



**NETWORK
TECHNOLOGIES
INCORPORATED**

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

ENVIROMUX® Series

E-MICRO-T(RHP)

Micro Environment Monitoring System Installation and Operation Manual



TRADEMARK

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

COPYRIGHT

Copyright © 2009, 2018 by Network Technologies Inc. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of Network Technologies Inc, 1275 Danner Drive, Aurora, Ohio 44202.

CHANGES

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

FIRMWARE VERSION

Current firmware version 3.4

TABLE OF CONTENTS

Introduction.....	1
Supported Web Browsers	2
Materials.....	2
Connectors and LEDs	3
Installation	4
Mounting	4
Connect Sensors	4
Ethernet Connection.....	8
Connect the Power	9
Cable Restraint	9
Overview.....	10
Administration	10
General Functions.....	10
Security	11
Device Discovery Tool.....	12
How to Use the Device Discovery Tool	12
Operation via Web Interface.....	13
Log In and Enter Password	13
Summary.....	15
Sensor Settings.....	17
Alerts.....	17
Configure Alerts	18
Smart Alert.....	20
Administration	24
System Settings	24
Network Configuration	25
SNMP Settings.....	26
Email Server Settings	27
Time Settings	28
Set Local Time	28
Users.....	29
IP Cameras	32
Update Firmware	33
Log.....	34
View Event Log	34
View Data Log.....	35
IP Devices.....	37
Support	38
Logout.....	38
Operation via Text Menu- ENVIROMUX.....	39
Connect to ENVIROMUX from Terminal through Ethernet	39
Connect to ENVIROMUX from Command Line.....	40
Using the Text Menu.....	41

Monitoring	41
Display Network Settings	44
Restore Defaults Button	45
How To Setup Email.....	46
Locating OIDs.....	48
REST API Support	51
Technical Specifications.....	55
Troubleshooting.....	56
E-MICRO Email Error Codes.....	57
Index.....	58
Warranty Information.....	58

TABLE OF FIGURES

Figure 1- Mount with sensor towards the floor	4
Figure 2- Connect Sensors	5
Figure 3- Terminal block for dry-contact sensors.....	5
Figure 4- Secure liquid detection sensor with tape	6
Figure 5- Portion of Water Sensor configuration page.....	7
Figure 6- Connect ENVIROMUX-MICRO to the Ethernet.....	8
Figure 7- Connect the AC adapter and power-up	9
Figure 8- Use cable restraint.....	9
Figure 9- Device Discovery Tool.....	12
Figure 10- Login prompt to access web interface	13
Figure 11- Summary page	14
Figure 12- Summary page	15
Figure 13- List of alerts configured	16
Figure 14- Sensor settings.....	17
Figure 15- List of configured alerts and their status	17
Figure 16- Select a sensor to add an alert configuration for	18
Figure 17- Alert Configuration page for Temperature/Humidity sensors.....	18
Figure 18- Alert configuration for Digital sensor- minor difference	19
Figure 19- Smart Alerts page.....	20
Figure 20- Sensor to be used for a predefined event.....	20
Figure 21- Event Logical Function Diagram.....	22
Figure 22- Examples of Smart Alert conditions.....	23
Figure 23- System Settings page.....	24
Figure 24- Network Settings page	25
Figure 25- SNMP Settings	26
Figure 26- Email Server Settings	27
Figure 27- Time and Date Settings	28
Figure 28- Users List.....	29
Figure 29- User2 added- ready to configure	29
Figure 30- Initial User Settings.....	29
Figure 31- User Settings-Contact Settings.....	30
Figure 32- User Settings- User Active Schedule.....	31
Figure 33- IP Camera Monitoring.....	32
Figure 34- Configure IP Cameras	32
Figure 35- Update Firmware page	33

Figure 36- Event Log page	34
Figure 37- Data Log page	35
Figure 38- Examples of emailed datalogs.....	36
Figure 39- IP Devices listing-none monitored yet	37
Figure 40- IP Device Configuration page.....	37
Figure 41- IP Device list with new devices added.....	38
Figure 42- Support.....	38
Figure 43- Logout	38
Figure 44- Terminal connection through Ethernet port	39
Figure 45- Text Menu Login screen	39
Figure 46- Text Menu- Administrator Main Menu.....	40
Figure 47- Text Menu-Monitoring Menu.....	41
Figure 48- Text Menu-Sensor Status.....	42
Figure 49- Text Menu- Digital Input Status	42
Figure 50- Text Menu-View IP Devices.....	43
Figure 51- Text Menu-Configure Sensors list	43
Figure 52- Text Menu-Network Settings	44
Figure 53- Location of Restore Defaults button	45
Figure 54- Email Server Settings example for sending emails.....	46
Figure 55- Configure user to receive alerts via email.....	47

INTRODUCTION

The ENVIROMUX® Micro Environment Monitoring System (ENVIROMUX) monitors (from a remote location) critical environmental conditions, such as temperature, humidity, liquid water presence, power, intrusion, and smoke. When a sensor goes out of range of a configurable threshold, the system will notify you via email, web page, network management (SNMP), and/or SMS messages (via email). For a complete list of sensors supported, visit our website at <http://www.networktechinc.com/environment-monitor-micro.html>.

The system functions independently or as an IP-connected remote sensor for the E-2D/5D/16D.

The E-MICRO-T features a built-in temperature sensor, two RJ45 sensor ports for external temperature/humidity sensors, and two dry contact inputs.

The E-MICRO-TRHP features a built-in temperature/humidity sensor, two RJ45 sensor ports for external temperature/humidity sensors, two dry contact inputs for the connection of contact-closure sensors and built-in Power over Ethernet (PoE).

Features and Applications

- Monitor and manage server room environmental conditions over IP.
- Monitors and operates at temperatures from -4°F to 167°F (-20°C and 75°C) and 0% to 90% non-condensing relative humidity.
- Includes one integrated temperature sensor
- Sensors supported:
 - 2 temperature/humidity sensors
 - 2 digital input devices (dry contact or water detection sensors)
- Operates and configures via HTTP web page.
- Six remote users can access the system simultaneously.
- Supports SMS alert messages via email
- Supports SMTP protocol
- Supports SNMPv1, v2c and v3 protocols
- Supports SNTP protocol
- Supports Microsoft Internet Explorer 6.0 and higher, Firefox 2.0 and higher, Chrome, Safari 4.0 or higher, and Opera 9.0 or higher
- Sensor alerts and log messages are sent using email, Syslog, and SNMP traps when any monitored environmental condition goes out of the user-specified range.
- Sensor alert and end of alerts are posted in message log, which is accessible through web interface.
- SNMP trap messages can be imported into Microsoft Excel
- Use in data centers, co-lo sites, web hosting facilities, telecom switching sites, POP sites, server closets, or any unmanned area that needs to be monitored.
- Security: HTTPS, TLS v1.2, AES 256-bit encryption, 3DES, Blowfish, RSA, EDH-RSA, Arcfour, SNMP(v1,v2c,v3) with AES and DES privacy protocol and MD5 or SHA as authentication protocols, 16-character username/password authentication, user account restricted access rights.
- Monitor (ping) up to 4 IP network devices.
 - Configure the timeout and number of retries to classify a device as unresponsive.
 - Alerts are sent if devices are not responding.
- Monitored sensors and devices can be individually named (up to 63 characters).
- Monitor environmental conditions.
 - Supports two temperature/humidity sensors and up to 2 dry contacts or water detection sensors.
 - When a sensor goes out of range of a configurable threshold, the system will notify you via email, syslog, web page, and network management (SNMP).
- Firmware upgradeable "in-field" using web interface.

Options:

- The E-TRHP includes an additional integrated humidity sensor and built-in Power over Ethernet (PoE) (supports IEEE 802.3af (PoE) and 802.3at (PoE+) standards.)

SUPPORTED WEB BROWSERS

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

- Microsoft Internet Explorer 6.0 or higher
- Mozilla FireFox 2.0 or higher
- Opera 9.0 or higher
- Google Chrome 9.0.5 or higher
- Safari 4.0 or higher for MAC and PC

MATERIALS

Materials supplied with this kit:

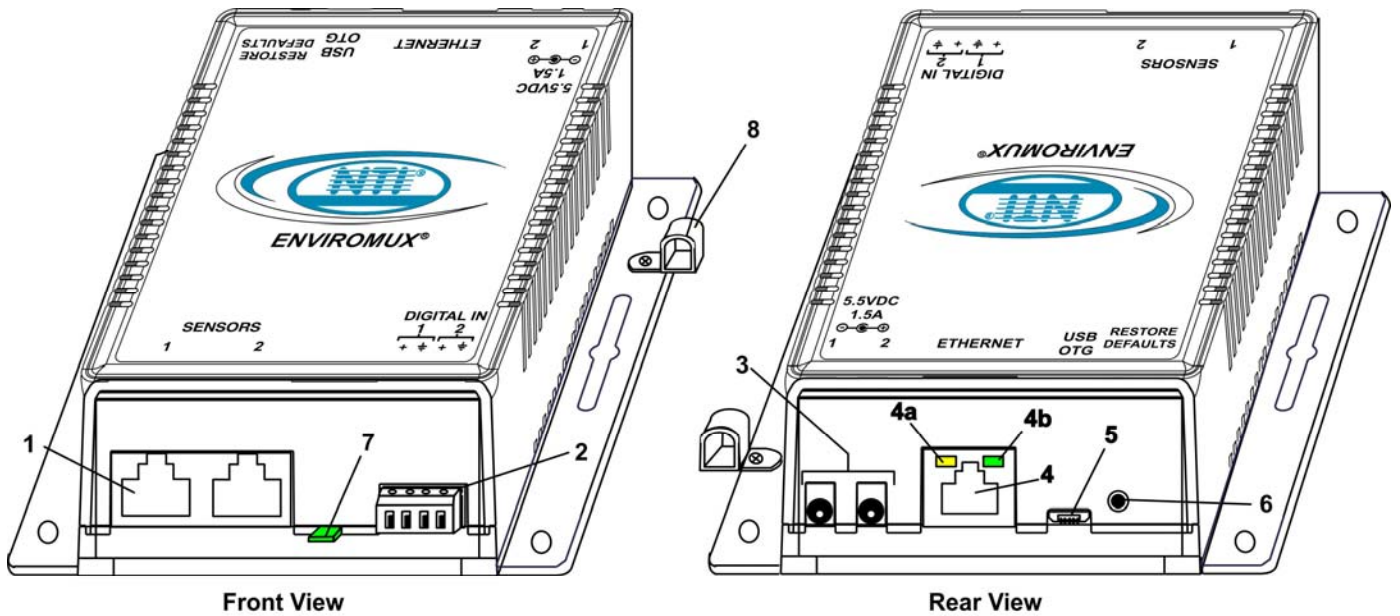
- NTI E-MICRO-T/TRHP Micro Environment Monitoring System
- 1- 120VAC or 240VAC at 50 or 60Hz-5.5VDC/1.5A AC Adapter (**E-MICRO-T** only)

Additional materials may need to be ordered;

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

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

CONNECTORS AND LEDS



#	LABEL	CONNECTOR/LED	DESCRIPTION
1	Sensors	RJ45 female connectors	For connection of optional temperature/humidity sensors (The left port is "#1", the right port is "#2" as listed in the Summary Page on Page 14.)
2	DIGITAL IN	Wire terminal block	For connecting dry-contact and liquid detection sensors
3	5.5V 1.5A	3.5x1.3mm Power Jacks	For connection of power supply(s)
4	Ethernet	RJ45 female connector	For connection to an Ethernet for remote multi-user control and monitoring <ul style="list-style-type: none"> • 4a-Yellow LED– illuminated when Ethernet link is present, strobing indicates activity on the Ethernet port • 4b- Green LED - indicates 100Base-T activity when illuminated, 10Base-T activity when dark
5	USB OTG	Micro USB female connector	Reserved for future use
6	Restore Defaults	Push button	For manually resetting the ENVIROMUX to default settings- a momentary press will activate
7	----	Sensor	Integrated temperature sensor (-T model) or temperature/humidity sensor (-TRHP model).
8	----	Cable Restraint	For securing the power cable

INSTALLATION

Mounting

Mount the ENVIROMUX in any dry location convenient for connection of the sensors, Ethernet cable, and power supply(s). The operating environment must be within -4°F to 185°F (-20°C to 85°C) with a relative humidity of 0 to 99% (non-condensing). When mounting the unit vertically, for best results mount the case with the integrated temperature sensor positioned towards the floor.

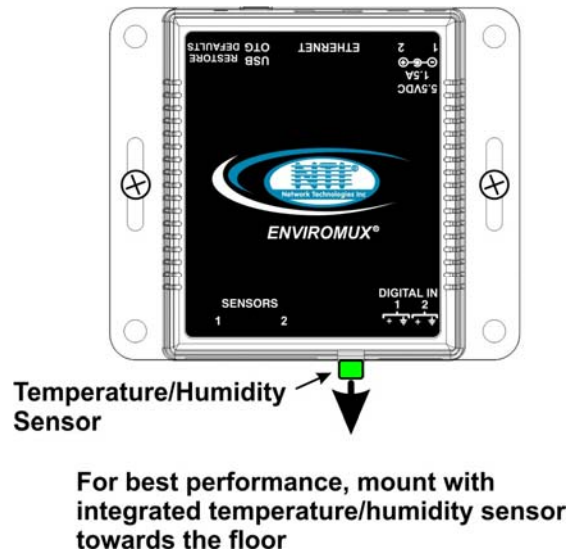


Figure 1- Mount with sensor towards the floor

Application Note: Airflow over the E-MICRO-T(THP) integrated temperature sensor of 2.5 M/s (8.2 Ft/s) or greater is required to reduce temperature reporting error due to self-heating.

Connect Sensors

E-MICRO-T(RHP) units are compatible with: E-T-E7, E-TRHM-E7 temperature and temperature/humidity sensors as well as other types of sensors. For a complete list, visit our website at <http://www.networktechinc.com/environment-monitor-micro.html>

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

Note: The maximum CAT5 cable length for attachment of temperature and humidity sensors in the E-MICRO-T(RHP) is 507 feet using minimum 24AWG cable.

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

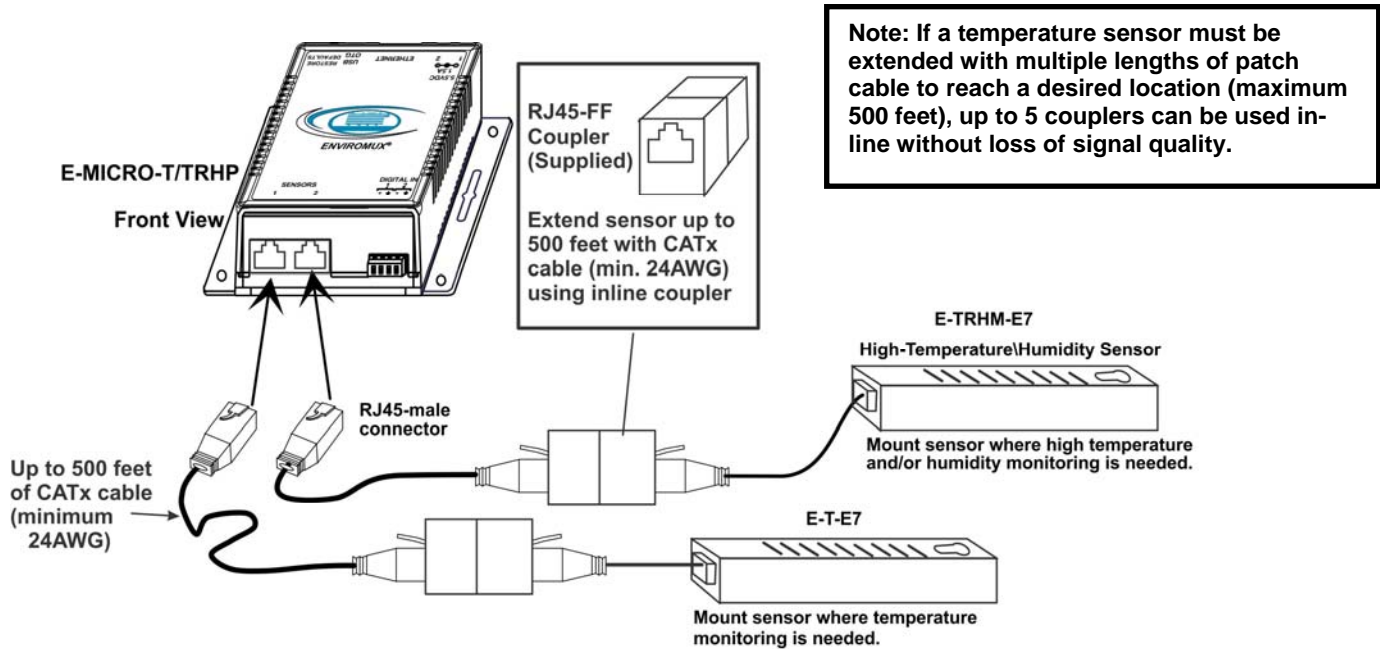


Figure 2- Connect Sensors

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

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

- A. Attach the positive lead to a terminal corresponding to a "+" marking on the ENVIROMUX and the ground lead to the next terminal to the right that will correspond to a $\frac{+}{-}$ marking on the ENVIROMUX. Tighten the set screw above each contact. Terminal sets are numbered 1-2.

