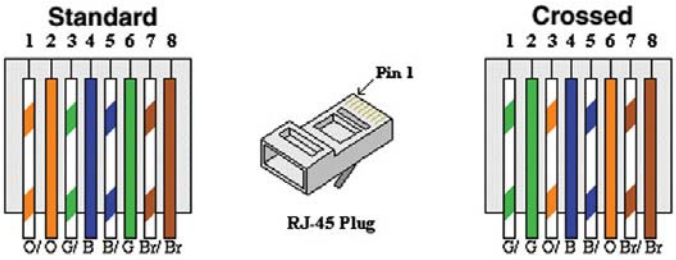
The HTTP and HTTPS port numbers may be changed by the administrator. If they are changed, contact the system administrator for the new assignments.

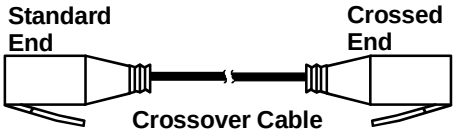
WIRING METHODS

PC-to ENVIROMUX Crossover Cable

In order to make a direct connection between a PC and the ETHERNET connector of the ENVIROMUX, a crossover cable must be used. The cable is made with CAT5 cable terminated with RJ45 connectors and wired according to the chart below.

Pin assignment at Standard End	Wire Color	Pin assignment at Crossed End
1	White/Orange	3
2	Orange	6
3	White/Green	1
4	Blue	4
5	White/Blue	5
6	Green	2
7	White/Brown	7
8	Brown	8

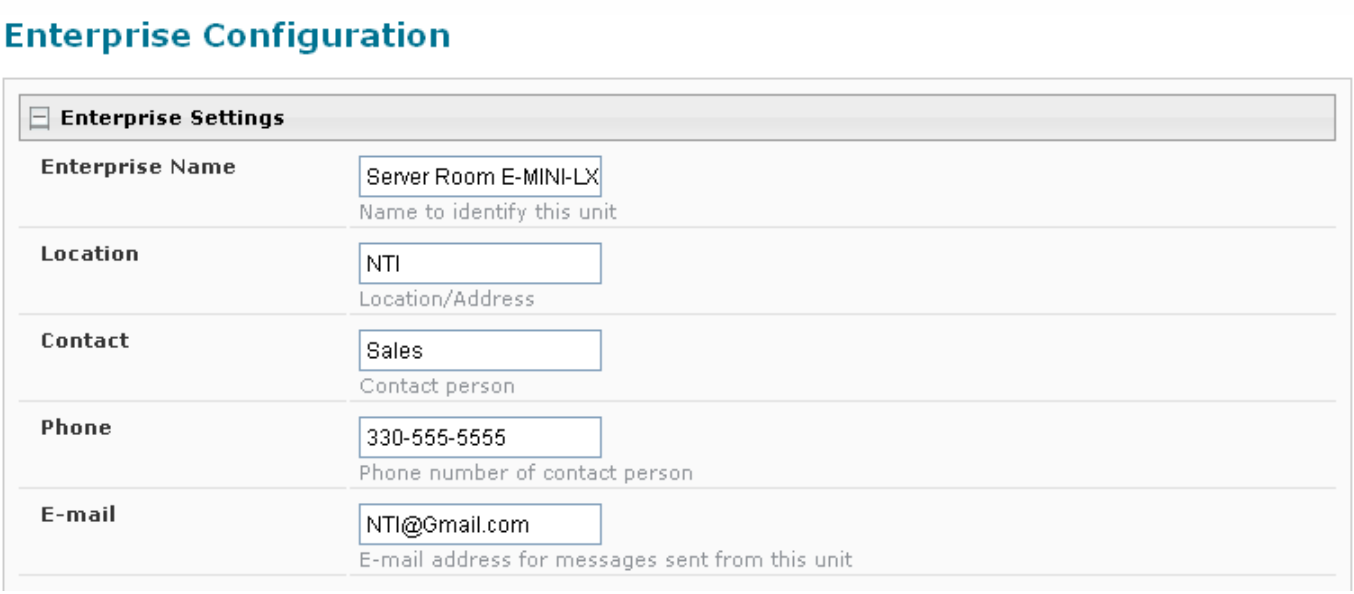




HOW TO SETUP EMAIL

Use this guide to assist in the configuration of the ENVIROMUX to send email messages.

1. Apply a valid email address for the ENVIROMUX to the Enterprise Setup Page (see page 40).



Note: When authentication is required (check your email server requirements) the Username and Password applied on the Network Configuration page must be for the user's email address applied in the Enterprise Setup Page. If no authentication is required, the Username and Password fields can be left empty.

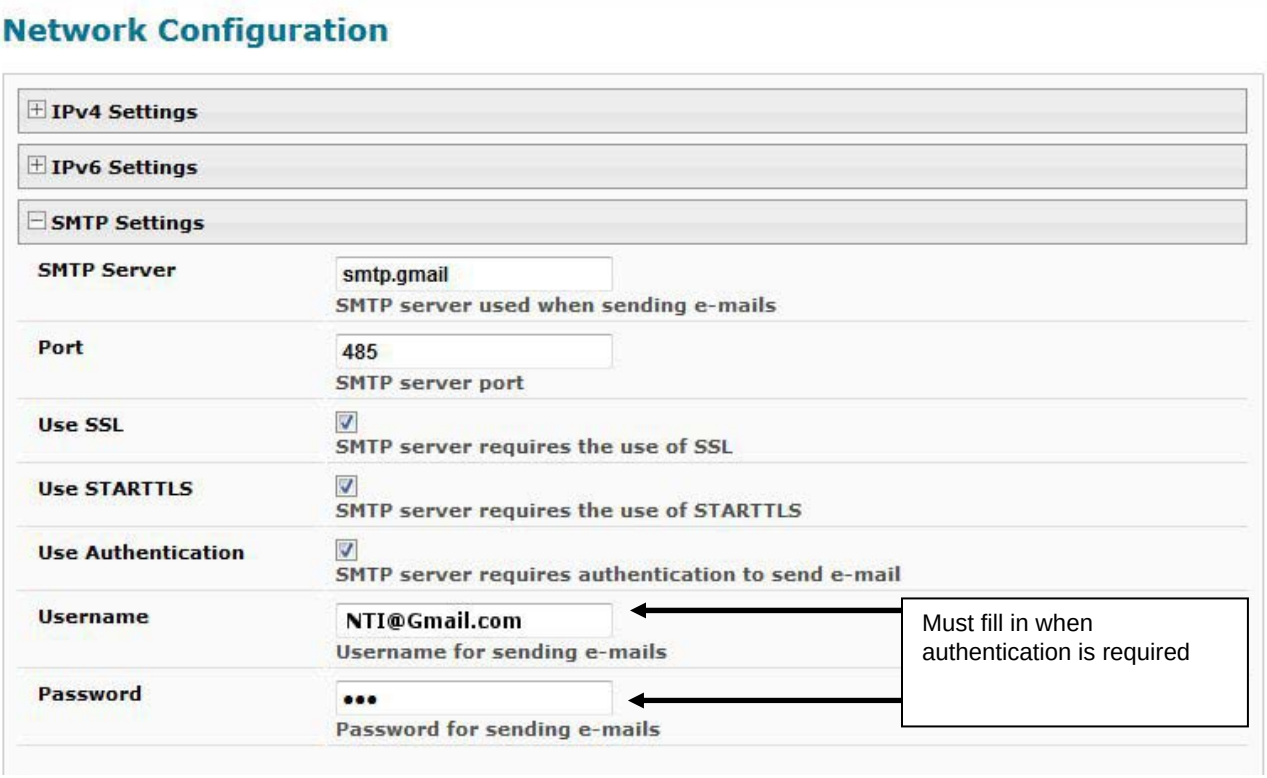


Figure 132- Example of configuration for Gmail server

2. Fill in Network Page (page 41) with valid information:

A. SMTP Server - check with your service provider as to what this should be.
Sometimes it is just the name of the provider (gmail.com), sometimes characters are added (mail.gmail.com, smtp.gmail.com, smtp-mail.gmail.com, etc)

B. The default port is 25. If authentication is required, a different port number may be required. Check with your service provider.

