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

ENVIROMUX® Series

E-1W

Environment Monitoring System with 1-Wire Sensor Interface Installation and Operation Manual

TRADEMARK

COPYRIGHT

CHANGES

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

FIRMWARE VERSION

Current firmware version 3.15

CAUTION

The ENVIROMUX is NOT intended to be used as a primary security, fire or smoke communication or control system.

TABLE OF CONTENTS

TABLE OF FIGURES

INTRODUCTION

The ENVIROMUX® Environment Monitoring System (ENVIROMUX) with 1-Wire Sensor Interface monitors (from a remote location) critical environmental conditions, such as temperature, humidity, dewpoint, 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 traps), syslog messages and/or SMS messages (via email). For a complete list of sensors supported, visit our website at http://www.networktechinc.com/environment-monitor-1wire.html .

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

The E-1W features two RJ11 6P4C sensor ports for the connection of up to 24 1-wire sensors, and two dry contact inputs.

The E-1WP features two RJ11 6P4C sensor ports for the connection of up to 24 1-wire sensors, two dry contact inputs for the connection of contact-closure sensors and built-in Power over Ethernet (PoE).

Features and Applications

- Multiplatform support: Windows 7/8/10, Windows Server 2008/2012/2016/2019, Solaris, Linux, FreeBSD, and MAC OS 10/11.
- Monitor and manage server room environmental conditions over IP.
- Monitors and operates at temperatures from -4°F to 167°F (-20ºC and 75ºC) and 0% to 90% non-condensing relative humidity.
- Sensors supported:
  - up to 24 1-wire sensors monitored at a time (temperature, humidity, dewpoint, 2-sensor digital input expanders, etc)
  - 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 SNMP v1,v2c and v3 protocols
- Supports SNTP protocol
- Supports Microsoft Internet Explorer 8.0 and higher, Firefox 3.x and higher, Chrome 9.0.5 or higher, Safari 4.0 or higher, and Opera 10.0 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, SNMP(v1,v2c,v3) with AES and DES privacy protocol and MD5 or SHA as authentication protocols, Arcfour, 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.
  - 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-1W**P** includes built-in Power over Ethernet (PoE) (supports IEEE 802.3af and 802.3at (PoE+) standards.)
To install in a Telecom environment, order E-1W-48V5V1A. This includes a power supply that operates on 36-72VDC.

The E-1W(P)-**D** includes a DIN clip option DIN clips can be installed for mounting to a DIN rail.

SUPPORTED WEB BROWSERS

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

- Microsoft Internet Explorer 8.0 or higher
- Microsoft Edge
- Mozilla FireFox 3.x or higher
- Opera 10.0 or higher
- Google Chrome 9.0.5 or higher
- Safari 1.3 for MAC

MATERIALS

Materials supplied with this kit:

- NTI E-1W(P) 1-Wire Environment Monitoring System
- 1- 120VAC or 240VAC at 50 or 60Hz-5.5VDC/1.5A AC Adapter (only included with **E-1W**)

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, pin 2 to pin 2, etc. for Ethernet connection

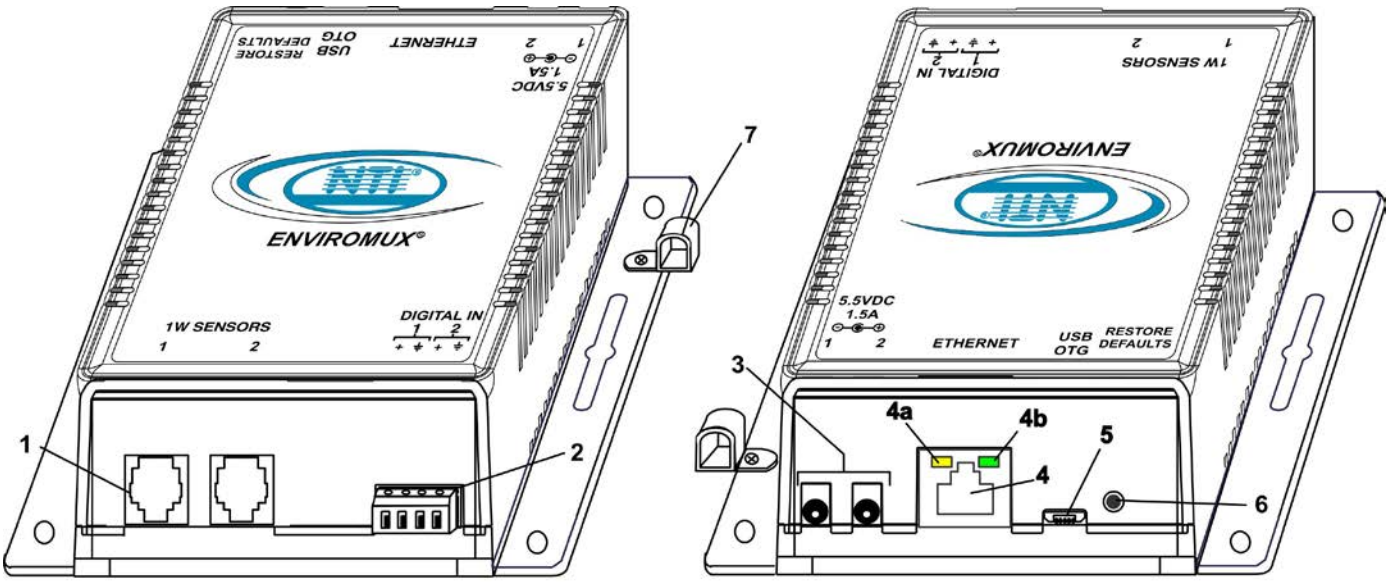
RJ11 4-Wire Patch Cables with RJ11 6P4C plugs on each end wired straight thru- pin 2 to pin 2, pin 3 to pin 3, pin 4 to pin 4, pin 5 to pin 5 .

E-RJ11-xx RJ11 6P4C patch cables can be ordered from NTI (where xx = 7, 25 or 50 foot).

RJ11-3JCK RJ11 6P4C splitter- one required at each point a sensor is connected in order to extend the sensor communication cable for additional sensors.

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



Front View

Rear View

#	LABEL	CONNECTOR/LED	DESCRIPTION
1	**1W Sensors**	RJ11 6P4C jacks	For connection of optional temperature/humidity/dewpoint sensors (The left port is "#1", the right port is "#2" as listed in the Summary Page on Page 16.)
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 • **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	**----**	Cable Restraint	For securing the power cable

INSTALLATION

Mounting

Mount the ENVIROMUX in any dry location convenient for connection of the sensors, Ethernet cable, modem and power supply(s). The operating environment must be within -4°F to 167°F (-20°C to 75°C) with a relative humidity of 0 to 99% (non-condensing).

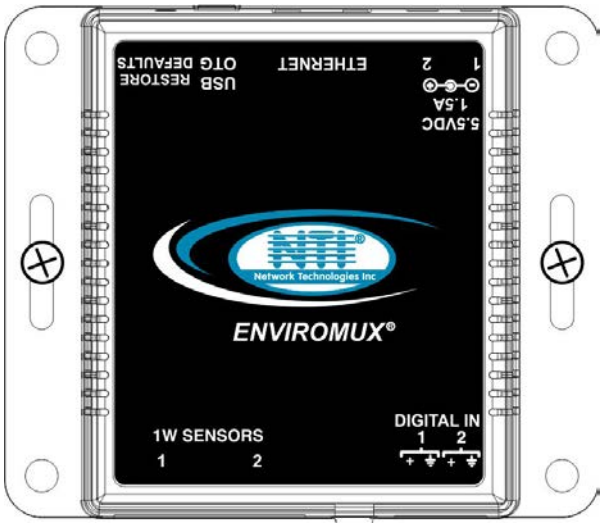


Figure 1- Mount ENVIROMUX in a dry location

DIN Clip Installation

If you purchased the DIN clip option for your ENVIROMUX (E-MICRO-TRH(P)**-D**), the clips can be attached using the hardware provided. Pass the screw through the flat washer, then through a hole in the mounting flange, and screw it tightly into the threaded hole in the clip. Orient the clips so they allow you to mount the E-MICRO-TRH(P)-D in the position your application demands.

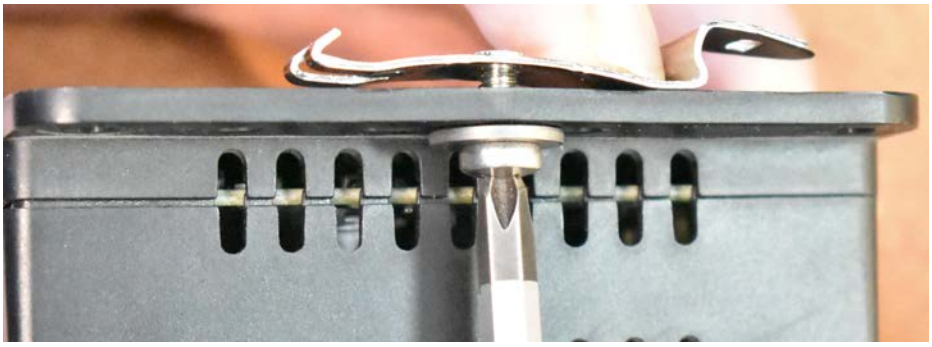


Figure 2- DIN Clip hardware

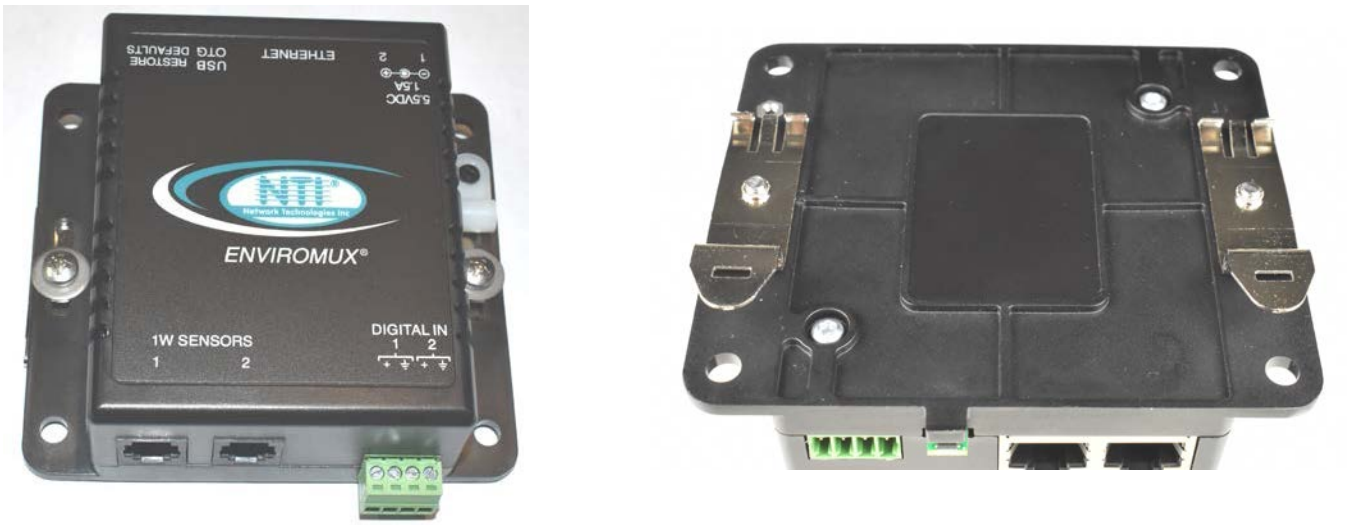


Figure 3- DIN Clips installed

Connect 1W Sensors

E-1W(P) units are compatible with: E-TH1W-7 (temperature/humidity/dewpoint) and E-T1W-7 temperature-only 1-wire sensors (sold separately).

The E-1W "1W Sensor" ports can support a combined total of 24 sensors. Since each E-TH1W-7 has 3 sensors (temperature, humidity and dewpoint), only 8 of these can be connected. If only 1 is connected, then up to 21 E-T1W-7 temperature-only sensors can be connected.

Sensors can be connected to either of the two RJ11 6P4C sensor ports, in series, using RJ11 6P4C 4-wire patch cable wired straight through (pin 1 to pin 1, pin 2 to pin 2, etc) (sold separately) and RJ11 6P4C splitters (NTI# RJ11-3JCK-sold separately). The maximum total distance the last sensor can be from the ENVIROMUX is 600 feet.

Tip: When the ENVIROMUX is placed in the middle between the sensors connected to "1W Sensor" port 1 and those connected to "1W Sensor" port 2, the total sensor cable length can be up to 1200 feet.

Note: The maximum total cable length for attachment of sensors to the E-1W(P) is 600 feet using minimum 28AWG (4-conductor) cable. This total length includes the cable length of each sensor (maximum 7 feet each) as it extends from the trunk line.

Power-cycle the ENVIROMUX after sensors have been plugged-in. Sensors will be auto-detected and applied to the Summary Page (page 16).

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.

If any additional sensors are connected to the E-1W, click on "Detect Sensors" on the Summary Page (page 16) to have the E-1W detect the presence of the sensor and add it to the list.