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

- B. Mount the sensors as desired.

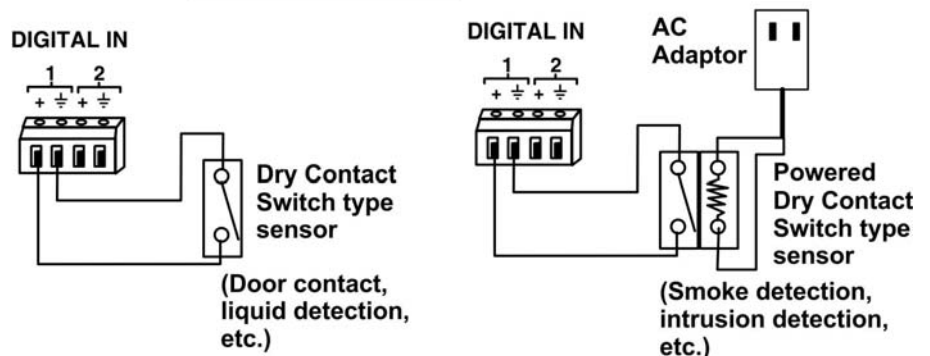


Figure 3- Terminal block for dry-contact sensors

Optionally, connect the two-wire cable from a liquid detection sensor (Figure 4) to a set of “DIGITAL IN” contacts. (Up to 4 sets of two-wire cables can be connected to a set of “DIGITAL IN” contacts. See image next page.)

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.

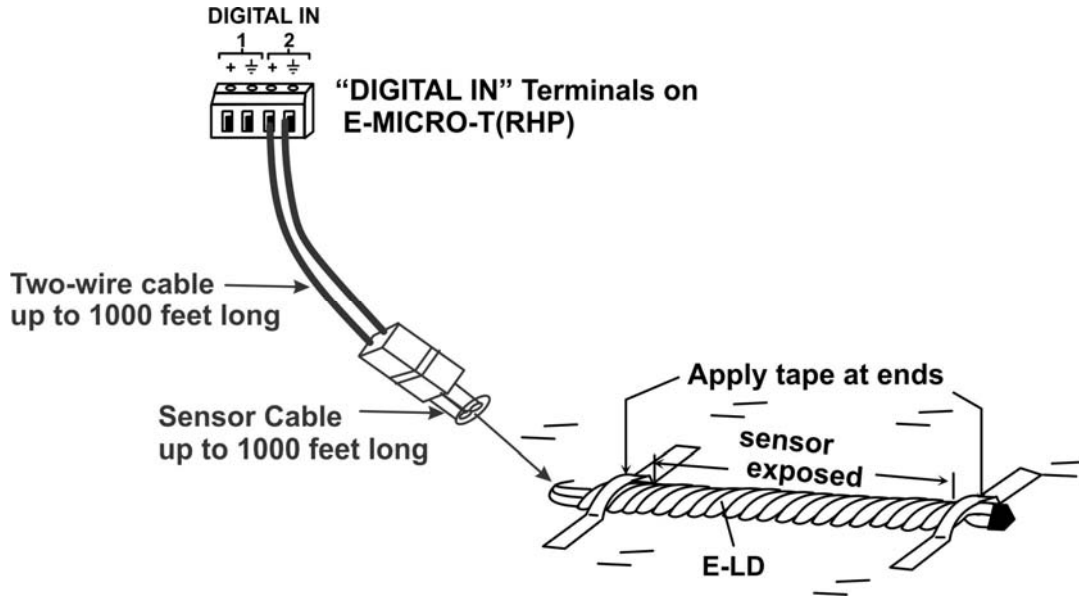
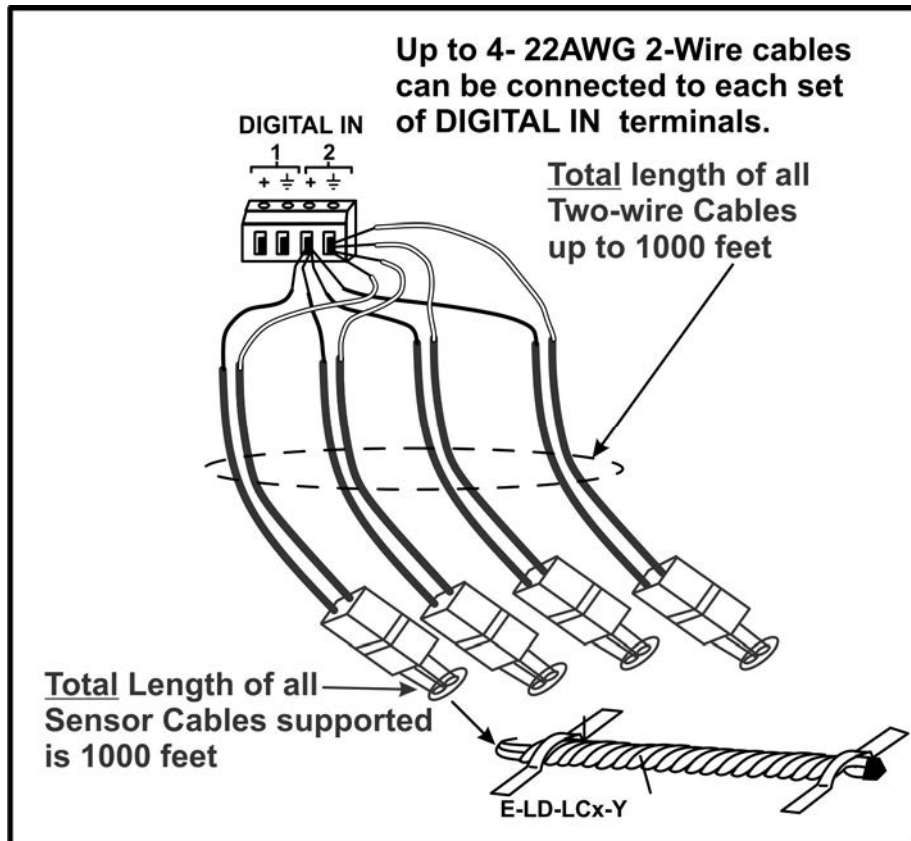


Figure 4- Secure liquid detection sensor with tape

NOTE:

When installing the E-LD-LC, it is very important to assure the sensing cable does not cross over itself or cross conductive surfaces to avoid false triggers.



To test the E-LD(-LC);

1. Configure the sensor (page 17). (Normal Status set to “Open”)
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 14) 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.

Configure Alert

Alert Settings	
Associated Sensor	<input type="text" value="Digital Input#1"/> <small>Sensor associated to this alert.</small>
Groups	<input type="checkbox"/> Group 1 <input type="checkbox"/> Group 2 <input type="checkbox"/> Group 3 <input type="checkbox"/> Group 4 <input type="checkbox"/> Group 5 <input type="checkbox"/> Group 6 <input type="checkbox"/> Group 7 <input type="checkbox"/> Group 8
Trigger Event	<input type="text" value="Open"/> ▾

Figure 5- Portion of Water Sensor configuration page

Ethernet Connection

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

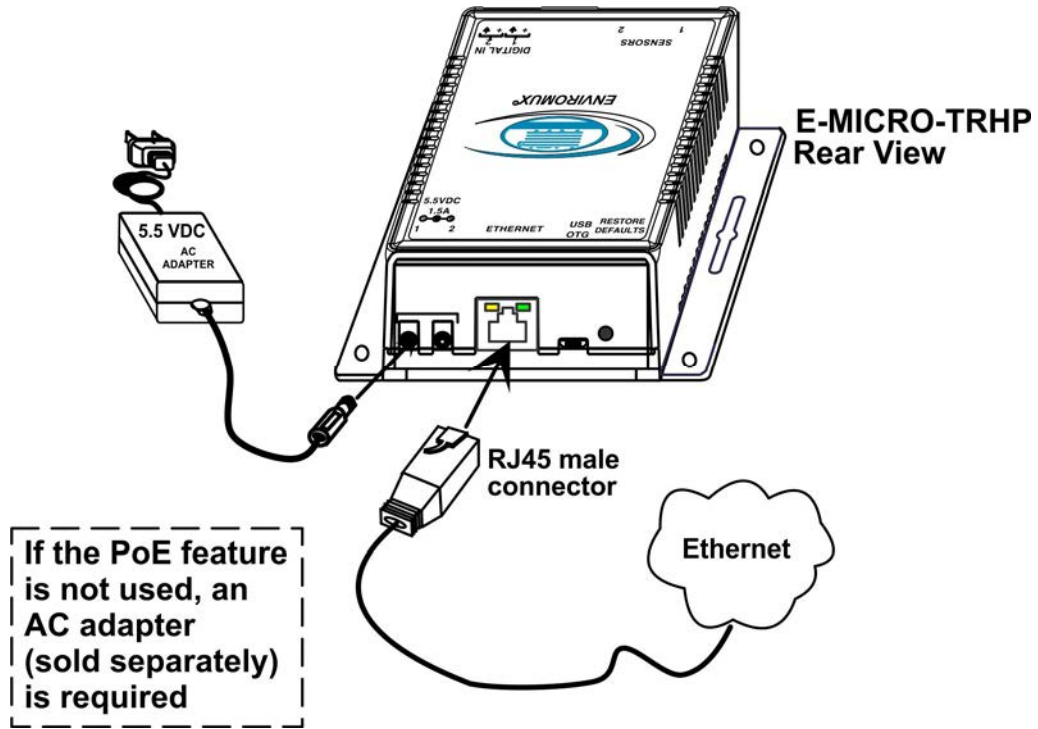
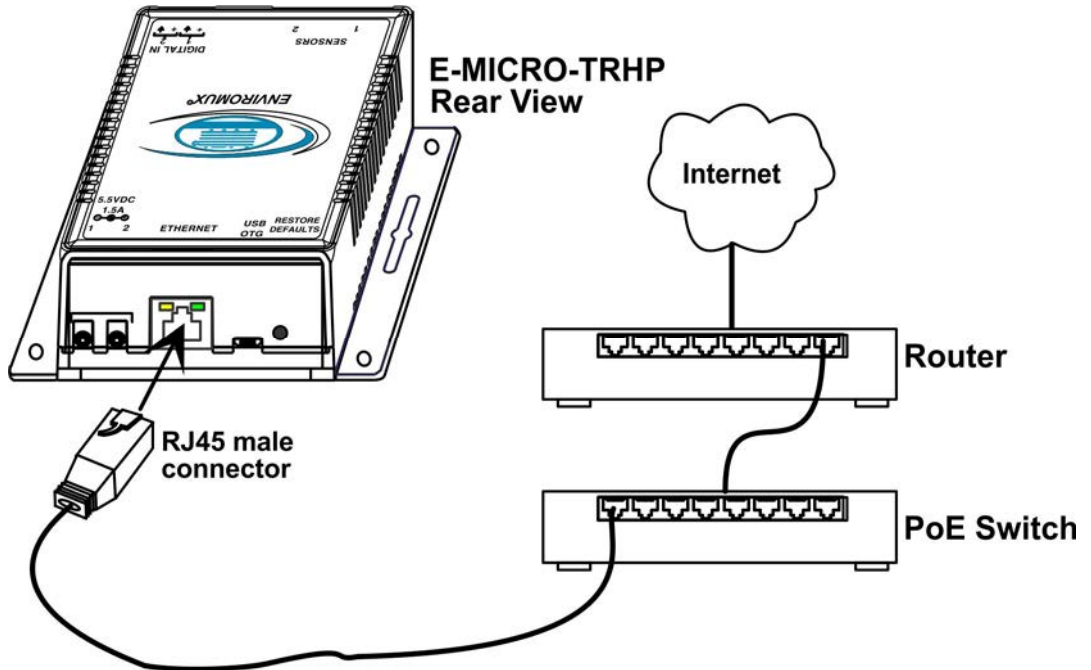


Figure 6- Connect ENVIROMUX-MICRO to the Ethernet

Note: A direct Ethernet connection can be made with a PC using the same CAT5 patch cable if desired.



Connect the Power

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

1. Connect the AC adapter to one of the connections marked "5.5VDC 1.5A" (either 1 or 2) on the ENVIROMUX and plug it into an outlet. If you have purchased an E-MICRO-T, this is required. Two power supply connections are provided in case you wish to have two independent sources of power in case one fails. If one source fails, the second will automatically take over. If a second AC adapter is desired, contact NTI and order PWR-SPLY-ELC.

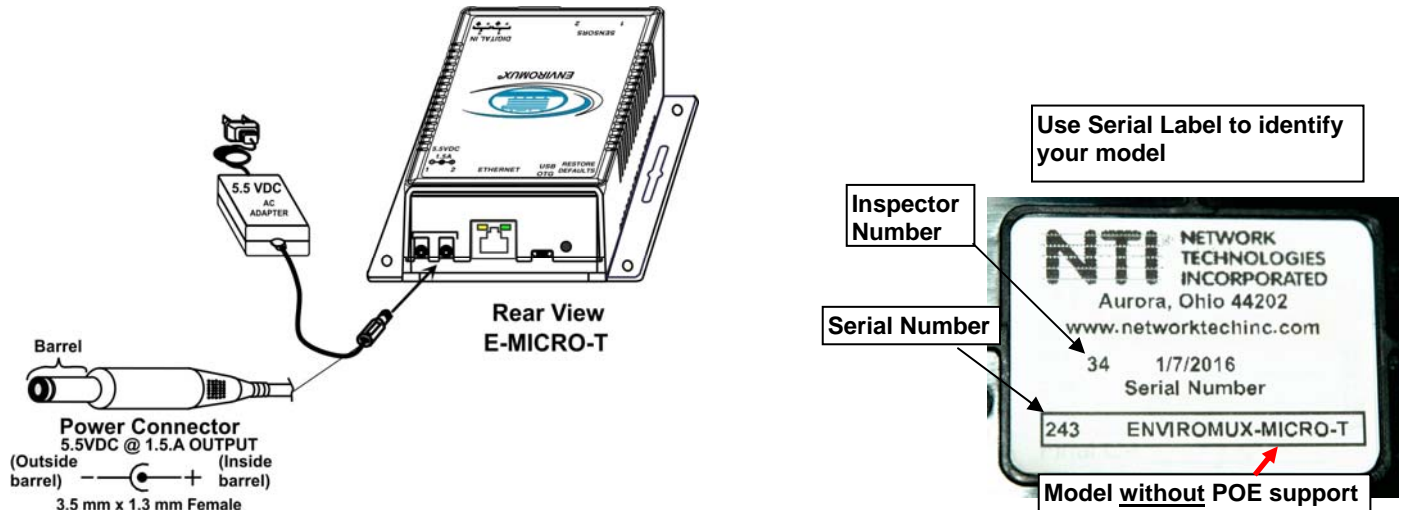


Figure 7- Connect the AC adapter and power-up

If you have purchased the E-TRHP and have connected it to a POE router or POE Adapter, an external power supply will not be needed as long as the router or adapter supports the IEEE 802.3af or 802.3at standards. (The Cisco Discovery Protocol is not supported.) If an AC adapter is needed, contact NTI and order PWR-SPLY-ELC.

Note: When power cycling the E-MICRO, whether by disconnecting the ETHERNET cable (model with POE support), or by unplugging the AC adapter, be sure to wait at least 10 seconds before re-connecting power.

Model with POE support

Note: We recommend power-cycling a POE router before connecting the E-MICRO if the connection socket in the router was used for another POE device previously.



2. Use the NTI Discovery Tool (page 12) to configure network settings.

Cable Restraint

To provide a secure power connection to the ENVIROMUX, a cable restraint has been provided. To secure the power cable, remove the screw that holds the restraint to the ENVIROMUX, make a loop in the power cable and insert it into the restraint. (The loop will prevent the cable from slipping through the restraint.) Re-secure the restraint to the ENVIROMUX with the screw.