C. Check "Use SSL" if your SMTP server requires SSL, or "Use STARTTLS" if it requires TLS.

D. Check "Use Authentication" if SMTP server requires authentication to send emails.
a. If required, Enter "Username" and "Password" that has been assigned to ENVIROMUX. Make sure they apply to the email address applied in the Enterprise Setup Page.

Example: username@gmail.com Most servers (not all, check with your service provider) use just the characters in front of the "@" for your Username on the account. These, and only these characters should be entered into the "Username" block.

Note: Passwords are case sensitive. Be sure to apply the password exactly as it is required by the server.

3. Verify User is configured to receive notifications for at least one sensor group as well as having "E-Mail Alerts" selected and a valid E-Mail address to send the notifications to entered.

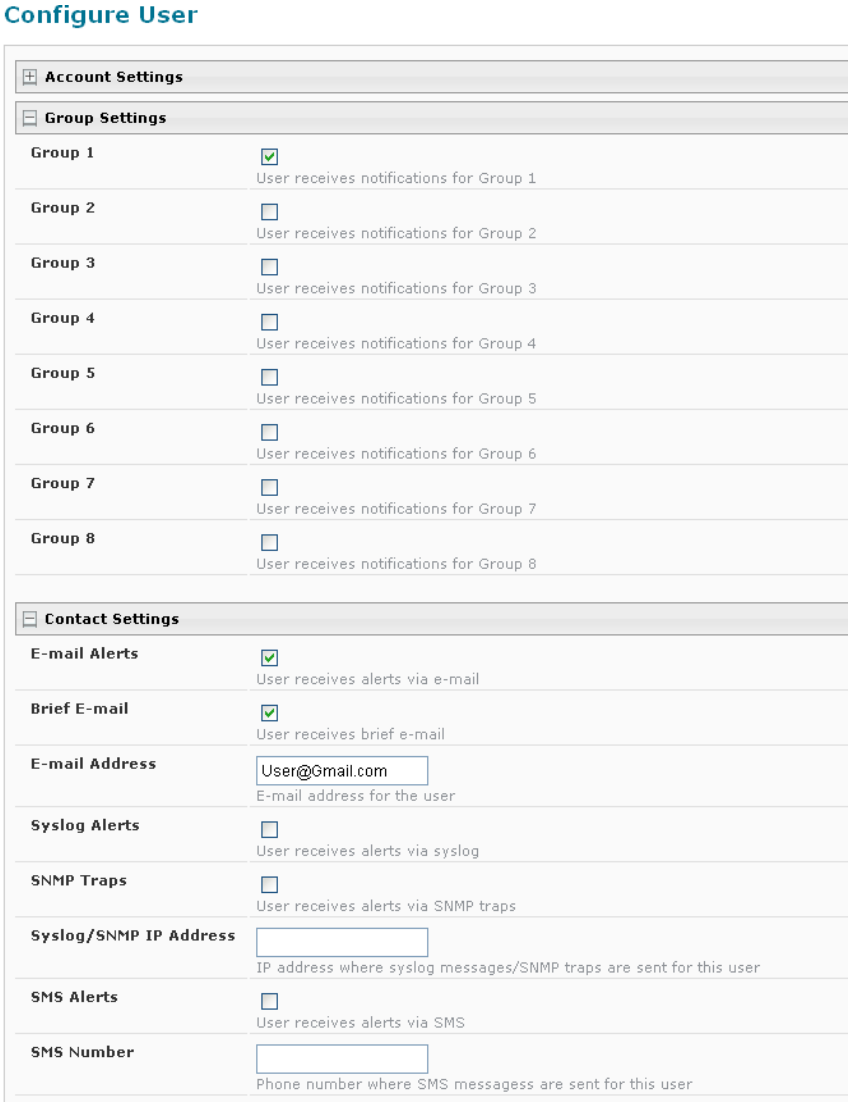


Figure 133- Configure user to receive alerts via email

LOCATING OIDS

To use SNMP (Simple Network Management Protocol) to monitor the sensors and control the functions of an E-MINI-LXO Environment Monitoring System (SYSTEM), you first need to install SNMP network management software. The software package will include an MIB (Management Information Base) browser and there are many different MIB browsers so we will be very general about the instruction provided herein. The MIB browser can be used to quickly view sensor data and the status of all characteristics of the SYSTEM. How you make use of that information is up to you.

General Information

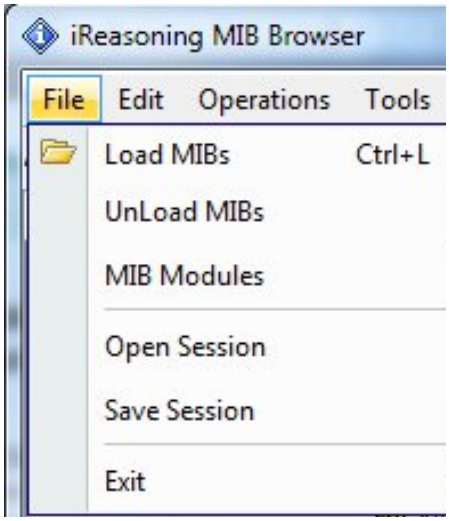
Every piece of information available from the SYSTEM through the MIB browser has an OID (Object Identifier). The MIB file provided with the SYSTEM (available http://www.networktechinc.com/download/d-environment-monitoring.html) provides a database to organize information received regarding sensors, IP Devices, etc.. Each piece of information derived from this database has a unique OID. To see the OID for any piece of information, select the variable and the OID assigned to it will be displayed.

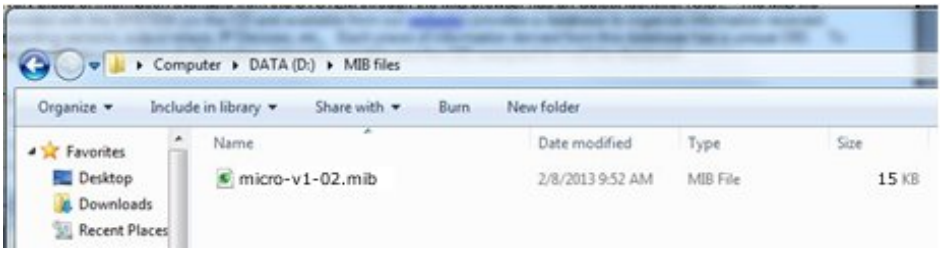
For this instruction we used the free MIB browser "iReasoning" found at http://ireasoning.com/mibbrowser.shtml.

View OIDs

To view this information, you must do the following:

1. Install the browser to your PC
2. Copy the MIB file associated with your SYSTEM to the hard drive on your PC.(perhaps to a new directory "MIB files" as shown below.)
3. Load the MIB file for the SYSTEM to your browser.



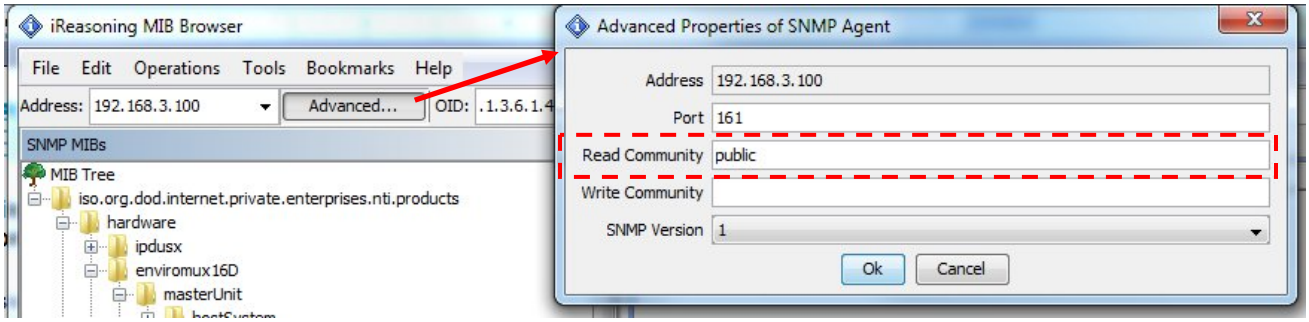


Select "Load MIBs" and locate the MIB file on your PC.

