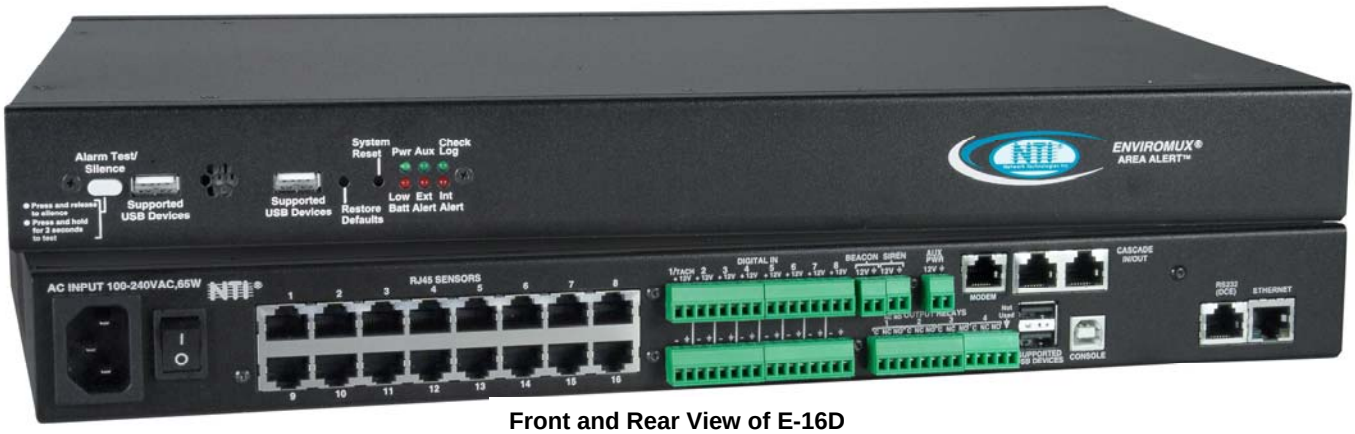
NETWORK TECHNOLOGIES INCORPORATED
1275 Danner Dr Tel:330-562-7070
Aurora, OH 44202 Fax:330-562-1999
www.networktechinc.com

ENVIROMUX® Series

E-16D/-5D/-2D

Enterprise Environment Monitoring System
Installation and Operation Manual



Front and Rear View of E-16D

Front View of E-5D

Front View of E-2D

CE

TRADEMARK

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

COPYRIGHT

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.

CE Statement

We, Network Technologies Inc, declare under our sole responsibility that the E-16D , E-5D and E-2D are in conformity with European Standard EN55022.

Firmware Version

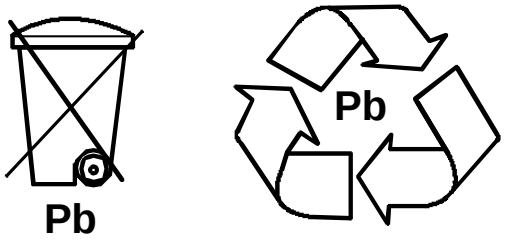
Current Firmware version 2.53

As of firmware version 2.35, the webserver in the E-xD supports only TLS v1.2 security encryption. Due to security vulnerability, SSL is no longer supported.

Exception: E-mail servers requiring SSL encryption will still be supported for alert messages.

WARNING

The E-16D contains a sealed lead acid battery. Battery maintenance must be performed by an authorized trained technician. Always follow local laws and regulations regarding the disposal of this unit.



CAUTION

Turn OFF power to the ENVIROMUX and discharge your body's static electric charge by touching a grounded surface or use a grounding wrist strap before performing any connections to the unit.

CAUTION

For continued protection against fire and electric shock this device should only be connected to an AC mains outlet equipped with a proper ground terminal.

TABLE OF CONTENTS

TABLE OF FIGURES

INTRODUCTION

The ENVIROMUX Enterprise Environment Monitoring System (ENVIROMUX) provides a way to supervise, from a remote location, the environmental conditions and security in cabinets and rooms containing servers, hubs, switches and other network components. Input data is filtered, collected, analyzed and processed to instantly and accurately display the status of the room. The user is able to specify parameters for all monitored conditions: if the parameters are exceeded, the unit will signal an alarm, which may include several pre-defined processes.

The E-16D, our most feature-filled model, includes sensors that monitor the internal temperature and humidity of the unit, giving readings that can be used as an estimate for the conditions of other nearby rack components.

All models are capable of monitoring external RS485 sensors and additional digital contact-type sensors (often called open-collector, contact-closure, relay-style, normal-open, or normal-closed). All sensors are sold separately, available from NTI. ENVIROMUX includes output relays to control devices such as door locks, keypads, and circulation fans. The E-16D and E-5D also include outputs specifically for the connection of an alarm siren and/or beacon.

The external sensors sold by NTI will monitor temperature and humidity, monitor AC line voltage, frequency, and current, detect smoke, and much more. The temperature and humidity sensors will provide current readings as well as alerts when thresholds are exceeded. The AC line monitor detects AC line input voltages between 50~250V AC, the Frequency (Hertz) between 47~63Hz, and the Power (Current) up to 12 amperes from a single AC line. The remainder of the sensors will simply provide alerts. These sensors can be manufactured by any third party, provided the alert notification method is compatible. Each of the aforementioned NTI sensors will connect to the ENVIROMUX via RJ45 connectors and CAT5 cable.

The ENVIROMUX can also work with both 4-wire and 2-wire contact-style sensors (4-wire sensors require a power connection, 2-wire do not). An external power supply for some 4-wire sensors may be required (sold separately). Screw terminals are provided for the connection of external contact-style sensors.

The Ethernet provides the main user interface for the ENVIROMUX. The ENVIROMUX provides data logging that can be viewed via a web browser and send alerts via email, Syslog, SNMP traps, SMS text messages and front panel LEDs. USB ports are provided for the connection of a USB modem and for downloading log data to a USB flash drive.

Features: (see Feature Differences chart on next page for more details)

- Enables up to 16 users to monitor environmental conditions and security status remotely
- Alerts users of environmental faults via email, Syslog, SMS messages, SNMP traps (v1, v2c, and/or v3), Illuminated front panel LEDs, or notifications on a web page
- Sensors are assigned to organized groups, and users can receive alerts from any group(s)
- Smart alerts provide sophisticated configurable multi-event triggering of alert messages or device control
- Up to 16 users can control simultaneously via Ethernet and a single user control serially via connected terminal
  - Connections include RJ45 and USB for local serial control
  - RJ45 w/ LEDs for Ethernet-based control
- Easy connections for sensors and devices
  - RJ45 connections w/o LEDs provided for sensors
  - Screw terminals for digital input devices
  - Screw terminals for digital output devices
- 12VDC provided for all digital inputs (E-16D only)
- RJ45 Sensors include Temperature, Humidity, Temperature and Humidity, Water, Vibration, Smoke, Motion Sensor, Glass break detector and many more
- Provides control for devices such as door locks, keypad, or a fan via digital outputs (1A/ 30VDC, .5A/ 100VAC)
- Full configuration via web-based graphic user interface
- Limited configuration using text menus via Telnet , SSH, RS232 or USB-to-serial interface
- Browser independent (IE, Netscape, Mozilla, Opera)
- Outgoing mail using SMTP or SMTP over SSL for alert notifications- up to 16 different email addresses
- Configurable Alarms to match specific user schedule
- Local Email Authentication, SSL3
- Data logging to keep viewable record of events such as changes in the environment or user access
- Monitors (ping) up to 64 configurable IP addresses. Response Timeout and number of retries are user configurable for each address
- Flash firmware upgradeable via FTP server or web page
- Internal temperature, humidity, and power sensors (E-16D, 5DB, 2DB (see chart on next page)
- USB ports for USB modem and USB flash drive

The E-5D Medium Enterprise Environment Monitoring System and E-2D Small Enterprise Environment Monitoring System have almost the same functionality as the E-16D, just fewer connection points.

E-16D vs. E-5D vs. E-2D
Feature Differences

Feature	E-16D	E-5D	E-2D
Internal Sensors	3	2	0
Temperature	✓	✓	N/A
Humidity	✓	✓	N/A
Battery	✓	only for E-5D**B**	only for E-2D**B**
RJ45 Sensor Ports	16	5	2
Digital Inputs	8	5	5
12VDC provided on Digital Inputs	✓	N/A	N/A
Output Relays	4	2	1
Auxiliary (12V) Power Terminal	✓	✓	✓
Alerts	8 Methods	8 Methods	6 Methods
Alarm Silence/Test Button	✓	✓	N/A
Control Methods	6 Methods	6 Methods	5 Methods**
USB Ports for Modem and Data Logging	4	4	2
Front Panel LEDs	**6**	**2**	**2**
Backup Battery	✓ (1 Hour)	Optional (2 Hour) (E-5D**B**)	Optional (2 Hour) (E-2D**B**)
Power	• 110 or 220 VAC at 50 or 60 Hz via IEC connector. 65W • Options: dual power, 18-36VDC, 36-72VDC, 18-36VDC dual power, 36-72VDC dual power	110 or 220 VAC at 50 or 60 Hz via AC adapter. 3A Optional Dual Power, 18-72VDC, 18-72VDC dual power	110 or 220 VAC at 50 or 60 Hz via AC adapter / 3A Optional Dual Power

*** No dedicated alarm beacon/siren terminals although they CAN be connected to E-2D**

**** E-2D does not include an RS232 port for console control, but a USB Type B "Console" port (and drivers) is provided for this control method.**

N/A= Not Available

Options:

- **E-16D**
  - **Dual Power** – ENVIROMUX with two power connections for optional redundant power source connection (see page 20) - add "DP" to the model number (i.e. E-16D**DP**)
  - **DC Power** - to install the ENVIROMUX in a Telecom environment (see page 21). Add "-48V" or "-24V" to the model number (i.e. E-16D**-48V**). A "48V" model ENVIROMUX accepts 36-72VDC while a "24V"model accepts 18-36VDC, positive or negative polarity and includes a 3-pole screw terminal for connecting the DC voltage input.
- **E-5D /-2D**
  - **DIN Rail Mounting**- E-5D or -2D can be ordered with a DIN rail mounting bracket- Add "D" to the part number (i.e. E-5D-**D**)
  - **Battery Backup**- E-5D or -2D 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-5D**B**)*
  - **48V/24V/12V/9V Power Option-** E-5D-**48V** can be ordered with power connections for 18-72VDC (24 or 48VDC nominal) in addition to jacks for 9-12VDC AC adapter connection. For dual 48V connections, just add **"DP"** to the model number (i.e. E-5D-48V**DP**).
  - **48VINDLT Industrial Low Temperature Option-** E-5D-48VINDLT will operate between 36-72VDC at temperatures between -40 to 185°F (-40 to 85°C)

MATERIALS

Materials included with the E-16D kit:

- E-16D Large Enterprise Environment Monitoring System
- Power Cord- country specific (2 power cords for model E-16D-DP)**(excluded in E-16D-48V/-24V)**
- 1-CB4306 USB2-AB-2M-5T 2 meter USB 2.0 male type A-male type-B transparent cable
- CT6182 DB9 Female-to-RJ45 Female adapter
- CT6488 DB9 Male-to-RJ45 Female adapter
- 2- CB7094 5 foot RJ45-to-RJ45 CAT5 SF patch cable
- Rack mount kit

Materials included with the E-5D kit:

- NTI E-5D Medium Enterprise Environment Monitoring System
- 1- PS4225 120VAC or 240VAC at 50 or 60Hz-9VDC/3A AC Adapter (**excluded in E-5D-48V(DP)**)
  -OR-
  1- PS4264 120VAC or 240VAC at 50 or 60Hz-9VDC/**5A** AC Adapter (**E-5D(B)-IND only**)
- 1- Line cord- country specific (**excluded in E-5D-48V(DP)**)
- 1- CB4306 USB2-AB-2M-5T 2 meter USB 2.0 male type A-male type-B transparent cable
- 1- CT6182 DB9 Female-to-RJ45 Female adapter
- 1- CT6488 DB9 Male-to-RJ45 Female adapter
- 1- CB7094 5 foot RJ45-to-RJ45 CAT5 SF patch cable

Materials included with the E-2D kit:

- NTI E-2D Small Enterprise Environment Monitoring System
- 1- PS4225 120VAC or 240VAC at 50 or 60Hz-9VDC/3A AC Adapter
- 1- Line cord- country specific
- 1- CB4306 USB2-AB-2M-5T 2 meter USB 2.0 male type A-male type-B transparent cable

Materials <u>required</u> for connection but not supplied:

- Cables required for connection:
  Cat5 for RS485 sensors with RJ45 connectors wired to the TIA/EIA-568B standard (see page 163 for specifications)
  E-2W-xx 2-wire sensor cables for dry contact sensors
- Cable required for Ethernet connection:
  Cat5 cable with RJ45 connectors wired straight through (pin 1 to pin 1, pin 2 to pin 2, etc..)
- E-TRMPLG Terminating Plug- one required if multiple E-16D units will be cascaded using the RS485 connection method (page 88)

See our webpage for the latest sensors available; http://www.networktechinc.com/environment-monitor-16d.html

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 www.networktechinc.com and we will be happy to be of assistance.

SUPPORTED WEB BROWSERS

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

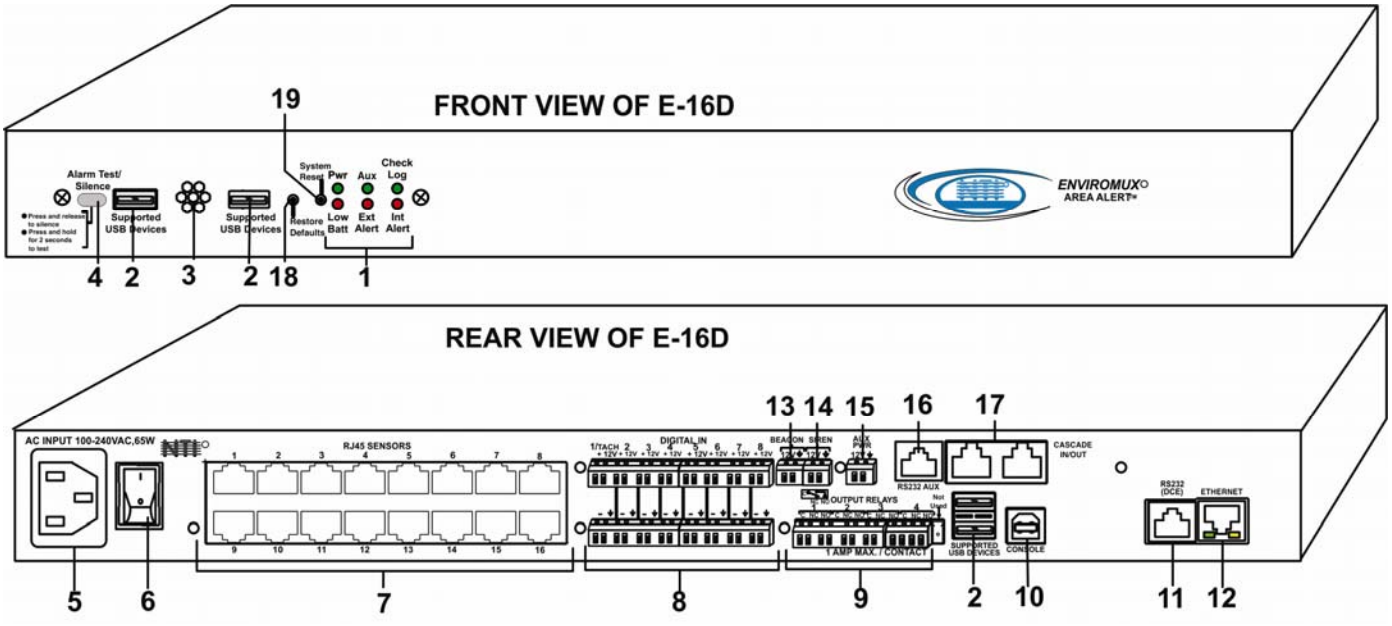
- Microsoft Internet Explorer 6.0 or higher
- Mozilla FireFox 1.5 or higher
- Opera 9.0
- Google Chrome

Note: If HTTPS pages cannot be viewed in the browser ("The page cannot be displayed" message appears) try to disable SSL 2.0 and TLS 1.0 from advanced options of the browser.

As of firmware version 2.35, the webserver in the E-xD supports only TLS v1.2 security encryption. Due to security vulnerability, SSL is no longer supported.

Exception: E-mail servers requiring SSL encryption will still be supported for alert messages.

FEATURES AND FUNCTIONS

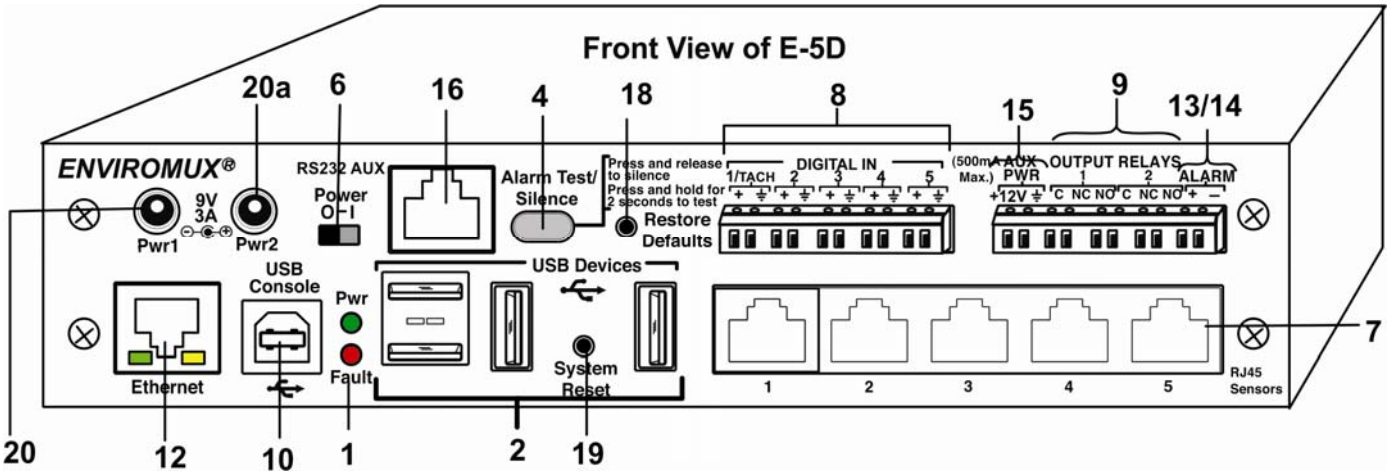


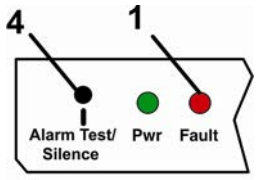
#	LABEL (LEDs)	DESCRIPTION
1	Pwr-	indicates when power to ENVIROMUX is ON (solid ON) and when power failure has occurred (battery power is ON- LED is blinking once per second)
	Low Batt-	indicates that the backup battery is running low on power, disconnected, or in failure
	Check Log-	illuminates when a new entry that is not an alert is added to the log
	Int Alert-	illuminates when an internal sensor generates an alert
	Ext Alert-	illuminates when an external sensor generates an alert
	Aux-	Not used as of this printing
	Fault-	red — illuminates if a sensor goes out of range of a configurable threshold (E-2D/5D Only)

See LED Status Chart (page 111) for more on LED indicators.

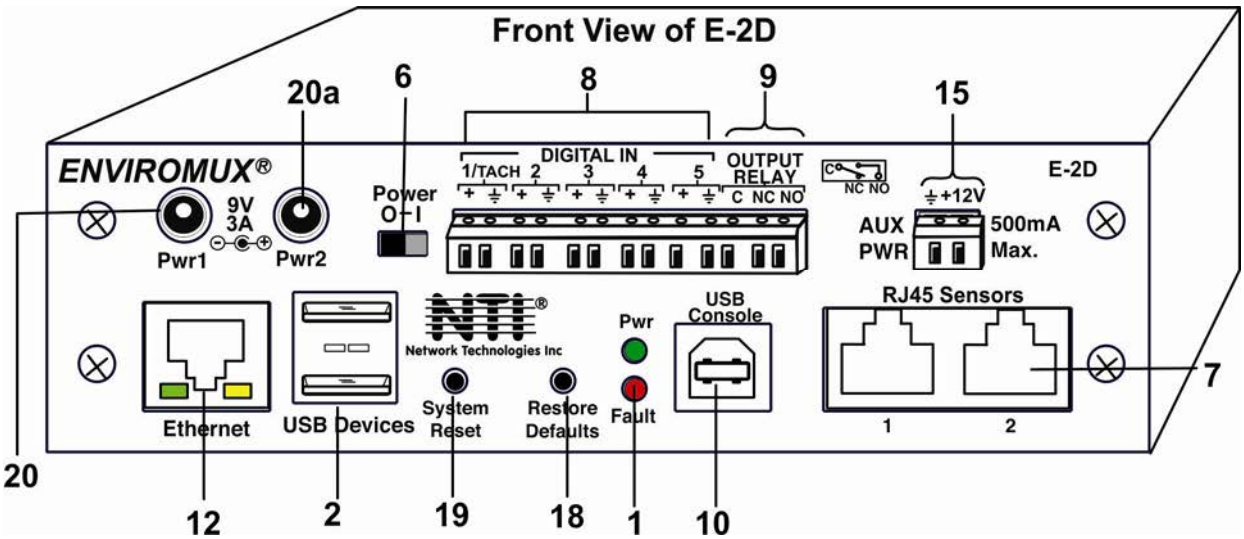
#	LABEL	CONNECTOR	DESCRIPTION
2	Supported USB Devices	USB Type A Female	for connection of supported USB 1.1 compatible devices (USB modem or flash drive for logging data)(see more information on pages 17 and 113)
3	None	None	Opening for humidity sensor to sense
4	Alarm Test/Silence	Button	Used to test or silence the alarm connected to the siren terminals
5	---	IEC Connector	for connecting the power cable (see also “Dual Power Option” on page 20)
6	---	Power Switch	used to turn the power to the ENVIROMUX ON/OFF
7	RJ45 Sensors	RJ45 female connectors	for attachment of various sensors
8	Digital IN	Terminal block	connection block for wired sensors (2-to-4 wire)
9	Output Relays	Terminal block	connection block for devices to be controlled in the event of alerts
10	Console	USB Type B female connector	For connecting USB cable for serial connection of a terminal to control the system
11	RS232 (DCE)	RJ45 female connector	Alternative port for RS232 serial connection of a terminal to control the system
12	Ethernet	RJ45 female connectors	for connection to a Local Area Network (LAN) for remote configuration, monitoring, and control
13	Beacon	Terminal block	for two-wire connection of visual indication of alarm (page 13)
14	Siren	Terminal block	for two-wire connections of audible indication of alarm (page 13)

#	LABEL	CONNECTOR	DESCRIPTION
15	Aux Pwr	Terminal block	for powering an auxiliary device with 12VDC power at 150mA maximum (fuse protected)
16	RS232 AUX	RJ45 female	for connection of a serial modem or remote RS232 device to be controlled
17	Cascade In / Out	RJ45 female connectors	used for RS485 method of cascading multiple E-16D units
18	Restore Defaults	Reset Button	for manually restoring the ENVIROMUX back to factory settings (see page 111 for details)
19	System Reset	Reset Button	for manually resetting the system (rebooting) the ENVIROMUX (see page 111 for details)
20	9V 3A- PWR1	2.1x5.5mm Power Jack	for connection of primary power supply
20a	9V 3A- PWR2	2.1x5.5mm Power Jack	for connection of backup power supply





E-5D REAR VIEW



INSTALLATION

Mounting Instructions-16D

The E-16D was designed to either sit on a shelf or be mounted in a rack. For mounting in a rack It includes a rack mount kit to make attachment easy.

1. Attach the ears to the ENVIROMUX using the #6-32x3/16" flat Phillips-head screws (6) provided as shown in the illustration below.

FYI: The same hole pattern is provided at the front and rear of the ENVIROMUX, enabling the ENVIROMUX to be mounted with the front facing out or rear facing out.

2. The holes in the ears should line up with pre-threaded holes in the sides of the ENVIROMUX. Tighten the screws securely.

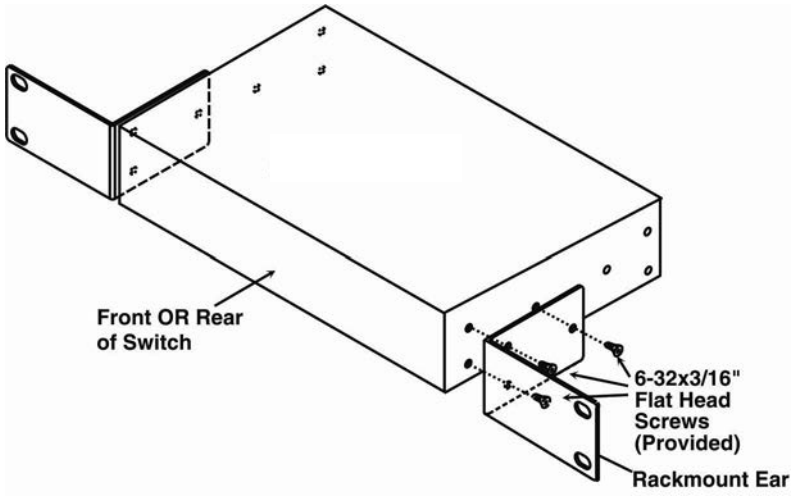


Figure 1- Secure rack mount ears to E-16D

3. Install 4 cage nuts to the rack in locations that line up with the holes in the mounting ears on the ENVIROMUX.
4. Secure the ENVIROMUX to the rack using four #10-32x3/4" screws and cage nuts (provided). Be sure to tighten all mounting screws securely.

Note: Do not block power supply vents in the ENVIROMUX case. Be sure to enable adequate airflow in front of and behind the ENVIROMUX.

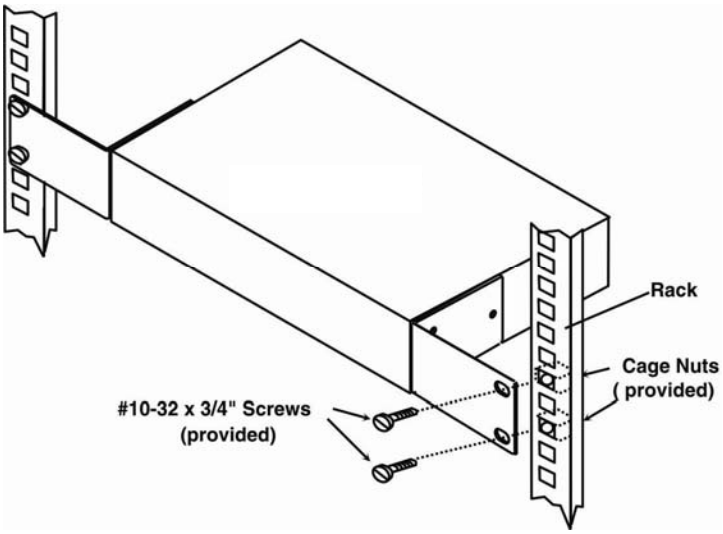


Figure 2- Mount ENVIROMUX in a rack

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

Mounting Instructions-5D / -2D

The E-5D and -2D can either be placed on a solid surface, mounted to a wall, mounted to a DIN rail 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 ENVIROMUX can be secured to any convenient surface. Use appropriate hardware (not supplied) when mounting.

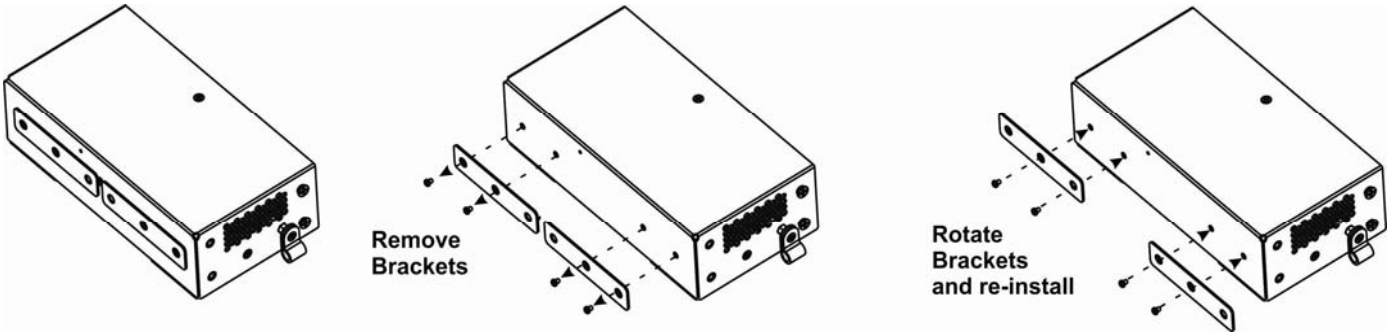


Figure 3- Rotate the tabs for Zero-RU mounting

If rack-mounting is preferred, the E-RK1-5D or E-RK1-2D rack-mount kit can be used (sold separately). Simply attach the ears (instructions included with the kit) and secure to a rack with the hardware provided.

FYI: Two sets of mounting holes are provided on the side of the ENVIROMUX to enable the ears to be attached such that the ENVIROMUX can be mounted with the front facing out or rear facing out, as desired.

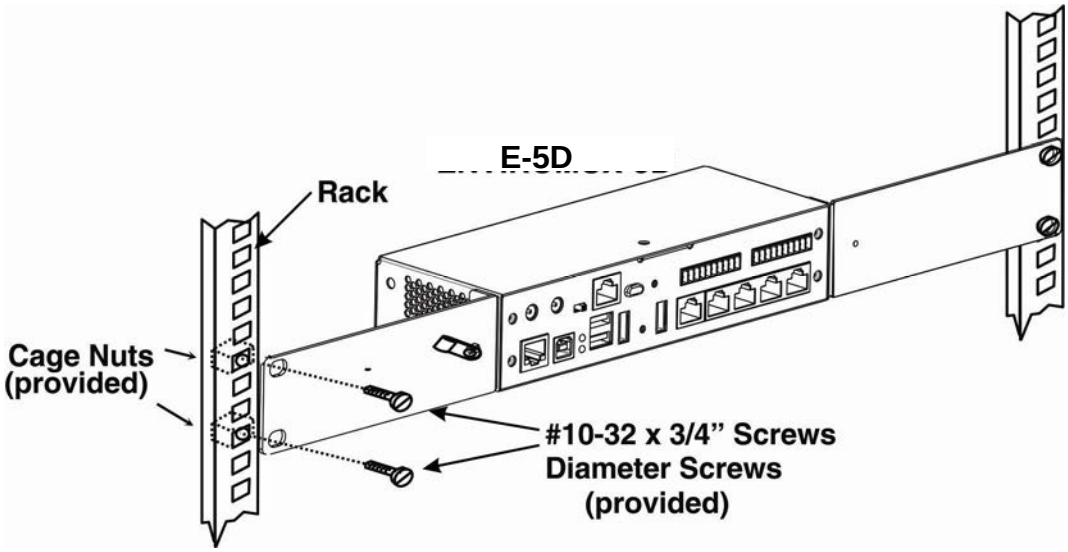


Figure 4- Mount E-5D/2D in a rack

DIN Rail Mounting

If DIN rail mounting is preferred, and you have purchased the E-5D-D or E-2D-D, then a DIN rail bracket has been pre-installed on the ENVIROMUX. Simply determine where on the DIN rail you want to place the ENVIROMUX and follow the instructions below for attaching it.

Note: You will either have a plastic DIN rail clip or a metal one. Instruction for each is provided below.

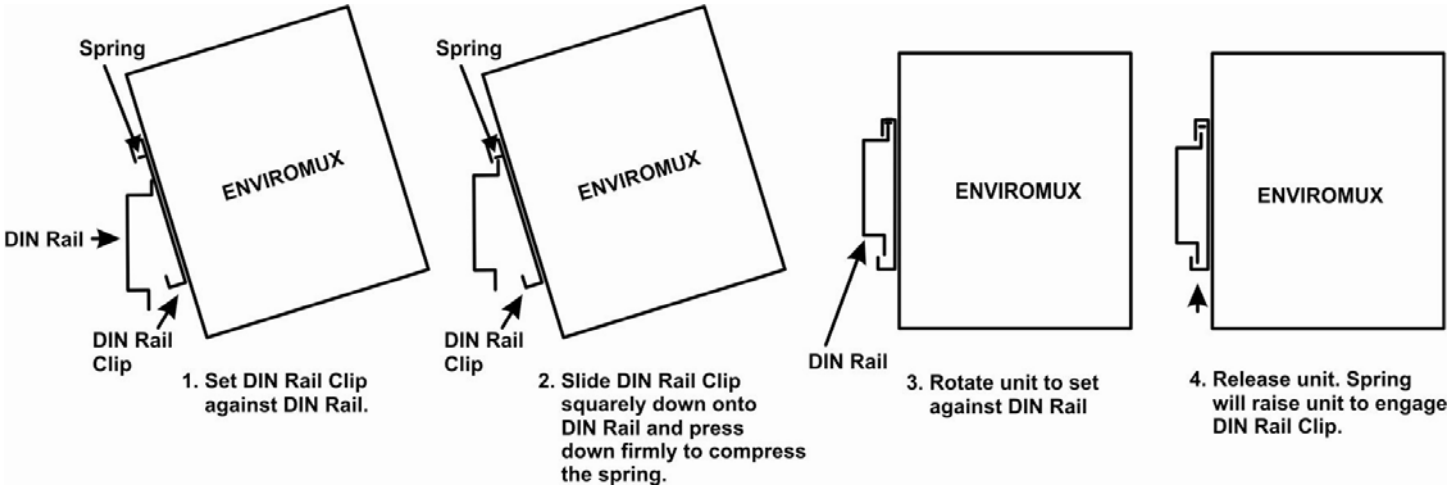


Figure 5- Mount E-5D/2D to DIN rail- plastic clip

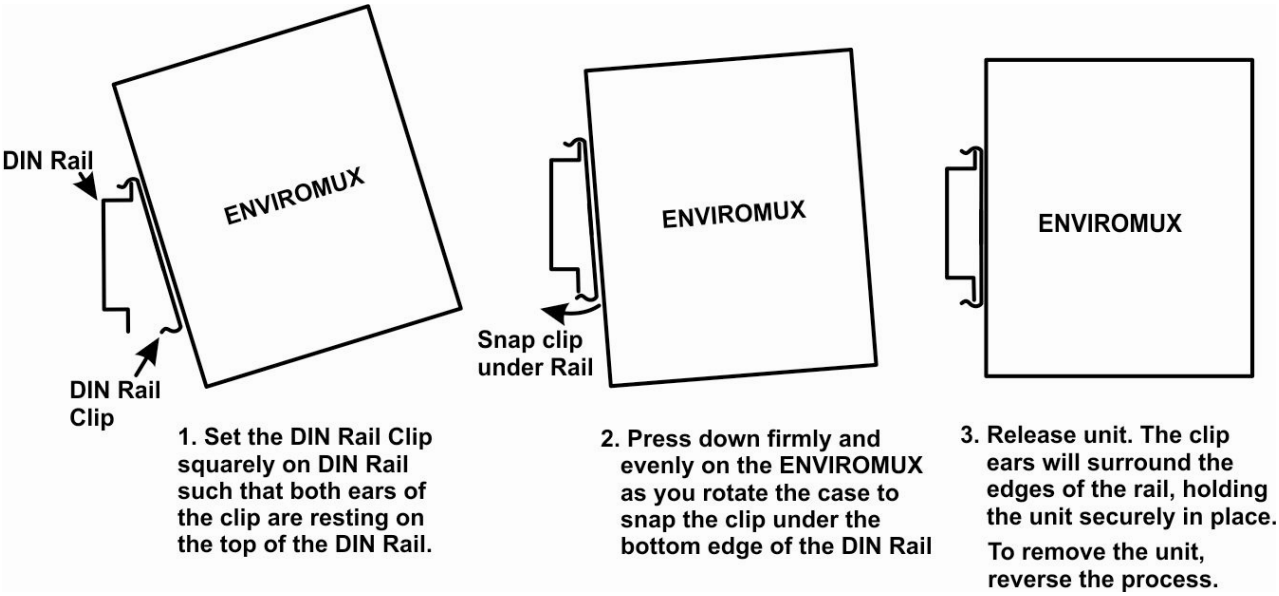


Figure 6- DIN Rail Mount with metal clip

Sensor Attachment

Connect the desired sensors (sold separately) to the available ports on the ENVIROMUX. Sensors come with one of two connection methods, RJ45 and individual wires for terminal connection. This section explains both methods of connection. Configuration of these sensors will come later in this manual.

RJ45 Sensor Ports

1. Connect each external sensor having an RJ45 male connector on it (E-STS, E-STHSB, E-LDS) to one of the female connectors labeled "RJ45 Sensors" on the ENVIROMUX. Male connectors should snap into place. Cables may be up to 1000 feet in length. See page 163 for wiring specification and pinout.

Note: It is very important to locate the temperature and/or humidity sensors away from ventilation sources and fans.

If CATx cabling will be installed near sources of EMI (electric motors, light ballasts, etc) use shielded cable to reduce the introduction of noise to the circuits. Otherwise, communications between the sensor and ENVIROMUX may be unreliable.

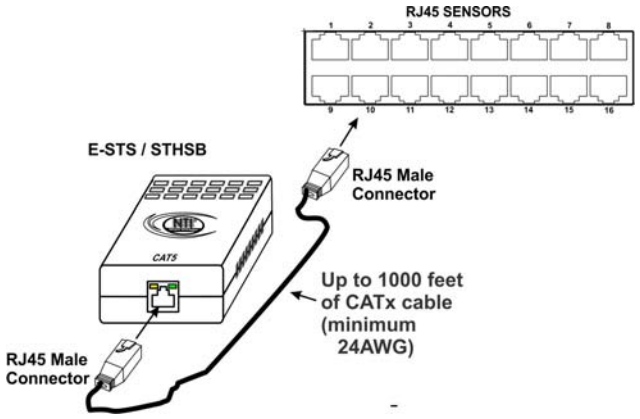


Figure 7- Sensors connected by cables with RJ45 connectors

The RJ45 SENSORS ports can be used to connect a variety of sensors. Specifically on the E-16D, the combined power load of all 12VDC sensors on each row of ports (ports 1-8 is one row and ports 9-16 is the second) **cannot exceed 500mA per row**. Some sensors use more power than others. The table below provides the top power users:

Sensor	12VDC Power Consumption in mA	Sensor	12VDC Power Consumption in mA
E-S420MA-24V	130	E-ACLM-V	70
E-ACLM-P	130	E-S5VDC(-5V)	100

Caution: Be careful not to overload the E-16D as failure may occur and damage to the ENVIROMUX may result.

2. Some sensors do not have RJ45 connectors on them and instead have terminal blocks. These can either be connected to the "DIGITAL IN" connectors or they can be terminated and plugged into the remaining RJ45 connectors (see figure-right). (The illustration uses CAT5 patch cable to make cable connection easy.) Some examples of these sensors include E-IMD, E-IMD-CM, E-VSS, E-SDS, and E-GBS. Cables may be up to 1000 feet in length.

Note: For sensors requiring 5VDC power source, connect the wht/brown wire to pin 4 instead of pin 7.

All contact sensors can be wired in this way and use the RJ45 sensor ports instead of the Digital In terminals if desired.

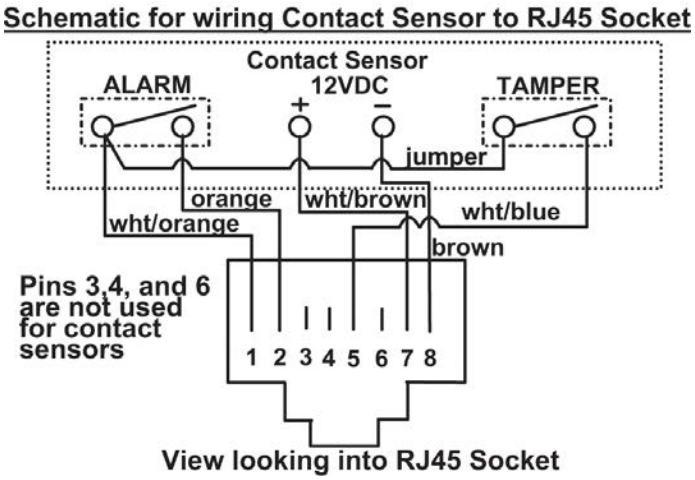


Figure 8- Contact sensor wired to RJ45 socket

Digital In Terminals

To connect contact sensors without using RJ45 connectors, terminal blocks have been provided labeled "DIGITAL IN". Two wire switch-only type sensors can be connected to the DIGITAL IN terminals as shown below. If the sensors require a 12V power source to operate, additional 12V and ground terminals have been provided on each model, with restrictions as shown. Connect each two-wire or four-wire contact sensor using 16-26 AWG wire.

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

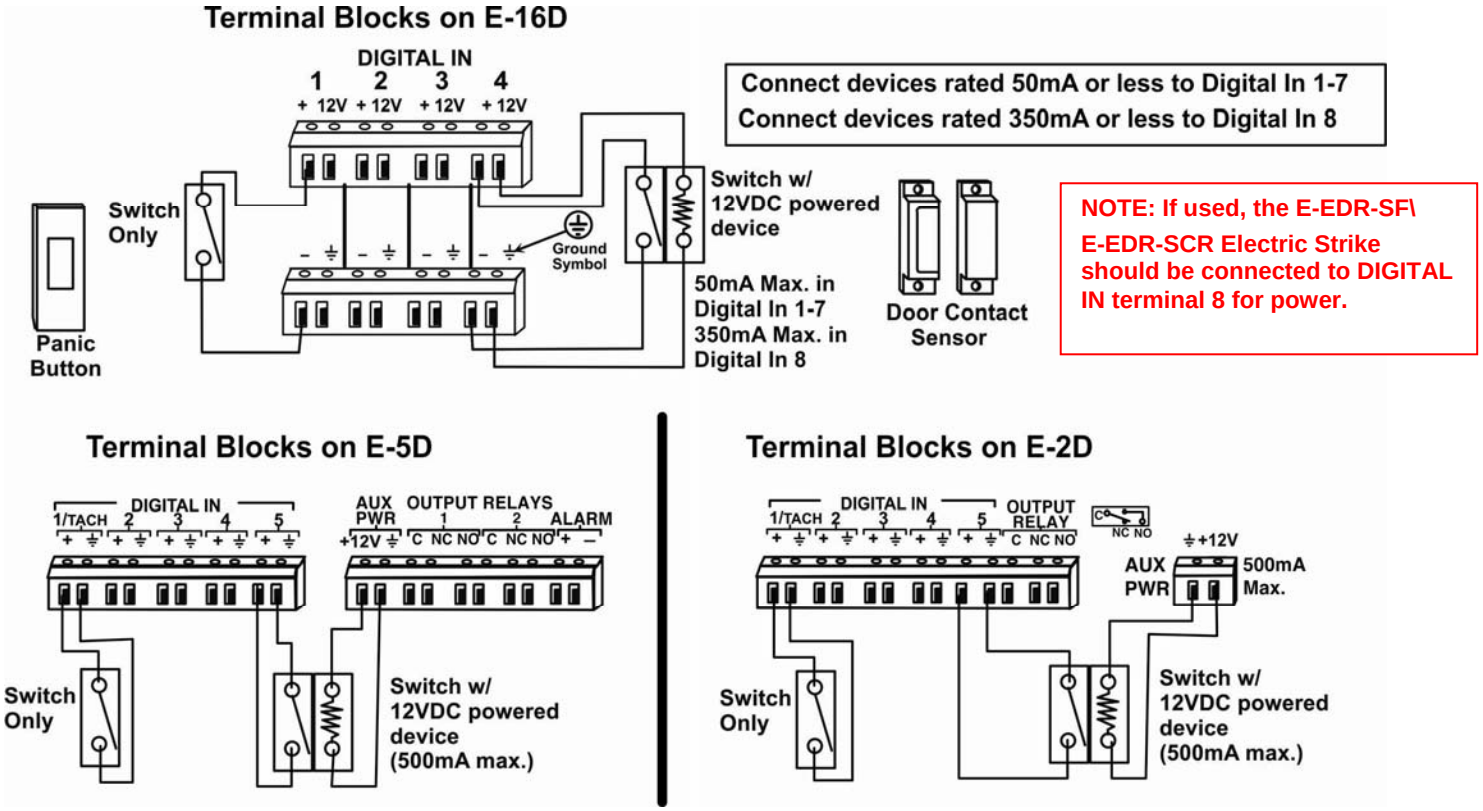


Figure 9- DIGITAL IN Terminal Connections

Liquid Detection Sensors

Liquid Detection Sensors are available for simple connection to **either** the "Digital In" terminals (use model E-LD) or the "RJ45 Sensor" ports (use model E-LDS).

Connect the two-wire cable (up to 1000 feet long) from a liquid detection sensor (E-LD shown in Figure 10-upper image) to a set of "DIGITAL IN" contacts. For added range (up to 1000 more feet), use an E-LDS (shown in Figure 10-lower image) and connect to an "RJ45 Sensor" port.

Note: If you are not looking to extend a liquid detection sensor (E-LDx-y) an additional 1000 feet, you can still connect the two-wire cable to pins 1 and 2 of the RJ45 connector (Figure 8) and plug it into an RJ45 Sensor Port instead of connecting it to a Digital In terminal. You do not have to use an E-LDS for the sensor to work, only to extend it an additional 1000 feet.

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 10)

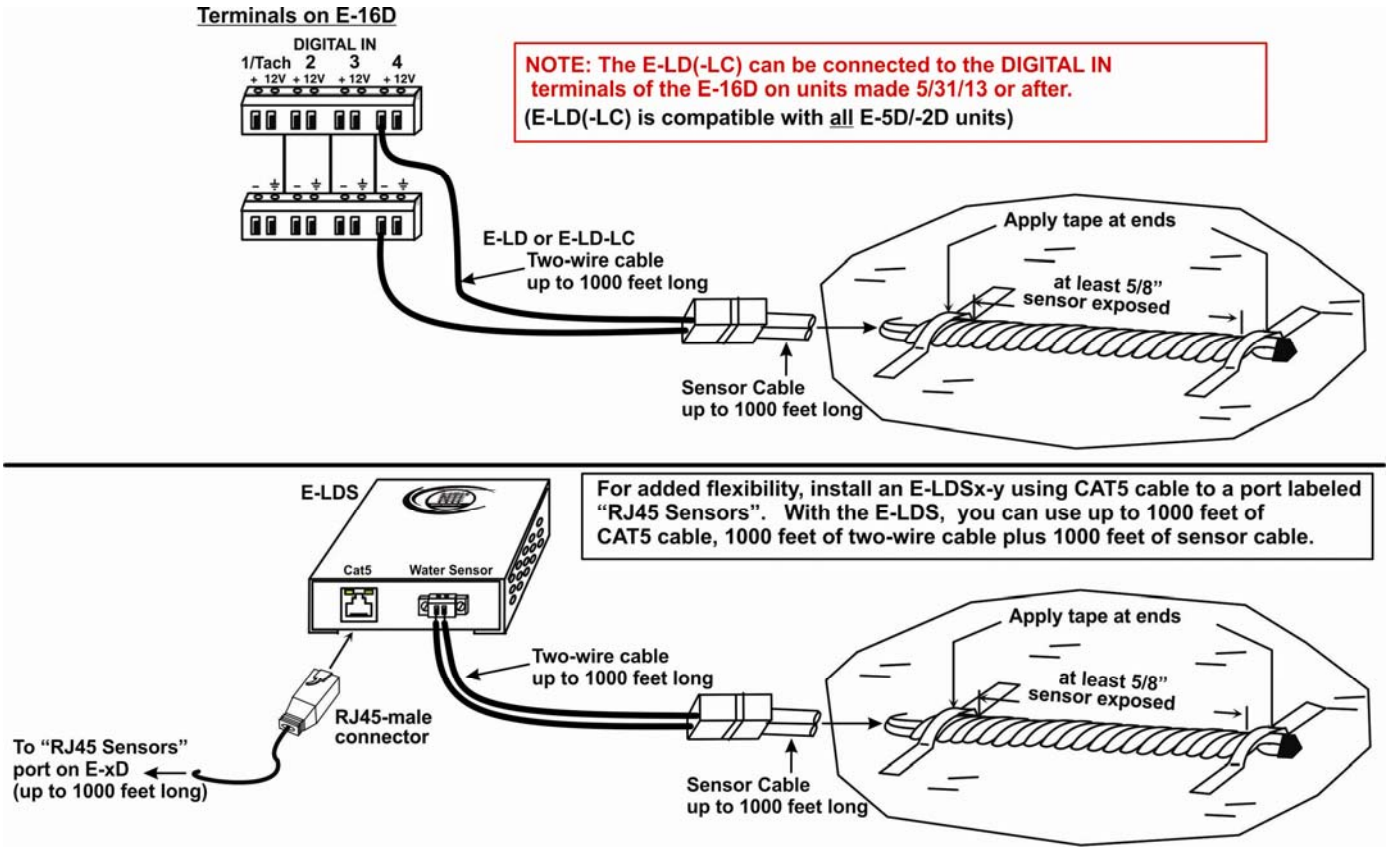


Figure 10- Secure liquid detection sensor with tape

To test the E-LD(S);

1. Configure the sensor (page 46). (Normal Status set to "Open", Sampling Period set to 5 seconds.)
2. Submerge at least 1/2 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 31) 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.

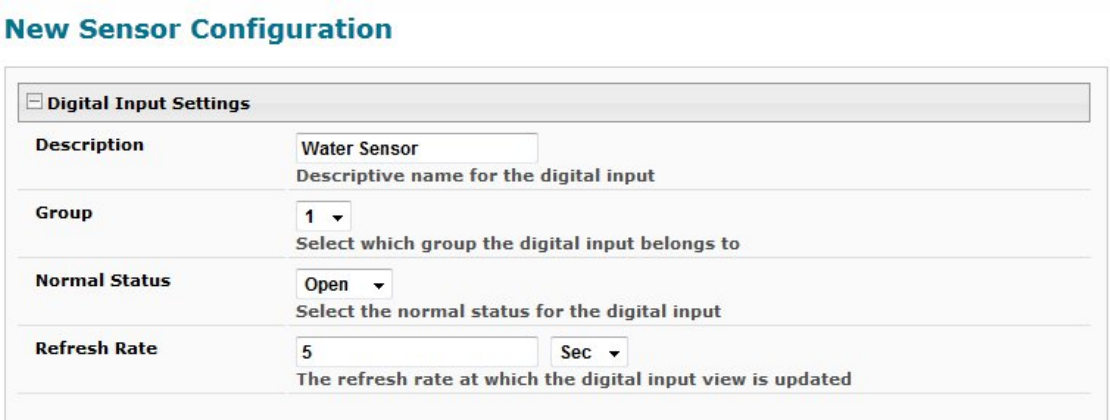
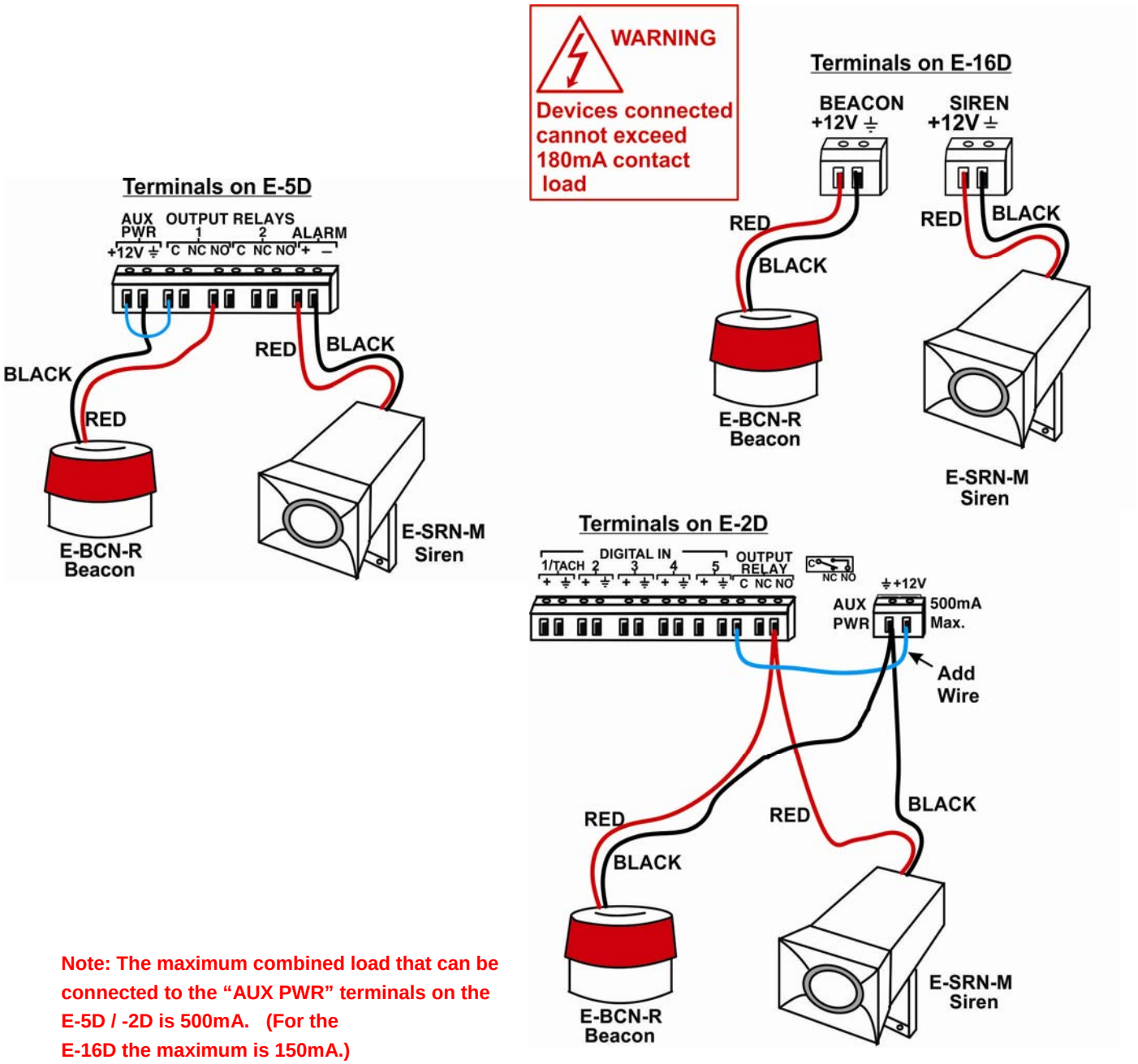


Figure 11- Portion of Water Sensor configuration page

Alarm(Beacon/Siren) Connections

Terminals have been provided for connection of the E-BCN-R Beacon and E-SRN-M Siren to use for visual alerts and audible alerts when configured. Devices such as this can be installed in locations best suited to get attention. The terminals for these connections will accept 16-26 AWG wire.



Note: The maximum combined load that can be connected to the "AUX PWR" terminals on the E-5D / -2D is 500mA. (For the E-16D the maximum is 150mA.)

Figure 12- Connect visual and audible external indicators

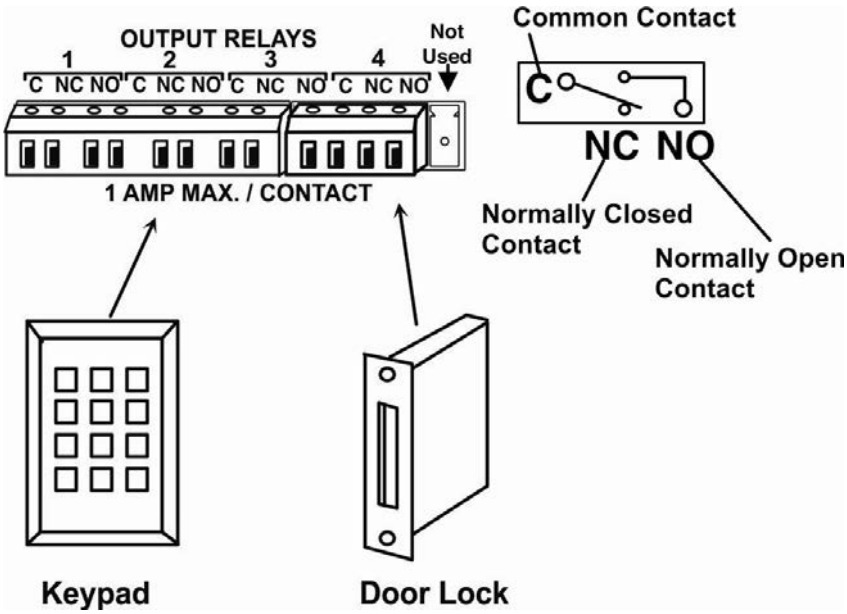
Connect Output Devices

For connection of additional output devices to be controlled by the ENVIROMUX, terminals labeled "Output Relays" have been provided. The contacts will work as switches to either close or open circuits (switch ON or OFF) when used. The "default" position of the switch is configurable independently (page 51) and how the switch reacts to sensor alerts can also be configured on any Sensor Configuration page (page 36).

The status page and any sensor configuration page describe the Output Relay's status as either "active" or "inactive".

- When a relay is "**active**", the circuit will be closed between the **Normally Open** and **Common** contacts of the relay.
- When a relay is "**inactive**", the circuit will be closed between the **Normally Closed** and **Common** contacts of the relay.

WARNING **OUTPUT RELAY dry contact ratings must not be exceeded. Dry contact rating: DC 30V, 1A; AC 100V, 500mA. The OUTPUT RELAY contacts are not to be connected directly to AC mains wiring.**



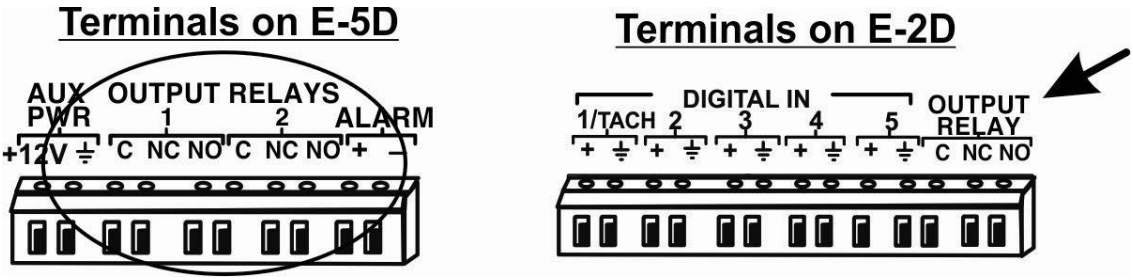


Figure 13- Install additional devices to output terminals

Terminal Connection for RS232

If control via serial connection is going to be used, serial control can be achieved using the "USB Console" port (**all models**) or the "RS232" port (E-16D only) or "RS232 AUX" port (E-5D only). A terminal connection is accessible by the user "root" only.

To use the "RS232" port, connect one end of a CAT5 patch cable (supplied) to the port labeled "RS232" on the rear of the ENVIROMUX. Plug the other end of the CAT5 cable into an RJ45-to-DB9F adapter (supplied), and connect the adapter to the RS232 port on the control terminal. Follow the instruction in the Serial Control Manual for configuration and use of the Serial Control feature.

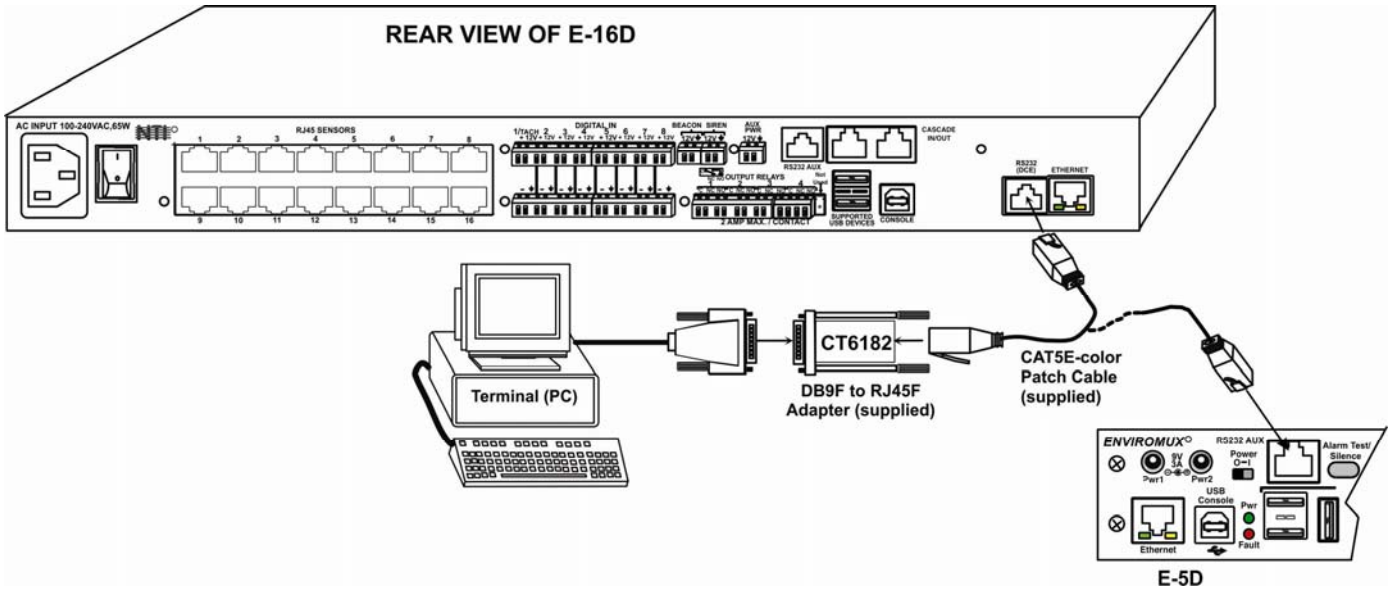


Figure 14- Connect a terminal for direct RS232 serial communication

To use the USB "CONSOLE" port, connect a USB cable (2 meter cable supplied) between the ENVIROMUX and your PC. Then install the drivers as described in the Serial Control Manual.

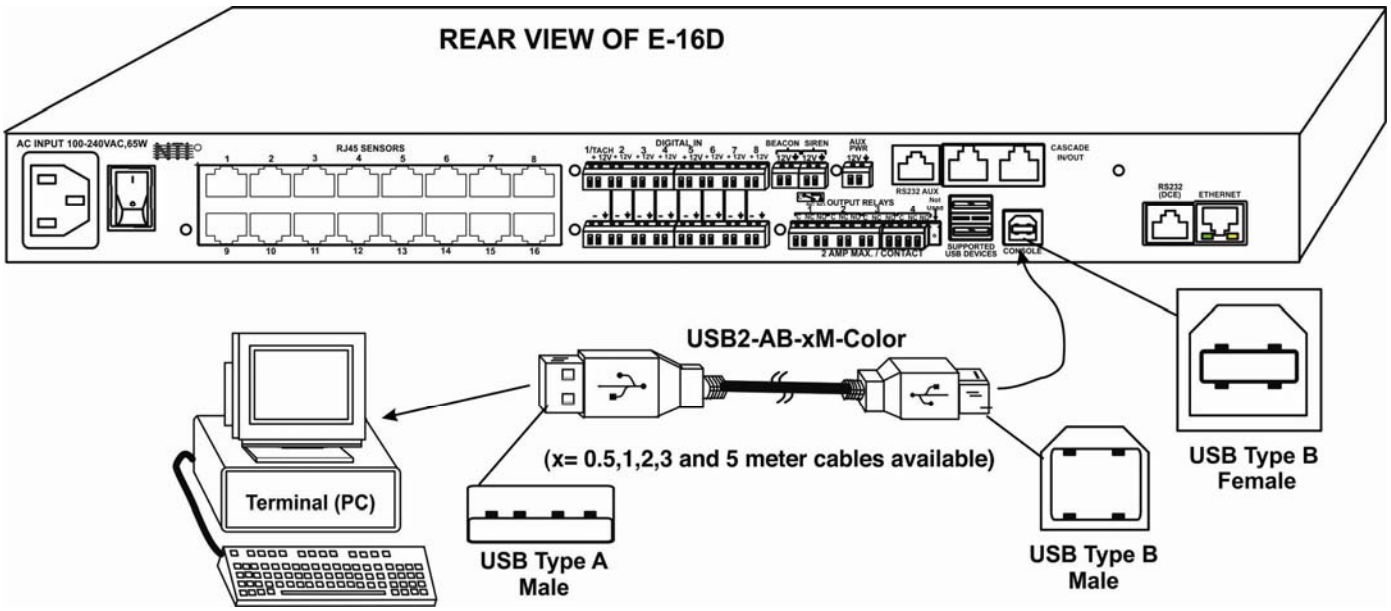


Figure 15- Connect a terminal using USB Console port

Ethernet Connection for Remote User Control

To make a remote connection, over the Ethernet, from anywhere on the local area network, connect a CAT5/5e/6 Ethernet cable with RJ45 male connectors on the ends, wired straight through (pin 1 to pin 1, pin 2 to pin 2, etc.). Up to 8 users can connect to the ENVIROMUX using the Ethernet at a time.

Note: A direct connection from a computer's Ethernet port to the ENVIROMUX "ETHERNET" port may also be made using the same cable.

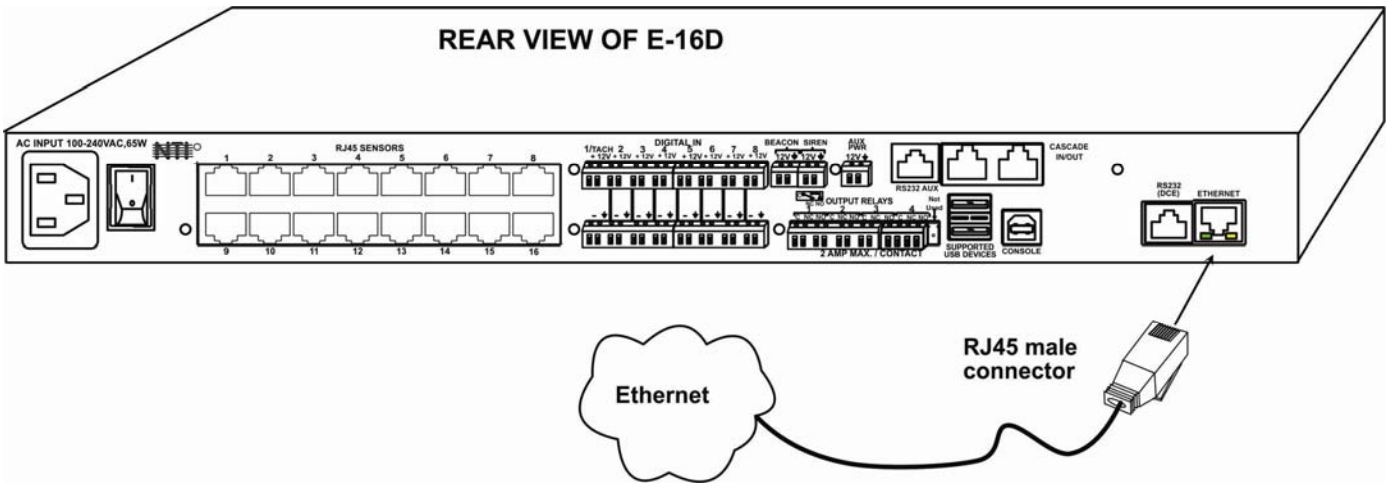


Figure 16- Connect ENVIROMUX to the Ethernet

Modem Connection

The ENVIROMUX includes support for a GSM modem to send alert notifications via SMS to a cell phone if desired. Either a USB GSM modem (**all** models) or a serial GSM modem (E-16D/-5D only) may be connected. Using a modem each user can receive SMS alert messages directly on their cell phone. When a USB 3G modem is used, SMS alert messages, all email messages, and web interface control over the ENVIROMUX is possible.

USB GSM Modem

To use a USB GSM Modem, a USB modem (with GSM SIM card configured for SMS messaging) can be connected to one of the USB ports on the ENVIROMUX. The remaining USB Type A connector(s) on the ENVIROMUX is available for the connection of a USB Flash Drive for data logging (pages 109 and 113).

Once installed, the ENVIROMUX will sense the modem and provide status information on the "Enterprise Setup" page in the web browser (page 64).

The USB GSM modems that have been tested and are confirmed to be compatible with the ENVIROMUX include:

- HiLink E303 3G Modem (**NTI # E-3GU**)
- E-Lins M300D Industrial USB Modem (**NTI# E-3GU-IND)**
- Zoom 4595 Modem
- iCON GI1505(M) 3G Modem
- iCON GI0452 3G Modem
- Teltonica USB/G10 Modem

Figure 17- Install USB GSM Modem

Cell phone 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 four standard sizes. The first is the size of a credit card (85.60 mm × 53.98 mm x 0.76 mm). The next, more popular "mini" version has a width of 25 mm, a height of 15 mm, and a thickness of 0.76 mm. The third, "micro" version measures 15 mm x 12 mm x 0.76 mm, and lastly the "nano" version measures 12.3 mm x 8.8 mm x 0.67 mm.

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

Your USB modem can be used for 3 different levels of functionality:

- SMS Messaging Only
- 3G Data Transfer And SMS Messaging
- 3G Data Transfer, SMS Messaging, and Web Interface

SMS Messaging Only

When using your modem only for SMS messaging, make sure the SIM card is for GSM communication (not CDMA), configured to send SMS messages, and that it is not locked (some SIM cards are "locked" to search for a specific IMEI number of the phone to operate).

Note: When configured for SMS messaging only, no access to the ENVIROMUX will be possible through the modem.

3G Data Transfer And SMS Messaging

To use your USB modem for 3G Data connection, your SIM card must be configured to support 3G data connections and have either **public or private** IP address. Make sure the account associated with the SIM card also has SMS messaging enabled if this feature will be used. With 3G data connection support, the ENVIROMUX can be configured (page 70) to send all alert messaging through the USB modem instead of requiring an Ethernet connection for these messages.

Note: When configured for 3G data transfer and SMS messaging only, no access to the ENVIROMUX will be possible through the modem.

3G Data Transfer, SMS Messaging, and Web Interface

To access the web interface through your USB modem, your SIM card must be configured to support 3G data connections and have a **public** IP address. The ENVIROMUX can be configured (page 70) to send all alert messaging through the USB modem instead of requiring an Ethernet connection for these messages. With a public IP address, you will also be able to access the web interface using the IP address of the SIM card for full control of the ENVIROMUX through the modem.

Make sure the account associated with the SIM card also has SMS messaging enabled if this feature will be used.

Contact your service provider to obtain a SIM card with the features you desire.

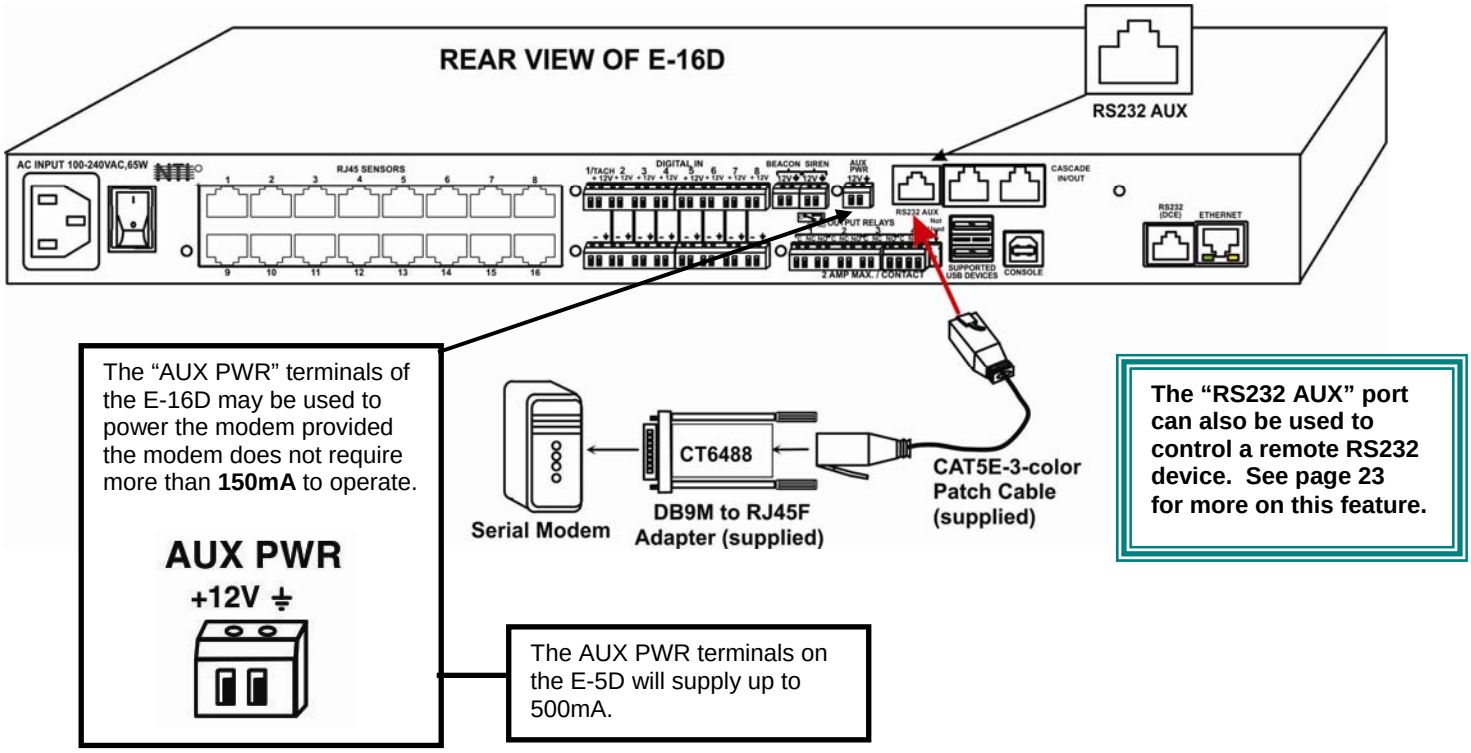
SMS Relay Via SNMP

Your ENVIROMUX can be used as an SMS relay through an SNMP browser (requires firmware version 2.51 or later). SMS messages, up to 160 characters in length, can be sent to up to 4 different phone numbers each when your SNMP browser is properly configured. For more details, see page 155.