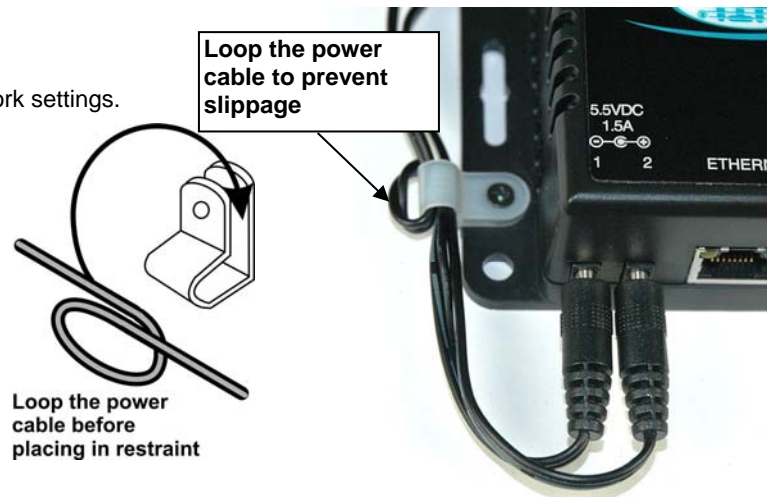


Figure 8- Use cable restraint

OVERVIEW

Administration

The ENVIROMUX can be managed and configured in any one of the following ways:

- Using Telnet protocol via the Ethernet Port.
- Using the web interface (HTTP/HTTPS protocol) via the Ethernet Port.

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

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

General Functions

Sensor Alerts

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

IP Monitoring & Alerts

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

Event Log

The ENVIROMUX maintains an event log. The event log includes power-ON, system, and alert notifications, as well as user alert handling. The maximum number of log entries is 200, and these entries are sorted in chronological order. The log can be viewed at any time through the web interface. Log entries can be removed individually or all at once.

Data Log

The ENVIROMUX maintains a data log. The data log includes readings taken from sensors, IP devices, and connected accessories being monitored. The log will record data for up to 30 days, at 1 minute intervals erasing the oldest data to make room for new. The log can be viewed at any time through the web interface, and can be saved as a text file in either Epoch time format or standard date/time format. Log entries can be cleared with the press of a button. The text file can be sent to any user automatically via syslog and/or email (see page 29).

Email

The ENVIROMUX can access an SMTP server to send outgoing email. Outgoing email would contain pre-formatted alert notifications. Email addresses can be configured through the web interface. Each user (up to 8) plus the "root" user (total of 9) can have their own email address. For assistance in setting up Email, see page 46.

The email messages sent by the ENVIROMUX have a fixed format. A sample message is shown below:

```
Subject: Message from E-MICRO P02 [Alert #1]
SENSOR: Test Switch 1
MESSAGE: Sensor value crossed over critical thresholds
VALUE: Closed
UNIT INFO: 192.168.1.24,00:0b:82:15:02:c3
```

Note: The E-MICRO-T(RHP) does not support Microsoft Office 365.

Alert messages can also be sent to a cell phone using Email-to-SMS by entering a User's full phone number@carrier instead of a User's email address (page 30).

SNMP

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

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

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

Security

User Settings

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

Secure Connections

The ENVIROMUX supports secure connections using HTTPS.

Authentications

The ENVIROMUX supports local authentication with up to 16 character usernames and passwords.

Encryption

The ENVIROMUX supports 256-bit AES and DES encryption.

DEVICE DISCOVERY TOOL

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

Note: The Device Discovery Tool requires the Java Runtime Environment (version 6 or later) to operate. Here is a [link](#) to the web page from which it can be downloaded.

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

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

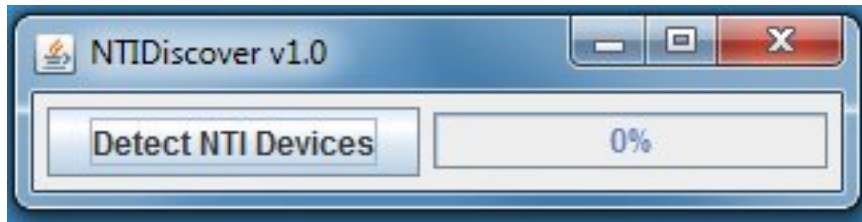


Figure 9- Device Discovery Tool

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.

Device	MAC Address	IP Address	Mask	Gateway		
ENVIROMUX-SEMS-16	00:0C:82:03:03:E8	192.168.3.80	255.255.255.0	192.168.3.3	Submit	Blink LED
ENVIROMUX-5D	00:0C:82:10:00:05	192.168.3.25	255.255.255.0	192.168.3.3	Submit	Blink LED
IPDU-Sx	00:0C:82:08:00:B2	192.168.3.85	255.255.255.0	192.168.3.3	Submit	Blink LED
ENVIROMUX-2DB	00:0C:82:0E:00:08	192.168.3.83	255.255.255.0	192.168.3.3	Submit	Blink LED
VEEMUX-MXN-C5AV	00:0C:82:09:00:25	192.168.3.82	255.255.255.0	192.168.3.3	Submit	Blink LED
VEEMUX-DVI	00:0C:82:07:01:8B	192.168.3.86	255.255.255.0	192.168.3.3	Submit	Blink LED
		Submit All	Refresh	Close		

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 (**one field at a time**) and click on the **Submit** button on that row. Update the IP Address, Mask, and Gateway as needed, **one at a time**. If the tool discovers more than one device, the settings for all devices can be changed in the same fashion. (The “Submit All” button is **not supported** by this product.)

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

- To change more than one field;
1. Change a field, click **Submit**, wait 30 seconds as the ENVIROMUX reboots automatically,
 2. Click **Refresh** to update the discovered settings.
 3. Change another field, and repeat. Click **Close** when finished.

“Blink LED” is not supported on this product.

OPERATION VIA WEB INTERFACE

A user may monitor and configure the settings of the ENVIROMUX and any sensor connected to it using the Web Interface via any web browser (see page 2 for supported web browsers). To access the Web Interface, connect the ENVIROMUX to the Ethernet (page 8). Use the Device Discovery Tool (page 12) 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 25.) 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 25 -default address shown below) will be used. If a DHCP server on the network has assigned the IP address, use the Device Discovery Tool to identify the IP address to enter when logging in to the ENVIROMUX.

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

Log In and Enter Password

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

http://192.168.1.24

A log in prompt requiring a user name and password will appear:

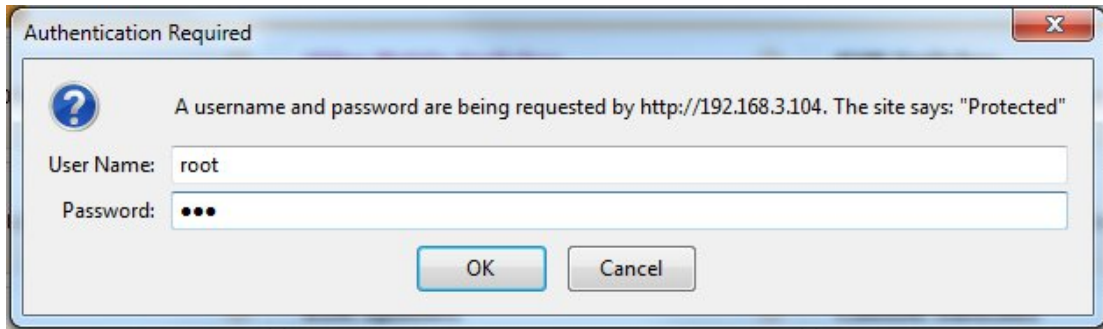


Figure 10- Login prompt to access web interface

User Name = root

Password = nti

(lower case letters only)

Note: *usernames and passwords are case sensitive*

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

The screenshot shows the NTI Network Technologies Incorporated web interface. The top right corner displays system information: Unit: Env Micro, Model: ENVIROMUX-MICRO, Uptime: 0 hours, 17 mins, 38 sec, and Current Time: 10-02-2015 3:53:44 PM. A navigation menu on the left includes Monitoring, Alerts, Smart Alerts, Administration, Log, Support, and Logout. The main content area is titled 'Summary' and contains several data tables:

Internal Sensors			
No.	Description	Value	Action
1	Internal Temperature	26.40 C	Edit
2	Internal Humidity	45.99 %	Edit
3	Internal Dew Point	13.84 C	Edit

External Sensors			
No.	Description	Value	Action
4	Temperature #2	28.12 C	Edit Delete
5	Humidity #2	45.97 %	Edit Delete
6	Dew Point #2	15.40 C	Edit Delete

Digital Inputs			
No.	Description	Value	Action
1	Digital Input #1	Open	Edit
2	Digital Input #2	Open	Edit

IP Devices			
No.	Description	Value	Action
Add New IP Device (maximum 4)			

Below the IP Devices table is a section for IP Cameras.

© 2014 Network Technologies Inc. All rights reserved.

Figure 11- Summary page

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

Function	Description
SUMMARY	Monitor the sensors, accessories, and IP devices of the ENVIROMUX (next page)
ALERTS	View and configure how alerts will be communicated to users (page 17)
SMART ALERTS	View and configure how smart alerts will be communicated to users (page 17)
ADMINISTRATION	Configure all system, network, multi-user access, and security settings as well as upgrade firmware (page 24)
LOG	View and manage the Event and Data Logs (page 34)
IP DEVICES	View the status of IP Devices located anywhere
SUPPORT	Links for downloading a manual, the MIB file, or firmware upgrades
LOGOUT	Log the user out of the ENVIROMUX web interface

Summary

Under Summary, the status of all sensors and IP Devices being monitored by the ENVIROMUX is displayed. Links to edit their description and for temperature and/or humidity sensors the scale can be changed between Fahrenheit and Celsius.

Summary

Integrated Sensors			
No.	Description	Value	Action
1	Temperature	27.11 C	Edit
2	Humidity	41.20 %	Edit
3	Dew Point	12.80 C	Edit

External Sensors			
No.	Description	Value	Action
1	Temperature #1	24.75 C	Edit Delete
2	Humidity #1	52.68 %	Edit Delete
3	Dew Point #1	14.43 C	Edit Delete
4	Temperature #2	24.75 C	Edit Delete
5	Humidity #2	55.71 %	Edit Delete
6	Dew Point #2	15.30 C	Edit Delete

Digital Inputs			
No.	Description	Value	Action
1	Digital Input 1	Open	Edit
2	Digital Input #2	Open	Edit

IP Devices			
No.	Description	Value	Action
Add New IP Device (maximum 4)			



IP Cameras	
Bench Camera 1	
Bench Camera 2	

Figure 12- Summary page

Summary

Integrated Sensors			
No.	Description	Value	Action
1	Temperature	27.11 C	Edit
2	Humidity	41.20 %	Edit
3	Dew Point	12.80 C	Edit
External Sensors			
No.	Description	Value	Action
1	Temperature #1	24.75 C	Edit Delete
2	Humidity #1	52.68 %	Edit Delete
3	Dew Point #1	14.43 C	Edit Delete
4	Temperature #2	24.75 C	Edit Delete
5	Humidity #2	55.71 %	Edit Delete
6	Dew Point #2	15.30 C	Edit Delete
Digital Inputs			
No.	Description	Value	Action
1	Digital Input 1	Open	Edit
2	Digital Input #2	Open	Edit

If the sensor is in alert status, the value will be shown in red text. To respond to the alert, open the Alerts page.

Alerts

Alerts				
No.	Sensor	Value	Status	Action
1	Internal Temperature	26.91 C	Normal	Edit Delete
2	Digital Input #1	Open	Alarm	Edit Delete Ack Dismiss

[Add New Alert](#)

Figure 13- List of alerts configured

From the Alerts page, the user has the option to either **acknowledge** the alert or **dismiss** it. If the user acknowledges the alert, no additional alert messages will be sent during that alert status cycle. If the user dismisses the alert, another alert message will be sent once the “notify again after” time designated on the configuration page (page 19) elapses.

The administrative user can open the alert configuration page by clicking on the **Edit** button under “Action” for that sensor. From the alert configuration page the user can apply settings to control how or if alert messages are sent in the event the sensor is in alert status.

Sensor Settings

To change the settings for a sensor, click on **Edit** on the Overview page. From the Sensor Settings page, you can change the description of the sensor as it appears in the overview page and as it will appear on alert messages you receive. For temperature sensors, you can also assign the unit of measure that is used for measurement and reporting.

Offset

The integrated temperature sensor is most accurate in environments where there is plenty of airflow around it. When the ENVIROMUX-MICRO is mounted in a location with little or no airflow, the integrated temperature sensor may be less accurate due to heat generated by nearby electronics. An "Offset" field is provided (for the integrated temperature sensor only) to allow you to enter a value that will compensate for stagnant air. The recommended Offset value in environments with little or no air movement is -1.5°C . The field will accept a value between -2.5° to 0°C .

Note: This value is always in Centigrade, even if the Temperature Unit is set to "°F".

To determine exactly how much the offset needs to be for your specific environment, you may want to use an accurate temperature measuring device in the same location as reference to assign a correction value to this field. Assign a value that will enable the reported temperature value report on the summary page to match your reference.

Sensor Settings

Description	Integrated Temperature <small>The description name for this sensor</small>
Unit	°C <small>Select Temperature Unit</small>
Offset	0.00 <small>Temperature Offset in C</small>

Figure 14- Sensor settings

Alerts

To view a list of what alerts have been configured for the sensors or IP devices, select Alerts from the side menu.

Alerts

Alerts				
No.	Sensor	Value	Status	Action
1	Internal Temperature	27.63 C	Normal	Edit Delete

[Add New Alert](#)

Figure 15- List of configured alerts and their status

To add an alert, click on “Add New Alert”. From the drop down box next to “Sensor”, select a sensor or IP device to configure an alert for.

Add Alert

The screenshot shows a form titled "Add Alert". At the top, there is a grey header "Sensor Selection". Below it, there is a "Sensor" dropdown menu currently showing "Internal Temperature". A list of options is visible below the dropdown, including "Internal Temperature", "Internal Humidity", "Internal Dew Point", "Temperature #1", "Humidity #1", "Dew Point #1", "Temperature #2", "Humidity #2", "Dew Point #2", "Digital Input #1", and "Digital Input #2". To the left of the dropdown is an "Add" button.

Figure 16- Select a sensor to add an alert configuration for

To edit settings for an alert, click on “Edit” next to the alert. The “Configure Alert” page will appear.

Configure Alerts

To configure how alerts are triggered and reported, the Configure Alert page is provided. From this page the user can determine who gets alert message and how.

Configure Alert

The screenshot shows the "Configure Alert" form. It has a grey header "Alert Settings". The form contains several fields and checkboxes:

- Associated Sensor:** Internal Temperature (with a dropdown arrow). Below it, the text "Sensor associated to this alert" is displayed.
- Groups:** A row of checkboxes for Group 1 through Group 8. Groups 1, 2, and 3 are checked.
- Trigger Event:** Greater than (with a dropdown arrow).
- Threshold:** 50.00 (with a text input field). Below it, the text "Threshold value" is displayed.
- Alert Delay:** 2 (with a text input field) (sec). Below it, the text "Duration the sensor must be out of thresholds before alert is generated" is displayed.
- Auto Acknowledge:** . Below it, the text "Automatically acknowledge alert when sensor returns to normal status" is displayed.
- Notify on return to normal:** . Below it, the text "Send a notification when this sensor returns to normal status" is displayed.
- Notify Again Time:** 120 (with a text input field) (min). Below it, the text "Time after which alert notifications will be sent again" is displayed.
- Enable Syslog:** . Below it, the text "Send alerts for this event via syslog" is displayed.
- Enable SNMP Traps:** . Below it, the text "Send alerts for this event via SNMP traps" is displayed.
- Enable E-mail Alerts:** . Below it, the text "Send alerts for this event via e-mail" is displayed.
- Enable SMS Alerts:** . Below it, the text "Send alerts for this event via SMS messages" is displayed.

At the bottom left of the form is a "Save" button.

Figure 17- Alert Configuration page for Temperature/Humidity sensors

Configure Alert

Alert Settings	
Associated Sensor	<input type="text" value="Digital Input#1"/> <small>Sensor associated to this alert</small>
Groups	<input type="checkbox"/> Group 1 <input type="checkbox"/> Group 2 <input type="checkbox"/> Group 3 <input type="checkbox"/> Group 4 <input type="checkbox"/> Group 5 <input type="checkbox"/> Group 6 <input type="checkbox"/> Group 7 <input type="checkbox"/> Group 8
Trigger Event	Open 
Alert Delay	<input type="text" value="0"/> (sec) <small>Duration the sensor must be out of thresholds before alert is generated</small>

Figure 18- Alert configuration for Digital sensor- minor difference

Alert Settings	Description
Description	The description of the sensor that will be viewed in the Summary page and in the body of alert messages - cannot be changed from this page (see Sensor Settings-page 17)
Group	Assign the alert to any group 1 -8
Units	This lets the operator choose between Celsius and Fahrenheit as the temperature measurement unit. (not applicable to digital sensors)
Trigger Event	Choose whether a threshold value greater than or less than the value entered under “threshold” will trigger an alert (not applicable to digital sensors) Select whether a sensor that is Open or one that is Closed will trigger an alert (digital sensors only)
Threshold	The user must define the lowest or highest (depending on the value assigned to “Trigger Event”) acceptable value for the sensor. If the sensor measures a value that exceeds this threshold, the sensor will move to alert status.
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.
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.
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 on return to normal " box for a sensor.
Notify Again Time	Enter the amount of time in minutes (1-999) before an alert message will be repeated
Enable Syslog	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
Enable SMS Alerts	Place a checkmark in this box to have alert notifications sent via SMS messages (not used as of this publication)

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

More about 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). Users (a maximum number of 9 including the root user) can receive alert messages from items in one or more groups (see user configuration on page 29).