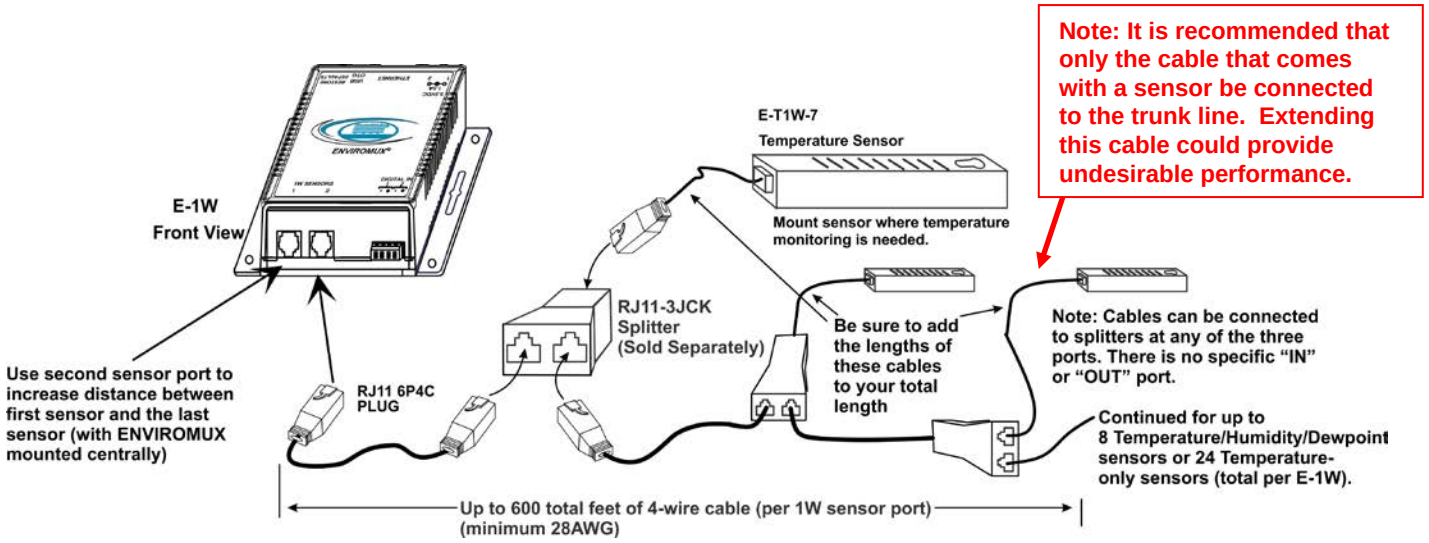


Figure 4- Connect Sensors

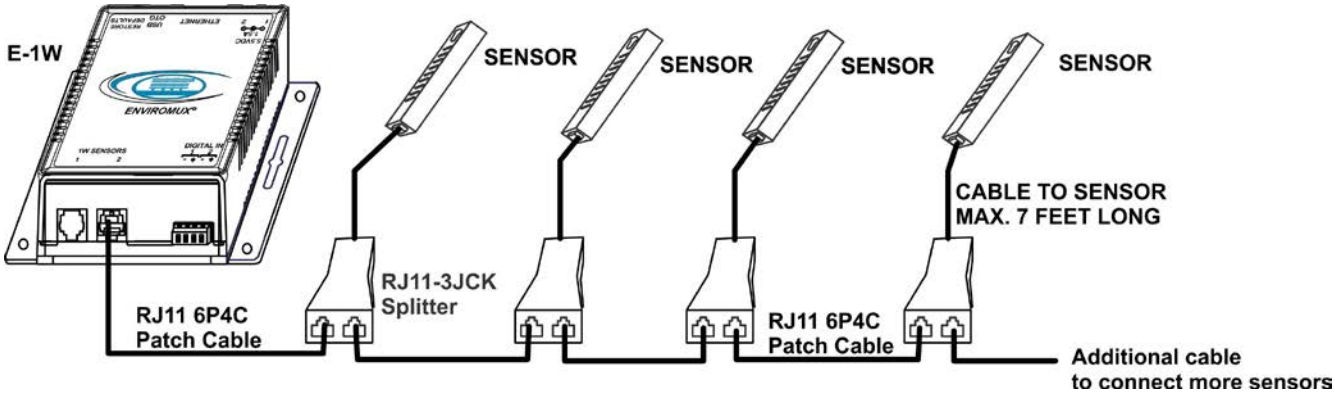


Figure 5- Example of Good Sensor Configuration- in series

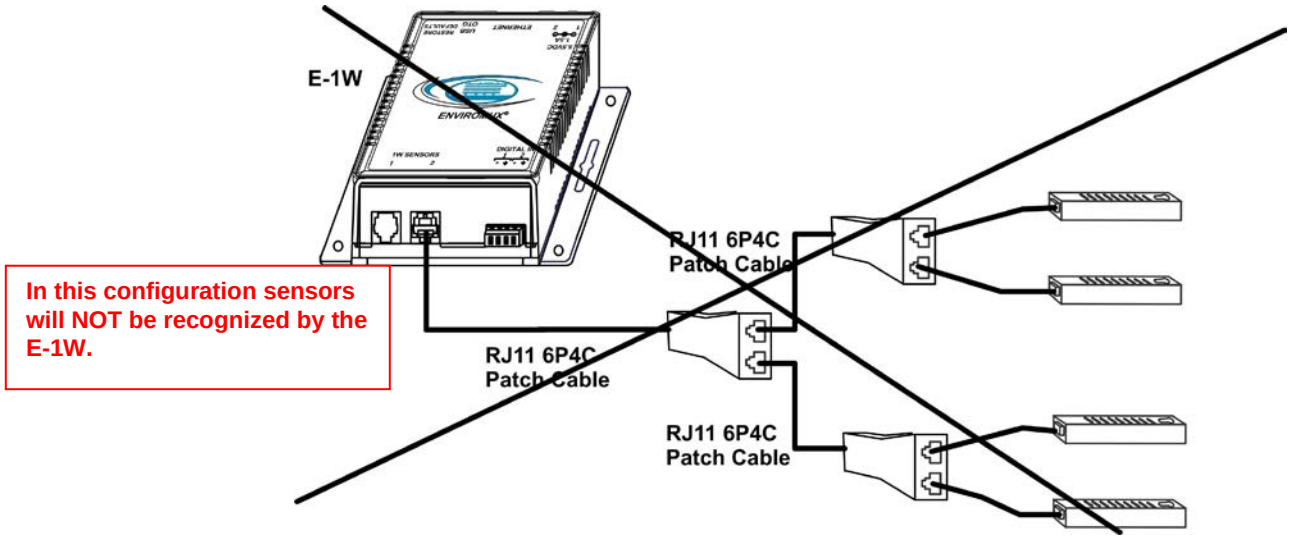


Figure 6- Example of bad configuration

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 ⏚ 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.

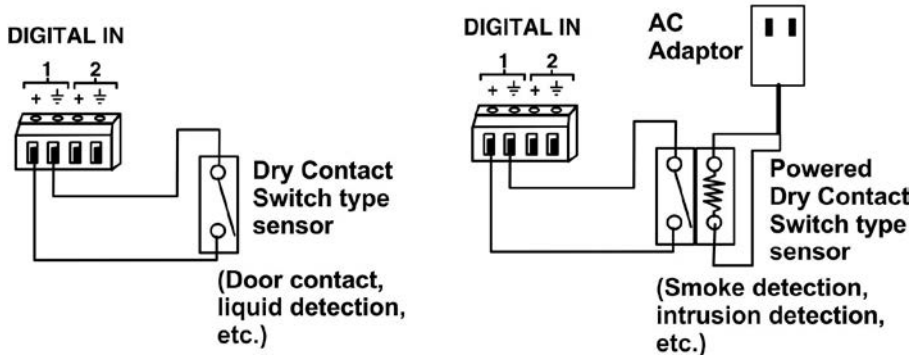


Figure 7- Terminal block for dry-contact sensors

Optionally, connect the two-wire cable from a liquid detection sensor (Figure 8) 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.

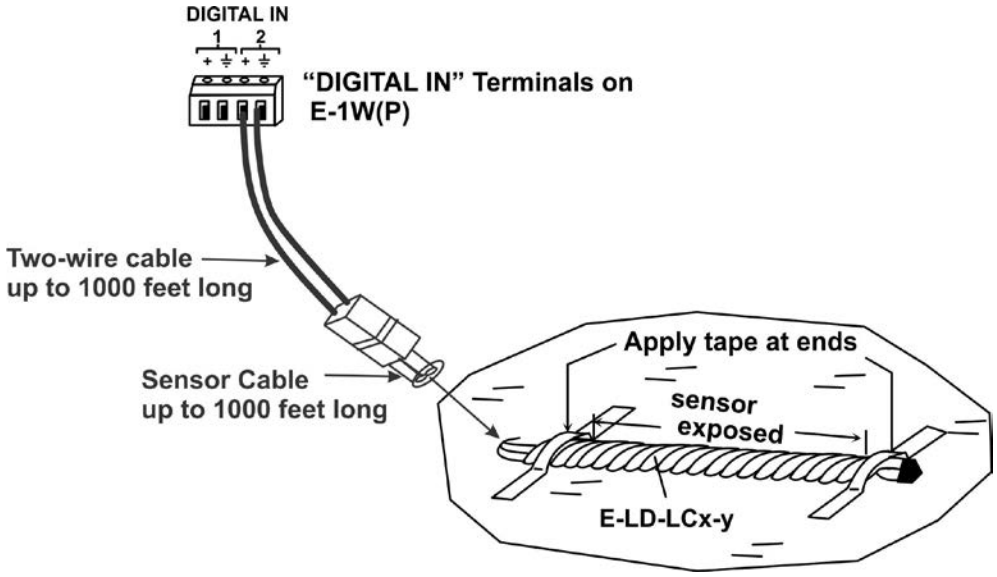
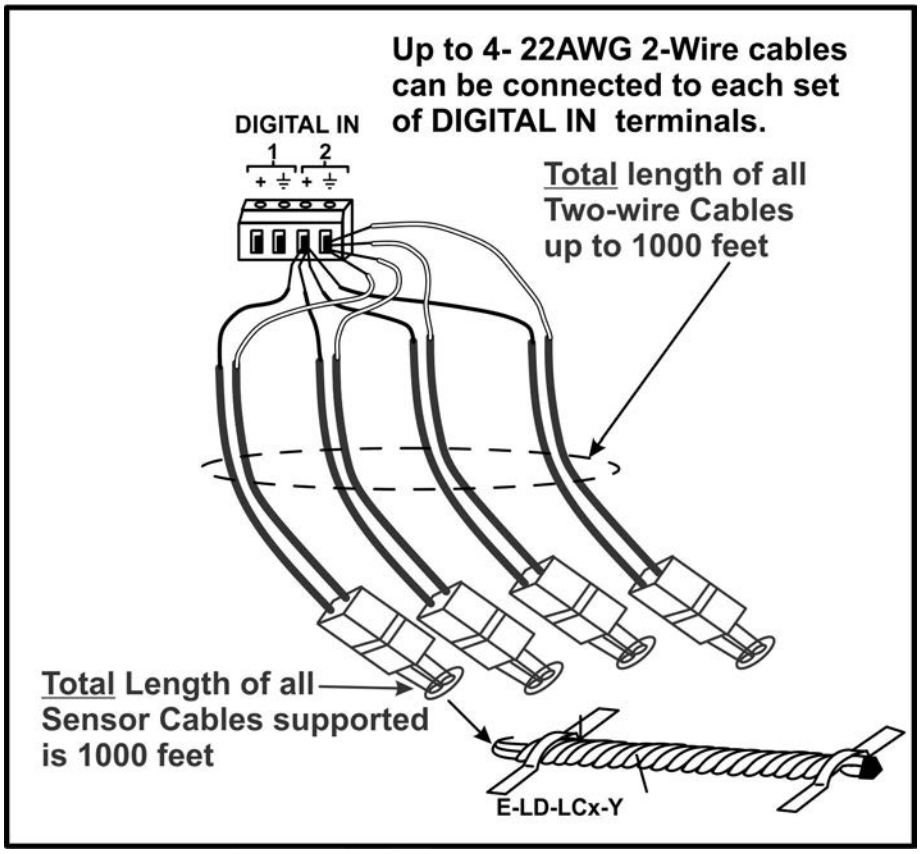


Figure 8- Secure liquid detection sensor with tape

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.



After installation of rope style leak detection sensor in its desired location, **it is very important** to test the sensor to verify correct installation. This applies to **all** rope-style leak detection sensors.

To test the rope style leak detection sensor;

1. Configure the sensor (page21). (Trigger Event set to "Closed")
2. Place approximately one table spoon of tap water across the sense cable so that the 2 thin sensing wires are connected by mutual contact with the water. Do NOT use distilled water as water must be conductive.
3. Monitor the sensor (page 16) to see the sensor "Value" change from "Open" (dry) to "Closed" (wet). (How quickly the change occurs is based on the amount of impurities in the water, so allow up to 30 seconds).
4. Dry the exposed area of sensor and the sensor "Value" should change back to "Open" within 30 seconds.

If the sensor fails to behave in this manner, contact NTI for support.

This completes the testing of the sensor.