TIP: iReasoning provided a couple of default MIB files that were preloaded. To clean up the resulting data tree, we used "UnLoad MIBs" (above) to remove those.

4. Enter the IP address of the SYSTEM so the browser knows where the SYSTEM is to retrieve data.

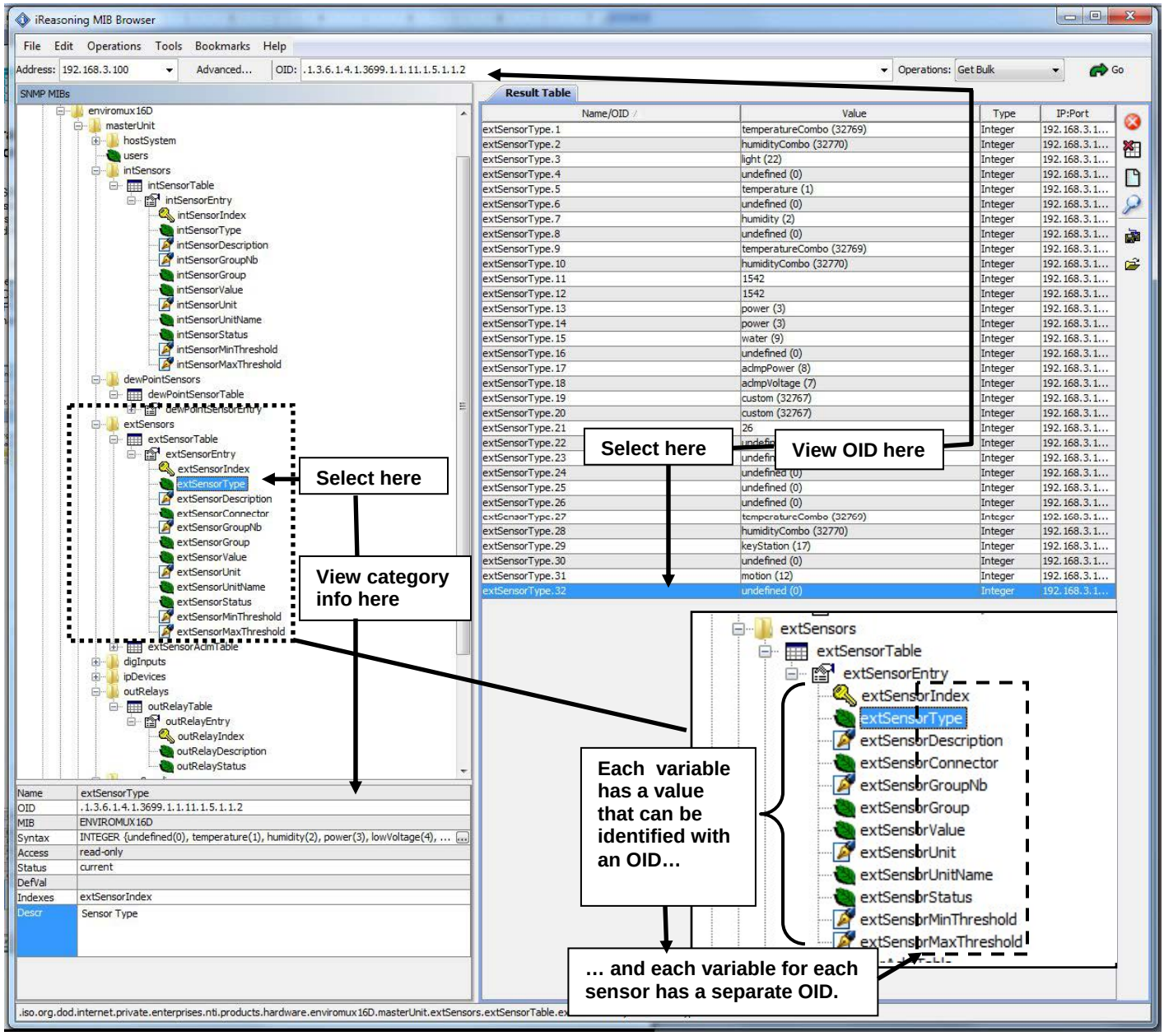
5. With the iReasoning browser, the Read-only Community Name (default is "public") was automatically sensed and applied when the IP address was entered, but if this doesn't happen in your browser, make sure the "Read Community" field in the agent properties includes the name "public" (or whatever you have changed it to in the E-MINI-LXO network configuration).



6. With that information entered, the default SYSTEM will be accessible for SNMP browsing.

A connection that uses security will require more configuration, Refer to page 42 and your browser manual to apply the required additional settings.

Once a connection is made, the browser will present a directory structure with tree organizing all the different variables of information available from the SYSTEM. Click on the various categories and sub categories to go as deep into the hierarchy as necessary. As seen in the image below, each variable of information presented has an OID assigned to it. These OIDs can be used in conjunction with other SNMP control systems to communicate and/or perform functions automatically.



Each RJ45 Sensor port has two OIDs assigned, because the sensors that connect to these ports often have two possible functions (Temperature/Humidity, ACLM-V with two connections, etc.). The image above shows they are numbered sequentially (The “extSensor Type” variable for Port 1 is extSensorType.1 and extSensorType.2, port 2 is extSensorType.3 and extSensorType.4, and so on, for a total of 4 extSensors (RJ45 Sensor) for an E-MINI-LXO.)

Each variable for a sensor that is reported has its own OID (i.e. Index number, type, description of the connected sensor, the connector number the sensor is plugged into, group the sensor belongs to, etc.). When using OIDs, be sure to create an association with the right variable.

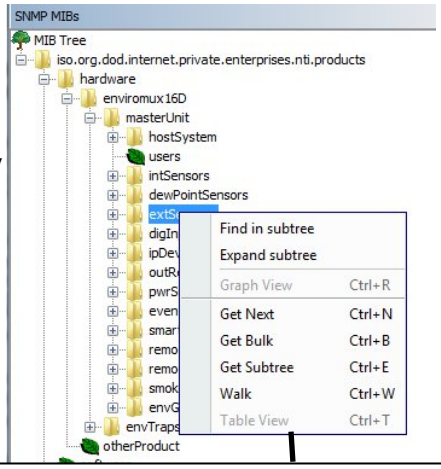
To get specific results in the Result Table, right click on an item in the MIB Tree and choose the type of search (“operation”) you want.

Get Next- will result in the next OID record of that category, displaying them one at a time.

Get Bulk- will result in all the OIDs of that category being displayed at once, but only that category