Smart Alert

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

To begin, Events must be defined and configured. Events are sensor conditions to be notified of. Events logged based on the sensor configurations described on page 18 will be managed separately from events logged by these pre-defined Events. Sensor configuration for these Events will have no impact on the general configuration of your sensors. Pre-defined Events provide more control over what you want to be notified of.

From the side menu, select "Smart Alerts".

Smart Alerts



Figure 19- Smart Alerts page

On the Smart Alerts page, click on "Add Smart Alert".

Configure Smart Alert

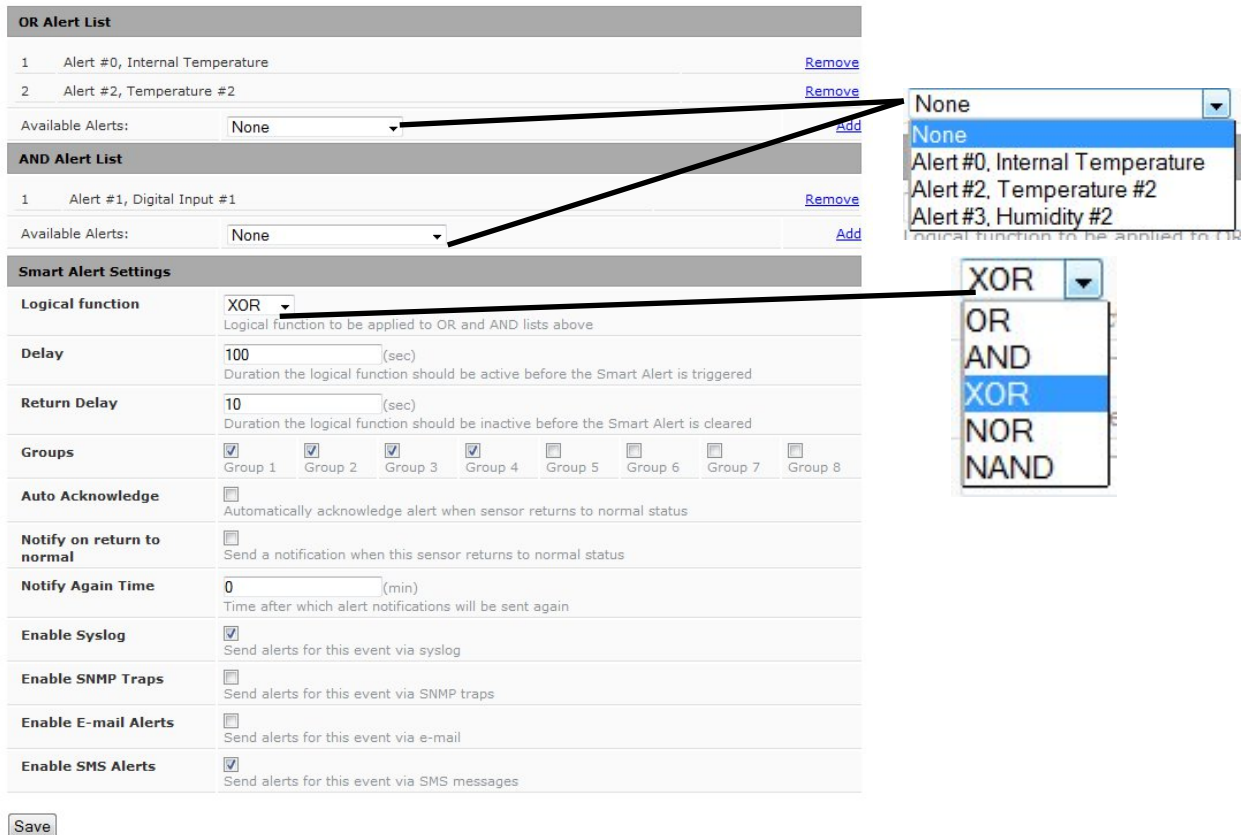


Figure 20- Sensor to be used for a predefined event

OR Alerts	
Available Alerts	Select from the predefined available Alerts (Figure 21) to have OR logic applied when that alert is triggered. One or more may be selected for a more complex configuration.
AND Alerts	
Available Alerts	Select from the predefined available Alerts (Figure 21) to have AND logic applied when that alert is triggered. One or more may be selected for a more complex configuration.
Smart Alert Settings	
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 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 logical function should be inactive before the Smart Alert will be cleared
Groups	Assign the Smart Alert to any group 1 -8 (see also page 19)
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.
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 on return to normal " box.
Notify Again Time	Enter the amount of time in minutes (0-999) before an alert message will be repeated
Enable Syslog	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
Enable SMS Alerts	Place a checkmark in this box to have alert notifications sent via SMS messages (not used as of this publication)

In the “OR” Alert List section, select from the drop-down list which alert configuration(s) to associate with the “OR” part of the Smart Alert equation. After each is selected, click “Add”.

For the “OR” logic to be effective, more than one would be selected. This would mean that **either** alert condition being triggered would satisfy this half of the logic equation.

In the “AND” Alert List section, select from the drop-down list which alert configuration(s) to associate with the “AND” part of the Smart Alert equation. After each is selected, click “Add”.

For the “AND” logic to be effective, more than one would be selected. This would mean that **both** alert conditions would have to be triggered to satisfy this half of the logic equation.

Next select the Smart Alert Settings to be used with your alert selections. The Logical function you select will determine the combined situation that would trigger a Smart Alert message to be sent.

After all options are selected, click the “Save” button. This Smart Alert will now be added to the Smart Alerts page (Figure 19). Only one Smart Alert can be defined.

More on Logical Functions

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

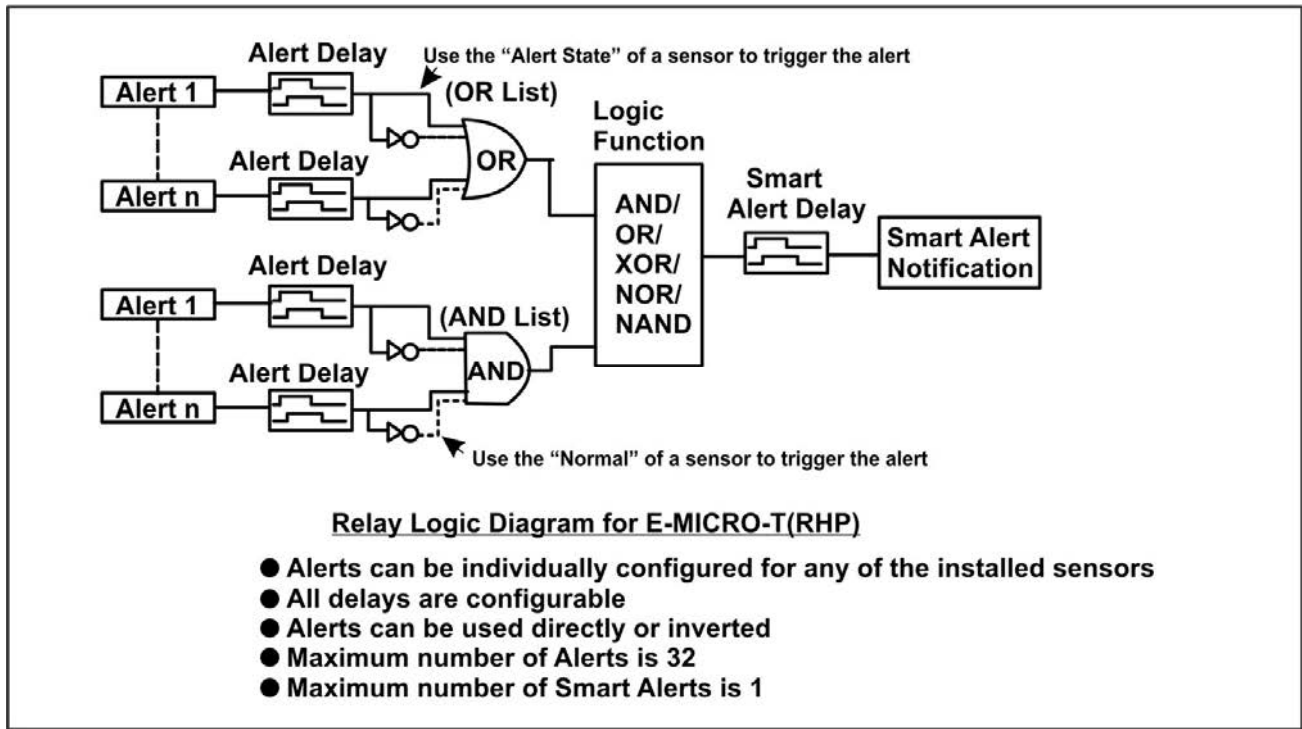


Figure 21- Event Logical Function Diagram

Smart Alert Rules:

- Any configured Alert can be applied to either the OR Alerts list or the AND Alerts list, or both lists.
- Alerts can be configured to be triggered by a sensor or monitored IP 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** Alert in the OR list is triggered, the output value of the OR list will be 1.
 - **All** Alerts 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.

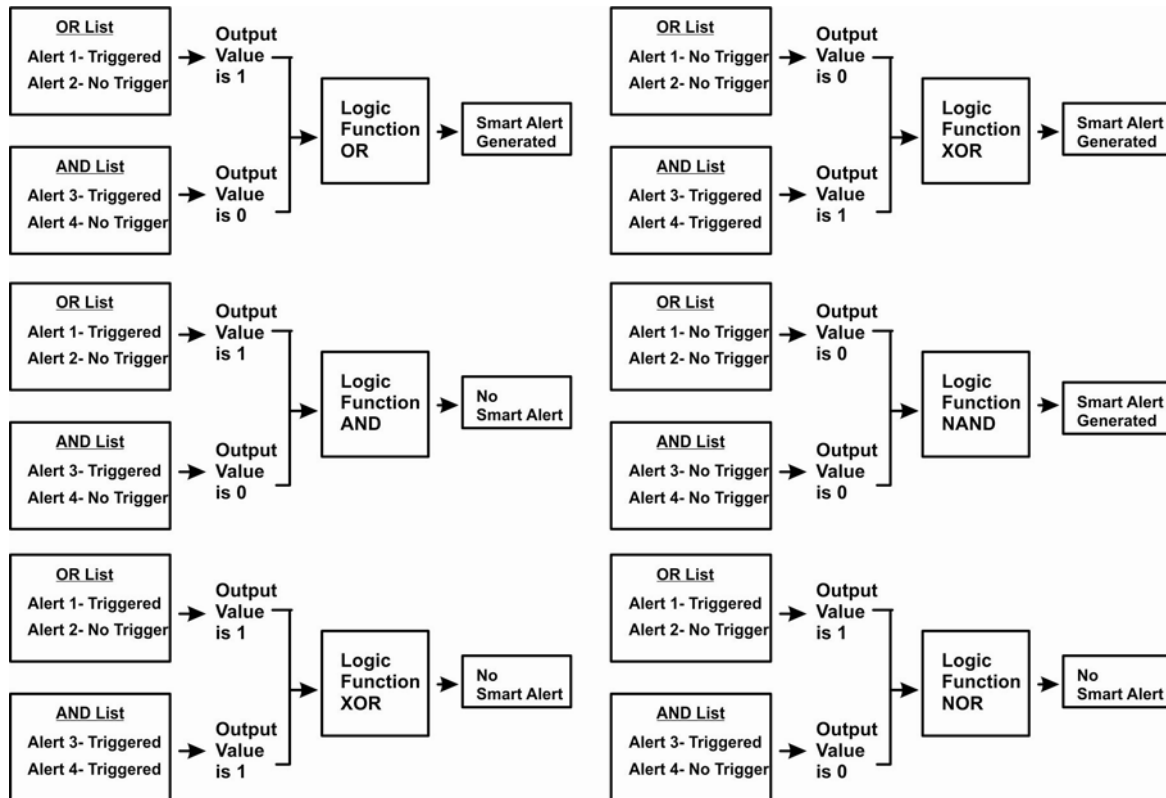


Figure 22- Examples of Smart Alert conditions

Administration

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

Administration
System
Network
SNMP
Email Server
Time
Users
IP Cameras
Firmware Update

System	Fields for applying time zone, date, time, NTP server, and backup and restore configuration settings
Network	Fields for providing all the network settings of the ENVIROMUX including IP address and DNS settings
SNMP	Fields for using SNMP
Email Server	Fields for setting up the ENVIROMUX email account
Time	Fields for setting time and date
Users	Fields for assigning users, access privileges, passwords and contact settings
IP Cameras	Fields for entering IP cameras to be monitored
Firmware Update	For updating the firmware of the ENVIROMUX when improved software becomes available.

System Settings

The System Settings section displays the Serial number, MAC Address, SNMPv3 Engine ID and Unit Name of the ENVIROMUX-MICRO. Only the Unit Name is user-configurable. To view the System Configuration page, click on **System** from the **Administration** section of the menu.

From the System Settings page the GSM Modem Status can also be viewed. The GSM Modem feature is reserved for future use.

System Settings

Serial Number:	E03
MAC Address:	00:0c:82:15:00:03
SNMPv3 Engine ID:	80001f8803000c82150003
Unit Name	<input style="width: 100%;" type="text" value="E-MICRO-E03"/> <small>Name assigned to this unit</small>

GSM Modem Status

Modem Status:	Not Connected
IMEI:	N/A
Signal Power:	N/A

© 2014,2016 Network Technologies Inc. All rights reserved.

Figure 23- System Settings page

Reboot the System

The ENVIROMUX can be remotely rebooted by anyone with administrative privileges. Click the **Reboot** button to cause the ENVIROMUX to reboot. This will disconnect any user and shut down all activity.

Network Configuration

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

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

Network Settings

Enable DHCP	<input type="checkbox"/>	Method of acquiring IP settings	Note: The values applied here are for local (static) address configuration only.
IP Address	<input type="text" value="192.168.3.103"/>	Statically assigned IPv4 address	
Subnet Mask	<input type="text" value="255.255.255.0"/>	Statically assigned IPv4 subnet mask	
Default Gateway	<input type="text" value="192.168.3.3"/>	Statically assigned IPv4 default gateway	
Preferred DNS	<input type="text" value="192.168.1.52"/>	Statically assigned preferred name server	
Alternate DNS	<input type="text" value="166.102.165.11"/>	Statically assigned alternate name server	
Web Server Type	<input type="text" value="HTTP"/>	Type of web server	
Enable Telnet	<input checked="" type="checkbox"/>	Enable Telnet	

Figure 24- Network Settings page

Network Settings	Description
Enable DHCP	Leave this blank for Static (manual IP setting) or enter a checkmark for DHCP (automatic IP settings) Note: If you select "DHCP", make sure a DHCP server is running on the network the ENVIROMUX is connected to.
IP Address	Enter a valid IP address (default address is 192.168.1.24)
Subnet Mask	Enter a valid subnet mask (default value shown above)
Default Gateway	Enter a valid gateway
Preferred DNS	Enter a preferred domain name server address
Alternate DNS	Enter an alternate domain name server address
Web Server Type	Select HTTP to enable non-secure browser access (default) or HTTPS for secure access.
Enable Telnet	Place a checkmark in this box to enable Telnet access to the Text Menu (default is disabled)

For added network security, leave the "Enable Telnet" block unchecked to prevent access to the E-MICRO-T(RHP) Text Menu (page 39).

When "Enable DHCP" is checked, 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 "IP Address" field will be used. If a DHCP server on the network has assigned the IP address, use the Device Discovery Tool (page 12) to identify the IP address to enter when logging in to the ENVIROMUX.

Note: If you are going to use the HTTPS Web Server Type, be aware that navigation between screens on the web interface will be a bit slower due to the added security encryption and decryption that is happening between the ENVIROMUX and your browser.

SNMP Settings

The SNMP Settings page contains the user configurable settings for using SNMP.

SNMP Settings

The screenshot displays the 'SNMP Settings' configuration interface. It includes the following fields and options:

- Read Community:** A text input field containing 'public'. Below it, the text reads 'Read community name for SNMP agent'.
- Write Community:** A text input field containing 'private'. Below it, the text reads 'Write community name for SNMP agent'.
- Trap Type:** A dropdown menu currently set to 'SNMPv2c'. Below it, the text reads 'Select type of traps accepted'.
- Agent Type:** A dropdown menu currently set to 'SNMPv1/v2/v3'. Below it, the text reads 'Select type of SNMP Agent enabled'.