Serial GSM Modem

To use a serial modem (E-16D/-5D only), connection of the modem to the ENVIROMUX requires a CAT5 patch cable and RJ45-to-DB9 male adapter (supplied). The modem connects to the "RS232 AUX" port and that port must be configured to use as a GSM Modem (page 61). The firmware in the ENVIROMUX must be version 1.3 or later.

Operation and use of the modem will be the same as that of the USB GSM modem. Once installed, the ENVIROMUX will sense the modem and provide status information on the "Enterprise Setup" page (page 64).



Up to 1000 feet of CAT5E (350Mhz) cable may be used at a baud rate of 115,200bps.

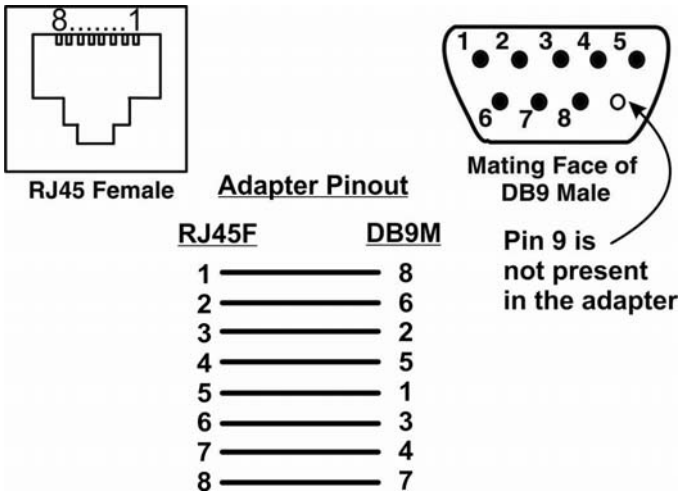
Serial Modems Tested Include:

- Sierra Wireless Airlink MP895
- Four-Faith F1103 (**NTI# E-GSM-IND**)
- MultiTech MTCBA-G-F2
- Enfora GSM1308
- Teltonika ModemCOM/G10

CT6488 Adapter

DB9 Male to RJ45 Pin Assignments

RJ45	Signal		DB9M	Signal
1	RTS	Connected to	8	CTS
2	DTS	Connected to	6	DSR
3	TxD	Connected to	2	RxD
4	GND	Connected to	5	GND
5	GND	Connected to	1	DCD
6	RxD	Connected to	3	TxD
7	DSR	Connected to	4	DTR
8	CTS	Connected to	7	RTS



Power Connection-E-16D

Connect the power cord supplied to the IEC connector on the rear of E-16D. Plug the other end into AC mains and use the switch to power ON ENVIROMUX.

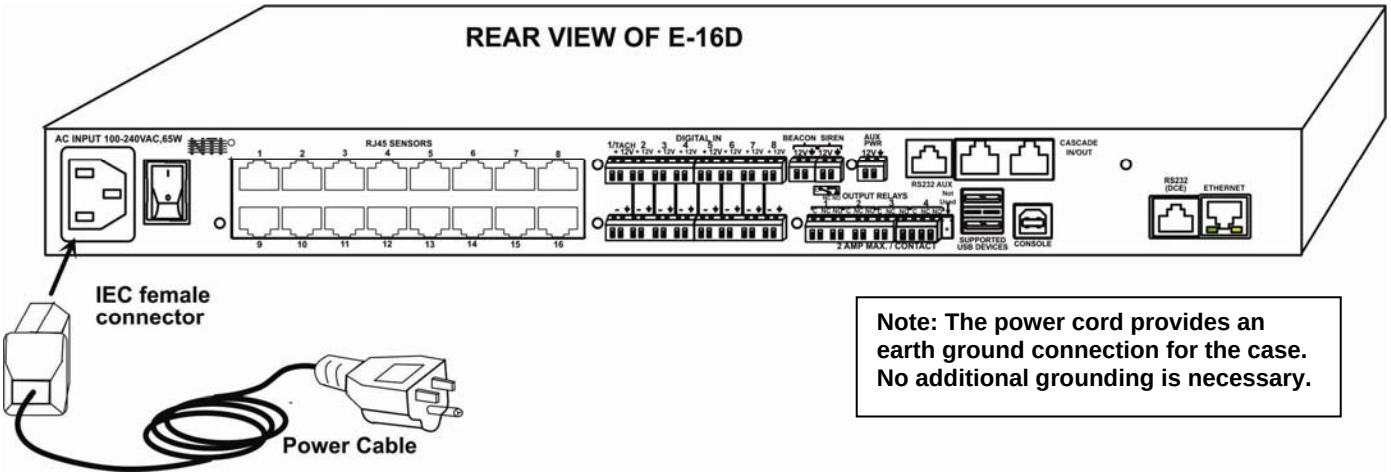


Figure 18- Connect the power cord

Dual Power Option

The E-16DDP has two IEC connectors on the rear, for connection to two separate power sources. If the power source connected to "PWR 1" fails, the ENVIROMUX will automatically and without interruption switch over to the power source connected to "PWR 2" before switching to the battery backup (page 112).

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

Note: The power ON/OFF switch is located on the front panel of ENVIROMUX when two IEC connectors are present.

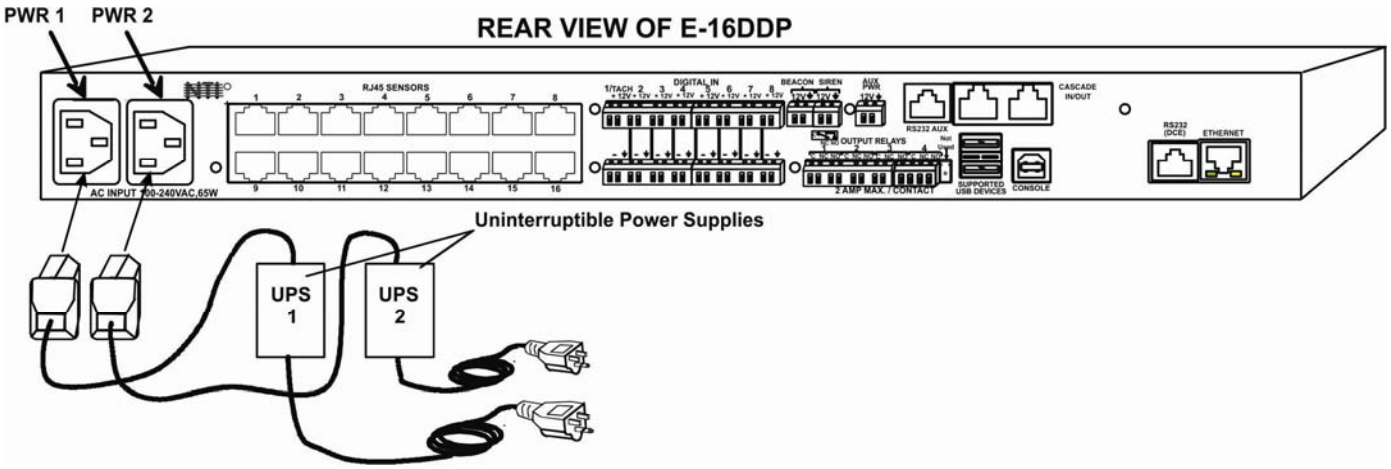


Figure 19- Power connections for ENVIROMUX with Dual Power Option

DC Power Option

The E-16D is available with connections for DC power connection. The E-16D-**48**V can be connected to a 36~72VDC (48VDC nominal) power supply. The E-16D-**24**V can be connected to a 18~36VDC (24VDC nominal) power supply. Each has connections on the rear for a user-supplied DC power supply (minimum 27 watt). This is typically used when the ENVIROMUX is installed in a Telecom environment. The E-16D-xxV will accept a DC power source with positive or negative polarity. A removable 3-pole screw terminal is provided for easy connection. The image below shows an E-16D-48VDP, which has dual 48VDC power connections for a dual power supply option (also available for the 24VDC model).

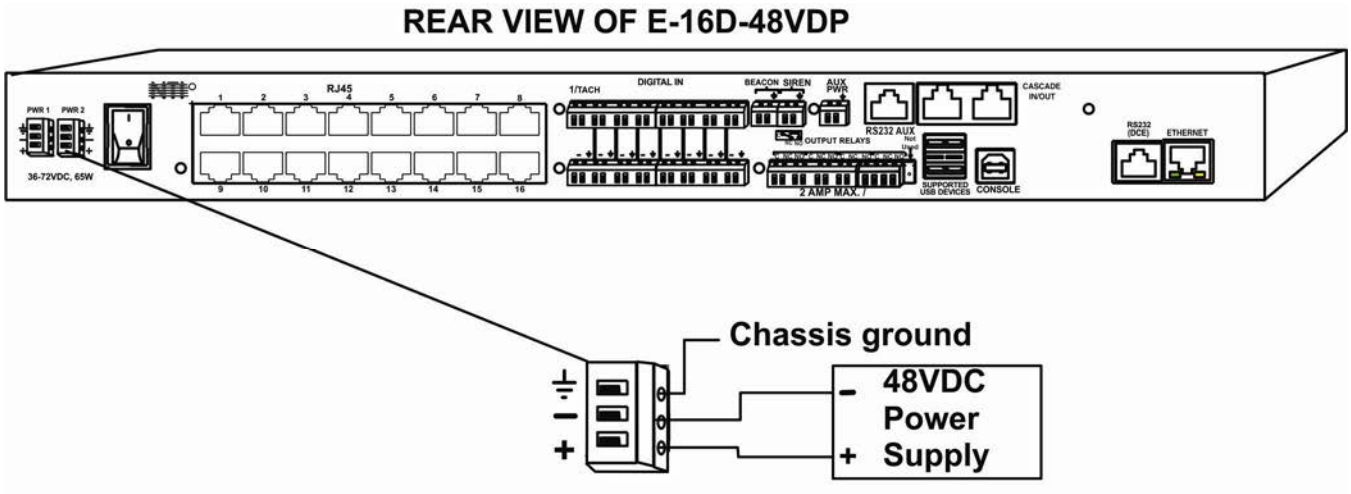
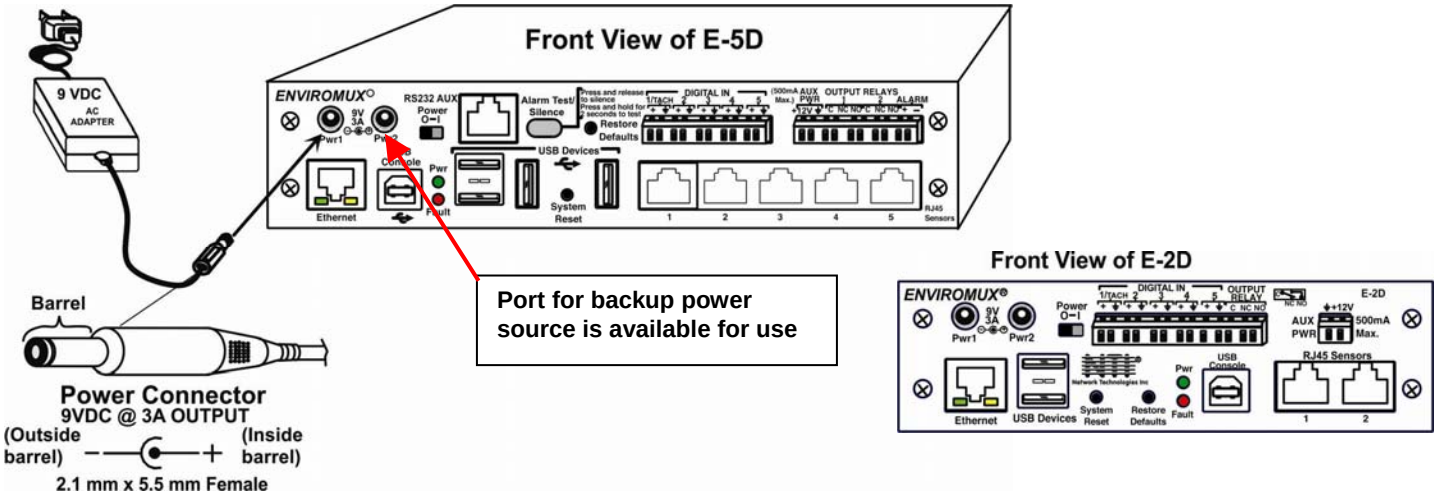


Figure 20- 48VDC Power Option Connections

Power Connection- E-5D/-2D

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

Connect the AC adapter to the connection marked "PWR1" or “PWR2” on the ENVIROMUX and plug it into an outlet. If you have an alternate source of 9V power for the ENVIROMUX, the second PWR connection is provided to make that source available. If the source connected to “PWR1” is lost for any reason, the ENVIROMUX will automatically switch to receiving power from the source connected to “PWR2”.



E-5D(B)-IND uses a 9VDC 5A power supply with 2.5mm x 5.5mm Female connector.

Figure 21- Connect the AC adapter and power-up

The E-5D-48V is available with connections for a 18~72VDC (24 or 48VDC nominal) user-supplied power supply. This is typically used when the ENVIROMUX is installed in a Telecom environment. The E-5D-48V will accept a DC power source with positive or negative polarity. A removable 3-pole screw terminal is provided for easy connection. The image below shows an E-5D-48VDP, which has dual 18-72VDC power connections for a dual power supply option.

For your convenience, the power jacks for connecting and AC adapter are also provided, and may be used as well. These jacks will accept 9-12VDC (9VDC 3A power supply may be purchased separately-order PWR-SPLY-9V3A). All power connections can be used simultaneously without damage to the ENVIROMUX.

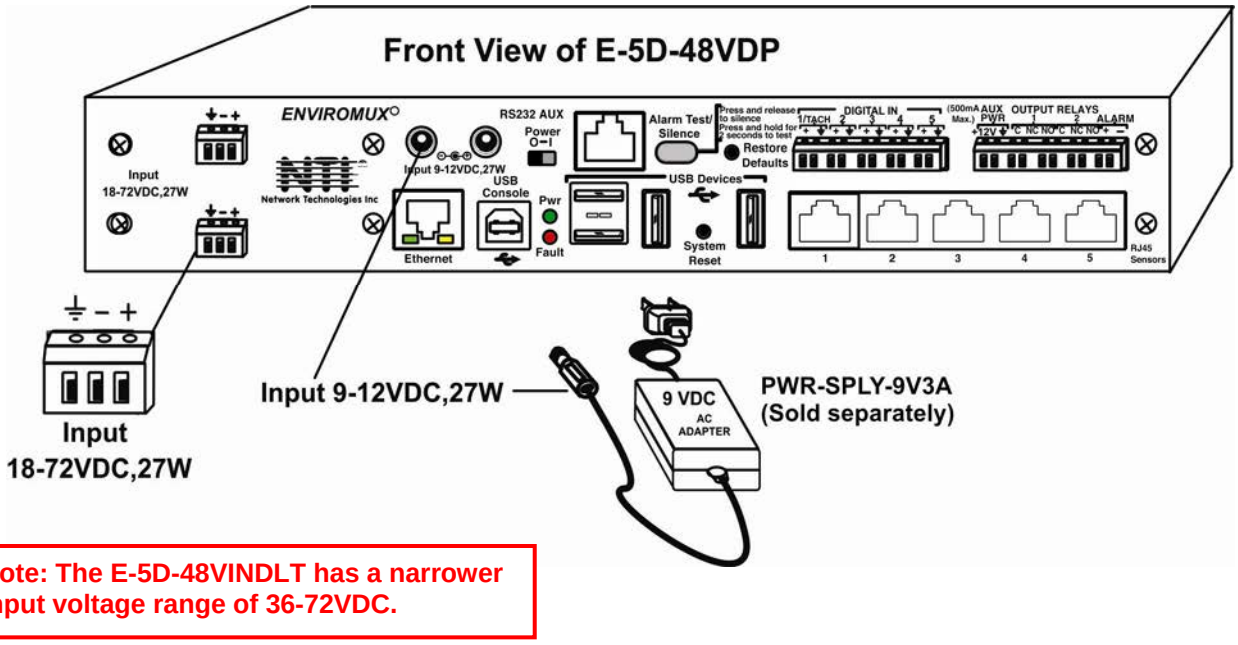


Figure 22- Power connections on E-5D-48VDP

Note: The power supply monitor on the sensor summary page will only display the status of the 18-72VDC connections. The 9-12VDC power connections will be ignored on the E-5D-48V(DP) models.

Power Supply

No.	Type	Value	Status	Action
1	Power Supply	OK	Normal	Ack Dismiss Edit
2	Power Supply	OK	Normal	Ack Dismiss Edit

Figure 23- Power Supply sensors-Summary Page

Remote RS232 Device Control

The “RS232 AUX” port can be used to connect a remote serially-controlled device (E-5D and -16D only). Once connected, a user named “rs232” can login to the ENVIROMUX from a command prompt and begin sending commands directly to the serial device.

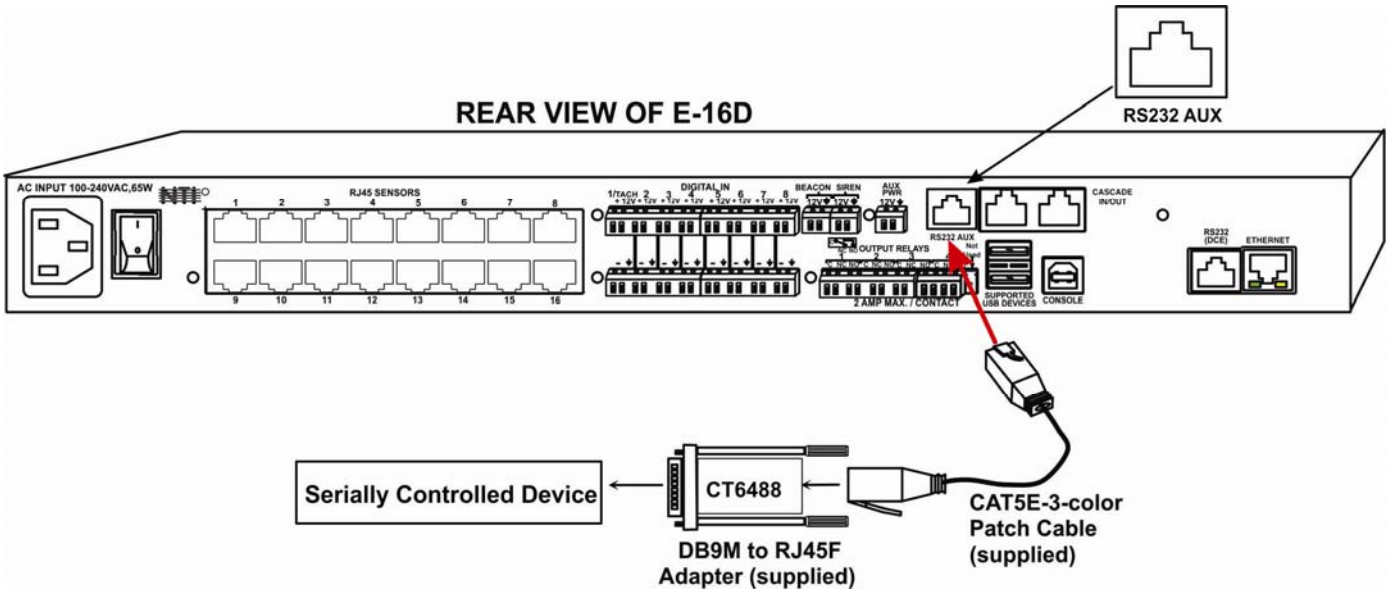


Figure 24- Connect serially controlled device

To control a remote serially-controlled device from the “RS232 AUX” port:

1. Configure the “Auxiliary Serial Port” under System Configuration (page 61) as a **Remote Serial Port** with the correct parameters for communication with the device.
2. Setup a user named “rs232” (**must be lowercase letters**) with password under User Configuration (page 75)

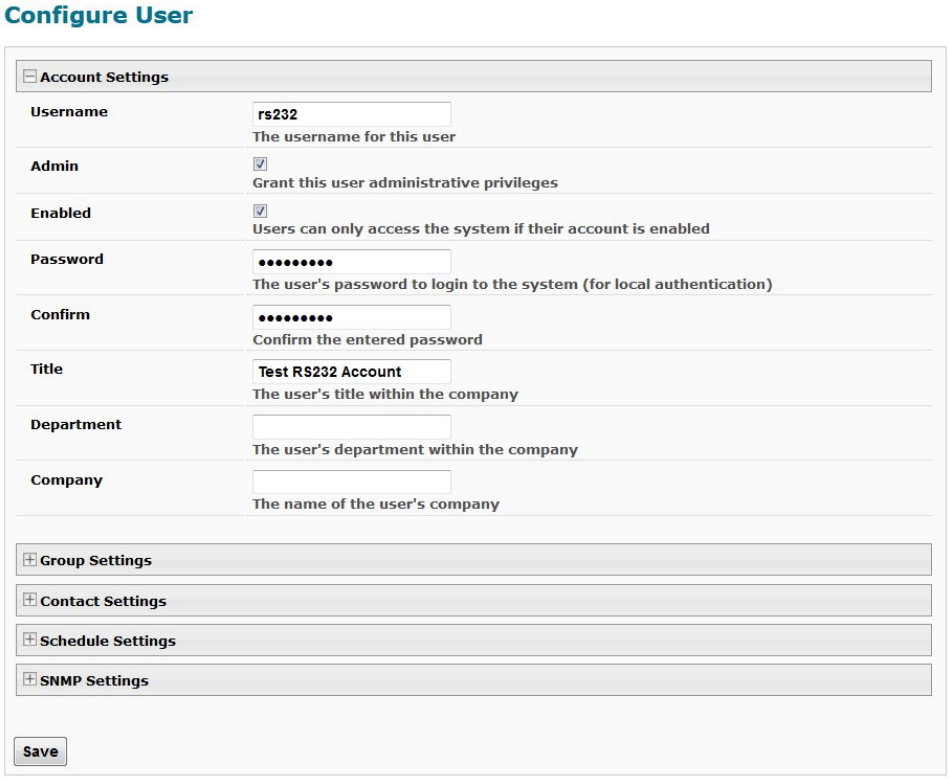


Figure 25- Create user "rs232"

3. Open a SSH client program (Putty, Tera Term, etc.), connect to the ENVIROMUX by entering the IP address of the ENVIROMUX.
4. When prompted for a login, enter "**rs232**".
5. When prompted, enter the password you have assigned.

With a successful login you will receive the message "Connected to RS232 port". You are now ready to send commands directly to the connected serially controlled device.

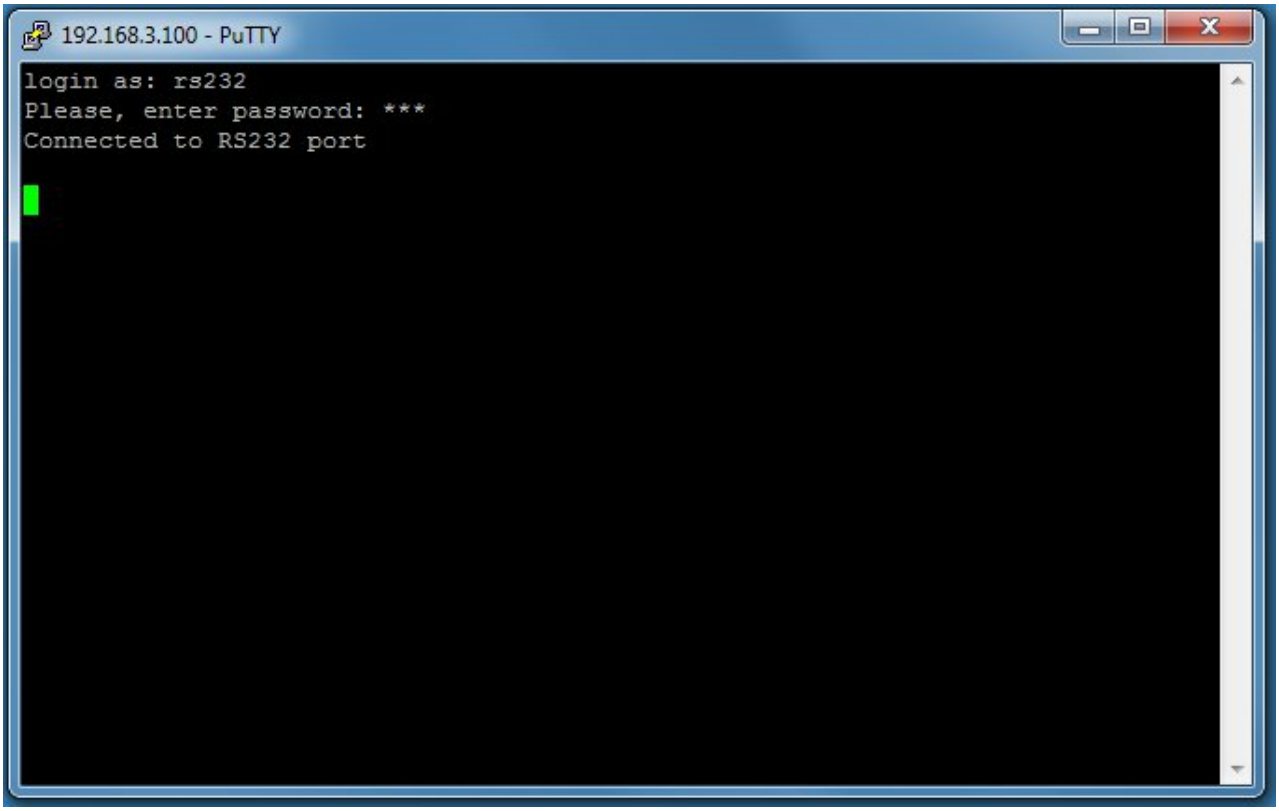


Figure 26- Connection to serial device successful

To exit the connection, close the command window.

OVERVIEW - USE AND OPERATION

The ENVIROMUX is controlled via RS232 or Ethernet using a terminal emulator, web browser, or SNMP monitor. The user interfaces are for viewing and configuring sensor data and system settings. However, full configuration of the system can be done only through the Web browser due to graphics limitations in the other interfaces.

The web interface allows for the configuration of the thresholds for all attached sensors, their alert methods, and the formats of the alerts. In addition, network information (IP address, subnet mask, default gateway, DNS, etc.), user administrative settings, and log settings can also be configured. All settings are saved in memory when applied. A user may also restore the unit back to its default settings at any time via the web interface (see page 60), text menu (see Serial Control Manual) or a button on the front panel (page 112).

Individual sensor status pages are available for each connected sensor. A sensor summary page allows the user to view the connected sensors' current values, threshold settings and alert statuses. Also, the user can view recorded sensor readings that have been stored in the system data log.

Sensors

The ENVIROMUX provides RJ45 sensor input jacks and screw terminal ports. Some available sensor configurations include Temperature, Humidity, or Temperature+Humidity, Liquid, Vibration, Smoke, Motion Sensor, Glassbreak detector, and AC Line Monitors. See page 2 for more on available sensors.

The temperature/humidity sensors have been given factory default settings and thresholds that can be changed (see page 36). Sensor readings can be reported continuously, only when readings change, or at a regular rate (for instance, a temperature reading could be updated once each hour).

Sensors connected to the terminals labeled "Digital In" must be manually configured, and can be any sensor of contact-closure / open-collector type that operate on 12VDC and 50mA, with a maximum load resistance of 10kΩ or less. (See page 48 for more info.)

IP Assignment

An IP address can be assigned to the ENVIROMUX through any of three methods:

- Using the NTI Device Discovery Tool (page 28)
- Through the web interface on the Network page (page 67)
- Using the RS232 interface (Serial Control Manual)

Initially, IP configuration will be the easiest to change using the NTI Device Discovery Tool, which will search for NTI devices on the user's network and allow IP assignment to them through its web interface. Other settings for subnet mask and default gateway may also be configured (see page 28). These settings must be configured properly in order to access the ENVIROMUX web interface.

User Management

The ENVIROMUX supports up to 16 user accounts plus the root account (page 75). Each user account is protected by local password authentication. Each user may be assigned "User" or "Administrative" privileges. Users accessing the ENVIROMUX will be granted access to only the monitoring functions, and will be able to view the log. An account with "Administrative" privileges has all of the privileges necessary to view and configure network settings, add/edit/delete other user accounts, configure sensors, etc..

Alerts

A high and low threshold limit can be set for each temperature or humidity sensor within the operating range of the sensor. Each open collector/contact-closure sensor can be set as normally-open or normally-closed. When a sensor takes a reading that is outside a threshold or a contact-closure sensor is not in its normal condition, an alert notification can be generated. The user can specify how often alert notifications are provided. Also, there is an adjustable alert delay time 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. Alerts may be sent if the condition of the sensor returns to normal or back within its threshold boundaries. Alert notifications (page 43) will be provided through any or all of six main methods:

- visible notification via the user interfaces (red LED on front panel, beacon, alert on webpage)
- emails (up to 17 different addresses)
- SNMP Traps
- SMS Messages (up to 68 different phone numbers)
- Syslog Messages
- audible notification via siren

Data and Event Logging

The ENVIROMUX can log sensor readings, sensor alerts, alert handling, sensor connections/removals, and user logins/logouts. The logs can be viewed at any time through the web interface (page 105). Additionally, as entries are generated, they can be emailed or sent as SNMP traps. Entries can be deleted from the logs via the web interface. The maximum size of each log is 1000 entries, listed in chronological order. Each log's behavior upon reaching this maximum size can be configured, allowing the log to either wrap (overwrite oldest entries), stop logging, or clear and start over. The entire log can be downloaded as a plain text file from the web interface at any time. Log entries can be removed individually, in groups, or all at once.

Email

The ENVIROMUX can access an outgoing SMTP server (authenticated or non-authenticated, with or without SSL encryption) to send email. Outgoing mail may contain pre-formatted alert notifications or data log messages (samples on page 105). The user can configure what conditions cause emails to be sent. The ENVIROMUX's email address can be configured through the web interface on the Enterprise Setup page (page 64), and SMTP server information can be configured on the Network Setup page (page 67). Up to 17 outgoing email addresses (112 characters max. including commas) may be configured (corresponding to the 16 user and 1 root email addresses). An example of email configuration can be found on page 124.

Syslog

The ENVIROMUX can send alerts as SYSLOG messages when a sensor enters/leaves alert mode, and for all log events. The destination for SYSLOG can be configured in each user profile (page 77). For detailed instructions on setting up Syslog, see page 131.

SNMP

The ENVIROMUX can send alerts as SNMP traps when a sensor 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, as well as configure sensor thresholds, sensor names, and the system name. Click on the checkbox for SNMP under contacts (page 77) for each user that should receive SNMP messages. The SNMP agent supports SNMP v1, v2c and v3.

Note: The SNMP MIB file (sems-16-v1.xx.mib), for use with an SNMP MIB browser, can be found at http://www.networktechinc.com/download/d-environment-monitor-16.html.

Modbus TCP/IP Support

The ENVIROMUX is equipped with Modbus TCP/IP support to enable PLC controls to read the value/state of sensors and read and command the state of relays.

External Modem

An external modem (GSM) can be connected to allow the system to send alert notifications via SMS messages. When a sensor crosses a threshold, an alert notification can be formatted to SMS message (see page 77) and the modem could transmit the message to pre-specified cellular numbers (up to 17- one for each user). The external modem can be supplied from an external power supply or from the USB port.

Power-on/Reset Operation

On power-up, after going through its boot sequence, the ENVIROMUX will launch the monitoring application, load any stored configuration values, and immediately identify and begin taking readings from any connected sensors. Alerts will be reported using the configured alert methods, and data will be logged using the stored preferences. A user can log in at any time after the system has launched the monitoring application (approximately 60 seconds after power is applied) to view and configure properties of the system and its sensors.

FYI: The boot sequence can also be initiated manually using the System Reset button. See page 111 for details.

Out-of-Box Operation

The operation of the unit directly out of the box is nearly identical to the Power-on/Reset operation. However, information about the unit will only be able to be monitored and controlled through the "RS232" or "CONSOLE" ports until valid network settings are assigned to the device (see page 67). The RS232 provides only limited configuration options, pertaining mostly to Ethernet settings.

Alert notifications will only be able to be viewed through the front panel until network settings are configured. Email and SNMP alert notifications must be configured within the web interface (page 59) before these methods can be used. The network settings must be compatible with the physical network to which the ENVIROMUX is attached. Once these configurations are made, they will be saved in the unit, even if the ENVIROMUX is powered-OFF.

Expandability

Multiple ENVIROMUX units may be used together on one system, so as to increase the number of sensors the user can have connected. Despite having multiple units, the user does not have to access the webpage of each ENVIROMUX individually. Up to 4 units can be cascaded from a single ENVIROMUX with all of the data from each of the units displayed on one webpage.

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-monitor-16.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. At http://java.com/en/download/manual.jsp will be a 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.

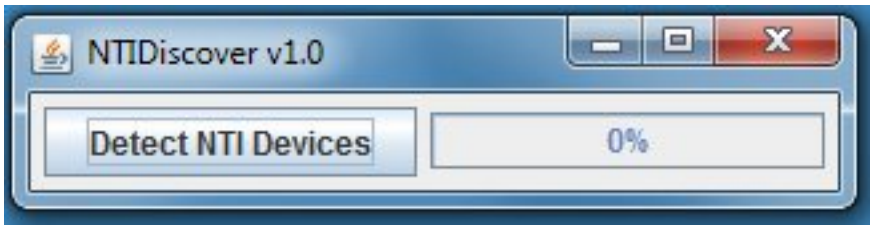


Figure 27- Device Discovery Tool

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

To Change a Device's Settings, 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.

To Refresh the list of devices, click on the **Refresh** button.

To Blink the LEDs of the unit, 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.

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

USE AND OPERATION VIA WEB INTERFACE

A user may monitor and configure the settings of any device connected to the ENVIROMUX using the Web Interface via any web browser (see page 4 for supported web browsers). To enable the Web Interface, connect the ENVIROMUX to the Ethernet (page 16). Use the Device Discovery Tool (page 28) to setup the network settings. Then, to access the web interface controls, the user must log in.

Note: In order to view all of the graphics in the Web Interface, the browser's JavaScript and Java must be enabled.

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 67.) 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 67 -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 for the ENVIROMUX is shown below):

http://192.168.1.21

Note: If an E-3GU USB modem is installed (page 17) and configured to enable access to the web interface through it (page 70), you can instead enter the IP address of the SIM card account (requires E-xD firmware version 2.5 or later.) If the ENVIROMUX is properly configured, you can view the SIM card IP address on the system information page (page 86).

Note: If HTTPS pages cannot be viewed in the browser ("The page cannot be displayed" message appears) try to disable SSL 2.0 and TLS 1.0 from advanced options of the browser.

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

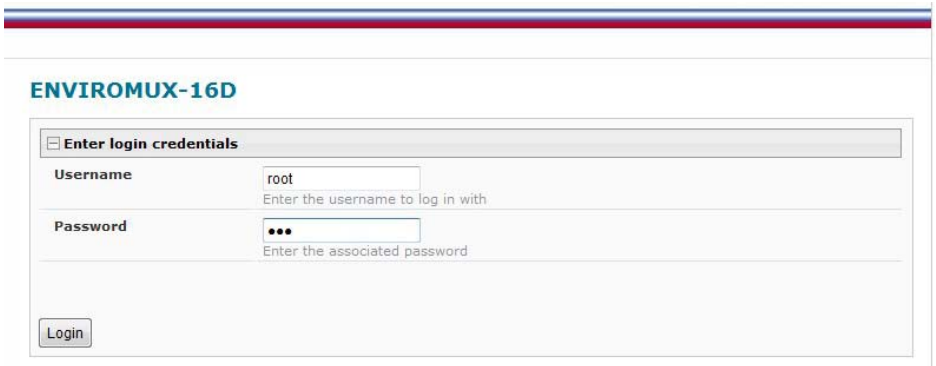


Figure 28- Login prompt to access web interface

With a successful log in, a screen similar to the following will appear:

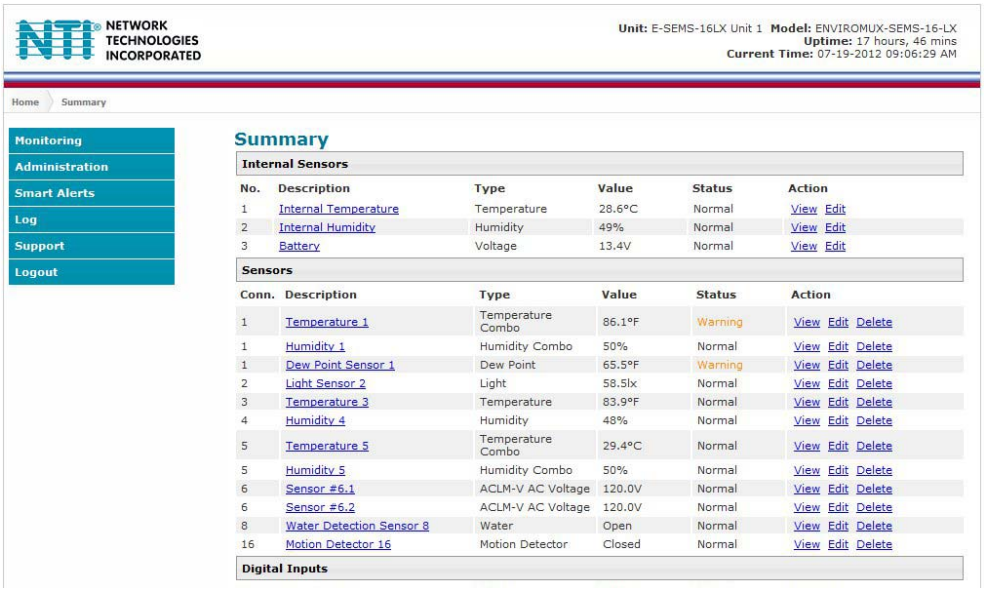


Figure 29- Summary page

The initial page includes the Summary page, and a menu to the left with access to all pages used to manage the functions of the ENVIROMUX.

Function	Description
MONITORING	Monitor all the sensor and data input received by the ENVIROMUX (below)
ADMINISTRATION	**Configure all network and multi-user access settings (page 59)**
SMART ALERTS	View and configure the Events used for Smart Alerts and the Smart Alerts themselves (page **94**)
LOG	View and configure the Event and Data Logs (page 107)
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 sensors, IP cameras, IP address data and more being monitored by ENVIROMUX.

Topic	Description
Summary	Lists all monitored items , including their type, description, value, and status
Alarm Summary	Lists all sensors that are in alarm state including their type, description, value, and status (page 34)
Sensors	Provides a link to view the status of specific Internal and External Sensors (page 35 and 40)
Digital Inputs	Provides a link to view the status of each Digital Input (page 48)
IP Devices	Provides a link to view the status of only the IP Devices and a link to add them (page 53)
IP Sensors	Provides a link to view the status of each IP Sensor configured (page 57)
Output Relays	Provides a link to view the status of each Output Relay (page 51)
IP Cameras	Provides a link to view each IP camera defined- with a link to the configuration page (page 53)
Power Supplies	Provides a link to view the status of each power supply- with a link to the configuration page (page 32)

Summary Page

The Summary Page displays the data for all categories of monitored items:

Category	Description
Internal Sensors	there are three inside the ENVIROMUX
Sensors	sensors that connect to the RJ45 connectors
Digital Inputs	sensors that connect to the terminals "Digital In"
IP Devices	IP Addresses that can be monitored by ENVIROMUX
IP Sensors	sensors connected to E-MICRO that are being monitored
Output Relays	Relays that open or close depending on alert status
AC Power	Indicates the status of the power supply(s)
Smart Alerts	Displays the status of each Smart Alert configuration (page **94**) and provides link to respond when triggered

To see the settings of each sensor, click on the link in the description column for the desired sensor. Click on the browser's Back button to return to the summary.

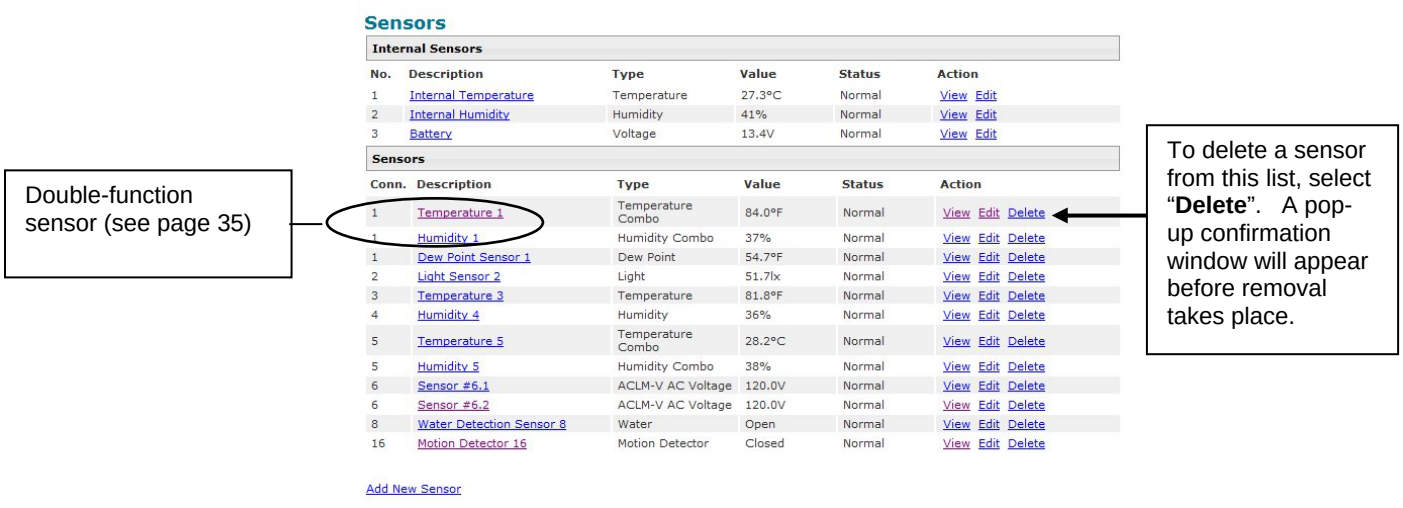


Figure 30- Summary Page

Power Supplies

The status of the power supply can be seen, and when a dual power supply model is present, both power supplies will be shown. Click on the power supply to open a web page that displays the type of item sensed, the status of the power supply, and the time and date of the most recent alert sent regarding the power supply.

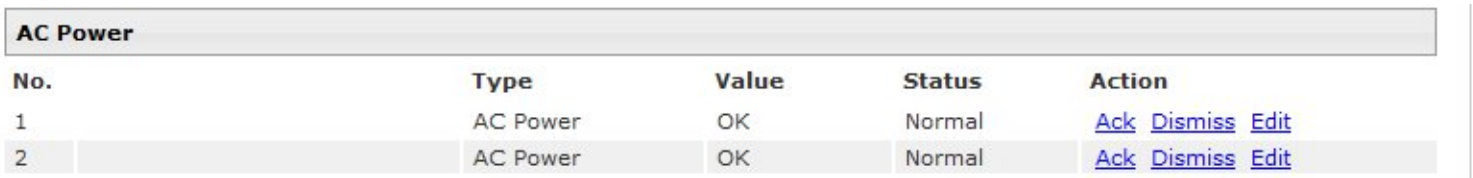


Figure 31- Power Supply status- Dual Power model

If the power supply 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 (below) elapses.

The **Edit** option allows the user to configure parameters of the power supply.

Power Supply Alert Configuration

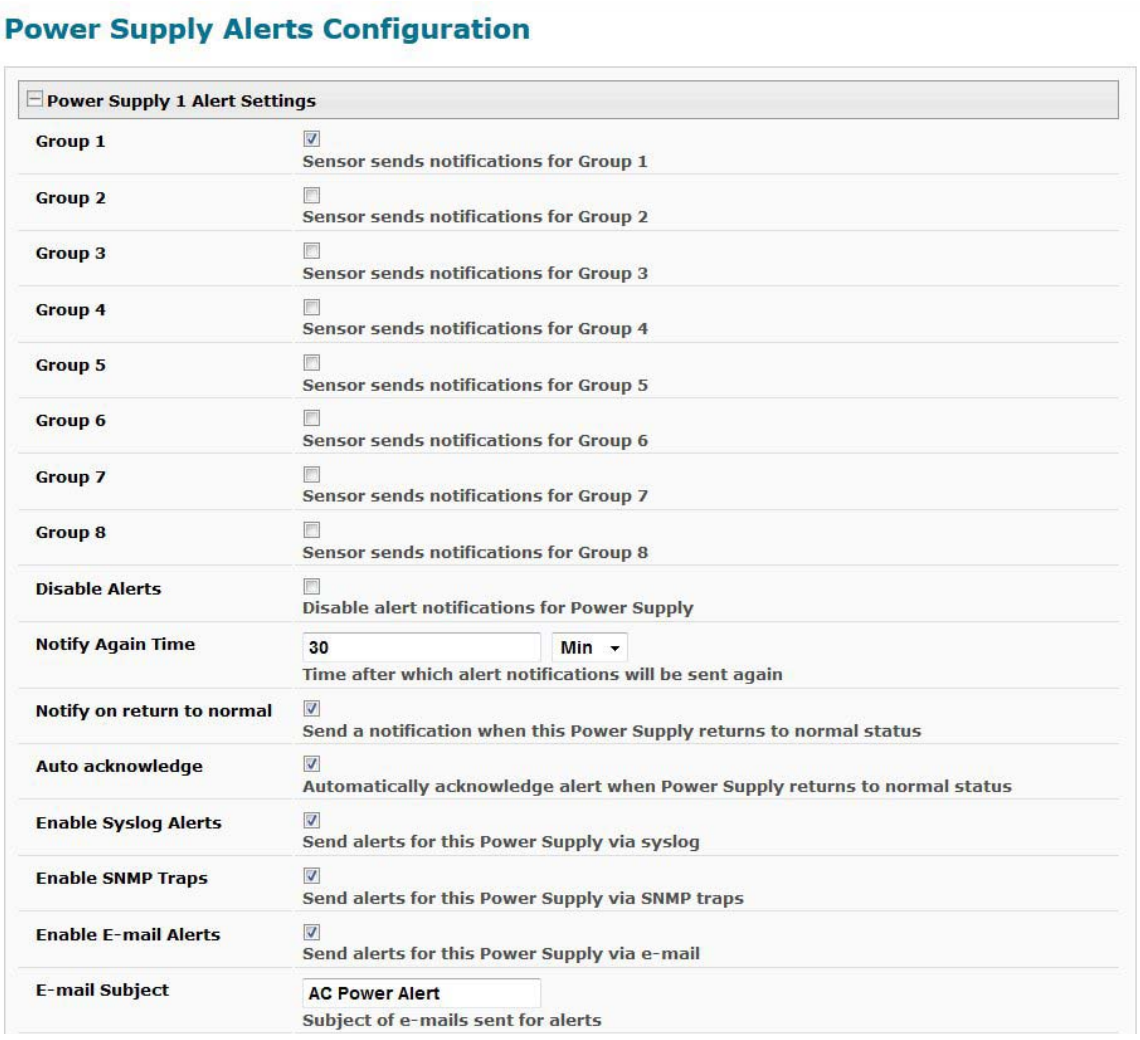


Figure 32- Power Supply alerts configuration-part 1

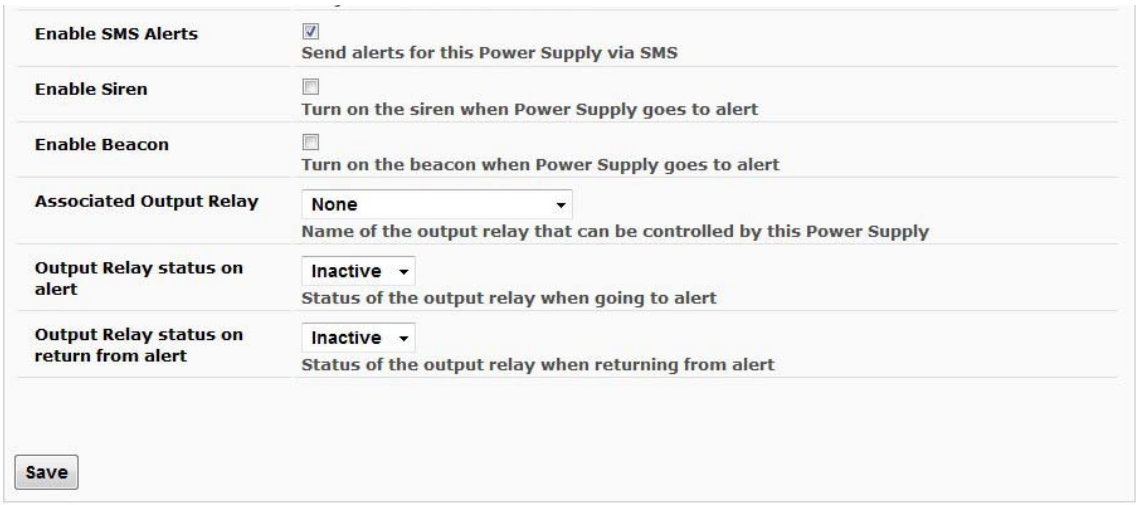


Figure 33- Power Supply alerts configuration-part 2

Alert Settings

Group: This is the group (or groups) of sensors the power supply sensor will belong to. Users that subscribe to alerts from this group will receive alerts from the power supply sensor. Each sensor can be configured to send alerts. Up to 8 sensor groups can be defined. Each user can receive alerts from any or all of the sensor groups.

Disable Alerts: Place a checkmark here if you don't want the ENVIROMUX to send alert messages regarding the AC power sensor.

Note: If alerts for a power supply are disabled, the associated output action will still take place. There just won't be any alert notifications that this is occurring. For example, this might be used to turn ON a device, such as a beacon, when the power supply loses power, and OFF again when power is restored. An alert message may not be desired under these circumstances.

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

Note: In the event of a line power failure, the battery backup (page 112) will power the ENVIROMUX for up to 1 hour.

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

Notify on return to normal: The user can also be notified when the power supply has returned to the normal operation by selecting the "***Notify on return to normal***" box.

Alert Notifications

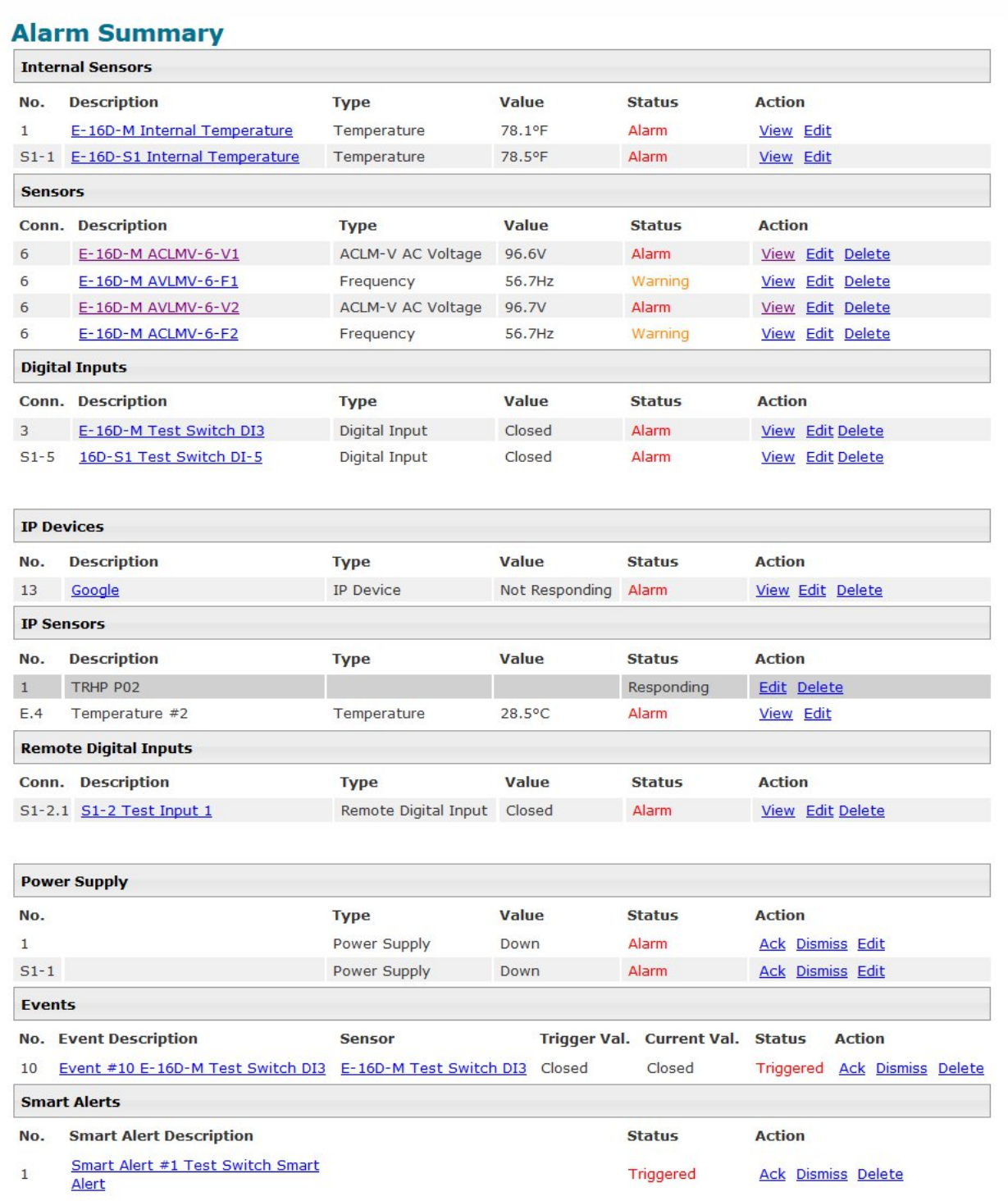
The alert can be configured to notify one or more users via email, SNMP traps (v1,v2c, v3), Syslog messages, or SMS alerts. It can also activate an audible siren, or an alarm beacon. Alerts are also indicated on the "Int Alert" or "Ext Alert " LEDs on the front of the ENVIROMUX and in the WEB interface.

Outputs

Each power supply can be associated with one of the connections labeled "Output Relays" (see page 14 or 51), and that connection can be set to “active” or “inactive” pertaining to the state of the contacts of the relay either on alert, or when returning to normal. The tamper can also block the output command generated by the alert. In this way other devices can be controlled by power supply alerts.

Alarm Summary

To view only those sensors in an alarm state, select the Alarm Summary page under Monitoring.



Alarm Summary

Internal Sensors

No.	Description	Type	Value	Status	Action
1	E-16D-M Internal Temperature	Temperature	78.1°F	Alarm	View Edit
S1-1	E-16D-S1 Internal Temperature	Temperature	78.5°F	Alarm	View Edit

Sensors

Conn.	Description	Type	Value	Status	Action
6	E-16D-M ACLMV-6-V1	ACLM-V AC Voltage	96.6V	Alarm	View Edit Delete
6	E-16D-M AVLMV-6-F1	Frequency	56.7Hz	Warning	View Edit Delete
6	E-16D-M AVLMV-6-V2	ACLM-V AC Voltage	96.7V	Alarm	View Edit Delete
6	E-16D-M ACLMV-6-F2	Frequency	56.7Hz	Warning	View Edit Delete

Digital Inputs

Conn.	Description	Type	Value	Status	Action
3	E-16D-M Test Switch DI3	Digital Input	Closed	Alarm	View Edit Delete
S1-5	16D-S1 Test Switch DI-5	Digital Input	Closed	Alarm	View Edit Delete

IP Devices

No.	Description	Type	Value	Status	Action
13	Google	IP Device	Not Responding	Alarm	View Edit Delete

IP Sensors

No.	Description	Type	Value	Status	Action
1	TRHP P02			Responding	Edit Delete
E.4	Temperature #2	Temperature	28.5°C	Alarm	View Edit

Remote Digital Inputs

Conn.	Description	Type	Value	Status	Action
S1-2.1	S1-2 Test Input 1	Remote Digital Input	Closed	Alarm	View Edit Delete

Power Supply

No.	Type	Value	Status	Action
1	Power Supply	Down	Alarm	Ack Dismiss Edit
S1-1	Power Supply	Down	Alarm	Ack Dismiss Edit

Events

No.	Event Description	Sensor	Trigger Val.	Current Val.	Status	Action
10	Event #10 E-16D-M Test Switch DI3	E-16D-M Test Switch DI3	Closed	Closed	Triggered	Ack Dismiss Delete

Smart Alerts

No.	Smart Alert Description	Status	Action
1	Smart Alert #1 Test Switch Smart Alert	Triggered	Ack Dismiss Delete

Figure 34- Alarm Summary Page

Internal Sensors

E-16D and -5D have three on-board sensors, which are permanently present:

- one temperature sensor
- one humidity sensor
- one power (battery) sensor

Internal sensors are monitored and fully configurable just as External Sensors are (see Figure 36 and page 40).

Internal sensors are always shown in the left menu of the web page and they cannot be removed.

External Sensors

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

RS485 Sensors

The following types of RS485 sensors are supported:

- Temperature Sensor (E-STS/STS-O/STSP)
- Humidity Sensor (E-SHS)
- Combined Temperature + Humidity Sensor (E-STHS/STHS-99/STHS-PRC) **(STHS-99/STHS-PRC also includes dewpoint reading)**
- Current Sensor (E-S420MA-24V)
- Voltage Detector Converter (E-S60VDC)
- AC Line Monitor (E-ACLM-V/ -P
- 5VDC Sensor Converter (E-S5VDC)
- Light Intensity Sensor (E-LIS)
- Dust and Smoke Sensor (E-DUST)

RS485 Sensor Management

The RS485 sensors are detected and identified by type automatically when they are connected to the RJ45 connector. The newly detected sensor will appear in the left menu of the web page under **Monitoring->Sensors**. A web page will be created for the sensor and the default name issued to the sensor by ENVIROMUX will be "***Undefined #n"***, where n is the number of RJ45 connector from 1 to 16.

If a **double-function sensor** is detected (E-STHS), it will be displayed as two sensors, each one with a single function (as shown in Figure 30). For example a Temperature/Humidity sensor will appear as separate sensors (Temperature sensor and a Humidity sensor) both with the same number connector. The default name of both sensors will be ***Undefined #n***, where n is the connector. A double-function sensor will be listed as a “Combo” type (i.e. Temperature Combo).

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

If the sensor is removed or communication lost for any reason (example: cable disconnected) the unit will detect this and show the sensor in "Non Responding" status. Question marks (???) will replace the name in the summary list. In this way the user will know the sensor has a problem or as been accidentally disconnected. If the user wants to remove a sensor (including a sensor now replaced by question marks) from the summary list, it must be done manually by selecting **Delete** in the summary listing (see Figure 30 on page 31). If Delete is selected, a pop-up will appear confirming this selection before removal takes place.

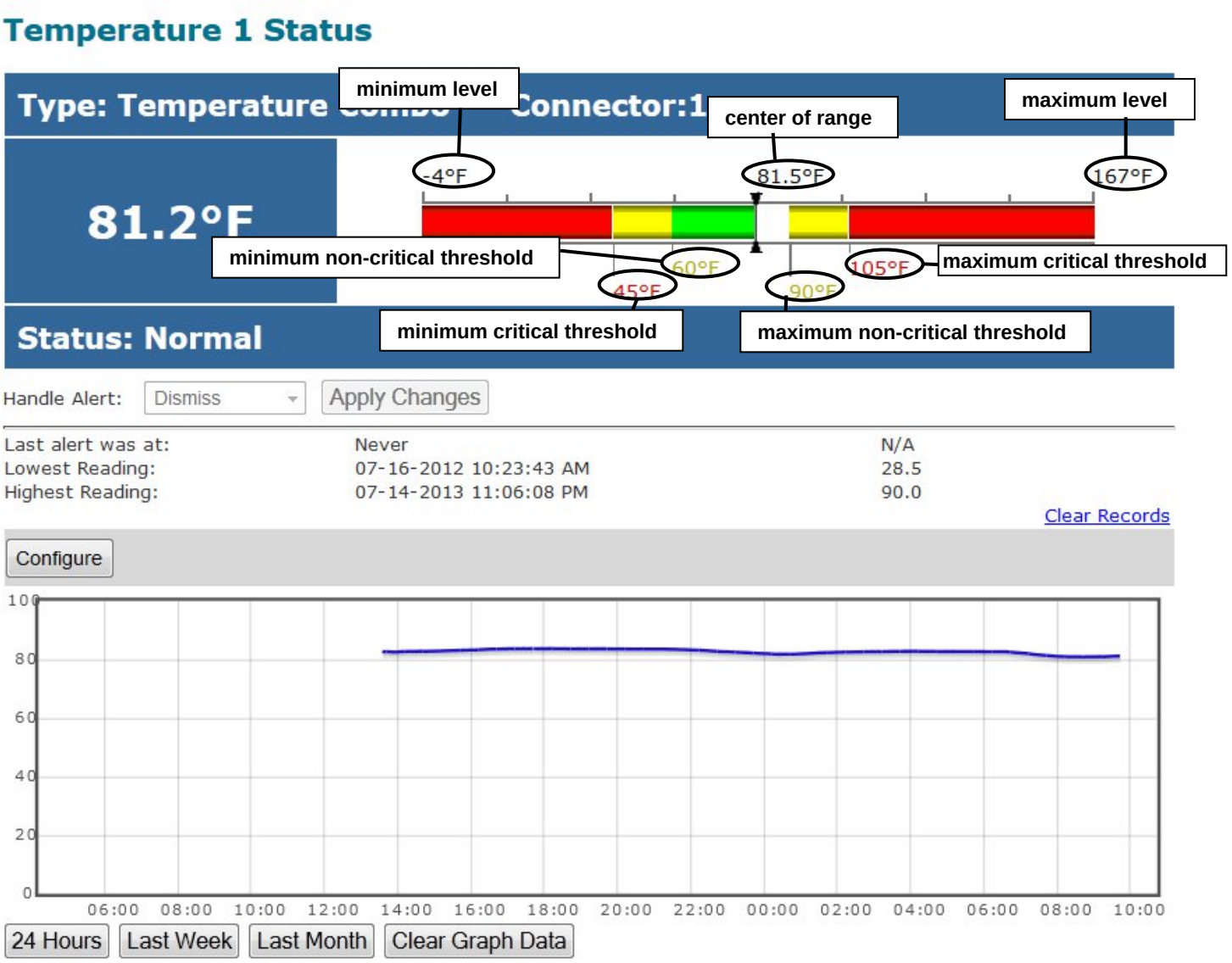


Figure 35- External Sensor Reading

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

The **Configure** button allows the user to configure parameters of the sensor.

A graph that shows a history of a sensor's readings is displayed (RS485 and TACH sensors only). The time period displayed can be changed to show the last hour, last week or last 30 days.

Note: If the ENVIROMUX is power-cycled, all history of sensor readings will be cleared.

The range of readings displayed will adjust as the readings are taken. For example, in the above image, for the time period displayed the range of readings was between 82.2°F. to 80.2°F. As the readings vary and the time period increases, the range will automatically update to a wider range of temperatures and adjust the graph accordingly.

To clear the readings for a sensor and start over, click on "**Clear Graph Data**". To disable the viewing of graphs, see page 63.

Note: If the sensor is a double-function sensor (E-STHS), then using "Clear Graph Data" will clear the data for both the temperature and humidity readings of that sensor.

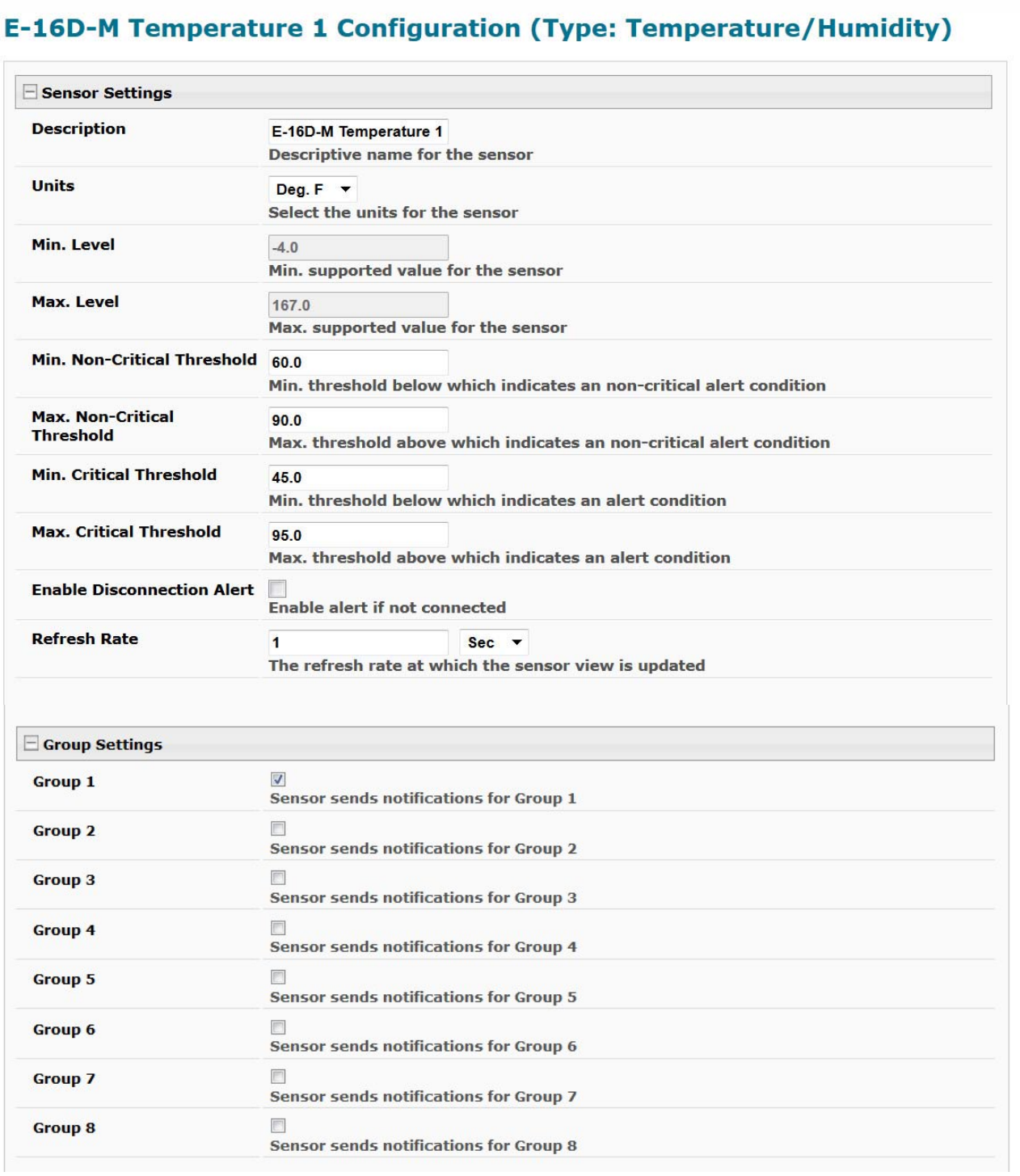


Figure 36- Sensor Configuration Page (1)

Figure 37- Sensor Configuration Page (2)

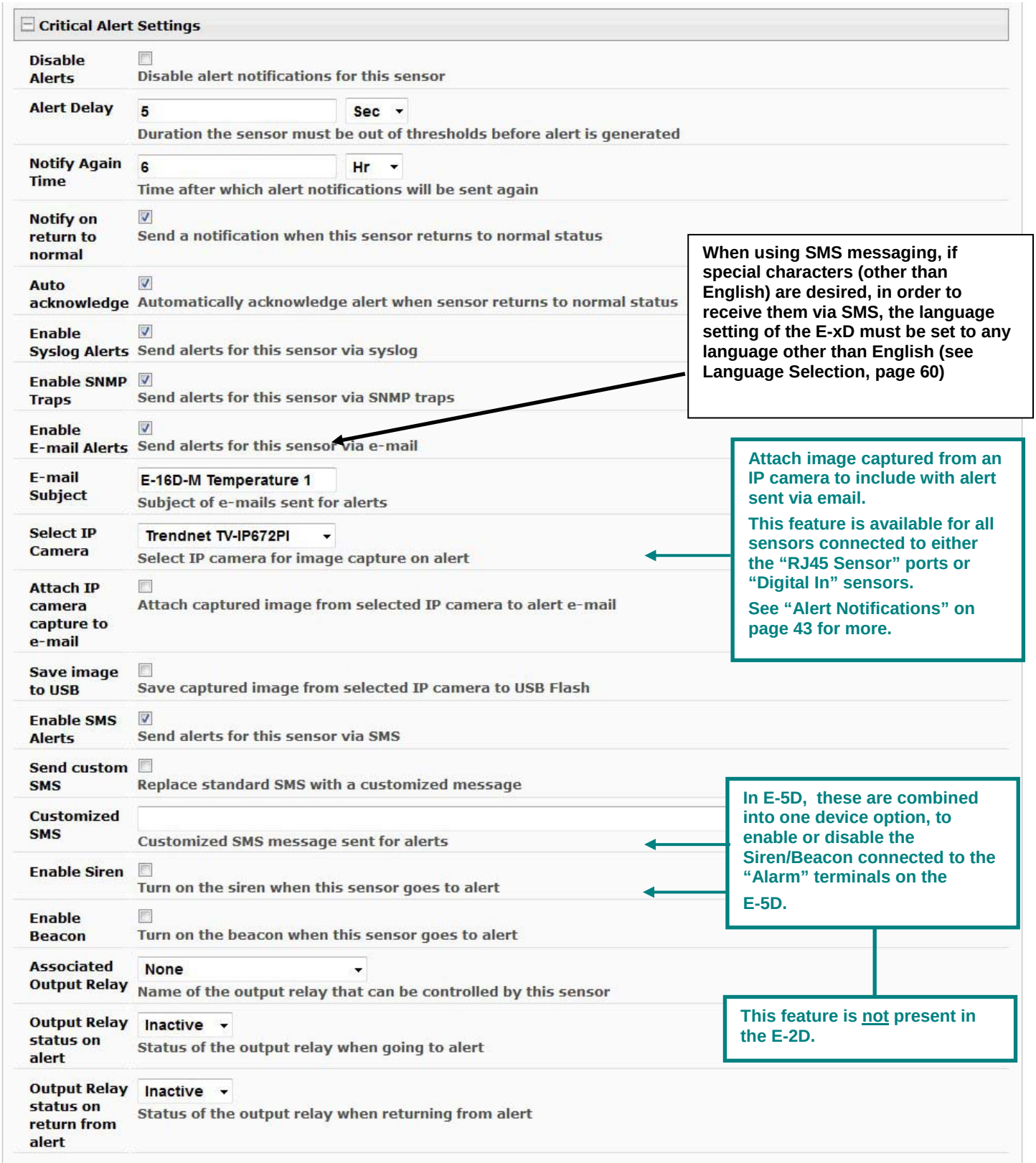


Figure 38- Sensor Configuration Page (3)

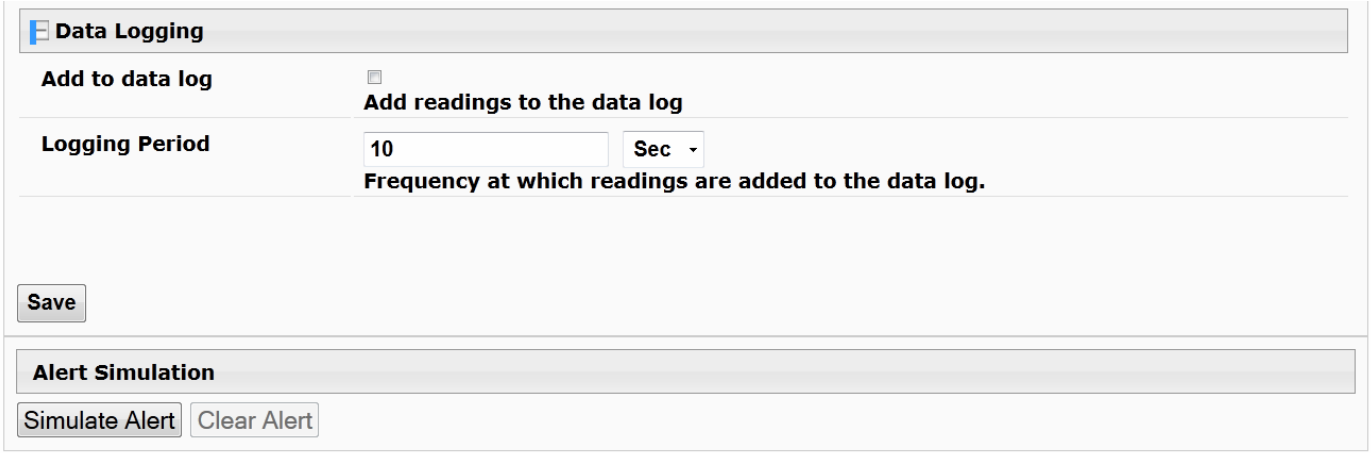


Figure 39- Sensor Configuration Page (4)

External Sensor Configuration

Sensor Settings	Description
Description	The description of the sensor that will be viewed in the Summary page and in the body of alert messages
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.
Enable Disconnection Alert	If this sensor is disconnected its status will change to alarm and an alert will be sent
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.
Group Settings	**Description**
Group	Assign the sensor to any or all groups 1 -8 (see also page 42)

Schedule Settings	
Schedule Type	**Always active**- sensor will react to alert conditions at all hours of each day **Active during defined times**- sensor will only react to alert conditions during times as outlined below
Start Day	First day of the week the sensor should react to alert conditions
End Day	Last day of the week the sensor should react to alert conditions
Start Hour	First hour of the day the sensor should begin reacting to alert conditions
End Hour	Last hour of the day the sensor should react to alert conditions
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 ***Note: If alerts for a sensor are disabled, the associated output action (see "Outputs"- page 33) will still take place. There just won't be any alert notifications that this is occurring. For example, this might be used to turn ON a device, such as a fan, when the server room gets too warm, and OFF again when the temperature returns to normal. An alert message may not be desired under these circumstances.*** ***Note: if the user wants to disable alerts for a sensor after the sensor is already in alert status, the user must either acknowledge or dismiss the alert first.***
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. For more on alert delay, see "Alert Settings" on page 43)
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 (Applies to Critical Alert settings only)	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 (up to 60 characters)
Attach IP Camera capture to email (Applies to Critical Alert settings only)	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 58) 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.*** ***Note: If "Brief email" is enabled under User Settings (page 77) for a user, this setting will have no effect for that user. No images will be sent to that user.***
Save Image to USB	Save the image captured by the IP Camera to the USB flash device when an alert is triggered
Enable SMS Alerts	Place a checkmark in this box to have alert notifications sent via SMS messages (requires a modem)
Send Custom SMS	Place a checkmark in this box to have a custom SMS message instead of using the standard SMS message
Customized SMS	Enter the customized SMS message (up to 160 characters) to be sent with an SMS Alert
Enable Siren	Turn ON the siren when this sensor goes to alert (not applicable to E-2D)
Enable Beacon	Turn ON the beacon when this sensor goes to alert (not applicable to E-2D)

Alert Settings (Applies to Critical and Non-Critical Alerts except where noted) (Cont'd)	
Associated Output Relay **Tip: Another way to have a single output relay react to the changes of more than one sensor is to use Events and Smart Alerts (page 94) to create that association.**	You can associate the sensor with the operation of the output relay, or not. By Default, the operation of an output relay can only be associated with one sensor or IP Device. To associate an output relay with more than one sensor or IP Device, place a checkmark in the checkbox under "System- Other Options- Disable Relay Interlock (page 63). ***Note: If the Output Relay is associated with a sensor/device, and configured to change state when a sensor crosses threshold into alert, it will change state even if the alerts are disabled.*** ***Note: Only one sensor/device 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.