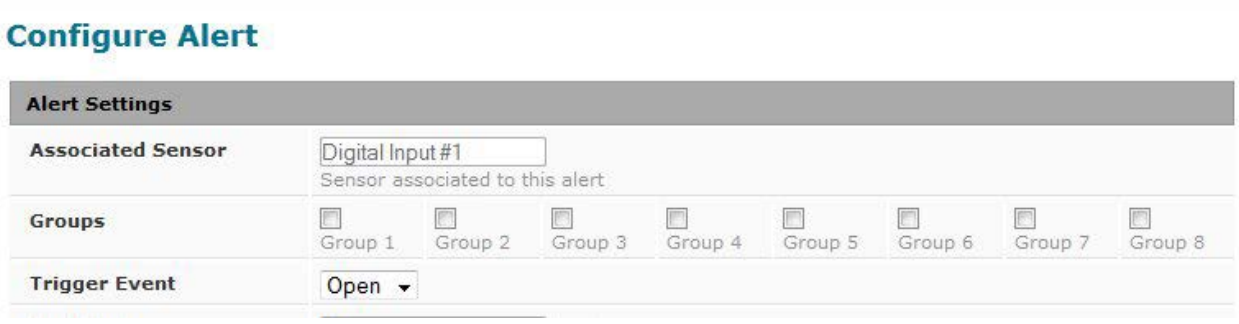


Figure 9- Portion of Water Sensor configuration page

Digital Input Expander

Another way to connect contact sensors and liquid detection sensors is through an E-DI2-1W Digital Input Expander.

The E-DI2-1W can be connected to either of the "1W Sensors" ports up to 600 feet away from the E-1W where up to two contact sensors and/or liquid detection sensors can be attached. Contact and liquid detection sensors can still be extended from the E-DI2-1W by up to 1000 feet of two-wire cable.

Note: The E-DI2-1W counts as two sensors to the total of 24 sensors than can be connected to the 1W Sensors ports.

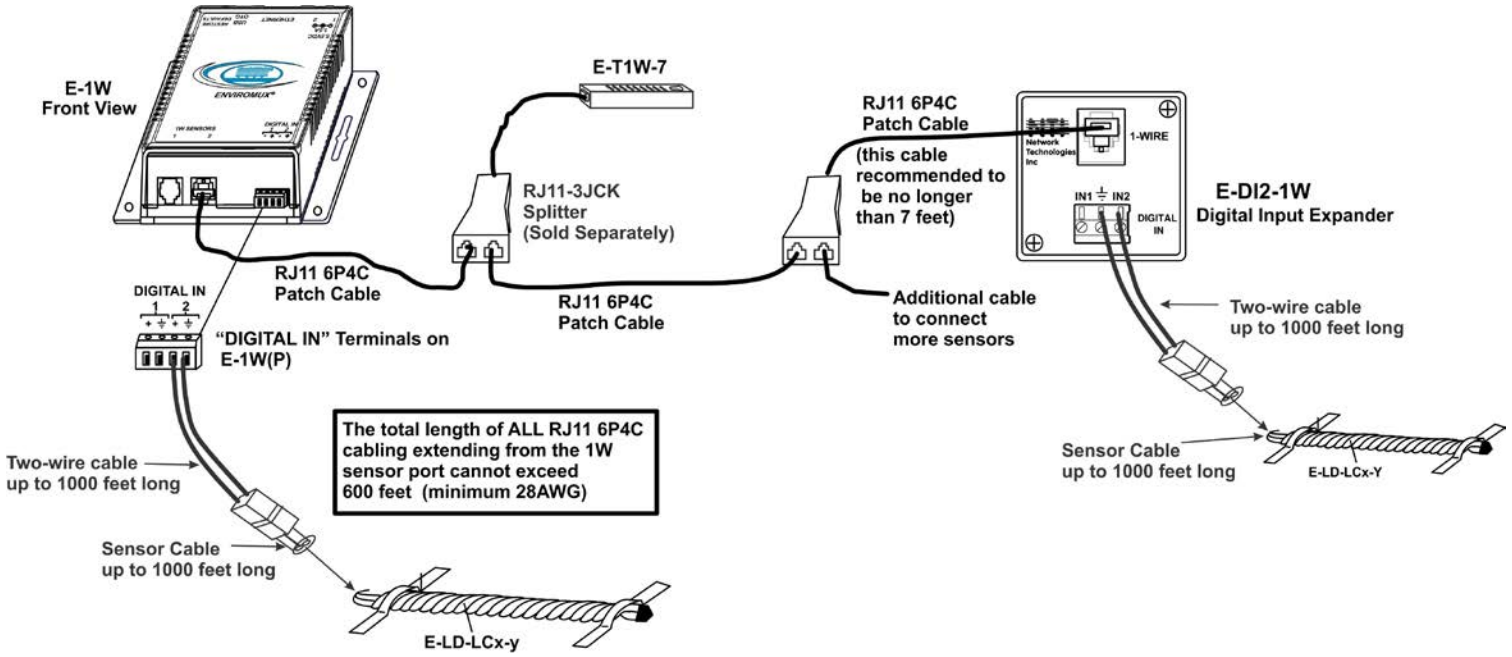


Figure 10- Digital Inputs connected using E-DI2-1

Sensors connected to the E-DI2-1W will be listed under "External Sensors" on the Summary Page in the web interface but will be configured the same as any other digital inputs.

Summary

External Sensors

No.	Description	Type	Value	Action
1	E-1W E01 DI-1	Digital Input	Open	Edit Delete
2	E-1W E01 DI-2	Digital Input	Open	Edit Delete
3	020000006DDFE912.1	Digital Input	Open	Edit Delete
4	020000006DDFE912.2	Digital Input	Open	Edit Delete

Detect Sensors

This shows two E-DI2-1W connected, one has sensor connections renamed "E-1W E01 DI-x" and the second has the default expander port names.

Figure 11- Sensors connected to E-DI2-1W Expander

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".

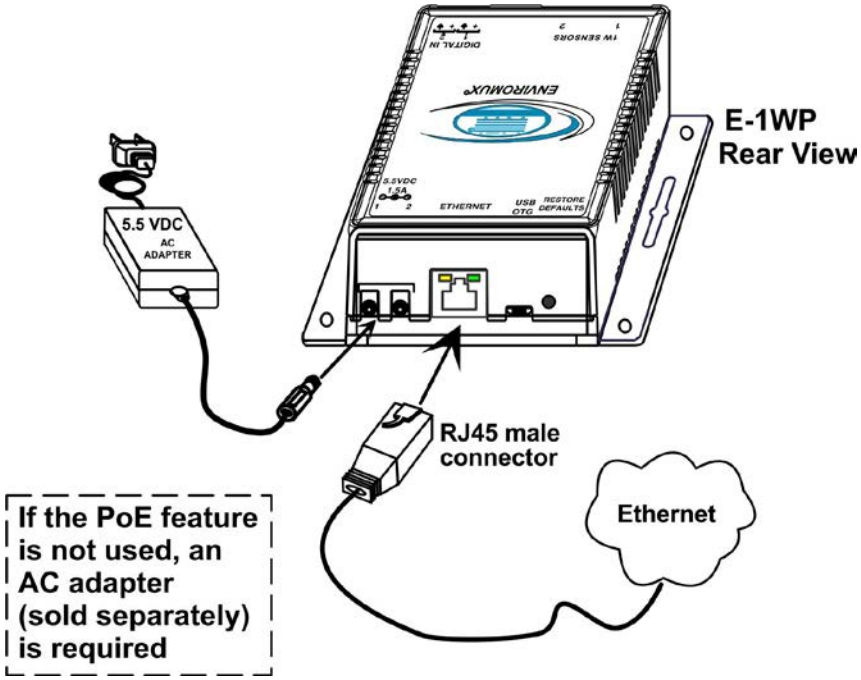


Figure 12- Connect E-1WP to the Ethernet

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

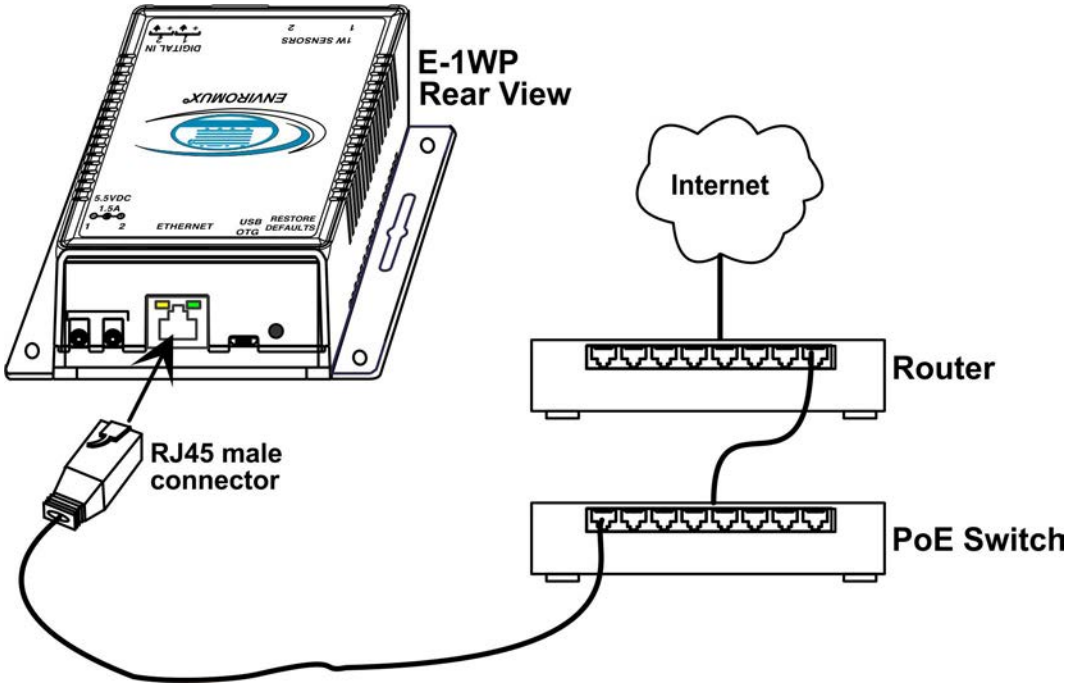


Figure 13- Connect to a PoE Switch

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.

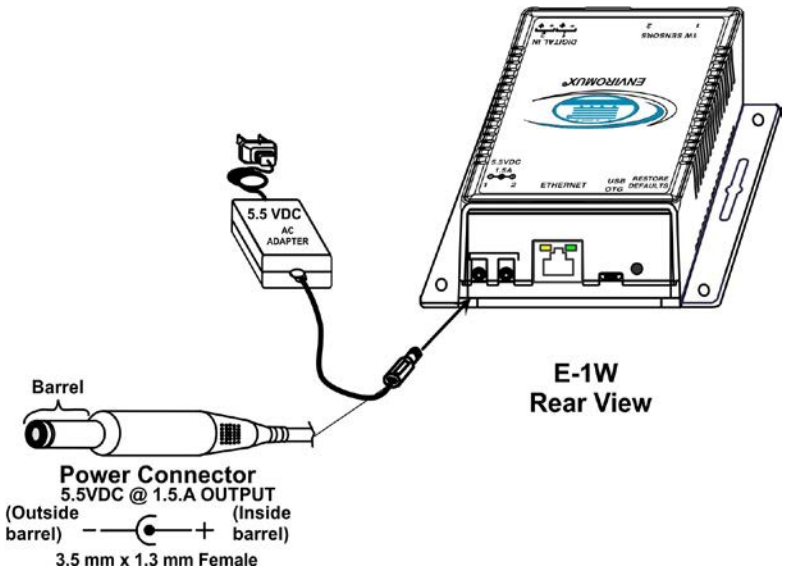


Figure 14- Connect the AC adapter and power-up

If you have purchased the E-1WP and have connected it to a POE router, an external power supply will not be needed as long as the router supports the IEEE 802.3af or 802.3at standards. (The Cisco Discovery Protocol is not supported.) When connected using the POE adapter, the power consumption by the E-1WP is 5 watts maximum.

2. Use the NTI Discovery Tool (page 14) 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.

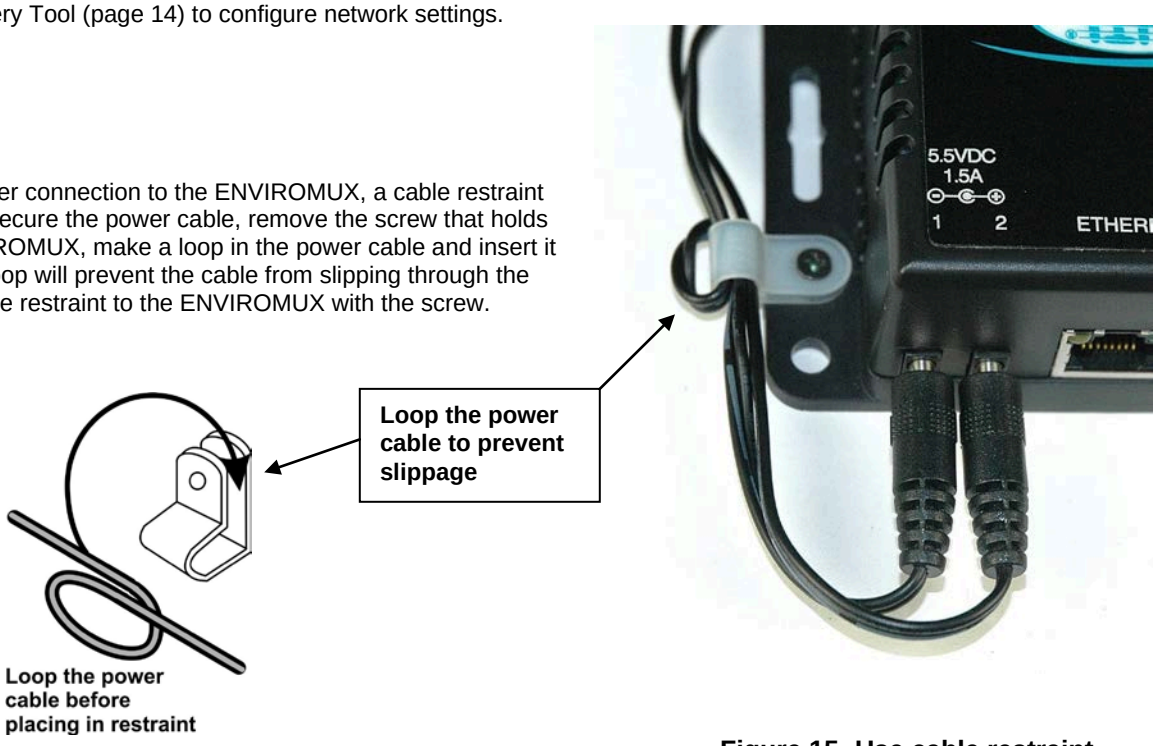


Figure 15- Use cable restraint

OVERVIEW

Administration

The ENVIROMUX can be managed and configured using the web interface (HTTP/HTTPS protocol) via the Ethernet Port. The ENVIROMUX also has a text menu that can be accessed for viewing only of the sensor and alert status and network configuration status using Telnet protocol via the Ethernet Port.