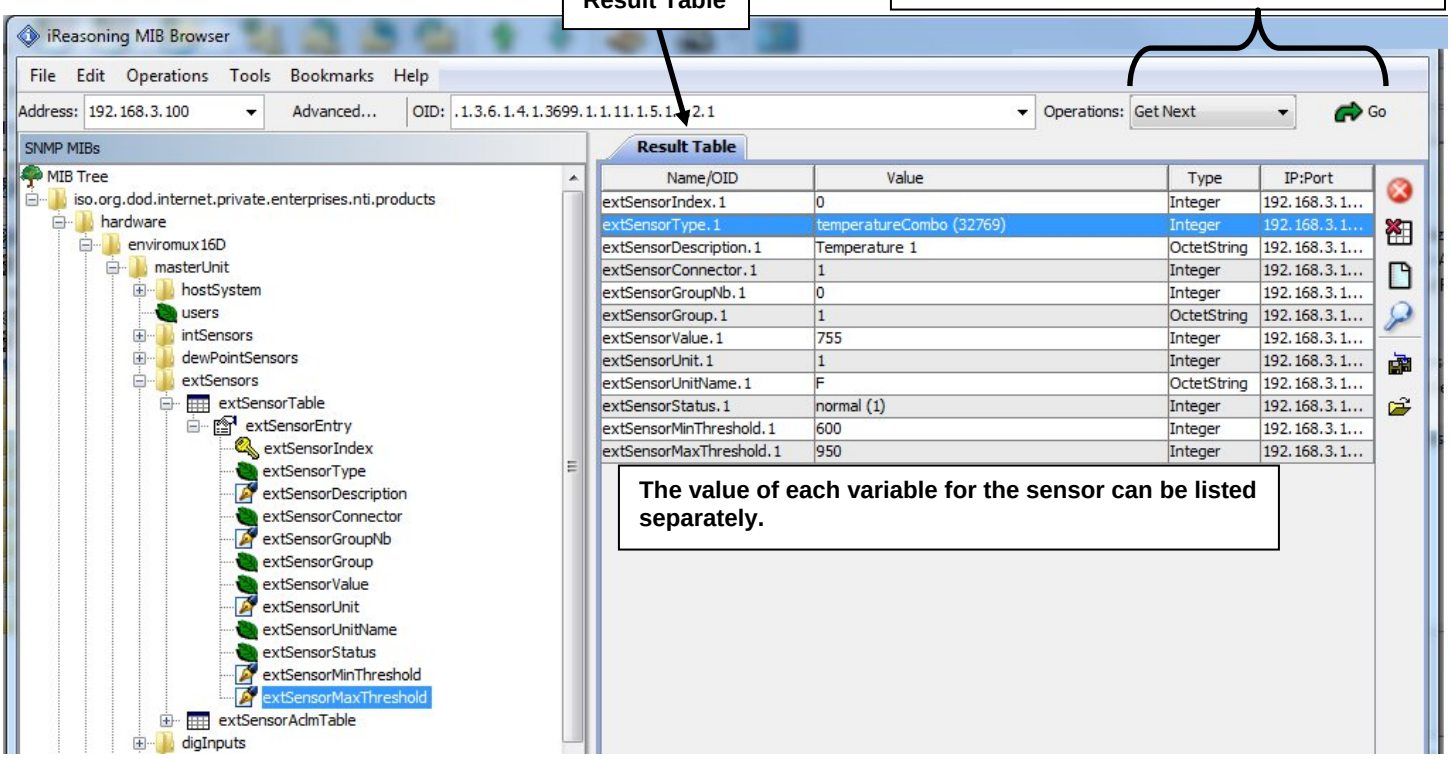
Get Subtree- will result in OIDs of that category and any sub-categories in the tree

Walk- will result in a listing of every OID in the system from the point at which you select it until the last category in the tree.



The operation can be selected with a right click (above), or using the “Operations” field (below). Once selected, press “Go”

Result Table



Using PRTG

When using PRTG Network Monitoring software, the sensor threshold OIDs listed in the E-MINI-LXO mib file will need to be configured in the PRTG sensors "Notifications" page (object Trigger ->Add Threshold trigger). Also, the sensor OIDs are numbered for identification within each sensor group like External Sensors. The sensor thresholds depend on the sensor type connected given by the Sensor Type OID with same number.

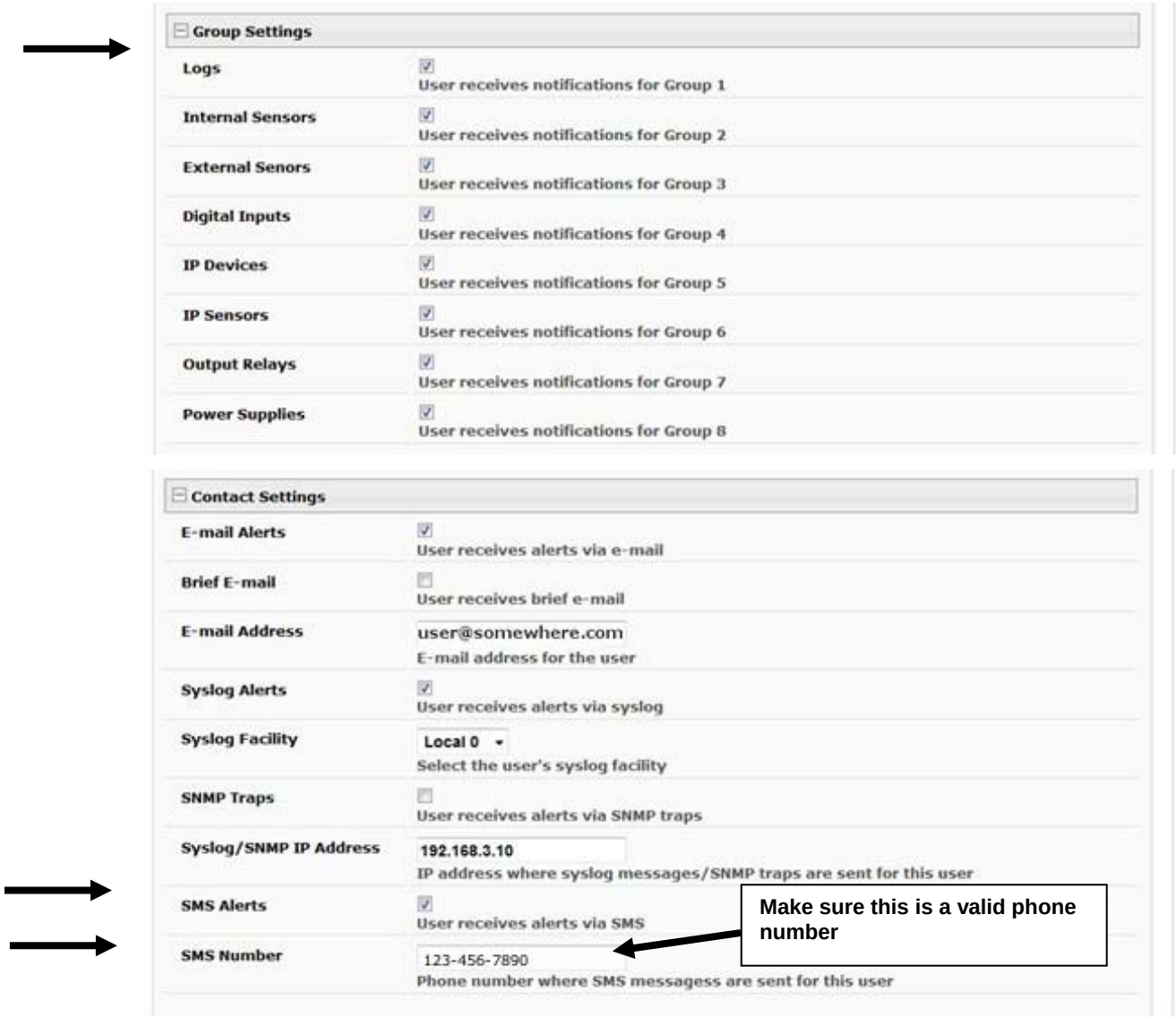
SETUP AND TEST SMS MESSAGING

To test a modem installed on an ENVIROMUX Monitoring System, you must first make sure the System has been configured properly to use the modem. This guide will take you through the basic steps to do that. For more details, see your respective product manual.

1. Install a USB modem as directed on page 19.

2. Configure the ENVIROMUX User Account Contact settings (Administration -> Users ->Edit User -> Contact Settings) to receive SMS Alerts and enter a valid phone number for the SMS messages to be sent to for that user.

Also make sure that user is set to receive messages from the type of sensor causing the message to be sent. Make sure enough boxes are checked under "Group Settings." .