Groups

Groups are used to create a common relationship between sensors, IP devices, etc. and their alert messages. Each item being monitored can be assigned to one or more groups (up to 8 possible). Users (a maximum number of 17 including the root user) can receive alert messages from items in one or more groups (see user configuration on page 75).

Test Alerts

With all 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.

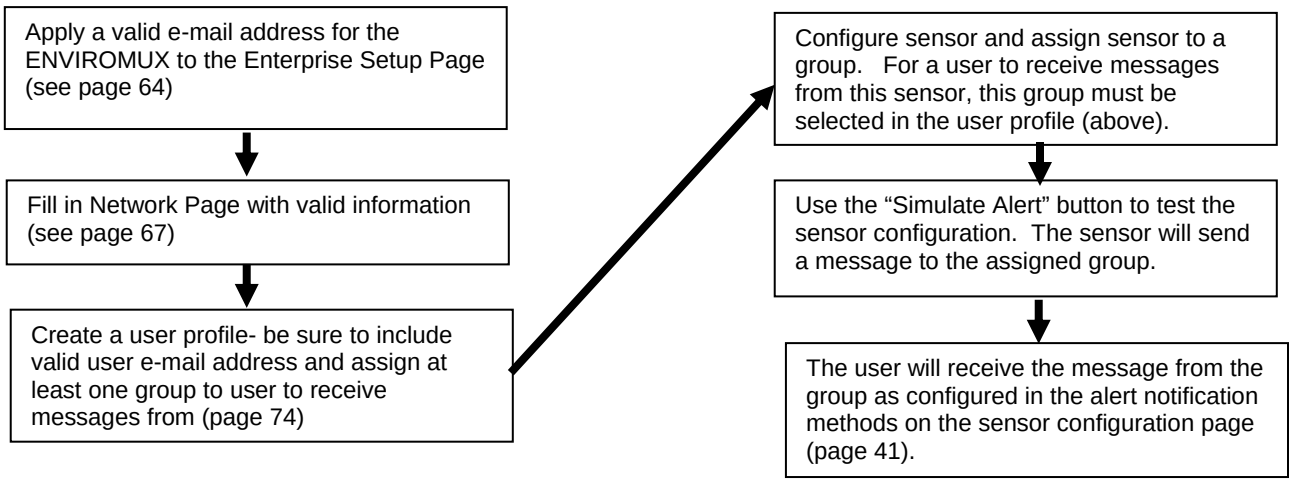


Figure 40- Chart to setup alert notification

Alert Settings

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

Example:

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

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

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

Alert Notifications

The alert can be configured to notify one or more users via e-mail, SNMP traps (v1,v2c,v3), Syslog messages, or SMS alerts. The e-mail subject line for e-mail notification can be customized for easy source identification. The alert can activate an audible siren, or an alarm beacon. Alerts are also indicated on the "Int Alert" or "Ext Alert " LEDs on the front of the ENVIROMUX and in the WEB interface.

External sensors have the added feature of being able to be associated with an IP camera. If a checkmark is added to the block "**Attach IP camera capture to email**" and an IP camera is selected 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 58) 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.

If a checkmark is added to "**Save Image to USB**", the image captured by the IP camera will also be saved to a flash drive connected to a USB port.

Thresholds

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

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

Outputs

Each sensor can be associated with one of the connections labeled "Output Relays" (see page 23), and that connection can be set to open or close the contacts of the relay either on alert, or when returning to normal. The tamper can also block the output command generated by the alert. In this way other devices can be controlled by sensor and tamper alerts.

Specialized Sensors (for E-S420MA-24V Current Sensor Configuration only)

When a E-S420MA-24V Current Sensor is connected to the ENVIROMUX, the summary page will update with two sensor names of the Type "Current". Various types of sensors can be connected to an E-S420MA-24V. In order to better define the sensor on the Summary Page, in SNMP traps, or in an MIB browser, click on the "Edit" link to open the sensor configuration page and configure the sensor. In the image below, an RTD Temperature sensor has been connected to the Current Sensor plugged into RJ45 port 3 and configured to be used.

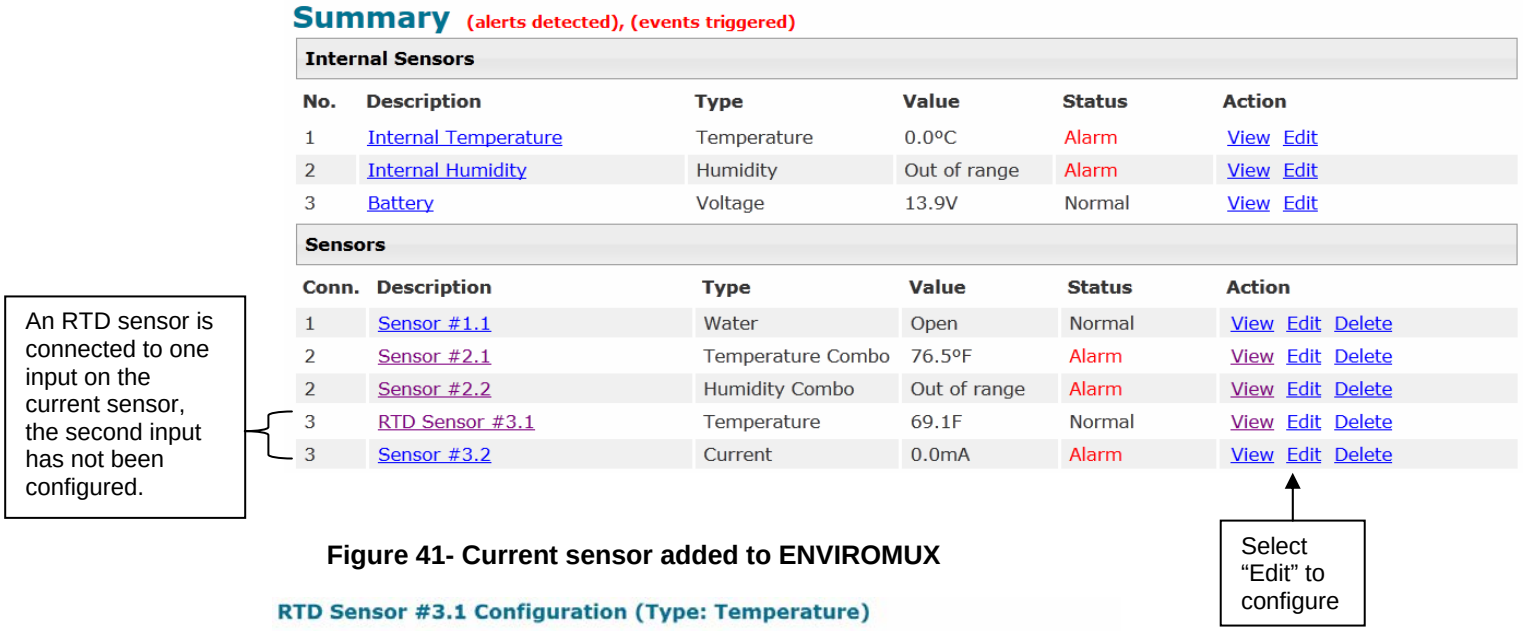


Figure 41- Current sensor added to ENVIROMUX

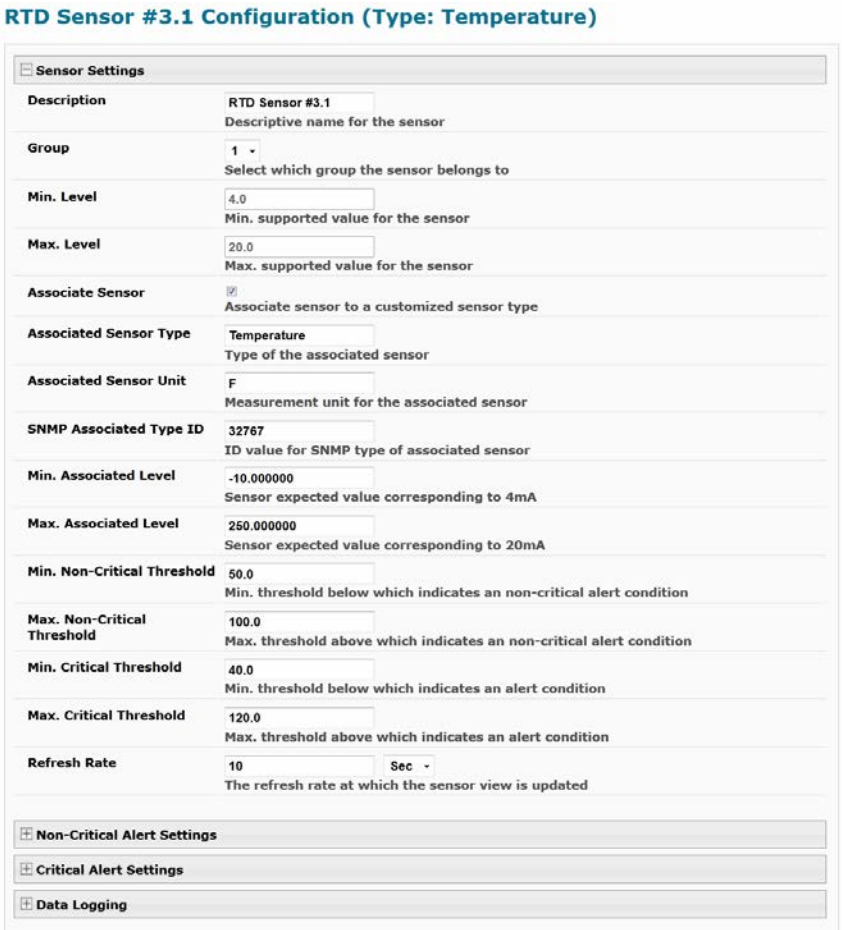


Figure 42- Configuration of sensor connected to E-S420MA-24V

Most of the sensor settings are the same as any other sensor configuration (page 40) but there are some differences:

Sensor Settings	Description
Associate Sensor	Select if the Type "Current" should be replaced by the sensor type to be entered in the next box
Associated Sensor Type	Enter the "Type" of sensor that should be displayed on the summary page and in all alert communications received regarding this sensor
Associated Sensor Unit	Enter between 1 and 3 alphabetical characters. These characters will be used by the ENVIROMUX to represent the unit of measure reported by the attached sensor. Leaving it empty will result in an empty string in the reported data.
SNMP Associated Type ID	Enter ID value from MIB file if SNMP traps will be used for alert notifications for this sensor (for more on this, see "SNMP Custom Type ID" below)
Min. Associated Level	The minimum range of the units to be associated with the current reading measured from the attached sensor.
Max. Associated Level	The maximum range of the units to be associated with the current reading measured from the attached sensor.

SNMP Custom Type ID: Use this field if SNMP traps will be used for alert notifications. The Type ID corresponds with a value defined in the MIB file under "extSensorType" (default value is 32767 for type "Custom"). Place the desired number in this box that represents the type of sensor to be reported in the MIB browser or SNMP trap.

To define a new type of sensor;

1. open the MIB file,
2. locate the section titled "extSensorType",
3. assign a description and a number not already in use (in the "SYNTAX" field) to associate with it ,
4. enter the number for the newly defined extSensorType in the SNMP Custom Type ID box.

If the Type ID is left blank, the value "0" will be assigned, which will be reported in the browser and SNMP trap as type "undefined".

Contact Sensors

Contact Sensors are sensors that close or open a contact according to the sensor condition. Their presence and their type cannot be automatically detected by the RJ45 Sensor port. The sensors have to be manually added to the unit list by the administrator or a user with administrator privileges. Contact sensors can be either connected to RJ45 Sensor ports, or more commonly to Digital Input terminals.

Add a Contact Sensor to RJ45 Sensor port

When adding a contact sensor to an RJ45 Sensor port, after connecting the sensor to an available port, the administrator must select "Add New Sensor" at the bottom of the **Monitoring->Sensors** page.

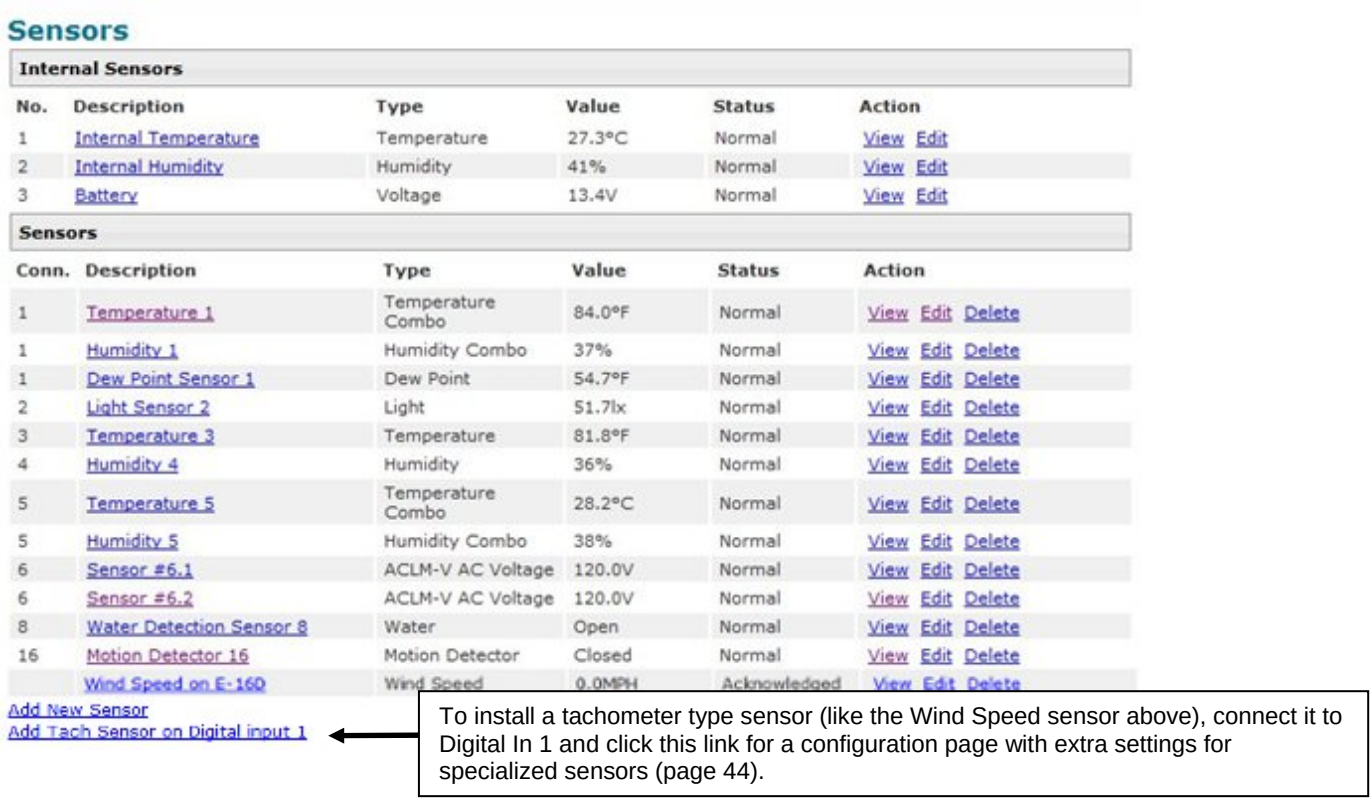


Figure 43- List of sensors

In the Add Sensor page, enter the type of sensor and the RJ45 connector where the sensor is connected. Then select "Add".

If the connector was already in use and has a sensor already defined for it, an error message will be displayed at the bottom of the Summary page.

Figure 44- Add a contact sensor

Many of the settings found in the RS485 configuration page are not present because they do not apply to contact sensors. As such, only “Critical Alert Settings” apply (see descriptions on page 40) and non-critical alert settings are omitted altogether.

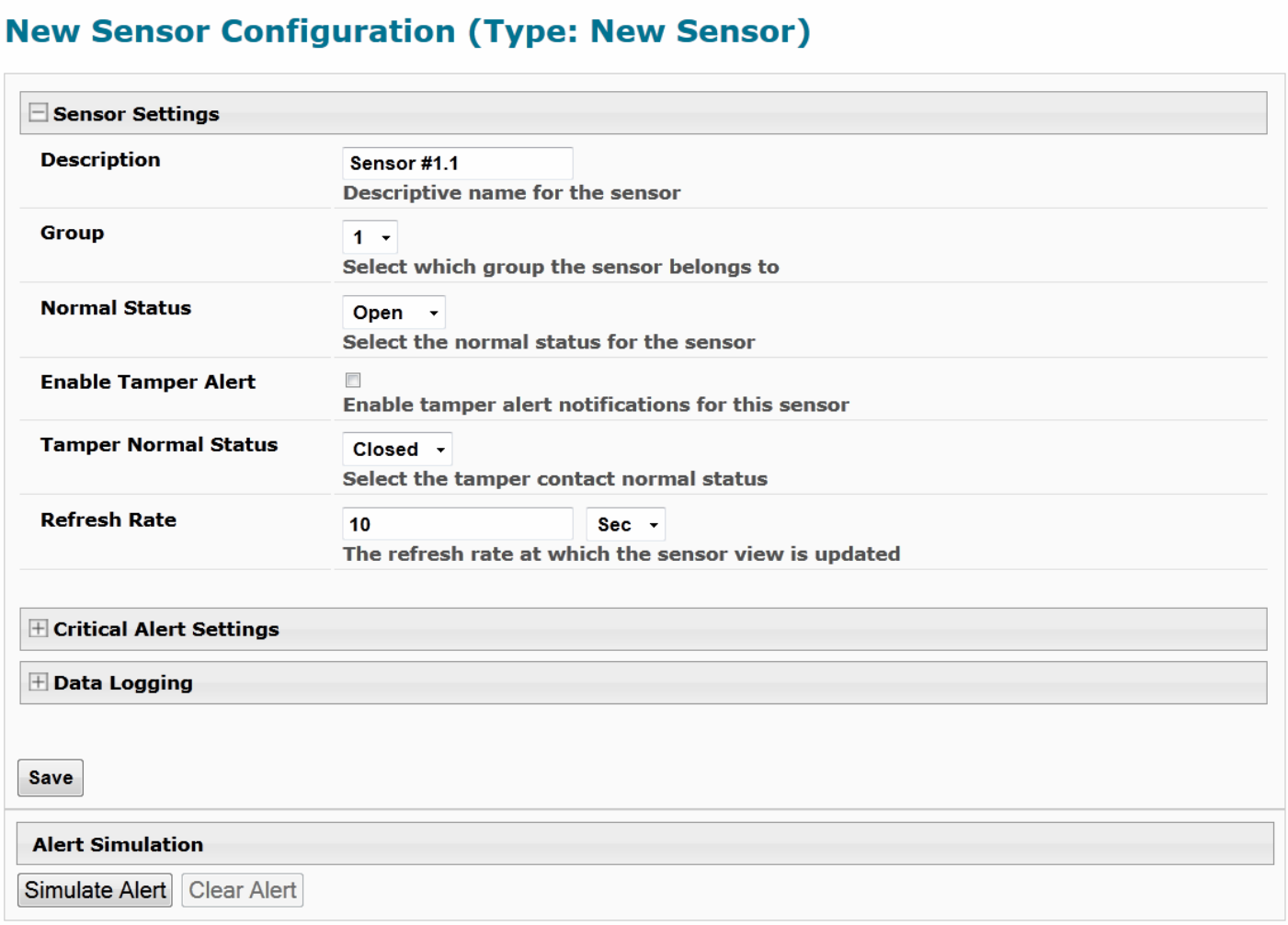


Figure 45- Contact Sensor configuration page

Aside from the usual Description, Group, and Refresh Rate settings to be applied, the configuration page introduces three new settings:

Normal Status: This will be the contact sensors state when it is not in alert, either with contact closed, or contact open.

Enable Tamper Alert: If the contact sensor has a tamper feature, and the feature is being connected to the ENVIROMUX, then this box can be selected if alert messages are desired in the event the contact sensor tamper feature’s state changes from its defined “Normal Status”.

Tamper Normal Status: This will be the normal state of the contact sensor’s tamper feature when not being tampered with.

Digital Inputs

The "Digital In" terminals (page 11) are for easy installation of contact sensors (as opposed to using the RJ45 sensor ports). Connect up to 8 different contact sensors having either 2-wire contacts (for open or closed circuit sensing) or 4-wire contacts (for open or closed circuit sensors requiring 12V power supplies to operate). 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 **Closed** contacts for the normal status of the sensor. (Water sensors are open contact when not in alert state.)

Note: The E-5D/2D have room for only 5 contact sensors, and do not provide 12V power to them individually.

An "Aux Pwr" terminal is available for up to 500mA of sensor support.

Before Digital Inputs will be listed in the Summary page or Digital Input page, they must first be added on the Digital Input page using "Add New Digital Input" (shown in image below).

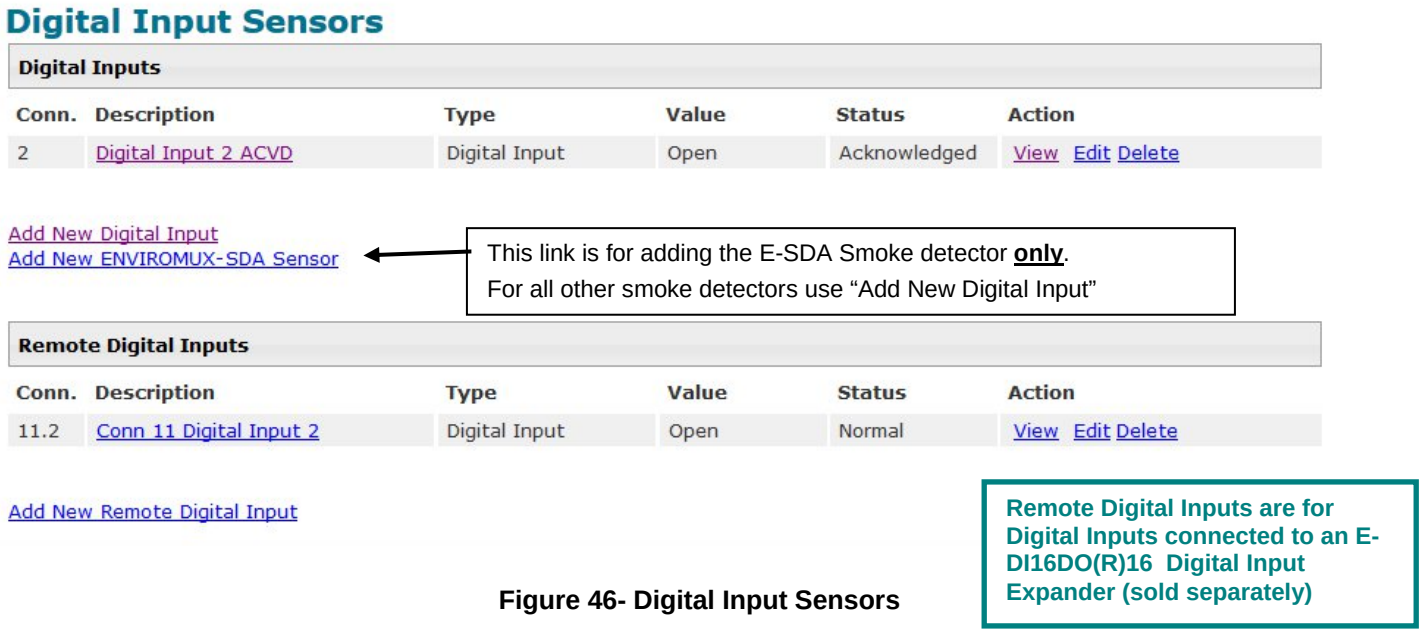


Figure 46- Digital Input Sensors

First, select a connector on the ENVIROMUX that you wish to view the status of.

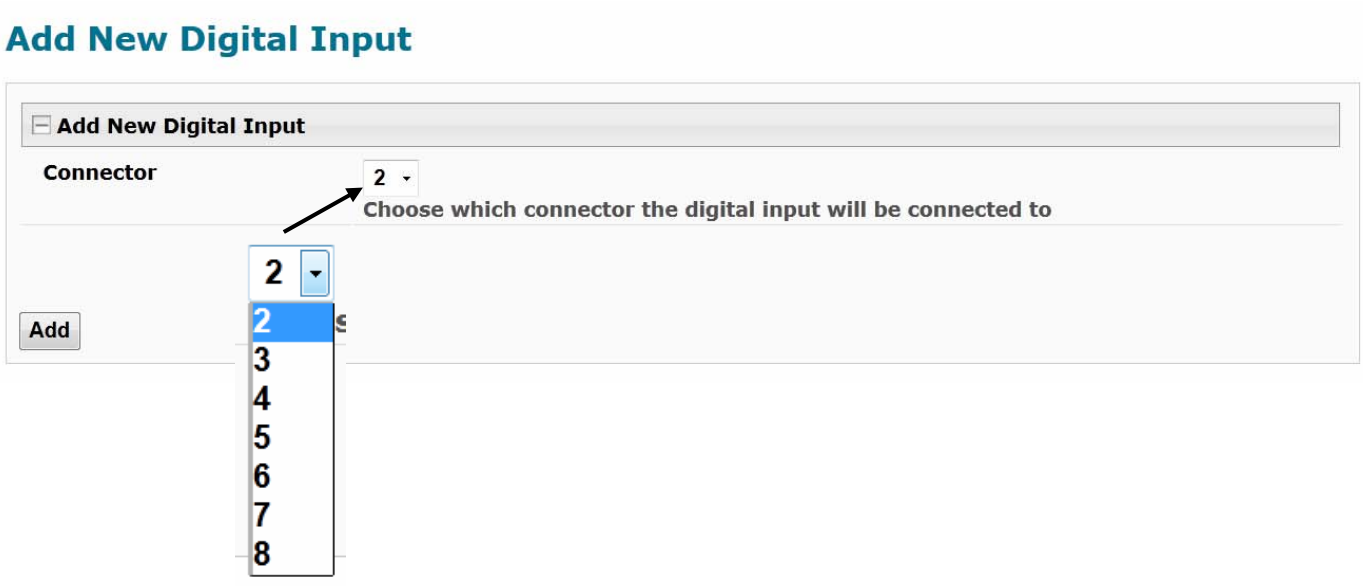


Figure 47- Select connector on ENVIROMUX

Once the connector is selected, a configuration window will open providing fields for the additional information available to setup the sensor.

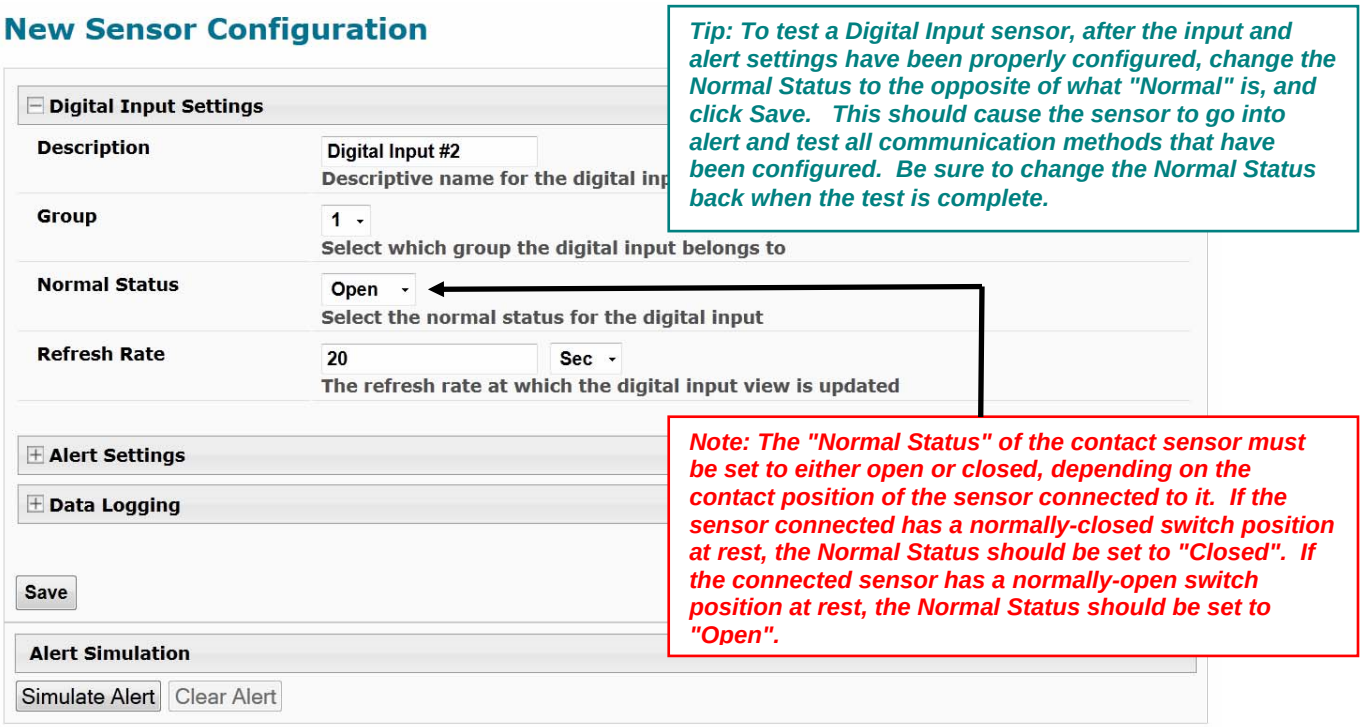
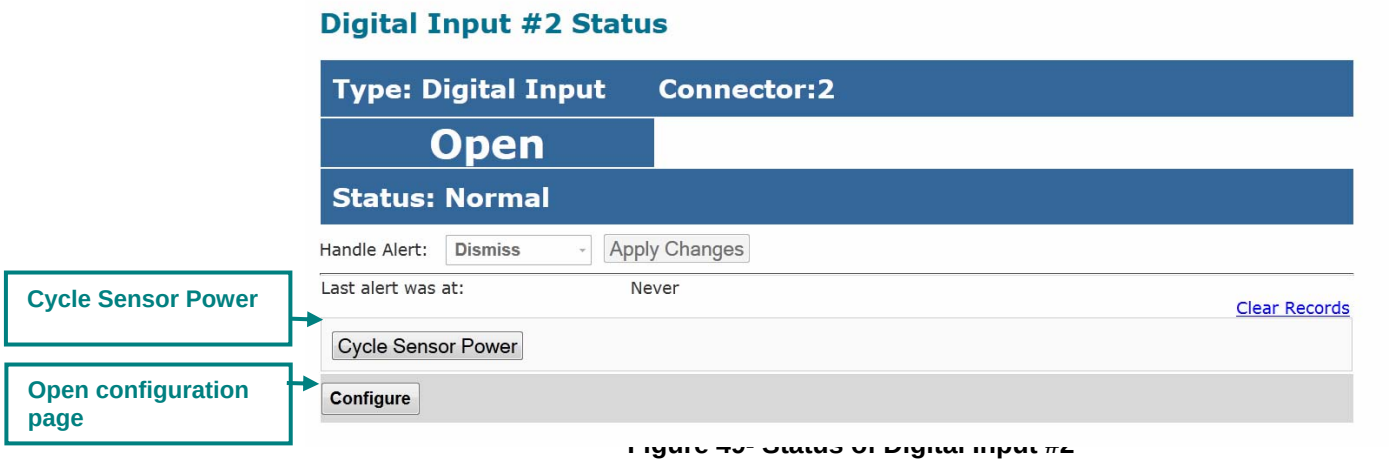


Figure 48- Configure New Sensor

After the Digital Input sensor has been installed, the management and configuration of it is similar to Contact Sensors (page 46). To view the status of a sensor, click on the sensor as listed in the Digital Input page (Figure 46).



To adjust configuration of an existing sensor, click on “Configure”. The configuration window can also be opened by clicking on “Edit” in the Digital Input page.

Figure 50- Open configuration from Digital Input page

Cycle Sensor Power

A “Cycle Sensor Power” button is also provided (see Figure 49) for each sensor connected to the “Digital In” terminals (locally-connected Digital Inputs only). To momentarily disrupt power to any sensor connected to a Digital Input terminal, click on this button. For example, when a smoke detector needs to be power-cycled in order to reset it. The 12VDC power will be disrupted to the sensor for 5 seconds and then automatically restored.

Note: On E-5D and -2D, the “Cycle Sensor Power” will cause the “AUX PWR” terminals to cycle power. This will only be effective for the sensor you are clicking the button for if that sensor is being powered from these terminals. If your sensor is powered, for example, from an AC adapter, the “Cycle Sensor Power” button will have no effect on that sensor, but it will still cycle power on the “AUX PWR” terminals, disrupting any device getting power from these terminals for 5 seconds. Keep this in mind if more than one sensor (or device) is being powered from these terminals.

To test your Digital Input configuration, click on "Configure" (Figure 49) for the sensor, and click on "Simulate Alert" (Figure 48). Now go to the Summary Page. The Status for that sensor should now show it to be in "Alarm" (provided your Alert Delay, under Alert Settings, is not set for too many seconds). If the Alert Delay is in play, you will have to wait for that time to expire before the Status will change.

Digital Inputs

Conn.	Description	Type	Value	Status	Action
2	E-16D-M ACVD DI2	Digital Input	Closed	Normal	View Edit Delete
3	E-16D-M Test Switch DI3	Digital Input	Open	Alarm	View Edit Delete
5	E-16D-M Digital Input 5	Digital Input	Open	Alarm	View Edit Delete
S1-2	E-16D-S1 DI 2	Digital Input	Open	Normal	View Edit Delete
S1-8	E-16D S1 Digital Input 8	Digital Input	Open	Normal	View Edit Delete

Add Tach Sensor

To add a Tach Sensor, make connections of the tachometer type sensor (ENVIROMU-WSS for example) to Digital Input 1 on the rear of the ENVIROMUX. Then select “Add Tach Sensor on Digital Input 1” on the Sensors summary page (page 46). The sensor configuration page with added settings for a custom sensor will appear. These settings are the same as those described under “Specialized Sensors” on page 44. This special purpose of Digital Input 1 can be used by any device that produces a frequency up to 255Hz.

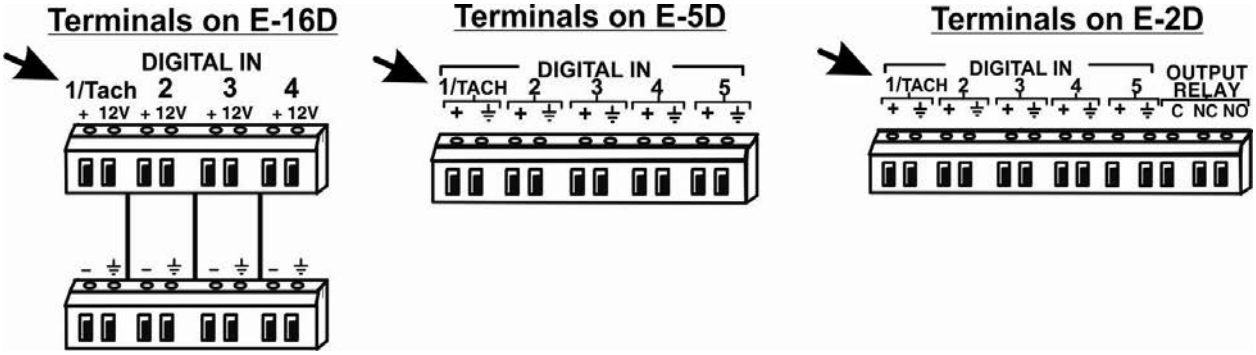


Figure 51- Connection that supports Tachometer Sensor

Note: Digital Input 1 is the only terminal connection point that supports a tach sensor.

To remove a digital input sensor from the displayed list, click on “**Delete**” under the Action column in the Digital Input Sensor list.

Monitor Output Relay

Output relays are provided to control external devices with a rating of up to 1A, 30VDC or 0.5A, 125VAC. Each 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 41).

Figure 52- Monitoring Output Relays

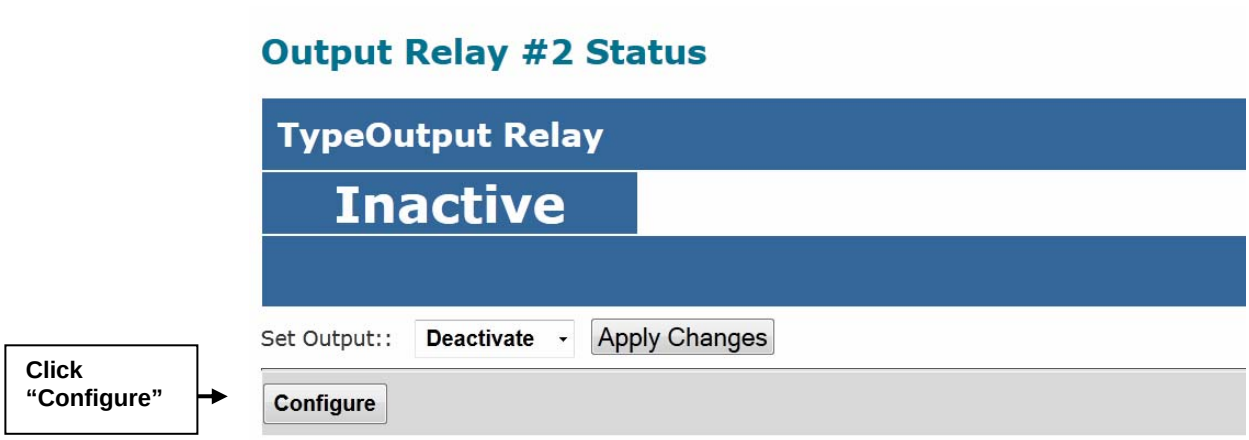


Figure 53- Output Relay Status

To test your connections and set the state of the relay manually, from the relay status page (Figure 53), select the arrow next to Set Output to drop down the window and select either "Deactivate" or "Activate". Then click the "Apply Changes" button.

The relay state can also be changed using SNMP. See page 70 for details.

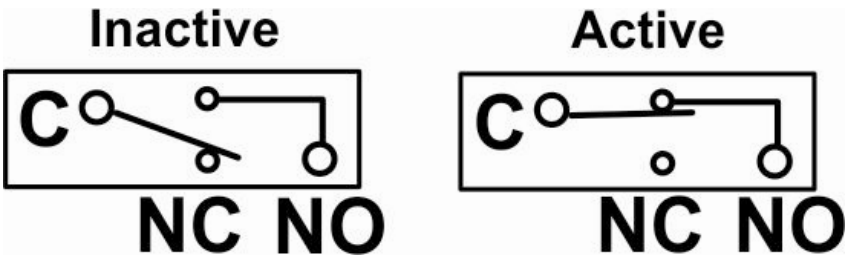


Figure 54- Output Relay Contact State

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

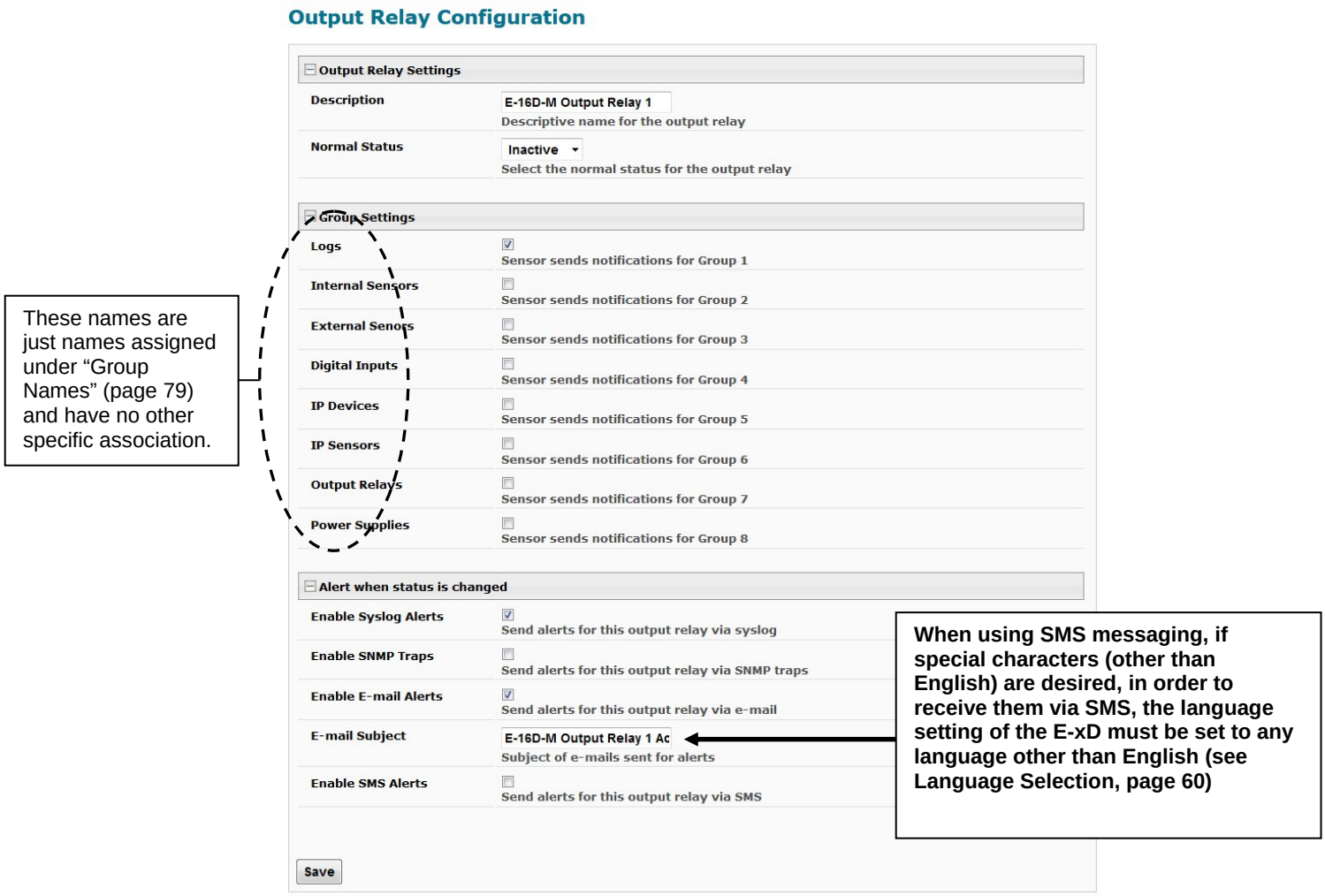


Figure 55- Configure Output Relay

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.

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.

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

When the relay is in 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).

Note: When the ENVIROMUX is powered OFF with the battery completely drained, each relay will revert to an inactive state, regardless of the “Normal Status” setting.

Once configured, output relays are controlled by their associated sensor and can be programmed to change state (from normally-open to normally-closed or vice versa) on an alert or on the return to normal conditions. Programming is done on the configuration page of the associated sensor or Smart Alert. Each output relay can be associated with any one sensor or Smart Alert.

IP Devices

Up to 64 IP addresses can be assigned to be monitored by ENVIROMUX. They will be displayed under the **Monitoring->IP Devices** item in the left side menu. The ENVIROMUX will periodically ping (test) these addresses to determine whether or not they are up and running. If the address is not running, an alert will be recorded.

For each device the user can configure the

* IP address,
* the name,
* the sensor group the IP device will belong to
* the ping period (period of time between two consecutive tests),
* the time-out period (in seconds) in which the address should respond
* the number of times the ENIROMUX should ping the address before reporting an alert
* how often, if at all, the reading taken should be added to the data log.

If the address fails to respond within the time-out for the selected number of times it will generate an alert. It will be tested again after the programmed period of time.

Just as with other sensors, the method of alert notification and the effect, if any, on output contacts can be configured in response to IP address connection failures.

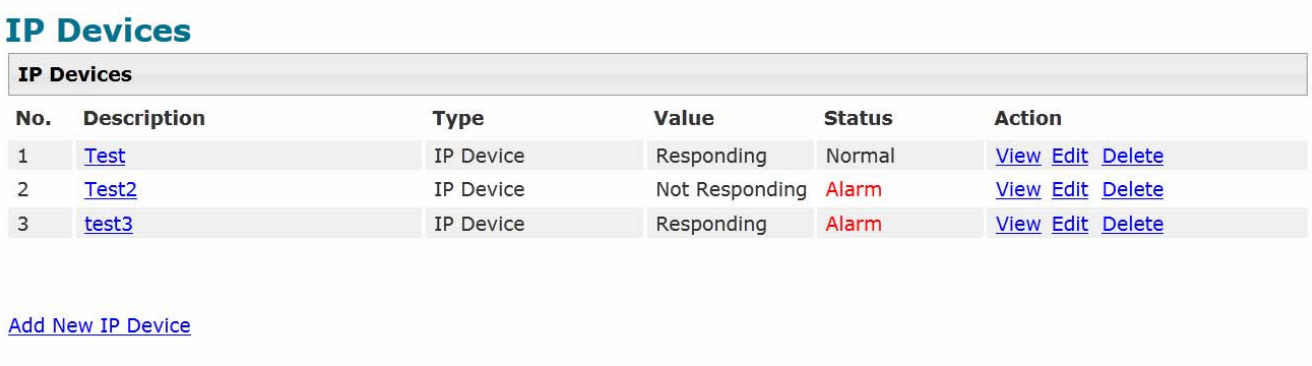


Figure 56- IP Devices monitored

To add an IP device to monitor, select “Add New IP Device” from the **Monitoring ->IP Devices page**.

Figure 57- Add new IP Device

Apply a descriptive name for the IP Device to be monitored, and the IP address of the device.

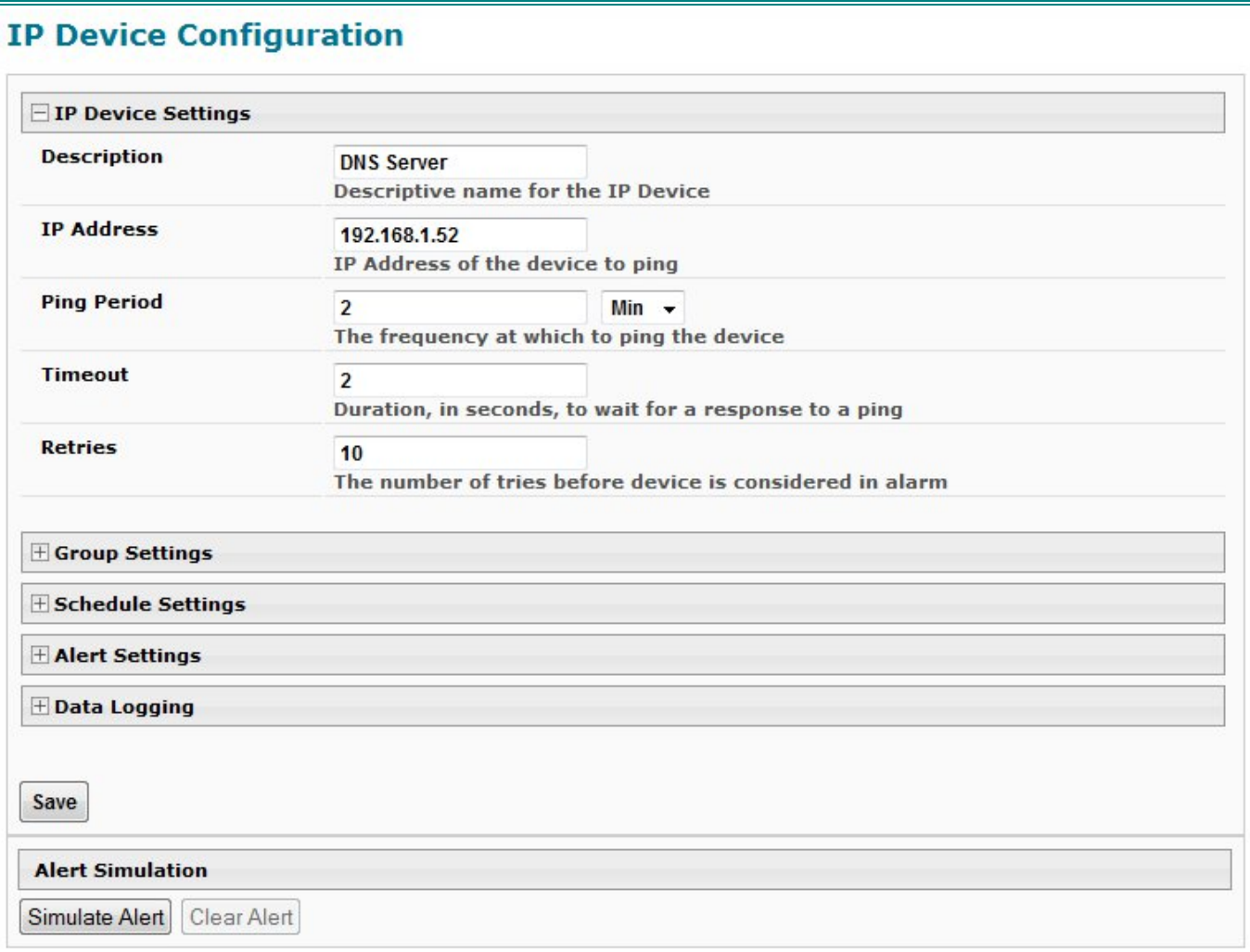


Figure 58- IP Device Configuration

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
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

There is no limit to the number of times you can retry to ping (retries), how long to wait for a response (timeout), or how long you can set it to wait between pings to a device(ping period). These values are up to you.

Under Group Settings, place a checkmark for each group that alert messages should be assigned to. This will determine who will receive an alert due to a ping failure.

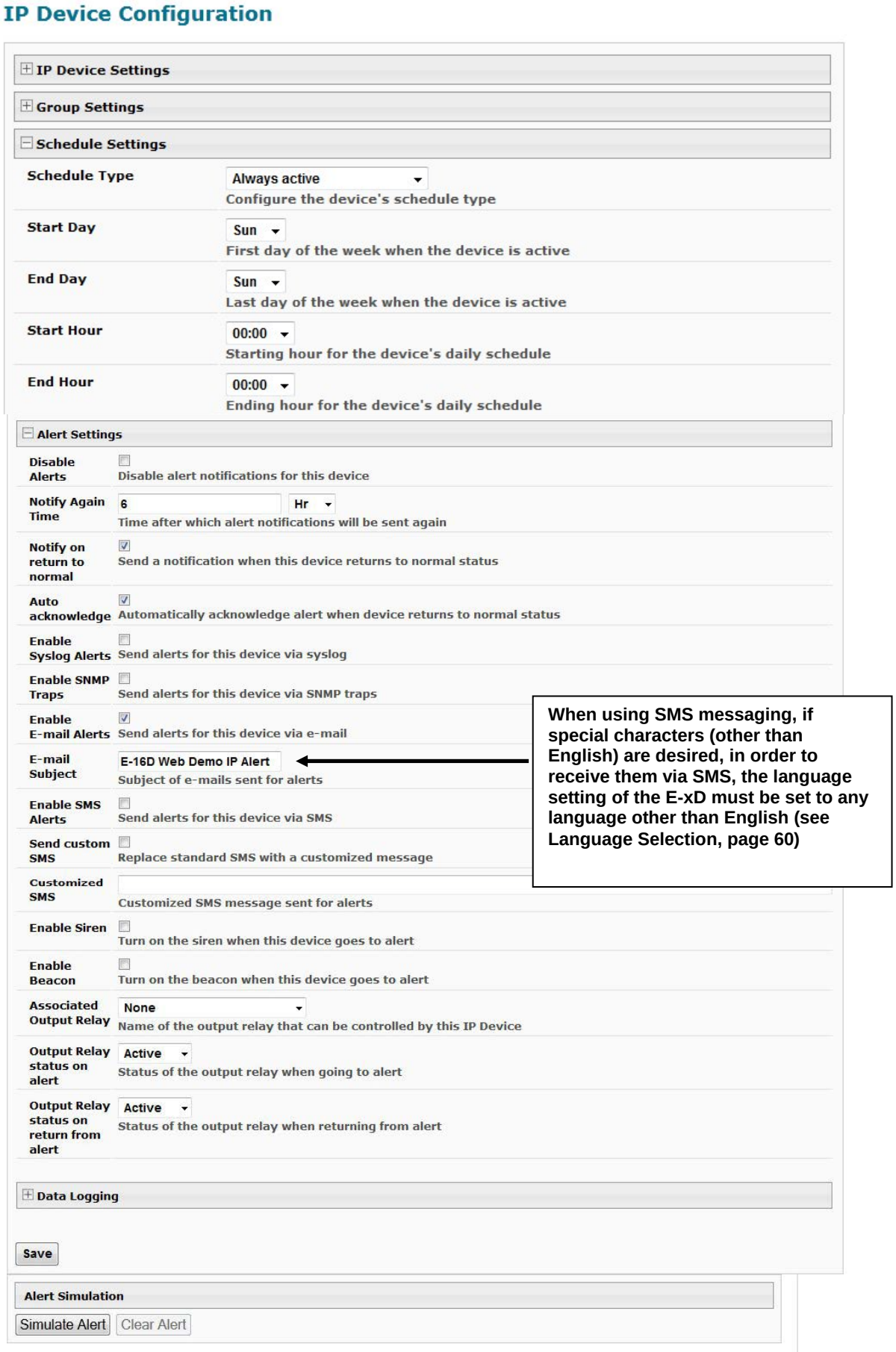


Figure 59- IP Device Configuration-more

Group Settings	Description
Group	Assign the device IP to any or all groups 1 -8 (see also page 42)
Schedule Settings	
Schedule Type	**Always active**- system will react to alert condition at all hours of each day **Active during defined times**- system will only react to alert condition during times as outlined below
Start Day	First day of the week the system should react to alert condition
End Day	Last day of the week the system should react to alert condition
Start Hour	First hour of the day the system should begin reacting to alert condition
End Hour	Last hour of the day the system should react to alert condition
Alert Settings	
Disable Alerts	Place a checkmark in the box to prevent alerts from being sent when the device's status changes ***Note: If alerts for an IP device are disabled, the associated output action (see outputs"- page 33) will still take place. There just won't be any alert notifications that this is occurring. For example, this might be used to turn ON a device, such as a fan, when the server room gets too warm, and OFF again when the temperature returns to normal. An alert message may not be desired under these circumstances.*** ***Note: if the user wants to disable alerts for an IP device after the device is already in alert status, the user must either acknowledge or dismiss the alert first.***
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 status has returned to normal by selecting the "***Notify when return to normal***" box for a device.
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.
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 (up to 60 characters)
Enable SMS Alerts	Place a checkmark in this box to have alert notifications sent via SMS messages (requires a modem)
Enable Siren	Turn ON the siren when this device goes to alert (not applicable to E-2D)
Enable Beacon	Turn ON the beacon when this device goes to alert (not applicable to E-2D)
Associated Output Relay **Tip: Another way to have a single output relay react to the changes of more than one sensor is to use Events and Smart Alerts (page 94) to create that association.**	Associate the IP Device with the operation of an output relay, or not. By Default, the operation of an output relay can only be associated with one sensor or IP Device. To associate an output relay with more than one sensor or IP Device, place a checkmark in the checkbox under "System- Other Options- Disable Relay Interlock (page 63). ***Note: Only one sensor/device 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.*** ***Note: If the Output Relay is associated with a sensor/device, and configured to change state when a sensor crosses threshold into alert, it will change state even if the alerts are disabled.***
Output Relay Status on Alert	State the output relay will be in when IP Device goes to an alert
Output Relay Status on Return from Alert	State the output relay will be in when IP Device 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

IP Sensors

Sensors connected to an E-MICRO-T(RHP) can be monitored and configured from the E-xD interface.

On the IP Sensors page, click on “Add New IP Sensor”. On the page that opens, enter a description to be viewed on the sensor summary page for this group of sensors, enter the IP Address of the E-MICRO or E-1W to be monitored, and select the Sensor Type between E-MICRO "MICRO" or E-1W "E-1W". Up to 8 different E-MICRO and up to 4 different E-1W IP Addresses can be added. When finished, click on “Add”.

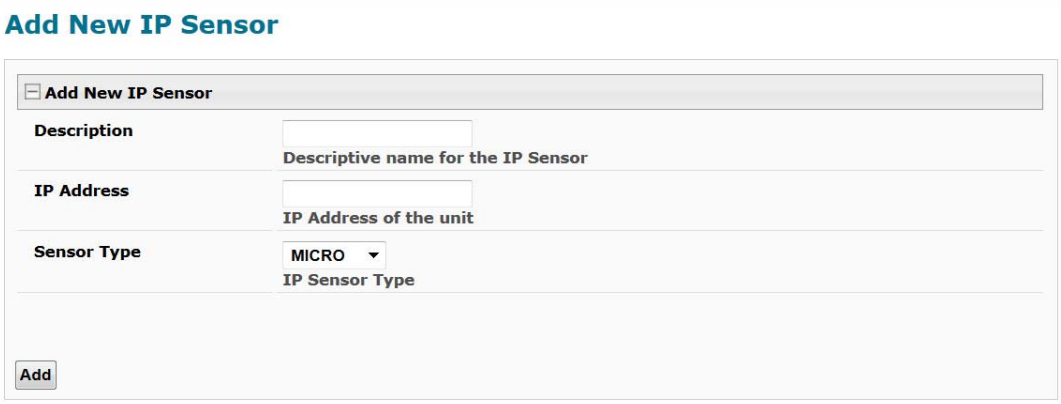


Figure 60- Add IP Sensor

The E-xD will then sense what sensors are attached to the E-MICRO and E-1W units and add them to your summary list under “IP Sensors”. Once listed, to view the status of an individual sensor, click on “View”. The change the configuration, click on “Edit”.

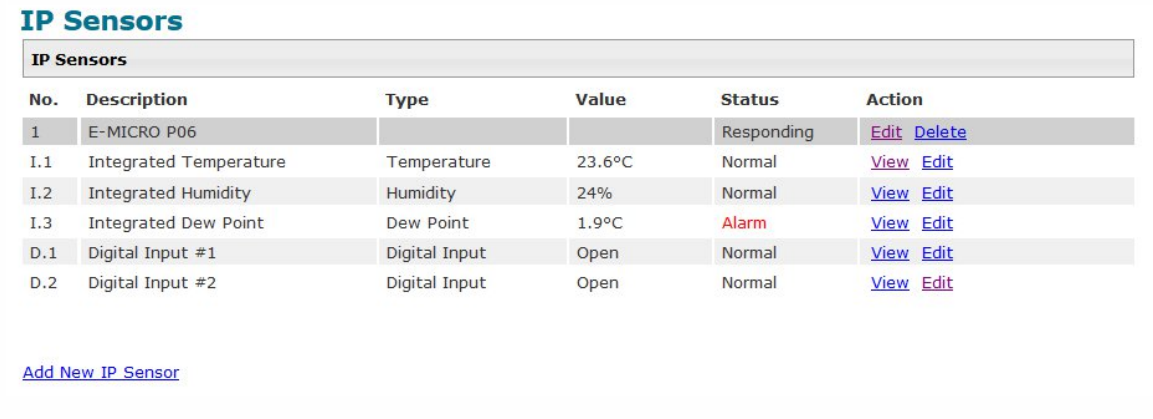


Figure 61- IP Sensor List

In a cascaded configuration of E-xD units, IP sensors (maximum of 12) must be configured from the Master unit to receive alerts about those sensors.

Note: The configuration settings applied to these sensors in this interface will not alter the settings as configured within the E-MICRO web interface.

IP Cameras

The IP Camera 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. Place a name, the URL or IP address of the link, and the name of the image taken by the camera in the blocks provided (examples in Figure 63). The images can be set to be refreshed every 100 msec (.1 second) up to 99,900 msec (almost 100 seconds).

Click ***Save*** at the bottom of the page. Then click on **Monitoring->IP Cameras** to see the images taken by those cameras. The user can click on any image and be connected to the site defined by the configuration.

If your camera requires authentication in order to view images or send images via email, place a checkmark in "**Enable HTTP Auth**" and add the **Username** and **Password** that your camera has been configured to accept.

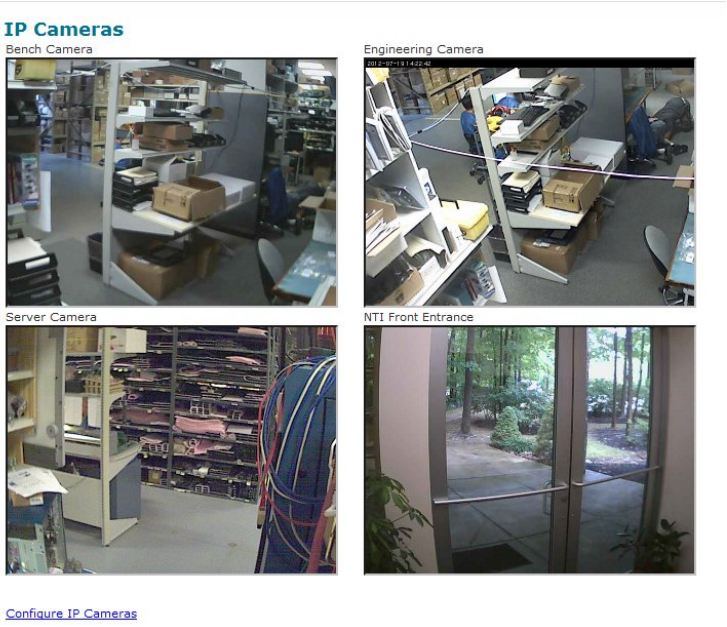
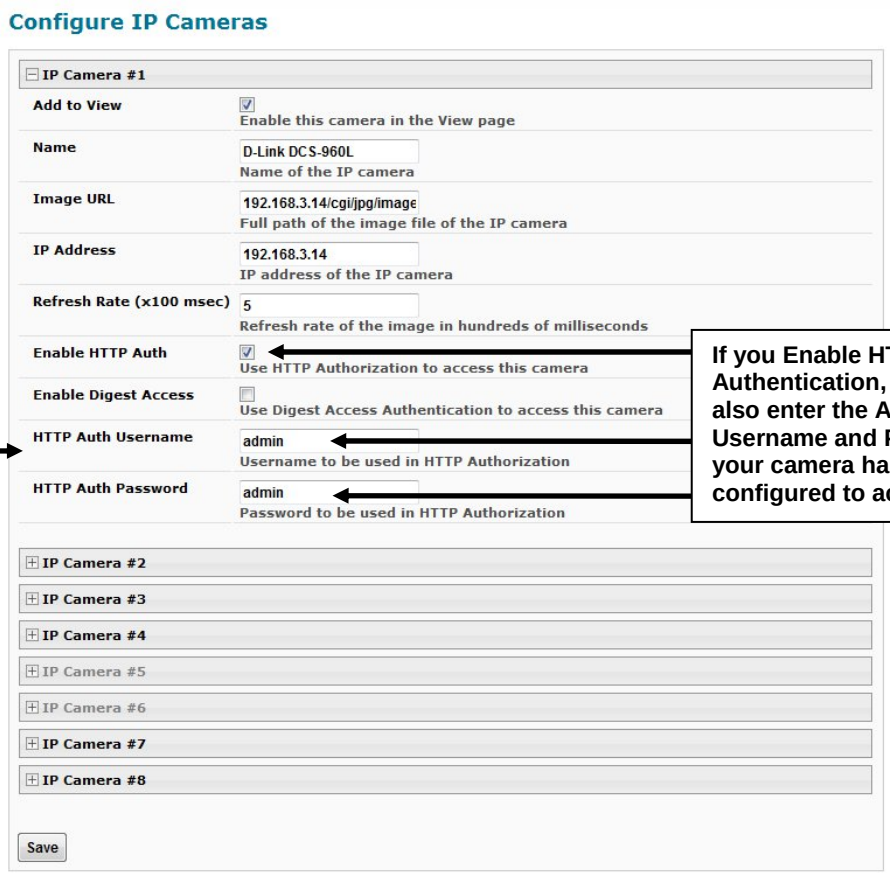


Figure 62- Monitoring IP Cameras

Once this is configured, test to see if images come via email. (See below)

If not, your camera may require "Digest Access Authentication" to work. In this case, place a checkmark in "**Enable Digest Access".**

Caution: Don't enable this unless it is necessary, because if it isn't needed, you won't get emails from cameras that don't support this feature.



If you Enable HTTP Authentication, you must also enter the Authentication Username and Password that your camera has been configured to accept.

Figure 63- IP Camera Configuration

The images from web cameras can also be associated with alert messages. When configured (page 43), an image from an IP camera can be taken and sent along with a sensor alert message via email and/or saved to a connected USB flashdrive.

Note: If your camera's security can be disabled, and you don't want to use it to be able to send IP camera captures as e-mail attachments, then disable it. The "Enable HTTP Auth" and "Enable digest Access" features are provided for cameras the require authentication to view images or send images via email. Consult your IP camera manual to see if this feature is present and for instructions on how to configure this.

Administration

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

System	Fields for applying time zone, date, time, NTP server, backup and restore configuration settings and settings for the "RS232 AUX" port
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
Groups	Fields for assigning names to the groups that will receive alerts and messages
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.
Cascading	For controlling up to 4 ENVIROMUX slaves from one master unit
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.

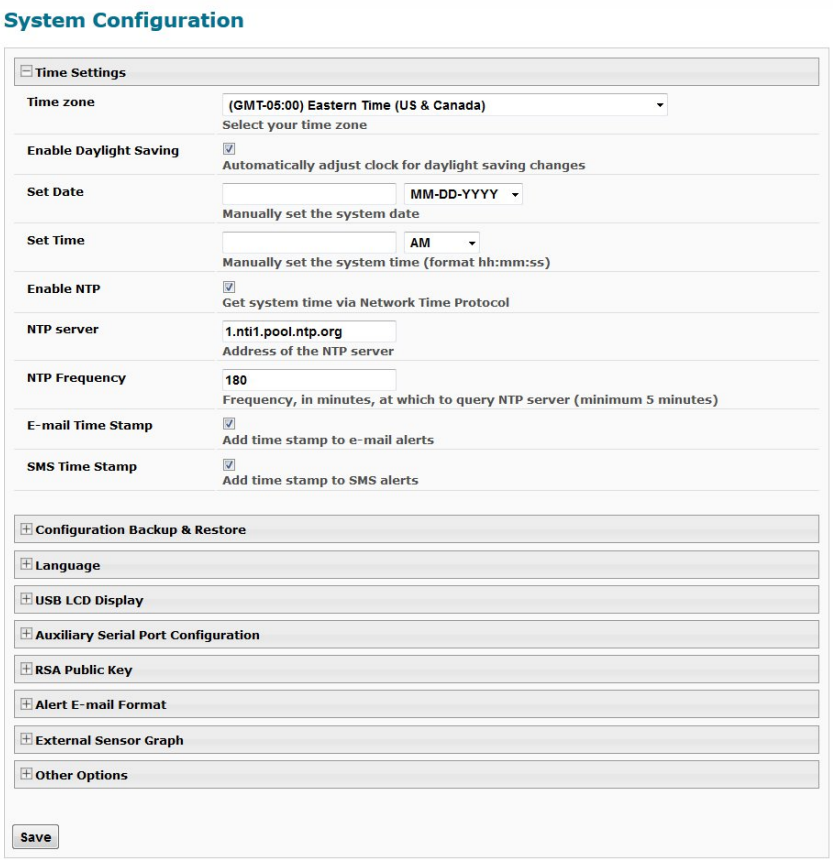


Figure 64- System Configuration page

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, press "Save" and 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*** ***Note: Before overwriting the existing configuration, consider whether the existing configuration should be saved first. If it will be saved, be sure to save the current configuration file under a different name than the configuration file to be loaded.***
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
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**.
Language Selection	
Select Language	Select between English, German (Deutsch) and Japanese for the language to read the ENVIROMUX menus in.

Note: If "Restore Defaults" is used, the IP address will also be restored to its default address (192.168.1.21) 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 28).

This is particularly useful when preparing to make changes to the configuration that may provide unsatisfactory results. If the configuration is saved in a file before changes are made, stepping backward and restoring the previous settings is as simple as clicking on the file saved. Just be sure to remember the name of the file saved and where in the PC it was saved.

Default settings can also be restored using the "Restore Defaults" button on the front of the ENVIROMUX (see page 112).