The following administrative controls are available in the ENVIROMUX, thru the web interface 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

Alerts

Alerts can be configured to be sent for all sensors and IP devices being monitored.

A high or low threshold limit can be set for each sensor (other than contact sensors). When a sensor takes a reading that is outside of 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.

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.

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 five main methods: visible notification via one of the user interfaces (alert on webpage, alert in text menu), emails, Syslog messages, SMS messages and/or SNMP traps.

Event Log

The ENVIROMUX maintains an event log. The event log includes power-ON, system, and alert notifications, as well as user 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. 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.

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) can have their own email address plus the "root" user (total of 9). For assistance in setting up Email, see page **Error! Bookmark not defined.**.

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

```
Subject: Message from E-1W P02 [Alert #1]
SENSOR: Test Switch 1
MESSAGE: Sensor value crossed over critical thresholds
VALUE: Closed
UNIT INFO: 192.168.1.24,00:0b:82:17:02:c3
```

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 40).

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 as an IP address.

Note: The SNMP MIB file (E-1W-v2-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-1wire.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.

Modbus TCP/IP Support

The ENVIROMUX is equipped with Modbus TCP/IP support to enable PLC controls to read the value/state of the sensors and digital inputs. Specific instruction on this topic can be found on page 71.

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-monitoring.html, unzipped and saved to a location on your PC. To open it just double-click on the file **`NTIdiscover.jar`** . This will open the NTI Device Discovery Tool.

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

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

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

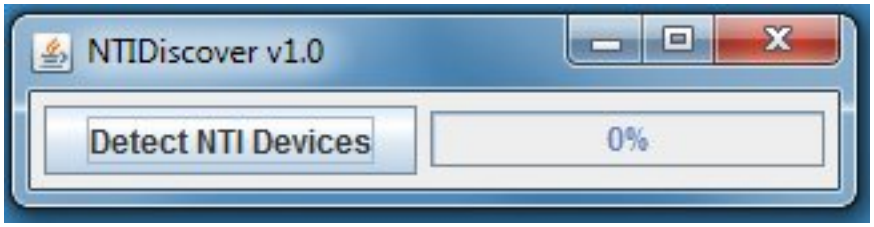
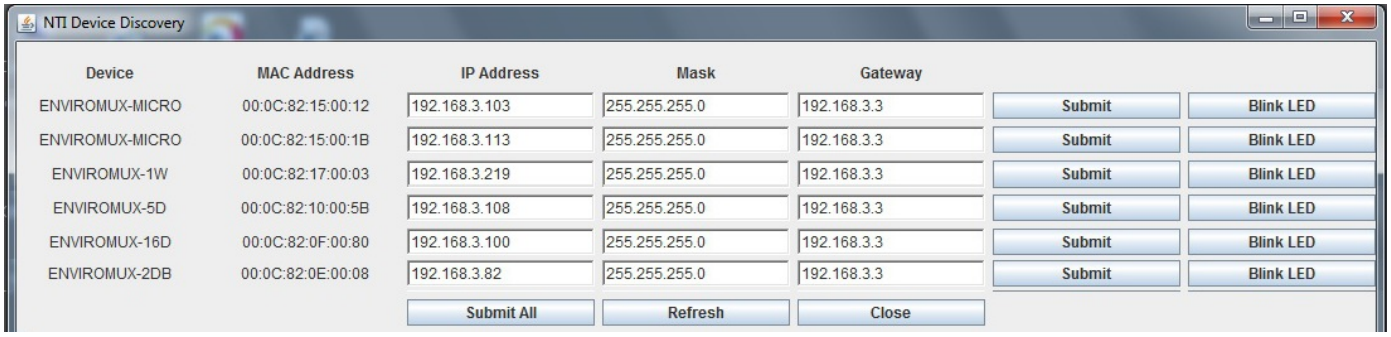


Figure 16- Device Discovery Tool

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



How to Use the Device Discovery Tool

To Change a Device's Settings, within the row of the device whose settings you wish to change, type in a new setting (**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 10). Use the Device Discovery Tool (page 14) 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 use the factory-set IP address indicated below. Alternatively, the ENVIROMUX can be changed (page 30) to dynamically assign network settings received from a DHCP server on the network it is connected to. 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 30) will be used. If a DHCP server on the network has assigned the IP address, use the Device Discovery Tool (page 14) 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:

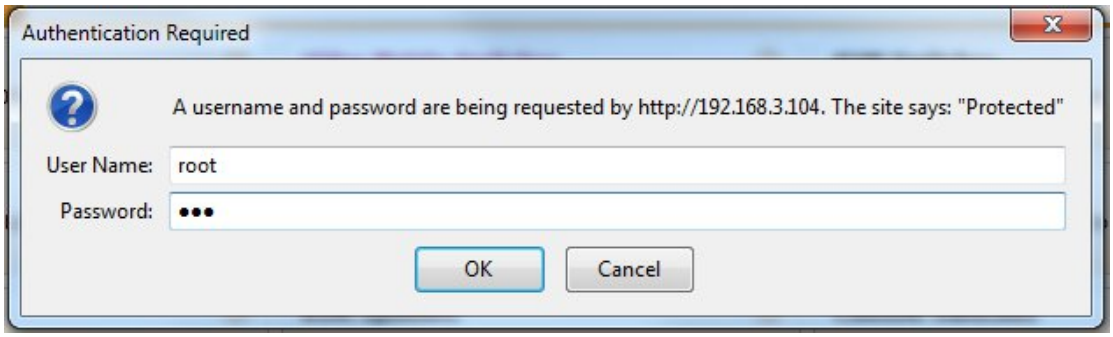


Figure 17- Login prompt to access web interface

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:

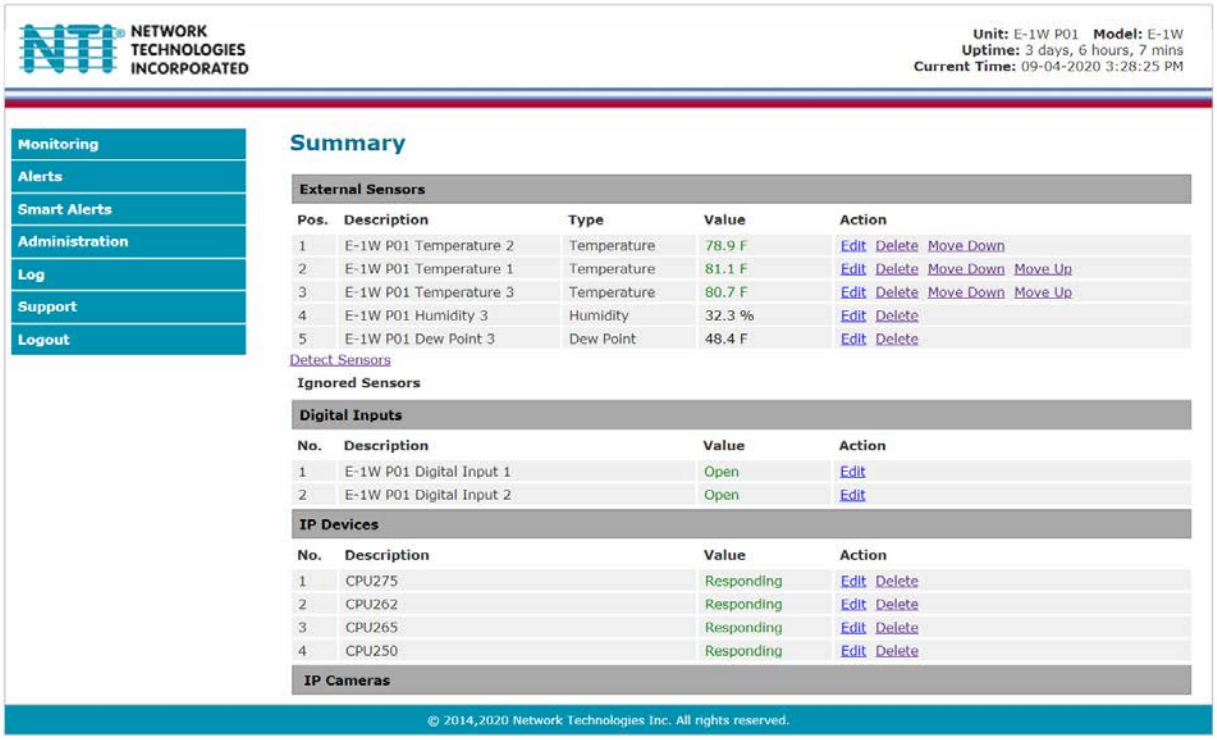


Figure 18- Summary page

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 20)
SMART ALERTS	View and configure how smart alerts will be communicated to users (page 20)
ADMINISTRATION	**Configure all system, network, multi-user access, and security settings as well as upgrade firmware (page 27)**
LOG	View and manage the Event and Data Logs (page 44)
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. Upon power-up, the E-1W will sense all connected sensors and apply them to the sensors listed on the Summary Page.

To add a sensor to the list of monitored sensors (maximum of 24) without having to cycle power, connect the sensor to the ENVIROMUX as described on page 5 and then click “Detect Sensors”. Up to 24 sensors will be displayed under “External Sensors”. If more than 24 are connected, **the extras that are connected will not be listed**.

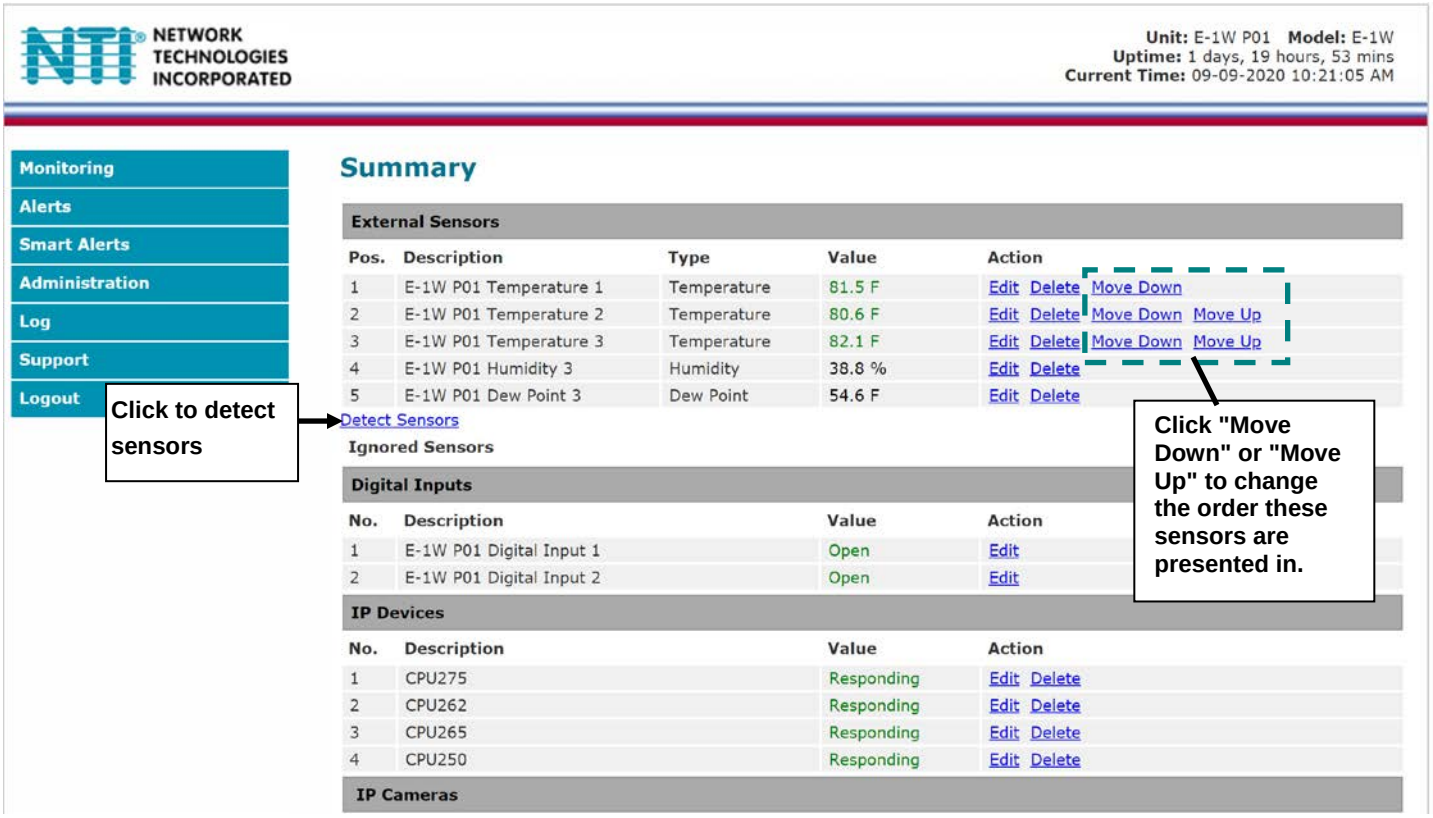


Figure 19- Summary page

If one of the sensors in an E-TH1W-7 (temperature, humidity, dewpoint) or an E-DI2-1W (2 sensors can connect to this) is not required and you wish to free up the space for another sensor, click on the “Delete” for that sensor. That sensor will be moved to the “Ignored sensors” list (see image next page). Notice, in the image above, there are no sensors in the "Ignored Sensor" list. Now an additional sensor can be connected and sensed by the ENVIROMUX by clicking “Detect Sensors”.