An expanded dropdown menu for 'Agent Type' is shown to the right, with three visible options: 'SNMPv1/v2/v3' (highlighted in blue), 'SNMPv1/v2/v3', and 'SNMPv3'. An arrow points from the 'Agent Type' field to this expanded menu. A 'Save' button is located at the bottom left of the form.

Figure 25- SNMP Settings

SNMP Settings	
Read community	Enter applicable read-only community name (commonly used- "public")
Write community name	Enter applicable read-write community name (commonly used- "private")
Trap Type	Select the type of traps that will be accepted by your software, v1 or v2c.
Agent Type	Select the type of SNMP Agent that is enabled, between SNMPv1/v2c/v3 or SNMPv3 only (Note: A change to this feature requires a system reboot to take effect.)

Read-Only Community Name

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

Read-Write Community Name

(not applicable as of this printing)

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

SNMP v3 Traps

The support in this device for SNMP v3 is limited to receiving readings or alert messages via polling. It does not include support for SNMP v3 traps. For more SNMP settings, see page 30

Email Server Settings

Email Server Settings

Common Port numbers:
 Default: 25 (Not secure)
 TLS: 465 (Secure)
 STARTTLS: 587 (used by Gmail)
 Contact your network administrator or email service provider for required settings.

Choose between TLS, STARTLS or None for the encryption type supported by the email provider.

Uncheck "Use Authentication" if no authentication is supported. If STARTLS or TLS is selected, then this must also be checked.

Password only needed if using authentication

Use this button to make sure your server and user email settings are correct.

Figure 26- Email Server Settings

Email Settings	Description
E-mail	Enter a valid email address the ENVIROMUX-MICRO can send emails <u>from</u>
SMTP Server	Enter a valid SMTP server name (e.g. yourcompany.com)
SMTP Encryption	If your server does not support encryption, select NONE. Otherwise, select between TLS or STARTTLS authentication methods, depending upon the type your server supports.
Port	Enter a valid port number (default port is 25, for TLS use 465, for STARTTLS use 587)
Use Authentication	Place a checkmark in the box if the SMTP server requires authentication to send email Note: If "TLS" or "STARTTLS" is selected, then this must also be checked.
Username	Enter a valid username to be used by the ENVIROMUX to send emails
Password	Enter a valid password assigned to the ENVIROMUX username

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 commonly assigned SMTP server port number is "25". For SMTP servers that support TLS, use port number 465. You may need to contact your email service provider to determine the correct port number setting.

The E-MICRO-T(RHP) sends alert messages using TLS authentication (supported by Google's Gmail). In choosing an email service to use with your E-MICRO-T(RHP), make sure that service either supports:

- 1) TLS v1.2 secure encrypted authentication,
- 2) STARTTLS secure encrypted authentication,
- 3) Standard authentication (authentication where just a username and password are required (non-encrypted)), or
- 4) messages sent with No authentication (no username or password required).

Once the email server settings are configured and the user settings are configured (page 29), click on "Test Email" button to verify that the configuration has been done correctly. Each configured user will receive an email from the ENVIROMUX-MICRO email address that reads "Test Email Configuration" in the body of it.

Note: The E-MICRO-T(RHP) does not support Microsoft Office 365.

If the message is not deliverable, due to wrongly entered settings or an invalid email address, an error will be recorded in the Event Log (page 34). **Event Log**

Email error in Event Log

Jump to page: 1 Entries per page: 10

Showing Entries 1 - 2 of 2 Event Log Free Space: 99.0%

Date/Time	Type	Value	Description
02-19-2016 10:23:42 AM	Start-Up	4	System auto restart, configuration checksum correct
02-19-2016 3:12:25 PM	E-mail Error		SMTP server name cannot be resolved

Delete Selected Clear Log

Time Settings

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.

Time Settings

Time Zone	(GMT-05:00) Eastern Time <small>Select Time Zone</small>
Enable DST	<input checked="" type="checkbox"/> Automatically adjust clock for daylight saving changes
Date Format	MM-DD-YYYY <small>Select Date Format</small>
Time Format	AM/PM <small>Select Time Format</small>
Enable NTP	<input checked="" type="checkbox"/> Get system time via Network Time Protocol
NTP server	0.nti1.pool.ntp.org <small>Address of the NTP server</small>
NTP Frequency	120 <small>Frequency, in minutes, at which to query NTP server (minimum 5 minutes)</small>

Save

Set Local Time

Year	Month	Day	Hour	Minutes	Seconds	
2016	2	11	9	36	51	Set Time
<small>(yyyy)</small>	<small>(1-12)</small>	<small>(1-31)</small>	<small>(0-23)</small>	<small>(0-59)</small>	<small>(0-59)</small>	

© 2014,2016 Network Technologies Inc. All rights reserved.

Figure 27- Time and Date Settings

Time Settings	Description
Time Zone	Enter the appropriate time zone
Enable DST	Apply a checkmark to have the time change according to Daylight Saving Time rules
Date Format	Set for AM/PM or 24 Hour format
Time Format	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 (the default NTP server is 0.nti1.pool.ntp.org)
NTP Frequency	Enter the frequency (in minutes) for the ENVIROMUX to query the NTP server (minimum is 5 minutes)

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

Set Local Time

Enter the date and your local current time of day. Then click **“Set Time”**. Entries here take immediate effect.

Users

Select Users from the side menu to display a list of the users that have been configured to access the ENVIROMUX. A maximum of 8 users (other than root) can be configured. From this page you can either choose to edit a user's configuration, delete them from the list, or add new users.

Users

Users				
No.	Username	Admin	Last Login	Action
1	root	yes	--	Edit
2	adrian	yes	--	Edit Delete

[Add New User](#)

Figure 28- Users List

Click "Add New User" to add "userx" to the list. To delete a user and their configuration, click on "Delete" link.

Users

Users				
No.	User Name	Admin	Action	
1	root	yes	Edit	
2	adrian	no	Edit Delete	
3	user2	no	Edit Delete	

[Add New User](#)

Figure 29- User2 added- ready to configure

Click "Edit" to bring up the User Settings.

User Settings

Account Settings	
Username	<input type="text" value="Test"/> <small>The username for this user</small>
Admin	<input checked="" type="checkbox"/> Grant this user administrative privileges
Password	<input type="password" value="••••••"/> <small>The user's password to login to the system (for local authentication)</small>
Confirm	<input type="password" value="••••••"/> <small>Confirm the entered password</small>

Figure 30- Initial 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
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

When adding a new user, the Configure User page will open with the username "userx" assigned, where x = the next consecutive number (up to 8) 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.

Note: A change to these features requires a system reboot to take effect.

Enable Remote Datalog to have the user receive datalog reports via Syslog

Figure 31- User Settings-Contact Settings

Contact 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 19 and 37 for group assignments)
Email alerts	Place a checkmark if the user should receive messages via email
Email address	Enter a valid email address if this user should receive email alert messages- Tip: Address can be user's telephone number and carrier to receive SMS messages on their cell phone (i.e. 1234567890@vtext.com for Verizon)
Email datalog	Place a checkmark if the user should receive sensor datalog reports via email
Datalog Email Frequency	Select the frequency to receive datalog reports- 30min, 1hr, 2hr,4hr,6hr or 8hr increments (Sensors report to the datalog once each minute)
Syslog alerts	Place a checkmark if the user should receive alerts via syslog messages
SNMP traps	Place a checkmark if the user should receive alerts via SNMP traps (v1 or v2c only)
Syslog/SNMP IP address	Enter a valid syslog/SNMP IP address for the user to receive syslog/SNMP messages (alerts and/or data logs, as configured)
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 readings or alert messages
Privacy Protocol	Choose between AES and DES 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 polling
Syslog Facility	Select a Syslog Facility for the messages to be sent to- Local0 thru Local7 (default is Local0).
SMS Alerts	Not used as of this publication
SMS Number	Not used as of this publication
Remote Datalog	Enter a checkmark if this user should receive sensor datalog reports via syslog at a rate of once each minute

Schedule

Use Schedule	<input type="checkbox"/> Configure the user's schedule type	Note: If "Use Schedule" is checked, and the "Test Email" button is clicked (page 27), Users who are not scheduled to be active at the time of the "test" will not receive a test email.
First day	Sun ▾ <small>First day of the week when the user is active</small>	
Last day	Sun ▾ <small>Last day of the week when the user is active</small>	
First hour	0:00 ▾ <small>Starting hour for the user's daily schedule</small>	
Last hour	22:00 ▾ <small>Ending hour for the user's daily schedule</small>	

Figure 32- User Settings- User Active Schedule

Schedule Settings	
Schedule Type	Without Checkmark- user will receive messages at all hours of each day With Checkmark- user will only receive alert messages during times as outlined below
Start Day	First day of the week the user should begin receiving messages
Last Day	Last day of the week the user should receive messages
First Hour	First hour of the day the user should begin receiving messages
Last Hour	Last hour of the day the user should receive messages

More about User Privileges

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

Users with user rights can see the current readings of monitored items, change their own passwords, configure alerts, configure the Smart Alert, and view Data and Event Logs.

More about SNMP v3

The support for SNMP v3 is limited to receiving readings or alert messages via polling. It does not include support for SNMP v3 traps.

Making a change to the Authentication Protocol, Authentication Passphrase, Privacy Protocol, or Privacy Passphrase requires a reboot of the E-MICRO-T(RHP) to take effect.

IP Cameras

Up to 4 IP Cameras can be monitored by the ENVIROMUX. The ENVIROMUX will display the video from specified IP addresses and provide images at 320 x 240 resolution. To see a list of IP cameras on the “IP Cameras” link in the side menu.

IP Cameras

IP Cameras		
No.	Name	Action
1	IP Camera #1	Edit Delete

[Add New IP Camera](#)

Figure 33- IP Camera Monitoring

To add an IP Camera, click on “Add New IP Camera.”

IP Camera Settings

Name	<input type="text" value="IP Camera #1"/> <small>The name assigned for this IP Camera</small>
Image URL	<input type="text"/> <small>Full path of the image file of the IP camera</small>
IP Address	<input type="text"/> <small>IP address of the IP camera</small>
Refresh Rate	<input type="text" value="10"/> (x100 msec) <small>Refresh rate of the image in hundreds of milliseconds</small>

Figure 34- Configure IP Cameras

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

Update Firmware

The Update Firmware page is used to change the firmware of the ENVIROMUX. Occasionally new features or changes to existing features will be introduced and new firmware with these changes will be made available on the NTI website (<http://www.networktechinc.com/download/d-environment-monitor-micro.html>). To view the Update Firmware page, select **Firmware Update** 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.

Firmware Revision:	1.10
Build Date:	Nov 9 2015 09:03:39
Update file	<input type="button" value="Browse..."/> No file selected. Choose the firmware update file.

Figure 35- Update Firmware page

Note: We recommend using the HTTP Web Server Type (page 25) when performing a firmware update.

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

Log

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

Overview
Alerts
Administration
Log
Event Log
Data Log
Logout

Event Log	View a log listing the date and time of startups and alerts
Data Log	View graph of data readings from sensors and IP addresses

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

Event Log

Jump to page: Entries per page:

Showing Entries 1 - 4 of 4 Event Log Free Space: 98.0%

<input type="checkbox"/>	Date/Time	Type	Value	Description
<input type="checkbox"/>	10-03-2015 1:32:14 PM	Start-Up	1	System start-up, configuration checksum correct
<input type="checkbox"/>	10-03-2015 1:32:36 PM	Alert	Closed	Digital input entered alert status
<input type="checkbox"/>	10-03-2015 1:32:36 PM	Alert Return	Open	Digital input returned to normal status
<input type="checkbox"/>	10-03-2015 1:32:36 PM	Smart Alert	0	Smart Alert cleared

Select all

→

Figure 36- 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.

View Data Log

The Data Log provides the administrative user with a graphical representation of all the analog sensor readings (no digital sensors) taken by the ENVIROMUX pertaining to the sensors being monitored. The event log will record the date and time of each reading and display those readings in a chart. Additionally, readings taken from digital sensors can be found in the log file if downloaded to a PC.

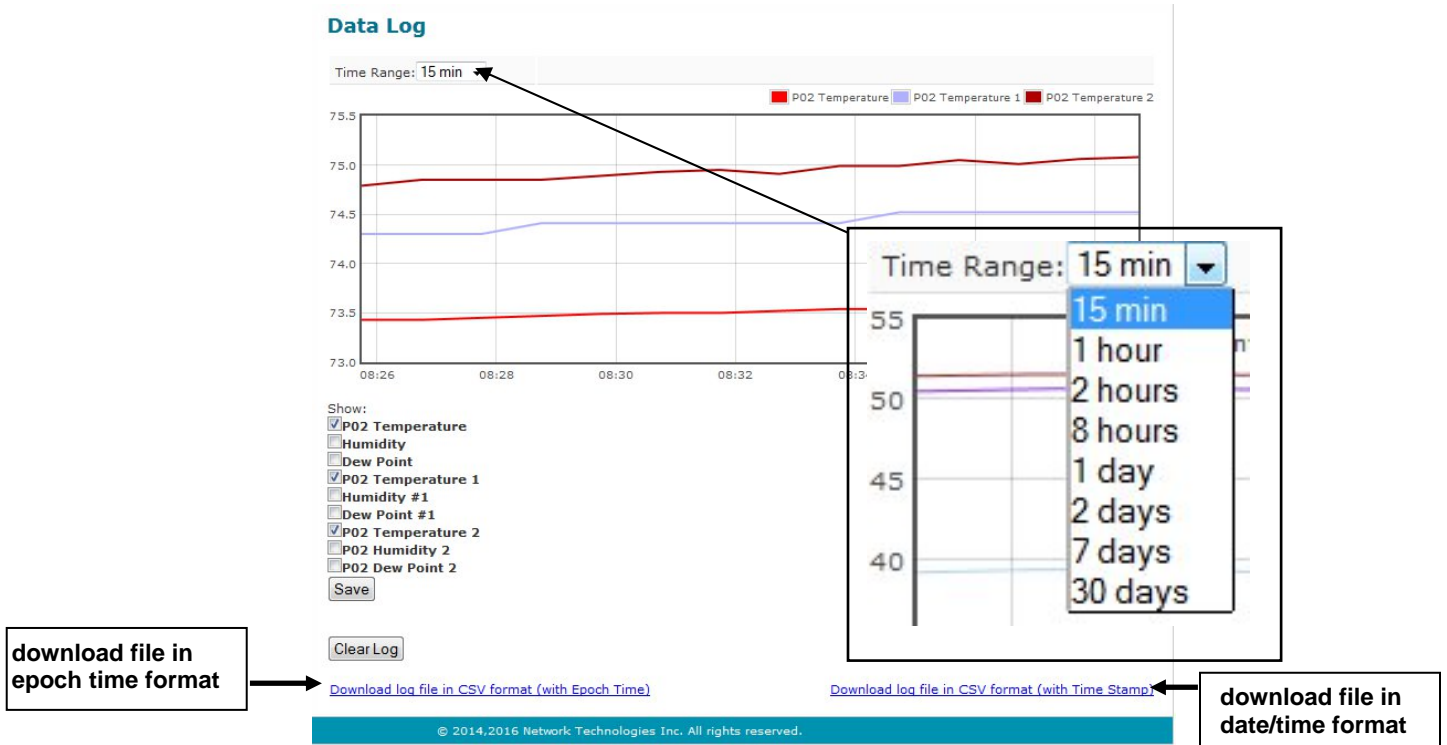


Figure 37- Data Log page

From the Data Log page the administrative user can view the logs, select specific logs to not be shown or press **Clear Log** to clear them all. The time range of readings shown can be changed for the user’s viewing preference, from as little as 15 minutes up to 30 days.

To hide specific log entries, remove the checkmark for each sensor to be hidden, and press **Save**. Before clearing the log, the user may want to save the log for future reference and to make space for more logs by downloading the data log to a file on a PC. Click on “**Download log file in CSV format**” to save the log file before clearing it. The log file can be saved with either an Epoch time format or in a standard date/time format.

Data logs that are sent via syslog and/or email (page 29) will be in CSV format and will include data for all sensor ports whether they are in use or not. (See examples on next page.) If an External Sensor port is not in use, the data log will include the entry “N/A”. A Digital Input sensor port not in use will be reported as “Open”.