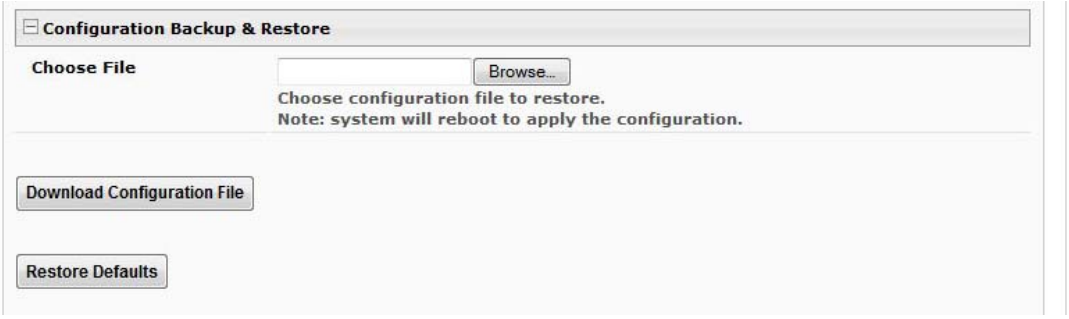


Figure 65- Configuration Backup and Restore

USB LCD Display	
Select Screen	Select what should be displayed on a USB LCD monitor when plugged into a USB port on the ENVIROMUX (see Figure 66) An USB LCD monitor can be connected to any of the USB Type A ports (page 113). The ENVIROMUX will automatically sense the monitor and send the selected images to the screen.
RJ45 Connector	When RJ45 Connector is selected for display on the LCD monitor, choose between RJ45 connector 1 or 2 as the sensor status page to be viewed on the monitor.
Auxiliary Serial Port Configuration ("RS232 AUX")	
Use Aux Port for	Choose between Remote Serial Port or GSM Modem or Console ➢ Configure as a **Remote Serial Port** when the port will be used to control a remote serial device. ➢ Configure as a **GSM Modem** port when a modem will be connected ➢ Configure as a **Console** port when a terminal will be connected for serial control of the ENVIROMUX (E-5D only)
Baud Rate	When "Remote Serial Port" is selected, set the Baud Rate to a speed compatible with the connected serial device. Speeds range from 1200bps through 115200bps. When GSM Modem is connected, no configuration is necessary here.. When Console is selected, set to a speed compatible with the connected terminal
Format	When "Remote Serial Port" is selected, enter the number of bits, parity, and number of stop bits for the remote serial device to be connected. When GSM Modem is connected, no configuration is necessary here. When Console is selected, enter the number of bits, parity, and number of stop bits for the terminal to be connected (usually 8-N-1)

Figure 66- Select what will be displayed on connected USB LCD Monitor

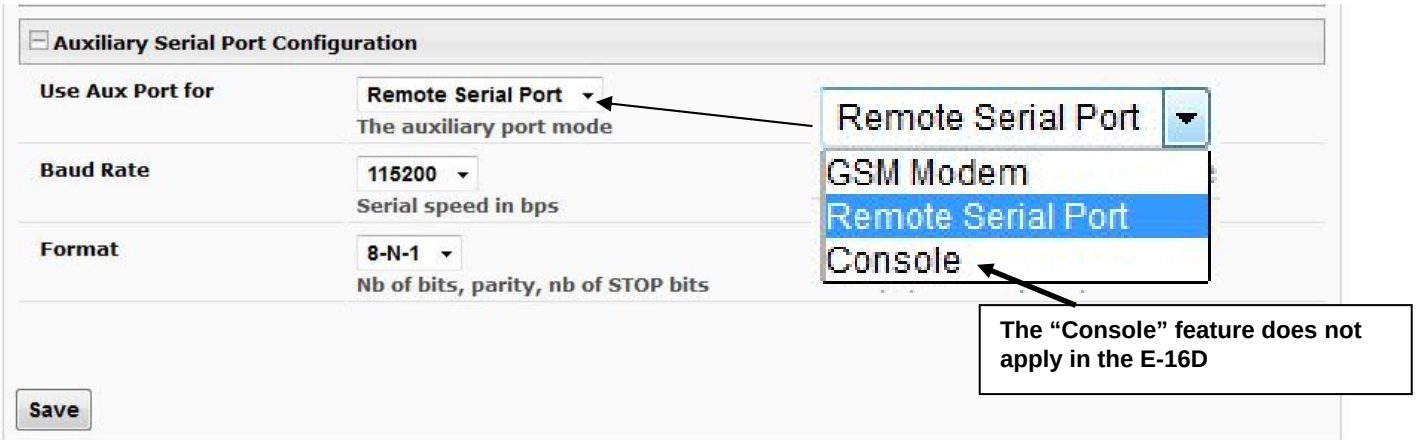


Figure 67- Configure the purpose of the "RS232 AUX" port

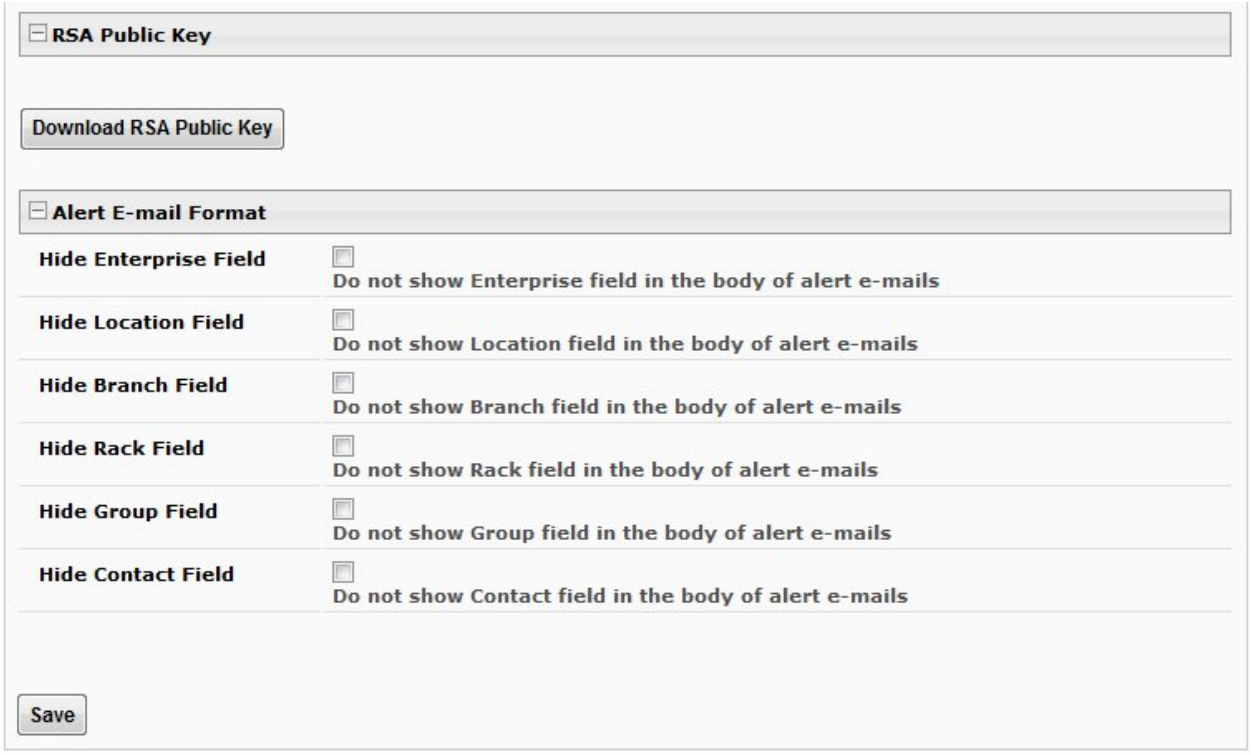


Figure 68- System Configuration-continued

RSA Public Key

Click on this button to save an authentication key to a Linux or Unix machine. In order to configure an Event or Smart Alert to cause an SSH command to be sent to a Linux or Unix machine automatically (see page 97 or page 101), the Linux or Unix computer must be configured to accept the command from the ENVIROMUX. To do this, save the RSA public key, filename **`id_rsa.pub`**, to the computer(s) to receive remote SSH commands.

Then, on the computer to take the command, while logged in as root, type the following command from the directory where the file was downloaded:

```
$ cat id_rsa.pub >> root/.ssh/authorized_keys
```

This command will append the ENVIROMUX key to the list of authorized keys

Then, to make the change take effect, restart the SSH server by typing:

```
$ sudo service ssh restart
```

Alert E-mail Format

To customize the content of the alert messages received via e-mail, pieces of information that would normally be contained in the emails can be omitted. For each piece of information that you do not want to be shown, place a checkmark in the category. Once you click on “Save”, your changes will be made in the ENVIROMUX.

Figure 69- Disable External Sensor Graph

Disable Sensor Graphs

When checking the status of external RS485 sensors, by default a graph is displayed with the accumulative readings for that sensor (see page 36). The display of that information will take some additional time for your browser to provide. If you don't wish to have that graph displayed and would rather speed up the status information of these sensors, you can place a checkmark in "Disable Sensor Graphs".

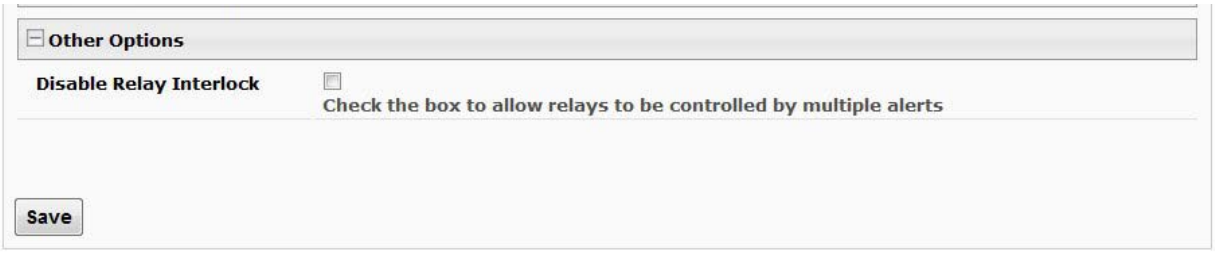


Figure 70- Disable/Enable Relay Interlock

Other Options

Under "Other Options" is a checkbox that allows you to enable or disable the ability to have output relays controlled by multiple alert conditions. By default this box is unchecked.

While unchecked, each output relay can only be associated with one alert.

When this box is checked, the same output relay can be associated with multiple alert conditions and will have its state (open or closed) changed according to the configuration with each association (see page 42).

Click on **Save** when finished with System Configuration.

Administration-Enterprise Setup

The Enterprise Setup page (**Administration ->Enterprise**) is used to enter basic company information to be applied to the body of alerts. Enter the information to the blocks provided with your company 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 E-16D.

If SMS messages will be used as an alert method, a GSM modem will be needed and this page will provide status information for that connection as well as the ability to configure alerts to be sent if the modem connection fails (see also page 17).

Note: If the e-mail address you supply doesn't work, one possible cause may be the policy of the server. Verify that the introduced Enterprise e-mail address will be accepted by the server. With some SMTP servers, messages may be rejected prompting an error message to be logged and alert messages being blocked from reaching their destinations.

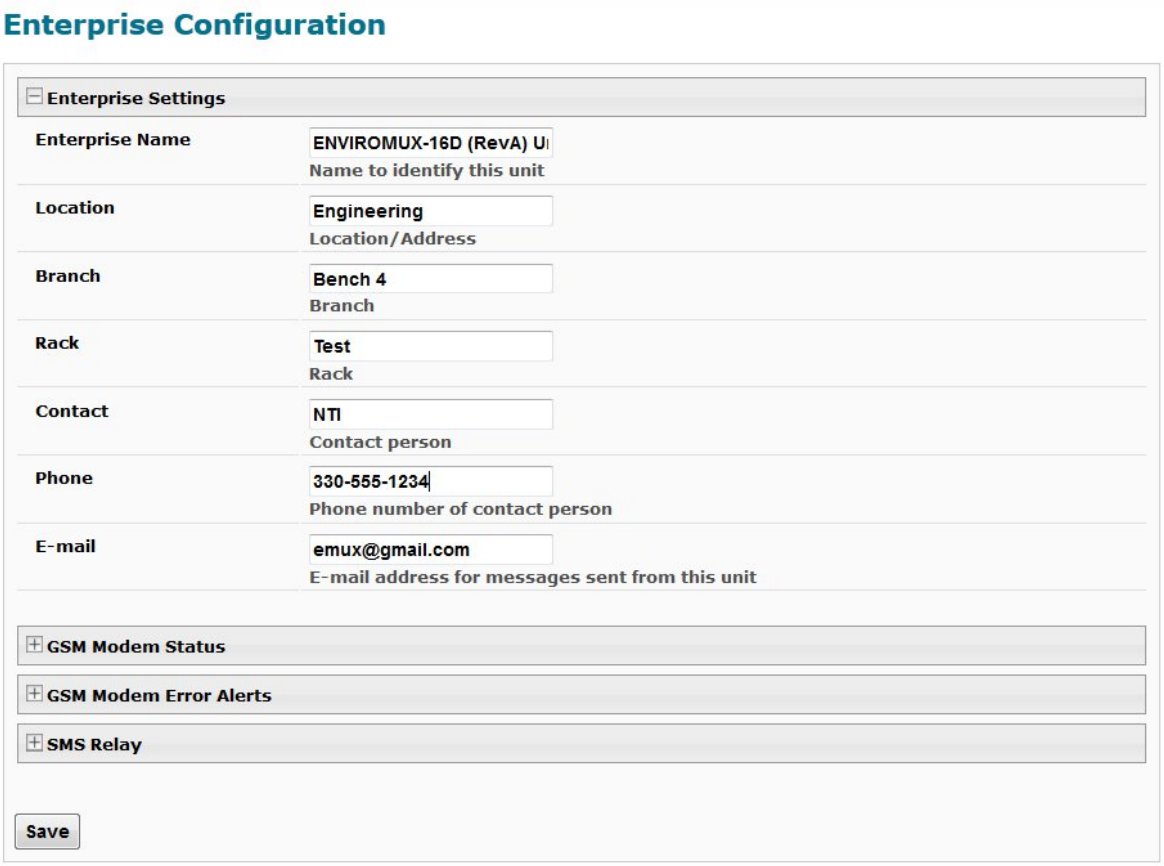
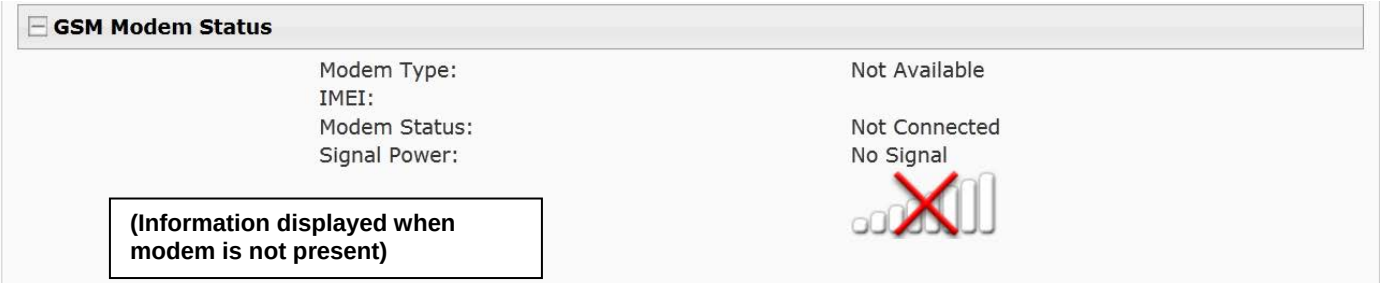


Figure 71- Enterprise Configuration Page

GSM Modem Status

If a modem has not yet been connected, the message "Not Available" will appear on the setup menu. The modem must be powered ON and connected before the ENVIROMUX is powered ON.



The connected modem must have a GSM type SIM card configured for SMS messaging and should be “unlocked” to prevent it from being limited to use in just this modem without further configuration.

When a modem is present, the type, status, IMEI number, and signal strength will be displayed. The modem will work with a signal strength between -111dBm (weak) and -51dBm (strong).

Figure 72- GSM Modem Status

GSM Modem Error Alerts

If the modem fails to send an SMS when prompted to do so due to loss of service provider connection, error in protocol, or if the connection runs out of prepaid minutes, the ENVIROMUX can be configured to send an alert message via Email, Syslog and/or SNMP. Select what group(s) this notification will belong to and what methods of communication to use and click “Save”.

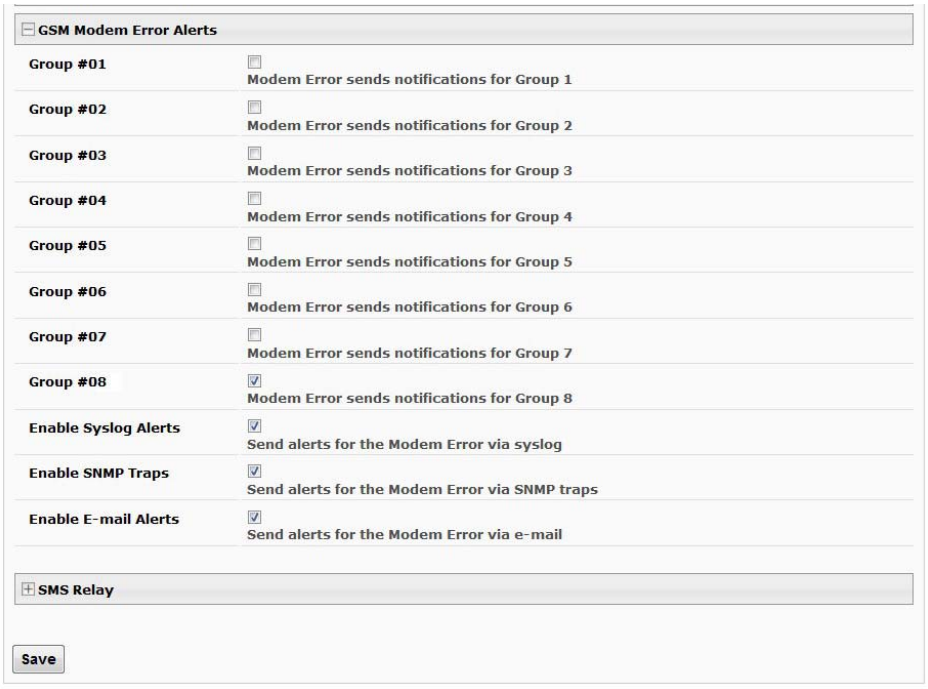


Figure 73- GSM Modem Error Alert Configuration

Enable SMS Relay

If your network includes more than one ENVIROMUX (E-16D, E-5D and/or E-2D), only one GSM modem is required for all the ENVIROMUX units to send SMS messages. That GSM modem can be connected to any of the ENVIROMUX units. Using the SMS Relay feature, all ENVIROMUX units can send SMS messages through the single GSM modem.

To use the SMS Relay feature;

- If the GSM modem is connected to the ENVIROMUX you are configuring, place a checkmark in "**Enable Server**" block.
- If the GSM modem is connected to another ENVIROMUX unit, leave "Enable Server" unchecked and instead place a checkmark in "**Use remote unit to send SMS**" and enter the IP address of the ENVIROMUX unit that has the GSM modem connected to it in the block "**Remote unit IP Address**".

Be sure to click "**Save**" to save the configuration.

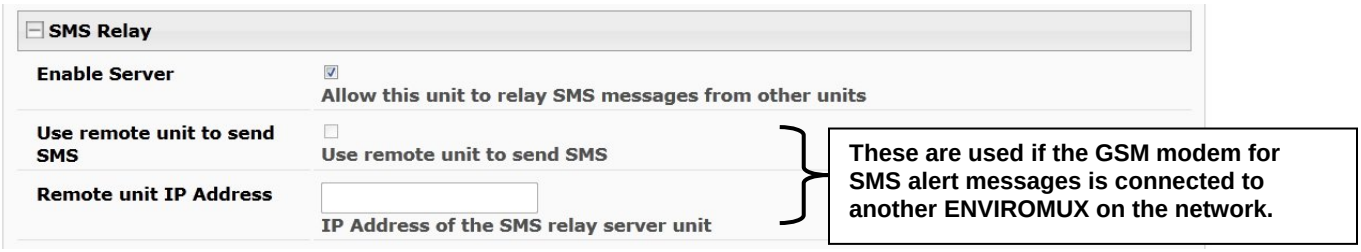


Figure 74- SMS Relay Configuration

Note: To use the SMS relay feature between two ENVIROMUXs on a network separated by a firewall, be sure to open ports 6001 and 6002 in the firewall configuration to enable SMS communication between the ENVIROMUXs

If your network has only one ENVIROMUX connected to it, the SMS Relay feature will have no effect

Administration-Network Setup

From the Network Configuration page (**Administration->Network**) 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.

Note: If you select "DHCP", make sure a DHCP server is running on the network the E-16D is connected to.

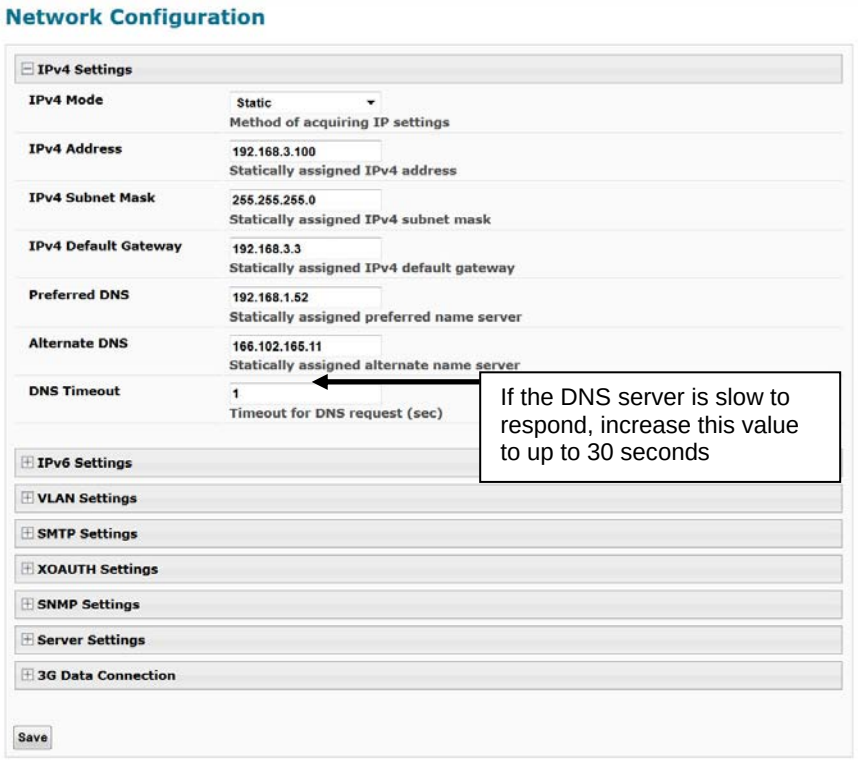


Figure 75- Network Configuration Page

Settings can be entered for either the IPv4 or IPv6 protocols.

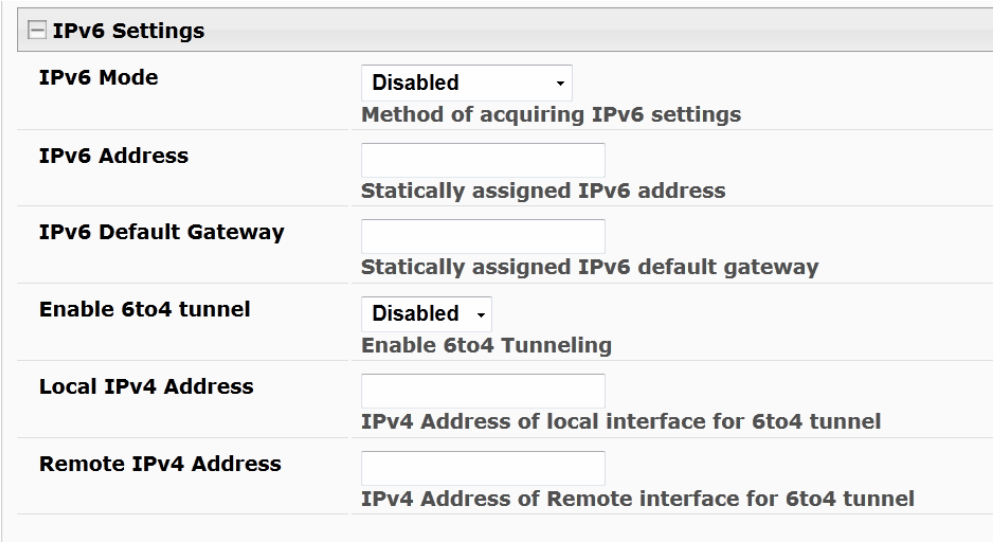


Figure 76- Apply IPv4 or IPv6 Settings

If the administrator chooses to have the DNS information filled in automatically, the SMTP server and port number still need to be entered for e-mail alerts to work. If the SMTP server requires a password in order for users to send e-mails, the network administrator must first assign a user name and password to the ENVIROMUX. Then apply the user name and password to the "User" and "Password" fields under "SMTP Settings". The ENVIROMUX must be power-cycled for changes to the SMTP server to take effect.

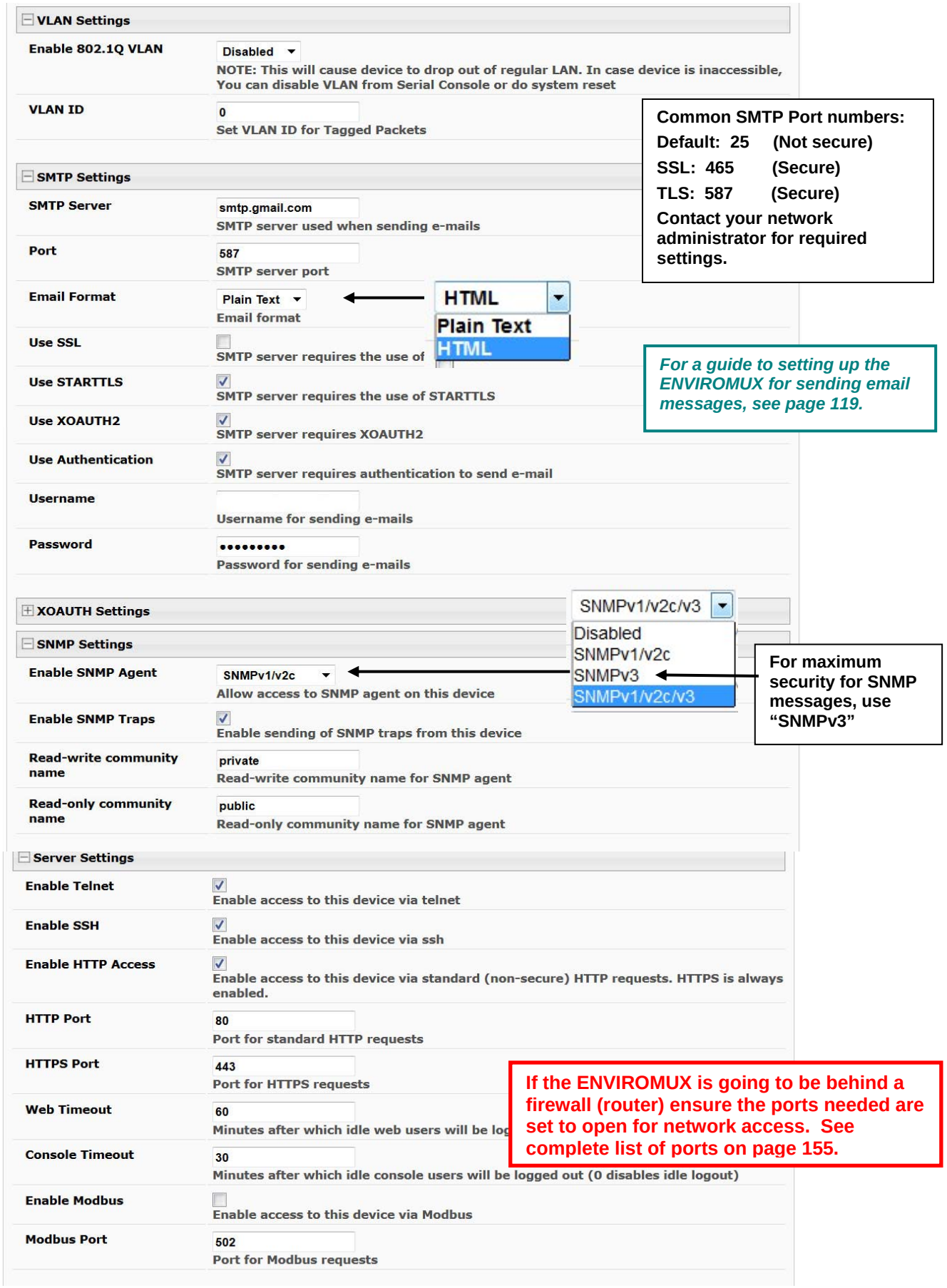


Figure 77- Configure SMTP, SNMP, and security settings

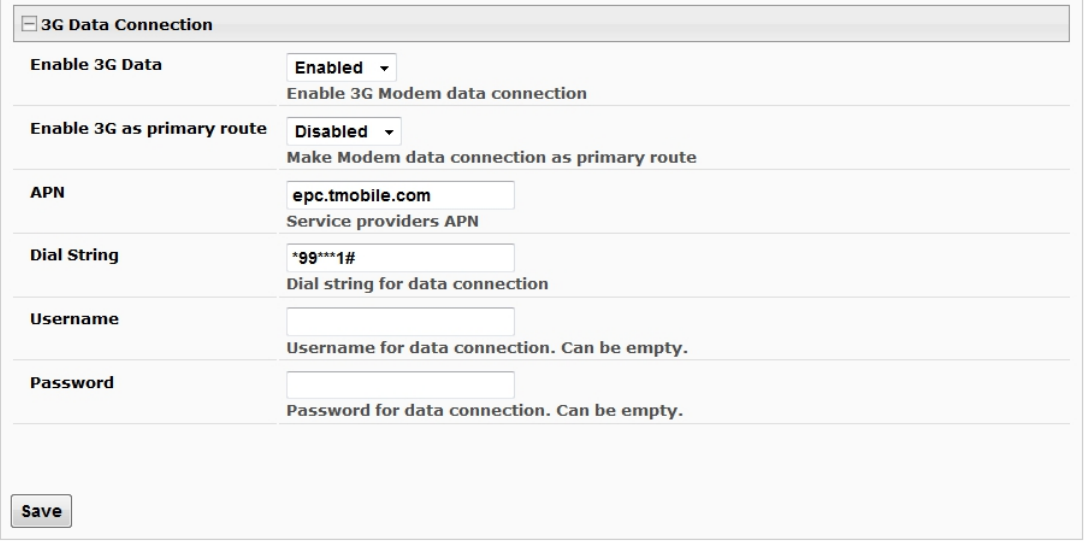


Figure 78- Configure 3G Data Connection

VLAN Settings	Description
Enable 802.1Q VLAN	Select between "Disabled" (the default) or "Enabled"
VLAN ID	Enter a number between 0-4095 for your VLAN ID
SMTP Settings	
SMTP Server	Enter a valid SMTP server name (e.g. yourcompany.com)
Port	Enter a valid port # (default port is 25, for SSL most use 465, for STARTTLS most use 587)
Email Format	Choose between sending emails in Plain Text format (the default) and HTML format
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 XOAUTH2	Place a checkmark in the box if the SMTP server supports OAUTH authentication (i.e. Gmail server)
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. Choose between v1/v2c, v3 only (maximum security), or v1/v2c/v3.
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")
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 **By default Telnet is disabled.**
Enable SSH	Place a checkmark in the box to enable access to the ENVIROMUX via SSH
Enable 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 notes below (the first two notes at the top of the next page).**
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)
Console Timeout	Number of minutes after which idle console user will be logged-out (enter 0 to disable this feature)
Enable Modbus	Place a checkmark in the box to enable access via Modbus software
Modbus Port	Enter a valid port number to be used to communicate via Modbus (default is 502)

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 84) and load it into the ENVIROMUX and any PC that will be required to access the ENVIROMUX.

Read-Only Community Name

The SNMP Read-only community name enables a user to retrieve "read-only" information from the ENVIROMUX using SNMP network management software or a MIB browser and a MIB file. This name must be present in the ENVIROMUX and in the proper field in the SNMP software. This name is **case sensitive** so be sure to enter it correctly in the ENVIROMUX as well as in the SNMP software.

Read-Write Community Name

The SNMP Read-Write community name enables a user to read information from the ENVIROMUX and to modify settings on the ENVIROMUX using SNMP network management software or a MIB browser and MIB file (MIB file version 1.05 or later). This name must be present in the ENVIROMUX **AND** in the proper field in the SNMP software. This name is **case sensitive** so be sure to enter it correctly in the ENVIROMUX as well as in the SNMP software.

This function is particularly useful if you want to control the state of the Output Relays (page 51) through SNMP. With the ENVIROMUX and SNMP network management software properly configured for SNMP control (enable agent, enable traps, apply Read-only and Read-write Community Names), a SET command can be sent either from the SNMP software or MIB browser (Windows) or through command line (Linux) to change the outputRelay value state. See images on page 72 for example of setup.

3G Data Connection	
Enable 3G Data	Enable if you want the option to have the ENVIROMUX send alert messages through the USB modem and the option to access the web interface using the IP address assigned to the SIM card account. The default is disabled. ***NOTE: In order to access the web interface through the modem, the SIM card must have a "public" IP address (page 18).***
Enable 3G as primary route	Enable if you want all messages that are sent by the ENVIROMUX to go through the modem connection instead of the Ethernet. The default is disabled. ***Note: If this feature is enabled, and then later disabled, the ENVIROMUX must be rebooted to reset outgoing messaging parameters.***
APN	Enter the APN address of the service provider (provided by the service provider)
Dial String	Enter the dial string required for data connection(provided by the service provider)
Username	Enter the username supplied by service provider for access to connection. Leave blank if no username is required.
Password	Enter the password supplied by service provider for access to connection. Leave blank if no password is required.

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 most common SMTP server port number is 25, but it is 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). This might be desired if the administrator wants a secure connection.

Note: If the port number is changed and forgotten, to determine what it has been changed to connect the ENVIROMUX for RS232 control (page 15) and review the Network Settings (page 67).

If the SMTP server supports SSL (user authentication), click the block next to "Use SSL" to place a check mark in it.

Note: If the 3G Data connection is enabled as the primary internet connection, make sure that a reliable signal exists between the modem and service provider. Otherwise attempts made by the ENVIROMUX to communicate with devices on the network may be delayed and cause unnecessary alert messages.

For a guide to setting up the ENVIROMUX for sending email messages, see page 124. For assistance in setting up SNMP messaging, see page 127.

For a complete list of ENVIROMUX factory-assigned port numbers, see page 162.

VLAN Settings

The ENVIROMUX supports 802.1Q VLAN tagging (firmware version 2.52 and later) which can be used on managed switches to get more bandwidth and improved security. Any ID number between 0 and 4095 can be used.

Note: If VLAN Tagging is enabled, the E-xD will drop out of the regular network (Native VLAN) and users won't be able to access it from an unmanaged switch. If the ID number is lost/forgotten, you can reset it by connecting to the ENVIROMUX through the serial port (page 61) or by using the "Restore Defaults" button (page 112) on the E-xD.

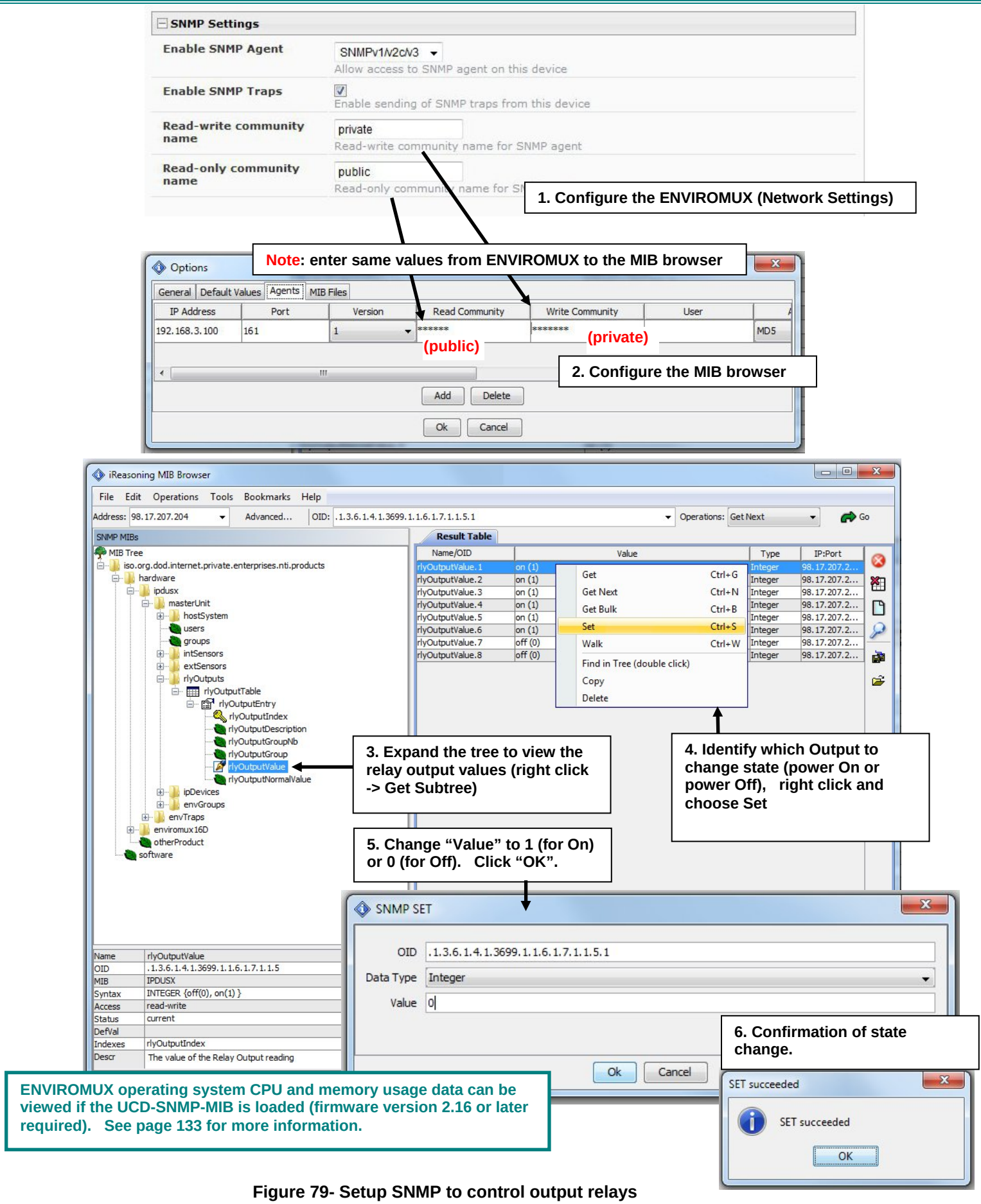


Figure 79- Setup SNMP to control output relays

XOAUTH Settings

On the Network Configuration page is a section for XOAUTH Settings, used to enable automatic user authentication verification when the SMTP server requires XOAUTH2 authentication (i.e. Gmail).

Note: Make sure your SMTP settings are entered correctly (username, password, "Use Authentication" is checked, etc.) before proceeding (page 68).

1. First place a checkmark in the box under SMTP settings to enable the use of XOAUTH authentication (page 68). Click "**Save**" at the bottom of the page to apply this change.

Notes: If your SMTP Server port is set to 587, make sure "Use STARTTLS" is checked (page 68).
If your SMTP Server port is set to 465, make sure "Use SSL" is checked.
Do NOT set the Server port to 25 when using XOAUTH.

2. Next click on "**Generate Verification URL**" under XOAUTH Settings.

Figure 80- XOAUTH- Generate Verification URL

3. A lengthy URL address will be generated. Copy and paste the **entire** URL into your browser.

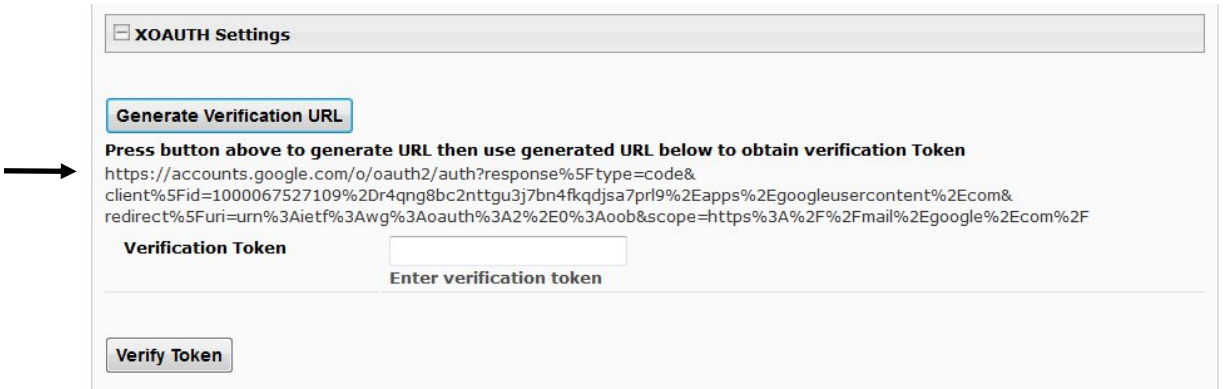


Figure 81- XOAUTH- Copy Verification URL

4. You will be prompted to login to the Gmail account you have setup for the ENVIROMUX. Once logged in, Gmail will ask if you want the ENVIROMUX to be able to view and manage email from this account. Click on "**Accept**".

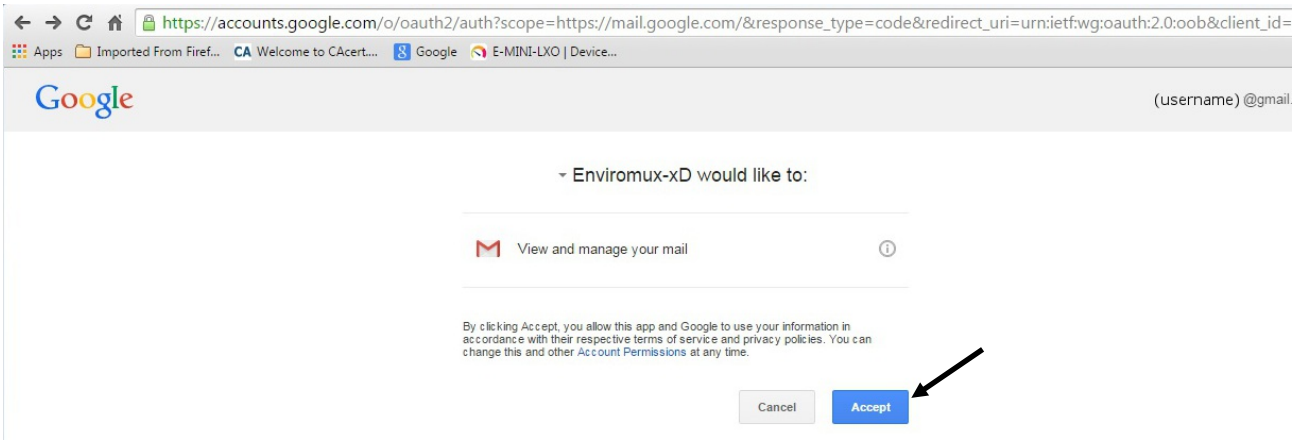


Figure 82- XOAUTH- Accept prompt to manage your mail

5. You will then be presented with a token. Copy the characters in the token to your clip board, and switch back to the web interface page of the ENVIROMUX. Paste those characters into the "**Verification Token**" block.

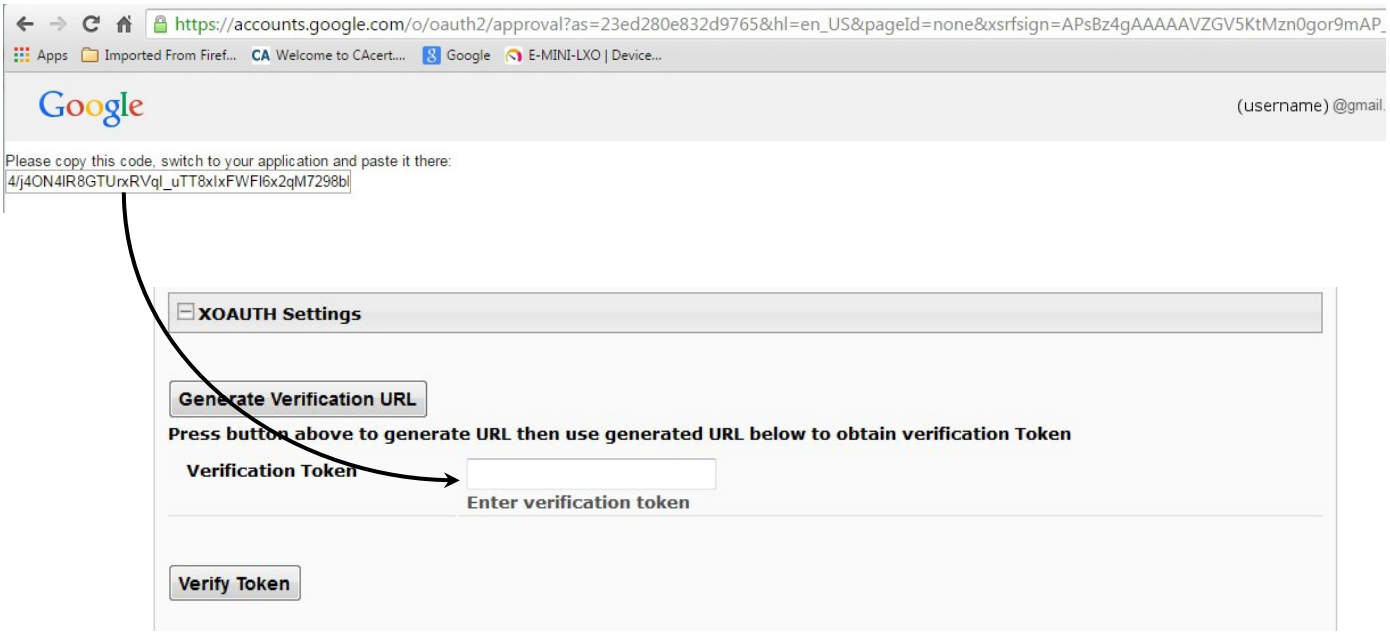


Figure 83- XOAUTH- Enter Verification Token

6. Click on "**Verify Token**" and if successful, you should see the message "**Changes Applied**" at the bottom of the page.

You will only need to perform this procedure once.

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 root user (or any user with administrator rights) 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. A user with Operator rights can perform some administrative functions, but not all. (See page 79). To view the Users page, click on **Users** from the **Administration** section of the r

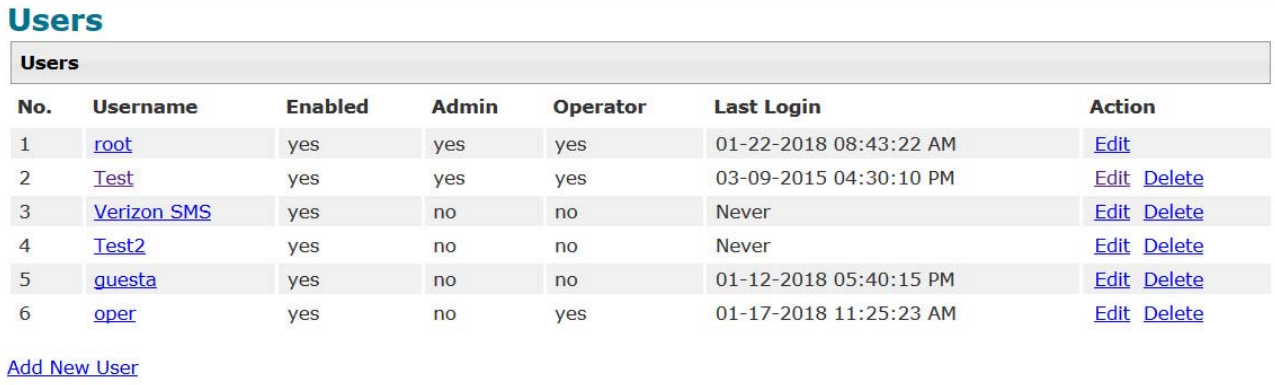


Figure 84- Usernames List and Status

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.

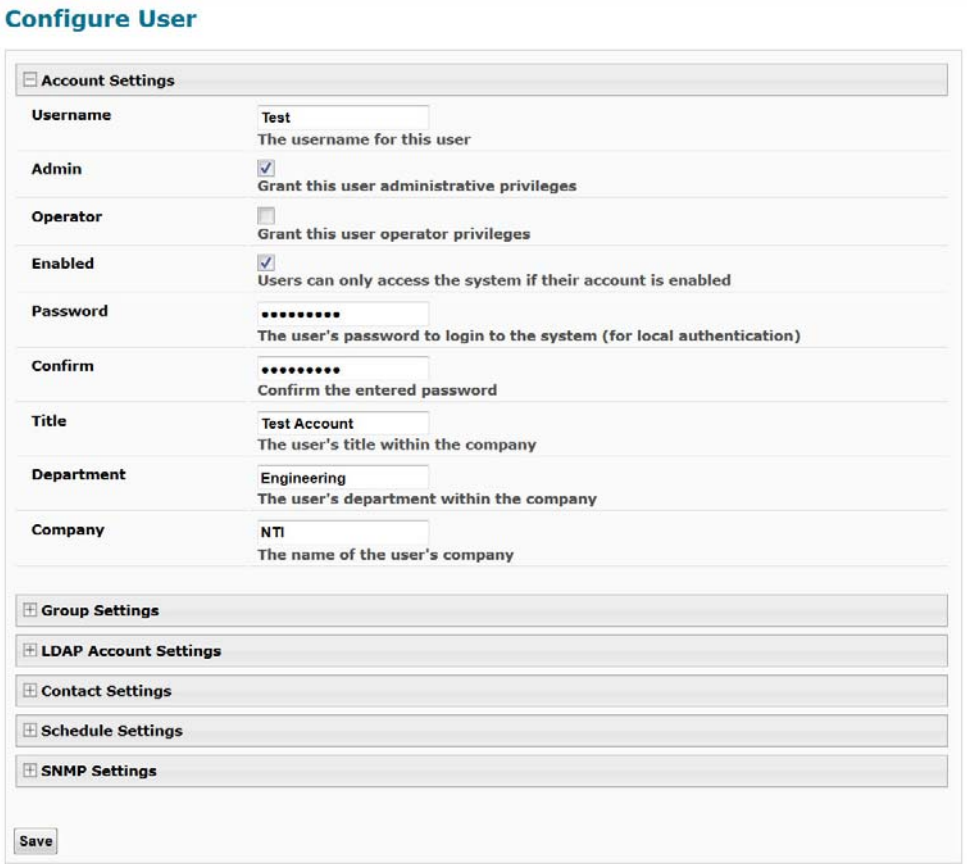


Figure 85- Edit user profile for root user

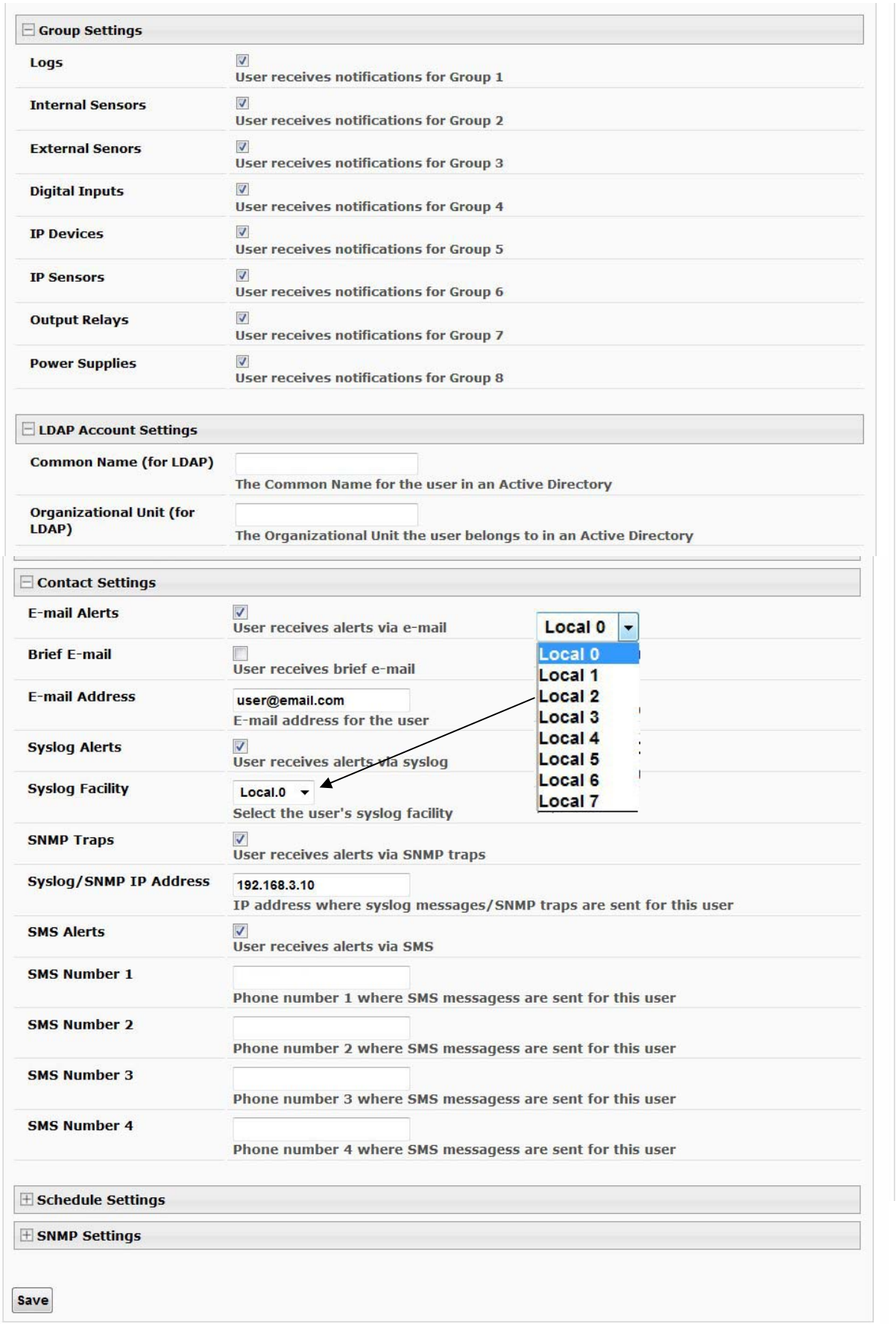


Figure 86- More user settings

Account Settings	Description
Username	Enter the desired username for this user
Admin	Place a checkmark here if this user should have administrative privileges
Operator	Place a checkmark here if this user should have operator 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
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 40 and 54 for group assignments)
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 86)
Contact Settings	
Email alerts	Place a checkmark if the user should receive messages via email
Brief email	Place a checkmark if email messages should be brief (contain only critical information) ***Note: Enabling this will also prevent images being sent from IP cameras to this user***
Email address	Enter a valid email address if this user should receive email alert messages (1 address only, maximum 63 characters) **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
Syslog facility	Select a Syslog Facility for the messages to be sent to- Local0 thru Local7 (default is Local0).
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 up to 4 different phone numbers to call to alert the user via SMS message

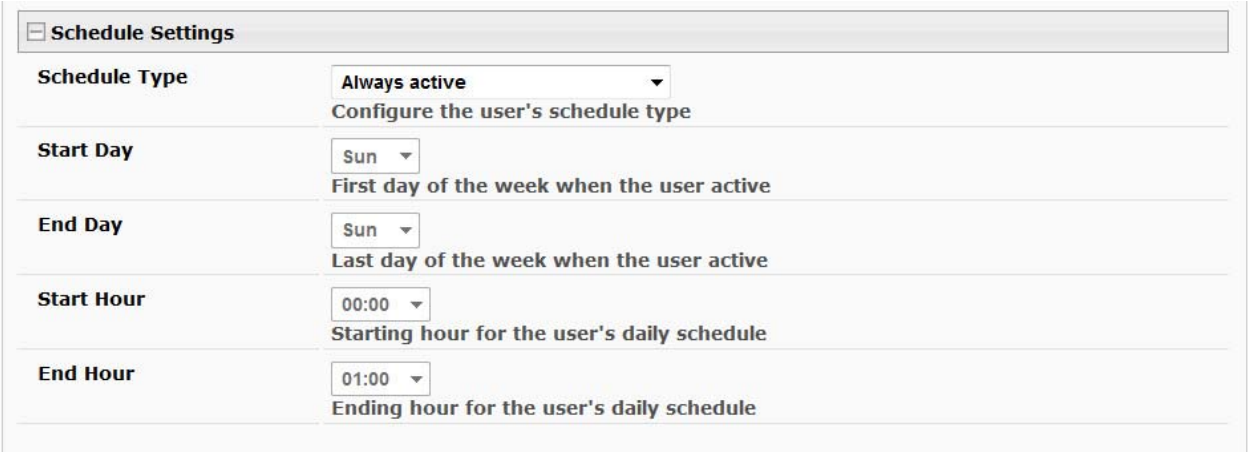


Figure 87- More user settings

Schedule Settings	
Schedule Type	**Always active**- user will receive messages at all hours of each day **Daily active during defined times-** user will receive message every day but during only the times specified **Active during defined times**- user will only receive alert messages during days and times as specified **Inactive during defined times-** user will receive alert messages at all hours EXCEPT those days and times specified.
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

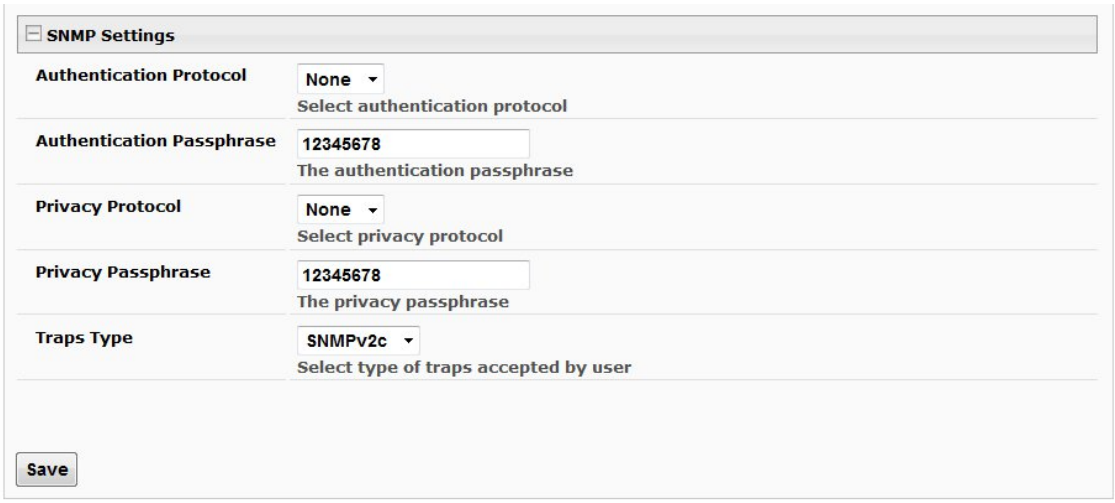


Figure 88- More user settings

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 “Save”.

If a user is set with only "User" rights instead of "Administrator" rights, the user will only be able to see current sensor readings and to change their password if so desired. No other ENVIROMUX access is possible.

Note: If the root user’s password is changed and forgotten, contact Network Technologies Inc at (800) 742-8324 (800-RGB-TECH) or (330) 562-7070 for assistance.

Note: Each user can have only one email address (maximum 63 characters) associated with that user. If an additional email address is needed, an additional user must be added with the desired email address. As long as both users are configured to get messages from the same sensor groups, both email addresses will get the same alert messages. For more on users and sensor groups, see page 42.

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.

The user with Operator privileges has fewer rights than an administrator but more rights than just the basic user rights. Operator privileges include:

- Ability to view alerts, acknowledge alerts and dismiss alerts of all Internal and External sensors.
- Ability to control output relays
- Ability to cycle the sensor power on digital inputs.
- Ability to view and download logs.
- Ability to reboot the unit.

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

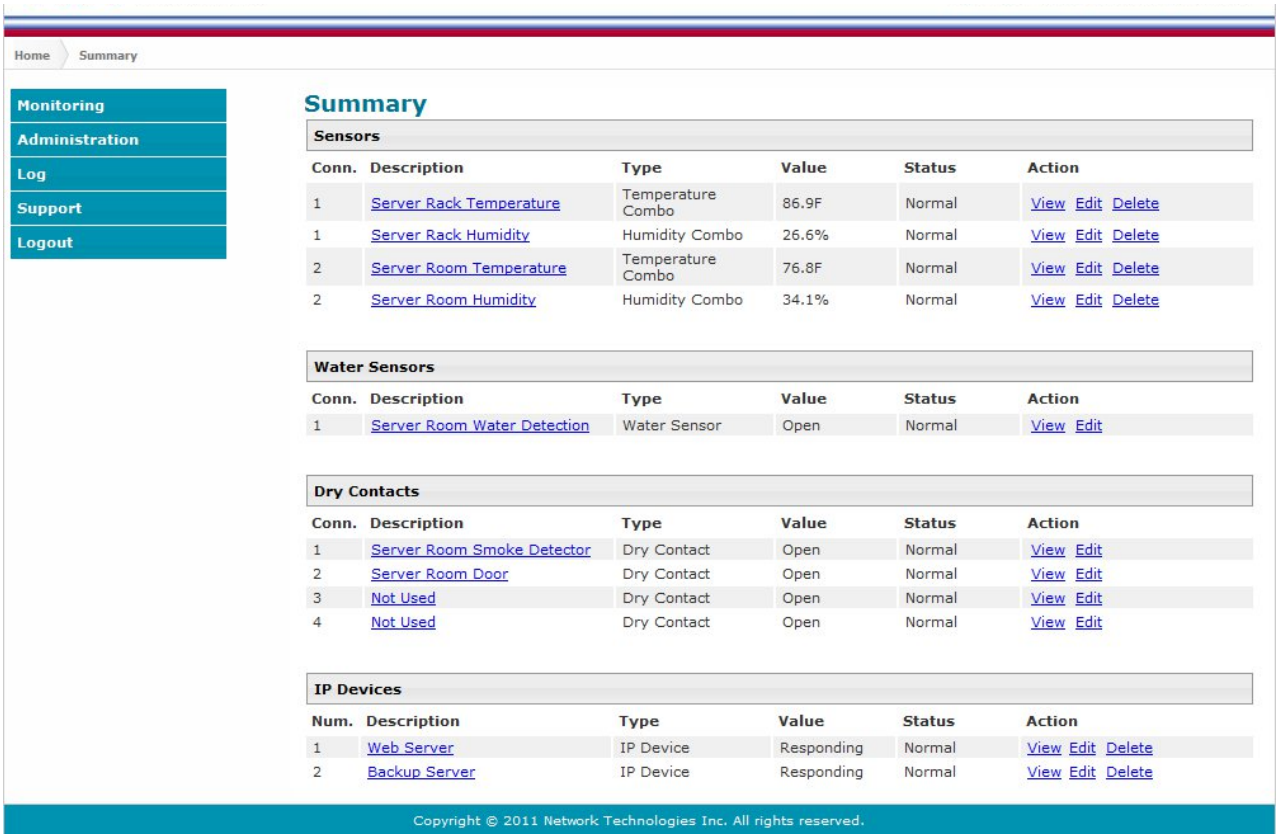


Figure 89-Summary page for User without Admin privileges

Group Names

Group names can be applied instead of the group numbers in the event an association is desired other than “Group 0x” . For each group (1-8), a name can be applied containing up to 64 English or 21 Kanji (Japanese) characters.

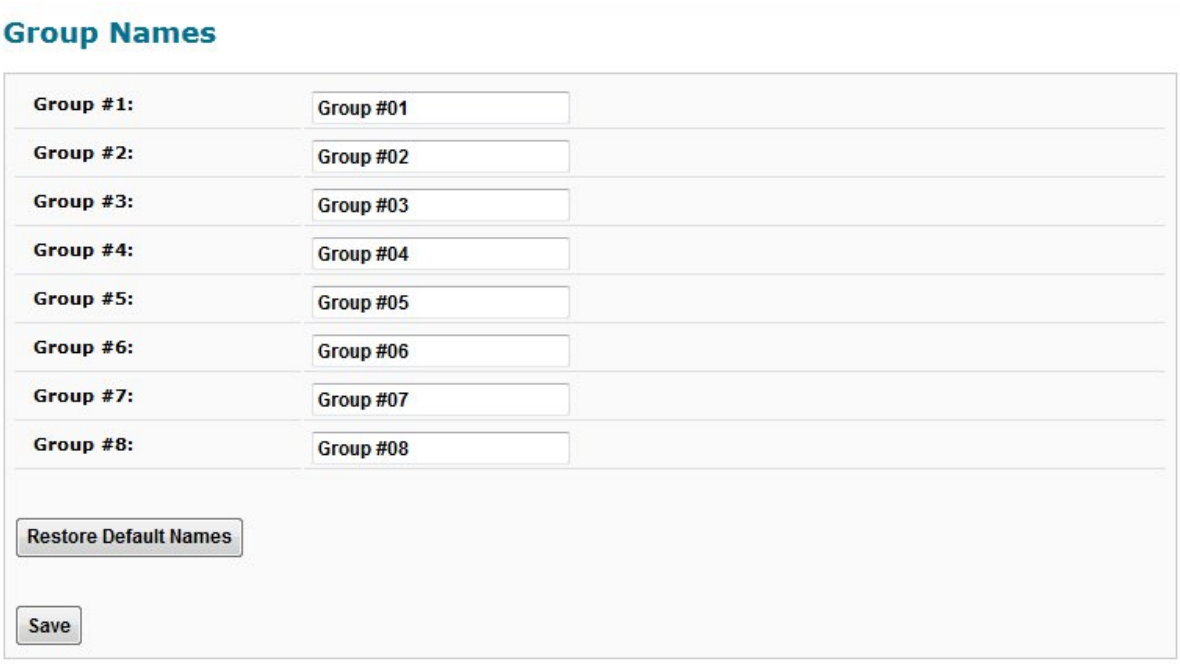


Figure 90- Enter custom group names

Security

Access to the web interface on the ENVIROMUX can be through standard methods (enable HTTP access- page 69) or limited to secure access only (disable HTTP access and only allow HTTPS access which is always enabled by default). Security in the ENVIROMUX can be managed one of three ways; through the local settings (passwords assigned in user settings on page 77), through an LDAP server or through a RADIUS 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.

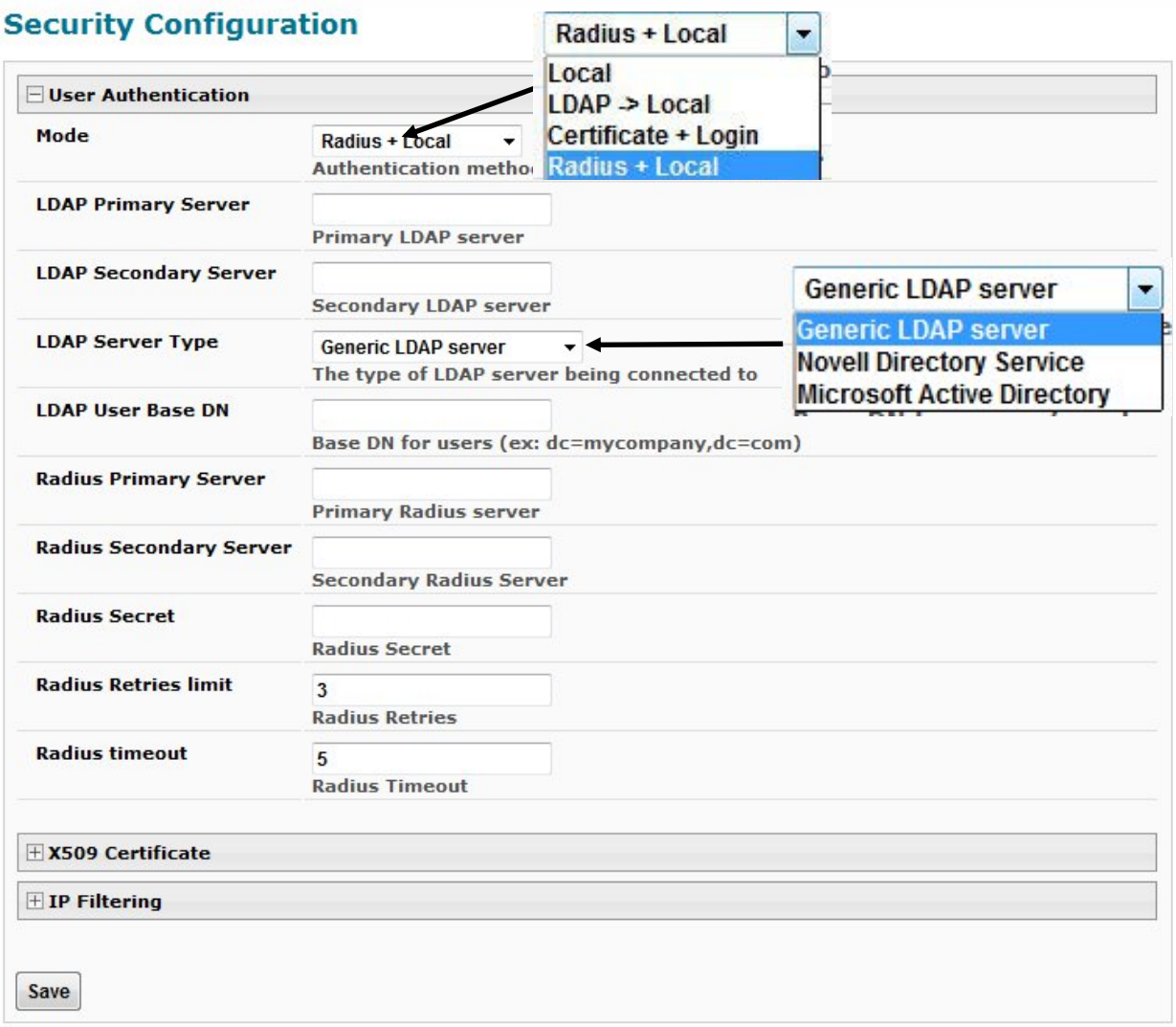


Figure 91- Security Configuration page

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 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 Select "Radius +Local" to use either local user authentication or authentication through a RADIUS server
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 server Microsoft Active Directory
LDAP User Base DN	Enter the Base DN for users (ex: ou=People,dc=mycompany,dc=com)
Radius Primary Server	Enter Hostname or IP address of Primary RADIUS Server
Radius Secondary Server	Enter Hostname or IP address of Secondary RADIUS Server (optional)
Radius Secret	Type the shared secret between the ENVIROMUX and the RADIUS server. The shared secret is case-sensitive, and it must be the same on the ENVIROMUX and the RADIUS server.
Radius Retries Limit	The number of times the ENVIROMUX will try to submit the provided username and password to the RADIUS server before it reports a failed connection attempt
Radius Timeout	The length of time in seconds that the ENVIROMUX will wait for a reply from the RADIUS server before either reporting a failed connection attempt or resubmitting as determined by the Radius Retries Limit

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

Using a RADIUS Server

1. The *dictionary.nti* file (this file has an *.nti* extension) must be saved to a location on the PC the RADIUS server is run from. (This file is found on the ENVIROMUX download page (http://www.networktechinc.com/download/d-environment-monitor-16.html).)

2. Edit the RADIUS ***dictionary*** file (no file extension) in the RADIUS server using a text editor, adding the following line:

```
$INCLUDE    /<path to dictionary.nti>/dictionary.nti
```

Example:

Open the file *dictionary* (no extension) found in the directory the RADIUS server is run from using a text editor

```
#       pre-defined dictionary files included with the server.
#
#       Any new/changed attributes MUST be placed in this file, as
#       the pre-defined dictionaries SHOULD NOT be edited.
#
#       $Id$
#
#
#
#       The filename given here should be an absolute path.
#

$INCLUDE        /etc/freeradius/dictionary.nti
$INCLUDE        /usr/share/freeradius/dictionary
#
#       Place additional attributes or $INCLUDEs here.  They will
#       over-ride the definitions in the pre-defined dictionaries.
#
```

(in this case the dictionary.nti file was saved to the directory /etc/freeradius)

Figure 92- Dictionary file of RADIUS server

3. Save the RADIUS ***dictionary*** file.

4. Once the ***dictionary.nti*** file has been included in the RADIUS server dictionary, users outlined in the RADIUS server users file (filename ***users***, again, no extension) can be assigned these properties. The values can be customized based on your requirements or kept the same for a group of users using a single variable. An example user configuration is below. Please note the tab characters preceding property names.

```
# Test Account
"Test"     Cleartext-Password := "T123est"
    Service-Type = Login-User,
    NTI-User-Permission := "readonly",
    NTI-User-Title := "Analyst",
    NTI-User-Department := "IT",
    NTI-User-Company := "VPI",
    NTI-User-Sensor-Groups := "1,3,4,5,6,7,8",
    NTI-User-Email := "network.technologies@gmail.com",
    NTI-User-Syslog-SNMP-Address := "192.168.3.10",
    NTI-User-Syslog-Facility := "2",
    NTI-User-SMS-Number := "1234567891",
    NTI-User-Enable-Email-Alert := 1,
    NTI-User-Enable-Brief-Email := 1,
    NTI-User-Enable-Syslog-Alert := 1,
    NTI-User-Enable-SNMP-Traps := 1,
    NTI-User-Enable-SMS-Alert := 0,
    NTI-User-Schedule-Type := "custom",
    NTI-User-Schedule-Start-Day := "sun",
    NTI-User-Schedule-End-Day := "sat",
    NTI-User-Schedule-Start-Hour := "01:00",
    NTI-User-Schedule-End-Hour := "22:00",
    NTI-User-SNMP-Auth-Protocol := "MD5",
    NTI-User-SNMP-Auth-Passphrase := "12345678",
    NTI-User-SNMP-Privacy-Protocol := "none",
    NTI-User-SNMP-Privacy-Passphrase := "123456789",
    NTI-User-SNMP-Traps-Version := "v3",
```

To save time, you could copy and paste this list into your *users* file and then edit it as needed for your custom installation.

Remember:
The files: *dictionary*
users
dictionary.nti
all need to be in the same directory (in the example in Figure 92 that is /etc/freeradius/)

The above username is "**Test**", and the password is "**T123est**". All the properties listed mirror those found in the user configuration in the ENVIROMUX web interface. Change "Test" and "T123est" as needed for a user. For the "Enable" properties, "1," means yes and "0," means no.

5. Once the ***dictionary*** file is updated and users are added to the ***users*** file, please restart the RADIUS server service and correct syntax errors if any.

6. In order to use a RADIUS server to access the ENVIROMUX, the Mode must be changed to "Radius + Local" and the additional RADIUS fields (all under Security Configuration-User Authentication (page 81)) must first be entered. When finished, click the "Save" button. Changes will have immediate effect.

7. After this the ENVIROMUX will auto add/update RADIUS users and log them in (if successful). Local users accounts can also be used to login if added through the Web Interface. A maximum of 16 users are enabled and active at a time on a device. If more than 16 users login, ENVIROMUX will evict the least recently logged-in user.

Note: If the user password as configured in the RADIUS server is different than that set in the ENVIROMUX user account, the RADIUS server will adjust the ENVIROMUX user account password to match the one in the RADIUS server.

All radius property names are optional. For a detailed list of available property values, please check ***dictionary.nti*** file.

Change User Attributes

To change user attributes on the RADIUS Server:

1. Edit the user's file in RADIUS (filename ***users***, no extension) and make the desired changes to the user attributes.

   ex. NTI-User-Permission := "admin"

2. Save the user file.
3. Restart the RADIUS service.
4. On the E-xD, delete the user that the changes have been made on in the RADIUS server.
5. Logout and Re-Login to the E-xD with the updated user's login and password.

The RADIUS server should automatically load the new user attributes into the E-xD unit.

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 167.