To re-instate all sensors in a combo sensor when one has been deleted and added to the “Ignore” list, you must first delete the remaining active sensors of that combo sensor. Make sure there is space to display all sensors in the External Sensors list. Then, click “Detect Sensors” and the sensors in the combo sensor will be re-sensed and added to the list. If there is not room in the External Sensors list for all of them, then none will appear in the list.

You can also change the order in which External Sensors are listed in the Summary Page. By clicking "**Move Down**" or "**Move Up**", you can change the order in which they are presented. Combination sensors (Temperature/Humidity/Dewpoint) will move as a block in the list. You can also use "Move Down" to leave a space for the next connected sensor to fill, provided you don't already have 24 sensors listed.

Note: Changing the order in which they are presented on the Summary Page will also change the order in which they are listed in the MODBUS registry, it will effect your alert configurations and it will change the order in which details are presented in your data log.

Position 3 skipped making room for the next connected sensor.

Summary

External Sensors

Pos.	Description	Type	Value	Action
1	E-1W P01 Temperature 2	Temperature	79.1 F	Edit Delete Move Down
2	E-1W P01 Temperature 1	Temperature	80.6 F	Edit Delete Move Down Move Up
4	E-1W P01 Temperature 3	Temperature	80.8 F	Edit Delete Move Down Move Up
5	E-1W P01 Humidity 3	Humidity	36.1 %	Edit Delete

Detect Sensors

Ignored Sensors

1	E8000017F9B01E01.3	Dew Point

Sensor from combination sensors that is not needed. Ignored to free up space for other connected sensor.

Summary

External Sensors

Pos.	Description	Type	Value	Action
1	E-1W P01 Temperature 2	Temperature	78.7 F	Edit Delete Move Down
2	E-1W P01 Temperature 1	Temperature	80.6 F	Edit Delete Move Down Move Up
3	E-1W P01 Temperature 3	Temperature	80.5 F	Edit Delete Move Down Move Up
4	E-1W P01 Humidity 3	Humidity	30.6 %	Edit Delete

Detect Sensors

Ignored Sensors

1	E8000017F9B01E01.3	Dew Point

Note: When the Values have different colors, the colors are an indication of the sensor state:

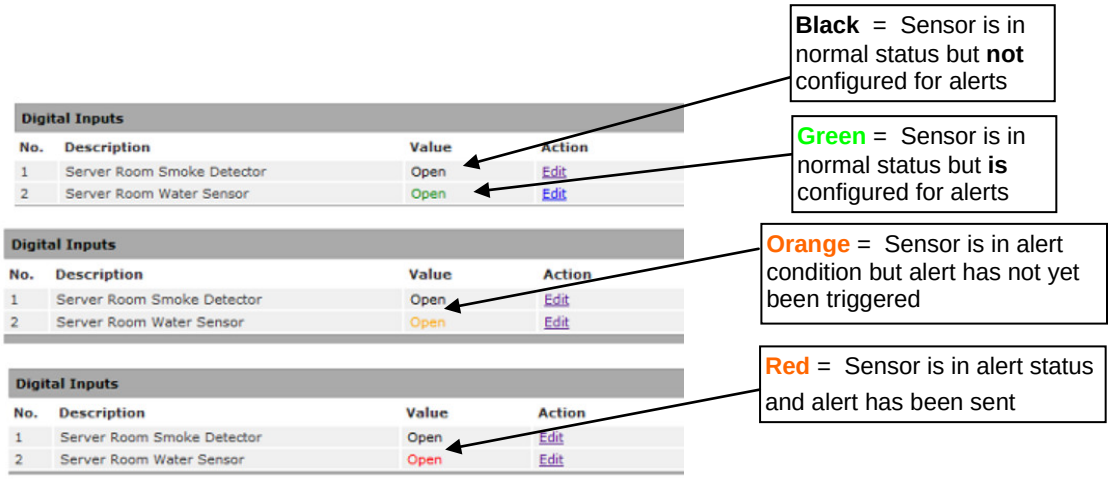


Figure 20-Sensor Values in color have meaning

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

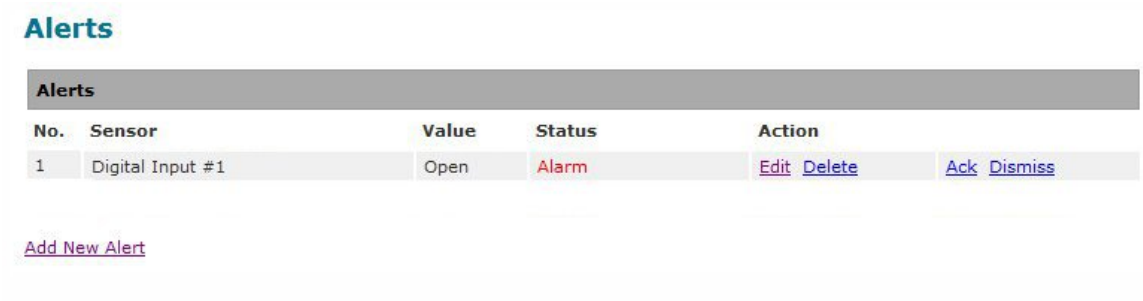


Figure 21- List of alerts configured

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 21) 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.

By default, when a sensor is detected the E-1W records the sensor's unique 64 byte address and enters it as the description of the sensor. If the sensor is a multi-sensor, the address will be followed by a dot and then a number (1, 2, 3) (like in the image below). The user can change this description to something more meaningful. The new name will remain even after using the Detect Sensors button multiple times unless that sensor is manually removed from the list using the "Delete" button.

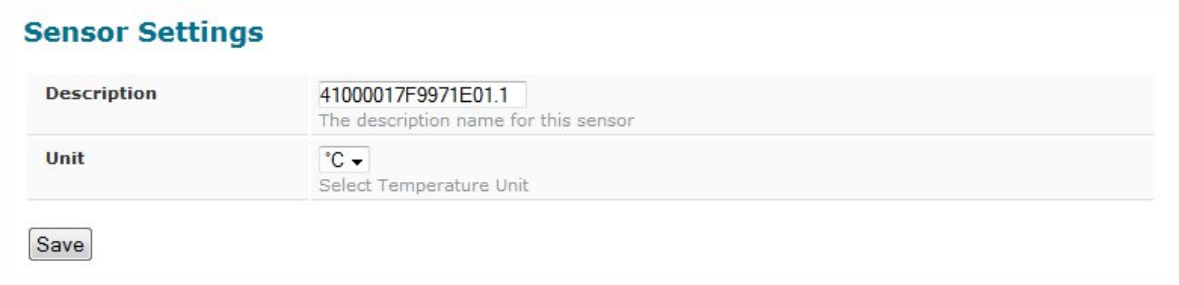


Figure 22- Sensor settings

Alerts

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

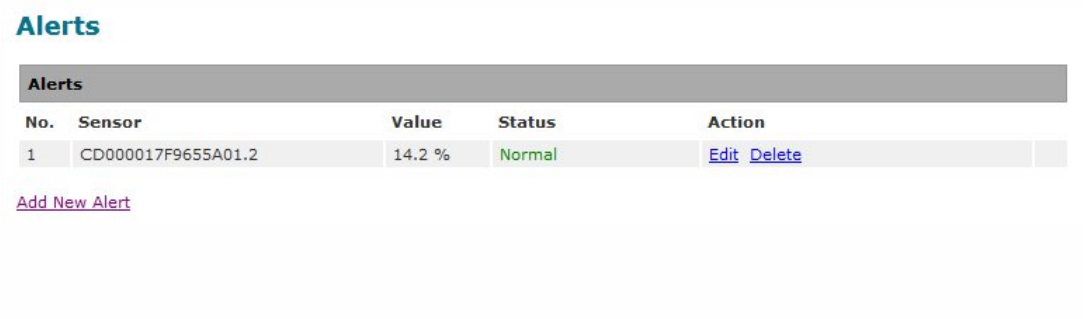


Figure 23- List of configured alerts and their status

ASHRAE Recommendation

According to ASHRAE's committee 9.9 for mission critical facilities, a class A1 data center can range in temperature from 59°F to 89.6°F and in relative humidity from 20% to 80%. This is very important for energy efficiency.

Temperatures for small hub rooms: 18-27°C / 64-80°F with ambient room humidity: 40% - 60% RH.

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, then click “Add”. The browser will redirect you back to the alert listing page.

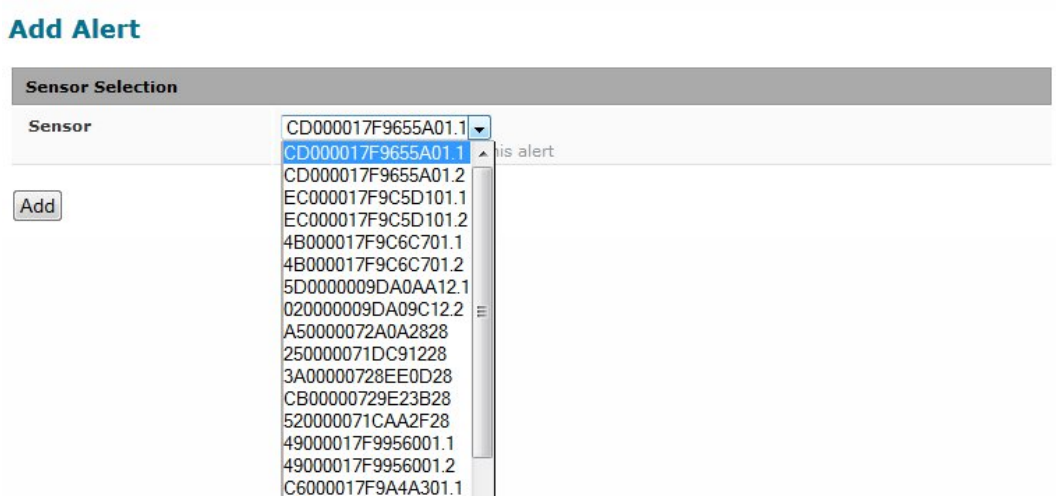


Figure 24- Select a sensor to add an alert configuration for

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.