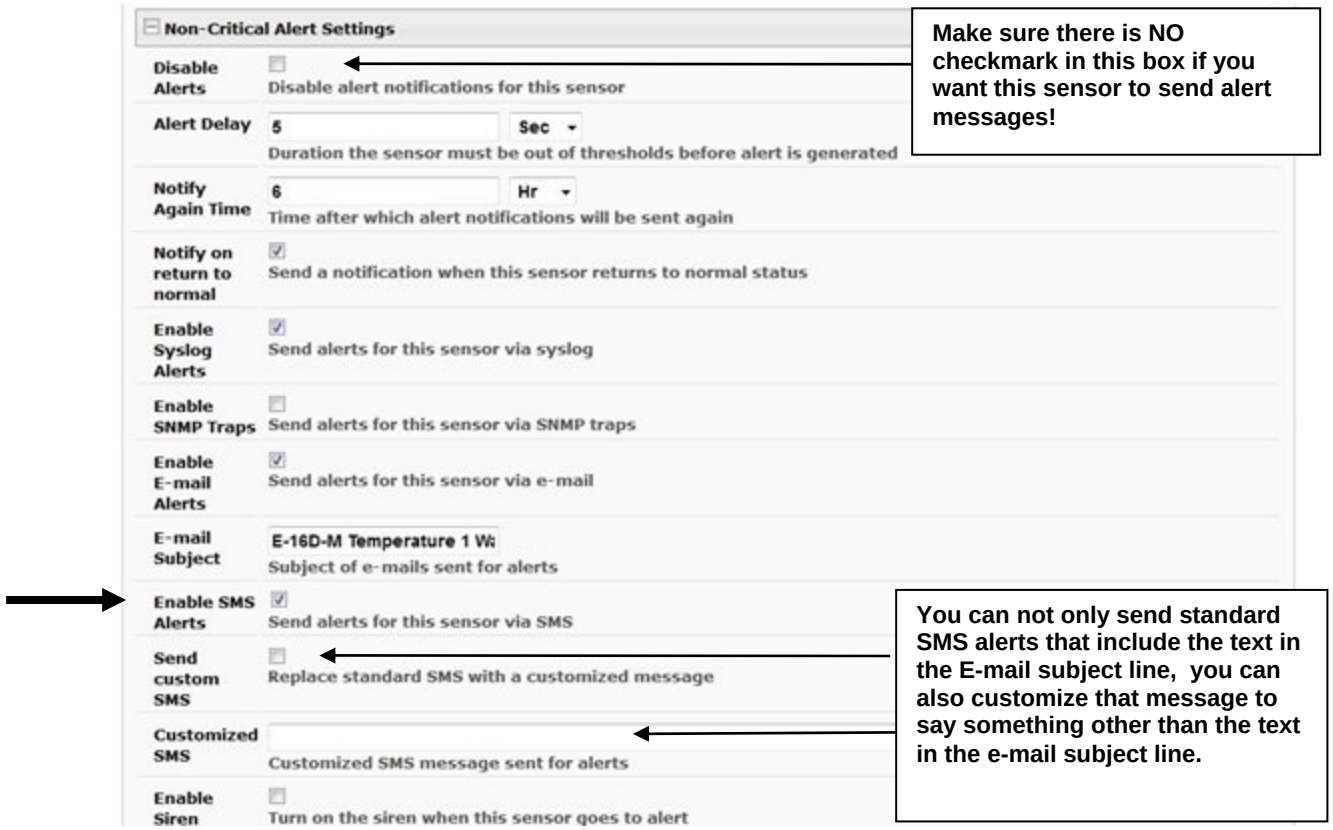


(Image from the E-XD web interface under User Settings)

3. Configure a sensor to send alerts via SMS messaging.

The Sensor Configuration has the settings to be changed. First make sure the sensor will send messages to a group the user is configured to get messages from, again, under "Group Settings" for that sensor.

Next make sure that “Enable SMS Alerts” is checked. Also make sure that “Disable Alerts” is **NOT** checked for this sensor.



(Image from the E-XD web interface under Sensor Configuration Settings)

4. Once the sensor is configured, and the user settings include the correct settings and valid phone number, a test can be conducted.

To test the settings you will need to cause a sensor to go outside the alert conditions (or, change the settings so that the current conditions ARE considered alert conditions).

Once the alert is tripped or simulated, the phone number for the configured user should receive the configured SMS message.

Troubleshooting

If no message is received, double-check all of the settings just described. Then check your modem status and strength under **Administration ->Enterprise**.

When installed and working, the modem status will say “Ready” and the signal strength will be indicated. Ideally, signal strength should always be at least -100db. (-99, -98 is better, -101,-102 is worse). If the modem is plugged in and not working, make sure your SIM card is up to date and paid for with your service provider.

No Modem Installed

Modem properly installed. (Note: Signal strength shown here is extremely poor)

If the signal to the modem is too weak, then either the ENVIROMUX will need to be moved or the modem will have to be moved (you can extend the modem up to 5 meters (16.4 feet) from the ENVIROMUX with a USB extension cable).

DATE/TIME BATTERY REPLACEMENT

The E-MINI-LXO is equipped with a replaceable battery that maintains the set date and time when the ENVIROMUX is powered OFF. In the event you find that the date has been reset to “08/31/2009” after a power-cycle, this means the battery has reached end of life and needs replacement.

To replace the battery:

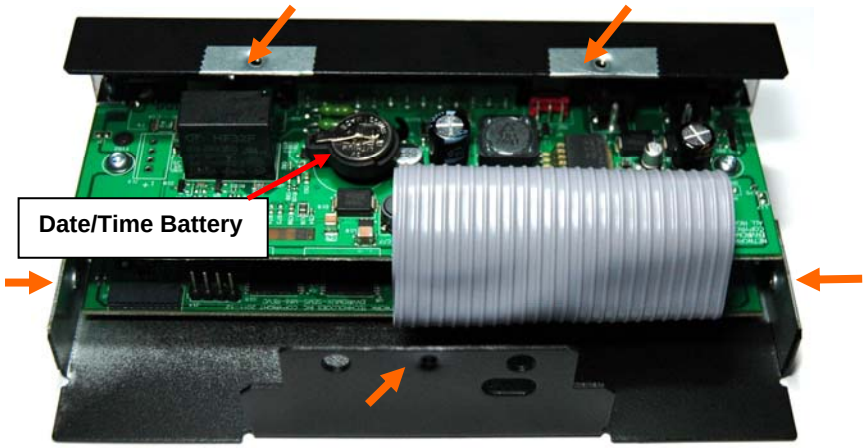
1. Avoid Electrostatic Discharge (ESD) by grounding yourself before touching the ENVIROMUX. Failure to follow this step may damage your ENVIROMUX.

2. Power OFF the ENVIROMUX.

WARNING: RISK OF ELECTRIC SHOCK!! If you prefer to change this battery while power is connected to avoid having to reset the date and time, be extremely careful not to touch any other part of the circuit boards. Also, **be careful** not to let the battery fall down onto the live circuit board.

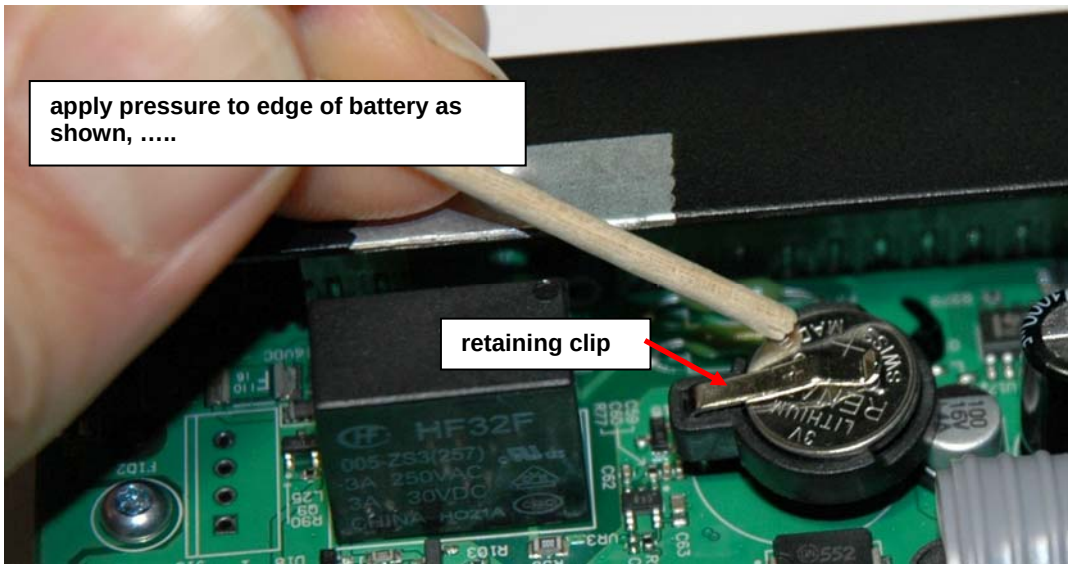
3. Remove the screws that hold the top of the case to the ENVIROMUX (5 screws), locations indicated below by orange arrows) and remove the cover to expose the circuit boards inside.