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 91). 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.**

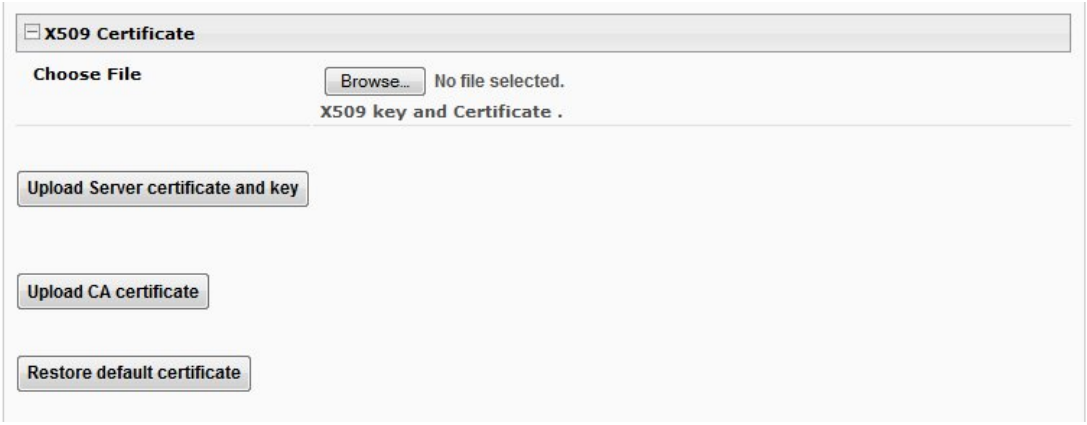


Figure 93- Security Configuration-X509 Certificate

Note: HTTP access can be enabled/disabled from web page under Administration -> Network -> Server Settings -> Enable HTTP (page 69). 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.

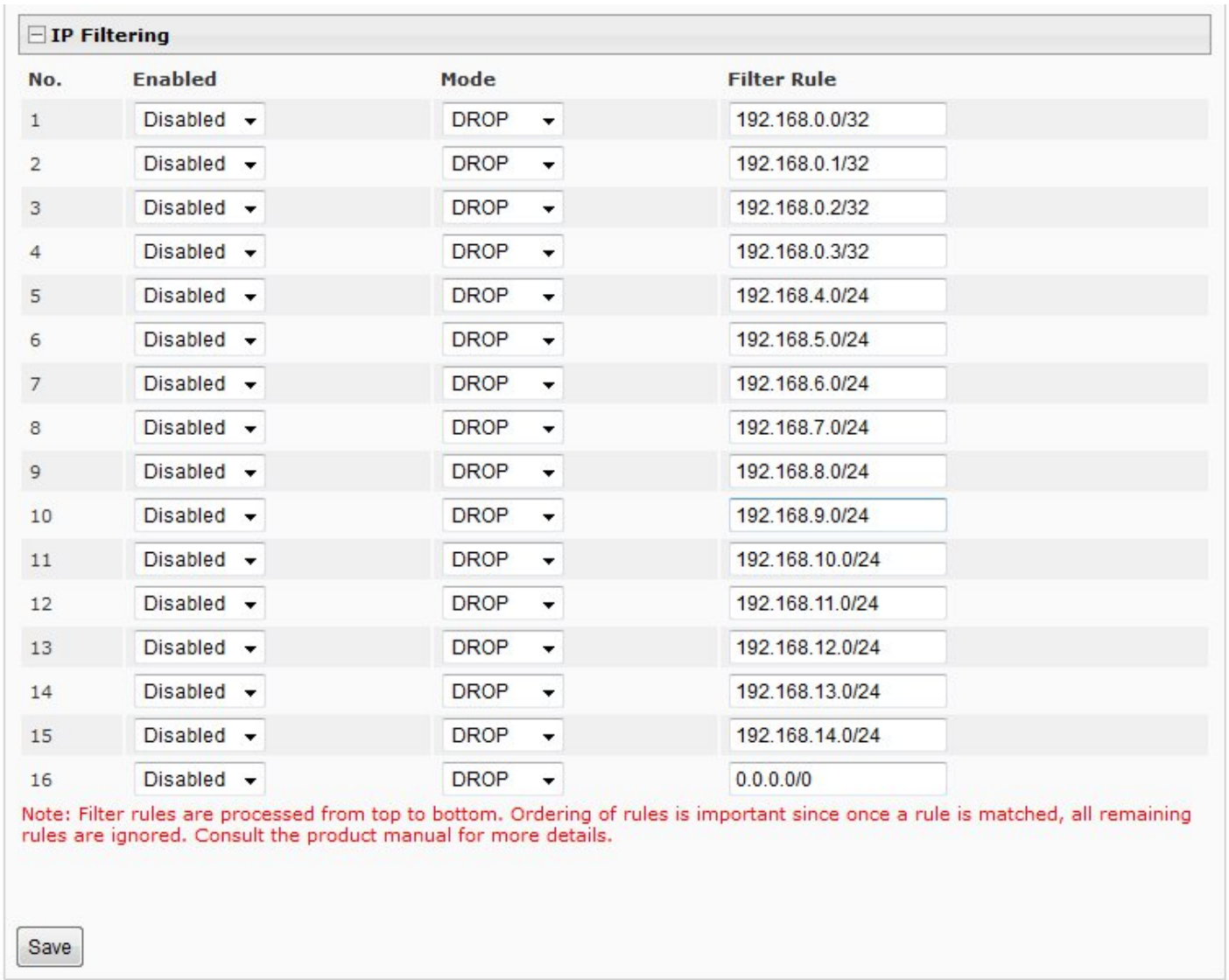
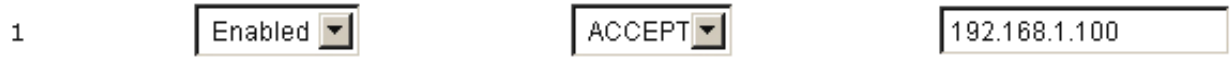


Figure 94- Security Configuration- IP Filtering Rules

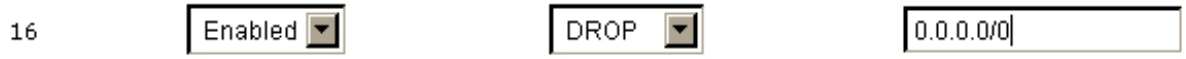
More on IP Filtering

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:



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



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

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

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

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

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.

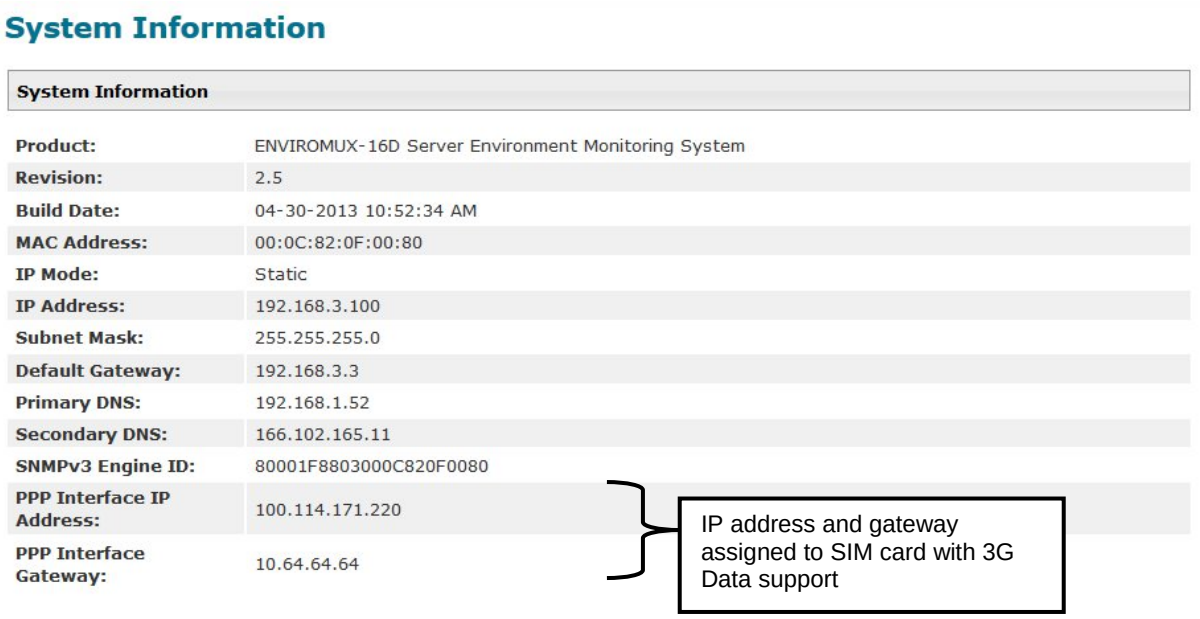


Figure 95- System Information page

Administration- 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-monitor-16.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.

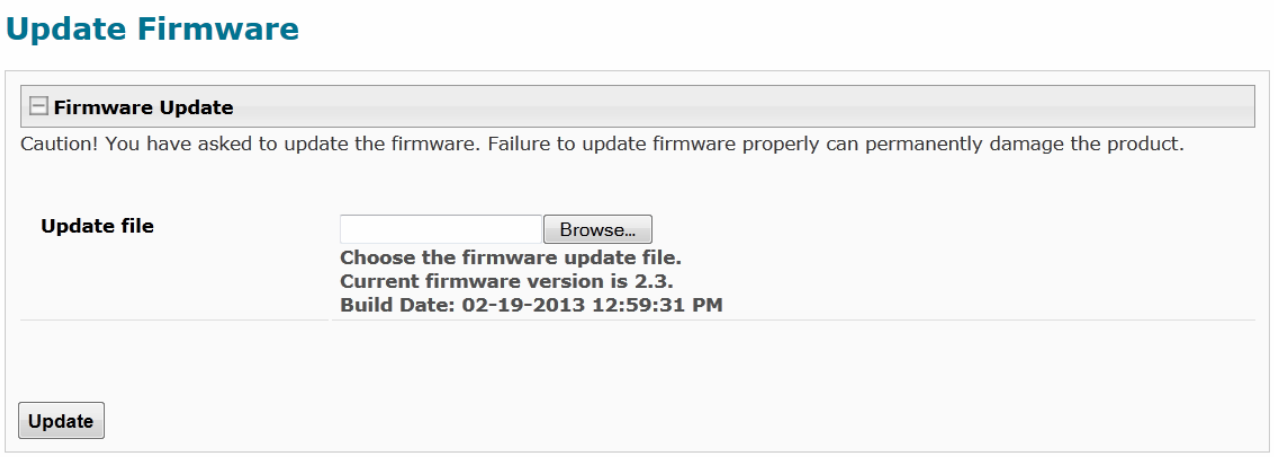


Figure 96- Update Firmware Page

1. Download the most current firmware file from http://www.networktechinc.com/download/d-environment-monitor-16.html to a location on your PC.
2. Click on the "Browse" button and locate and select the firmware file for the ENVIROMUX (***enviromux-xd-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 (this will take another 4-5 minutes after a firmware update) and the login screen will appear.

Note: In the event the ENVIROMUX firmware should be corrupted, such that connection through the web interface is no longer possible, contact NTI for instruction and recovery files to access the ENVIROMUX and restore the firmware using a TFTP server and Terminal connection (page 15).

Advanced-Cascade Configuration

From the **Administration->Advanced>Cascade** menu, the administrator can configure the ENVIROMUX to either be

- a master system,
- an Ethernet slave
- an RS485 local slave

When cascading via Ethernet, the E-16D, -5D or -2D can be used as master or slave in any combination.

In a cascaded configuration, there can be 1 master unit and up to 4 slave units.

A cascaded configuration can consist of one or more Ethernet slaves and one or more RS485 slaves, but a maximum of 4 slaves total.

Notes:

-When ENVIROMUX units are connected as slaves, only their sensors and output relays are used and are monitored through the master unit.

-Only E-16D units can be used as Master and Slaves in an RS485 cascaded configuration.

-E-16D,-5D and -2D units can be Master or Slaves when cascading via Ethernet.

-E-2D used in a cascaded configuration must be the "REV C" design (includes 2- 9VDC power jacks).

-After setting up cascading for ENVIROMUX units, we recommend re-booting the slaves completely before re-booting the master to have the master properly recognize the slaves and their sensors.

-Do not configure sensors from the Slave web interface, do not put a check in "Add to datalog" (page 40) and do not enable any alert methods. Only enable datalogging and alert methods for sensors when configuring them from the Master interface. Otherwise accumulative data at the Slave will cause a loss in communication with the Master.

1. Go to the Administration -> Cascading page for each ENVIROMUX and using the choices in the drop down box (Figure 97), select the position each ENVIROMUX will hold in the cascaded system.

   If you select **Ethernet Slave**, make sure each Ethernet Slave has a unique IP address (must be different from the Master unit and any other Ethernet Slave). With "Ethernet Slave" selected and a unique IP address assigned, press "Save" and exit the web interface. This unit will be controlled and configured from the Master unit web interface.

   If you select **RS485 Slave (E-16D only)**, also enter an RS485 address value from 1-255 to be used when defining what RS485 slaves are part of a cascaded configuration. Make note of the address entered. Each RS485 slave must have a unique address, but any value from 1-255 can be used. Once the address values have been saved, connect the RS485 slaves to the master as described in step 2 (Figure 98).

   If you select **Master**, then be sure to designate and connect the Slave units properly (unique IP addresses must be assigned for Ethernet Slaves and unique RS485 addresses assigned to RS485 Slaves and connected as shown in Figure 98 and Figure 99) before continuing to step 4. To prevent unnecessary alert messages due to LAN connectivity issues, configure a response timeout value between 2 and 20 seconds. This will be the amount of time that a slave must have lost connection before an alert message regarding connectivity will be sent. This will apply to all connected slaves.

Enter a unique value between 1-255 if "RS485 Slave" is selected.

(Each RS485 slave **must** have a different RS485 address.)

Otherwise, leave this blank.

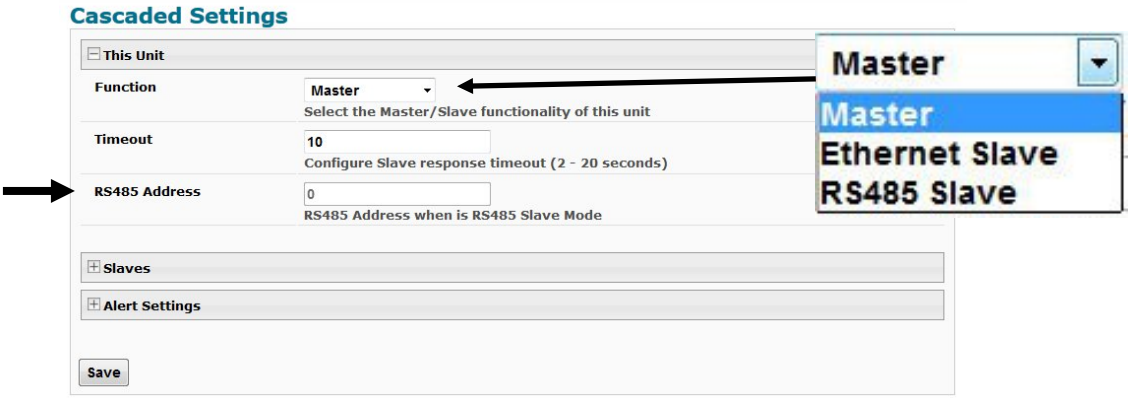


Figure 97- Cascade configuration options

2. Connect the RS485 slaves to the master as shown below using CAT5/5e/6 patch cables with RJ45 connectors wired straight thru (pin 1 to pin 1, pin 2 to pin 2, etc.). The maximum total distance from the master to the final slave unit cannot exceed 4000 feet. The last slave **must** have a terminating plug (E-TRMPLG-sold separately) in the empty socket.

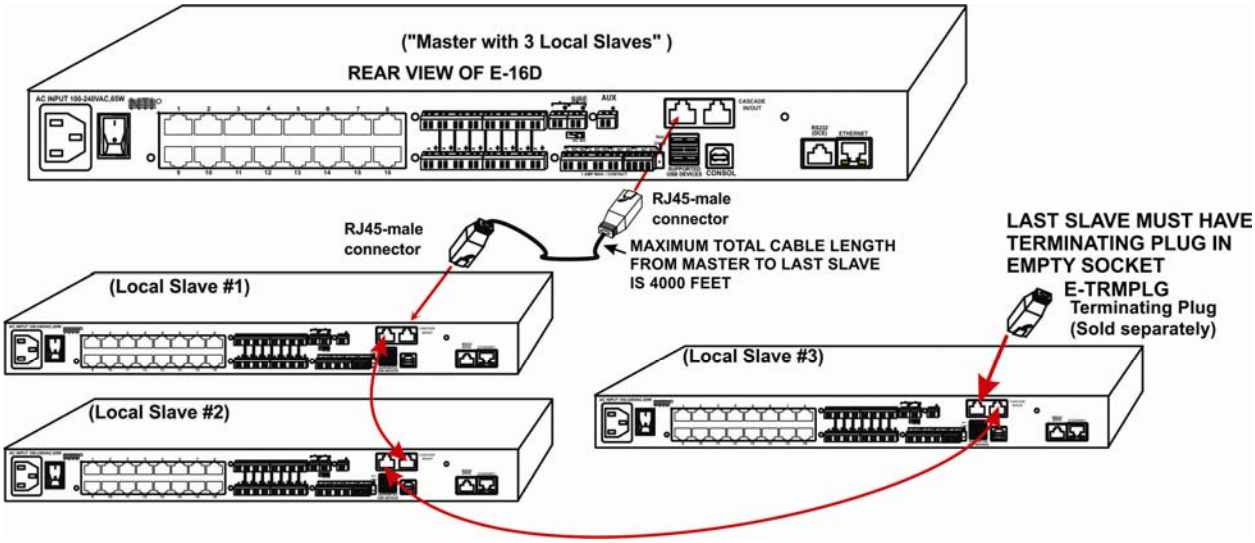


Figure 98- Master with local (RS485) slaves

3. Each ENVIROMUX unit configured as an Ethernet Slave must be given a unique IP address. Connection of an Ethernet Slave will be through its Ethernet connection alone. An Ethernet Slave can be located anywhere provided the Master Unit has access to it through equipment settings (routers, firewalls, etc.).

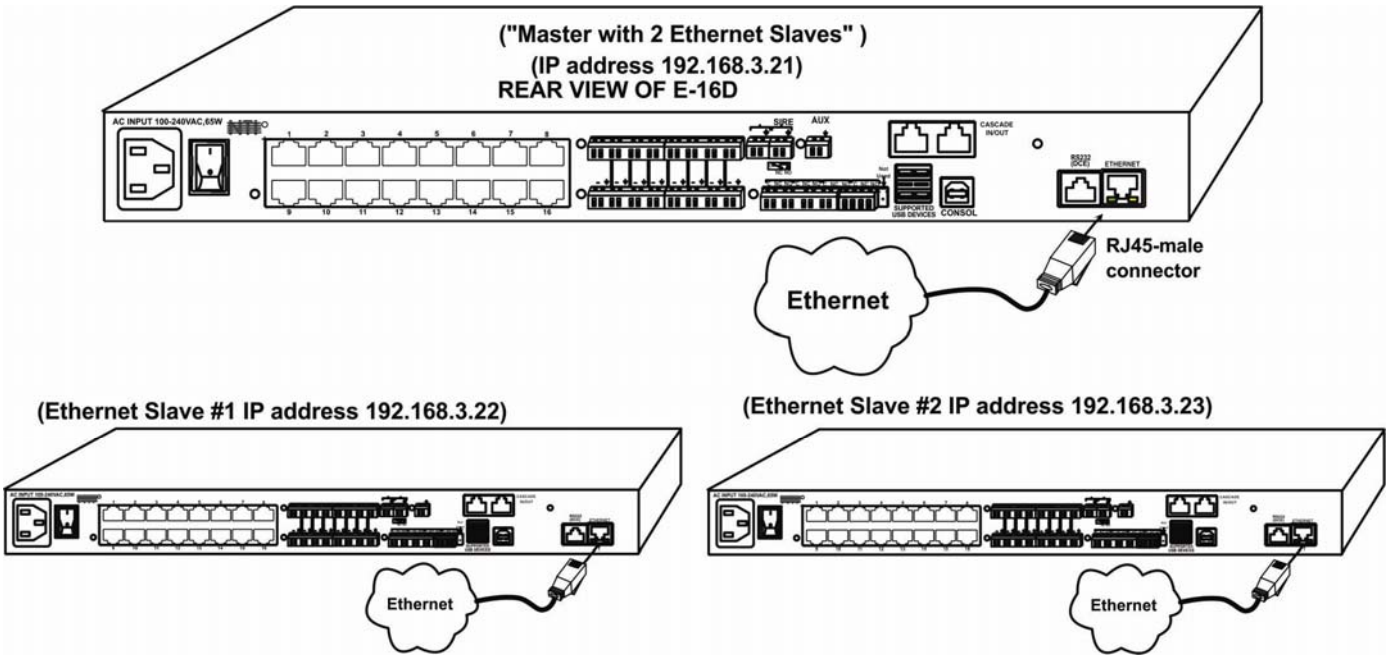


Figure 99- Cascade configuration with Ethernet slaves

4. From the Cascaded Settings page of the Master unit, enter a checkmark for each slave that will be present in the configuration. This enables the slave and defines the slave sequence (number 1-4) as it will appear on the sensor summary page.

5. Enter the type of Slave (Ethernet or RS485) to be connected at that sequence number.

6. Either enter the IP address of the Ethernet Slave, or the RS485 address of the RS485 slave.

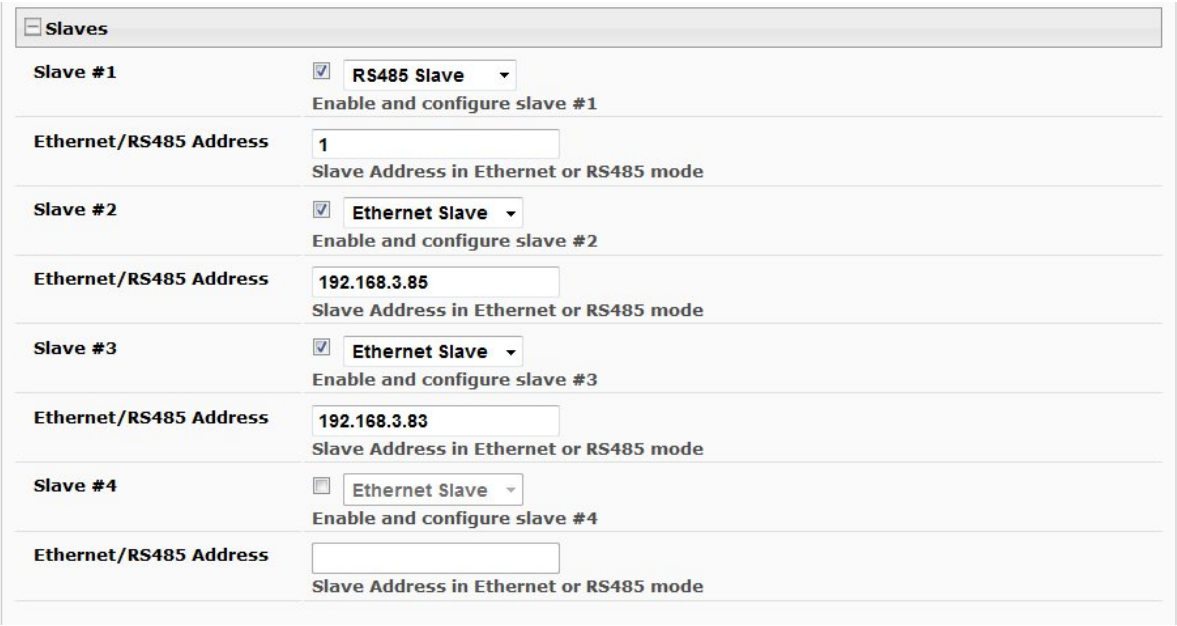


Figure 100- Configure which Slaves will be connected to the Master

7. In the web interface of the Master unit, configure the Alert Settings that will determine how the user will be alerted if any of the Slave units lose communication with the Master unit. This configuration is **only** performed in the Master unit.

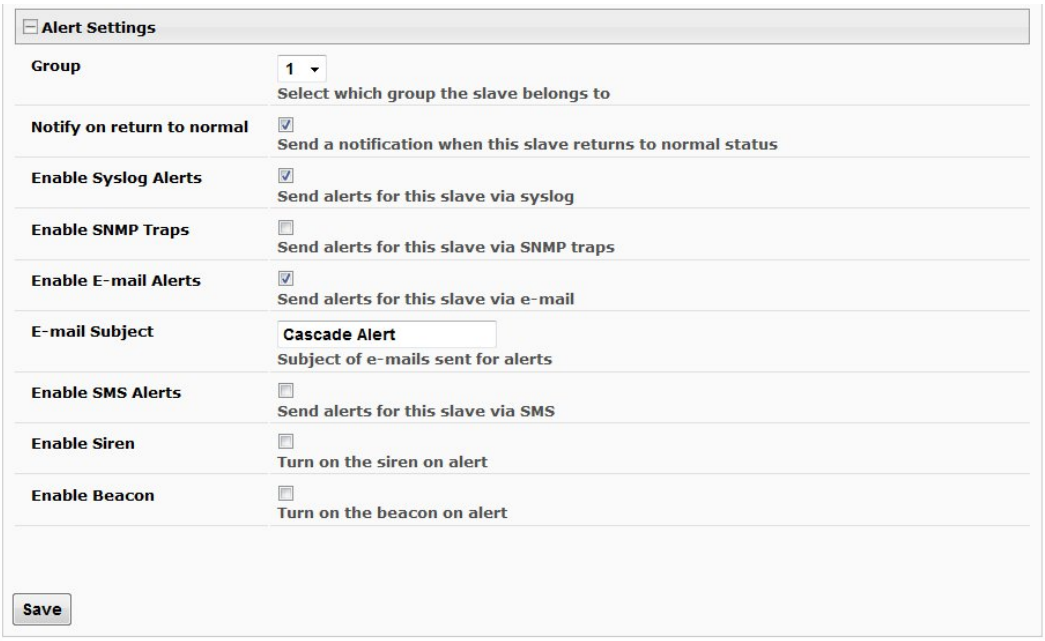


Figure 101- Apply alert settings to alert for Slave connection loss

Alert Settings	
Group	Just as sensors are assigned to a group, a Slave loss alert can be assigned to a group. In the event a Slave loses connection with the Master, for any reason, an alert notification will be sent to all users subscribing to alerts from this sensor group.
Notify on Return to Normal	The user can also be notified when the connection to a Slave has been restored by selecting the "***Notify when return to normal***" box.
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
Enable SMS Alerts	Place a checkmark in this box to have alert notifications sent via SMS messages (requires a modem)
Enable Siren	Turn ON the Master unit siren when a Slave connection is in an alert state
Enable Beacon	Turn ON the Master unit beacon when a Slave connection is in an alert state

Note: The Beacon and Siren connections of the Slave units are not used.

Be sure to click **Save** before exiting this page.

Note: The master and each slave must be power-cycled for changes to take effect.

8. Power-cycle each Slave unit and allow to fully boot up.
9. Power-cycle the Master unit

Sensors attached to the connected slaves will appear when viewing the Summary Page for the master (see Figure 102).

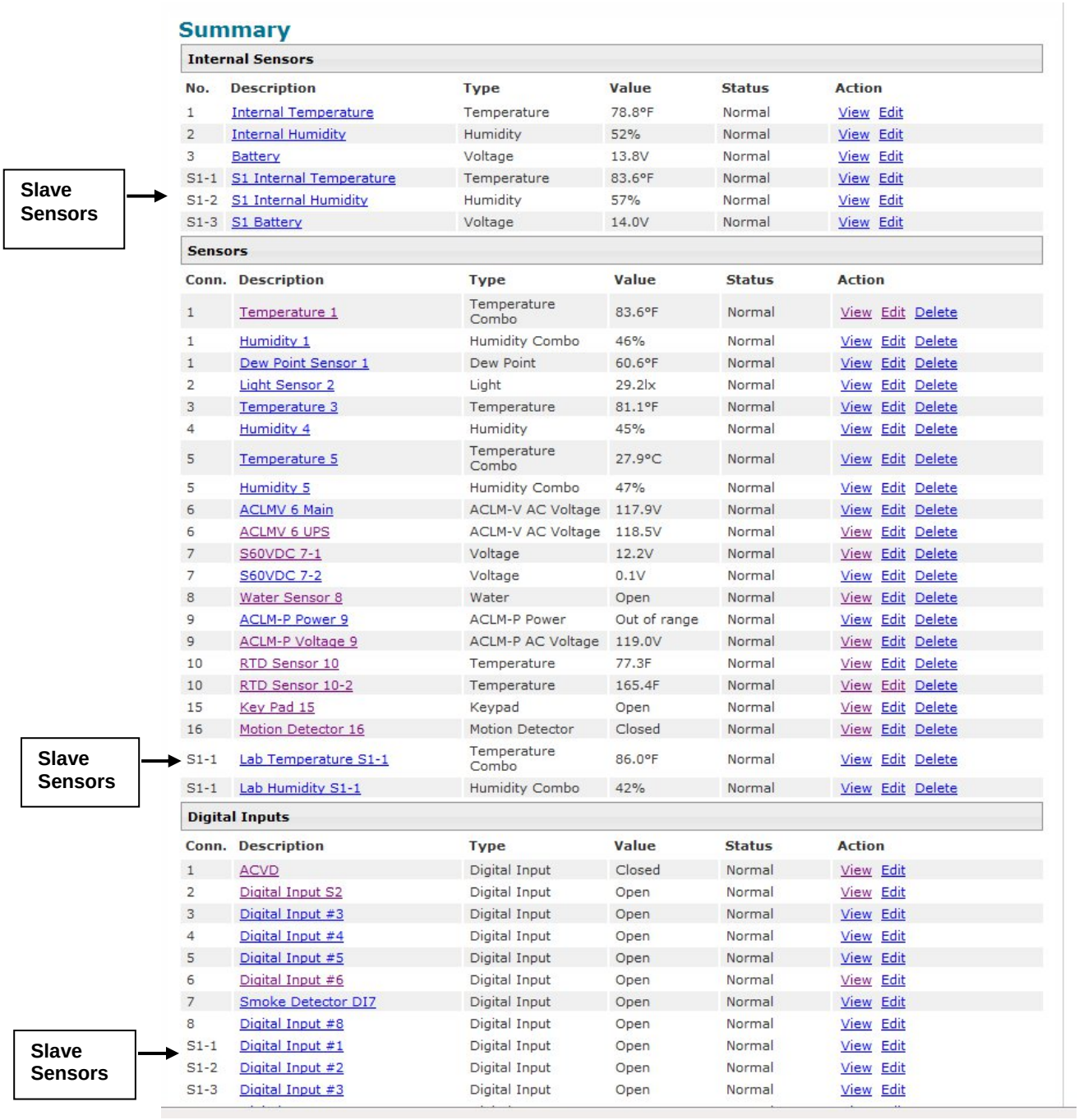
Note: Contact sensors wired to "RJ45 Sensor" ports and any sensor connected to "Digital Input" terminals must first be added to the sensor list from the web interface of the Slave unit before they can be monitored and configured from the Master unit.

If the ENVIROMUX in a cascade configuration is behind a firewall, be sure to open port 5919 so that it can communicate with other ENVIROMUXs.

Summary- Steps to Setup Cascading

1. Define whether the unit will be the Master, an Ethernet Slave or an RS485 slave.
2. Assign unique IP addresses to Ethernet Slaves
3. Assign unique RS485 addresses to RS485 slaves and connect to Master unit with CAT5 cable. Don't forget to install the terminating plug!
4. Configure Master unit to communicate with each Slave unit (Figure 100).
5. Configure alert settings for cascaded slaves (in Master unit only) to alert user(s) when connection to any slave is lost and restored.
6. Power-cycle each Slave, allow them to fully boot up, then power-cycle the Master unit.
7. Configure sensors of all units (Master and Slaves) as desired from the web interface of the Master unit.

Note: Contact sensors wired to "RJ45 Sensor" ports and any sensor connected to "Digital Input" terminals must first be added to the sensor list from the web interface of the Slave unit before they can be monitored and configured from the Master unit.



Summary

Internal Sensors

No.	Description	Type	Value	Status	Action
1	Internal Temperature	Temperature	78.8°F	Normal	View Edit
2	Internal Humidity	Humidity	52%	Normal	View Edit
3	Battery	Voltage	13.8V	Normal	View Edit
S1-1	S1 Internal Temperature	Temperature	83.6°F	Normal	View Edit
S1-2	S1 Internal Humidity	Humidity	57%	Normal	View Edit
S1-3	S1 Battery	Voltage	14.0V	Normal	View Edit

Sensors

Conn.	Description	Type	Value	Status	Action
1	Temperature 1	Temperature Combo	83.6°F	Normal	View Edit Delete
1	Humidity 1	Humidity Combo	46%	Normal	View Edit Delete
1	Dew Point Sensor 1	Dew Point	60.6°F	Normal	View Edit Delete
2	Light Sensor 2	Light	29.2lx	Normal	View Edit Delete
3	Temperature 3	Temperature	81.1°F	Normal	View Edit Delete
4	Humidity 4	Humidity	45%	Normal	View Edit Delete
5	Temperature 5	Temperature Combo	27.9°C	Normal	View Edit Delete
5	Humidity 5	Humidity Combo	47%	Normal	View Edit Delete
6	ACLMV 6 Main	ACLM-V AC Voltage	117.9V	Normal	View Edit Delete
6	ACLMV 6 UPS	ACLM-V AC Voltage	118.5V	Normal	View Edit Delete
7	S60VDC 7-1	Voltage	12.2V	Normal	View Edit Delete
7	S60VDC 7-2	Voltage	0.1V	Normal	View Edit Delete
8	Water Sensor 8	Water	Open	Normal	View Edit Delete
9	ACLM-P Power 9	ACLM-P Power	Out of range	Normal	View Edit Delete
9	ACLM-P Voltage 9	ACLM-P AC Voltage	119.0V	Normal	View Edit Delete
10	RTD Sensor 10	Temperature	77.3F	Normal	View Edit Delete
10	RTD Sensor 10-2	Temperature	165.4F	Normal	View Edit Delete
15	Key Pad 15	Keypad	Open	Normal	View Edit Delete
16	Motion Detector 16	Motion Detector	Closed	Normal	View Edit Delete
S1-1	Lab Temperature S1-1	Temperature Combo	86.0°F	Normal	View Edit Delete
S1-1	Lab Humidity S1-1	Humidity Combo	42%	Normal	View Edit Delete

Digital Inputs

Conn.	Description	Type	Value	Status	Action
1	ACVD	Digital Input	Closed	Normal	View Edit
2	Digital Input S2	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
6	Digital Input #6	Digital Input	Open	Normal	View Edit
7	Smoke Detector DI7	Digital Input	Open	Normal	View Edit
8	Digital Input #8	Digital Input	Open	Normal	View Edit
S1-1	Digital Input #1	Digital Input	Open	Normal	View Edit
S1-2	Digital Input #2	Digital Input	Open	Normal	View Edit
S1-3	Digital Input #3	Digital Input	Open	Normal	View Edit

Figure 102- Portion of Summary Page from a Master with a Slave

From the Summary page of the Master (above), sensors connected to Slave unit can be viewed and configured just as if they were directly connected to the Master unit itself.

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. Any configuration changes that were made prior to this action will be made active.

Figure 103- Reboot System page

The message "System is rebooting, please wait..... " will appear and after approximately 45-60 seconds the login screen will appear.

Log in to resume activity.

Figure 104- System is rebooting

Note: In the event of a power failure, using REBOOT will cause the ENVIROMUX to shut OFF.

Click on the "Reboot Now" button to shut down the ENVIROMUX in the event of a power failure or use the System Reset button on the front of the ENVIROMUX. During a power failure, this will be the only way the ENVIROMUX can be shut OFF. **The battery backup will power the ENVIROMUX for up to 1 hour.**

The power switch will only shut down the ENVIROMUX during normal operation. If the power switch is not shut OFF during a power failure, when AC power has been restored the ENVIROMUX will power ON automatically.

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 36.

Assorted conditions can produce configurable events (up to 50) that can then be used in numerous scenarios to produce Smart Alert messages (up to 20) that are sent to users. In addition, the already configured alert status of any sensor or group of sensors can be used to trigger Smart Alerts.

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 36 will be managed separately from events logged by these user-defined Events. Sensor configuration for these Events will have no impact on the general configuration of your sensors. User-defined Events provide more control over what you want to be notified of.

For example, if an IP camera is located just inside a monitored entranceway, and an image is desired of each person that goes through that entrance, it may be difficult to get the image consistently since people move at different rates of speed. Using multiple events triggered by the same sensor, each having the Event Delay configured for a different time period and/or a different camera to take the image, you can use Events to be assured of taking a snapshot of the person entering/leaving.

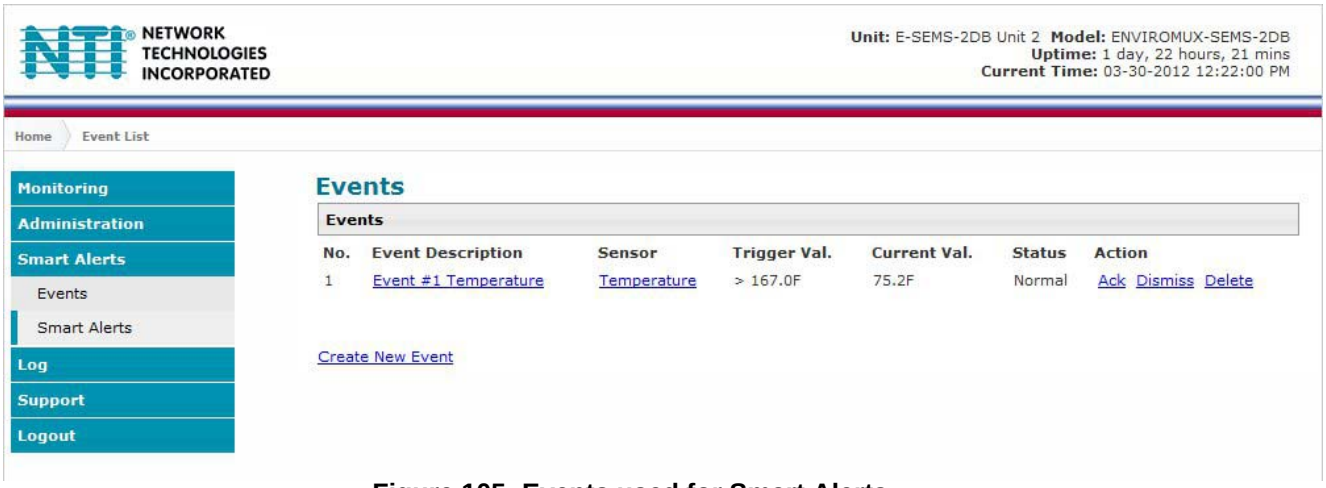


Figure 105- Events used for Smart Alerts

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

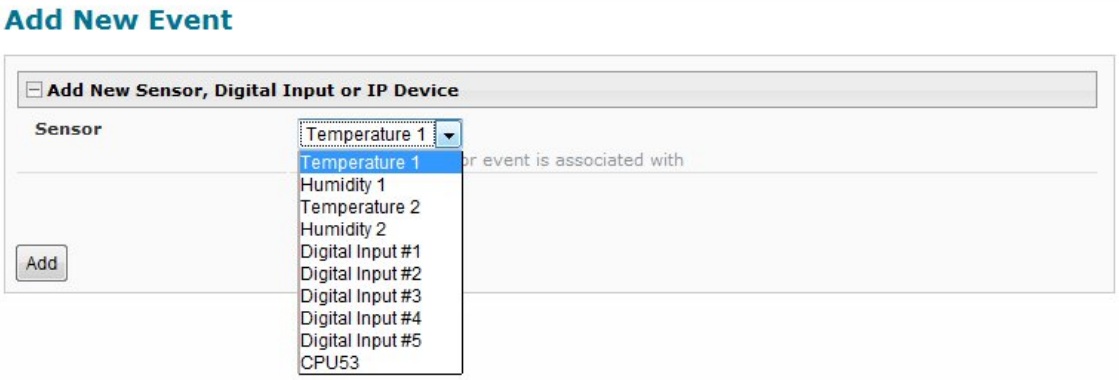


Figure 106- Sensor to be used for a predefined event

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 the sensor is selected, click “Add”.

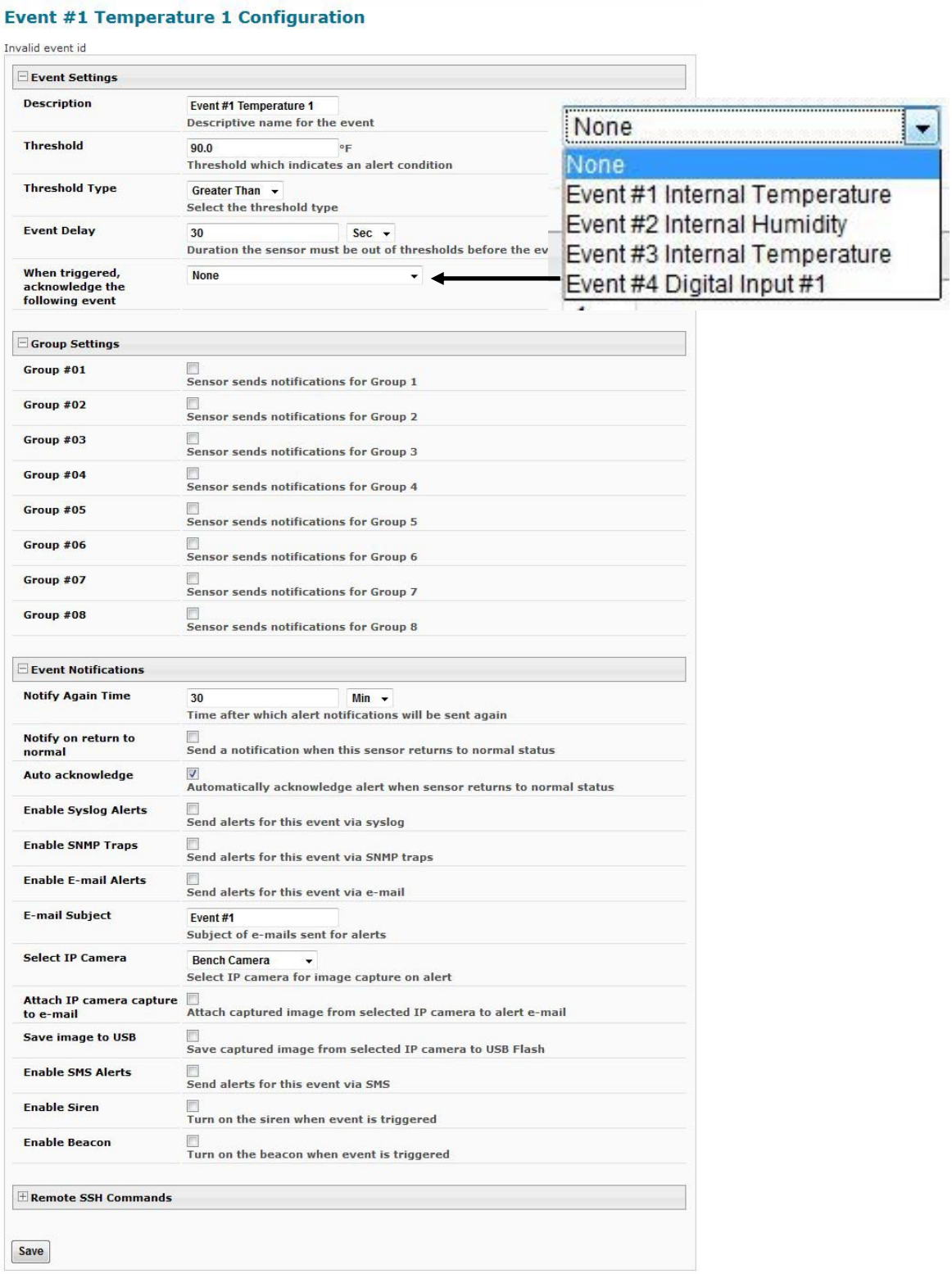


Figure 107- Configuration options for new event

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 90.0 degrees C for more than 30 seconds, an 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
Group Settings	
Group#xx	Assign the Event to any group 1 -8 (see also page 42)
Event Notifications	
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.
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
Select IP Camera	Associate an Event with an IP camera. Select an IP camera from the drop-down box.
Attach IP Camera capture to email	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 58) 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.***
Save image to USB	Save the image captured by the IP camera to a connected USB Flash Drive
Enable SMS Alerts	Place a checkmark in this box to have alert notifications sent via SMS messages (requires a modem)
Enable Siren	Turn ON the siren when this event goes to alert (E-16D only)
Enable Beacon	Turn ON the beacon when this event goes to alert (E-16D only)

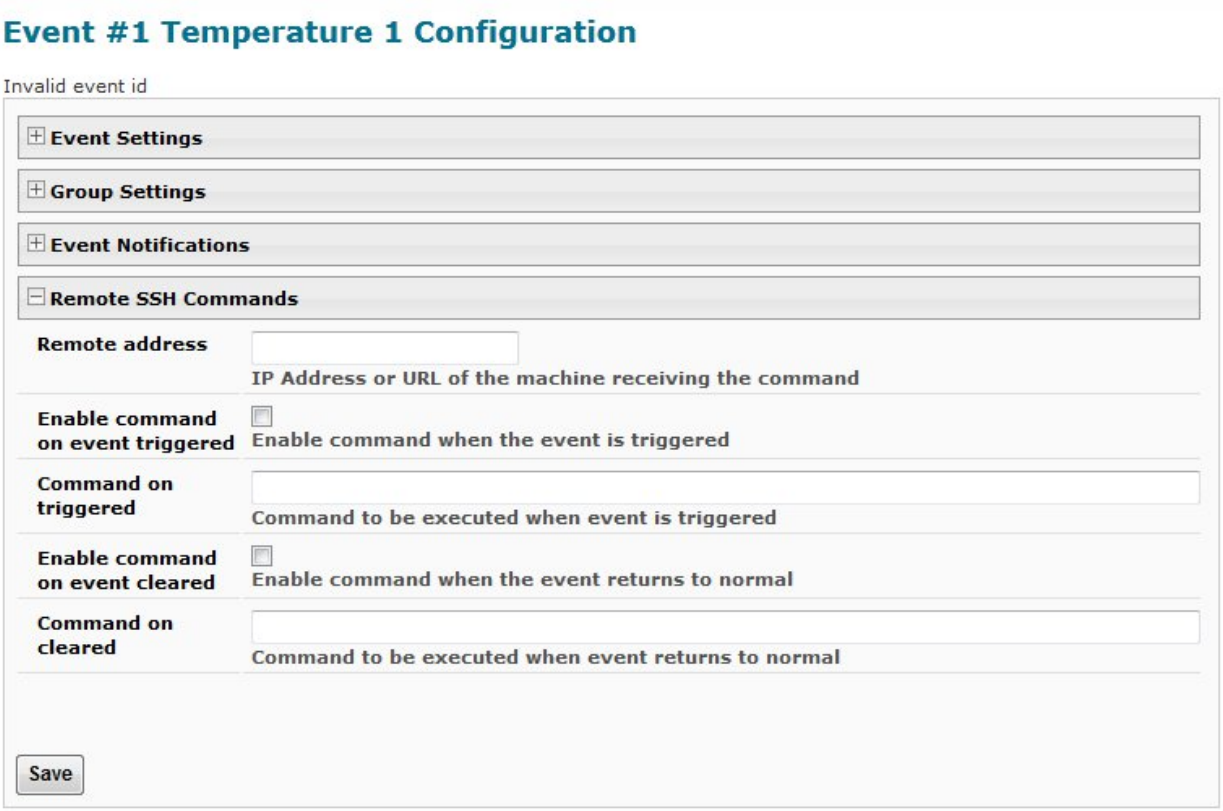


Figure 108- Event Configuration options continued

Remote SSH Commands	
Remote address	Enter the IP address or host name of the Linux or Unix computer to be sent a command via an SSH connection.
Enable command on event triggered	Place a checkmark here to send a command when this Event is triggered
Command on triggered	Enter an SSH command to be sent to the remote address when this Event is triggered (examples of commands include "**poweroff**" and "**reboot**")
Enable command on event cleared	Place a checkmark in this box to send a command when this Event is cleared
Command on cleared	Enter an SSH command to be sent to the remote address when this Event is cleared

After all options are selected, click the "Save" button. This Event will now be added to the Events page (Figure 105). 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. Smart Alerts can also be triggered by combinations of basic sensor alerts without having to provide specific Event configurations.

More on Remote SSH Commands

There are also some things that need to be done on the computer side to accept the commands sent by the ENVIROMUX.

1. The computer needs to have an SSH server installed and running. It needs to accept connection as "root". (On some installations of Linux the "root" connection may be disabled by default.)
2. The SSH connection will be done without a password as it uses authentication keys. To install the authentication key of E-xD on the computer, download that key from the Administration->System->RSA Public key page (see page 62), on the computer to take the command. The downloaded file will have the default name **`id_rsa.pub`**.
3. On the computer to take the command, logged in as root, from the directory where the file was downloaded, type the command:

$ **`cat id_rsa.pub >> root/.ssh/authorized_keys`**

Then, to make the change take effect, restart the SSH server by typing:

$ **`sudo service ssh restart`**

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

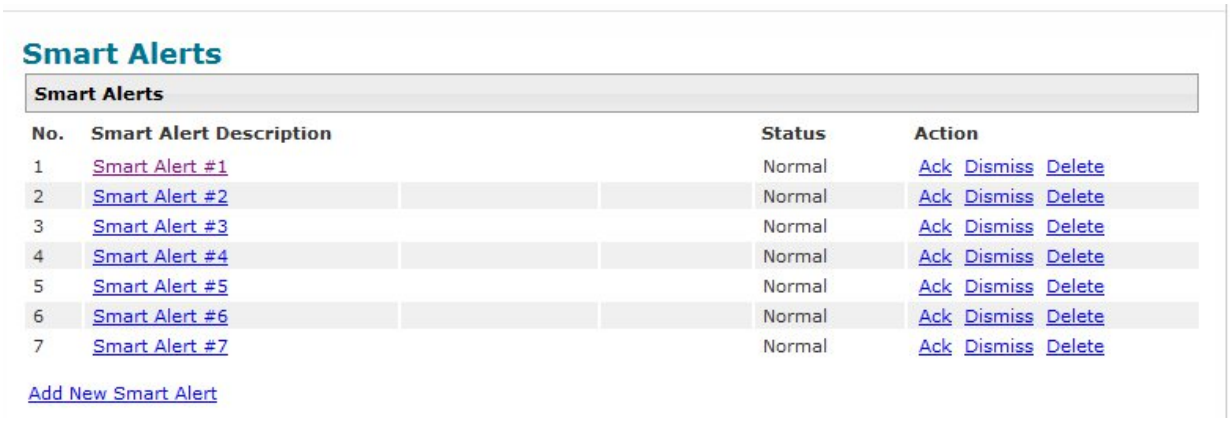


Figure 109- Smart Alert summary page

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 and/or to use simple sensor alerts to configure Smart Alerts.

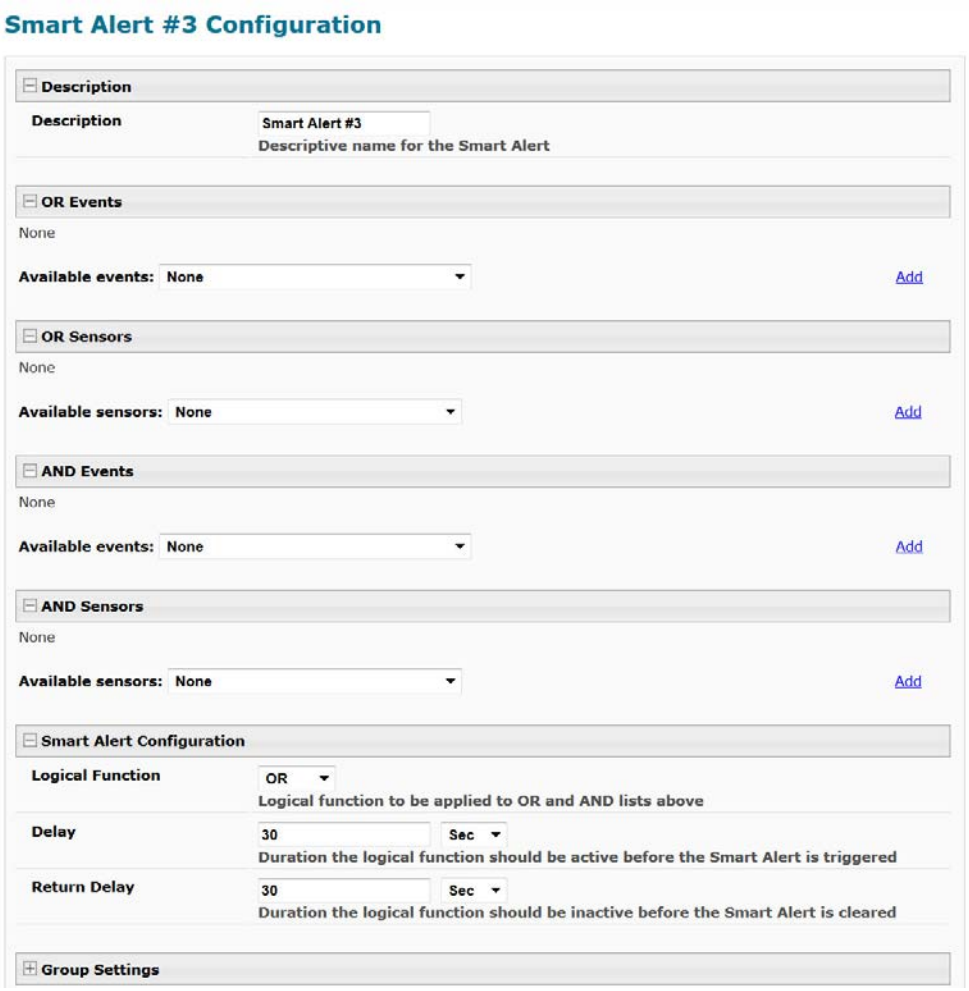


Figure 110- Smart Alert configuration

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 105) to have OR logic applied to a triggered Event
OR Sensors	
Available Sensors	Select from any configured sensors to have OR logic applied to a triggered sensor alert. No other sensor configuration necessary.
AND Events	
Available Events	Select from the predefined available Events (Figure 105) to have AND logic applied to a triggered Event
AND Sensors	
Available Sensors	Select from any configured sensors to have AND logic applied to a triggered sensor alert. No other sensor configuration necessary.
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.
Return Delay	The amount of time the Smart Alert Event status must have returned to normal condition before a Smart Alert message is cleared. The Delay value can be set for 0-999 seconds or minutes.
Group Settings	
Group#xx	Assign the Smart Alert to any group 1 -8 (see also page 42)

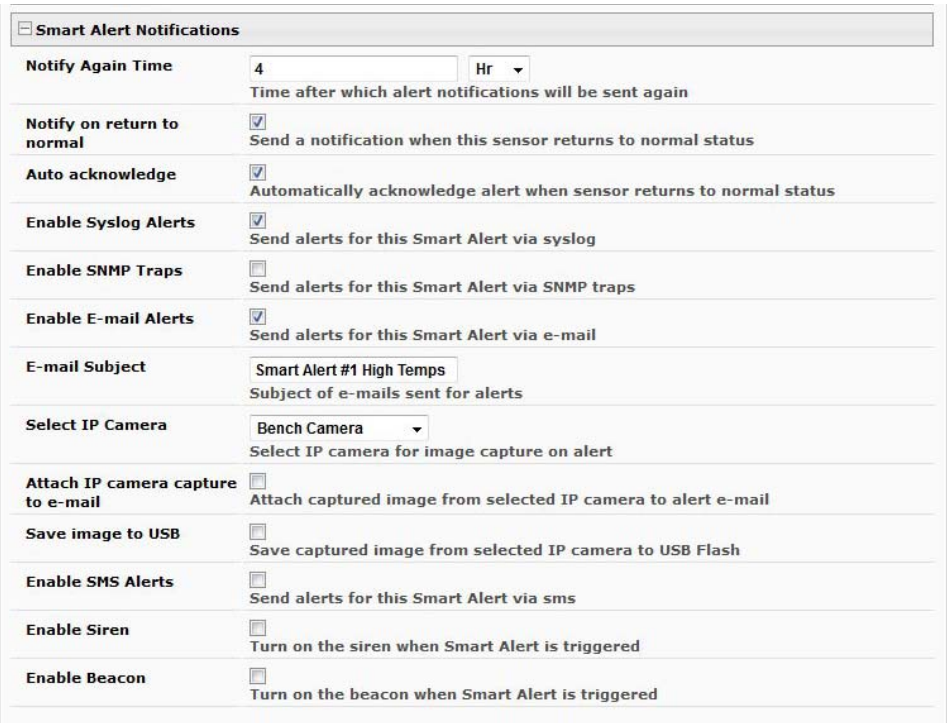


Figure 111- Smart Alert configuration- continued

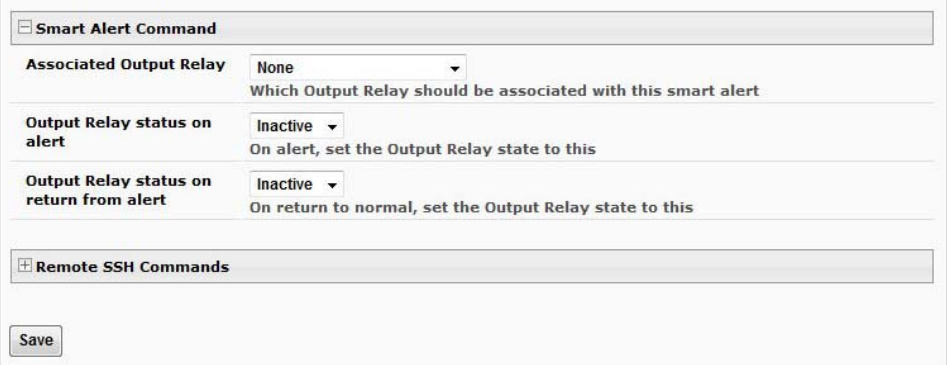


Figure 112- Smart Alert configuration- continued

Smart Alert Notifications	
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
Select IP Camera	Associate an Event with an IP camera. Select an IP camera from the drop-down box.
Attach IP Camera capture to email	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 58) 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.***
Save image to USB	Save the image captured by the IP camera to a connected USB Flash Drive
Enable SMS Alerts	Place a checkmark in this box to have alert notifications sent via SMS messages (requires a modem)
Enable Siren	Turn ON the siren when this event goes to alert (E-16D only)
Enable Beacon	Turn ON the beacon when this event goes to alert (E-16D only)
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

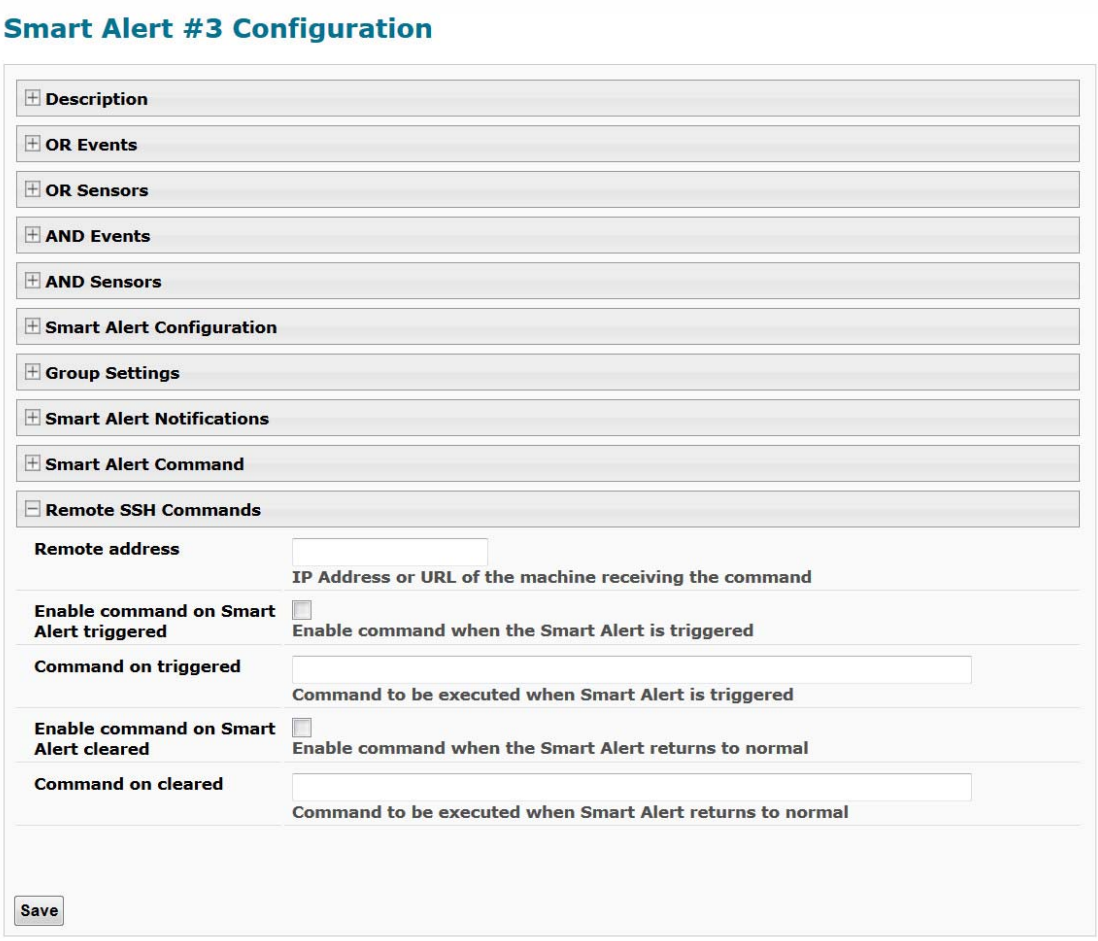


Figure 113- Smart Alert Configuration- continued

Remote SSH Commands	
Remote address	Enter the IP address or host name of the Linux or Unix computer to be sent a command via an SSH connection.
Enable command on event triggered	Place a checkmark here to send a command when this Smart Alert is triggered
Command on triggered	Enter an SSH command to be sent to the remote address when this Smart Alert is triggered (examples of commands include "**poweroff**" and "**reboot**")
Enable command on event cleared	Place a checkmark in this box to send a command when this Smart Alert returns to normal
Command on cleared	Enter an SSH command to be sent to the remote address when this Smart Alert returns to normal

After all options are selected, click the "**Save**" button. This Event will now be added to the Events page (Figure 105). 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.

The Unix or Linux machine to receive the commands must be configured to receive them before these commands will work. See "**More on SSH Commands**" on page 97 for instruction to setup the Unix or Linux machine.

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.

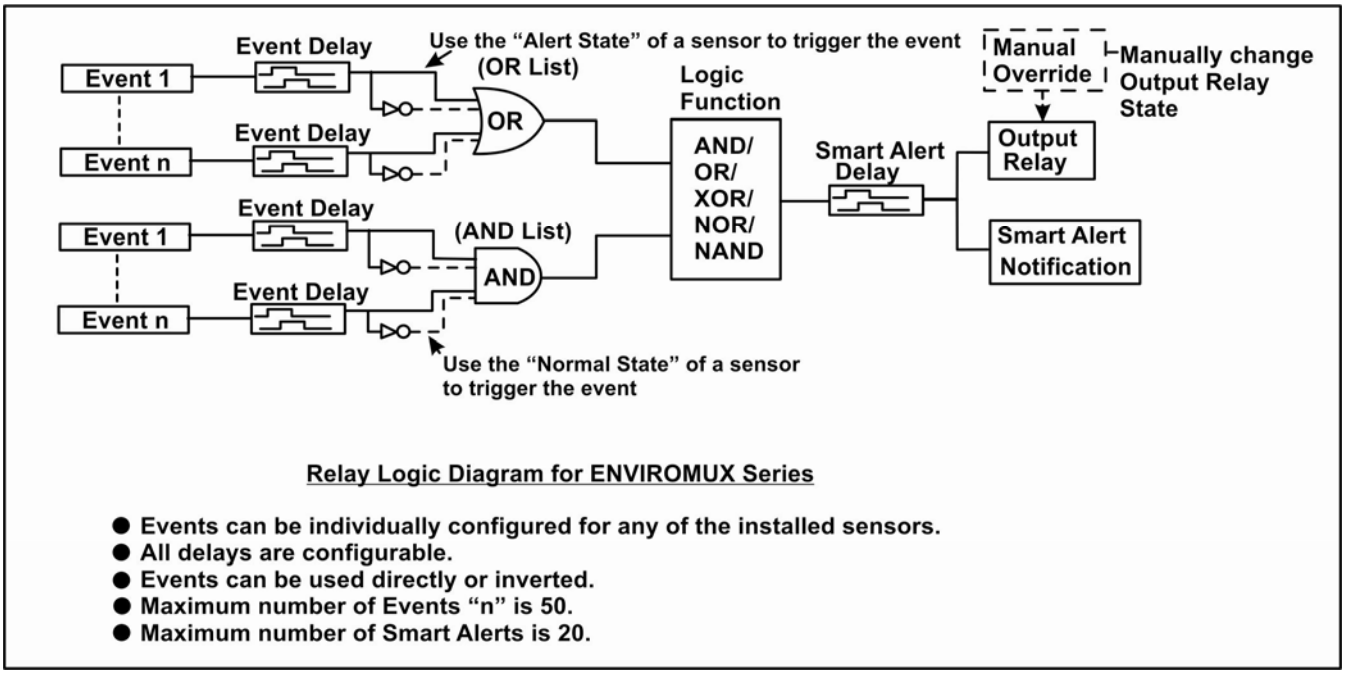


Figure 114- Event Logical Function Diagram

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.

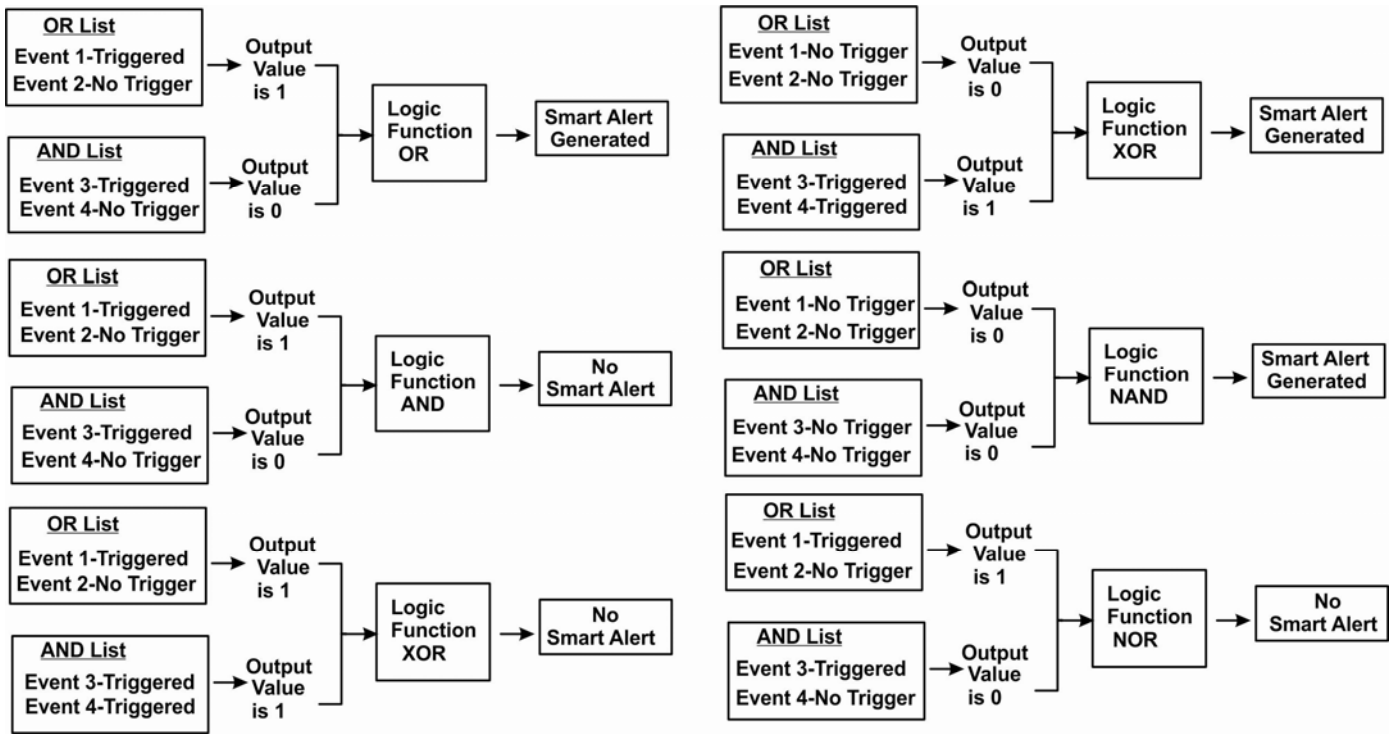
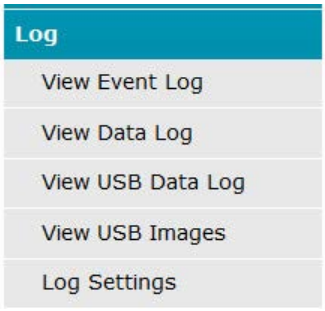


Figure 115- Examples of Smart Alert conditions

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
View USB Data Log	View data readings that have been saved to a connected USB flash drive- Up to 1000 files will be displayed.
View USB Images	View images that have been saved on a connected USB flash drive- A list of up to 1000 jpg images will be displayed
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

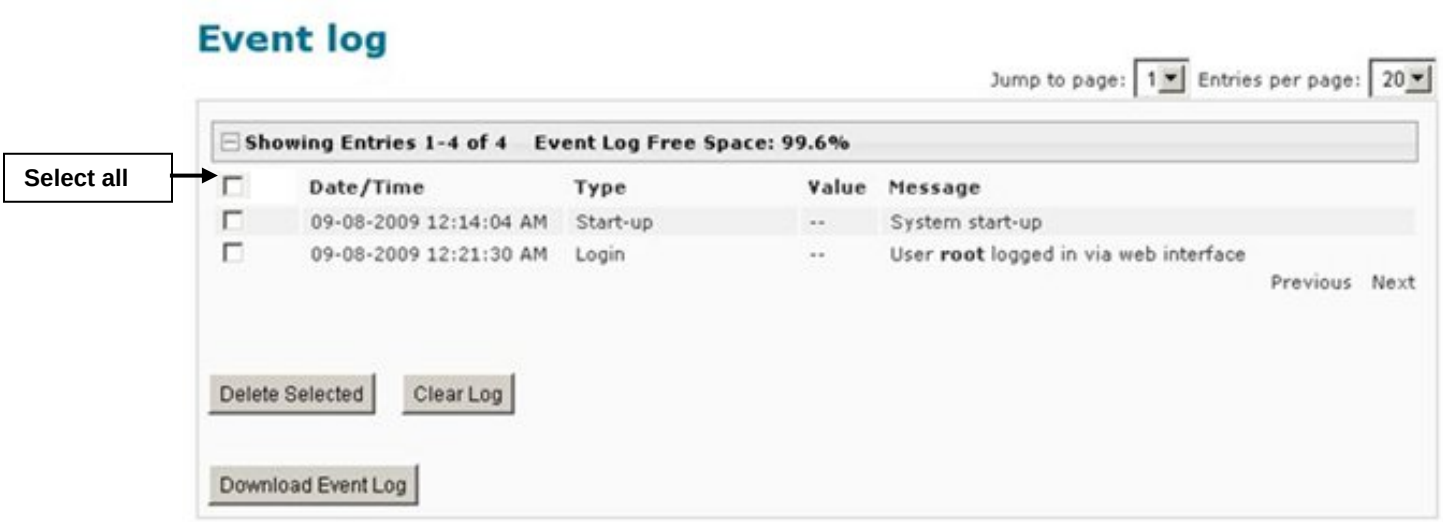


Figure 116- Event Log page

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.

Example of an Event Log Message:

TIME: 07-27-2012 02:15:44 AM
ENTERPRISE: E-16D Unit 1
LOCATION: Engineering
BRANCH: RACK: CONTACT: NTI
DESCRIPTION: Temperature 1
CONNECTOR: 1
TYPE: Temperature
MESSAGE: Sensor value crossed over non-critical thresholds
VALUE: 85.0F

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.