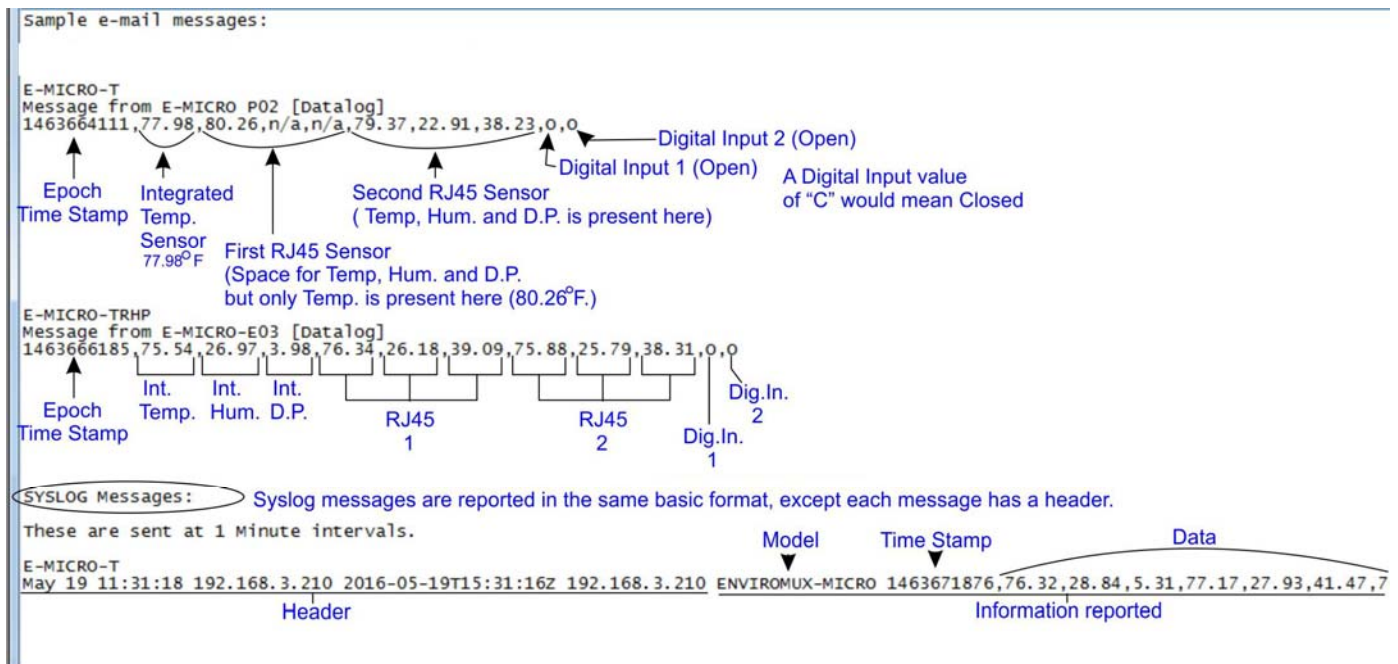


Figure 38- Examples of emailed datalogs

IP Devices

IP devices such as servers, routers, cameras, etc. can be monitored (up to 4) to make sure network connections are open to them. In order to monitor an IP Device the devices must be added to the list of IP Devices being monitored. From the **Monitoring** page, click on **Add New IP Device**.



Figure 39- IP Devices listing-none monitored yet

The IP Device Configuration page will immediately open. Here you can configure the ENVIROMUX to ping the IP Device (up to 4) as often as desired and to react to a lack of response by sending alert messages.

IP Device Settings

Description	<input type="text" value="IP Device #1"/> <small>The description name for this IP device</small>
IP Address	<input type="text" value="192.168.0.1"/> <small>The IP address of the device</small>
Ping Period	<input type="text" value="600"/> (sec) <small>The frequency at which to ping the device</small>
Retries	<input type="text" value="3"/> <small>The number of tries before device is considered in alarm (max 20)</small>
Timeout	<input type="text" value="2"/> (sec) <small>Duration, in seconds, to wait for a response to a ping</small>

Figure 40- IP Device Configuration page

IP Device Settings	Description
Description	The description of the IP Device that will be viewed in the Summary page and in the body of alert messages
IP Address	The IP address of the IP Device
Ping Period	Enter the frequency in seconds that the ENVIROMUX should ping the IP Device (range is 10 to 60000)
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. Range is Min = 0, Max = 20
Timeout	Enter the length of time in seconds (up to 10) to wait for a response to a ping before considering the attempt a failure

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

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

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

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

The alert settings and data logging are the same as for sensor configuration, described on page 17.

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

IP Devices			
No.	Description	Value	Action
1	IP Device #1	Not Responding	Edit Delete
2	IP Device #2	Responding	Edit Delete

[Add New IP Device \(maximum 4\)](#)

Figure 41- IP Device list with new devices added

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.

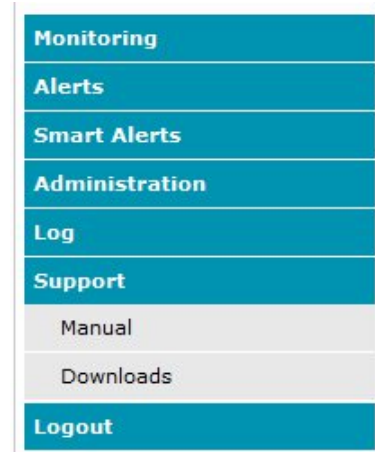


Figure 42- Support

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 point you can close your browser or log back in.



Figure 43- Logout

OPERATION VIA TEXT MENU- ENVIROMUX

The ENVIROMUX can be controlled through a text menu using the Telnet provided a connection has been made to the Ethernet Port (page 8) and provided Telnet has been enabled (page 25). The text menu can be used to view sensor data, sensor alert status, and network settings of the ENVIROMUX as an alternative to the Web Interface (page 13).

Note: Some terminal programs must be configured to use the Raw protocol instead of Telnet (i.e. Putty) due to extra features used by the program that aren't supported by the ENVIROMUX. In either case, be sure to configure the terminal program to use port 23.

Note: Only one user can connect to the Text Menu at a time.

Connect to ENVIROMUX from Terminal through Ethernet

The Text Menu can be accessed using a Terminal program such as HyperTerminal, TeraTerm, Putty, etc.. provided the ENVIROMUX is properly connected to your LAN through the Ethernet port (page 8).

1. Enter the IP address of the ENVIROMUX,
2. Select the Telnet connection type (you may have to use Raw, depending upon your program features),
3. Make sure the port number assigned is "23".

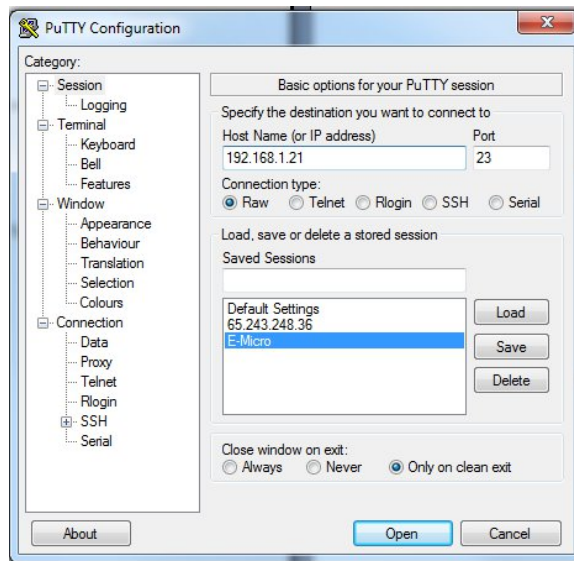


Figure 44- Terminal connection through Ethernet port

4. Make sure the ENVIROMUX is powered ON.
5. Press <Open> and a login prompt will appear- "micro login:" , type <root> (all lowercase letters) and press <Enter>.
6. At "User: " type <root> (all lowercase letters) and press <Enter>.
7. At "Password" type <nti> (all lowercase letters) and press <Enter>.



Figure 45- Text Menu Login screen

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

Connect to ENVIROMUX from Command Line

To access the Text Menu from the command line, the ENVIROMUX must first be connected to the Ethernet (page 8).

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

```
telnet <ENVIROMUX IP address>
```

<ENVIROMUX IP address> is the IP address assigned by the DHCP server unless you have manually assigned one. (default is 192.168.1.24).

The user will be prompted for username and password to connect to the ENVIROMUX. The default user is “**root**” and password is “**nti**”

The main menu of the Text Menu will be displayed.

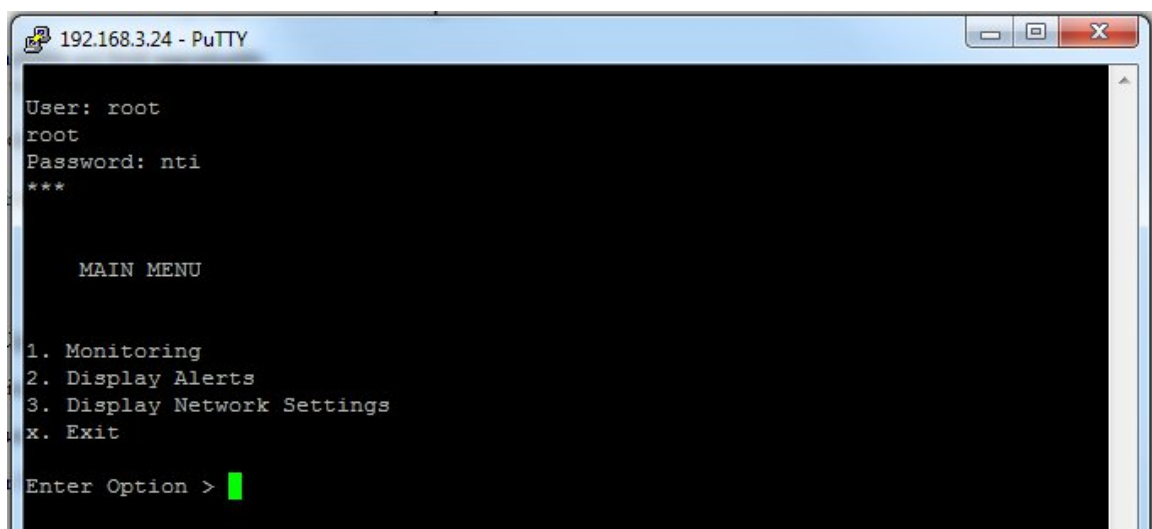


Figure 46- Text Menu- Administrator Main Menu

Using the Text Menu

Text Menu Navigation

For some terminal programs, just pressing the keyboard number associated with the menu item will select and execute that choice. For other terminal programs, you will additionally need to press the <Enter> key after pressing the number.

Depending upon the terminal program you use, and its configuration, keystrokes entered may or may not be visible. For example, when you enter <1> - <Enter> to select the Monitoring menu, you may see “1” appear next to “Enter Option” or you may not.

When prompted to “Press any key to continue.....” press any key followed by <Enter> to return to the last menu.

The Main Menu is broken into 3 categories:

Function	Description
Monitoring	Monitor the sensors, digital inputs and IP devices
Display Alerts	Show the status of any configured alerts
Display Network Settings	Show the values of each of the network settings

Monitoring

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

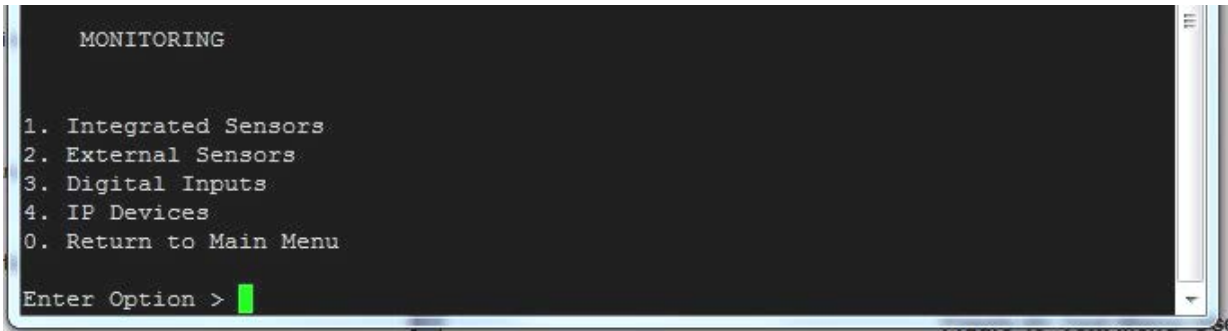


Figure 47- Text Menu-Monitoring Menu

View Sensors

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

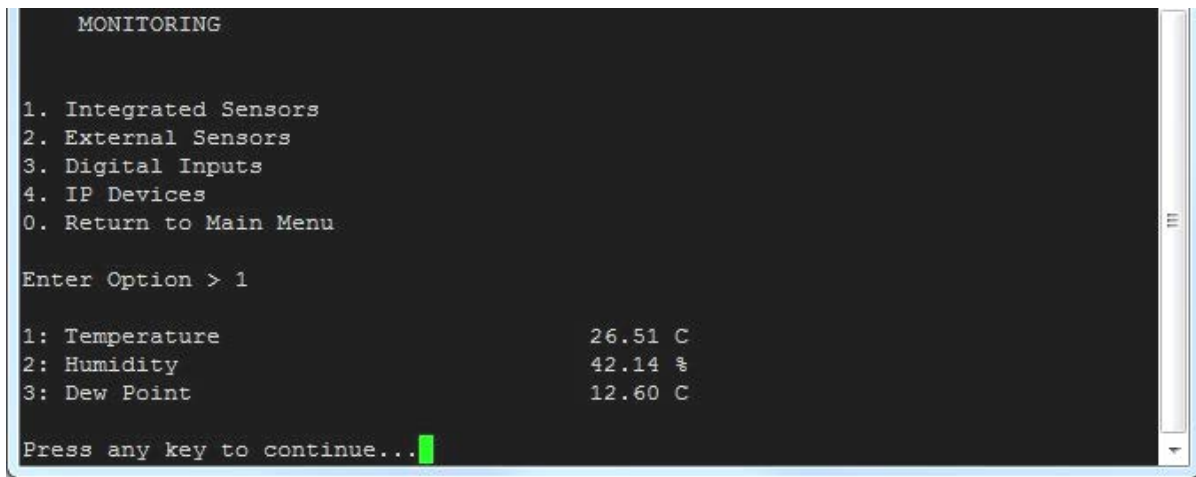


Figure 48- Text Menu-Sensor Status

Digital Inputs

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

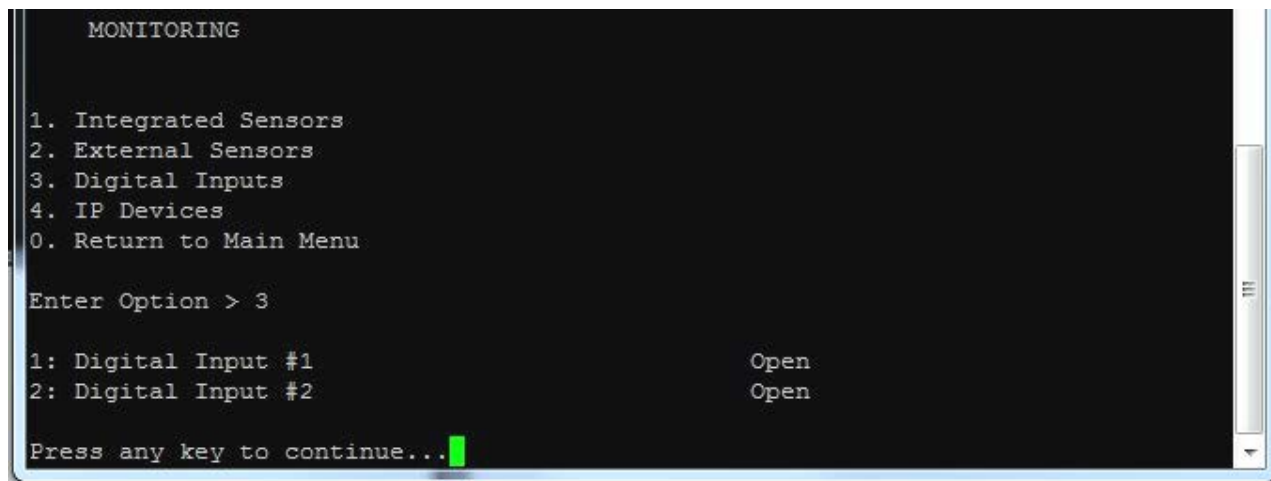


Figure 49- Text Menu- Digital Input Status

IP Devices

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

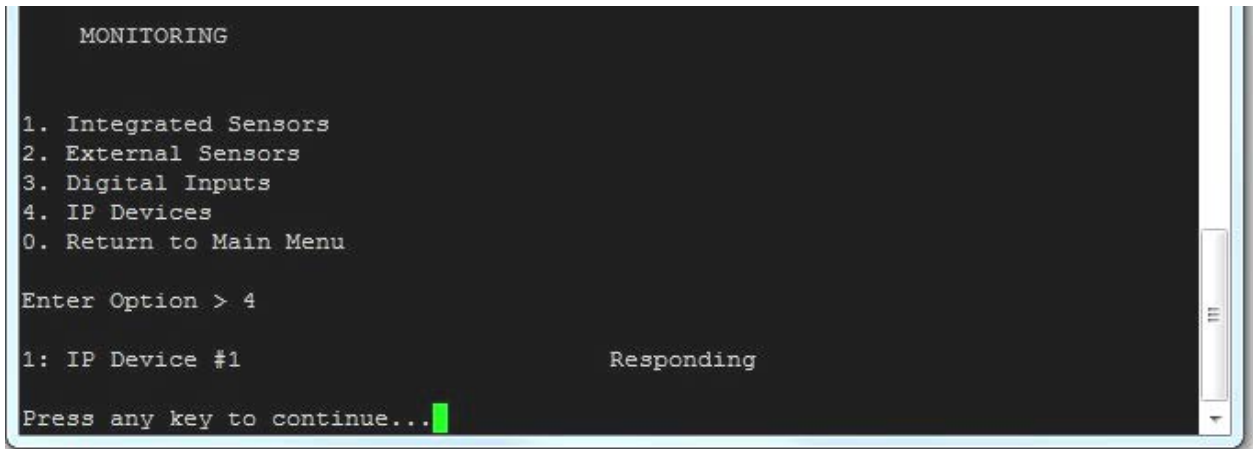


Figure 50- Text Menu-View IP Devices

Display Alerts

Select "Display Alerts" to see the current status of each alert. It will show the status of the sensor being monitored and it will indicate if the sensor is in alert status or normal.