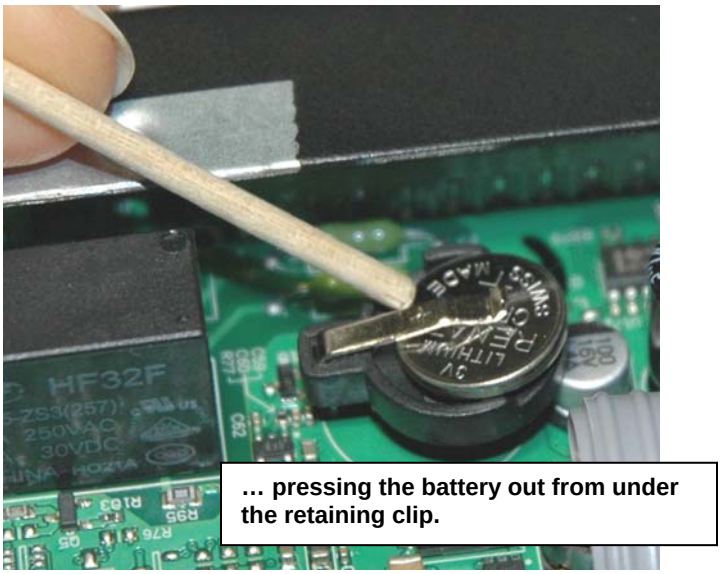
Note: Earlier models had soldered-in battery (not field replaceable). These units will have to be returned to NTI for battery replacement.



4. Locate the date/time battery in the ENVIROMUX (see image above).

5. Using a **non-conductive** stick-like object (ex. a Q-tip with the cotton removed from one end), press the battery out of the battery holder. **Be careful not to let it fall onto the circuit board** if you are doing this with power ON.





… pressing the battery out from under the retaining clip.

6. Re-install the new battery by reversing the process. (**CR1225**) Be very careful not to lift up too hard on the retaining clip. Lift only far enough to slip the edge of the new battery under it and slide the battery back into place.

7. Carefully reinstall the cover to the base and install the screws removed.

8. If the ENVIROMUX was powered OFF during this procedure, power ON the ENVIROMUX and configure the correct time and date using one of the control methods described earlier in this manual.

TECHNICAL SPECIFICATIONS

Ports	
Temperature/Humidity Inputs	Two female RJ45 connectors for connecting temperature sensors, humidity sensors, and/or combined temperature/humidity sensors.
Max. Sensor Cable Length	Temperature and Humidity Sensors- 25 feet Liquid and Contact Sensors- 1000 feet
DIGITAL IN Dry Contact Closures	Five screw terminal pairs for connecting dry contact devices and liquid detection sensors. * Potential-free. * Output voltage: +5 V DC * Current limited to 10 mA * Maximum contact resistance: 10K Ohm
Ethernet Port	One female RJ45 connector with LEDs. 10 BaseT Ethernet interface.
USB Console Port	Virtual Serial Port- USB Type B female connector
USB Devices Ports	Two female USB Type A connector Supports USB 2.0 Full Speed
Output Relay	SPDT relay- contacts rated for up to 1A, 30VDC or 0.5A, 125VAC
Environmental	
Operating temperature	32°F to 122°F (0°C to 50°C)
Storage temperature	-13°F to 149°F (-25°C to 65°C)
Operating and Storage Relative Humidity	0 to 90% non-condensing RH
General	
Compatible Modems	E-GSM-3GU (NetComm N3GS003)
Protocols	HTTP, HTTPS,SNMP, SMTP, TCP/IP, UDP, Xmodem, SSHv2, SSLv3, IP Filtering, LDAPv3, AES 256-bit encryption, SNMPv1,v2c,v3
Power Supply	120VAC or 240VAC at 50 or 60Hz-9VDC/1.5A AC Adapter
Dimensions WxDxH (in.)	2.14x5.68x2.14
Approvals	RoHS

TROUBLESHOOTING

Each and every piece of every product produced by Network Technologies Inc is 100% tested to exacting specifications. We make every effort to insure trouble-free installation and operation of our products. If problems are experienced while installing this product, please look over the troubleshooting chart below to see if perhaps we can answer any questions that arise. If the answer is not found in the chart, a solution may be found in the knowledgebase on our website at http://information.networktechinc.com/jive/kbindex.jspa or please call us directly at (**800) 742-8324 (800-RGB-TECH)** or **(330) 562-7070** and we will be happy to assist in any way we can.

Problem	Cause	Solution
Cannot connect via telnet	telnet service not enabled	Enable telnet (page 43)
Cannot connect via web interface- no login screen	• wrong IP address • HTTP not enabled • HTTP moved from default (port 80)	• Use Discovery Tool to locate configured IP address (page 22) • Enable HTTP (page 41) • Identify port number assigned (page 41)
Cannot get Discovery Tool to work	Java not installed	Java Runtime Environment must be installed before the Discovery Tool can be used (page 22)
LDAP user cannot login	Login username and/or password does not match same in ENVIROMUX user list	Make sure the username and password used in the LDAP server matches the username and password in the ENVIROMUX user configuration (page 44)
Cannot login	cannot remember root password	Either restore default settings (page 85) or contact NTI for assistance

Note: Do not try to manually edit the downloaded configuration file and then restore it to the ENVIROMUX (page 39). The ENVIROMUX will quit working and you will have to return it to NTI to have default settings restored. Factory restoration of the default settings is not covered under the product warranty.

SMTP Error Codes:

Without SSL enabled:	Meaning	Comments
-1	SMTP_CONN_ERR,	Cannot establish a connection to the SMTP server. Possible reasons: bad setting for IP of SMTP server, firewall blocking the connection
-4	SMTP_SERVER_NOT_READY_ERR,	Server denied connection
-5	SMTP_EHLO_ERR,	Server did not answer to HELO command
-6	SMTP_AUTH_NO_SUPPORT_ERR,	Authentication method is not supported
-7	SMTP_AUTH_FAILURE_ERR,	Authentication failure (user or password rejected)
-8	SMTP_BAD_FROM_ERR,	SMTP Server did not accept the sender e-mail address
-9	SMTP_BAD_TO_ERR,	SMTP Server did not accept the destination e-mail address
-10	SMTP_DATA_ERR,	SMTP Server did not accept the DATA command
-11	SMTP_BAD_DATA_ERR,	SMTP Server did not accept the body of e-mail message
With SSL enabled:		
-100	SMTP_SSL_CONN_ERR,	Failed to resolve connection to DNS server
-99	SMTP_SSL_CONN_ERR1,	Cannot establish a connection to the SMTP server. Possible reasons: bad setting for IP of SMTP server, firewall blocking the connection
-98	SMTP_SSL_CONN_ERR2,	System failed to create a socket (this is for internal reasons - like network down (a highly unlikely occurrence))
-97	SMTP_SSL_PROTOCOL_ERR,	SMTP server connected but did not accept SSL connection
-95	SMTP_SSL_SERVER_NOT_READY_ERR,	Server denied connection
-94	SMTP_SSL_EHLO_ERR,	Server did not answer to HELO command
-93	SMTP_SSL_AUTH_NO_SUPPORT_ERR,	Authentication method is not supported
-92	SMTP_SSL_AUTH_FAILURE_ERR,	Authentication failure (user or password rejected)
-91	SMTP_SSL_BAD_FROM_ERR,	SMTP Server did not accept the sender e-mail address
-90	SMTP_SSL_BAD_TO_ERR,	SMTP Server did not accept the destination e-mail address
-89	SMTP_SSL_DATA_ERR,	SMTP Server did not accept the DATA command
-88	SMTP_SSL_BAD_DATA_ERR,	SMTP Server did not accept the body of e-mail message
-87	SMTP_TLS_ERROR,	Cannot connect through STARTTLS protocol. SMTP server probably does not support this protocol. Disable STARTTLS.