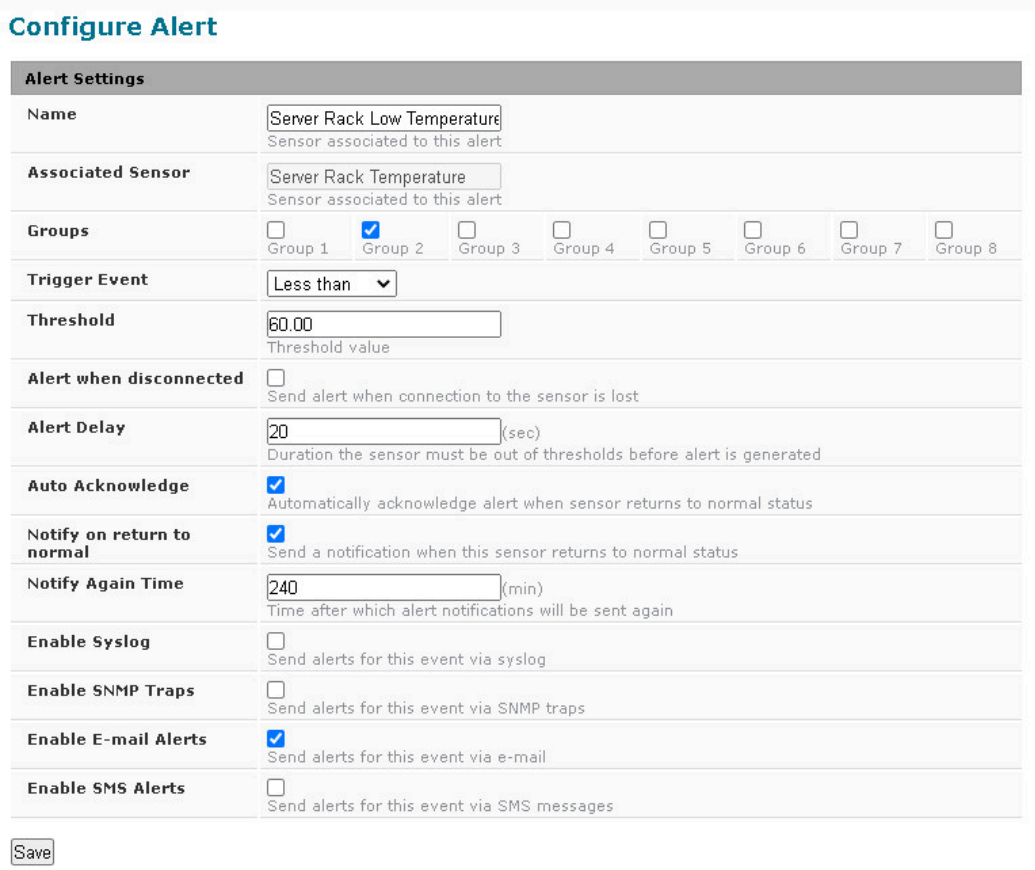


Figure 25- Alert Configuration page for Temperature/Humidity sensors

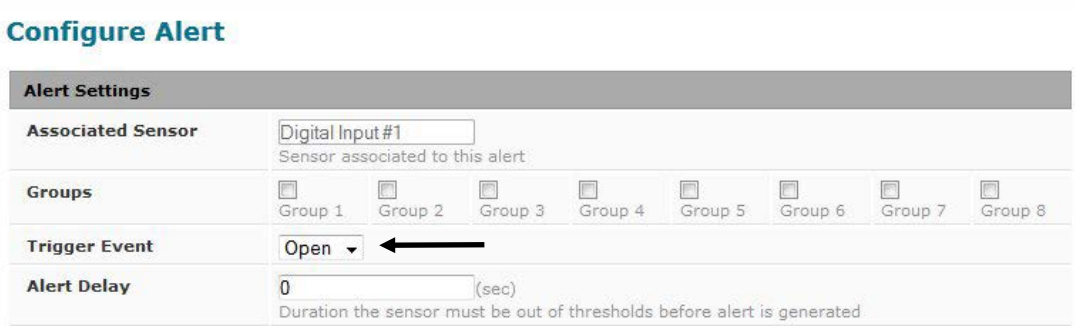


Figure 26- Alert configuration for Digital sensor- minor difference

Alert Settings	Description
Name	Apply a descriptive name for this specific alert.
Associate Sensor	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 19)
Group	Assign the alert to any group 1-8 (Note: Users intended to receive this alert must be assigned to the same group- page 39)
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 when disconnected	Place a checkmark in this box to have alert notification if the sensor is disconnected
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 39).

Note: For a user to receive alerts for a sensor, both the user and the alert configuration must have a common group number assigned.

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 21.

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

To begin, Alerts must be defined and configured. Events are sensor conditions to be notified of. Sensor configuration for these Alerts will have no impact on the general configuration of your sensors.

From the side menu, select “Smart Alerts”.

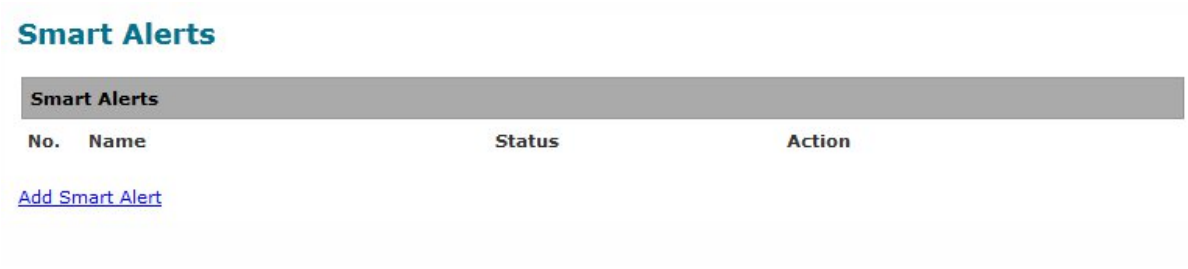


Figure 27- Smart Alerts page

On the Smart Alerts page, click on “Add Smart Alert”.

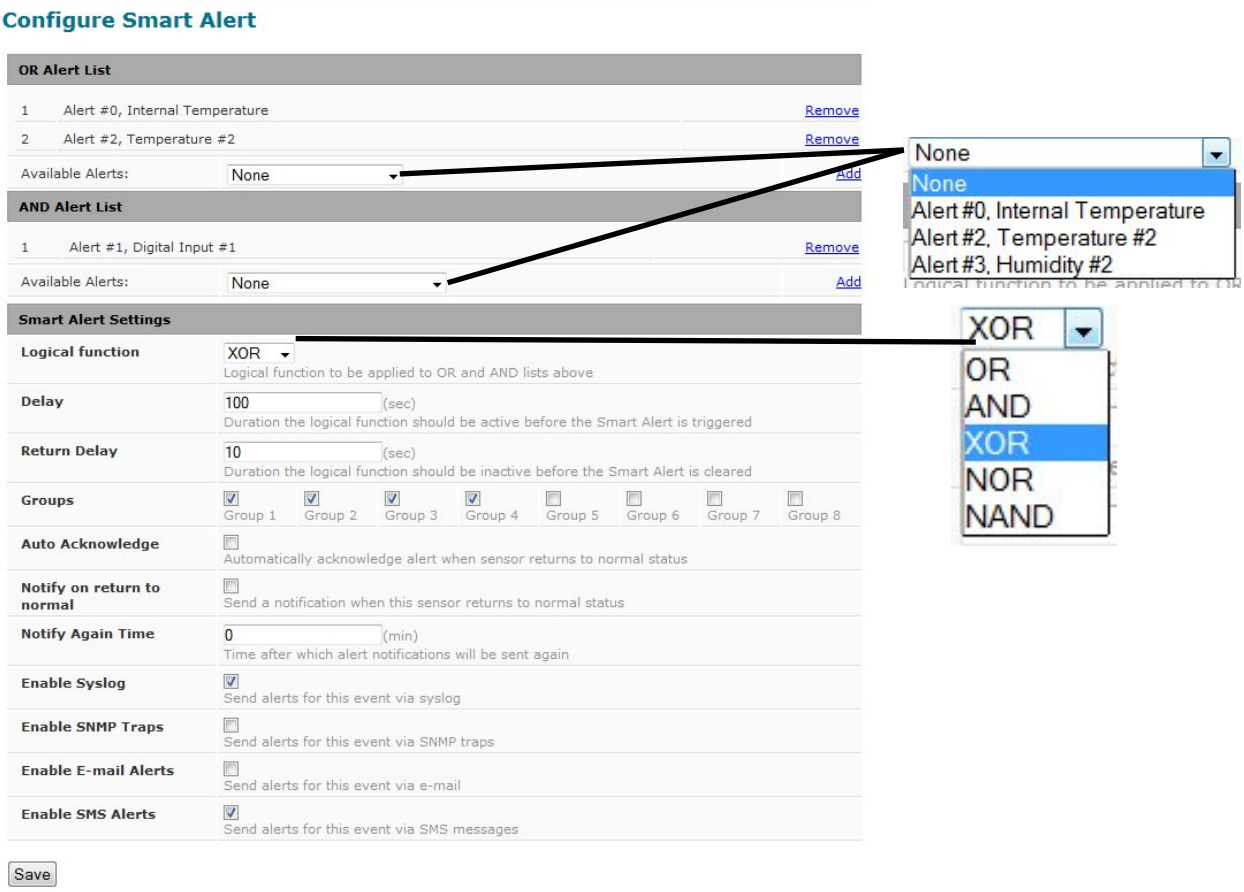


Figure 28- Sensor to be used for a predefined event

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 22)
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 27). 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.

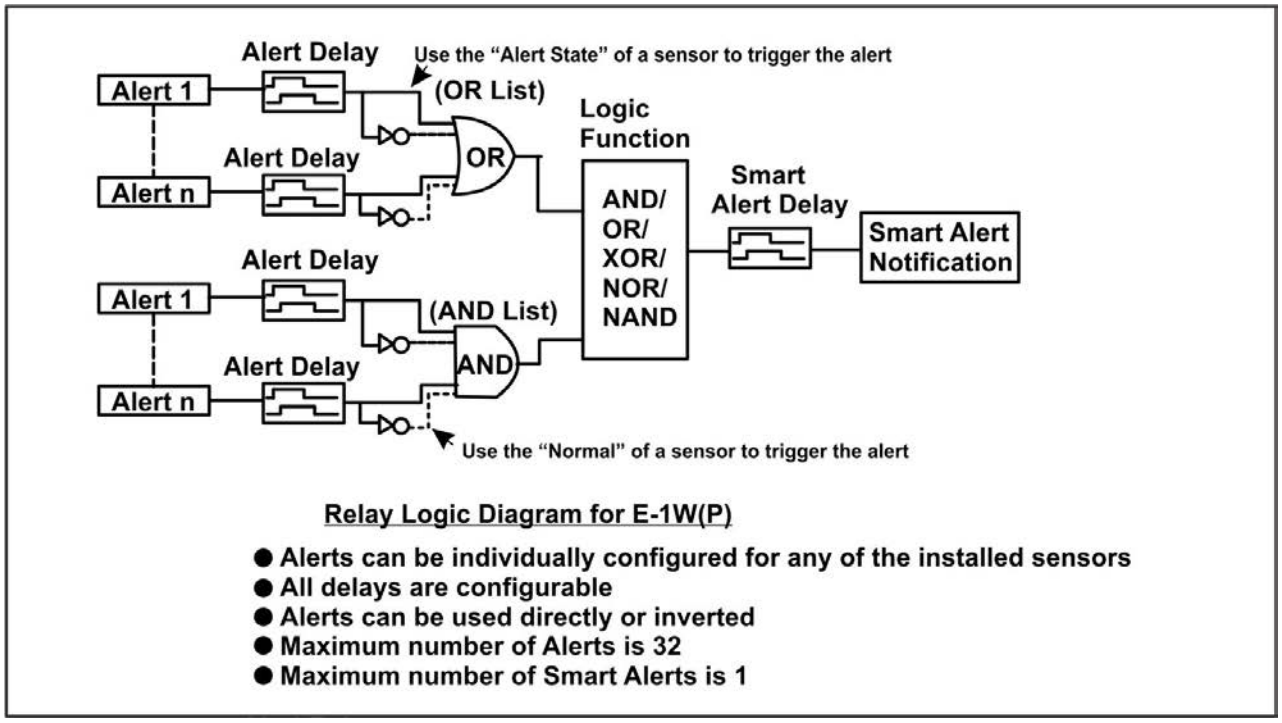


Figure 29- Event Logical Function Diagram

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.

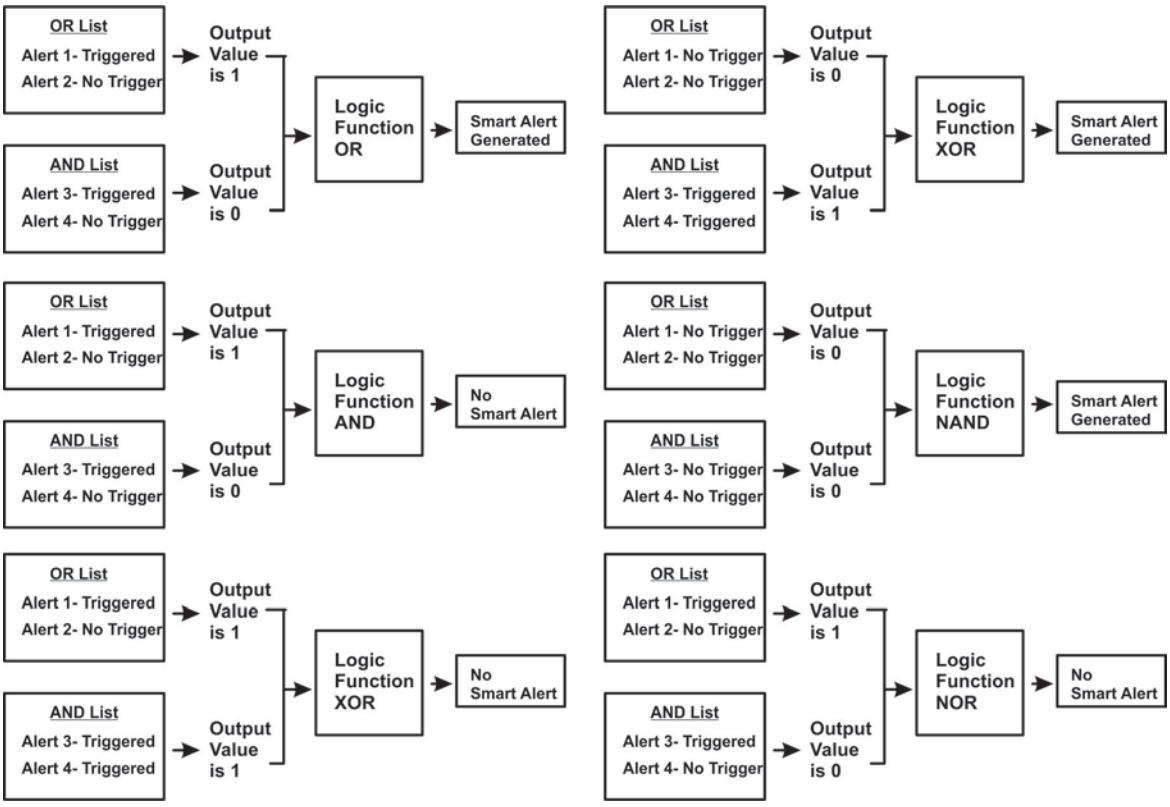


Figure 30- Examples of Smart Alert conditions

Administration

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

System	Field for applying unit name. Page also contains serial number, MAC address, Configuration file maintenance and certificate maintenance
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, Unit Name and Location of the E-1W. Only the Unit Name and Location is user-configurable. To view the System Configuration page, click on **System** from the **Administration** section of the menu.