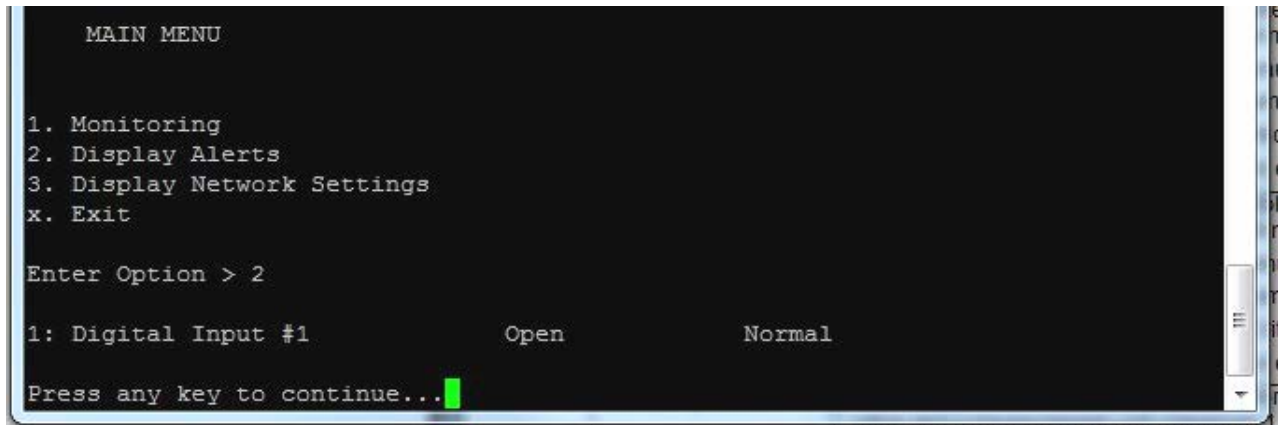
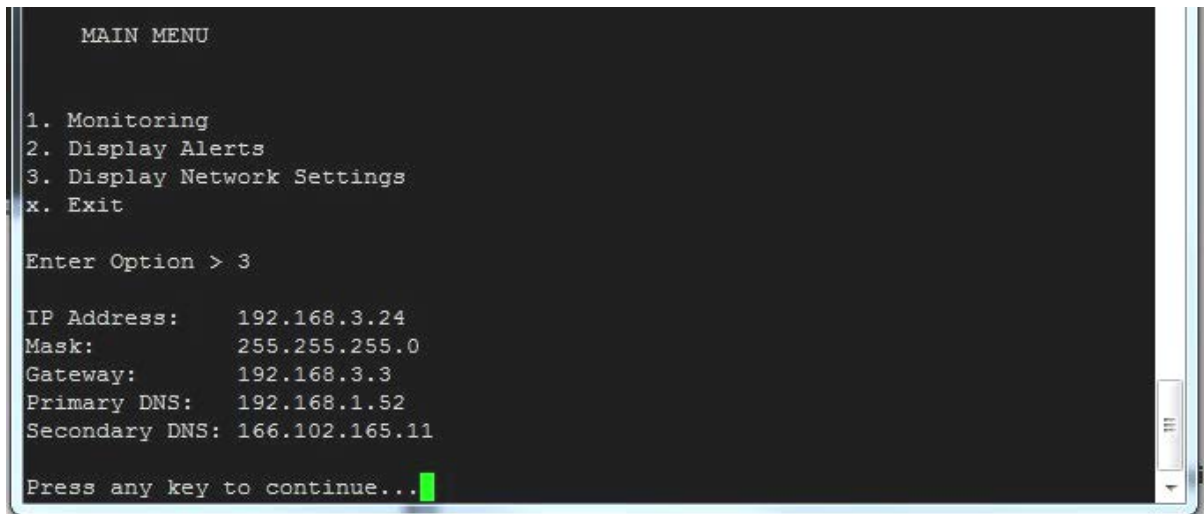


Figure 51- Text Menu-Configure Sensors list

Display Network Settings

Select "Display Network Settings" to view the current Network configuration of the ENVIROMUX.

A screenshot of a terminal window displaying a text-based menu. The menu is titled "MAIN MENU" and lists four options: "1. Monitoring", "2. Display Alerts", "3. Display Network Settings", and "x. Exit". Below the menu, the prompt "Enter Option > 3" is shown. The network configuration details are listed as follows: "IP Address: 192.168.3.24", "Mask: 255.255.255.0", "Gateway: 192.168.3.3", "Primary DNS: 192.168.1.52", and "Secondary DNS: 166.102.165.11". At the bottom, the prompt "Press any key to continue..." is displayed with a green cursor. The terminal window has a standard Linux-style window border with a title bar and a scrollbar on the right side.

```
MAIN MENU

1. Monitoring
2. Display Alerts
3. Display Network Settings
x. Exit

Enter Option > 3

IP Address: 192.168.3.24
Mask: 255.255.255.0
Gateway: 192.168.3.3
Primary DNS: 192.168.1.52
Secondary DNS: 166.102.165.11

Press any key to continue...
```

Figure 52- Text Menu-Network Settings

Press <x> to exit the text menu.

RESTORE DEFAULTS BUTTON

A “Restore Defaults” button is located on the front of the E-MICRO-T(RHP). 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.

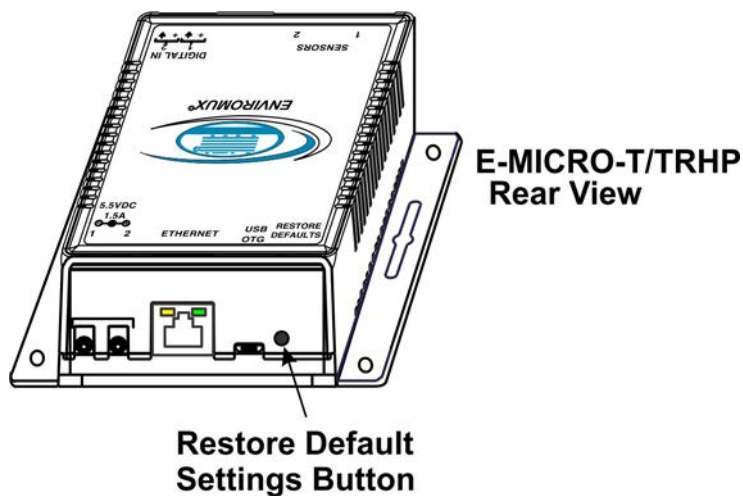


Figure 53- Location of Restore Defaults button

Note: If “Restore Defaults” is used, the IP address will also be restored to its default address of 192.168.1.24 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 12).

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 assigned to the ENVIROMUX to the Email Server Settings Page (see page 27) to send notifications from.

Email Server Settings

E-mail	<input type="text" value="user@gmail.com"/> E-mail sender address for this unit
SMTP Server	<input type="text" value="smtp.gmail.com"/> SMTP server used when sending e-mails
SMTP Encryption	TLS Select the type of SMTP Encryption to use in email
Port	<input type="text" value="465"/> SMTP server port. Usual Port #- for no encryption: 25, TLS: 465, STA
Use Authentication	<input checked="" type="checkbox"/> SMTP server requires authentication to send e-mail
Username	<input type="text" value="user@gmail.com"/> Username for sending e-mails
Password	<input type="password" value="••••••••"/> Password for sending e-mails

For TLS support , enter 465
For STARTTLS, enter 587

Must fill in when authentication is required

Figure 54- Email Server Settings example for sending emails

Note: When authentication is required (check your email server requirements) the Username and Password must be entered. If no authentication is required, uncheck “Use Authentication” and the Username and Password fields can be left empty.

2. Fill in Email Settings (page 25) 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 (someone.com), sometimes characters are added (mail.someone.com, smtp.someone.com, smtp-mail.someone.com, etc)
- B. The default port is 25. If authentication is required, a different port number may be required. Check with your service provider. For TLS support , use 465. For STARTTLS, try 587.
- C. Check “Use Authentication” if SMTP server requires authentication to send emails.
 - a. If required, Enter “Username” and “Password” that has been assigned to ENVIROMUX.

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

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

Note: The E-MICRO-T(RHP) does not support Microsoft Office 365.

User Settings

Account Settings	
Username	<input type="text" value="user2"/> The username for this user
Admin	<input type="checkbox"/> Grant this user administrative privileges
Password	<input type="password" value="••••••"/> The user's password to login to the system (for local authentication)
Confirm	<input type="password" value="••••••"/> Confirm the entered password
Contact Settings	
Groups	<input checked="" type="checkbox"/> Group 1 <input type="checkbox"/> Group 2 <input type="checkbox"/> Group 3 <input type="checkbox"/> Group 4 <input type="checkbox"/> Group 5 <input type="checkbox"/> Group 6 <input type="checkbox"/> Group 7 <input type="checkbox"/> Group 8
E-mail Alerts	<input type="checkbox"/> User receives alerts via e-mail
E-mail Address	<input type="text"/> E-mail address for the user
Syslog Alerts	<input type="checkbox"/> User receives alerts via syslog
SNMP Traps	<input type="checkbox"/> User receives alerts via SNMP traps
Syslog/SNMP IP Address	<input type="text"/> IP address where syslog messages/SNMP traps are sent for this user
SMS Alerts	<input type="checkbox"/> User receives alerts via SMS
SMS Number	<input type="text"/> Phone number where SMS messages are sent for this user

Without a valid email address entered, the ENVIROMUX won't be able to send an alert to this user.

Figure 55- Configure user to receive alerts via email

3. Verify the 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](#).

Once the Email Server Settings are setup to send emails from the ENVIROMUX-MICRO, and email settings are setup for Users to receive the emails under User Settings, use the "Test Email" button on the Email Server Settings page to make sure you have everything setup correctly.

Note: Alert messages can also be sent to a cell phone using Email-to-SMS by entering a User's full phone number@carrier instead of a User's email address (page 30). The "SMS Alerts" and "SMS Number" fields are not in use as of this publication.

LOCATING OIDS

To use SNMP (Simple Network Management Protocol) to monitor the sensors and control the functions of an ENVIROMUX Micro 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

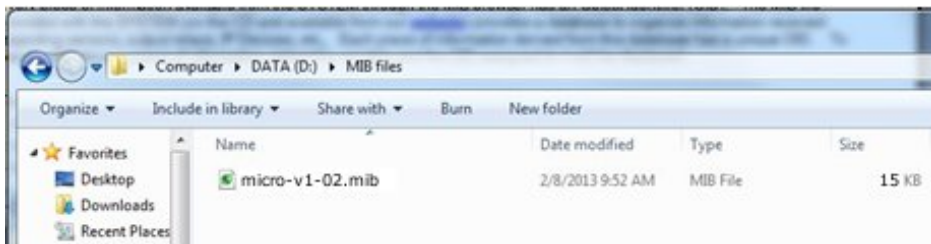
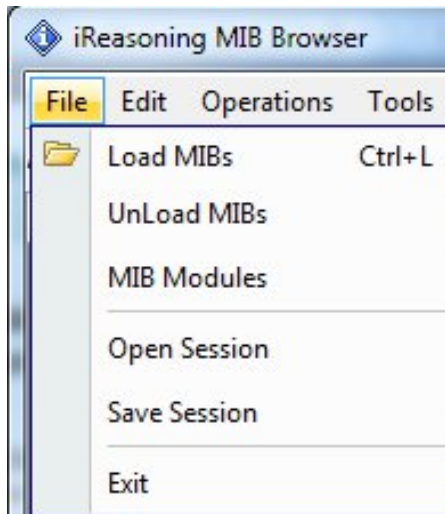
Every piece of information available from the SYSTEM through the MIB browser has an OID (Object Identifier). The MIB file provided with the SYSTEM (available from <http://www.networktechinc.com/download/d-environment-monitor-micro.html>) provides a database to organize information received regarding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

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

View OIDs

To view this information, you must do the following:

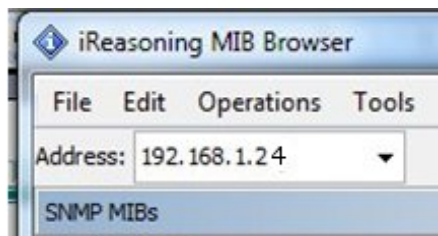
1. Install the browser to your PC
2. Copy the MIB file associated with your SYSTEM to the hard drive on your PC.(perhaps to a new directory “MIB files” as shown below.)
3. Load the MIB file for the SYSTEM to your browser.



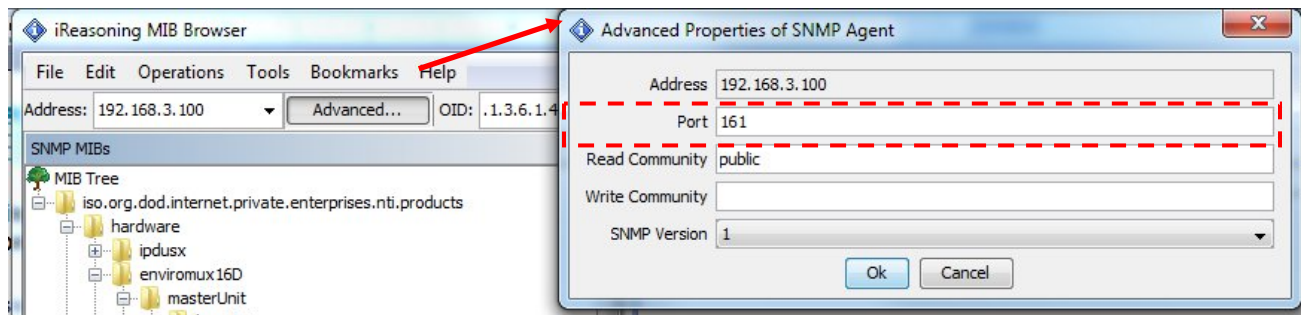
Select “Load MIBs” and locate the MIB file on your PC.

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

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



5. With the iReasoning browser, the Read-only Community Name (default is “public”) was automatically sensed and applied when the IP address was entered, but if this doesn’t happen in your browser, make sure the “Read Community” field in the agent properties includes the name “public” (or whatever you have changed it to in the ENVIROMUX-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 26 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.

Select here

View category info here

Select here

View OID here

Each variable has a value that can be identified with an OID...

... and each variable for each sensor has a separate OID.

Name/OID /	Value	Type	IP:Port
extSensorType.1	temperatureCombo (32769)	Integer	192.168.3.1...
extSensorType.2	humidityCombo (32770)	Integer	192.168.3.1...
extSensorType.3	light (22)	Integer	192.168.3.1...
extSensorType.4	undefined (0)	Integer	192.168.3.1...
extSensorType.5	temperature (1)	Integer	192.168.3.1...
extSensorType.6	undefined (0)	Integer	192.168.3.1...
extSensorType.7	humidity (2)	Integer	192.168.3.1...
extSensorType.8	undefined (0)	Integer	192.168.3.1...
extSensorType.9	temperatureCombo (32769)	Integer	192.168.3.1...
extSensorType.10	humidityCombo (32770)	Integer	192.168.3.1...
extSensorType.11	1542	Integer	192.168.3.1...
extSensorType.12	1542	Integer	192.168.3.1...
extSensorType.13	power (3)	Integer	192.168.3.1...
extSensorType.14	power (3)	Integer	192.168.3.1...
extSensorType.15	water (9)	Integer	192.168.3.1...
extSensorType.16	undefined (0)	Integer	192.168.3.1...
extSensorType.17	acImpPower (8)	Integer	192.168.3.1...
extSensorType.18	acImpVoltage (7)	Integer	192.168.3.1...
extSensorType.19	custom (32767)	Integer	192.168.3.1...
extSensorType.20	custom (32767)	Integer	192.168.3.1...
extSensorType.21	26	Integer	192.168.3.1...
extSensorType.22	undefined (0)	Integer	192.168.3.1...
extSensorType.23	undefined (0)	Integer	192.168.3.1...
extSensorType.24	undefined (0)	Integer	192.168.3.1...
extSensorType.25	undefined (0)	Integer	192.168.3.1...
extSensorType.26	undefined (0)	Integer	192.168.3.1...
extSensorType.27	temperatureCombo (32769)	Integer	192.168.3.1...
extSensorType.28	humidityCombo (32770)	Integer	192.168.3.1...
extSensorType.29	keyStation (17)	Integer	192.168.3.1...
extSensorType.30	undefined (0)	Integer	192.168.3.1...
extSensorType.31	motion (12)	Integer	192.168.3.1...
extSensorType.32	undefined (0)	Integer	192.168.3.1...