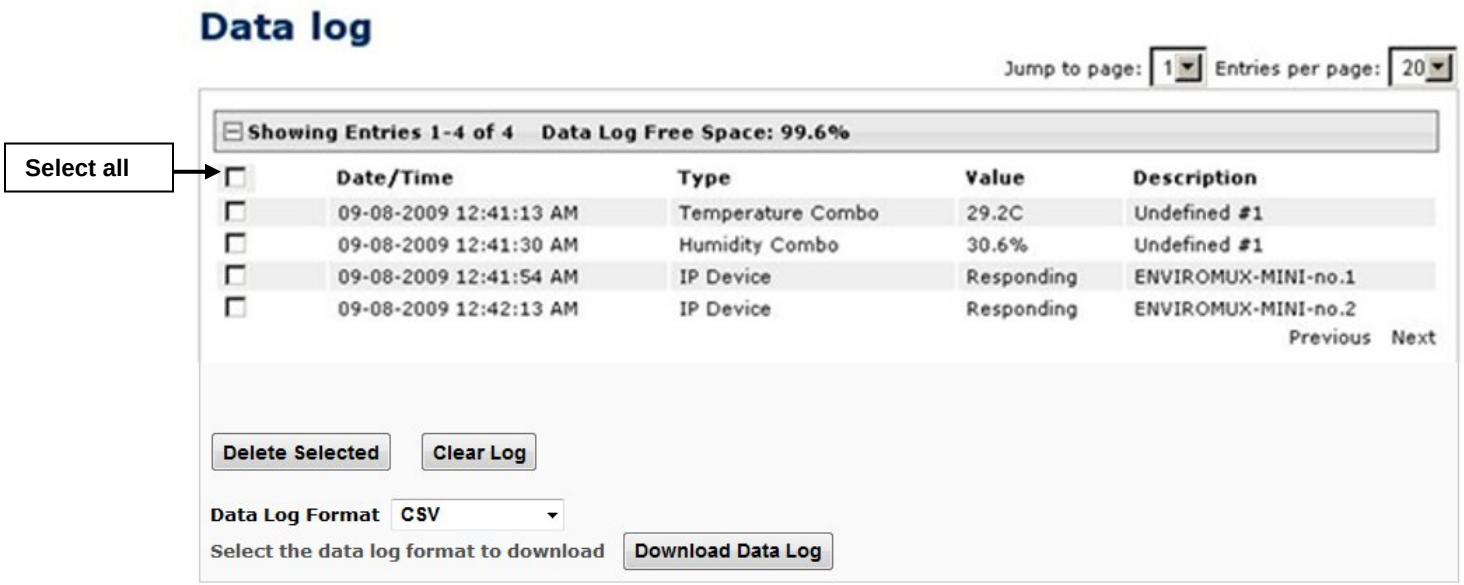


Figure 117- Data Log page

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. Choose the **Data Log Format** (CSV or Tab Delimited), then press **Download Data Log** to save the log file before clearing it.

Example of a Data Log Message:

TIME: 07-27-2012 09:12:28 AM
ENTERPRISE: E-16D Unit 1
LOCATION: Engineering
BRANCH: Bldg. B

RACK: IPMI
DESCRIPTION: ACLMV 6 Main
TIME:07-27-2012 09:12:28 AM
TYPE: ACLM-V AC Voltage 1
VALUE:115.5V

View USB Data Log

If any Data Logs have been saved to the USB flash drive connected to a USB port on the ENVIROMUX, a list of those logs can be viewed and opened for review.

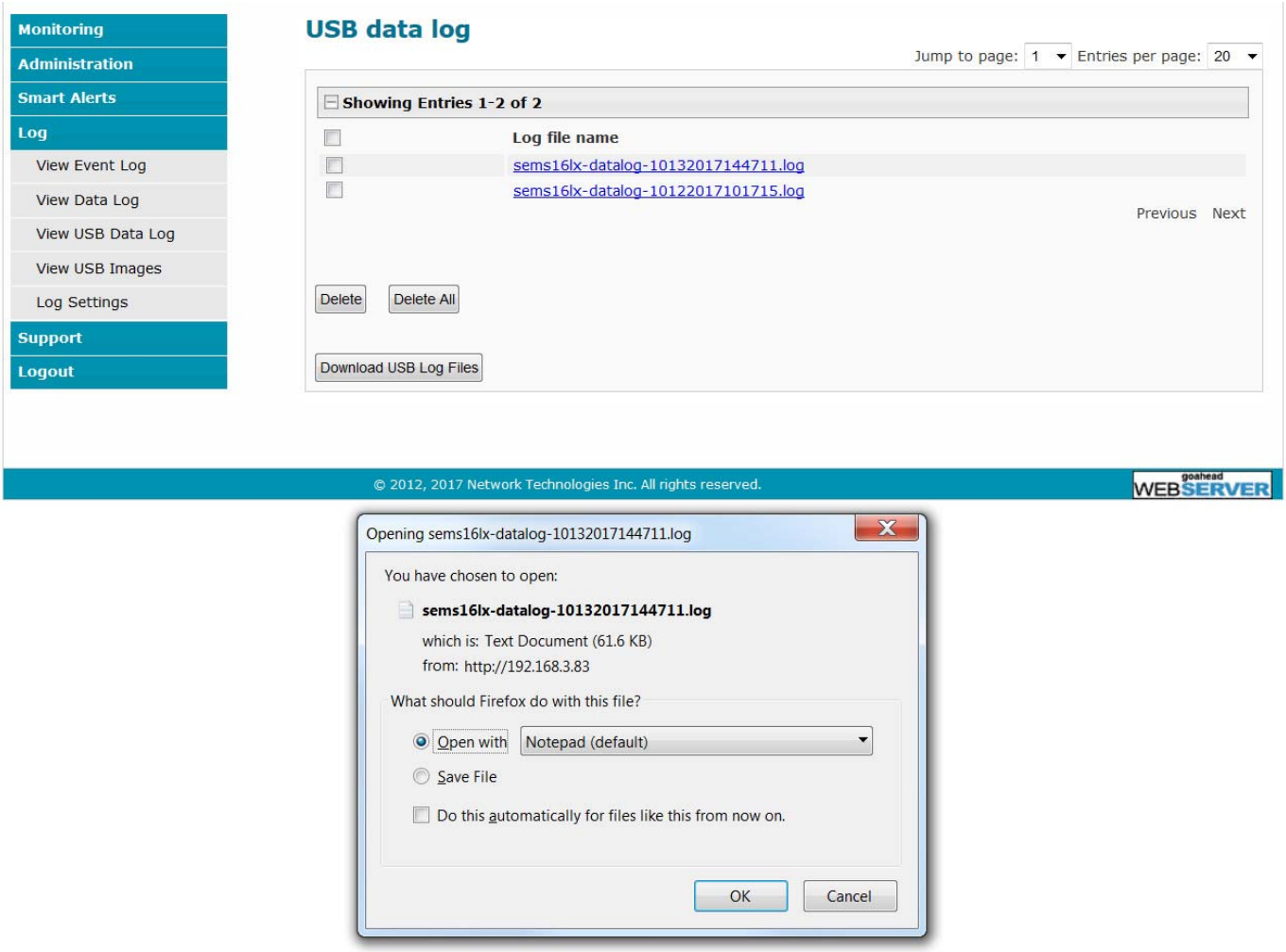


Figure 118- View Saved USB Data Log

View USB Images

If any IP camera images have been saved to the USB flash drive connected to the ENVIROMUX, a list of those images, up to 20 at a time, will be displayed. Click on an image to view it.

To delete specific images from the flash drive, place a checkmark in the box on the left side and click "Delete Selected", or, to erase them all select "Delete All".

To open more than one image sequentially or download them as a group, place a checkmark in several images and select "Download JPG Images". You will be prompted to either open the images or download them to your PC.

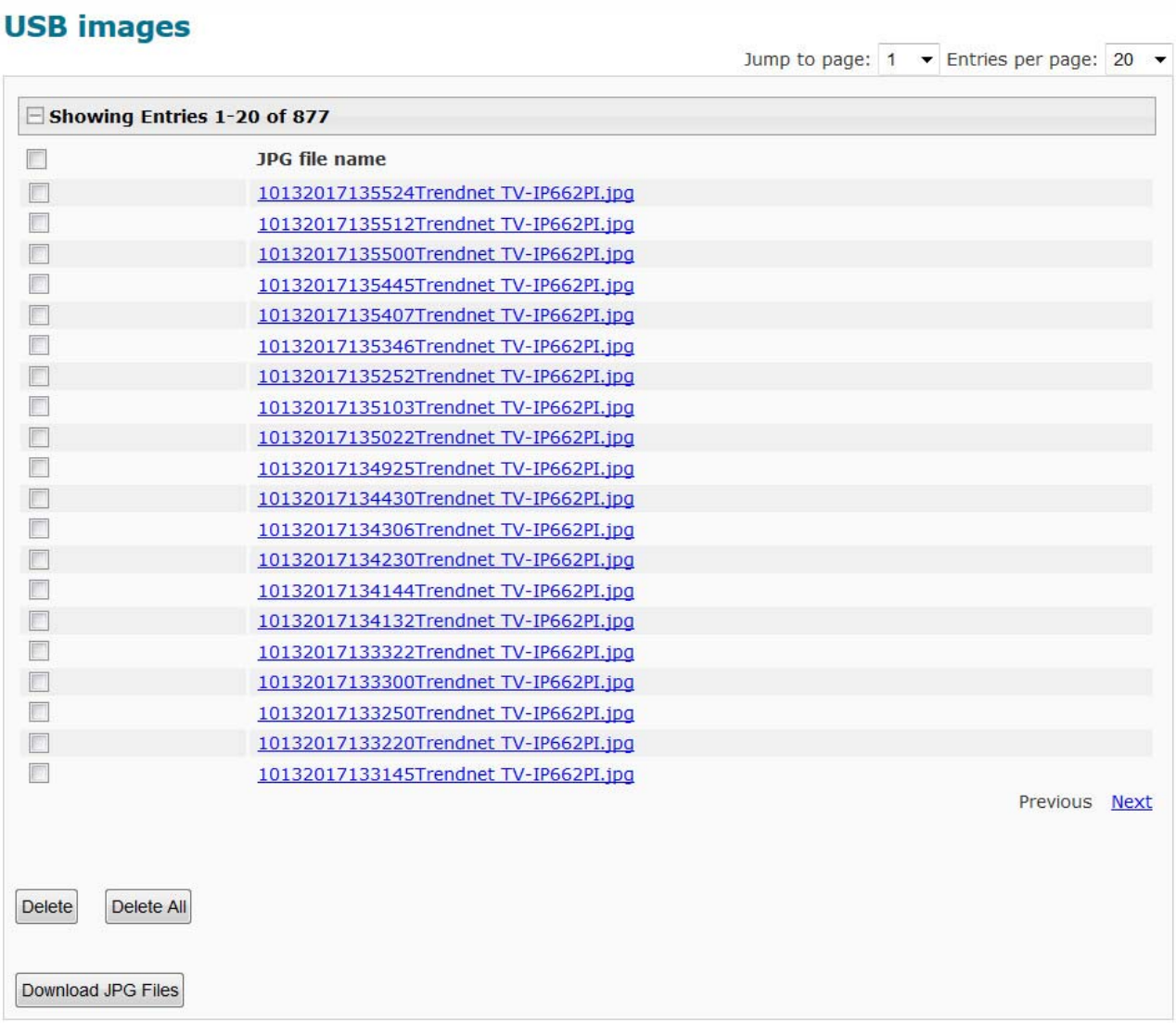


Figure 119- View Images saved on USB Flash Drive

Log Settings

The Log Settings page (Figure 120) 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)
- Alert: 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
- Debug: shows more frequent and detailed errors however the log will fill up much more rapidly

Log can be assigned to multiple groups and any user that receives messages from those groups 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, SMS 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, SMS and/or SNMP traps to users in addition to the entries it records internally. Enable Remote Logging for email, syslog, or SNMP as desired.

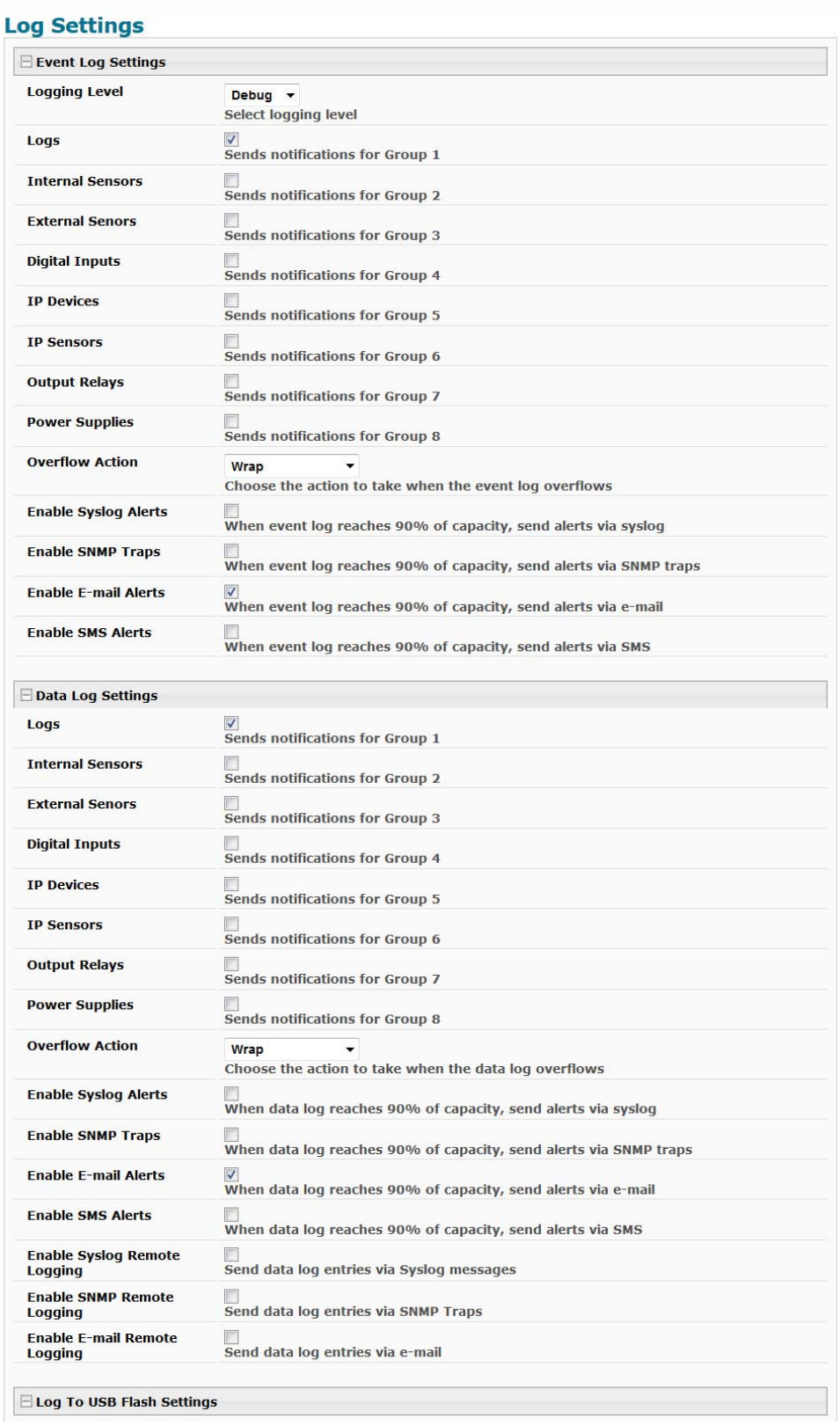


Figure 120- Log Settings page

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 (it doesn't matter which of the 4 ports it is plugged-into), 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, first connect a flash drive to an available USB port on the ENVIROMUX. Then change "Unmount" to "Mount" and click "Save". Then place a checkmark in the "Enable Log to Flash drive" box and click "Save" again.

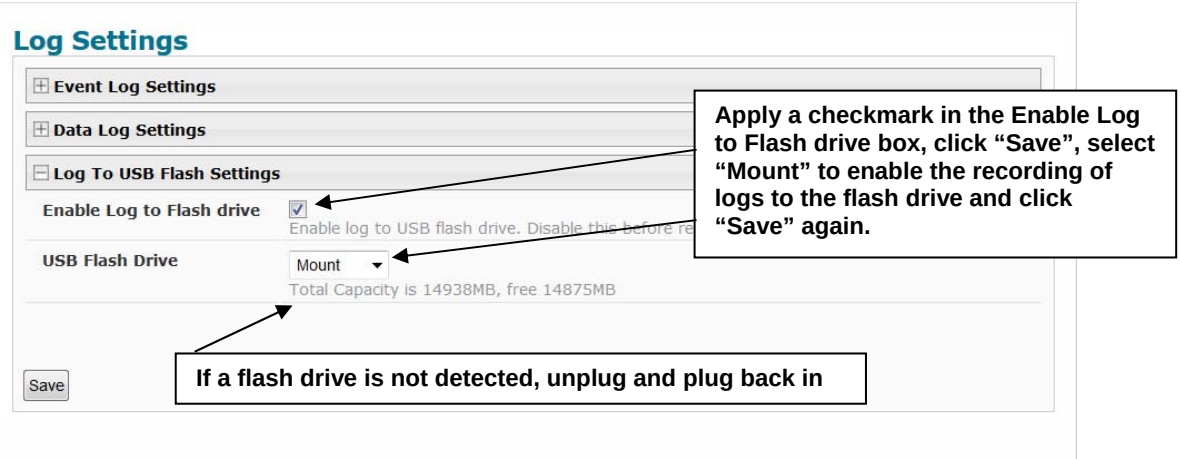


Figure 121- Mount a USB Flash Drive

Note: Only 1 flash drive can be connected to the ENVIROMUX at a time.

Note: If the "Overflow Action" under Data Log Settings is set to "Discontinue Log", then logging to the flash drive will also be stopped when the data log has reached capacity.

Note: The file system of the flash drive must be formatted FAT32 (not NTFS). Make sure there is plenty of space on it.

To remove a flash drive from the ENVIROMUX,

1. Uncheck "Enable Log to Flash drive" and click "Save",
2. Change "Mount" to "Unmount".
3. Click "Save" again. Now it is safe to remove the flash drive.

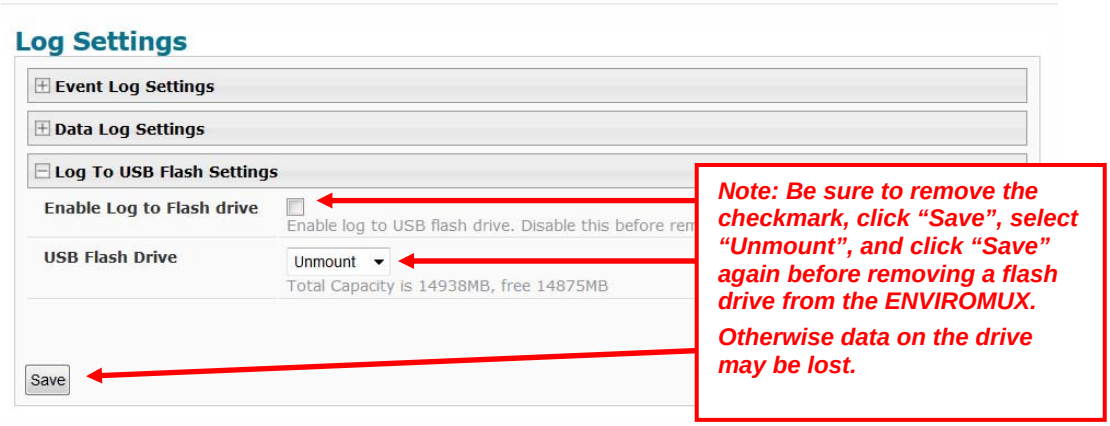


Figure 122- Steps to unmount a flashdrive

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.

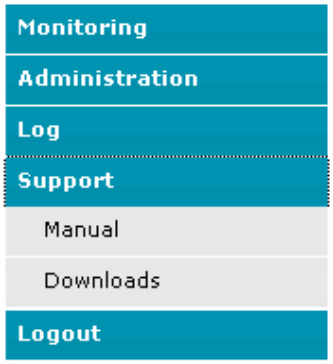


Figure 123- Support

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.

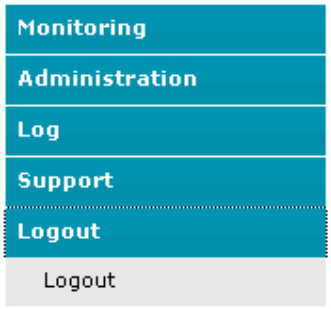


Figure 124- Logout

FRONT PANEL CONTROLS AND LED INDICATORS

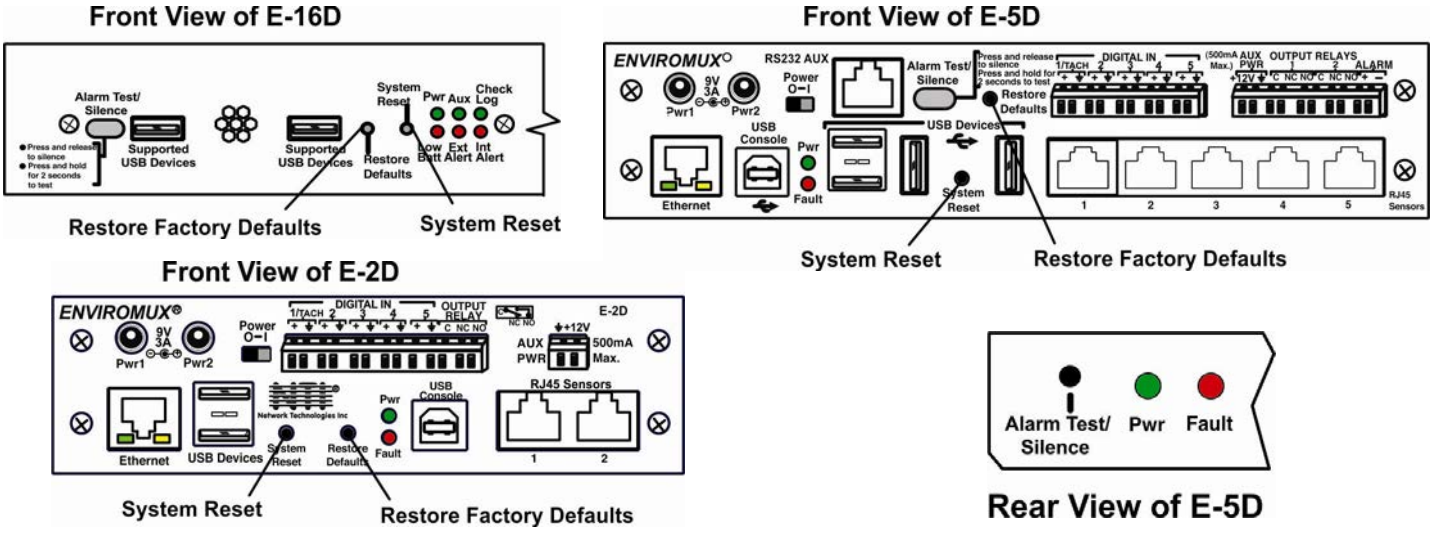


Figure 125- Front panel

Front Panel LED Status Chart

LED Label	Status	Meaning
Pwr	OFF	No Power
	Solid ON	AC Power is ON
	Blinking slowly (once /second)	AC Power has failed, Battery backup (pg. 112) is ON (The LED will not blink if the unit is powered OFF by the switch.)
	Blinking rapidly	Discovery Tool (pg. 28) is in use and communicating with the ENVIROMUX
Low Batt	OFF	Battery is OK, AC power is ON
	Solid ON	Battery is below 12V and charging (no action required)
	Blinking	Battery has been disconnected (battery is below 10.7V), requires attention, contact NTI
Check Log	OFF	No new messages in Data Log since last viewing
	ON	New message in Data Log-not an alert
Int Alert	OFF	No new alert message in Event Log re: internal sensors
	ON	New alert message in Event Log re: internal sensors
Ext Alert	OFF	No new alert message in Event Log re: external sensors
	ON	New alert message in Event Log re: external sensors
Fault	ON	A sensor has gone out of range of a configurable threshold

Note: When power is first applied to the E-2D or -5D, both the Power LED (green) and Fault LED (red) will illuminate for the first 30 seconds of the boot process. After this the fault LED will turn OFF until a sensor alarm is generated which will turn the fault LED back ON.

System Reset Button

A reset button is located on the front of the ENVIROMUX (see Figure 125). The button can be used to reboot/restart the firmware of the ENVIROMUX. Pressing this button supersedes the use of the power on/off switch and battery backup to allow the firmware to easily reboot in the event of a system lockup. To activate a reset, momentarily press the button with a pen or other small pointed object. The ENVIROMUX will reboot and be ready for login within its usual start-up time period.

Alarm Test/Silence Button

A button is provided on the front of the E-16D and E-5D (and on the rear of the E-5D) to be used to test or to silence the alarm siren when connected. To test the alarm function, press and hold the button for at least 2 seconds. The siren and beacon will "alarm" until the button is released. To silence an alarm, press and immediately release the button.

Restore Defaults Button

Another button is located on the front of the ENVIROMUX (see Figure 125). The button can be used to clear all configuration changes and restore the ENVIROMUX to default settings including the administrative password. To use this button, press it with a pen or other small pointed object and hold it for 5 seconds. The ENVIROMUX will reboot and be ready for login within its usual start-up time period. If possible, consider saving the ENVIROMUX configuration before using this button (page 60).

BATTERY BACKUP

E-16D

E-16D has a rechargeable sealed lead-acid battery backup that will prevent the monitoring system from shutting down in the event of a power failure. Should a service power failure occur, **the ENVIROMUX will continue to operate as normal for 1 hour under full load** and approximately 30 minutes after the "Low Bat" LED on the front panel (page 53) illuminates.

When the battery is not being used, it is being charged as long as line power is provided. It will take 24 hours for the battery to fully charge from a fully discharged state. While charging the "Low Batt" LED will be solid ON.

If the power is ON and the battery is fully charged, the "Low Batt" LED will be dark.

If the battery fails to charge or if the battery's output voltage drops from 12VDC to below 10.7 volts, the "Low Batt" LED will blink. The battery will automatically be disconnected from the system. If this happens, the battery must be replaced. Contact NTI to arrange for return and service.

Note: While operating on the battery backup, to shut OFF the ENVIROMUX, switch the power switch to OFF and press the System Reset button.

CAUTION

RISK OF ELECTRIC SHOCK. Do not remove cover. No user serviceable components inside. All repairs and maintenance must be performed by authorized service personnel only.

E-5DB / -2DB

E-5DB /-2DB has a rechargeable sealed lead-acid battery backup that will prevent the monitoring system from shutting down in the event of a power failure. Should a service power failure occur, **the ENVIROMUX will continue to operate as normal for 2 hours under full load.**

When the battery is not being used, it is being charged as long as line power is provided. It will take 24 hours for the battery to fully charge from a fully discharged state.

CAUTION

RISK OF ELECTRIC SHOCK. Do not remove cover. No user serviceable components inside. All repairs and maintenance must be performed by authorized service personnel only.

USB PORT

The ENVIROMUX are each equipped with USB Type A female ports on the front and rear panel for connection of a USB flash drive, a GSM modem or for receiving alert messages via SMS, or a USB LCD Monitor (page 61).

- The ports are compatible with USB 2.0 Full Speed flash drives. When enabled (page 109) 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 17), it will automatically be sensed by the ENVIROMUX (page 64).
- When an USB LCD monitor is connected, and a selection is made as to what will be viewed on the monitor (page 61), the ENVIROMUX will automatically send video to the connected monitor.

Figure 126- USB Flash Drive/Modem/LCD Monitor port

To enable recording logs to a flash drive,

1. Connect a FAT32 formatted flash drive to an available USB port on the ENVIROMUX. Make sure there is plenty of space on it.

2. Apply a checkmark to the check box “Enable Log to Flash Drive”, click “Save”, change “Unmount” to “Mount” and click “Save” again on the Log Settings page (page 109).

While the flash drive is present, the Event and Data Logs will be written to a text file on the flash drive in addition to the memory in the ENVIROMUX.

Note: When using the USB port with a flash drive, be sure to remove the checkmark from the “Enable Log to Flash Drive”, click “Save”, change “Mount” to “Unmount” and click “Save” again in the Log Settings page (page 109) before removing the flash drive from the port. Failure to do so may result in a loss of data stored on the drive.

Note: Only 1 flash drive can be connected to the ENVIROMUX at a time. Additional drives will be ignored.

Note: The file system of the flash drive must be formatted FAT32 (not NTFS).

SERIAL CONTROL

The ENVIROMUX can be controlled serially through a text menu using one of these methods:

- a terminal program (e.g. HyperTerminal) from a PC connected to the RJ45 “RS232” port (page 15),
- a terminal program from a PC connected to the USB “Console” Port (page 15),
- Telnet protocol using an Ethernet connection (page 16),
- SSH protocol using an Ethernet connection (page 16).

Either of these methods will work to access the ENVIROMUX text menu. The text menu can be used to control most functions of the ENVIROMUX as an alternative to the Web Interface (page 29). For more on using the text menu, see the Serial Control Manual.

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://192.168.1.21/

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 69) 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://192.168.1.21:95)

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

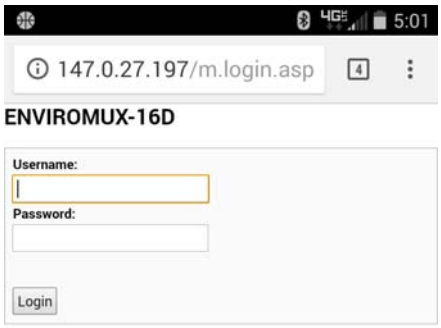


Figure 127- Mobile Login page

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

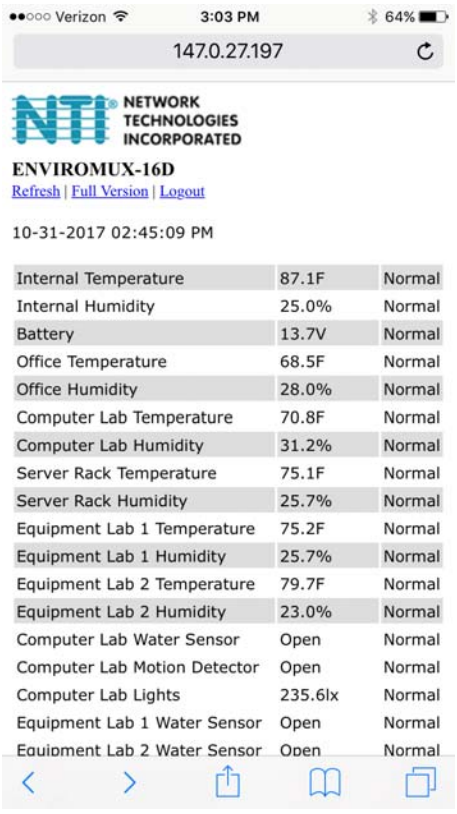


Figure 128- Mobile Summary page

JSON API SUPPORT

Support has been built into the ENVIROMUX firmware to use JSON API to poll sensors using HTTP protocol like cURL command. To automate the interface between servers and the ENVIROMUX and provide data, the following instruction is provided.

Using cURL

Step 1: Get the session cookie by a HTTP POST request:

Get session cookie by sending 'username' and 'password' in POST body to endpoint '/goform/login'. We'll receive a JSON response with the 'sessionId' as a 'cookie' variable

Request:

curl -X POST -d "username=root&password=nti" http://192.168.3.216/goform/login

Response:

{ "success":"true", "cookie":"sessionId=cm9vdDpudGk6MTA=" }

Step 2: Get the sensor details using appropriate end point and by providing the session cookie in header.

Example with Endpoint of /json/get/appISens.json:

Request:

curl -v -H "Host: 192.168.3.216" -H "Cookie: sessionId=cm9vdDpudGk6MTA" http://192.168.3.216/json/get/appISens.json

Response:

Please refer to page 117 for example of the response format.

Using HTTP browser as an example

First login to the ENVIROMUX from the web browser. Then enter any of the listed requests in the URL bar to be provided with the desired information.

Note: Command syntax is case sensitive.

List of available API endpoints:

IPADDRESS/json/get/appISens.json - for Internal Sensors
IPADDRESS/json/get/appESens.json - for External Sensors
IPADDRESS/json/get/appDiginp.json - for Digital Inputs
IPADDRESS/json/get/appIpdev.json - for IP Devices
IPADDRESS/json/get/appEvents.json - for Events
IPADDRESS/json/get/appSmalerts.json - for Smart Alerts
IPADDRESS/json/get/appNetwork.json - to get Network Settings
IPADDRESS/json/get/appDevice.json - to get Device Settings
IPADDRESS/json/get/appAll.json - to get all of the above information in one API

The tables on the following page provide definitions for the Type and Status numbers that will be provided. See Figure 129 for an example of a json response via HTTP.

Sensor ID Definitions:

Sensor Type ID	Sensor Type	Sensor Type ID	Sensor Type	Sensor Type ID	Sensor Type
0	ID_UNDEFINED	20	ID_PING	42	ID_ACLM3_C
1	ID_TEMPERATURE	21	ID_NOT_RESPONDING	43	ID_ACLM3_W
2	ID_HUMIDITY	22	ID_LIGHT	44	ID_ACLM3_VAR
3	ID_POWER	23	ID_TEMPERATURE_EX	230	ID_POWER_SUPP
4	ID_LOW_VOLTAGE	24	ID_DEWPOINT	513	ID_TEMP_HUM
5	ID_CURRENT	25	ID_NLS	540	ID_TEMP_HUM_EX2
6	ID_ACLM_V	26	ID_TAC_DIO16	552	ID_TEMP_HUM_EX3
7	ID_ACLM_V_OF_P	27	ID_HUMIDITY_D	771	ID_POW_POW
8	ID_ACLM_P	28	ID_TEMPERATURE_EX2	1285	ID_CURR_CURR
9	ID_WATER	29	ID_TAC_DIP1	1028	ID_LOWV_LOWV
10	ID_SMOKE	30	ID_AIR_VELOCITY	1542	ID_ACLM_V_V
11	ID_VIBRATION	31	ID_DUST	1800	ID_ACLM_P_V
12	ID_MOTION	33	ID_RTD_TRANSMITTER	6913	ID_TEMP_HUM_D
13	ID_GLASS	35	ID_FREQUENCY	32769	ID_TEMP_COMBO
14	ID_DOOR	36	ID_AC_V	32796	ID_TEMP_COMBO_EX2
15	ID_KEYPAD	37	ID_AC_C	32808	ID_TEMP_COMBO_EX3
16	ID_PANIC_BUTTON	38	ID_DC_V	32770	ID_HUM_COMBO
17	ID_KEY_STATION	39	ID_DC_C	32767	ID_CUSTOM
18	ID_DRY_CONTACT	40	ID_TEMPERATURE_EX3	9767	ID_DCLM6
19	ID_DIG_INPUT	41	ID_ACLM3_V	9253	ID_ACLM3

Sensor Status ID	Sensor Status	Sensor Status ID	Sensor Status
0	STATUS_NOTCONNECTED	6	STATUS_DISCONNECTED
1	STATUS_NORMAL	7	STATUS_TAMPER_ALERT
2	STATUS_WARNING	8	STATUS_PREDIZZY
3	STATUS_ALERT	9	STATUS_DIZZY
4	STATUS_ACKNOWLEDGED	10	STATUS_IN_USE
5	STATUS_DISMISSED	11	STATUS_NOT_USED

HTTP Example:

Entered into the browser URL bar: **`<IP Address>/json/get/appESens.json`**

Response:

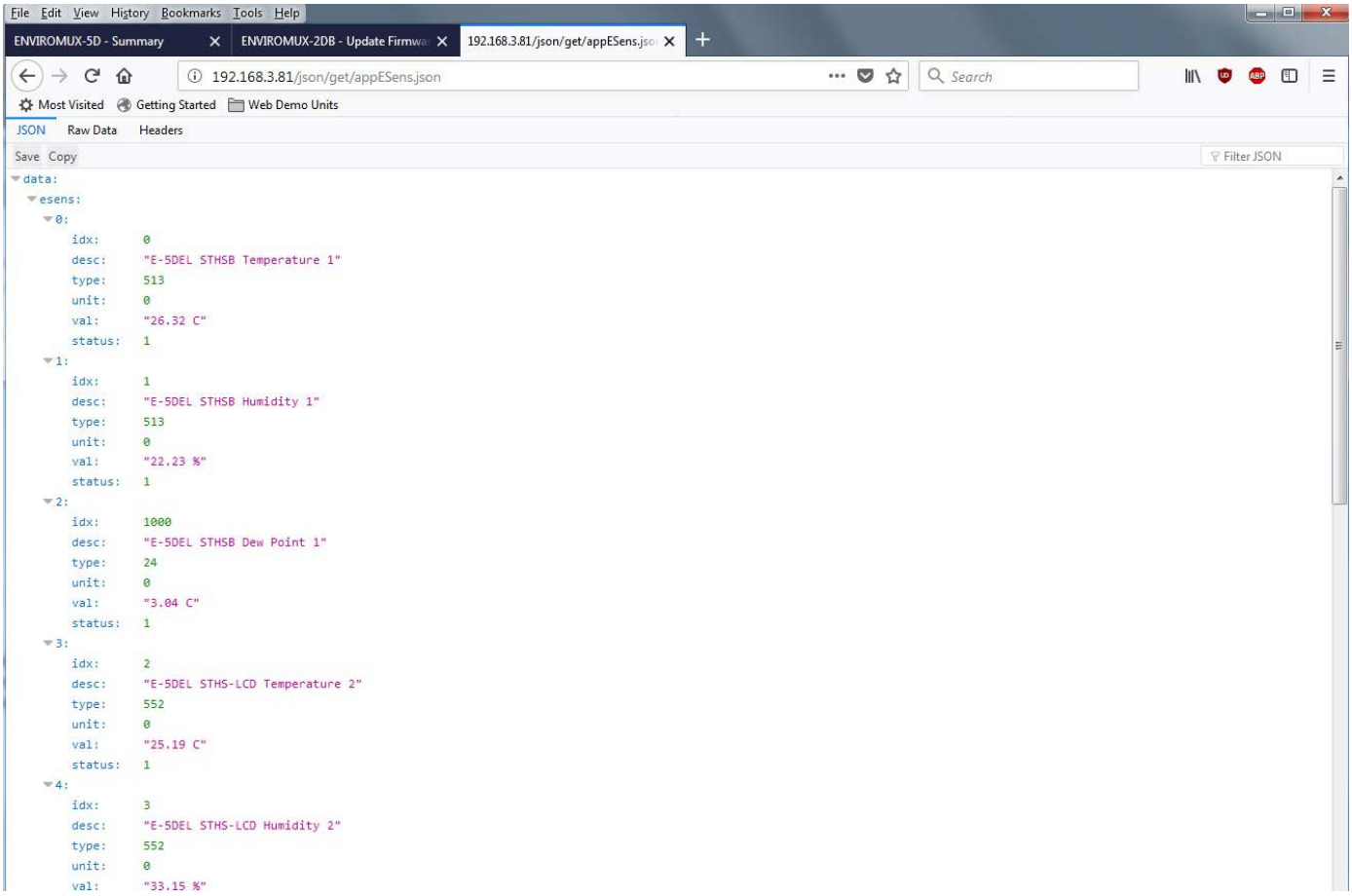


Figure 129- Example JSON Response for External Sensors shown on browser

cURL Example:

Entered at the command line after getting sessionId:

```
curl -v -H "Host: 192.168.3.216"  -H "Cookie: sessionId=cm9vdDpudGk6MTM"
http://192.168.3.216/json/get/appAll.json
```

Response:

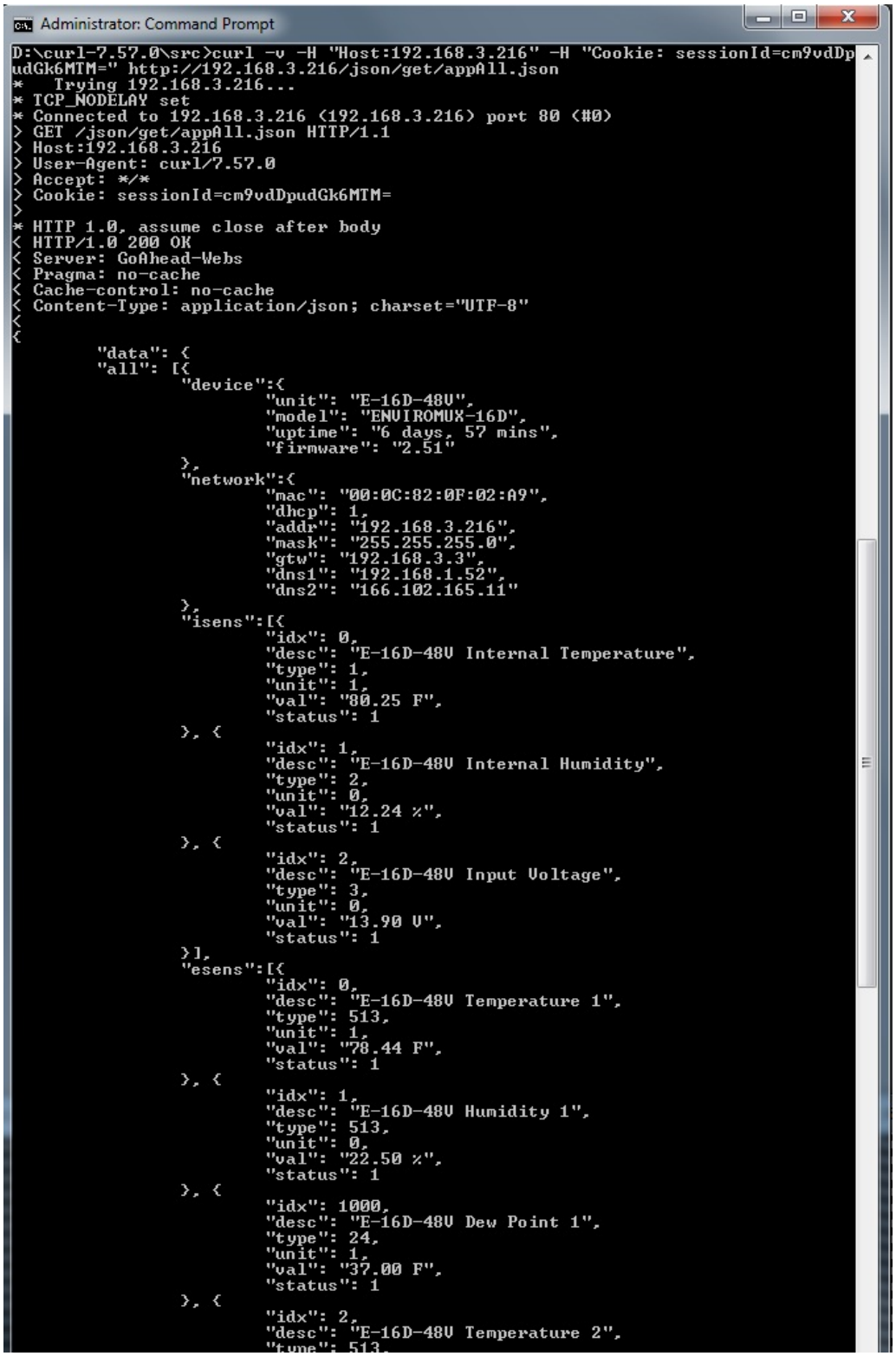


Figure 130- Example JSON Response for all information using cURL

MODBUS TCP/IP SUPPORT

The ENVIROMUX is equipped with Modbus TCP/IP support to enable PLC controls to read the value/state of sensors and read and command the state of relays. Using the Modbus communication protocol devices can be programmed over TCP/IP to treat the ENVIROMUX as a Modbus slave device reacting to readings from available sensors and controlling relays as needed.

Modbus TCP Function Codes Definition

Function Code	Name	Usage
01	Read Coils	Read the state of Output Relays
02	Read Discrete Inputs	Read the state of Digital Inputs
03	Read Holding Registers	Not Available
04	Read Input Registers	Read Internal/External Sensors floating point values
05	Write Single Coil	Write data to force Output Relay Active/Inactive
06	Write Single Holding Register	Not Available
15	Write Multiple Coils	Write data to force multiple Output Relays Active/Inactive
16	Write Multiple Holding Registers	Not Available

Function Code 01 - Read the state of Output Relays

Description:

Function code 01 is used to read the status of Output Relays (Active/Inactive) of the E-xD slave device in a binary data format.

Query:

Device ID (0,1 or 255)	Function Code	Starting Address High	Starting Address Low	Quantity of coils High	Quantity of coils Low	CRC	CRC

Response:

The Relay Outputs status in response message is packed as one Relay Output per bit of data field. The first Relay Output addressed by Starting Address is the LSB. A value of “1” for a bit means that the relay is INACTIVE while “0” means relay ACTIVE.

Mapping:

Coil # (Address)	E-16D	E-5D	E-2D
0	Relay Output #1	Relay Output #1	Relay Output #1
1	Relay Output #2	Relay Output #2	N/A
2	Relay Output #3	N/A	N/A
3	Relay Output #4	N/A	N/A
4	Remote DO #1-1	Remote DO #1-1	Remote DO #1-1
...	...	...	...
19	Remote DO #1-16	Remote DO #1-16	Remote DO #1-16
20	Remote DO #2-1	Remote DO #2-1	Remote DO #2-1
…	...	...	...
35	Remote DO #2-16	Remote DO #2-16	Remote DO #2-16

Mapping (Cont'd):

Coil # (Address)	E-16D	E-5D	E-2D
…	…	…	N/A
4 + (M – 1) * 16 + N - 1	Remote DO #M-N	Remote DO #M-N	N/A
…	…	…	N/A
68	Remote DO #5-1	Remote DO #5-1	N/A
…	…	…	N/A
83	Remote DO #5-16	Remote DO #5-16	N/A
244	Remote DO #16-1	N/A	N/A
		N/A	N/A
259	Remote DO #16-16	N/A	N/A

Function Code 02 - Read the state of Digital Inputs

Description:

Function code 02 is used to read the status of Digital Inputs (Open/Closed) of the E-xD slave device in a binary data format

Query:

Device ID (0,1 or 255)	Function Code	Starting Address High	Starting Address Low	Quantity of inputs High	Quantity of inputs Low	CRC	CRC

Response:

The Relay Outputs status in response message is packed as one Digital Input per bit of data field. The LSB of the first data byte. The other inputs follow toward the high order end of this byte, and from low order to high order in subsequent bytes. If the returned input quantity is not a multiple of eight, the remaining bits in the final data byte will be padded with zeros (toward the high order end of the byte). The byte count field specifies the quantity of data.

A value of "1" for a bit means that the corresponding Digital Input is "Open", a value of "0" means it is closed.

Device ID (0,1 or 255)	Function Code	Byte Count	Data	Data	….	CRC	CRC

Mapping:

Input # (Address)	E-16D	E-5D	E-2D
0	Digital Input #1	Digital Input #1	Digital Input #1
1	Digital Input #2	Digital Input #2	Digital Input #2
2	Digital Input #3	Digital Input #3	Digital Input #3
3	Digital Input #4	Digital Input #4	Digital Input #4
4	Digital Input #5	Digital Input #5	Digital Input #5
5	Digital Input #6	N/A	N/A
6	Digital Input #7	N/A	N/A
7	Digital Input #8	N/A	N/A

Mapping (Cont'd):

Input # (Address)	E-16D	E-5D	E-2D
8	Remote DI #1.1	Remote DI #1.1	Remote DI #1.1
…	…	…	…
23	Remote DI #1.16	Remote DI # 1.16	Remote DI #1.16
24	Remote DI #2.1	Remote DI #2.1	Remote DI #2.1
…	…	…	…
39	Remote DI #2.16	Remote DI #2.16	Remote DI #2.16
…	…	…	N/A
8 + (M – 1) * 16 + N - 1	Remote DI #M.N	Remote DI #M.N	N/A
…	…	…	N/A
72	Remote DI #5.1	Remote DI #5.1	N/A
…	…	…	N/A
87	Remote DI #5.16	Remote DI #5.16	N/A
248	Remote DI #16.1	N/A	N/A
		N/A	N/A
263	Remote DI #16.16	N/A	N/A

Function Code 04 - Read Internal/External Sensors floating point values

Floating Point Format

The values of analog sensors are in floating point format. For this reason, two 16-bit registers are used to represent the value of each sensor. The format is IEEE 32-bit Floating Point Big Endian with byte-swapped (the order of bytes is 3,4,1,2)

Description:

Function code 04 is used to read the values of Internal Sensors and External Sensors. If external sensors are of a contact type, a value of 0.0 will represent a closed contact and a value of 1.0 will represent an open contact. Two consecutive 16-bit registers are used for each sensor.

Query:

Device ID (0,1 or 255)	Function Code	Starting Address High	Starting Address Low	Quantity of Inputs High	Quantity of Inputs Low	CRC	CRC

Note: because two registers are needed to represent any sensor in Input Registers, the Quantity of Inputs value should be the double of the number of sensor to read.

Response:

The sensors value in response messages are packed as IEEE 32-bit Floating Point Big Endian format and they use 4 bytes for each value. The Modbus protocol has a single byte count which represents the number of 16 bits register. Because of this, the protocol can process up to maximum 64 floating point values in a single request.

Device ID (0,1 or 255)	Function Code	Byte Count	Data	Data	….	CRC	CRC

Mapping:

Input # (Address)	E-16D	E-5D	E-2D
0	Internal Sensor #1	Internal Sensor #1	
1	Internal Sensor #2	Internal Sensor #2	N/A
2	Internal Sensor #3	N/A	N/A
3	External Sensor #1.1	External Sensor #1.1	External Sensor #1.1
4	External Sensor #1.2	External Sensor #1.2	External Sensor #1.2
5	External Sensor #2.1	External Sensor #2.1	External Sensor #2.1
6	External Sensor #2.2	External Sensor #2.2	External Sensor #2.2
7	External Sensor #3.1	External Sensor #3.1	N/A
8	External Sensor #3.2	External Sensor #3.2	N/A
9	External Sensor #4.1	External Sensor #4.1	N/A
10	External Sensor #4.2	External Sensor #4.2	N/A
11	External Sensor #5.1	External Sensor #5.1	N/A
12	External Sensor #5.2	External Sensor #5.2	N/A
13	External Sensor #6.1	N/A	N/A
14	External Sensor #6.2	N/A	N/A
...	...	N/A	N/A
3 + 2 * (M – 1) + N - 1	External Sensor #M.N	N/A	N/A
	…	N/A	N/A
33	External Sensor #16.1	N/A	N/A
34	External Sensor #16.2	N/A	N/A
35	Auxiliary Sensor #1.1	Auxiliary Sensor #1.1	Auxiliary Sensor #1.1
36	Auxiliary Sensor #1.2	Auxiliary Sensor #1.2	Auxiliary Sensor #1.2
37	Auxiliary Sensor #2.1	Auxiliary Sensor #2.1	Auxiliary Sensor #2.1
38	Auxiliary Sensor #2.2	Auxiliary Sensor #2.2	Auxiliary Sensor #2.2
39	Auxiliary Sensor #3.1	Auxiliary Sensor #3.1	N/A
40	Auxiliary Sensor #3.2	Auxiliary Sensor #3.2	N/A
41	Auxiliary Sensor #4.1	Auxiliary Sensor #4.1	N/A
42	AuxiliarySensor #4.2	Auxiliary Sensor #4.2	N/A
43	Auxiliary Sensor #5.1	Auxiliary Sensor #5.1	N/A
44	Auxiliary Sensor #5.2	Auxiliary Sensor #5.2	N/A
45	Auxiliary Sensor #6.1	N/A	N/A
46	Auxiliary Sensor #6.2	N/A	N/A
...	...	N/A	N/A
35 + 2 * (M – 1) + N - 1	Auxiliary Sensor #M.N	N/A	N/A
...	...	N/A	N/A
65	Auxiliary Sensor #16.1	N/A	N/A
66	Auxiliary Sensor #16.2		
67	Tachometer #1	Tachometer #1	Tachometer #1

Write data to force multiple Output Relays Active/Inactive

Description:

Function code 15 is used to force the status of Output Relays (Active/Inactive) of the E-xD slave device in a binary data format.

Query:

Device ID (0,1 or 255)	Function Code	Starting Address High	Starting Address Low	Quantity of coils High	Quantity of coils Low	Byte Count (N)	Data

	Data	Data	CRC	CRC

N in Byte Count field is Quantity of Coils / 8 (if the remainder is different of 0, add 1).

The Relay Outputs status in data field(s) is packed as one Relay Output per bit of data field. The first Relay Output addressed by Starting Address is the LSB. A value of “1” for a bit means that the relay is INACTIVE while “0” means relay ACTIVE.

Response:

The Relay Outputs status in response message has the following format:

Function Code	Starting Address High	Starting Address Low	Quantity of Inputs High	Quantity of Inputs Low	CRC	CRC

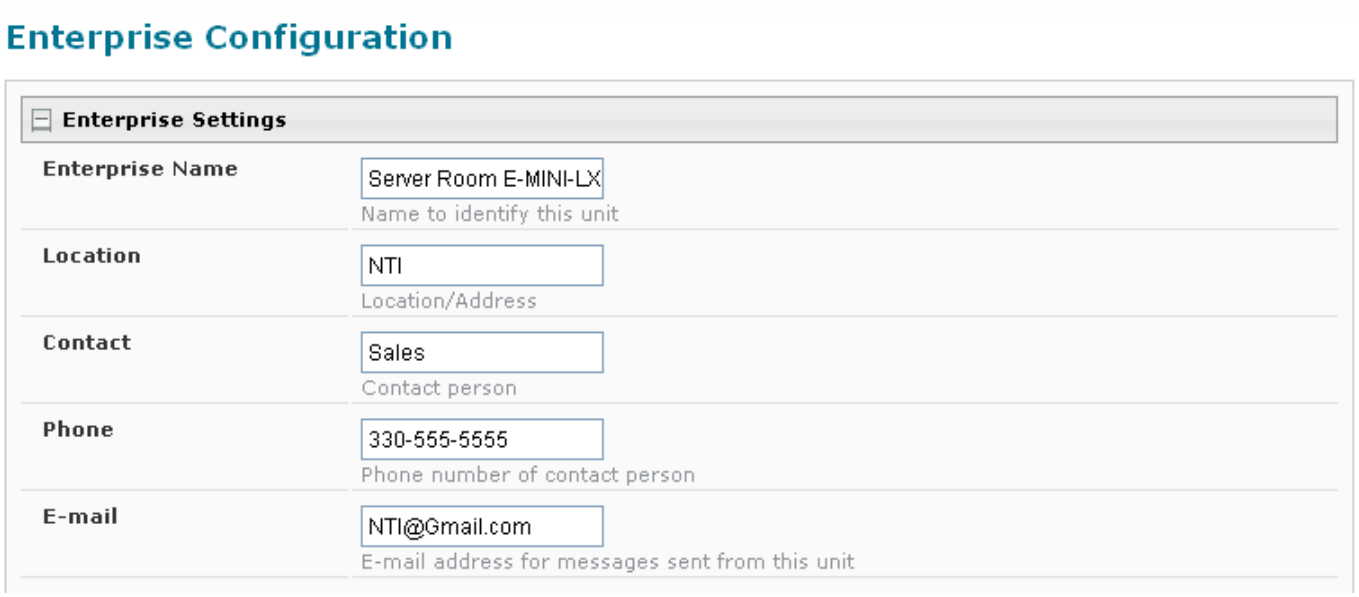
Mapping:

The mapping of output relays is the same as for Function Code 01

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 64).



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.

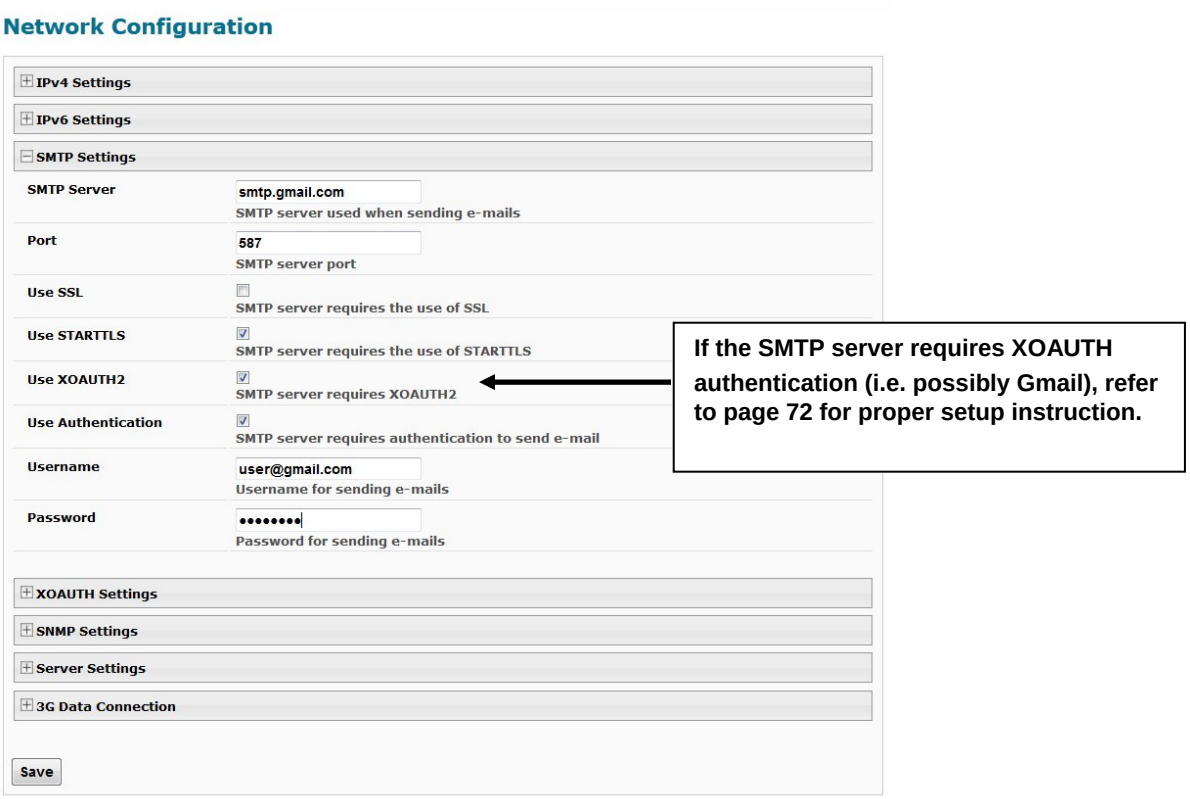


Figure 131- Example of configuration for Gmail server

2. Fill in Network Page (page 67) 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.

D. Check "Use STARTTLS" if your SMTP server requires STARTTLS.

E. 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: If the SMTP server requires XOAUTH authentication (i.e. possibly Gmail), refer to page 73 for proper setup instruction.

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.

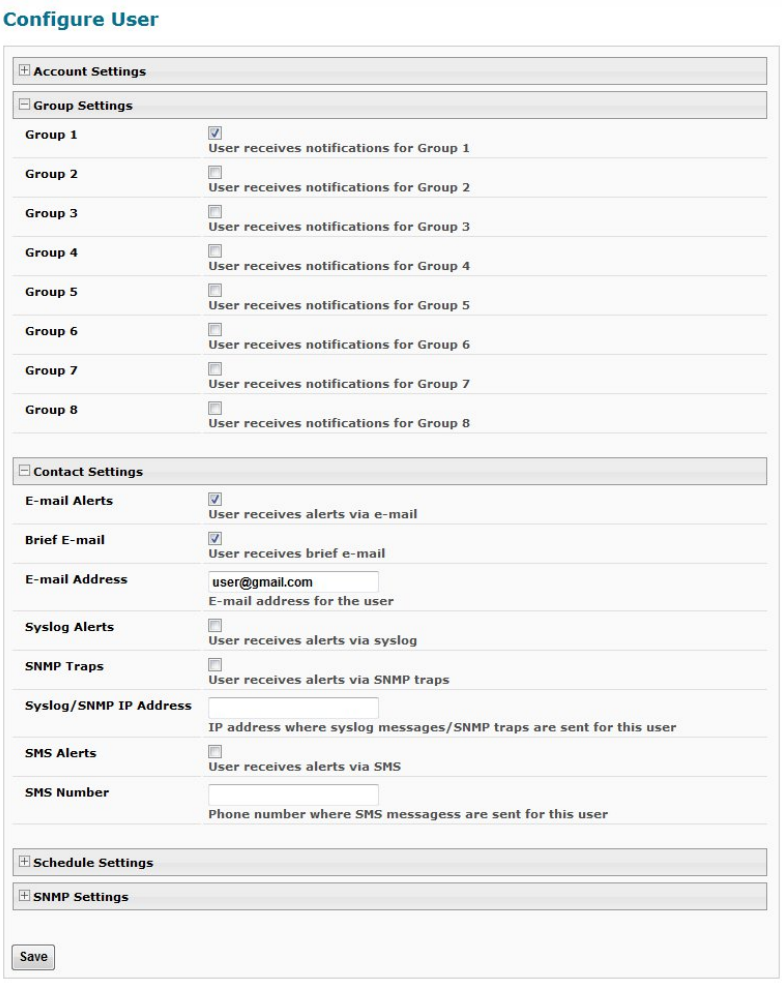


Figure 132- Configure user to receive alerts via email

Email Settings to be used in conjunction with Office 365

1. Enter on the Enterprise page (page 64) the full Office 365 account e-mail address being used.
2. On the Network > SMTP settings page (page 68) enter the following settings:
    - SMTP Server: smtp.office365.com
    - Port: 587
    - Select: STARTTLS
    - Select: Use Authentication
    - Username: This should be the full user account e-mail address.
        - **Note: This is case sensitive!**
    - Password: This should be the user account password
        - **Note: This is also case sensitive**

This must be the same username as applied on the Enterprise Settings screen (page 113)

HOW TO SETUP SNMP

Follow these steps to prepare the ENVIROMUX to send SNMP traps to ENVIROMUX users.

Under Network Settings:

1. Enable the proper SNMP Agent type (v1/v2c , v1/v2c/v3, or just v3) depending upon what type of SNMP browser you use.
   - v1/v2c = no security required
   - v1/v2c/v3 = messages with or without security
   - v3= only secure messages will be sent

2. Place a checkmark in “Enable SNMP Traps”.
3. Enter names for the Read-write community and Read-only community (usually just “private” and “public” as shown).

Figure 133- SNMP Settings under Network Settings

Under Sensor Configuration:

4. Under the sensor configuration for each sensor, enter a Group number that the sensor should belong to. Users can receive alert messages from some, all, or no sensor groups, as configured under User Settings.

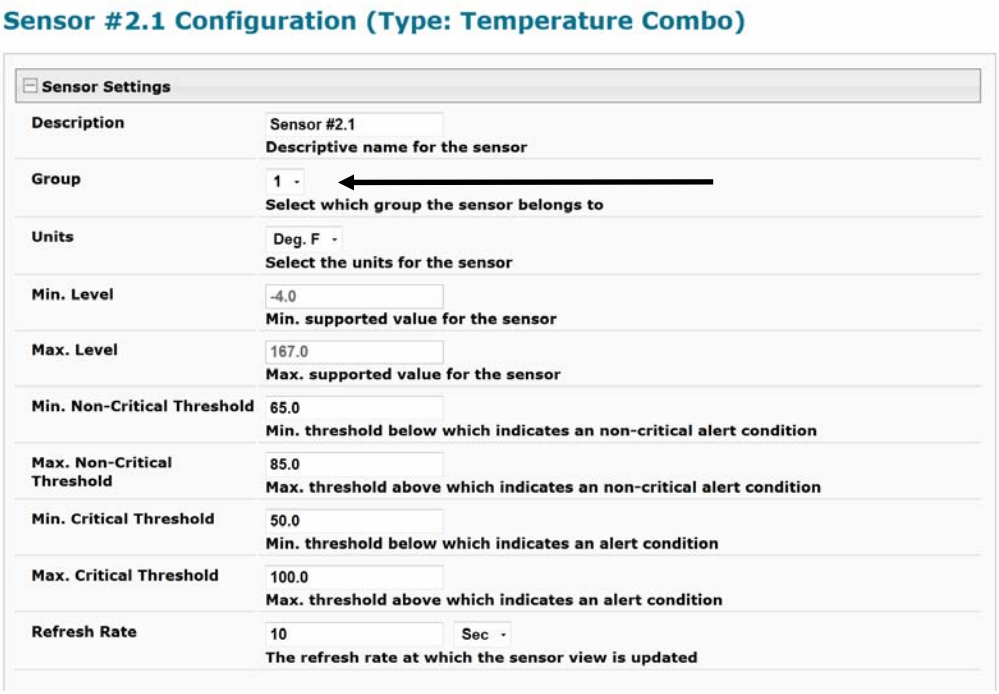


Figure 134- Enter at least one group number to sensor configuration

5. Place a checkmark in “Enable SNMP Traps” checkbox under the sensor configuration for each sensor that should send traps when there is an alert. If you want them sent for Critical Alerts and Non-Critical Alerts, there is a checkbox for each level.

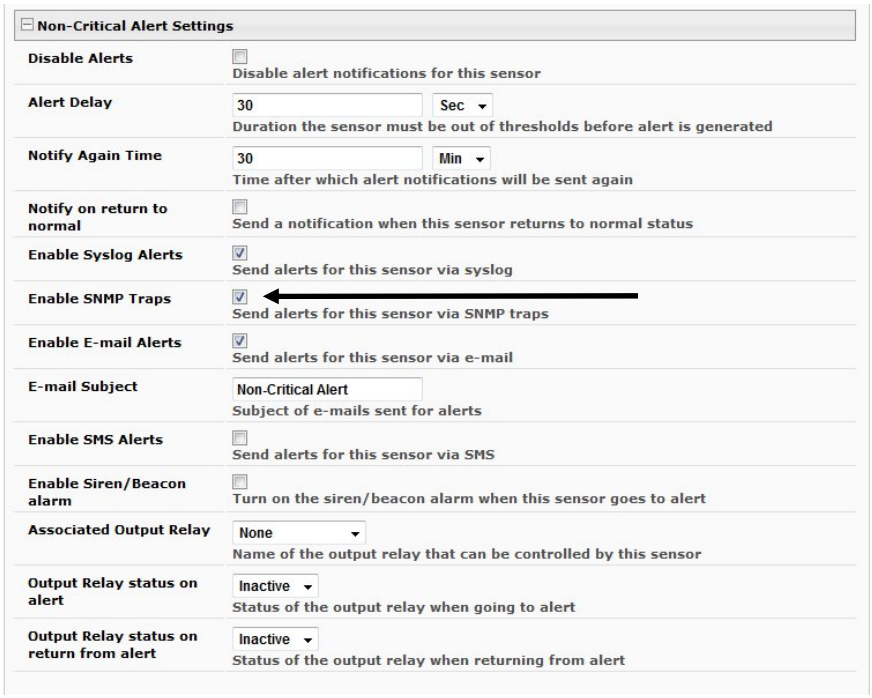


Figure 135- Enable SNMP Traps for the sensor

Under User Settings:

6. Apply a checkmark to the Group number(s) for the sensor(s) you want to receive SNMP traps about.

7. Be sure to apply a checkmark in the “SNMP Traps” box under Configure User ->Contact Settings for each user that should receive SNMP traps

8. Enter a valid IP address where traps are to be sent for each user.

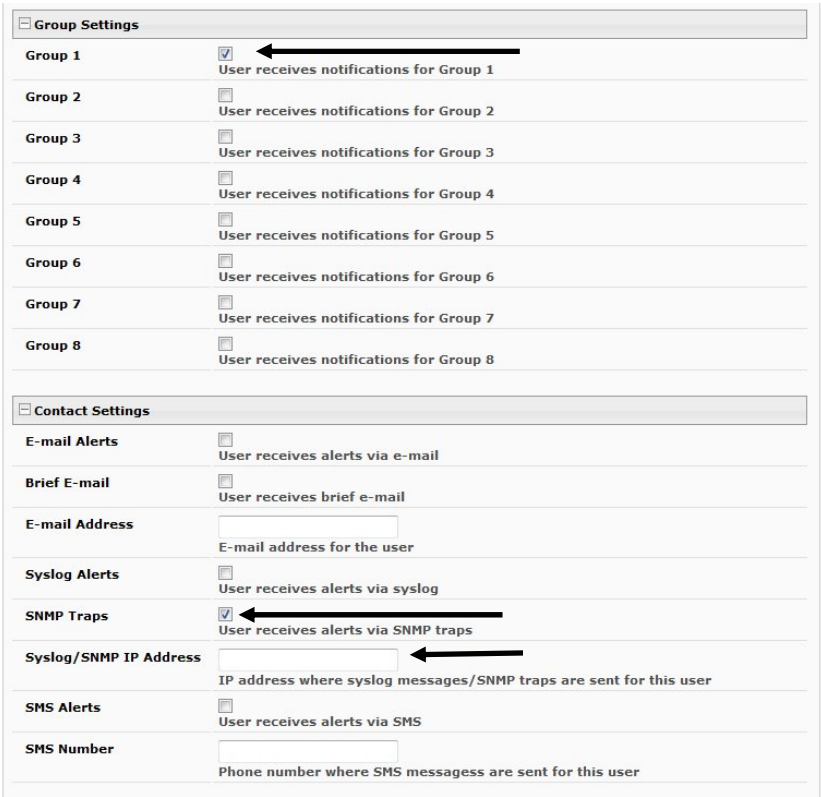


Figure 136- User Settings required for SNMP Traps

9. If the “Enable SNMP Agent” setting under “Network Settings” was SNMPv1/v2c/v3, then the Authentication Protocol (MD5 or SHA), Authentication Passphrase, Privacy Protocol (DES or AES), and Privacy Passphrase will only need to be filled in for users that will receive secure messages.

If only aSNMPv3 was selected, then these settings **must** be filled in for each user.

The protocol types will be dependent upon the type of SNMP Agent you are using (refer to your SNMP Agent specifications).

- Authentication Protocol = MD5 or SHA
- Privacy Protocol = DES or AES

If only SNMPv1/v2c will be used, the default settings of “None” will apply.

The passphrases will be those that have been setup in your SNMP agent for the user being configured.

Note: The username in the ENVIROMUX user configuration must match the username in the SNMP browser configuration.

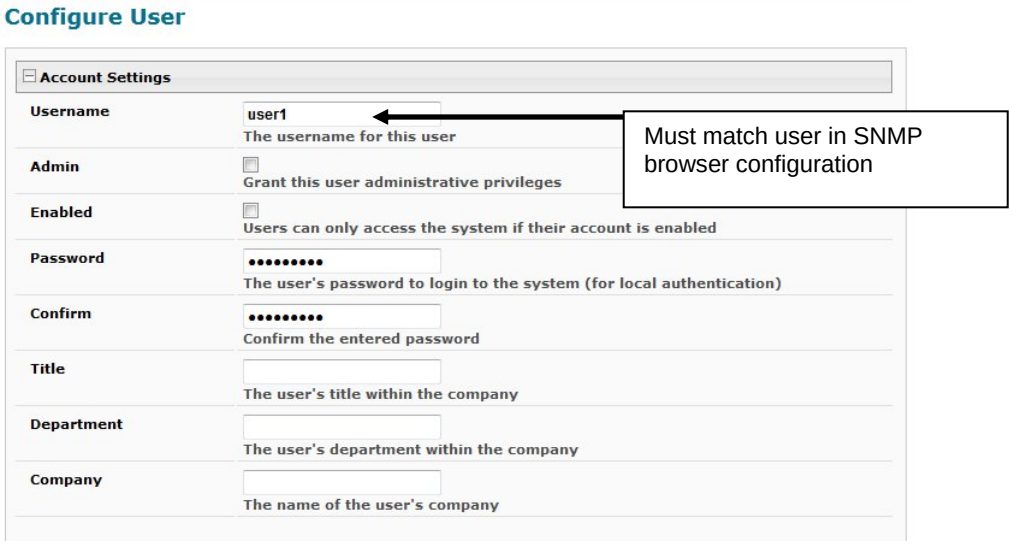


Figure 137- Username must match SNMP configuration

10. Select which Traps type the user should receive. If SNMPv1 or SNMPv2c are selected, the Authentication and Privacy settings below do not need to be configured as they are only required to receive SNMPv3 messages.

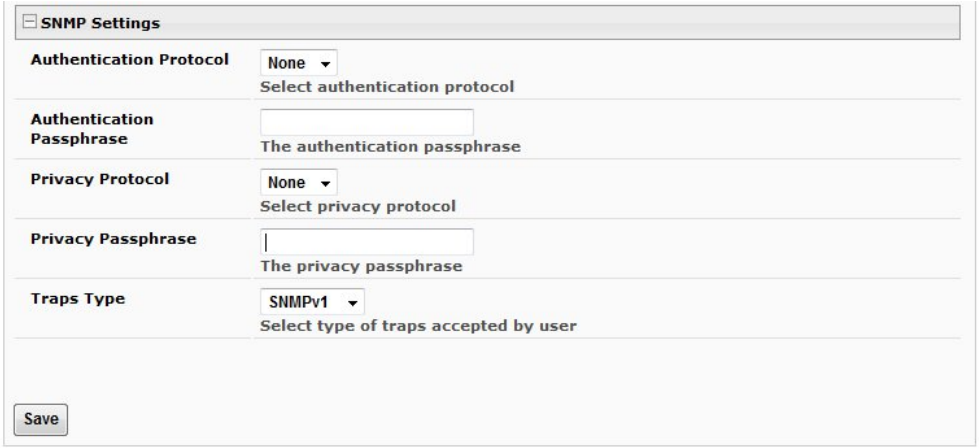


Figure 138- Apply applicable authentication settings

11. Use the MIB file (below) with your SNMP browser to setup and manage SNMP traps.

The MIB file is available for download from the firmware update website:
http://www.networktechinc.com/download/d-environment-monitor-16.html for E-16D / -5D / -2D

BASIC SNMP SET COMMANDS

In order to Acknowledge and Dismiss Alerts only:

Internal Sensor Status

External Sensor Status

Aux Sensor Status (devices like the E-ACLM-V, E-ACDCLM, and E-ACLM-3P480)

Tac Sensor Status

Digital Input Status

Remote Digital Input Status

IP Device Status

Event Status

Smart Alert Status

IP Sensor Status

In order to Activate or Deactivate Relays only:

Output Relay Status

Remote Output Relay Status

SNMP DEFINITIONS

Definitions of Integer Values reported by an SNMP Trap for Sensors

(From the mib file:)

```
digInputStatus          OBJECT-TYPE
        SYNTAX          INTEGER {notconnected(0), normal(1), prealert(2), alert(3), acknowledged(4),
                          dismissed(5), disconnected(6), reserved(10) }
        MAX-ACCESS      read-write
        STATUS          current
        DESCRIPTION       "The status of the sensor"
```

(Also applies to extSensorStatus)

INTEGER Value Definitions:

0- Not connected : No sensor has been connected to the referenced digital input.