HOW TO CREATE AN X.509 CERTIFICATE FOR ENVIROMUX

The ENVIROMUX family of products are designed to be configurable with security to limit access to their web interface controls. The use of x.509 client authentication is one of the methods that may be used, and although the ENVIROMUX includes a default x.509 CA certificate (page **Error! Bookmark not defined.**), this procedure will help you create your own custom x.509 CA certificate to use with this feature. This procedure was created using Ubuntu Linux and OpenSSL (a requirement for creating the certificate).

Note: Do not disable access to the ENVIROMUX web interface using http before you verify that the https client authentication works properly (see page 131).

Creating a Certificate Authority using OpenSSL

The Root CA certificate will be used by a web server (ENVIROMUX) to authenticate the client (browser). It also needs to be imported in a web browser as a Trusting authority.

An example SSL config file (**openssl.cnf) can be found at http://www.networktechinc.com/environment-monitor-16d.html#tab-6 .** **(You can edit it in any text editor to customize for your own needs.)**

Creating the Certificate Management Directories and Files

1. Create directory "ntiCA" in /usr/local/ssl for ntiCA certificate management and change to that directory.

("nti" can be changed to whatever you want throughout this procedure, but do it consistently. Whatever you change it to, make sure the openssl.cnf file is edited to match your changes)

```
mkdir /usr/local/ssl/ntiCA
cd /usr/local/ssl/ntiCA
```

Create following directories in the ntiCA directory:

```
mkdir CA
mkdir server
mkdir server/certificates
mkdir server/requests
mkdir server/keys
mkdir user
mkdir user/certificates
mkdir user/requests
mkdir user/keys
```

The CA directory will be populated with the certificate authority certificate request, keys and certificate used to sign server and user certificates. The server directory hierarchy will be used to manage certificate requests, keys and certificates issued for web server hosts. The user directory hierarchy will be used to manage certificate requests, keys and certificates for users.

2. Issue the following commands to setup default contents of certificates and revocation list for these files:

(The percent sign (%) is the command prompt, not part of the command.)

```
% cd /usr/local/ssl/ntiCA
% echo "01" > serial
% touch index.txt
```

The openssl.cnf file that you edited earlier (if you did) references these files so make sure they are created in the ntiCA directory.

Creating the ntiCA Key and Certificate

The general process for creating a certificate includes:

1. Creating a private key
2. Creating a certificate request
3. Creating and signing a certificate from the certificate request

1. Create the CA key:

Recommended for hi level of security

```
% cd /usr/local/ssl/ntiCA
% openssl genrsa -out ./CA/ntiCA.key 2048
Generating RSA private key, 2048 bit long modulus
.....++++++
......++++++
e is 65537 (0x10001)
```

2. Create the CA certificate request:

```
% openssl req -sha512 -new -key ./CA/ntiCA.key -out ./CA/ntiCA.csr
```

You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a **Distinguished Name** or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

```
Country Name (2 letter code) [US]:
State or Province Name (full name) [OH]:
Locality Name (eg, city) [Aurora]:
Organization Name (eg, company) [NTI]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:your_user_name
Email Address [sales@ntigo.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:password
An optional company name []:
```

3. Self-sign the CA certificate:

```
% openssl x509 -req -sha512 -days 3650 -in ./CA/ntiCA.csr -out ./CA/ntiCA.crt -signkey
./CA/ntiCA.key
Signature ok
Getting Private key
```

Verifying the CA certificate contents

At this point we have our self-signed CA certificate and our CA key, which will be used to sign the web server and client certificates that we create. To verify the certificate contents, use the following command:

```
% openssl x509 -in ./CA/ntiCA.crt -text
```

Creating a Web Server Certificate (This will need to be done for each web server)

The procedure for creating a web server certificate is similar to that for creating the CA certificate except that the web server certificate will be signed using the CA key rather than self-signing with a web server-specific key.

1. Create the web server private key using a fully qualified DNS name (or IP address). When prompted for the pass phrase, **enter a password that you can remember.**

```
% cd /usr/local/ssl/ntiCA
% openssl genrsa -des3 -out ./server/keys/your_device_fqdn_or_ipaddress.key 2048
Generating RSA private key, 2048 bit long modulus
.......++++++
.++++++
e is 65537 (0x10001)
Enter pass phrase for ./server/keys/your_device_fqdn_or_ipaddress.key:
Verifying - Enter pass phrase for ./server/keys/your_device_fqdn_or_ipaddress.key:
```

2. Create the web server certificate request using the same fully qualified DNS name (or IP address) you used for the private key. When prompted for the pass phrase for the keys in file ./server/keys/your_device_fqdn_or_ipaddress.key, enter the pass phrase that you used for the private key. Also, **it is vitally important** that you set the Common Name value to the fully qualified DNS name of your web server because that's the value that a browser client will verify when it receives the web server's certificate.

```
% openssl req -sha512 -new -key ./server/keys/your_device_fqdn_or_ipaddress.key -out
./server/requests/your_device_fqdn_or_ipaddress.csr
Enter pass phrase for ./server/keys/your_device_fqdn_or_ipaddress.key:

You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [OH]:
Locality Name (eg, city) [Aurora]:
Organization Name (eg, company) [NTI]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:your_device_fqdn_or_ipaddress
Email Address [ca@ntigo.com]:sales@ntigo.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

3. Sign the web server certificate with the CA key:

```
% openssl ca -days 3650 -in server/requests/your_device_fqdn_or_ipaddress.csr -cert
./CA/ntiCA.crt -keyfile ./CA/ntiCA.key -out
./server/certificates/your_device_fqdn_or_ipaddress.crt -config <path_to_config
file>\openssl.cnf
```

In the command above, substitute the path to the config file “openssl.cnf” in place of “<path_to_config_file>”.

```
DEBUG[load_index]: unique_subject = "yes"
  Check that the request matches the signature
  Signature OK
  Certificate Details:
  Serial Number: 3 (0x3)
  Validity
  Not Before: Aug 18 17:41:07 2005 GMT
  Not After : Aug 18 17:41:07 2006 GMT
  Subject:
  countryName = US
  stateOrProvinceName = OH
  organizationName = NTI
  commonName = your_device_fqdn_or_ipaddress
  emailAddress = sales@ntigo.com
  X509v3 extensions:
  X509v3 Basic Constraints:
  CA:FALSE
  Netscape Comment:
  OpenSSL Generated Certificate
  X509v3 Subject Key Identifier:
  0A:6B:79:E7:98:5F:30:7F:A0:67:4A:12:83:9C:0A:58:BE:8B:41:2A
  X509v3 Authority Key Identifier:
  DirName:/C=US/ST=OH/L=Aurora/O=NTI /CN=NTI CA/emailAddress=sales@ntigo.com
  serial:CD:93:0B:9F:5A:71:EB:8B

  Certificate is to be certified until Aug 18 17:41:07 2026 GMT (365 days)
  Sign the certificate? [y/n]:y

  1 out of 1 certificate requests certified, commit? [y/n]y
  Write out database with 1 new entries
  Data Base Updated
```

To verify the web server certificate contents, use the following command:

```
% openssl x509 -in ./server/certificates/your_device_fqdn_or_ipaddress.crt -text
```

Key values to look for are:

```
Subject CN=your_device_fqdn_or_ipaddress
Issuer CN=NTI CA
```

Uploading Server Certificate to NTI device

The NTI ENVIROMUX webserver expects the certificate and key as a single file in "PEM" format.

Note: If your key has a password then you need to create a key without password.

Use the following command to export the file without the password.