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

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.

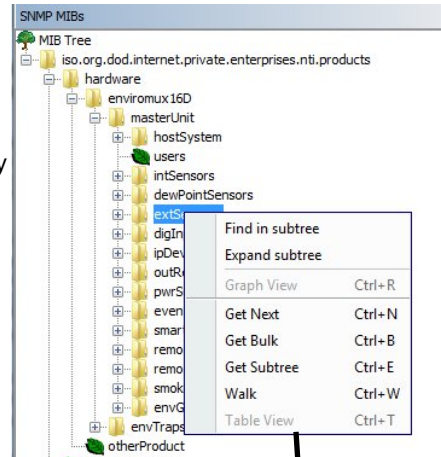
To get specific results in the Result Table, right click on an item in the MIB Tree and choose the type of search (“operation”) you want.

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

Name/OID	Value	Type	IP:Port
extSensorIndex.1	0	Integer	192.168.3.1...
extSensorType.1	temperatureCombo (32769)	Integer	192.168.3.1...
extSensorDescription.1	Temperature 1	OctetString	192.168.3.1...
extSensorConnector.1	1	Integer	192.168.3.1...
extSensorGroupNb.1	0	Integer	192.168.3.1...
extSensorGroup.1	1	OctetString	192.168.3.1...
extSensorValue.1	755	Integer	192.168.3.1...
extSensorUnit.1	1	Integer	192.168.3.1...
extSensorUnitName.1	F	OctetString	192.168.3.1...
extSensorStatus.1	normal (1)	Integer	192.168.3.1...
extSensorMinThreshold.1	600	Integer	192.168.3.1...
extSensorMaxThreshold.1	950	Integer	192.168.3.1...

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

REST API SUPPORT

ENVIROMUX MICRO Firmware Version 3.1 (and later) provides a REST API to query the sensor values and settings. This API provides the response in JSON format which can be used to integrate into other software programs.

API Request Details:

API Endpoint: `http(s)://<DEVICE_ADDRESS>/appAll.json`

Note: API Endpoint needs to use the http or https protocol as set in the ENVIROMUX-MICRO configuration.

Request Header: Base 64 encoded Basic HTTP Authorization header:

```
'Authorization:Basic <Base_64_Encoded <user>:<password> String>'
```

Request Method: GET

Request Sample using curl:

```
curl -v -X GET -u <username>:<password> "http://192.168.1.1/appAll.json"
```

API Response Details:

Response content type: 'application/json'

Response Sample Format:

```
{
  "data": {
    "all": [{
      "device": {
        "unit": "Device-8106",
        "model": "E-MICRO-T(RHP) ",
        "uptime": "3 days, 2 hours, 8 mins",
        "firmware": "3.1"
      }
    },
    {
      "network": {
        "mac": "00:0c:82:00:00:06",
        "dhcp": 0,
        "addr": "192.168.1.1",
        "mask": "255.255.255.0",
        "gtw": "192.168.1.0",
        "dns1": "192.168.1.52",
        "dns2": "192.168.1.53"
      }
    }
  ],
  "isens": [{
    "idx": 0,
    "desc": "temperature",
    "type": 1,
    "unit": 0,
    "val": "30.5 C"
  }, {
    "idx": 1,
    "desc": "Humidity1",
    "type": 2,
    "unit": 0,
    "val": "35.5 %"
  }
  ],
}
```

```

        "idx": 2,
        "desc": "Dew Point",
        "type": 24,
        "unit": 0,
        "val": "13.6 C"
    }
  ],
  {
    "esens": [{
      "idx": 0,
      "desc": "Temperature #1",
      "type": 1,
      "unit": 0,
      "val": "27.9 C"
    }, {
      "idx": 1,
      "desc": "Humidity #1",
      "type": 2,
      "unit": 0,
      "val": "39.2 %"
    }, {
      "idx": 2,
      "desc": "Dew Point #1",
      "type": 24,
      "unit": 0,
      "val": "12.7 C"
    }, {
      "idx": 3,
      "desc": "Temperature #2",
      "type": 1,
      "unit": 0,
      "val": "27.8 C"
    }, {
      "idx": 4,
      "desc": "Humidity #2",
      "type": 2,
      "unit": 0,
      "val": "39.8 %"
    }, {
      "idx": 5,
      "desc": "Dew Point #2",
      "type": 24,
      "unit": 0,
      "val": "12.9 C"
    }
  ]
},
{
  "diginp": [{
    "idx": 0,
    "desc": "Digital Input #1",
    "type": 19,
    "val": "Open"
  }, {
    "idx": 1,
    "desc": "Digital Input #2",
    "type": 19,
    "val": "Open"
  }
]
},
{
  "ipdev": [{
    "idx": 0,
    "desc": "IP Device #1",
    "ip": "8.8.8.8",
    "val": "Responding",
    "retries": 3,
    "timeout": 5,
    "repeat": 60
  }
]
},
{

```

```

        "alerts": [{
            "idx": 0,
            "sensor": "Humidity1",
            "status": "2",
            "alertMsg": "Sensor value greater than 25.0",
            "alertStatus": "Alarm",
            "val": "35.5 %",
            "sensorType": 1,
            "sensorClass": 0,
            "sensorId": 1
        }],
    },
    {
        "smalerts": [{
            "idx": 0,
            "status": "Alarm"
        }]
    }
]
},
"msg": "Request Successful",
"code": 200
}

```

Response Description:

If request is successful, return 'code' will be 200 with device data present in 'data' block.
 If request is unsuccessful 'code' will contain non-200 integer with 'msg' field describing the error.

Field Descriptions:

Value	Description
isens	Internal sensor
esens	External Sensor
diginp	Digital Inputs
ipdev	IP Devices
alerts	Alerts
smalerts	Smart Alerts
unit	Device name given by user
model	ENVIROMUX-MICRO model type
mac	MAC address of Ethernet adapter in ENVIROMUX-MICRO
dhcp	Indicates if DHCP is enabled (integer) (0 = disabled, 1 = enabled)
gtw	Gateway for network
idx	Sensor Position within the sensor class (integer)
desc	Sensor description given by user
Type	Sensor Type (integer)
Unit	Sensor unit (integer) (if temperature sensor, 0 = Celsius, 1 = Fahrenheit)
val (sensors)	Sensor value string which will have either: 1. floating value and unit separated by whitespace 2. sensor status string (Open, Closed, Responding, Not Responding)
Timeout	IP Device Timeout to wait for response in seconds (integer)
Repeat	Time to wait before checking the IP device again in seconds (integer)
status (alert)	Alert status as given by alert status ID's
alertMsg	Reason why the alert is in alarm mode
alertStatus	Status of alert as a string (Normal, Alarm, Acknowledged, Dismissed, Disconnected, Unknown)
val (alerts)	Current value of the sensor used in alert
sensorType	Sensor Type as given by ID (integer)
sensorClass	Sensor Class as given by ID (integer)
sensorId	Sensor position within the sensor class
status(smalert)	Status string of the smart alert (Normal, Alarm, Acknowledged, Dismissed, Disconnected, Unknown)

Sensor Class ID's

Value	Description
0	Internal Sensor
1	External Sensor
2	Digital Inputs
3	IP Devices
4	Smart Alerts
5	Alert Test Class
6	Alert Datalog Class

Alert States Definition

Value	Description
0	Normal
1	Entering Alarm
2	Alarm
3	Exiting Alarm
4	Waiting for Acknowledgement or Dismissal
5	Acknowledged
6	Dismissed
7	Disconnected

Sensor Type ID's

Value	Description	Value	Description
0	Undefined		//Other
1	Temperature	19	Digital Input
2	Humidity	20	IP Device
3	Power	21	Not Responding
4	Low Voltage	22	Light
5	Current	23	Temperature Ex (Ext. Range)
6	ENVIROMUX-ACLM-V	24	Dewpoint
7	ENVIROMUX-ACLM-V of -P	25	Noise Level Sensor
8	ENVIROMUX-ACLM-P	26	TAC DI16DO16
	//Contact Sensors	27	Humidity D
9	Water	28	Temperature EX2
10	Smoke	29	TAC DIP1 (Tac Dig. In1)
11	Vibration	30	Air Velocity
12	Motion	31	Dust
13	Glass	32	Humidex
14	Door	33	Heat Index
15	Keypad	34	Bar Pressure
	//Keypad	35	HG Pressure
16	Panic Button	36	Disconnected
17	Key Station		
18	Dry Contact		

TECHNICAL SPECIFICATIONS

Ports	
Sensor Inputs	Two female RJ45 connectors for connecting temperature and/or temperature/humidity sensors
Max. Sensor Cable Length	Temperature Sensors- 507 feet Liquid and Contact Sensors- 1000 feet
DIGITAL IN Dry Contact Closures	Two screw terminal pairs for connecting dry contact devices and liquid detection sensors. <ul style="list-style-type: none"> * Potential-free. * Output voltage: +5 V DC * Current limited to 10 mA * Maximum contact resistance: 10K Ohm
Ethernet Port	One female RJ45 connector with LEDs. 10 BaseT Ethernet interface.
Environmental	
Operating/Storage temperature	-4°F to 167°F (-20°C to 75°C)
Operating and Storage Relative Humidity	0 to 90% non-condensing RH
General	
Protocols	HTTP, HTTPS,SNMP, SMTP, TCP/IP, UDP, Xmodem, IP Filtering, AES/DES 256-bit encryption, SNMPv1,v2c,v3, TLS v1.2, STARTTLS
PoE Support (-TRHP model only)	IEEE 802.3af and 802.3at standards
Power Supply	120VAC or 240VAC at 50 or 60Hz-5.5VDC/1.5A AC Adapter
Dimensions WxDxH (in.)	4x3.437x1.37
Approvals	RoHS

TROUBLESHOOTING

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

Problem	Cause	Solution
Cannot connect via web interface- no login screen	wrong IP address	Use Discovery Tool to locate configure IP address (page 12)
Cannot get Discovery Tool to work	Java not installed	Java Runtime Environment must be installed before the Discovery Tool can be used (page 12)
Cannot connect via Telnet	<ul style="list-style-type: none"> Ethernet cable not connected wrong IP address wrong port number telnet not supported via operating system telnet not enabled 	<ul style="list-style-type: none"> check Ethernet cable connection Use Discovery Tool to locate IP address (page 12) Configure terminal to use port 23 Use a terminal program instead of the command line Go to Network Settings and enable Telnet (page 25)
Not receiving alert messages	<ul style="list-style-type: none"> using email that supports encryption using email the does not support encryption, but uses standard authentication 	<ul style="list-style-type: none"> If security is required, make sure email server supports TLSv1,2 Authentication Protocol. If only using standard authentication (just requires username and password), make sure the username and passwords are entered correctly and that "Use Authentication" is checked (see pages 27 or 45) Make sure the port number entered is correct (check with the system administrator)
Cannot login	cannot remember root password	Either restore default settings (page 45) or contact NTI for assistance
Cannot get POE router to power the unit	<ul style="list-style-type: none"> The ENVIROMUX-MICRO you have does not support POE The POE router does not support the IEEE 802.3af or 802.3at standards 	<ul style="list-style-type: none"> Only the E-MICRO-TRHP supports POE. Use the required 5.5VDC 1.5A AC Adapter (see page 9) Connect the E-MICRO-TRHP to a router that supports the IEEE 802.3af or 802.3at standards or connect the required 5.5VDC 1.5A AC Adapter (see page 9)

Note: The E-MICRO-T(RHP) does not support Microsoft Office 365.

E-MICRO Email Error Codes

Below is list of email error codes specific to the E-MICRO (version 3.0 and later). Like the HTTPS connections on the E-MICRO, the email connections have a limitation of how many emails can be sent in parallel. We cannot be specific as to the exact nature of this "limitation" because it also depends on the response time of the customer's email server.

ERROR MESSAGE	ERROR CODE#	MEANING
TCPIP_SMTPC_RES_MESSAGE_ERROR	-1	mail message error
TCPIP_SMTPC_RES_MESSAGE_SERVER_ERROR	-2	message indicated wrong mail server
TCPIP_SMTPC_RES_MESSAGE_RCPT_ERROR	-3	message mail recipient error: from, to, etc
TCPIP_SMTPC_RES_MESSAGE_BUFFER_ERROR	-4	attachment buffer error
TCPIP_SMTPC_RES_MESSAGE_FILE_ERROR	-5	attachment file error
TCPIP_SMTPC_RES_MESSAGE_AUTH_REQUIRED	-6	server requires authentication but username or password haven't been provided
TCPIP_SMTPC_RES_MESSAGE_AUTH_LEN_ERROR	-7	provided credentials are too long, buffer overflow
TCPIP_SMTPC_RES_MESSAGE_ADDR_LEN_ERROR	-8	email address too long, buffer overflow
TCPIP_SMTPC_RES_MAIL_BUSY	-9	all mail connections are busy; try later
TCPIP_SMTPC_RES_DNS_ERROR	-10	failure to resolve server name
TCPIP_SMTPC_RES_SKT_OPEN_ERROR	-11	failure to open a communication socket
TCPIP_SMTPC_RES_SKT_BIND_ERROR	-12	failure to bind a socket to the mail server
TCPIP_SMTPC_RES_SKT_CONNECT_TMO	-13	connection to mail server timeout
TCPIP_SMTPC_RES_SKT_TLS_ERROR	-14	TLS is required but failed to start TLS on the communication socket
TCPIP_SMTPC_RES_SERVER_TMO	-15	server timeout
TCPIP_SMTPC_RES_CONNECTION_REJECT	-16	server rejected the connection
TCPIP_SMTPC_RES_CONNECTION_CLOSE	-17	server closed the connection
TCPIP_SMTPC_RES_HELLO_REJECT	-18	server rejected the hello greeting
TCPIP_SMTPC_RES_AUTH_UNKNOWN	-19	server requires authentication mechanism unsupported by SMTPC - Currently LOGIN and PLAIN authentications are supported
TCPIP_SMTPC_RES_AUTH_LOGIN_REJECT	-20	server rejected the login authentication request
TCPIP_SMTPC_RES_AUTH_LOGIN_SERVER_ERROR	-21	unexpected server reply to login authentication request
TCPIP_SMTPC_RES_AUTH_REJECT	-22	server rejected the supplied authentication
TCPIP_SMTPC_RES_TLS_REJECT	-23	server rejected the TLS start
TCPIP_SMTPC_RES_TLS_FAILED	-24	TLS session negotiation failed
TCPIP_SMTPC_RES_TLS_TMO	-25	TLS session timeout
TCPIP_SMTPC_RES_MAIL_FROM_REJECT	-26	server rejected the "from" address
TCPIP_SMTPC_RES_MAIL_RCPT_REJECT	-27	server rejected the "recipient" address
TCPIP_SMTPC_RES_MAIL_DATA_REJECT	-28	server rejected the "data" field
TCPIP_SMTPC_RES_MAIL_BODY_REJECT	-29	server rejected the mail body

INDEX

- AC adapter, 9
- acknowledge, 16
- Administration**, 24, 34
- connect sensors, 4
- data log-view, 35
- default IP address, 13
- Device Discovery Tool, 12
- DHCP server**, 25
- dismiss, 16
- downloads, 38
- email setup, 46
- Ethernet connection, 8
- event log-view, 34
- firmware update-web, 33
- groups, 19
- IP Cameras, 32
- IP devices-configure, 37
- IP devices-monitor, 37
- Java Runtime Environment**, 12
- liquid detection sensor, 5
- log in, 13
- login-web interface, 13
- monitoring-web interface, 15
- Network configuration, 44
- Network Configuration**, 25
- overview, 10
- Password**, 13
- reboot, 24
- reset button, 45
- REST API, 51
- sensors-configure**, 43
- setup email, 46
- smart alerts**, 20
- SMTP server, 27
- SNMP settings, 26, 30
- SNTP server, 28
- Summary page**, 14
- system configuration, 24
- Telnet, 40
- Telnet enable, 25
- text menu navigation, 41
- threshold, 19
- troubleshooting, 56
- username and password, 13
- web browsers supported, 2

WARRANTY INFORMATION

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

MAN220 Rev. 3/23/18