1- Normal : Sensor is connected and operating within the parameter defined by “normal status” for that sensor, or in the case of external sensors, working between the values set by “Minimum Level” and “Maximum Level”.

2- Prealert: Sensor is connected and has entered alert status but has not been in alert status longer than the value defined by the “alert delay” for that sensor. Once that delay time has been satisfied, if still in alert status an alert will be sent by the ENVIROMUX.

3- Alert: Sensor is connected and has been in alert status longer than the time specified in the “alert delay” field.

4- Acknowledged: User has acknowledged the alert that has been reported by the ENVIROMUX for the sensor. The ENVIROMUX will not report another alert until the status for the sensor has returned to normal and then returns to alert status.

5- Dismissed: User has dismissed the alert reported by the ENVIROMUX for the sensor. The ENVIROMUX will report another alert if the sensor status does not return to normal when the time period configured in the “notify again after” field elapses.

6- Disconnected: Sensor was previously connected to the ENVIROMUX but has since lost its physical connection with the ENVIROMUX

10- Reserved : This field is not in use and is held for future reporting purposes.

HOW TO SETUP SYSLOG

Follow these steps to prepare the ENVIROMUX to send Syslog messages to ENVIROMUX users. This instruction assumes you have Syslog software configured to receive and record messages sent by the ENVIROMUX and know how to use it.

Configure the ENVIROMUX to send alerts via Syslog

1. Configure each sensor that will cause a message to be sent via Syslog to be included in one or more groups.

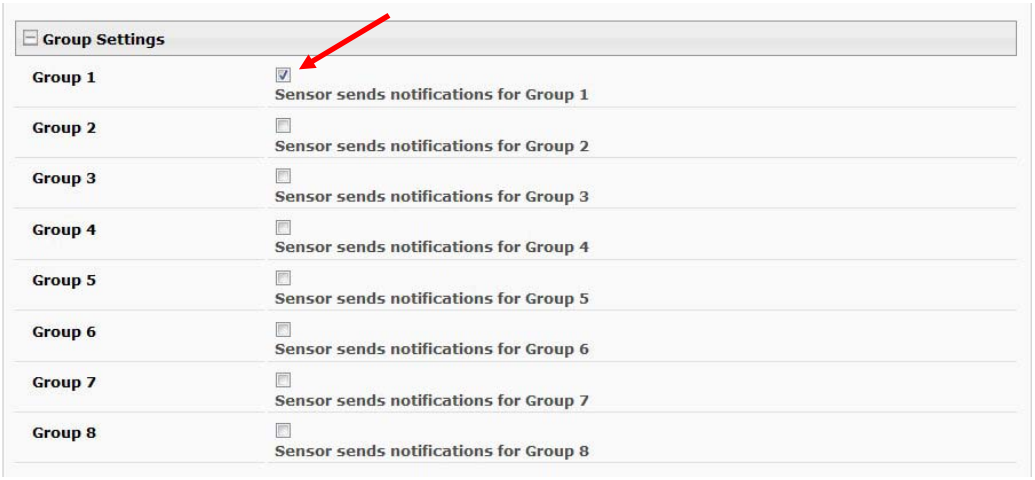


Figure 139- Configure which group(s) a sensor will belong to

2. Apply a checkmark in "Enable Syslog Alerts" under Non-Critical Alert Settings and/or Critical Alert Settings on the configuration page for each sensor that will cause Syslog Alerts.

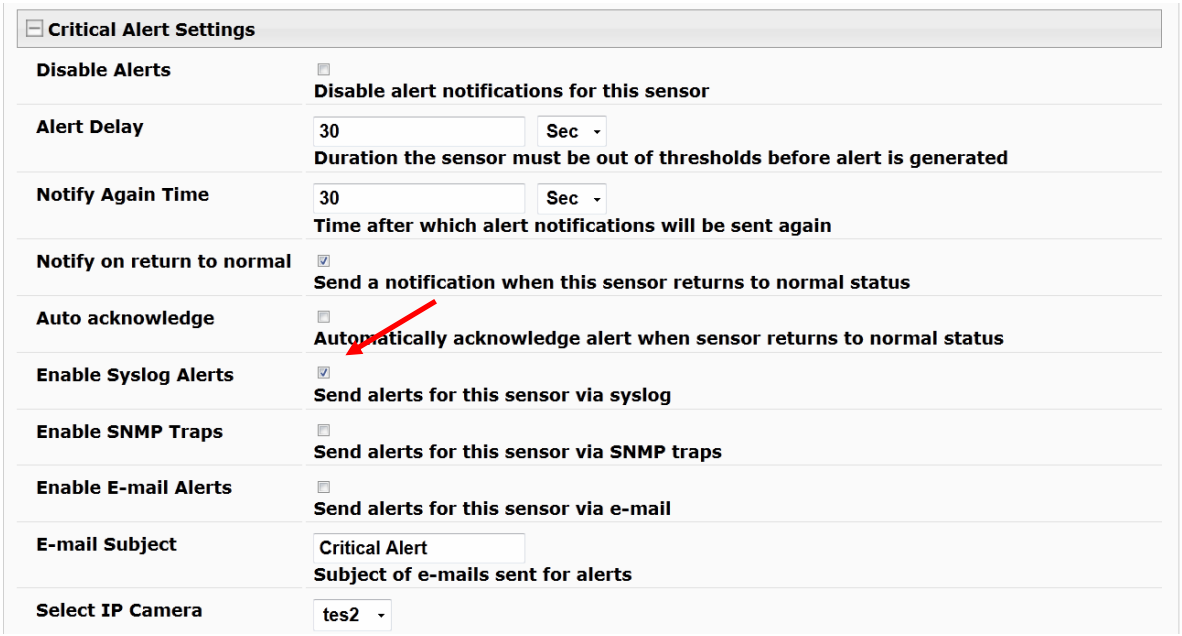


Figure 140- Enable Syslog alerts for the sensor

3. Under User configuration, place a checkmark in the group number(s) that the sensors belong to. (These are the groups that you checked off in step 1.)

4. Place a checkmark in the box for Syslog Alerts under Contact Settings so that the user can receive Syslog messages.

5. Enter a valid IP address where the Syslog messages for that user are to be sent.

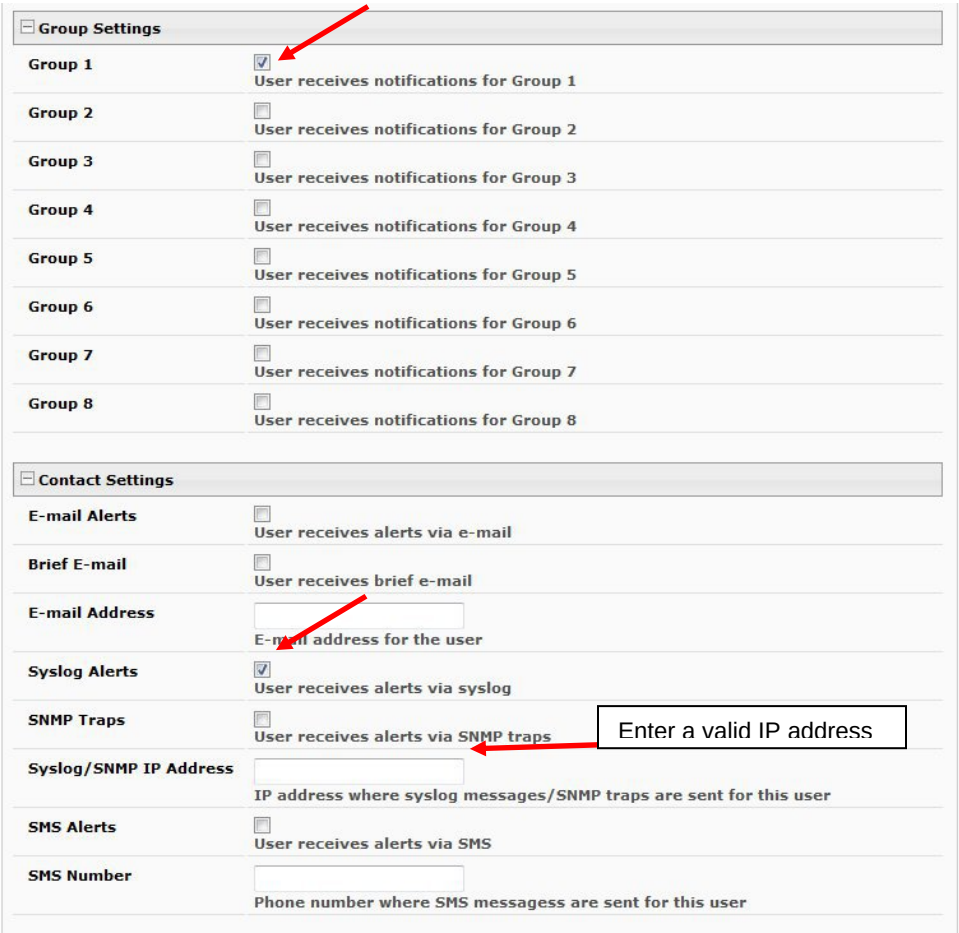


Figure 141- Configure user to receive alerts via Syslog

With sensors properly configured to send Syslog messages to specified groups, and Users enabled to receive messages from the same specified groups at a valid IP address, Syslog messages for sensor alerts will now be received.

Configure the ENVIROMUX to send sensor data via Syslog

1. Under Sensor Configuration, Data Logging, place a checkmark under "Add to data log" to have sensor readings added to the log. Set the time period for the frequency at which readings will be added to the data log. Press "Save".

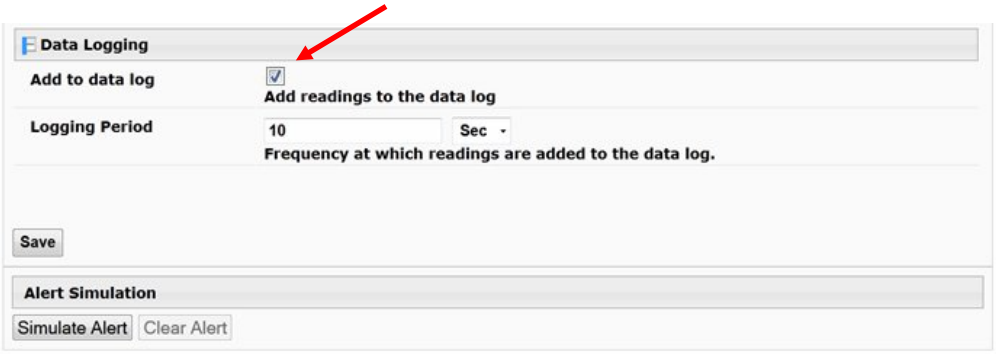


Figure 142- Configure sensor readings to be added to data log

2. Under Log, Log Settings, place a checkmark under "Enable Syslog Remote Logging". This will then send all data logs via Syslog message. To receive alerts regarding data logs, place a checkmark under "Enable Syslog Alerts". Make sure the group numbers are checked that the User is configured to receive Syslog messages from (under Configure User- Group Settings- see Figure 141).

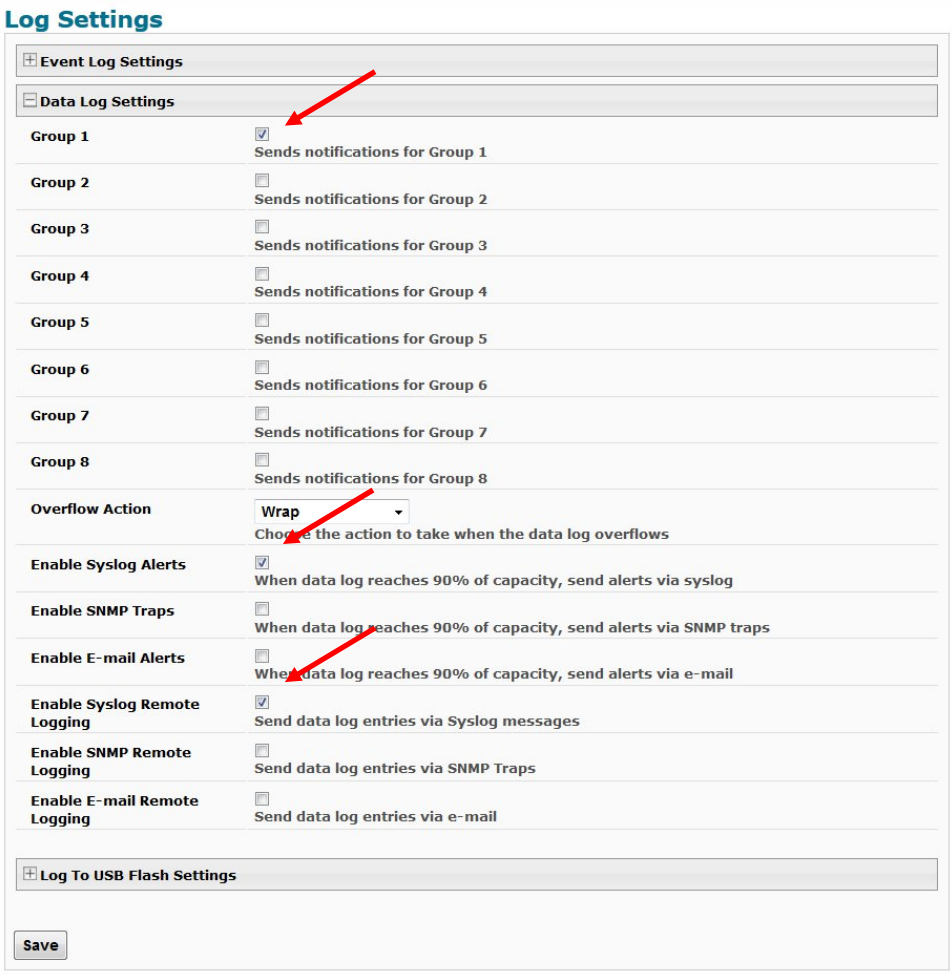


Figure 143- Configure data logs to send Syslog messages

LOCATING OIDS

To use SNMP (Simple Network Management Protocol) to monitor the sensors and control the functions of an ENVIROMUX Enterprise 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 from http://www.networktechinc.com/download/d-environment-monitor-16.html) provides a database to organize information received regarding sensors, output relays, 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.

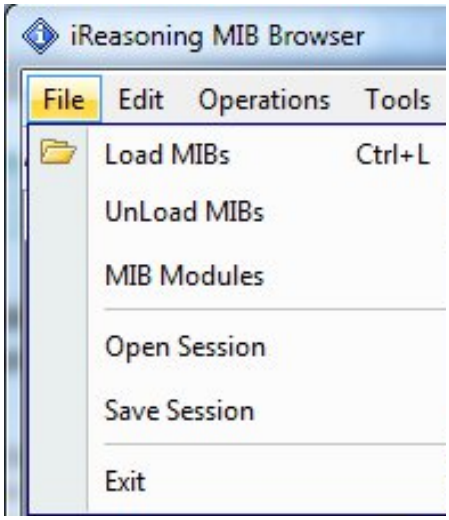
View OIDs

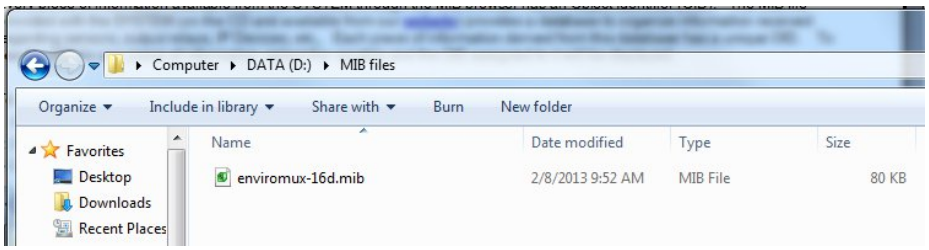
To view this information, you must do the following:

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.

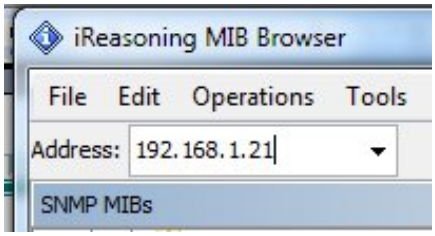




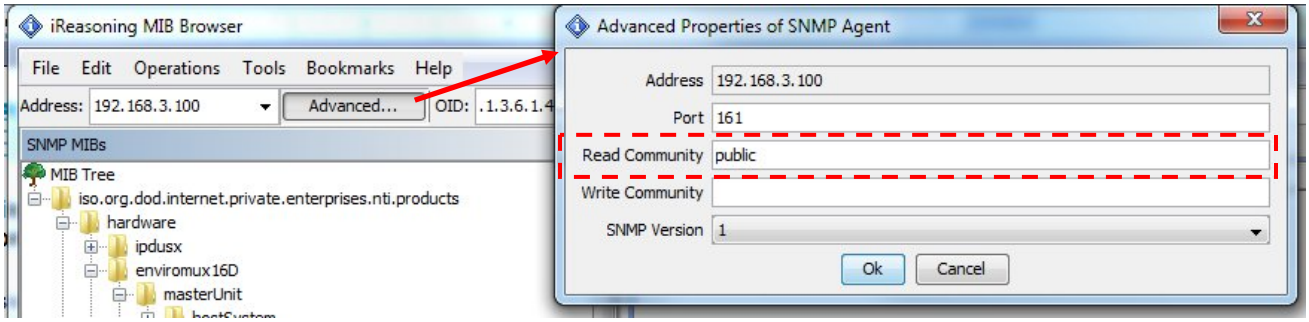
Select "Load MIBs" and locate the MIB file on your PC.

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.

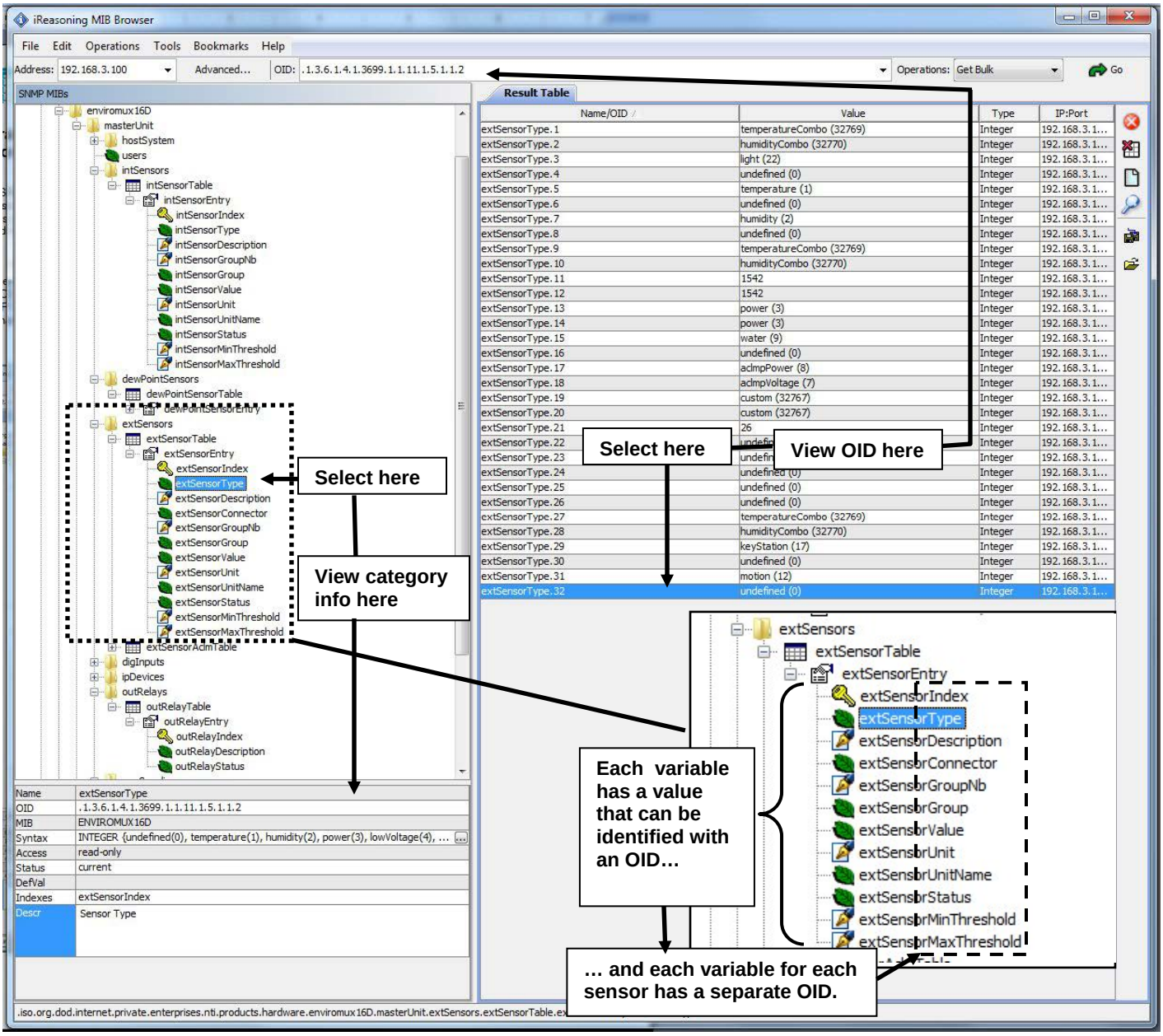


5. With the iReasoning browser, the Read-only Community Name (default is "public") was automatically sensed and applied when the IP address was entered, but if this doesn't happen in your browser, make sure the "Read Community" field in the agent properties includes the name "public" (or whatever you have changed it to in the E-16D 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 127 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 32 extSensors (RJ45 Sensor) for an E-16D.)

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.

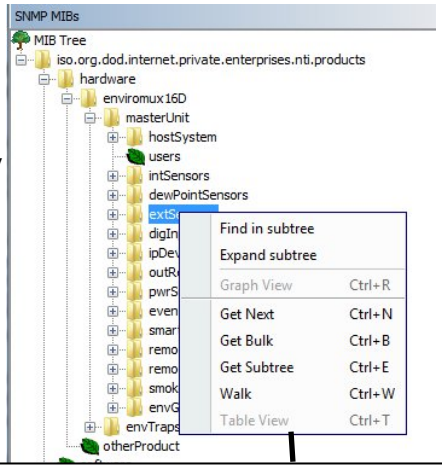
To get specific results in the Result Table, right click on an item in the MIB Tree and choose the type of search ("operation") you want.

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

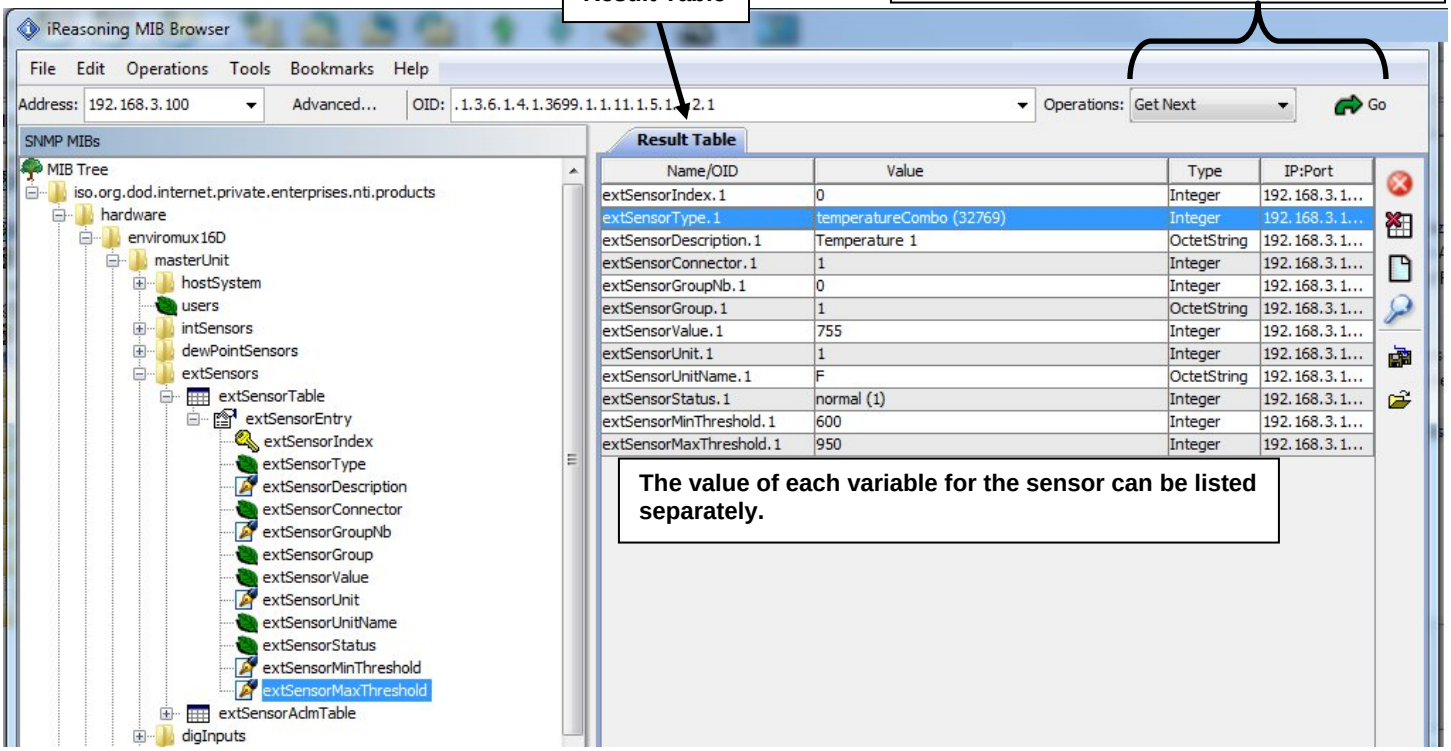
Get Subtree- will result in OIDs of that category and any sub-categories in the tree

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.



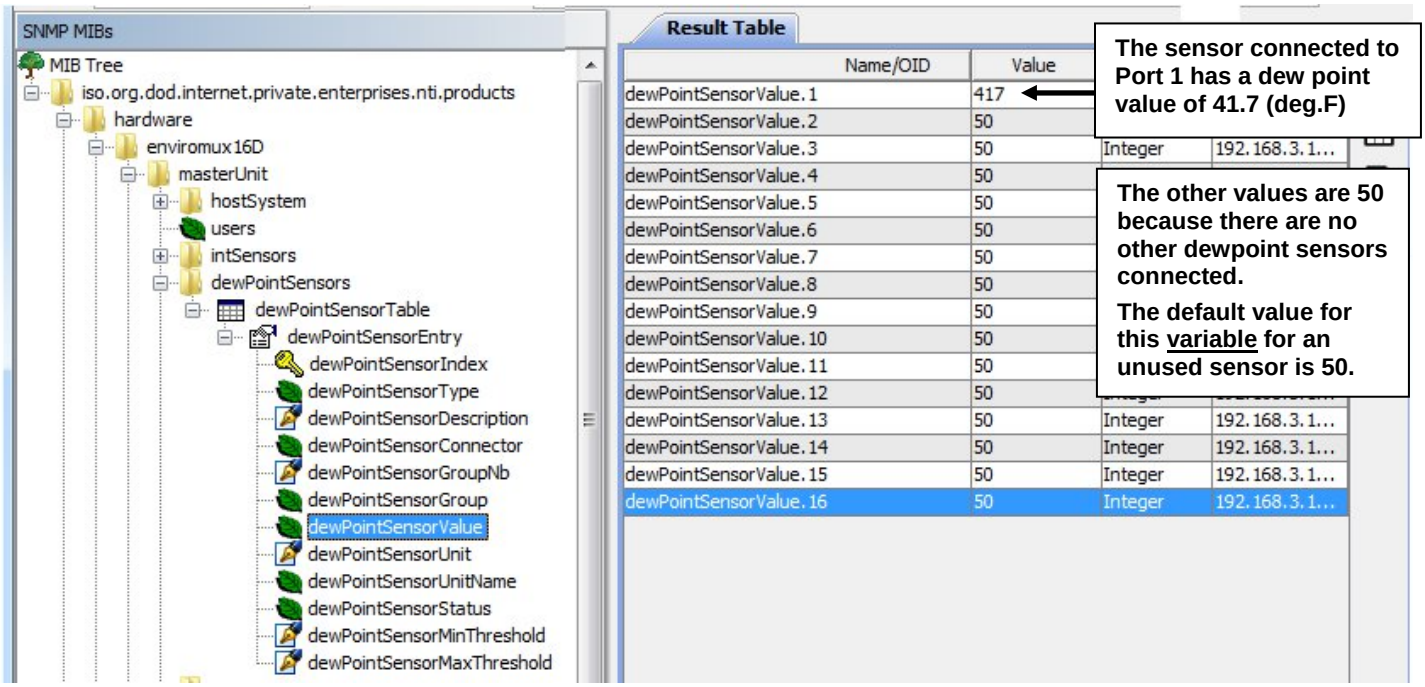
The operation can be selected with a right click (above), or using the "Operations" field (below). Once selected, press "Go"

Result Table

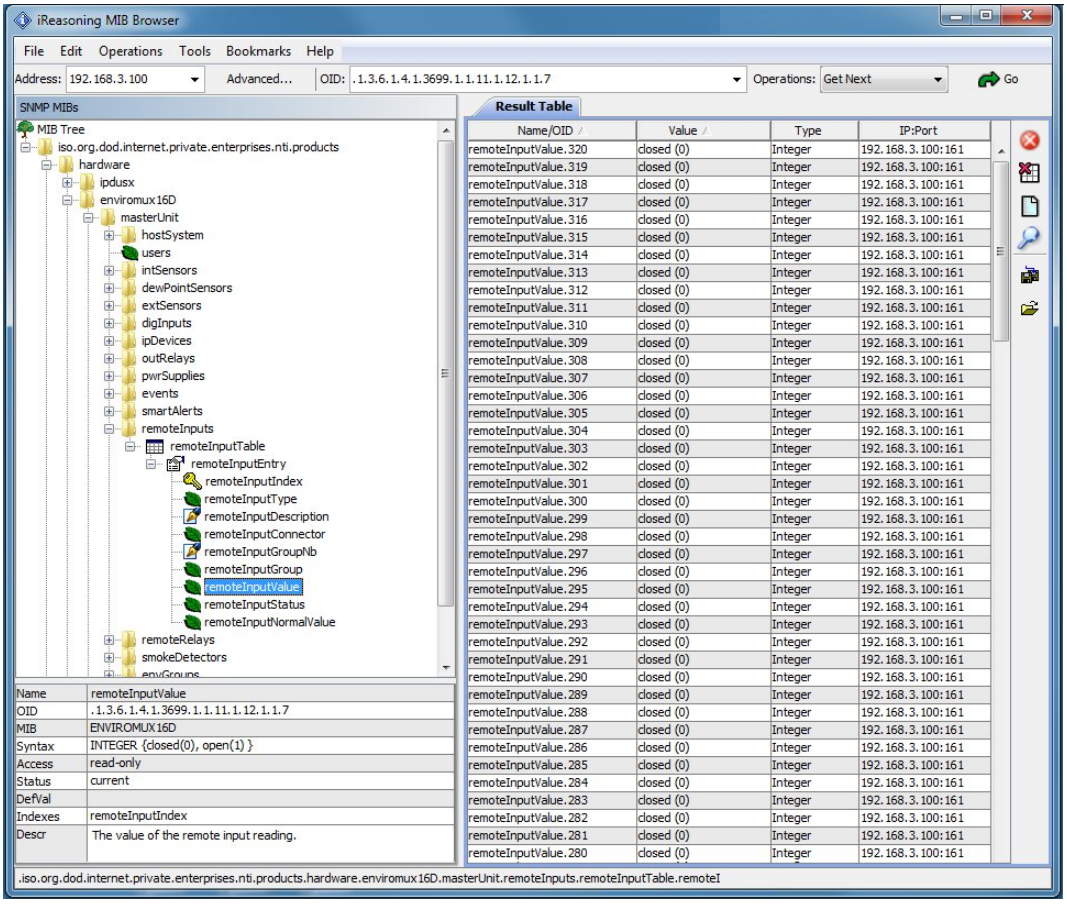


The value of each variable for the sensor can be listed separately.

The E-STHS-99 is a specialty sensor that provides a third piece of information (dew point) managed through an additional category with virtual ports named “dewPoint Sensors”.



The category remoteInputs and remoteRelays are reserved for identifying contact sensors connected through E-DI16DO16(R) expansion units. No remoteInputs are connected to this SYSTEM (the default value of the remoteInputValue is closed (0)).



USING SNMP TO ACQUIRE CPU/MEMORY USAGE DATA

You can use a MIB browser to acquire ENVIROMUX memory and CPU usage information (requires firmware version 2.16 or later). By loading the U.C. Davis MIB file "UCD-SNMP-MIB.mib" (copy found at http://www.net-snmp.org/docs/mibs/ucdavis.html) into your MIB browser, memory and CPU usage information for the operating system in the ENVIROMUX can be readily viewed.

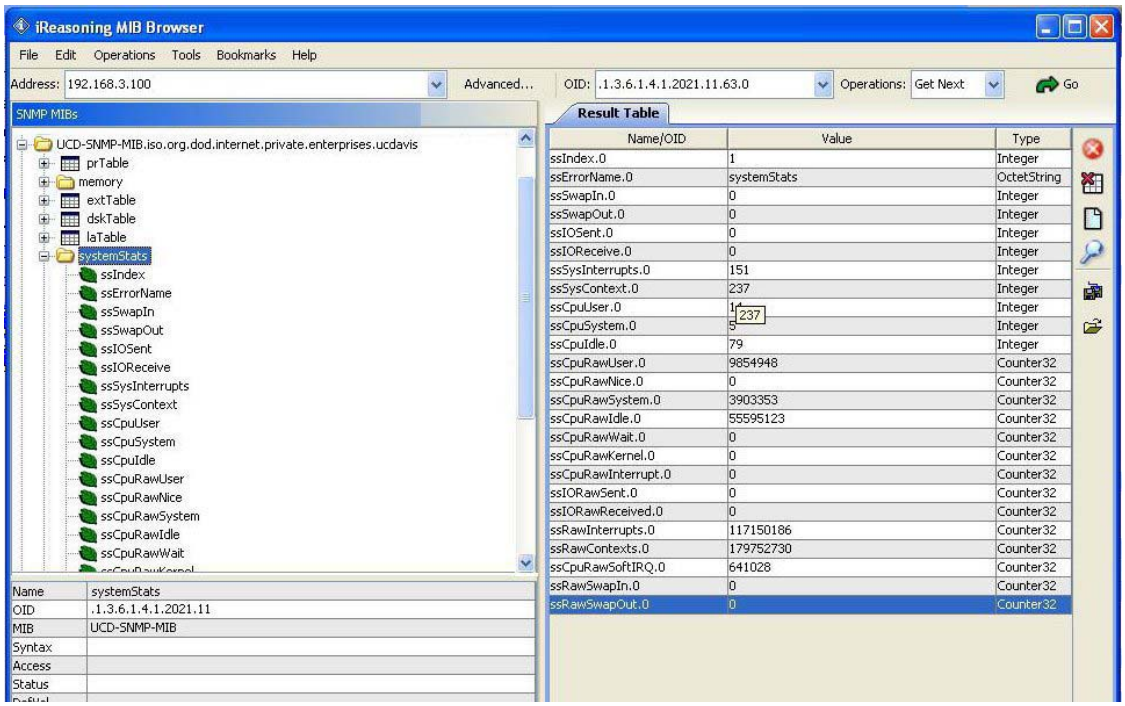


Figure 144- CPU Information found in the "systemStats" folder

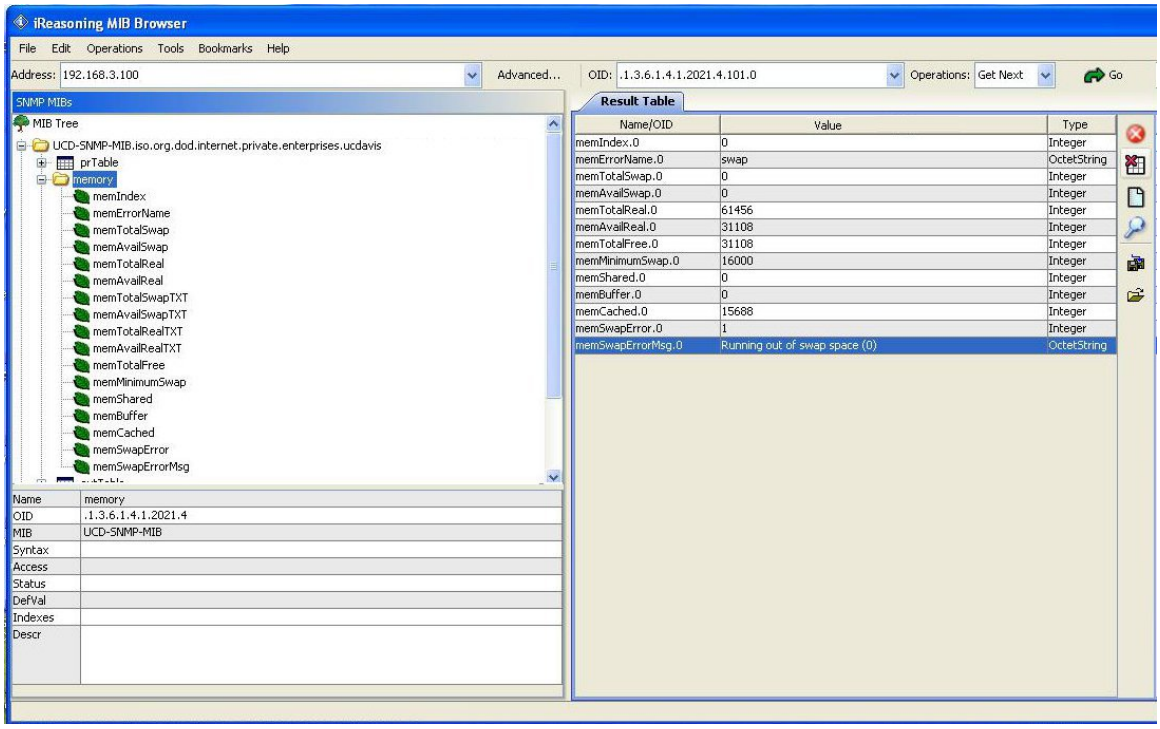


Figure 145- Memory usage information found in the "memory" folder

USING SNMP TO VIEW AND CONFIGURE SETTINGS

You can use a MIB browser to view System Information as well as view and change ENVIROMUX network settings (requires firmware version 2.53 or later).

To see System Information values, click on "masterUnit" under the ENVIROMUX model, then click on "hostSystem" , right click to open the menu and click on "Get Subtree".

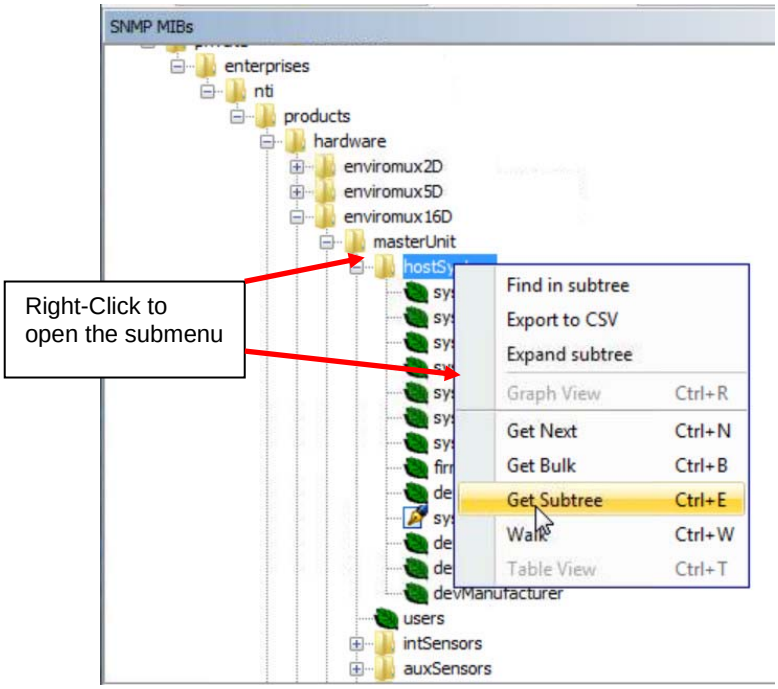


Figure 146- Get SNMP values for System Information

All the settings under System Information will be displayed.

Figure 147- System Information displayed in SNMP

From this, the user can change settings by right-clicking any property and clicking on "Set". Enter the desired value and click "OK" to make the change.

Note: When you select "Set" for "sysReset", you can cause the ENVIROMUX to reboot by changing the value to "1" and click "OK". The ENVIROMUX will immediately reboot. All connections to it will be lost.

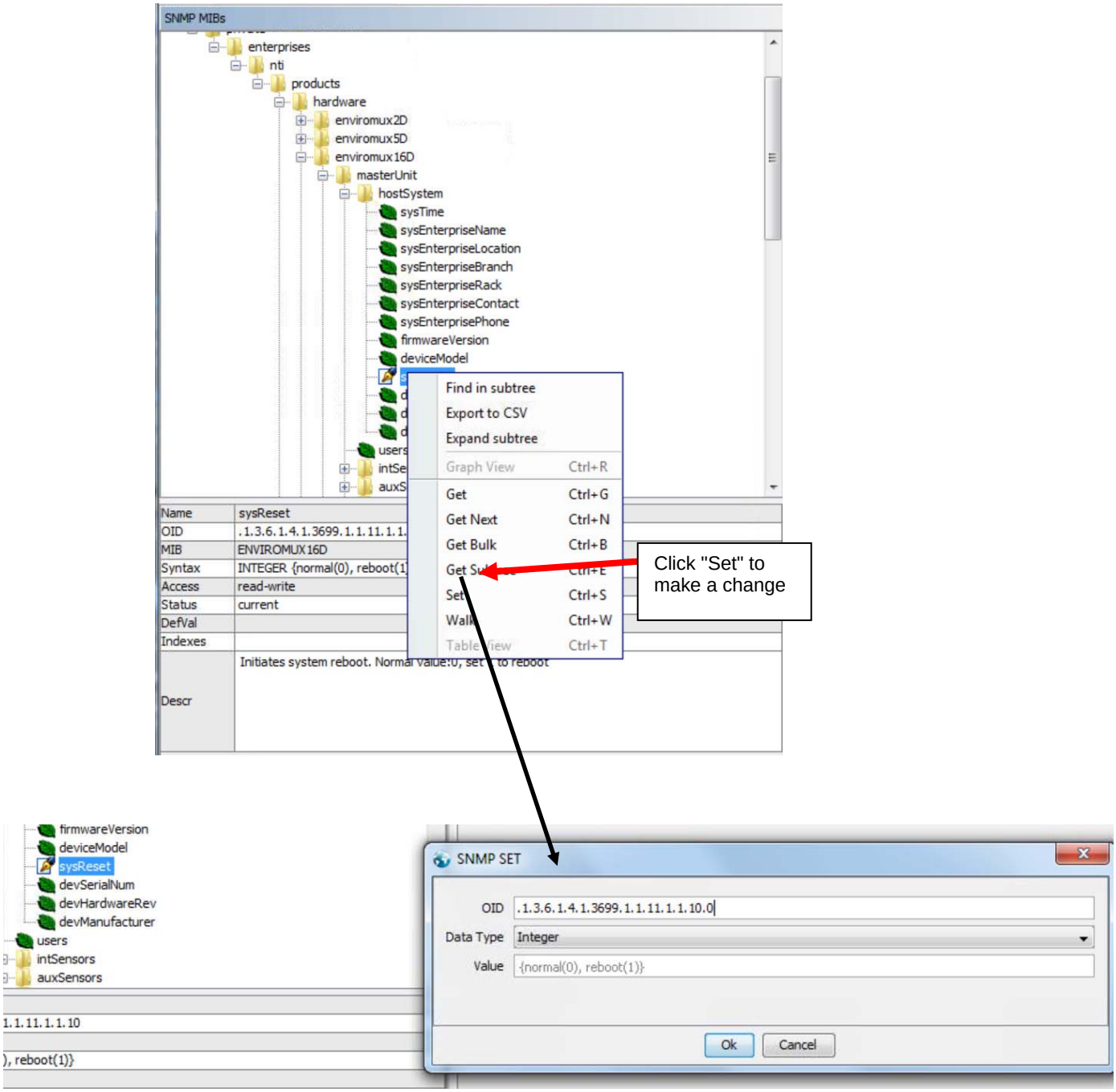


Figure 148- Use SNMP to reboot the ENVIROMUX

To view and change network settings, double-click "NetConfRegisters" from the SNMP MIBs tree.

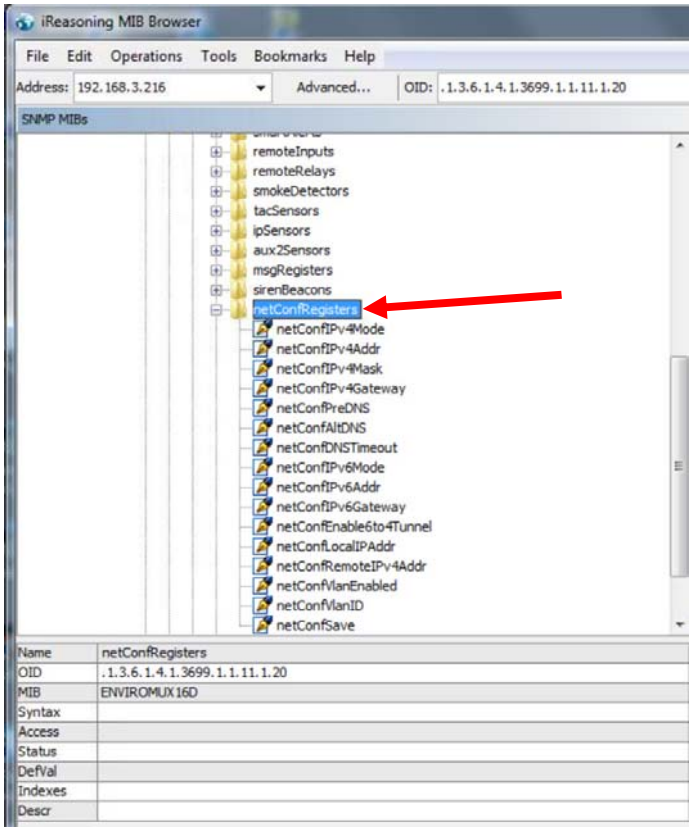


Figure 149- Network Configuration topics through SNMP

To view the current setting of any property, right click the topic and click "Get". The value for that property will appear in the Result Table.

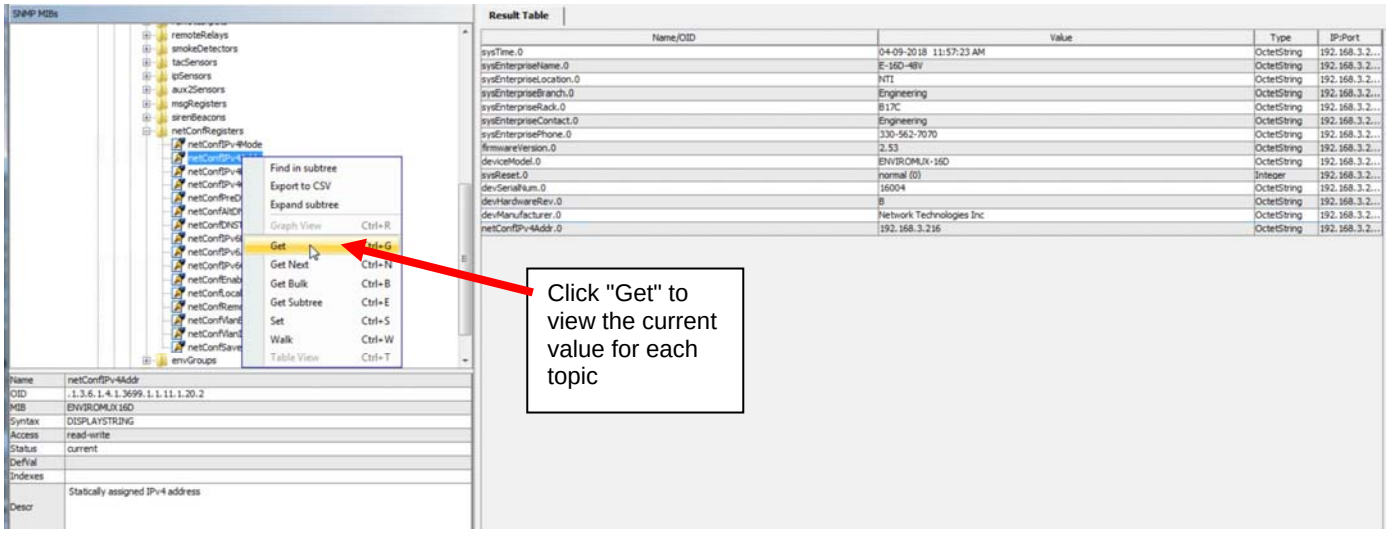
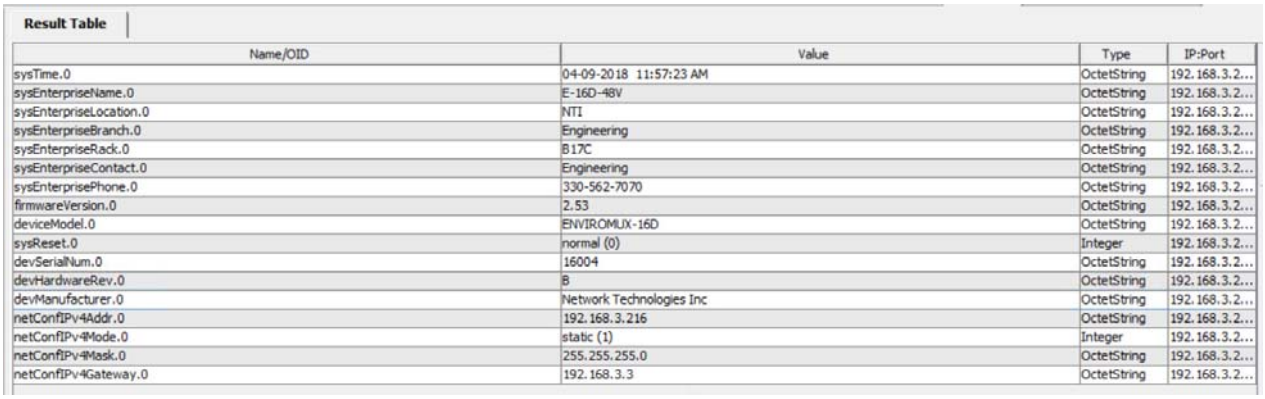


Figure 150- View Network Configuration settings in SNMP

To change a network setting, right click the topic and click "Set". In the window that pops up, enter the value that you want to change that topic to. Then click "OK". Repeat for each of the network settings to be changed.

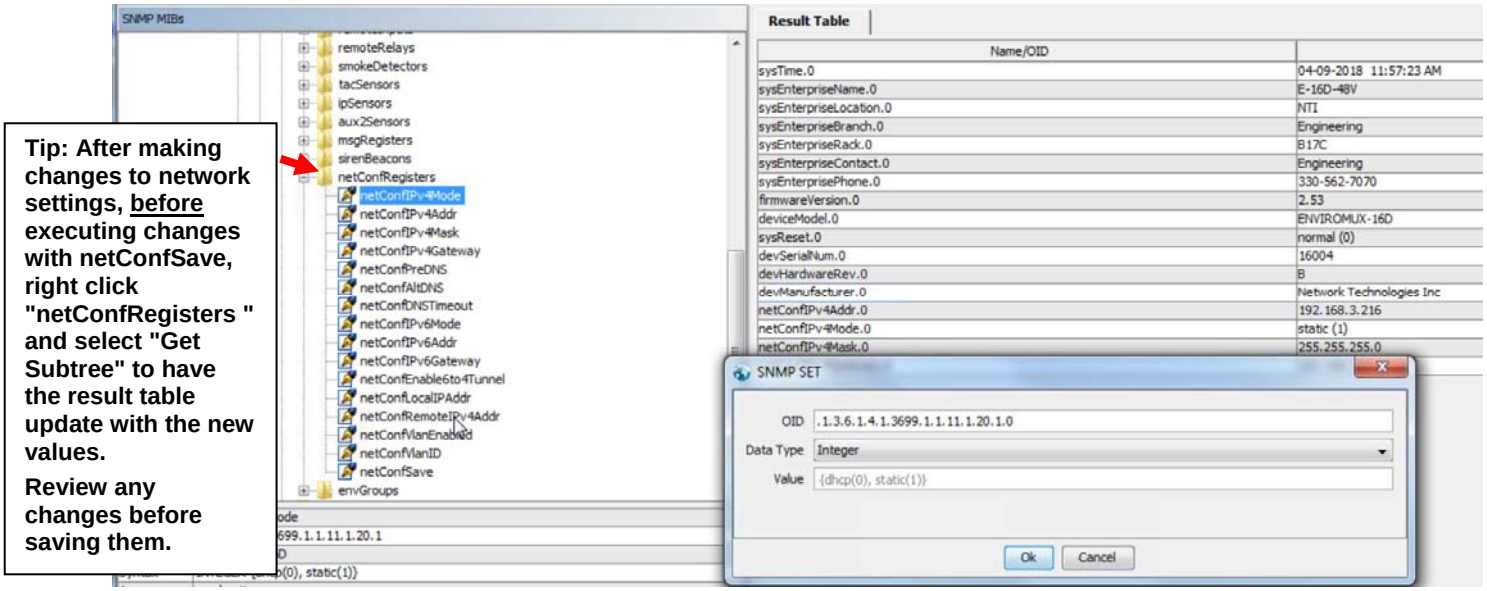
Note: Individual network setting value changes will not take immediate affect. Once you are done making all network setting changes, right click the topic "netConfSave", enter the value "1" and click "OK". All network settings changes made will now take immediate affect.



Result Table

Name/OID	Value	Type	IP:Port
sysTime.0	04-09-2018 11:57:23 AM	OctetString	192.168.3.2...
sysEnterpriseName.0	E-16D-48V	OctetString	192.168.3.2...
sysEnterpriseLocation.0	NTI	OctetString	192.168.3.2...
sysEnterpriseBranch.0	Engineering	OctetString	192.168.3.2...
sysEnterpriseRack.0	B17C	OctetString	192.168.3.2...
sysEnterpriseContact.0	Engineering	OctetString	192.168.3.2...
sysEnterprisePhone.0	330-562-7070	OctetString	192.168.3.2...
firmwareVersion.0	2.53	OctetString	192.168.3.2...
deviceModel.0	ENVIROMUX-16D	OctetString	192.168.3.2...
sysReset.0	normal (0)	Integer	192.168.3.2...
devSerialNum.0	16004	OctetString	192.168.3.2...
devHardwareRev.0	B	OctetString	192.168.3.2...
devManufacturer.0	Network Technologies Inc	OctetString	192.168.3.2...
netConfIPv4Addr.0	192.168.3.216	OctetString	192.168.3.2...
netConfIPv4Mode.0	static (1)	Integer	192.168.3.2...
netConfIPv4Mask.0	255.255.255.0	OctetString	192.168.3.2...
netConfIPv4Gateway.0	192.168.3.3	OctetString	192.168.3.2...

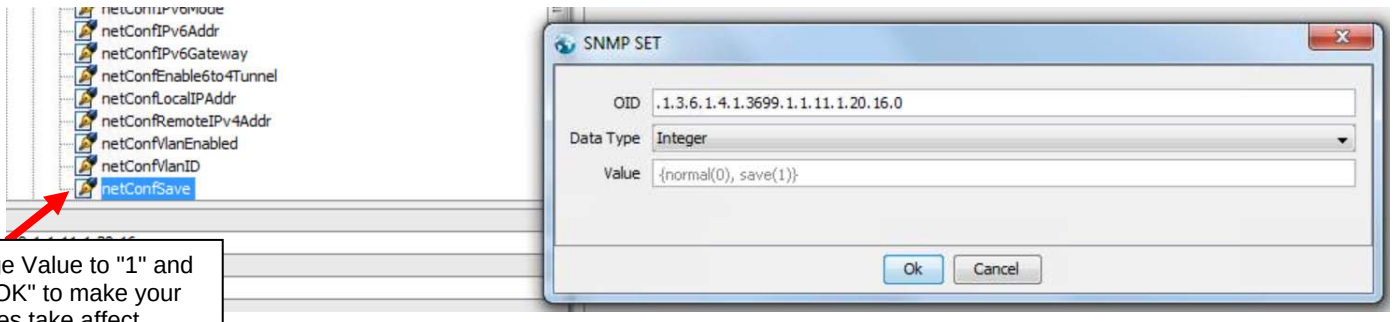
Figure 151- SNMP-Present Network Configuration



Tip: After making changes to network settings, before executing changes with netConfSave, right click "netConfRegisters " and select "Get Subtree" to have the result table update with the new values.

Review any changes before saving them.

Figure 152- Que up changes to Network Settings



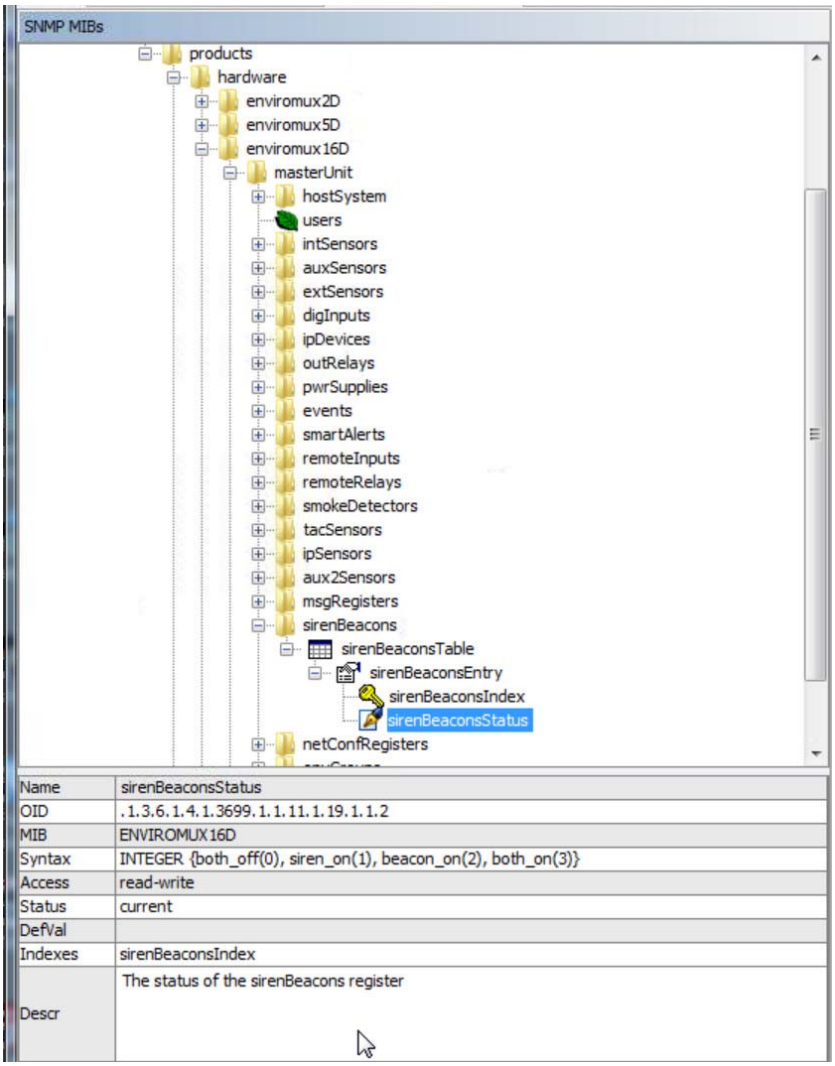
Change Value to "1" and click "OK" to make your changes take affect.

Figure 153- Save and execute changes made to network settings

USING SNMP TO CONTROL SIREN AND/OR BEACON

You can use a MIB browser to toggle the siren and beacon ON and OFF. (requires firmware version 2.52 or later).

To see the siren and beacon entries, click on "masterUnit" under the ENVIROMUX model, then click on "sirenBeacons" , double-click to open the subtree.



To see status, right click "sirenBeaconsStatus" to open menu, and click on "Get Next".
The status will show up in the results table to the right.

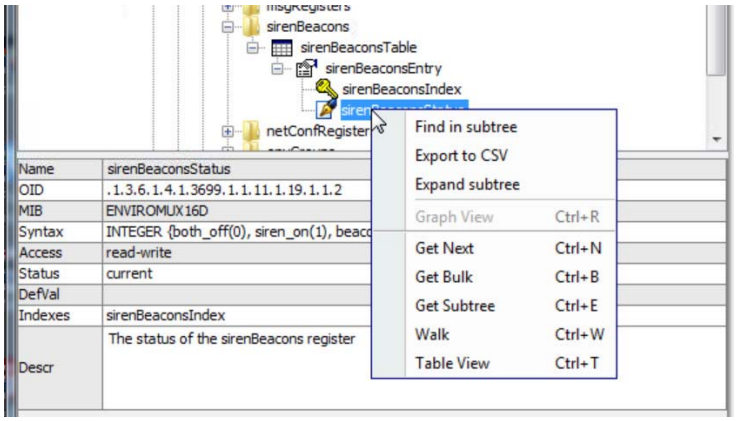


Figure 154- Siren and Beacon status viewed from MIB browser

In the results table, right-click "sirenBeaconStatus.1" to open menu. Click "Set" to see window where the settings of the Siren and Beacon can be changed.

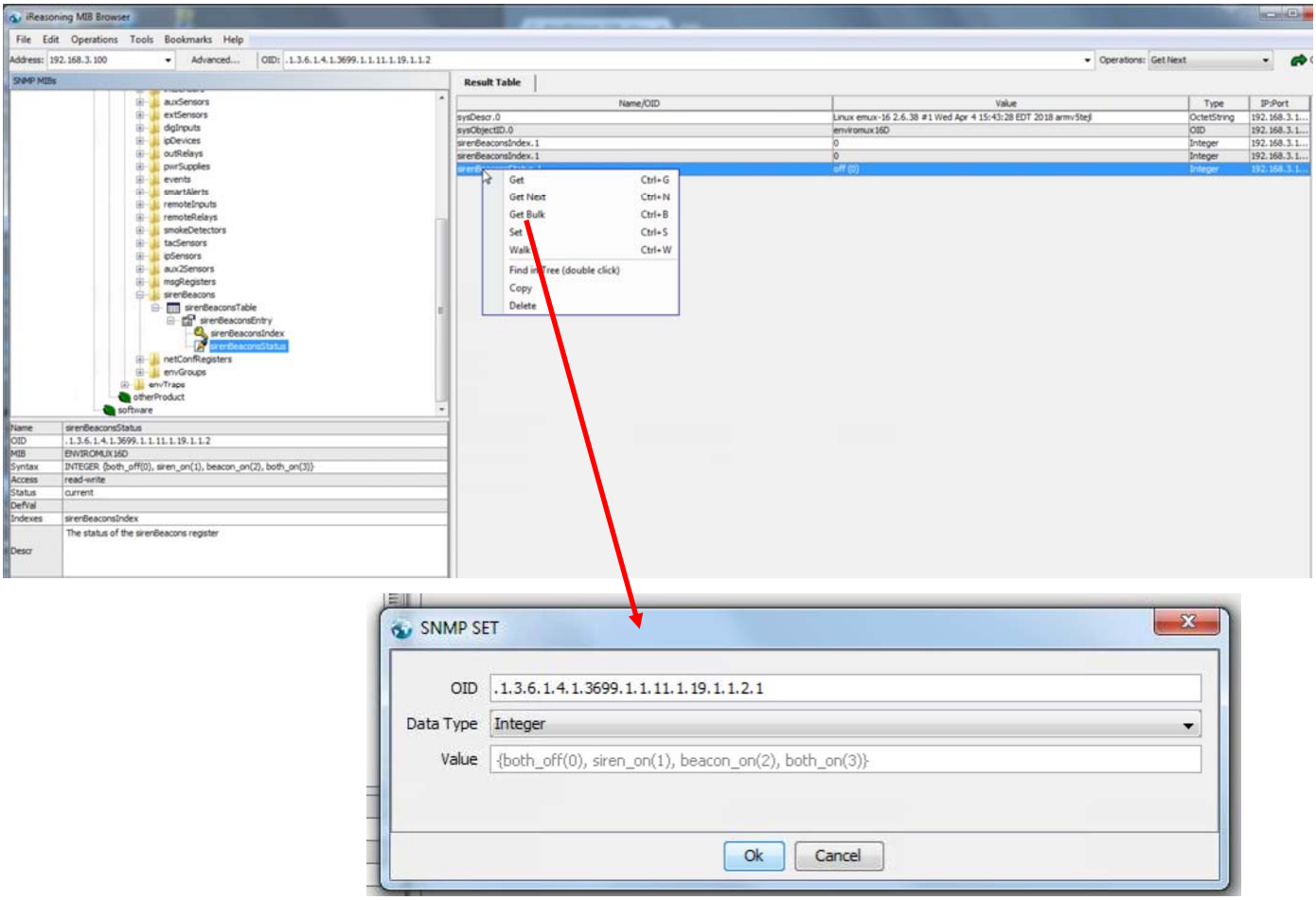


Figure 155- Control Siren and Beacon operation from MIB browser

Enter a value of 0 to turn both OFF
1 to turn the siren ON
2 to turn the beacon ON
3 to turn both the siren and beacon ON

Then click OK to execute the change. The change will have immediate affect.

SHUTDOWN WINDOWS SERVER USING REMOTE SSH COMMAND

Following the steps outlined below, a Windows server can be shutdown automatically by the ENVIROMUX SYSTEM.

Cygwin Method

1. Setup a user account on the Windows PC named “root” (must be all lower case) and make sure user “root” has administrative privileges.

2. Install an SSH server on the Windows PC. (We used Cygwin for our test. We found instruction on Oracle for installation that was very helpful http://docs.oracle.com/cd/E24628_01/install.121/e22624/preinstall_req_cygwin_ssh.htm).

3. Setup a user account in your SSH server named “root”.

4. Check to make sure the SSH configuration file has RSA authorization enabled and if not, edit the SSH server configuration file to enable it (in cygwin the file was found at c:\cygwin64\etc\sshd_config). Other SSH servers might have different configuration filenames.

5. Download the RSA Public Key (page 62) to the Windows computer. The downloaded file will have the default name **`id_rsa.pub`**.

6. Create a directory in the SSH server directory called “/home/root/.ssh” (i.e. `c:/cygwin64/`**`home/root/.ssh`** and don’t forget to put the period before the “ssh”).

7. On the computer to take the command, logged in as root, from the directory where the file was downloaded, type the command:

$ **`cat id_rsa.pub >> /home/root/.ssh/authorized_keys`**

8. Then, to make the change take effect, restart the SSH server. To do this, **right** click on “Computer” (in the Start Menu) and click on “Manage”. Locate the SSH server in the list of Services and select it. Then click on “Restart”.

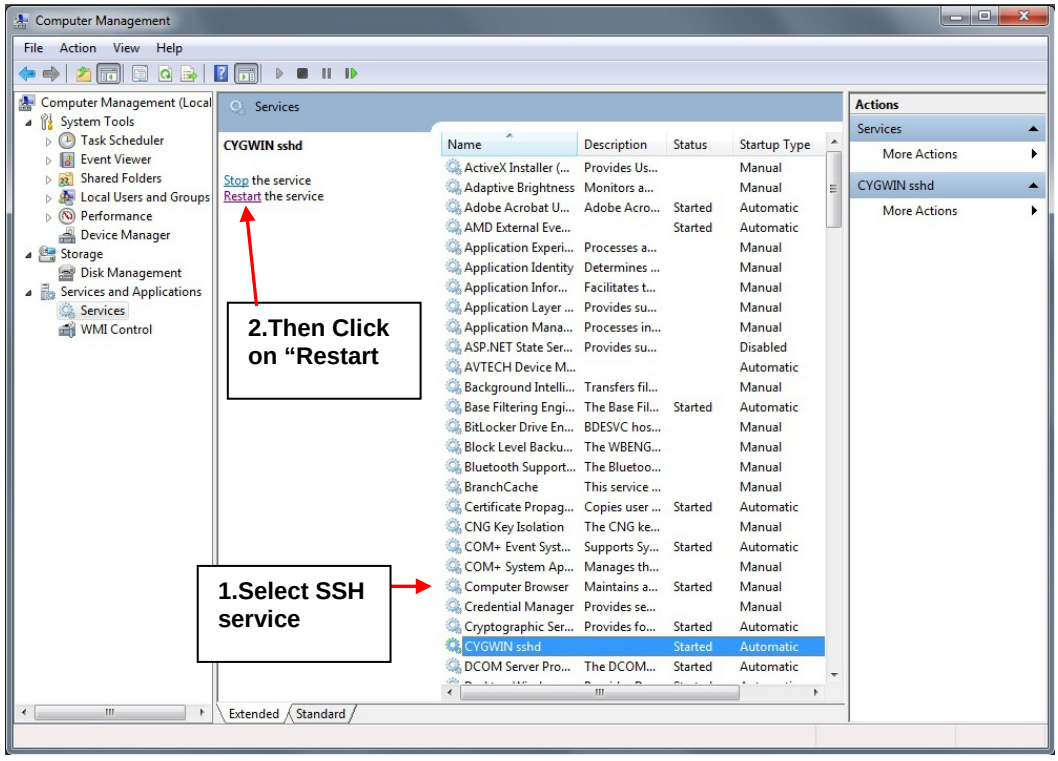


Figure 156- Restart CYGWIN service

9. Configure a Smart Alert to include an Event that will be used to trigger the shutdown of the Windows Server (page 94).

10. Within the Event configuration, apply the address of the Windows Server as the “Remote Address”, place a checkmark in “Enable command on event triggered” and add a command to be executed as a Remote SSH command under ”Command on triggered”. (We used “shutdown –s” but there are more possibilities (http://technet.microsoft.com/en-us/library/cc780360%28v=ws.10%29.aspx).

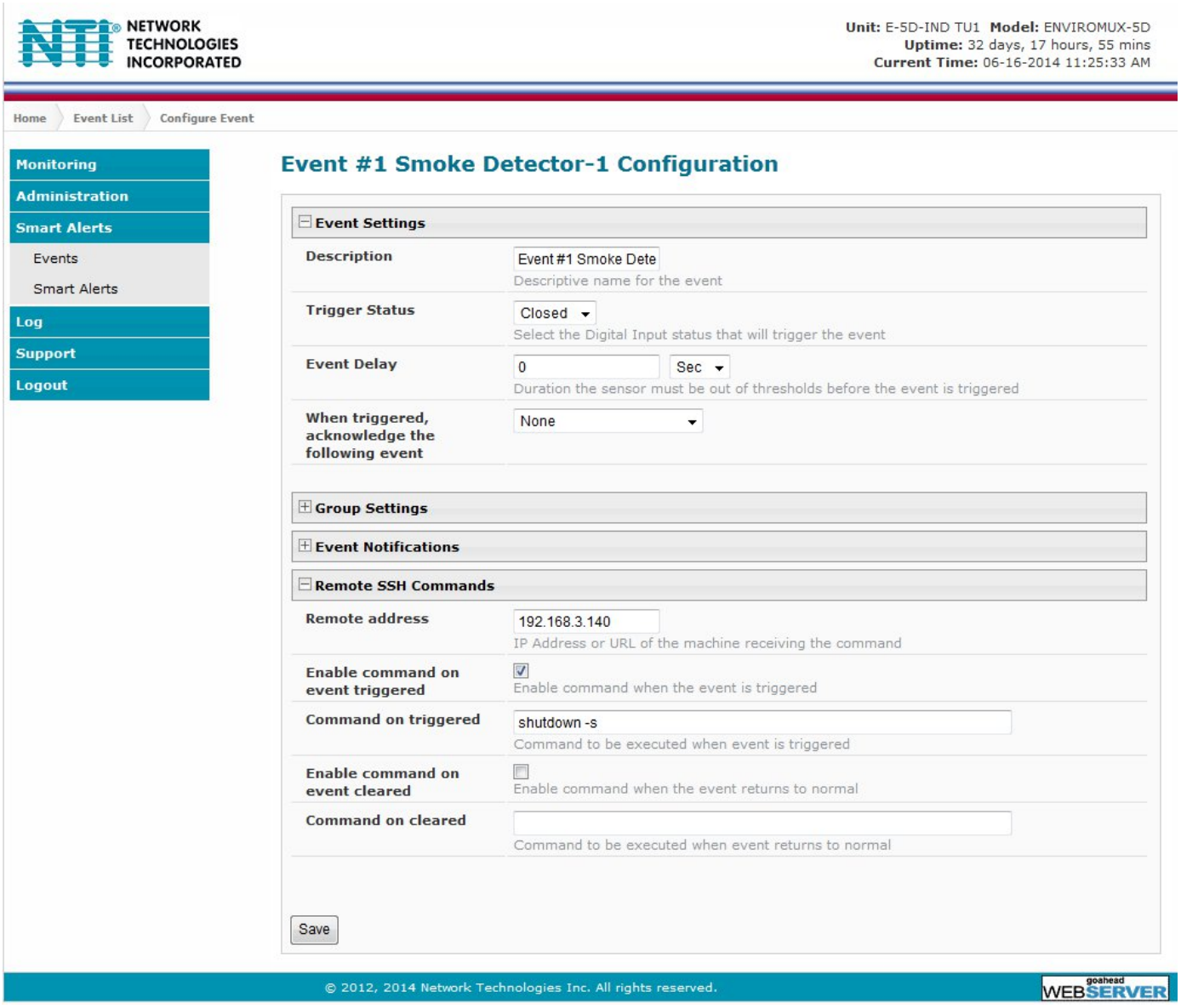


Figure 157- Configure Event for remote shutdown

10. Be sure to click “Save” when finished.

OPEN SSH Method

1. Setup SSH server on Windows machine with public key access. If this procedure is already done, skip to step 2
   a. We are using OpenSSH for windows to setup SSH server. Any SSH server compatible for your Windows OS can be used.
   b. Please install SSH to the location as in below link and execute the commands to setup SSH server and Setting up Public Key Authentication.
      https://winscp.net/eng/docs/guide_windows_openssh_server
      https://winscp.net/eng/docs/guide_public_key
   c. Make sure you can start the SSH service listed in your windows services list (services.msc application).
   d. Troubleshooting:

      * During execution of SSH setup commands if you receive syntax error for

```
powershell.exe -ExecutionPolicy Bypass -File .\FixHostFilePermissions.ps1 -Confirm:$false
```

please use the below command instead:

```
     powershell.exe -ExecutionPolicy Bypass -File .\FixHostFilePermissions.ps1
```

      * During startup process if you receive error related to a permission issue, please make sure LOCAL SERVICE is added to “Replace a process level token”. If not it can be added by opening the application secpol.msc -> Local Policies -> User Rights Assignment -> 'Replace a process level token' as mentioned in below link.

      https://social.technet.microsoft.com/Forums/en-US/419ba006-4413-4036-8c49-252b08593131/service-fails-to-start-error-1297-and-7000?forum=winserverDS

2. Add E-xD user to Windows SSH service user list.
   a. E-xD logs in as user root. If you do not have a 'root' user on the PC add this user by going in to Control Panel -> Manage User Accounts -> 'Advanced' tab -> Advanced -> Right click on User and add New User as shown in root_user.jpg. User password can be anything you wish as this is not used by the E-xD.