```
openssl rsa -in <your_key>.key -text > private.key
```

Use following command to create pem certificate file

```
cat <your_certficate_name>.crt private.key > <server_name>.pem
```

On the ENVIROMUX WEB Interface menu Under “Administration” select “Security”.
In X509 certificates
Select the above file and press the button **"Upload Server certificate and Key"**

<your_key> , <your_certificate_name> and <server_name> are placeholders. “Your_ certificate” is the web server certificate you created, “your_key” is the CA key you created, and the “server_ name” is whatever you want the pem file to be named.

Creating a Client Certificate

The procedure for creating a client certificate is similar to that for creating the web server certificate.

Creating a user key

The following instructions create a private key for a user named your_name@ntigo.com. When prompted for the pass phrase, enter a password that you can remember.

```
% cd /usr/local/ssl/ntiCA
% openssl genrsa -des3 -out ./user/keys/your_name@ntigo.com.key 2048
Generating RSA private key, 2038 bit long modulus
...++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase for ./user/keys/your_name@ntigo.com.key:
Verifying - Enter pass phrase for ./user/keys/your_name@ntigo.com.key:
```

Create the user certificate request

1. The following command creates a certificate request for a user with email address: your_name@ntigo.com and common name your_name. When prompted for the pass phrase for the keys in file ./user/keys/your_name@ntigo.com.key, enter the pass phrase that you used to create the user key (e.g. “password”).

```
% openssl req -sha512 -new -key ./user/keys/your_name@ntigo.com.key -out
./user/requests/your_name@ntigo.com.csr
Enter pass phrase for ./user/keys/your_name@ntigo.com.key:
```

You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a **Distinguished Name** or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

```
Country Name (2 letter code) [US]:
  State or Province Name (full name) [OH]:
  Locality Name (eg, city) [Aurora]:
  Organization Name (eg, company) [NTI]:
```

```
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:your_name
Email Address [ca@ntigo.com]:your_name@ntigo.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

2. Sign the user certificate request and create the certificate

```
% openssl ca -in ./user/requests/your_name@ntigo.com.csr -cert ./CA/ntiCA.crt -keyfile
./CA/ntiCA.key -out ./user/certificates/your_name@ntigo.com.crt
```

Using configuration from /usr/local/ssl/openssl.cnf

```
DEBUG[load_index]: unique_subject = "yes"
```

3. Check that the request matches the signature

```
Signature OK
Certificate Details:
Serial Number: 4 (0x4)
Validity
Not Before: -----
Not After : -----
Subject:
countryName = US
stateOrProvinceName = OH
organizationName = NTI
commonName = your_name
emailAddress = your_name@ntigo.com
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
 -----
X509v3 Authority Key Identifier:
DirName:/C=US/ST=OH/L=Aurora/O=NTI/CN=your_nameCA/emailAddress=sales@ntigo.com
serial:CD:93:0B:9F:5A:71:EB:8B
----
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Verifying the user certificate contents

To verify the user certificate contents, you can use the following command:

```
% openssl x509 -in ./user/certificates/your_name@ntigo.com.crt -text
```

Importing a Client Certificate into Web Browsers

Web browsers like Firefox and IE can't use the certificates in the PEM format that is generated by OpenSSL . Consequently, we'll need to export the user certificate to file formats that can be imported by web browsers.

Importing the client certificate in PKCS#12 format

Firefox and Internet Explorer 6.0 support the PKCS#12 certificate format. Use the following command to convert the user certificate to this format.

NOTE: During the conversion process, you'll be asked for an export password. Enter anything you can remember, but don't let it be empty because the file will contain your private key.

```
% openssl pkcs12 -export -clcerts -in ./user/certificates/your_name@ntigo.com.crt -inkey
./user/keys/your_name@ntigo.com.key -out ./user/certificates/your_name@ntigo.com.p12
```

Copy the `your_name@ntigo.com.p12` file to a location where you can access it from your web browser via the file system.

Import Using Internet Explorer 6.0

To import a certificate, start IE and follow the instructions below:

Navigate to the Tools menu and click Internet Options
Click the Content tab
Click the Certificates button
Click the Import button
Follow the wizard instructions to select the certificate file
Enter the password you used to protect your certificate and private key
Import client certificates into the Personal store and root certificates for the CA that signed the web server certificates into the Trusted Root Certification Authorities store
Click the imported certificate and then on the View button in the Certificate intended purposes group box. Click the Details tab and then the Edit Properties button. Make sure that the Client Authentication option is checked.

For more detailed information, please see Microsoft Internet Explorer 6 Resource Kit, Chapter 6 - Digital Certificates.

Import using FireFox 1.5

To import a certificate, start FireFox and follow the instructions below:

Navigate to the Tools menu and click Options
Click the Advanced icon
Click the Security tab
Click the View Certificates button
Click the Import button and select the certificate file
Enter your master password for the Software Security Device
Enter the password you used to protect your certificate and private key

Importing the nti CA root certificate into web browsers

In order to establish a chain of trust between the imported user certificate and the issuing certificate authority, you'll need to import the nti CA certificate into your web browser.

Though the user interface for accepting the CA certificate varies, it is possible to import it for Firefox and IE 6.0 in this way.

Firefox 1.5

A dialog box appears and offers the choice of importing the CA certificate. Select the “Trust this CA” to identity web sites option, then click the “OK” button. You may also select the “View” button to see the certificate contents before accepting it.

Internet Explorer 6.0

A dialog box appears and asks “Do you want to open or save this file?”. Select the “Open” option, then click the “Install Certificate” button when the certificate dialog appears.

Once you've successfully imported the nti CA you will be able to access the URL of the ENVIROMUX without being prompted to accept the web server certificate.

Configuring NTI device to require Client Certificate

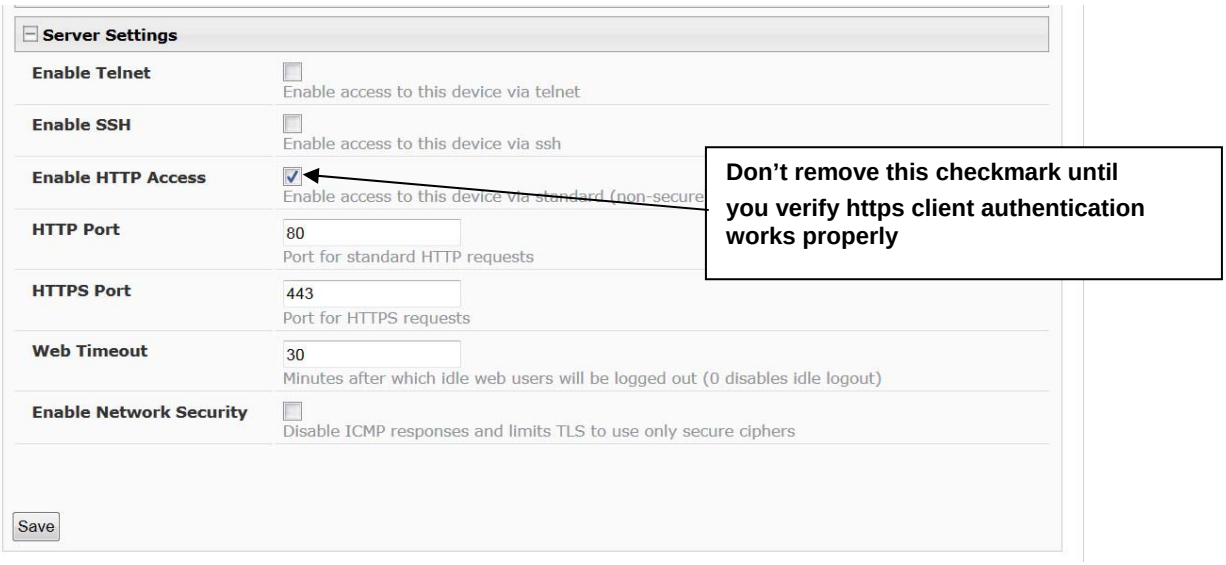
On the ENVIROMUX WEB Interface menu Under “Administration” select “Security”.

In X509 certificates select the file `ntiCA.crt` and press button "Upload CA certificate"

To enable the device to ask for client certificate select “certificate + login” in the "Mode" field under “User Authentication”.

Use https communication.

Note: Before disabling http be sure to verify https client authentication works properly.



Server settings section of Network configuration from ENVIROMUX web interface

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.

MAN143 Rev. 5/29/18