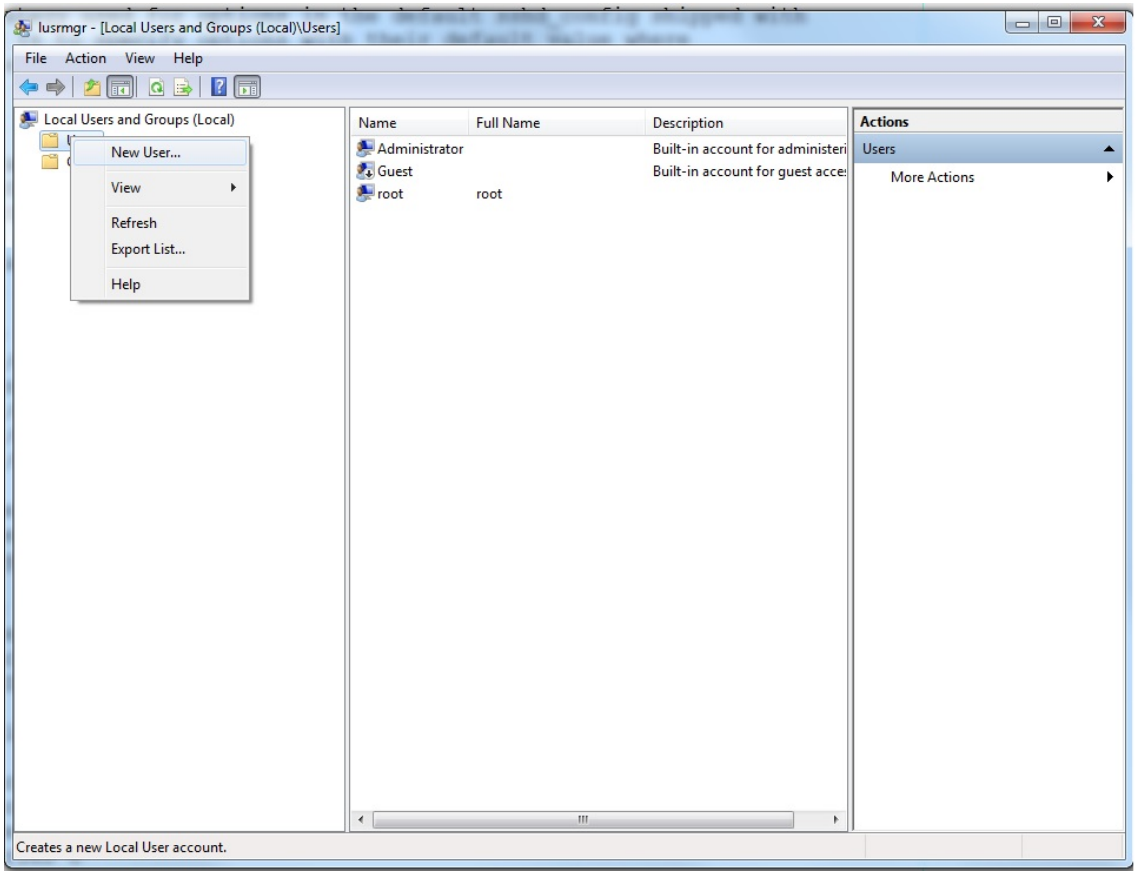


Figure 158- Add user "root" to PC

b. Download RSA public key from E-xD as shown in Figure 159 and rename the file to 'authorized_keys'. Place this file into the following path:

`C:\Program files\OpenSSH\ssh\authorized_keys`

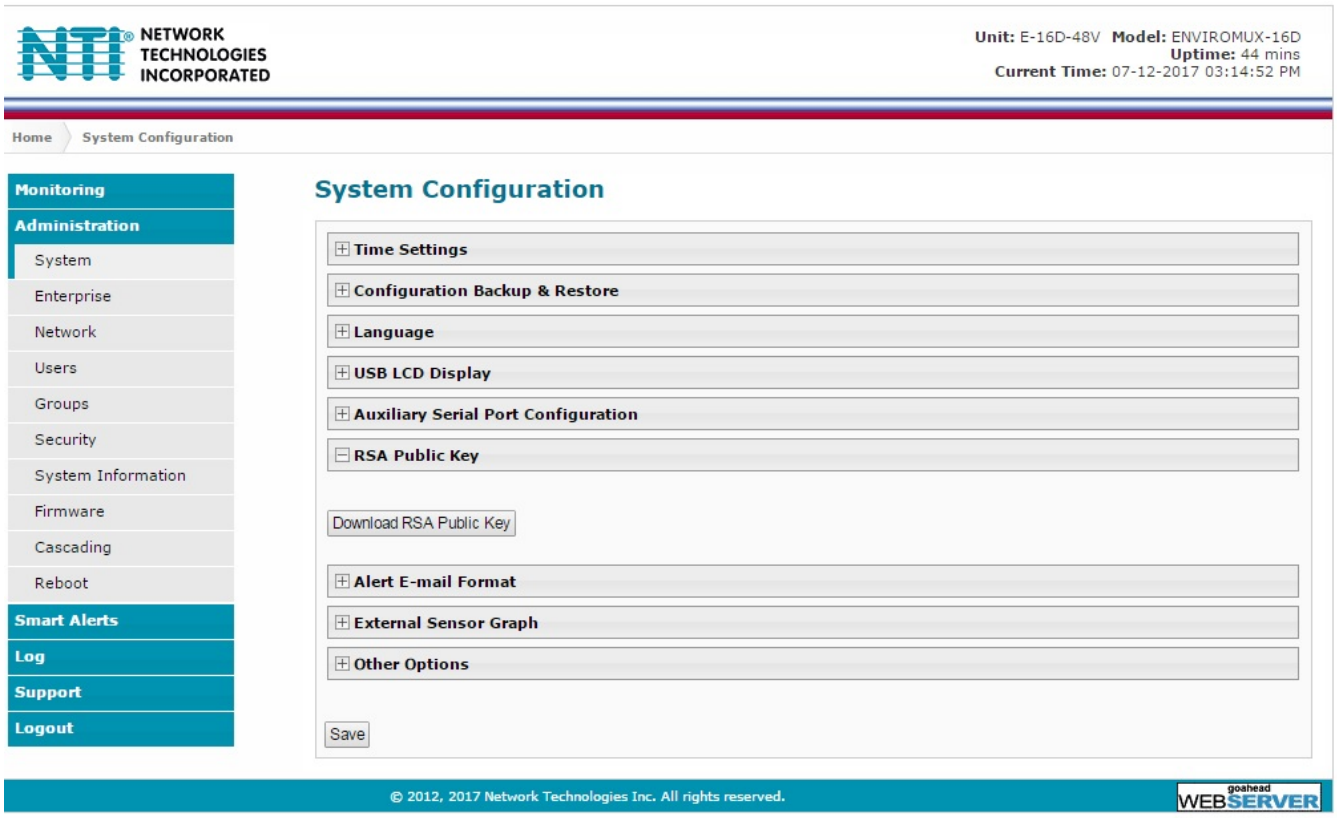


Figure 159- Download RSA Public Key

c. The permissions on this file needs to be limited to the user running SSH service. If not please disable Strict Mode in sshd_config file as shown in Figure 160. Please make sure the path of public key and pid file is correct and accessible by SSH service.

```
# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

# The default requires explicit activation of protocol 1
#Protocol 2

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
LogLevel DEBUG3

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
StrictModes no
#MaxAuthTries 6
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile  "C:\Program Files\OpenSSH\.ssh\authorized_keys"
PidFile "C:\Program Files\OpenSSH\logs\sshd.pid"
```

Figure 160- sshd_config file

d. To troubleshoot any errors please set log level to DEBUG3 as shown in the image above.

3. Setup of SSH command on E-xD:

a. To test, try logging into windows machine using any user and password. You can also try testing public key authentication by generating your own SSH key and adding its rsa key to the authorized_keys file.

b. Any windows commands can be executed on Windows machine through E-xD. To shutdown, add an event with remote SSH command 'shutdown -s' as shown in Figure 161. Shutdown parameters like timeout can be configured as described in the link below:

https://technet.microsoft.com/en-us/library/bb491003.aspx

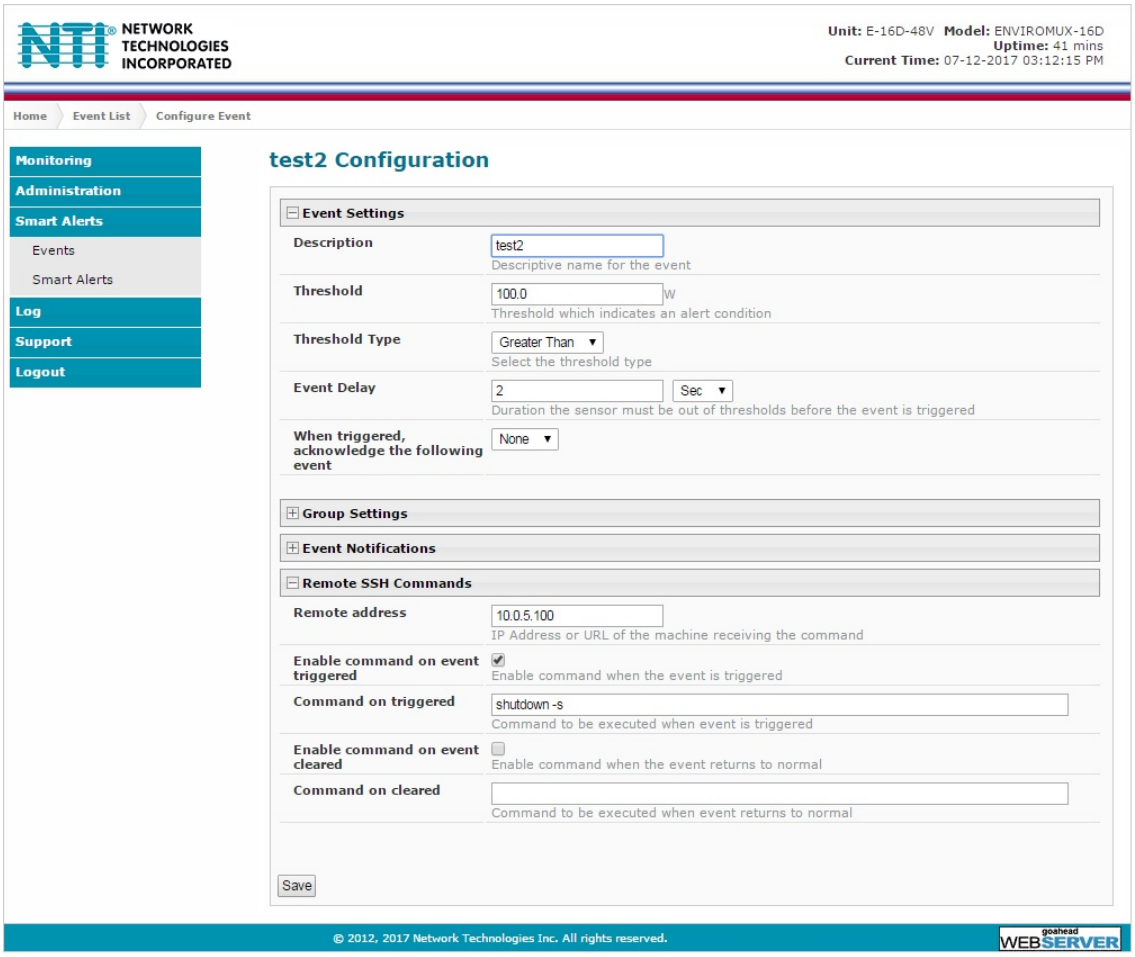


Figure 161- Configure Event for Remote SSH Command

c. To troubleshoot any issues please check event log on E-xD which should show a message if there was any error. Also SSH logs will be helpful to fix an issue.

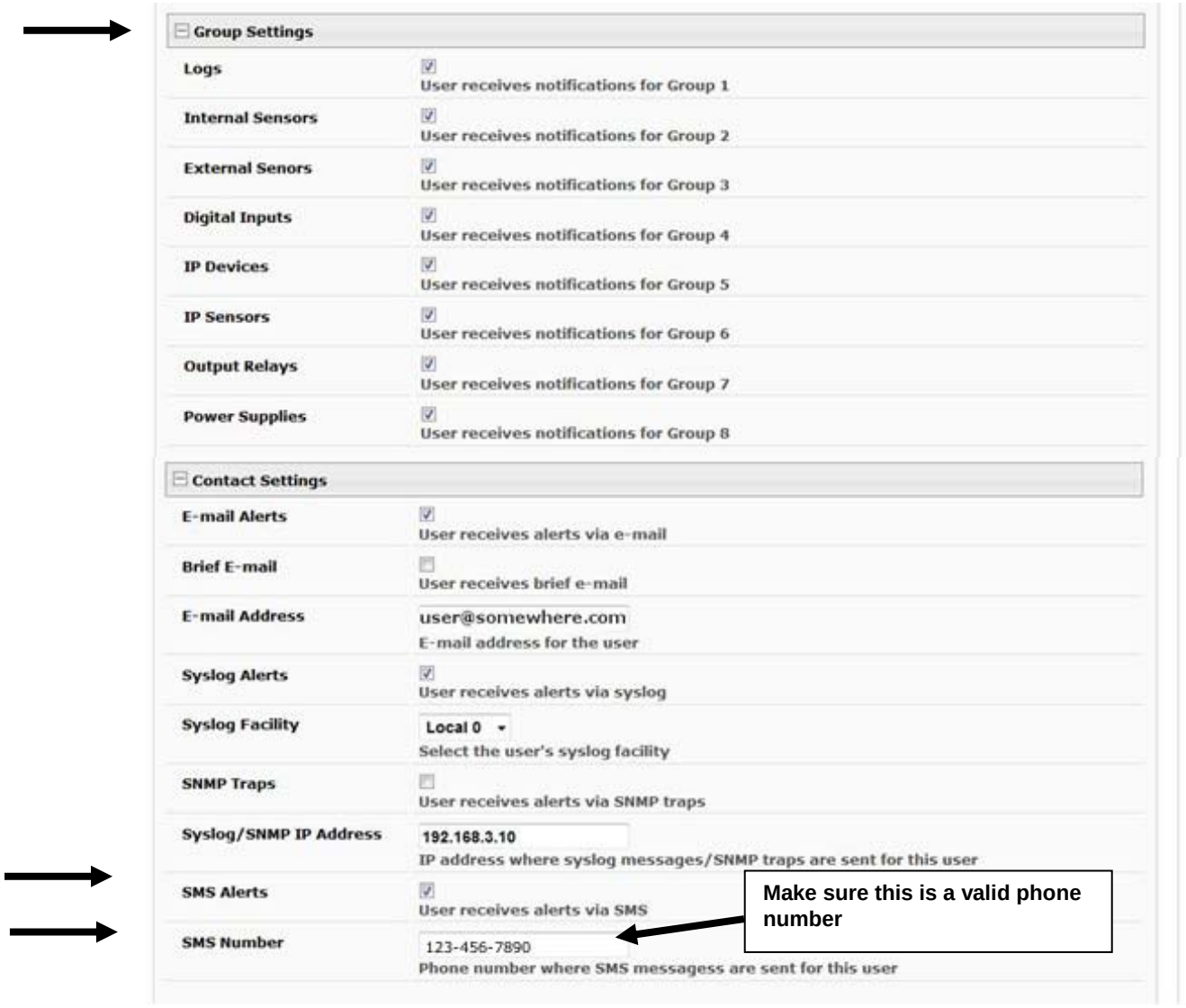
SETUP AND TEST SMS MESSAGING

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 other parts of this manual.

1. Install a USB modem as directed on page 17.

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.

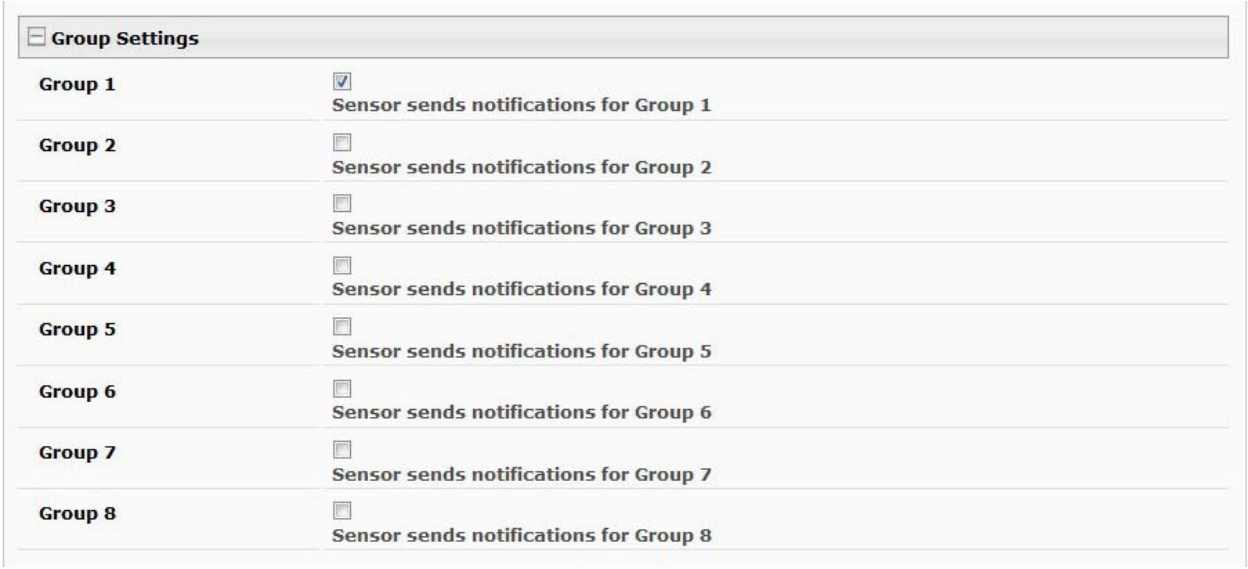
Also make sure that user is set to receive messages from the type of sensor causing the message to be sent. Make sure enough boxes are checked under "Group Settings." .



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

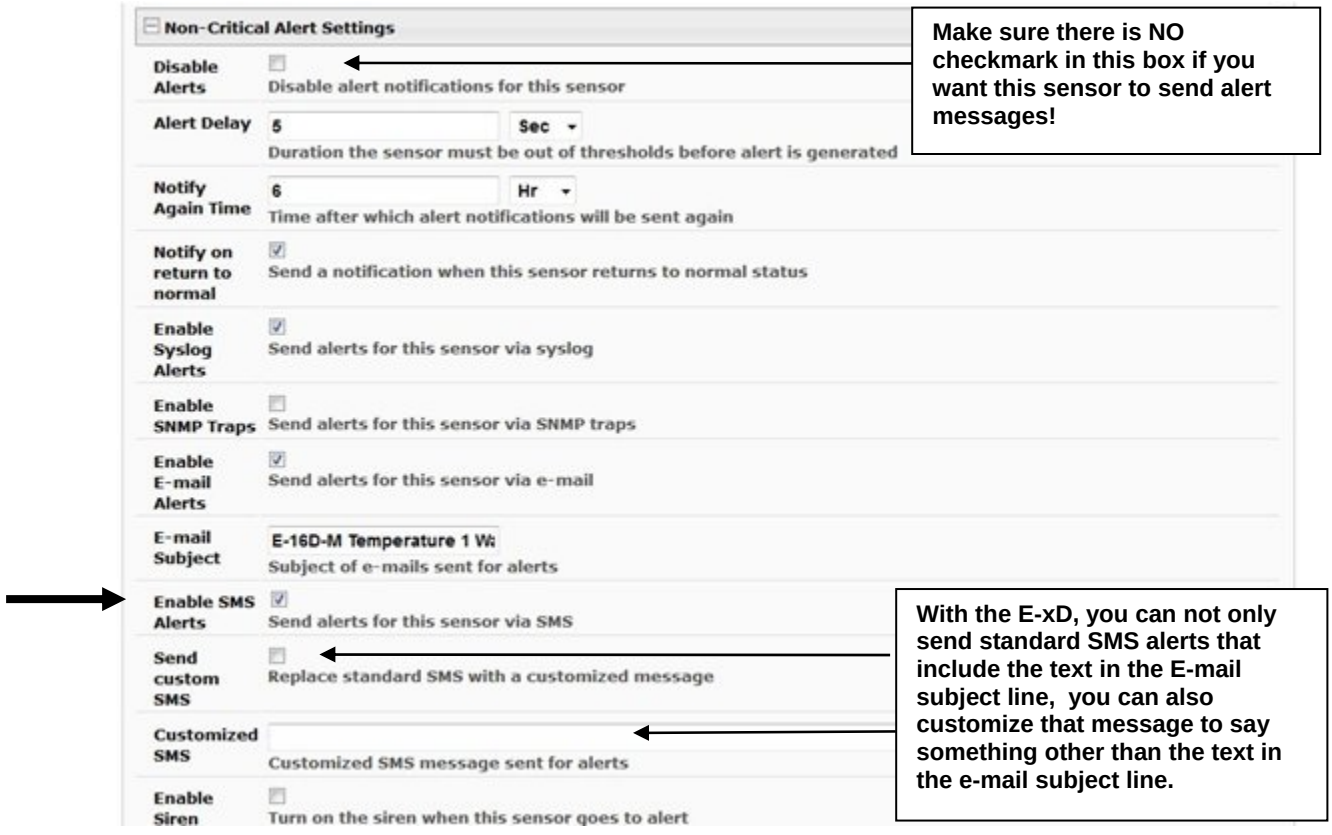
3. Configure a sensor to send alerts via SMS messaging. These settings can be found under Sensor Configuration on page 81.

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.



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

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.

The web interface for the E-xD includes a button that simulates an alert message being sent. This is found under the sensor configuration for each sensor.

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 (see page 64).

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.

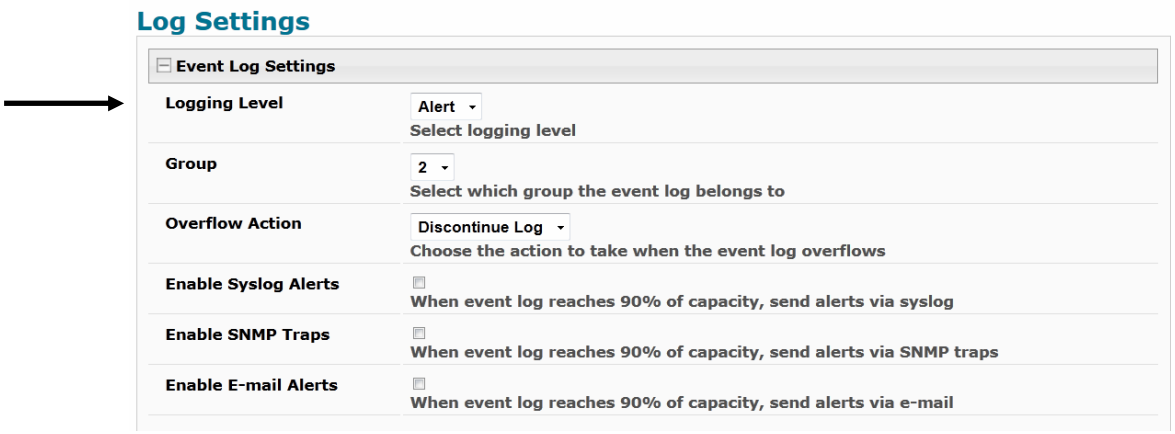
No Modem Installed

Modem properly installed in an E-xD (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).

CMS Error Codes

With E-xD units, there is also a feature under Log Settings for setting the Logging Level. Try setting the Logging Level to "Debug", and test the SMS messaging again. If the SMS message does not work, check the event log for an error code. "CMS error #500" for example, might show up. Perform a web search on the error code to investigate the possible cause ("SIM card inactive") for example.



Log Setting configuration in E-xD

SMS RELAY VIA SNMP

The ENVIROMUX has the ability to send an SMS text message via SNMP using the ENVIROMUX as a relay (applies to ENVIROMUX firmware version 2.51 and later). The ENVIROMUX must have a GSM modem installed (page 17).

1. From within your SNMP browser, click on **msgRegisters** ->**msgRegisterDescription**.

2. Right click **msgRegisterDescription1** and select SET.

3. Under Value, enter the number of phone numbers to send the text message to (up to 4 different numbers), enter the phone numbers to be called (no hyphens), and enter a text message up to 160 characters in length. Each piece of information must be separated by a "#" sign.

Example:

#number of phone numbers (1-4)#phone number#next phone number#text message to be sent

#2#3305627070#3305622622#SMS SAMPLE MESSAGE

Note: If your Log Settings are set to Debug (page 107), when a text message is sent, a record of it being sent will be logged.

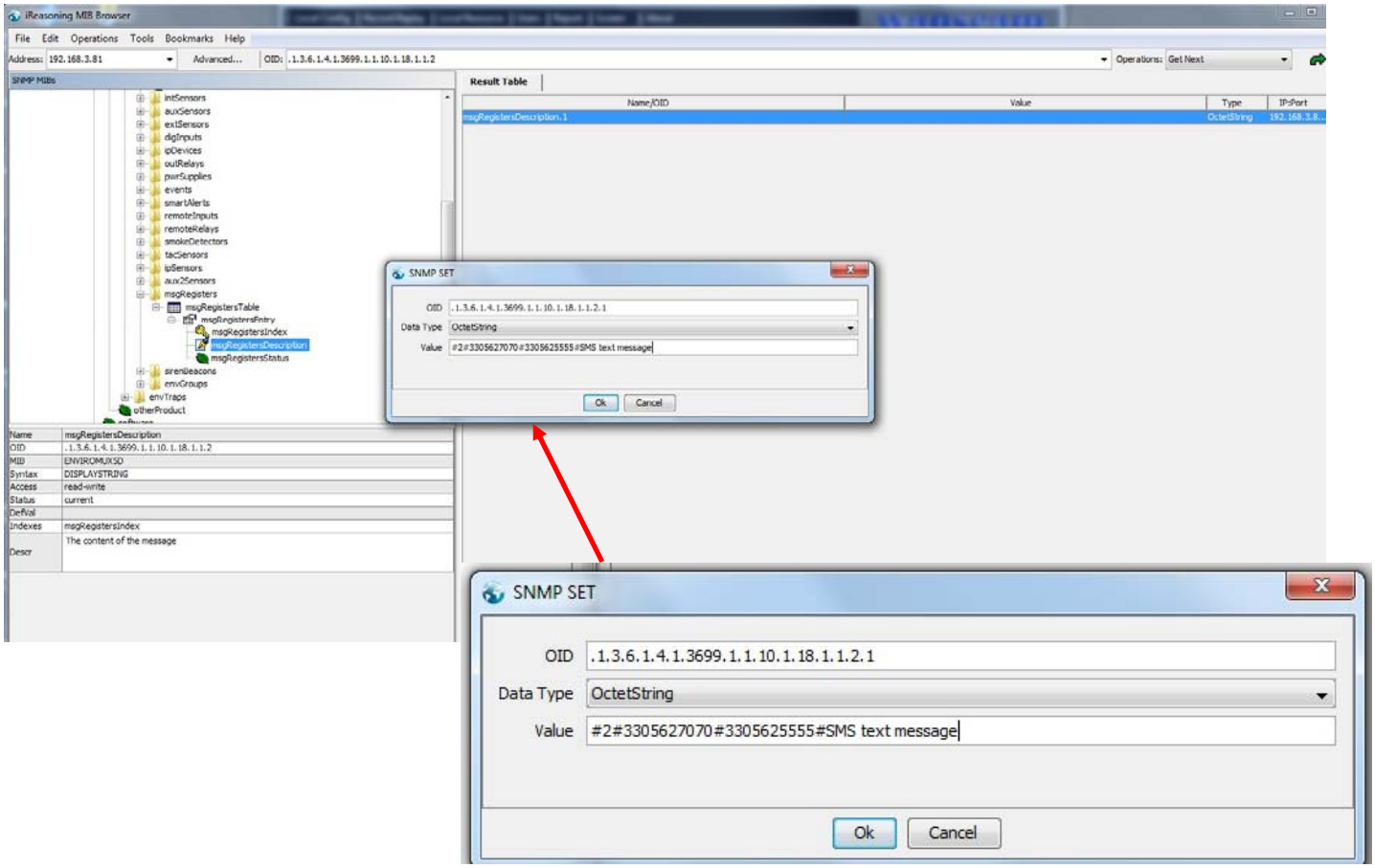


Figure 162- Use SNMP as SMS Relay

E-16D SPECIFICATIONS

Front Panel Interface

LEDs.....Green – Power, Solid for Main power, flashing for Backup power
.....Red – Low Bat (solid for charging battery, blinking for fault)
.....Green – Check Log
.....Green – AUX (not used)
.....Red – Internal Sensor Alert
.....Red – External Sensor Alert
USB.....USB Type A Female X2, USB 2.0 Full Speed compatible

Buttons.....Alarm Test/Silence- momentary switch
..... Restore Defaults- momentary switch
..... System Reset- momentary switch

RJ45 Sensor Inputs

Connector .....RJ45 connector
Voltage Supply.....5VDC and 12VDC
Signal Type.....RS485 for RS485 sensors; 2-wire for contact sensors
Max. Cable Length.....1000 FT
ESD Protection .....IEC 61000-4-2
Fuse Protection.....Resetable poly fuse – 500mA hold, 1A trip; 15VDC max. One fuse shared by ports 1-8, another fuse shared by ports 9-16. .

Digital Inputs

Connector .....Detachable terminal block-plug-in, 8 x 4 contacts
Wire Range.....16-26 AWG
Max. Input Voltage.....25VDC
Max. Contact Resistance.....1K Ohm
Auxiliary Voltage Supply .....12VDC+/-10%
Max. Current Supply .....**50 mA** (terminals 1-7) **350mA** (terminal 8 **only**)
ESD Protection .....IEC 61000-4-2
Fuse Protection.....Resetable poly fuse – 200mA hold, 400mA trip; 16VDC max. One fuse shared by 2 ports

Output Relays

Connector .....Detachable terminal block-plug-in, 4 x 3 contacts
Wire Range.....16-26 AWG
Output Type .....Dry contact, relay isolated
Output Rating.....1A / 30 VDC, 0.5A / 100VAC
Contact Resistance.....20 milliohm
ESD Protection .....No, Relay Isolated.
Fuse Protection.....Non-resetable, 2A Hold, 4A trip, 125V

Warning: The digital output relay contacts are not to be connected directly to AC mains wiring.

Beacon Port & Siren Port

Connector .....Detachable terminal block-plug-in, 1x2 contacts
Wire Range.....16-26 AWG
Voltage Output.....12VDC+/-10%
Current Output 180mA
ESD Protection .....IEC 61000-4-2,
Fuse Protection.....Resetable poly fuse – 200mA hold, 400mA trip; 16VDC max.

USB Device Ports

Connector.....USB Type A Female
Version.....USB 2.0 Full Speed compatible

Control Serial Port “RS232”

Connector ..... RJ45 Female
Supported Signals ..... TXD, RXD, RTS, CTS, DTR, DSR
Baud Rate ..... max 115,200 bps
Data Format ..... 8 bits
Parity ..... odd, even or no parity
Stop Bits ..... 1, 2 stop bits
ESD Protection IEC1000-4-2

USB-Serial Port “Console”

Connector ..... USB Type B Female
Supported Signals ..... D+ ,D-
Baud Rate ..... max 115,200 bps
Data Format ..... 8 bits
Parity ..... no parity
Stop Bits ..... 1 stop bits
ESD Protection IEC1000-4-2

Auxiliary Power Port

Connector ..... Detachable terminal block-plug-in, 1x2 contacts
Wire Range ..... 16-26 AWG
Voltage Output ..... 12VDC+/-10%
Current Output 150mA
ESD Protection ..... IEC 61000-4-2
Fuse Protection ..... Resetable poly fuse – 200mA hold, 400mA trip; 30VDC max.

Ethernet Port

Connector ..... RJ45 Female
Connection Speed ..... 10/100 Base-T
Security ..... SSL
Supported Protocols ..... http, https, Telnet,SSH

Back-Up Battery

Type ..... Rechargeable Sealed Lead-Acid Battery
Voltage, Current Rating 12VDC, 2.9Ahrs
Battery Operational Time ..... 1 hr, fully loaded; 30 min. after ‘Low Bat’ LED illuminates
Battery Charging Time ..... 32 hrs (from fully discharged to fully charged).
Replaceable ..... Yes – can be replaced by authorized personnel only (NTI)

General Specifications

Power Input ..... 110/220VAC, 50 – 60 Hz, 45W
Operating Temperature ..... 32° -104°F (0-40˚C)
Operating Humidity ..... 17-90%RH, non-condensing
MTBF ..... 39,685 hours
Enclosure Size(WxDxH) ..... 1 RU metal enclosure (19 x 9.5 x 1.73 inches)

TCP/IP

Supported Browsers ..... IE, Netscape, Mozilla, Opera,Chrome
Network Configuration ..... Allows Static or Dynamic IP Configuration
Max Number of Email Addresses ..... 17; 1 per User Account + 1 for Administrator

E-5D SPECIFICATIONS

User Interface

LEDs.....Green – Power (solid when ENVIROMUX is powered ON)
.....Red – Fault (solid when any sensor is in alert)

RJ45 Sensor Inputs

Connector.....RJ45 connector
Voltage Supply.....5VDC and 12VDC
Signal Type.....RS485 for RS485 sensors; 2-wire for contact sensors
Max. Cable Length.....1000 FT
ESD Protection.....IEC 61000-4-2
Fuse Protection.....Resetable poly fuse – 1.1A (5VDC); 500mA (12VDC) One of each fuse shared by 5 ports.

Digital Inputs

Connector.....Detachable terminal block-plug-in, 5 x 2 contacts
Wire Range.....16-26 AWG
Max. Input Voltage.....25VDC
Max. Contact Resistance.....300K ohm
ESD Protection.....IEC 61000-4-2

Output Relays

Connector.....Detachable terminal block-plug-in, 2 x 3 contacts
Wire Range.....16-26 AWG
Output Type.....Dry contact, relay isolated
Output Rating.....1A / 30 VDC, 0.5A / 100VAC
Contact Resistance.....20 milliohm
ESD Protection.....No, Relay Isolated.
Fuse Protection.....Non-resetable, 2A Hold, 4A trip, 125V

Warning: The digital output relay contacts are not to be connected directly to AC mains wiring.

Alarm Port

Connector.....Detachable terminal block-plug-in, 1x2 contacts
Wire Range.....16-26 AWG
Voltage Output.....12VDC+/-10%
Current Output.....180mA
ESD Protection.....IEC 61000-4-2,
Fuse Protection.....Resetable poly fuse – 200mA hold, 400mA trip; 16VDC max.

USB Device Ports

Connector.....USB Type A Female
Version.....USB 2.0 Full Speed compatible

USB-Serial Port “Console”

Connector .....USB Type B Female
Supported Signals .....D+ ,D-
Baud Rate.....max 115,200 bps
Data Format.....8 bits
Parity.....no parity
Stop Bits .....1 stop bits
ESD Protection IEC1000-4-2

Auxiliary Power Port

Connector .....Detachable terminal block-plug-in, 1x2 contacts
Wire Range.....14-22 AWG
Voltage Output.....12VDC+/-10%
Current Output 500mA
ESD Protection .....IEC 61000-4-2
Fuse Protection.....Resetable poly fuse – 1.1A hold, 1.95A trip; 16VDC max.

Ethernet Port

Connector .....RJ45 Female
Connection Speed .....10/100 Base-T
Security.....SSL
Supported Protocols .....http, https, Telnet,SSH

General Specifications

Power Input.....120VAC or 240VAC at 50 or 60Hz-9VDC/3A AC Adapter
Operating Temperature.....32° -140°F (0-60˚C) / (-5DB model) 32° -104°F (0-40˚C)
Operating Humidity .....17-90%RH, non-condensing
MTBF.....170,344 / (-5DB model) 169,279 hours
Enclosure Size(WxDxH) .....7.9 x 3 x 1.73 inches

TCP/IP

Supported Browsers .....IE, Netscape, Mozilla, Opera,Chrome
Network Configuration .....Allows Static or Dynamic IP Configuration
Max Number of Email Addresses .....17; 1 per User Account + 1 for Administrator

Optional Battery

Type……Lithium-ion-rechargeable
Rated Capacity……2400mAh
Maximum current……...2A
Output……...7.4VDC
Duration……...2 Hrs Minimum

E-2D SPECIFICATIONS

User Interface

LEDs.....Green – Power (solid when ENVIROMUX is powered ON)
.....Red – Fault (solid when any sensor is in alert)

RJ45 Sensor Inputs

Connector.....RJ45 connector (2)
Voltage Supply.....5VDC and 12VDC
Signal Type.....RS485 for RS485 sensors; 2-wire for contact sensors
Max. Cable Length.....1000 FT
ESD Protection.....IEC 61000-4-2
Fuse Protection.....Resetable poly fuse – 200mA shared (5VDC); 200mA independent (12VDC)

Digital Inputs

Connector.....Detachable terminal block-plug-in, 5 x 2 contacts
Wire Range.....16-26 AWG
Max. Input Voltage.....25VDC
Max. Contact Resistance.....300K ohm
ESD Protection.....IEC 61000-4-2

Output Relays

Connector.....Detachable terminal block-plug-in, 3 contacts
Wire Range.....16-26 AWG
Output Type.....Dry contact, relay isolated
Output Rating.....1A / 30 VDC, 0.5A / 100VAC
Contact Resistance.....20 milliohm
ESD Protection.....No, Relay Isolated.
Fuse Protection.....Non-resetable, 2A Hold, 4A trip, 125V

Warning: The digital output relay contacts are not to be connected directly to AC mains wiring.

USB Device Ports

Connector.....USB Type A Female
Version.....USB 2.0 Full Speed compatible

USB-Serial Port “Console”

Connector.....USB Type B Female
Supported Signals.....D+ ,D-
Baud Rate.....max 115,200 bps
Data Format.....8 bits
Parity.....no parity
Stop Bits.....1 stop bits
ESD Protection.....IEC1000-4-2

Auxiliary Power Port

Connector ..... Detachable terminal block-plug-in, 1x2 contacts
Wire Range ..... 16-26 AWG
Voltage Output ..... 12VDC+/-10%
Current Output 500mA
ESD Protection ..... IEC 61000-4-2
Fuse Protection ..... Resetable poly fuse – 1.1A hold, 1.95A trip; 16VDC max.

Ethernet Port

Connector ..... RJ45 Female
Connection Speed ..... 10/100 Base-T
Security ..... SSL
Supported Protocols ..... http, https, Telnet,SSH

General Specifications

Power Input ..... 120VAC or 240VAC at 50 or 60Hz-9VDC/3A AC Adapter
Operating Temperature ..... 32° -140°F (0-60˚C)
Operating Humidity ..... 17-90%RH, non-condensing
MTBF ..... 229,580 / (-2DB model) 230,693 hours
Enclosure Size(WxDxH) ..... 5.822 x 2.988 x 1.720 inches

TCP/IP

Supported Browsers ..... IE, Netscape, Mozilla, Opera, Chrome
Network Configuration ..... Allows Static or Dynamic IP Configuration
Max Number of Email Addresses ..... 17; 1 per User Account + 1 for Administrator

Optional Battery

Type……Lithium-ion-rechargeable
Rated Capacity……2400mAh
Maximum current……..2A
Output……..7.4VDC
Duration……..2 Hrs Minimum

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)
- 502 MODBUS (default port)
- 514 SYSLOG
- 5908 Sensor info for the Management Software
- 5919 Cascading via Ethernet
- 6000 Management Software

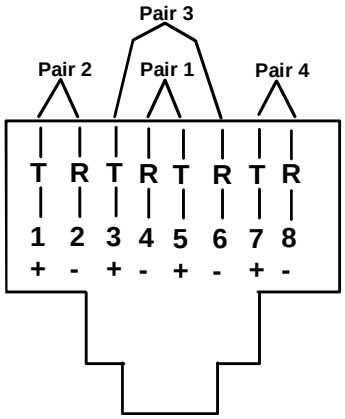
The HTTP, HTTPS and MODBUS port numbers may be changed by the administrator. If they are changed, contact the system administrator for the new assignments.

WIRING METHODS

RS485 Sensor Cable

The CAT5 connection cable between the ENVIROMUX and the external RS485 Sensors (page 10) is terminated with RJ45 connectors and must be wired according to the EIA/TIA 568 B industry standard. Wiring is as per the table and drawing below.

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



(View Looking into RJ45 Socket)

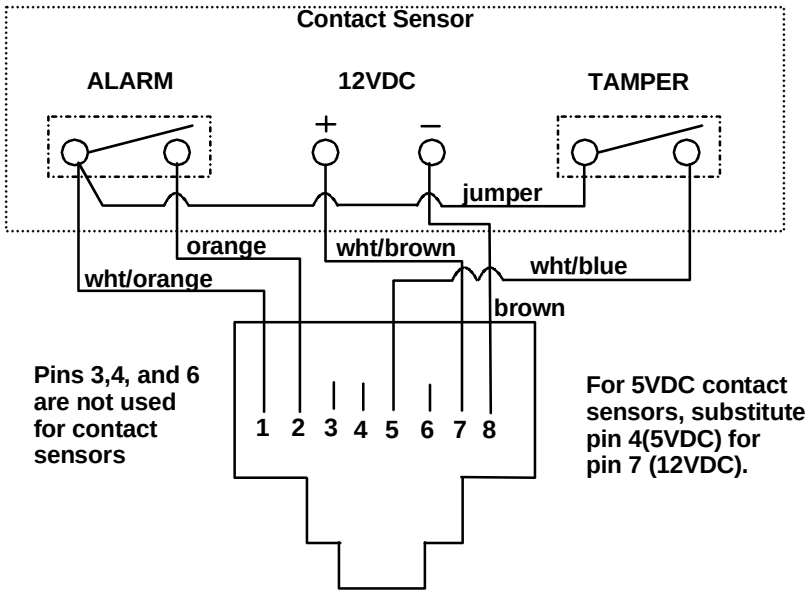
Contact Sensor Wiring

When applying CAT5 cables to contact sensors for plug-in to the RJ45 Sensor sockets, the following socket-to-sensor wiring must be followed:

RJ45 Sensor Socket Pinout

Pin #	Pin Name
1	GND
2	SENSE
3	RS485 +
4	+5 VDC
5	TAMPER SWITCH
6	RS485 -
7	+12 VDC
8	GND

Schematic for wiring Contact Sensor to RJ45 Socket



Pins 3,4, and 6 are not used for contact sensors

For 5VDC contact sensors, substitute pin 4(5VDC) for pin 7 (12VDC).

View looking into RJ45 Socket

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
"Pwr" LED is blinking (E-16D only)	• Blinking 1/sec =Power is OFF, battery backup is powering the ENVIROMUX • Blinking rapidly= discovery tool in use	• Restore AC power to the ENVIROMUX • Nothing wrong- close Discovery Tool to stop
Cannot access ENVIROMUX through my browser	• Browser not supported • Trying to connect to wrong IP address • User not authorized	• See supported browsers on page 4 • Type correct IP address into browser URL field. If IP address is unknown, use Discovery Tool (page 28) to identify it. • See administrator for user name and password
Cannot access ENVIROMUX user interface with direct Ethernet connection	• Telnet not enabled • Cable not wired correctly	• Must enable Telnet through web interface (page 67) • Cable should be wired pin-to-pin (1 to 1, 2 to 2, etc.)
ENVIROMUX will not recognize sensor	Previously used sensor port was never cleared from memory upon removal	Click on "???" in summary page, click on "Configure " button, click on "Remove" at bottom of Configure page to remove sensor and clear the port. (see page 36)
Device Discovery tool will not work	• Java not installed • PC and ENVIROMUX are on different physical networks	• Download and install Java (see page 28) • Make sure PC and ENVIROMUX or both on same physical network
Not receiving e-mail alert messages	• Ethernet cable disconnected • Wrong or no IP address provided for SMTP server • User does not have user profile correctly configured • Email address not accepted by SMTP server	• Check Ethernet cable connections • Check all Network Settings (page 67) • Check user profile. Make sure groups have been selected and the contact settings are correct (see page 77) • Check policies of SMTP server for restrictions
Beacon not illuminating	• Wires are not connected properly • Beacon in use is improperly rated • Sensor is not configured to power-ON the beacon	• Check wire connections • Make sure Beacon is rated at 12VDC, 180mA or less • Check sensor configuration- make sure Beacon is selected under "Alert Notifications" (-16D)
Siren not making noise	• Wires are not connected properly • Siren in use is improperly rated • Sensor is not configured to power-ON the siren	• Check wire connections • Make sure Siren is rated at 12VDC, 180mA or less • Check sensor configuration- make sure Siren is selected under "Alert Notifications" (-16D)
Ethernet cascading is not working	Ethernet Configuration not complete	• Make sure the correct IP of the Slave unit is entered into the Master configuration • Make sure Slave is configured as "Ethernet Slave" (page 88) • If behind a firewall, make sure port 5919 is open for the ENVIROMUX to pass data through
The sensor page does not display the current readings	Java scripts cannot be displayed-java not enabled in browser	Enable the Java Scripts and Java in the browser

Problem	Cause	Solution
Sensor status alternates between "normal" and "no answer" on summary page **User is receiving alert notifications about sensors being disconnected and then reconnected**	Electronic noise is being induced into sensor cables (near large motors, electronic ballasts, etc) causing errors in RS485 communication between ENVIROMUX and sensor. (this pertains to "RJ5 SENSORS" only)	Change the unshielded CATx cable to the RJ45 sensor(s) to shielded cable to reduce noise being introduced. If the issue is ignored it could potentially lead to damage of the RS485 communication circuit and require the ENVIROMUX unit to be returned for repair
Sensors connected to RJ45 Sensor ports stop working	Sensors applied collectively exceed current rating.	Disconnect sensors. After approx. 10 minutes fuse inside ENVIROMUX should reset. **For E-16D**: Make sure the load of all 8 sensors per row does not exceed 500 mA. (i.e. only one keypad per row (row 1 = ports 1-8, row 2= ports 9-16))
Unit will not boot up-access via Ethernet not possible	Firmware has been corrupted	Contact NTI for FTP recovery software and procedure.
Sensor connected to DIGITAL IN terminal stops working **(E-16D only)**	Sensor is rated for more current than terminal can supply. Fuse protecting port has opened. E-EDR-SF and E-EDR-SCR Electric Strike may cause this if connected to DIGITAL IN terminals 1-7	Disconnect failed sensor. After approx. 10 minutes internal fuse should reset. Reconnect sensor to terminals provided sensor current requirements fall within terminal limitations. **DIGITAL IN terminals 1-7 max. load = 50mA** **DIGITAL IN terminal 8 max. load = 650mA**
Event Log has "GSM Error code -3"	GSM Modem failed to communicate with cell tower due to a weak signal	Adjust the modem antenna using the Enterprise Setup screen (page 64) as a guide for the best signal
Attempt at connection via HTTPS from outside the LAN errors out	Port in Firewall not open to secure connection to ENVIROMUX	***Configure your firewall to allow communication through the port assigned to HTTPS connection (page 67).***
Slave in cascaded configuration keeps losing communication with Master	Slave configured (within the web interface for the slave) to add sensor values to datalog.	***Do not configure sensors from the Slave web interface, do not put a check in "Add to datalog" (page 40) and do not configure any alert methods. Only enable datalogging and alert methods for sensors when configuring them from the Master interface.***

For a complete list of ENVIROMUX factory-assigned port numbers, see page 162.

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.

Communication Ports used by the ENVIROMUX:

Port Number	Purpose
80	HTTP (also IP sensor monitoring)
443	HTTPS
22	SSH
23	Telnet
161	SNMP (system config, sensor data and mgmt. software sensor data)
162	SNMP (traps)
502	MODBUS (default)
514	SYSLOG
5908	Sensor info for Management Software
5919	Cascading via Ethernet
6000	Management Software

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 84), 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 174).

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
```

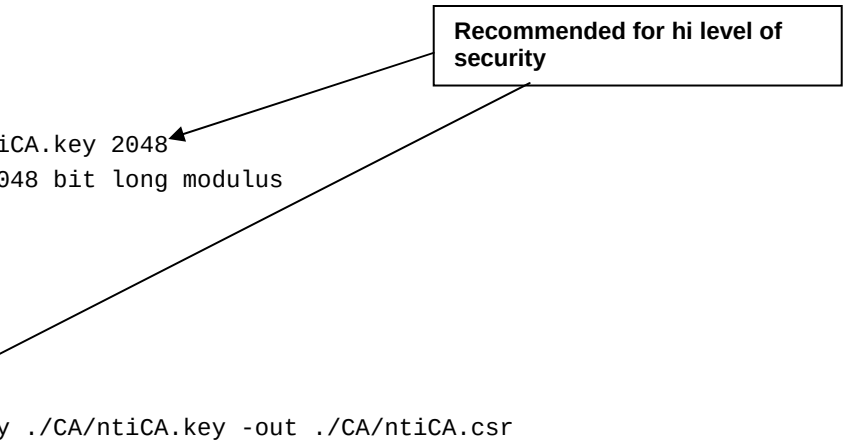
The openssl.cnf file that you edited earlier (if you did) references these files so make sure they are created in the ntiCA directory.

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:




```
% 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
```

<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.

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"**

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

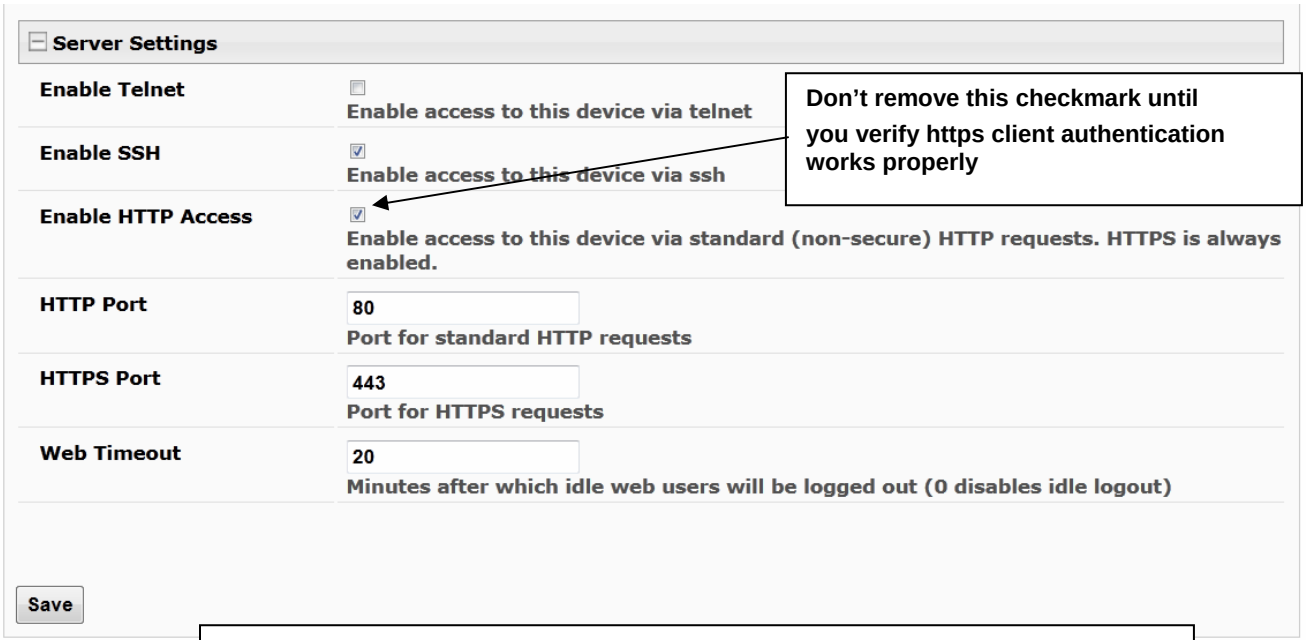
On the ENVIROMUX WEB Interface menu Under “Administration” select “Security”.

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

DATE/TIME BATTERY REPLACEMENT

The E-xD 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.

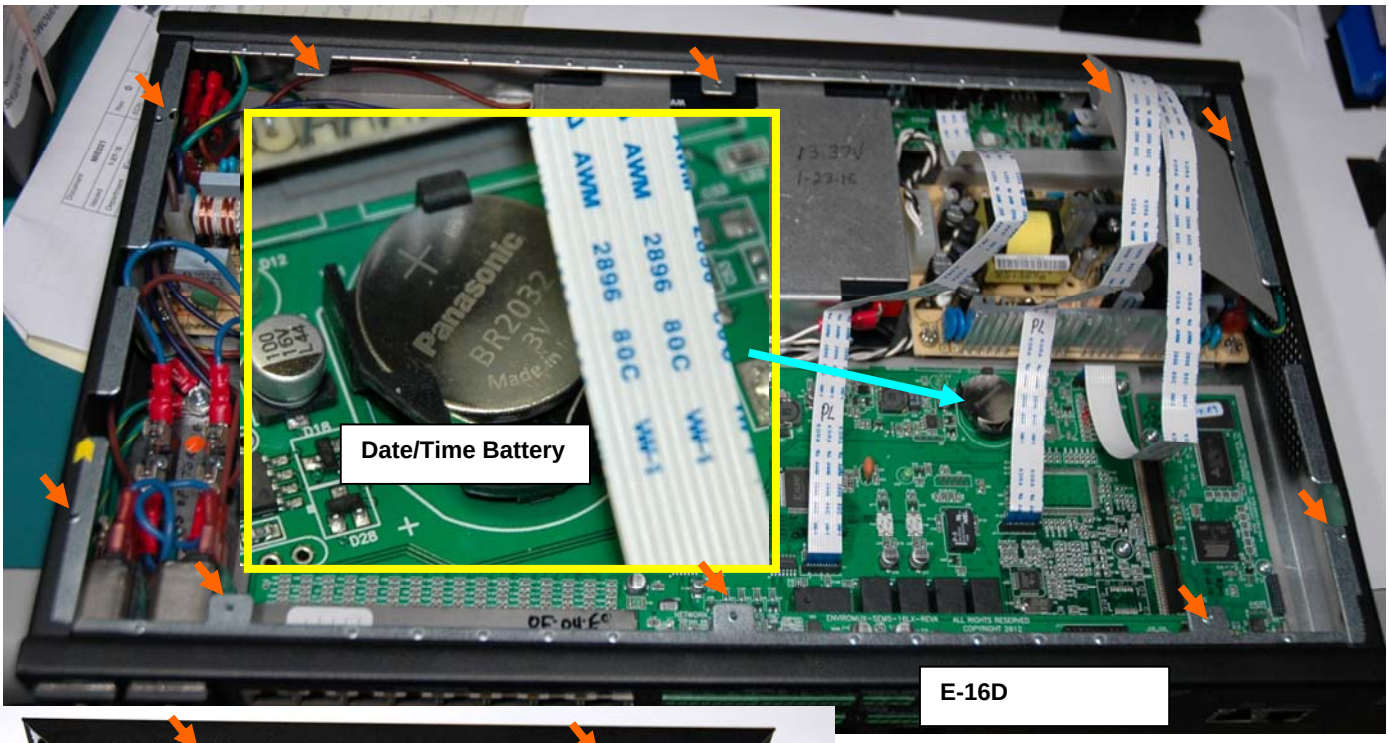
To replace the battery:

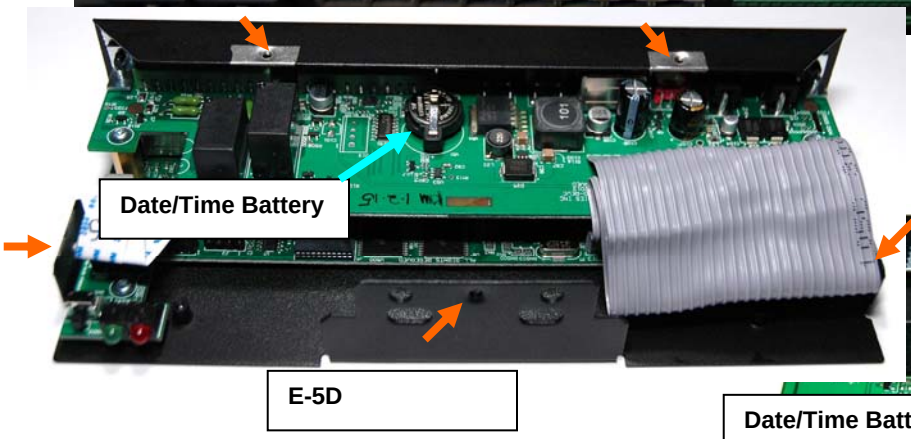
1. Avoid Electrostatic Discharge (ESD) by grounding yourself before touching the ENVIROMUX. Failure to follow this step may damage your ENVIROMUX.

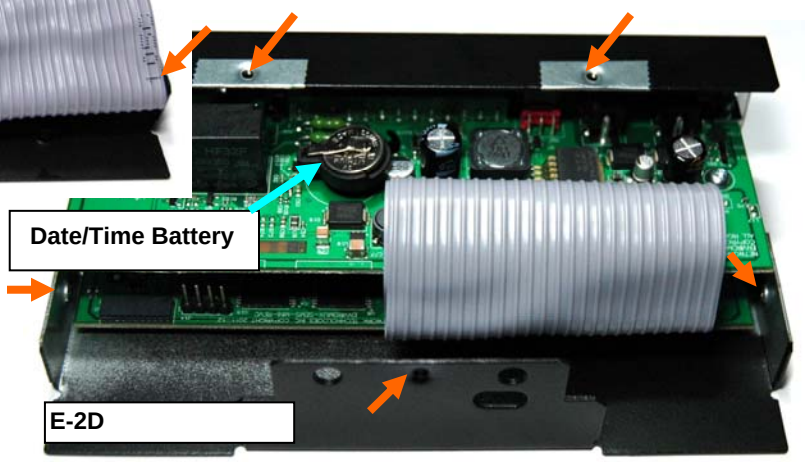
2. Power OFF the ENVIROMUX.

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 the exposed 120 or 240VAC line voltage (E-16D) or 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 (10 in the E-16D, 5 in the E-2D/5D, locations indicated below by orange arrows) and remove the cover to expose the circuit boards inside.



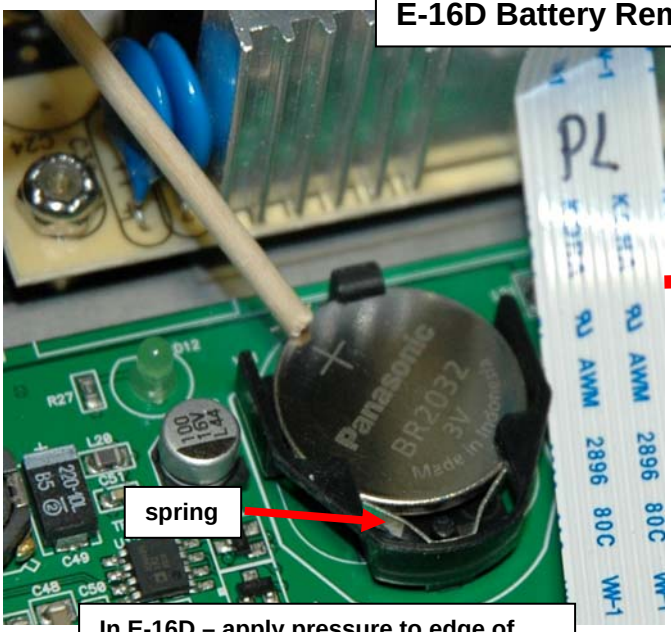




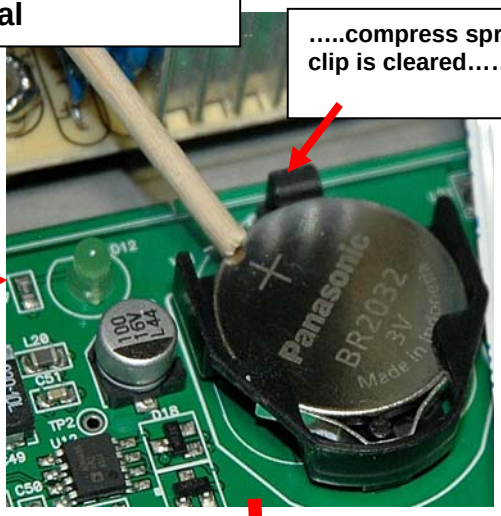
4. Locate the date/time battery in the ENVIROMUX (see images above).

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.

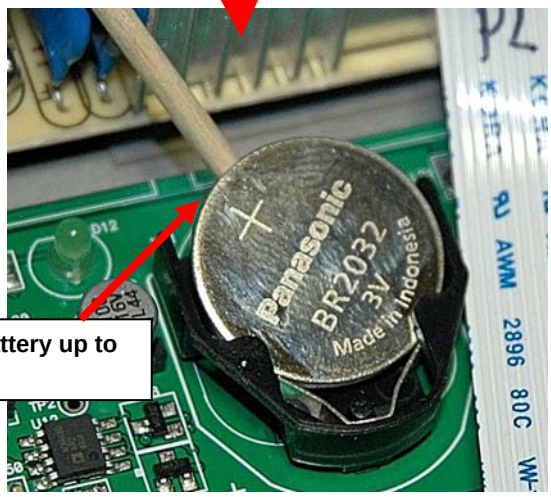
E-16D Battery Removal



In E-16D – apply pressure to edge of battery as shown, pressing the battery against the spring…..



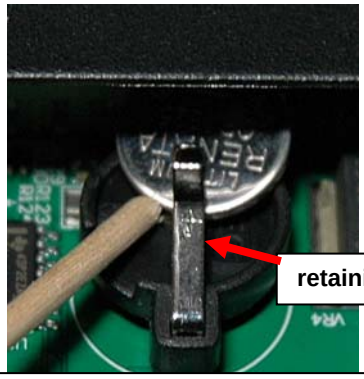
…..compress spring until clip is cleared……



…then tilt the battery up to remove it.

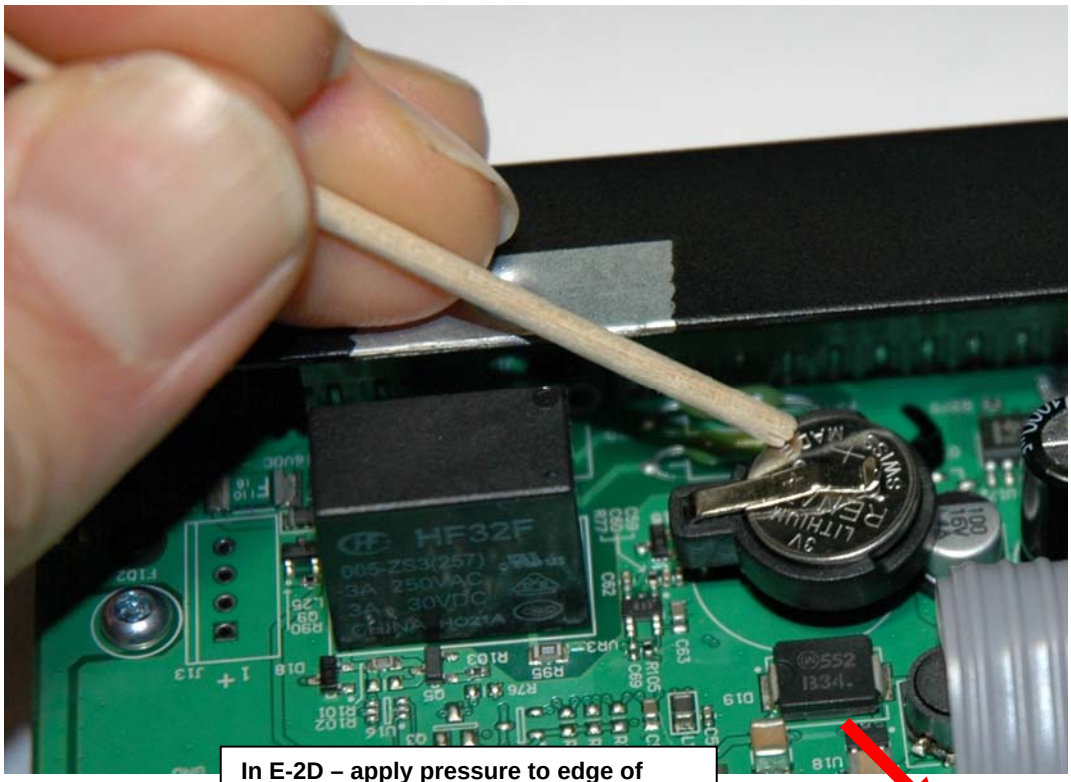
ENVIROMUX-5D Battery Removal

In ENVIROMUX-5D – apply pressure to edge of battery as shown, …..

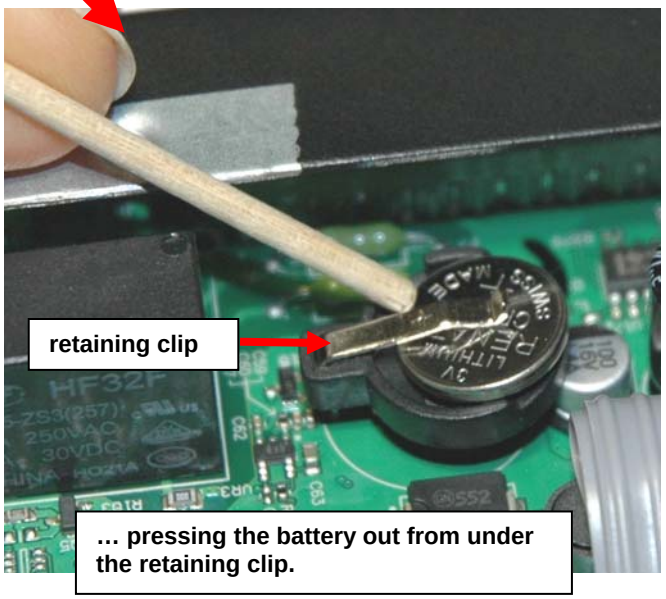


… pressing the battery out from under the retaining clip.

E-2D Battery Removal



In E-2D – apply pressure to edge of battery as shown, …..



… pressing the battery out from under the retaining clip.

6. Re-install the new battery by reversing the process. (**CR1225** for E-2D/5D, **CR2032** for E-16D) With the E-2D/5D, be very careful not to lift up to 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.

E-16D BACKUP BATTERY REPLACEMENT

The NTI E-16D contains a sealed lead acid battery that may at some point need replacement. **If the unit is under warranty, contact NTI to arrange for return and factory replacement to prevent voiding the warranty.** If the unit is outside of the warranty, field replacement may be preferred (contact NTI to order part no. E-BATTERY2). In either case, the failed battery must be properly disposed of. To replace the battery, carefully follow all instructions.

WARNING

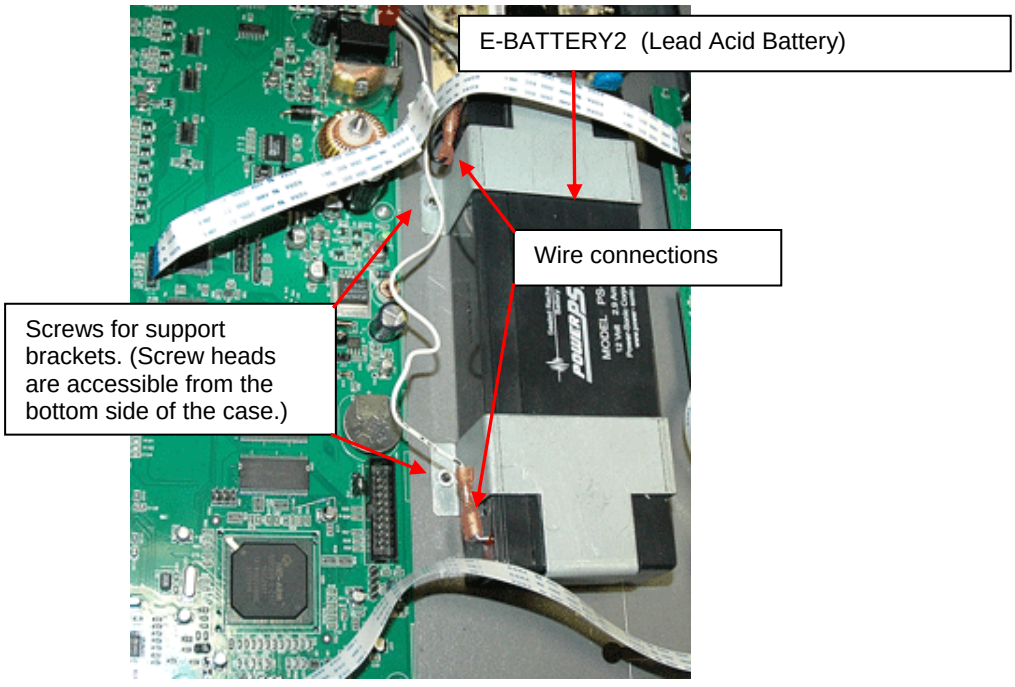
RISK OF ELECTRIC SHOCK! FAILURE TO FOLLOW ALL INSTRUCTIONS MAY RESULT IN ELECTRICAL SHOCK.

Disconnect ALL power and connection cables from the ENVIROMUX before proceeding.

1. Remove 10 Phillips-head screws securing the cover of the ENVIROMUX to expose the components inside.
2. Locate the battery inside the ENVIROMUX. (See figure below)
3. Remove the two wires connected to the battery using pliers.
4. Remove the 4 Phillips-head screws securing the two brackets holding the battery to the case. Screw heads are accessible from the bottom side of the ENVIROMUX.
5. Remove the battery.
6. Place the new battery in the case with the terminals in the same position as the battery that was removed.
7. Reinstall the two brackets to secure the battery using the 4 Phillips-head screws.
8. Attach the two wires. Be sure the wire connectors are fully on the battery terminals.
9. Reinstall the cover of the ENVIROMUX.
10. Dispose of the battery according to local requirements.

Note: Charge new battery (power up the ENVIROMUX) for at least 48 hours before putting the ENVIROMUX in storage, and if kept in storage, recharge the battery every 3 months.

For instruction on the proper disposal of the battery, either contact the Rechargeable Battery Recycling Corporation (RBRC) at 800-822-8837 or go to their website at www.call2recycle.org. Disposal will be at no cost to you.



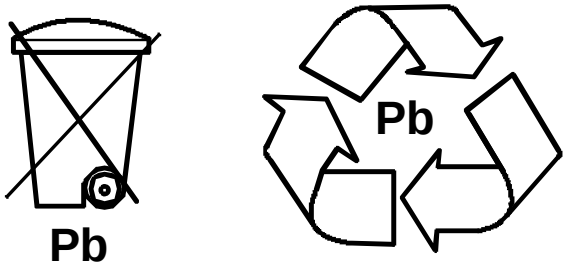
RECYCLING INFORMATION

Attention: Residents of New York, USA

The E-16D is subject to New York's recycle laws regarding lead acid batteries.

WARNING

The E-16D contains a sealed lead acid battery. Battery maintenance must be performed by an authorized trained technician. Always follow local laws and regulations regarding the disposal of this unit.



For instruction on the proper disposal of the battery contained in this unit, either contact the Rechargeable Battery Recycling Corporation (RBRC) at 800-822-8837 or go to their website at www.call2recycle.org. Disposal will be at no cost to you.

For instruction on the safe removal of the battery, see page 178.

In order to return the E-16D to Network Technologies Inc for any reason, please contact us at **(800) 742-8324** (800-RGB-TECH) or **(330) 562-7070** to receive a return goods authorization. All packaging and shipping expenses will be the sole responsibility of the customer.

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 www.networktechinc.com for information regarding repairs and/or returns. A return authorization number is required for all repairs/returns.

MAN154 Rev. 4/11/18