You can **Use Custom Certificates** when using HTTPS web server mode. With custom certificates, you will be able to solve certificate warnings that show up with default certificates and also improve encryption security. If this option is unchecked, a default certificate will be loaded instead.

If changes are made, be sure to click on "**Save**".

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.

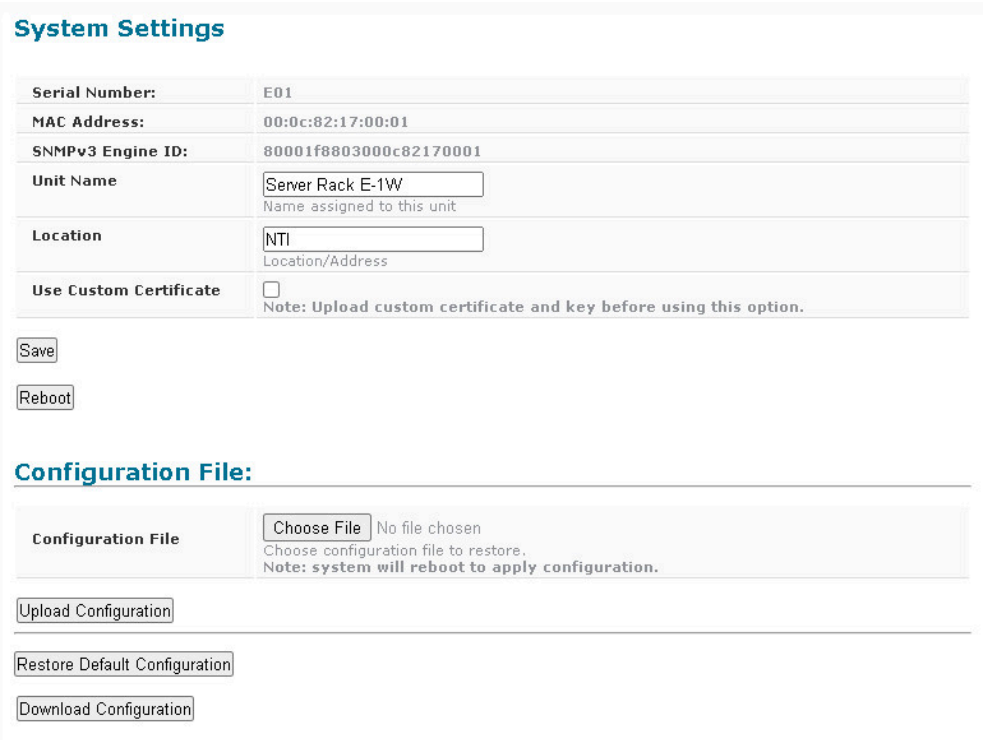


Figure 31- System Settings page

Configuration File

The Configuration File section provides a means to save and load the configuration settings for the entire E-1W. By saving this file before changes are made, you can easily restore a working configuration in the event a mistake occurs or changes are made that are only temporary in nature.

Configuration File Settings	
Choose file	Browse for a saved configuration file to be restored to the ENVIROMUX. Upon selection, press "Upload Configuration" and the ENVIROMUX will restore the configuration settings and reboot. Allow 1 minute before trying to reconnect and log in again. ***Note: The IP address will be set to the IP address in the file and may be different*** ***Note: Before overwriting the existing configuration, consider whether the existing configuration should be saved first. If it will be saved, be sure to save the current configuration file under a different name than the configuration file to be loaded.***
Upload Configuration	Click this button after choosing the configuration file to be uploaded.
Download Configuration	Click this button to save the current configuration of the ENVIROMUX to a location on your PC. This file can be restored using the "Choose file" and "Upload Configuration" buttons in the event you wish to return the ENVIROMUX to a former state
Restore Default Configuration	Click this button to restore the ENVIROMUX to the configuration settings it had upon receipt from the factory. **Be careful!** This will erase all user configuration settings. Upon restoration, the ENVIROMUX will reboot. Allow 1 minute before trying to reconnect and log in again. **Confirmation is required**.

Note: If "Restore Default Configuration" is used, and there is no DHCP server being used, the IP address will also be restored to its default address (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, or if defaults were restored and a DHCP server has assigned the IP address, use the Discovery Tool (page 14).

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

Default settings can also be restored using the "Restore Defaults" button on the ENVIROMUX (see page 3).

Certificates

If you want to solve certificate warnings, a valid certificate and key file can be uploaded provided the certificate and key are in ***.der*** format.

Note: Only RSA key lengths of up to 2048 bits are supported.

The Certificate Authority and certificates are normally provided in "CRT" or “PEM” format. Please see section I or section II of "How to Create x509 Certificate" for more information.

Either way, the certificate must be converted to DER format before uploading to the E-1W. See page 66 for DER conversion and upload instruction.

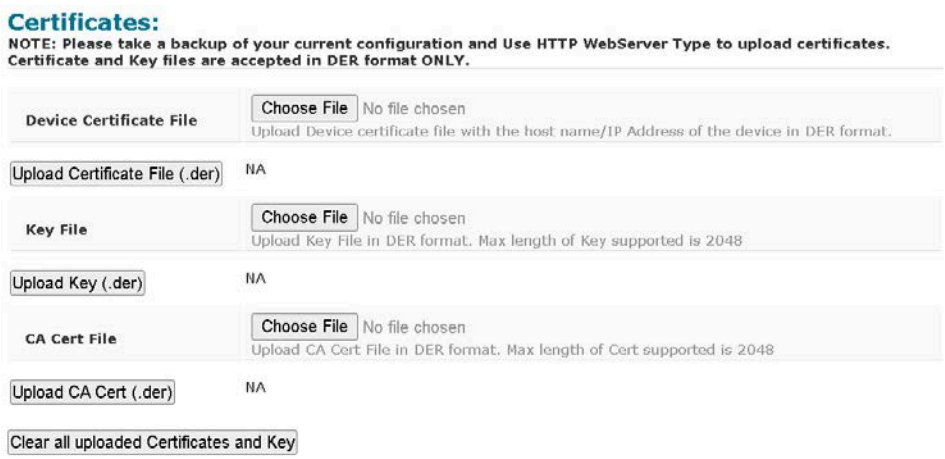


Figure 32- Certificates Upload on Settings Page

If you want to start over and clear all loaded certificates and key from the E-1W, click the “**Clear all uploaded Certificates and Key**” button will restore the unit’s default self-signed certificates if needed. Upon doing so, the default certificate will be reloaded to the E-1W.

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, or manually fill in the fields (use a static address). Settings can be entered for the IPv4 protocol. 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. If no DHCP server is found, the unit will boot to the address entered under "IP Address".

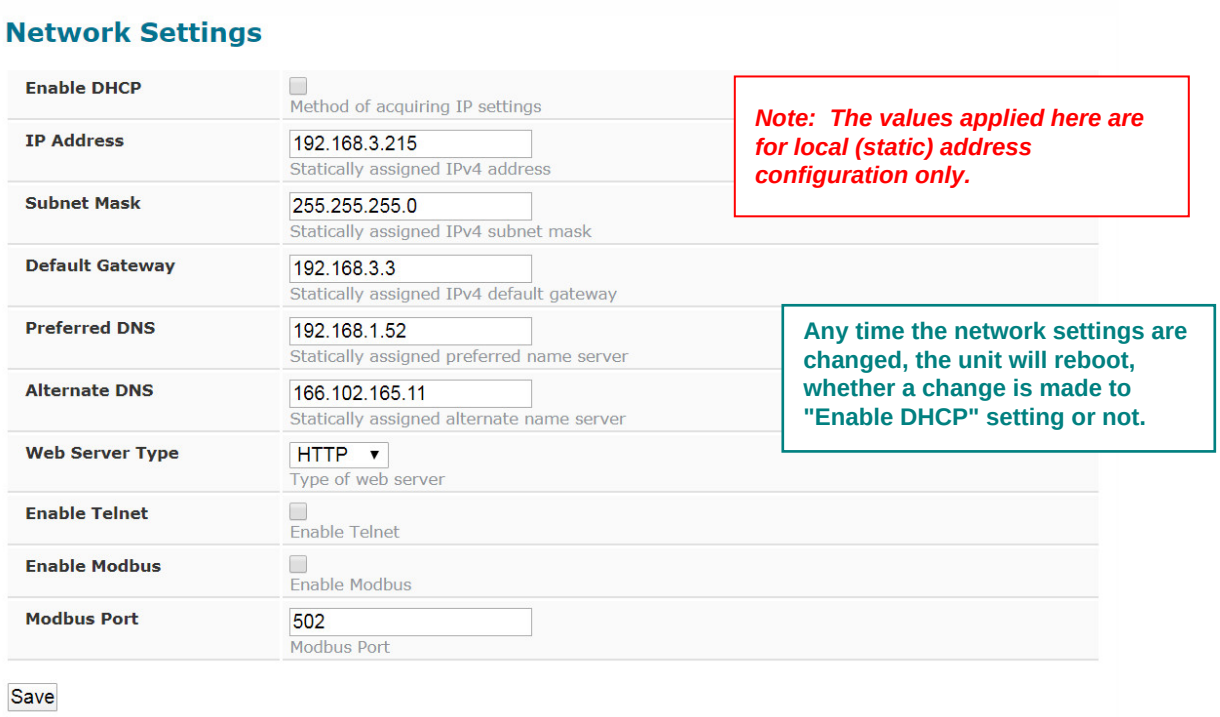


Figure 33- Network Settings page

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)
Enable Modbus	Place a checkmark in the box to enable access via Modbus software (see next page)
Modbus Port	Enter a valid port number to be used to communicate via Modbus (default is 502)

For added network security, leave the "Enable Telnet" block unchecked to prevent access to the E-1W Text Menu (page 49).

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 14) 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. The ENVIROMUX has a built-in fixed certificate so you will need to add a browser exception to connect to the ENVIROMUX. Accessing HTTPS via API is more responsive and is supported with exception for certificate validity check.

Modbus TCP/IP Support

The ENVIROMUX is equipped with Modbus TCP/IP support to enable PLC controls to read the value/state of the sensors and digital inputs. Specific instruction on this topic can be found on page 71.

SNMP Settings

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

Figure 34- 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 to be used, either SNMPV1/2C, SNMPv3, support all three with SNMPv1/v2c/v3, or disable it altogether.
SNMP Write	Enable or Disable Set action over SNMP, allowing to disable SNMP writes on entire device for security

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 **41**

Email Server Settings

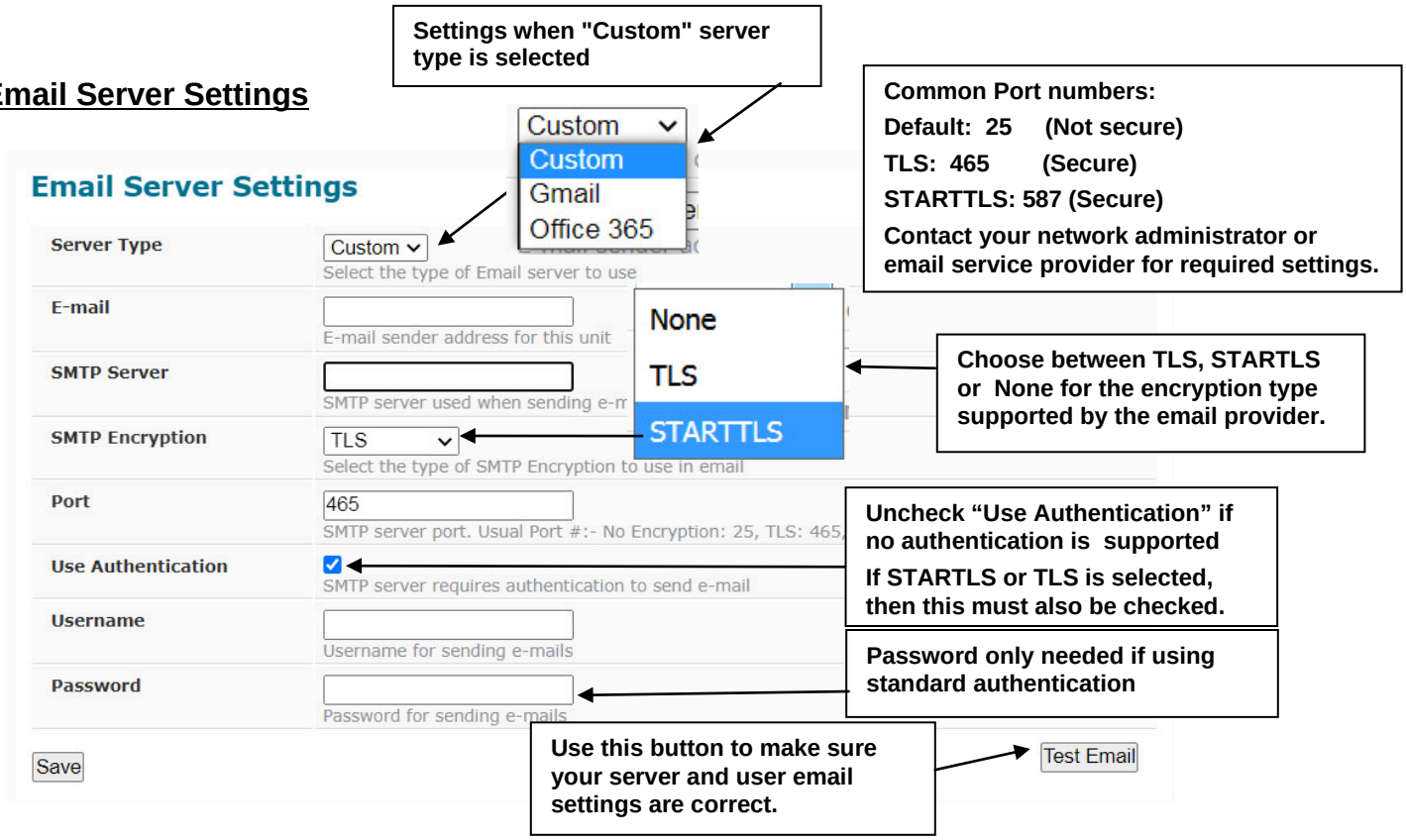


Figure 35- Email Server Settings- Custom Server Type

Email Settings	Description
Server Type	Choose between Custom, Office 365 and Gmail. Selecting Gmail or Office 365 will auto-select several fields.
E-mail	Enter a valid email address the E-1W can send emails from
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-1W(P) sends alert messages using TLS authentication.
In choosing an email service to use with your E-1W(P), make sure that service either supports:

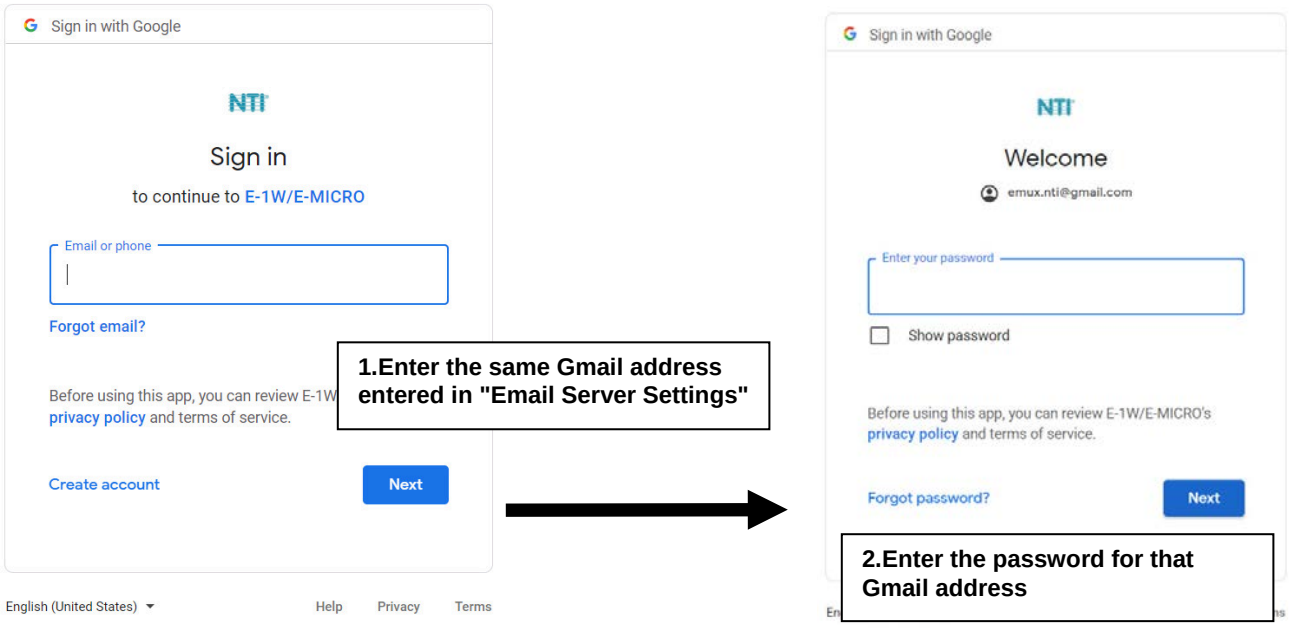
1) TLS v1.2 secure encrypted authentication,
2) STARTTLS secure encrypted authentication,
3) Standard authentication (authentication where just a username and password are required (non-encrypted)), or
4) messages sent with No authentication (no username or password required).

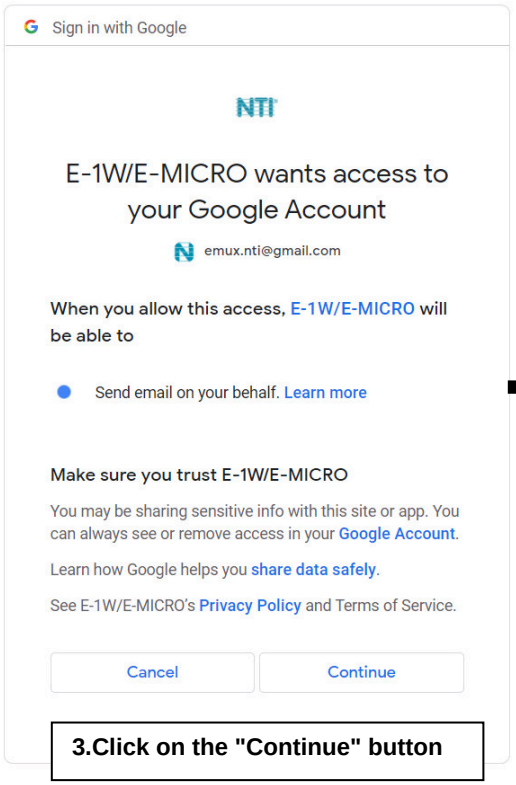
Figure 36- Email Server Setting- Gmail Server Type

Gmail Server Type

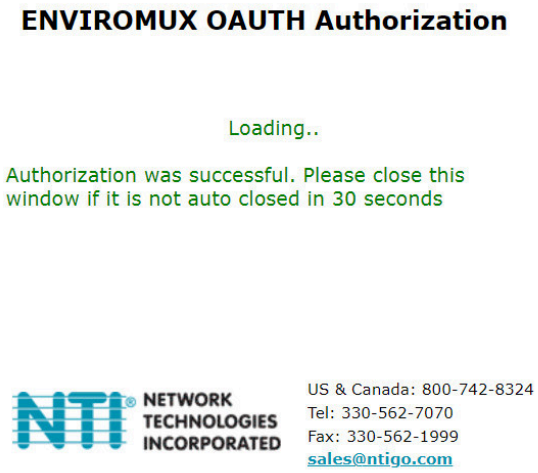
When the Server Type is Gmail, most of the rest of the settings are pre-selected for you. Only the E-mail address at Gmail that the ENVIROMUX will use to send out alert messages needs to be entered. Then click "Save" button.

After saving, Click the "Authorize with Google" button to complete the process. The following screens will pop-up.

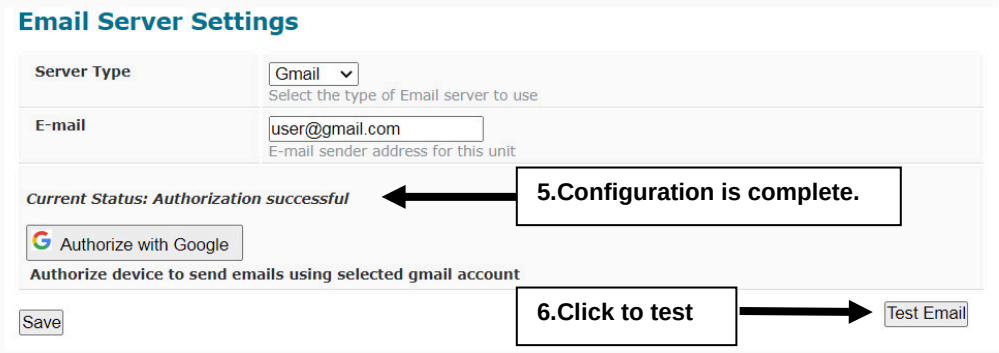




3.Click on the "Continue" button



4.Gmail authorization is successful



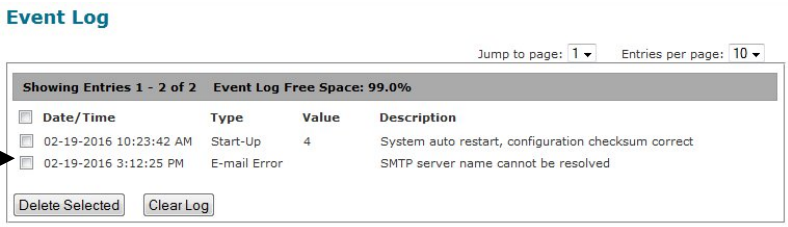
5.Configuration is complete.

6.Click to test

Once the email server settings are configured and the user settings are configured (page 39), click on "**Test Email**" button to verify that the configuration has been done correctly. Each configured user with "E-mail Alerts" enabled will receive an email from the E-1W email address that reads "Test Email Configuration" in the body of it.

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 44).

Email error in Event Log



NOTE: Device needs access to the Google servers (https://accounts.google.com, https://www.googleapis.com) to send emails. Additionally, device also needs access to the NTI server (https://www.networktechinc.com) during OAUTH setup. Ensure any firewall in between allows connections to Google and NTI servers from the device.

Office 365 Server Type

When the Server Type is Office 365, most of the rest of the settings are pre-selected for you. If you do not have existing email address with Microsoft, please create and register a new Office365 account with Microsoft. Then enter that email address in the E-1W web interface for the Email Server Setting. That will be the email address that the ENVIROMUX will use to send out alert messages. Then click "Save" button.

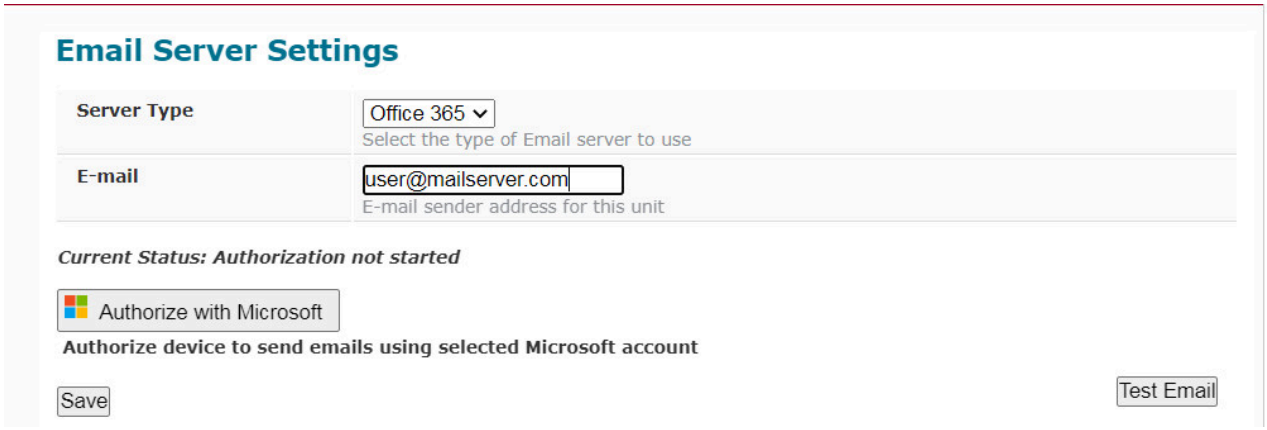
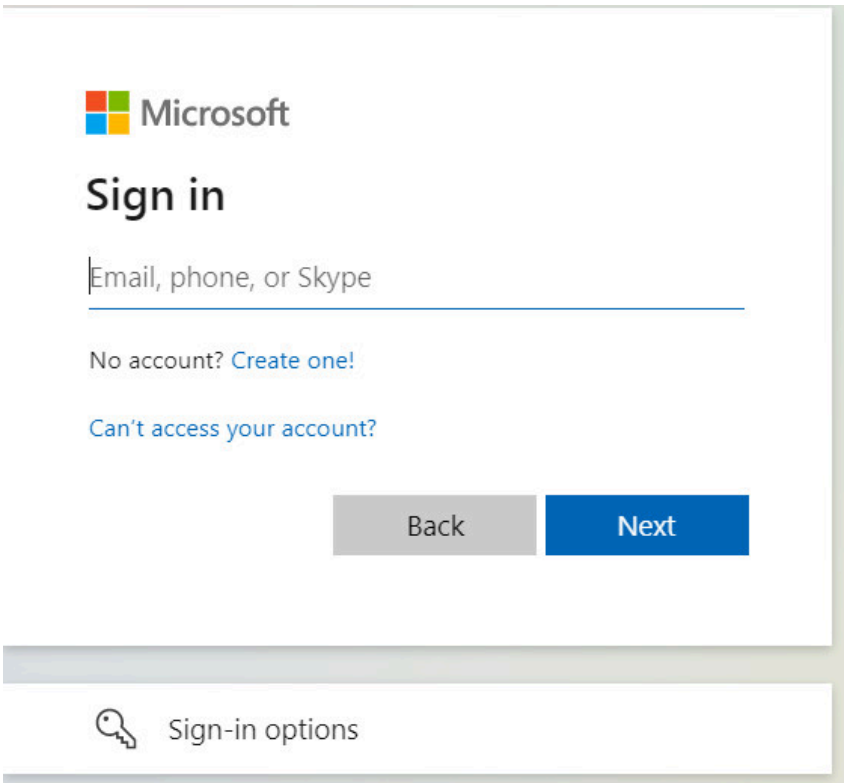


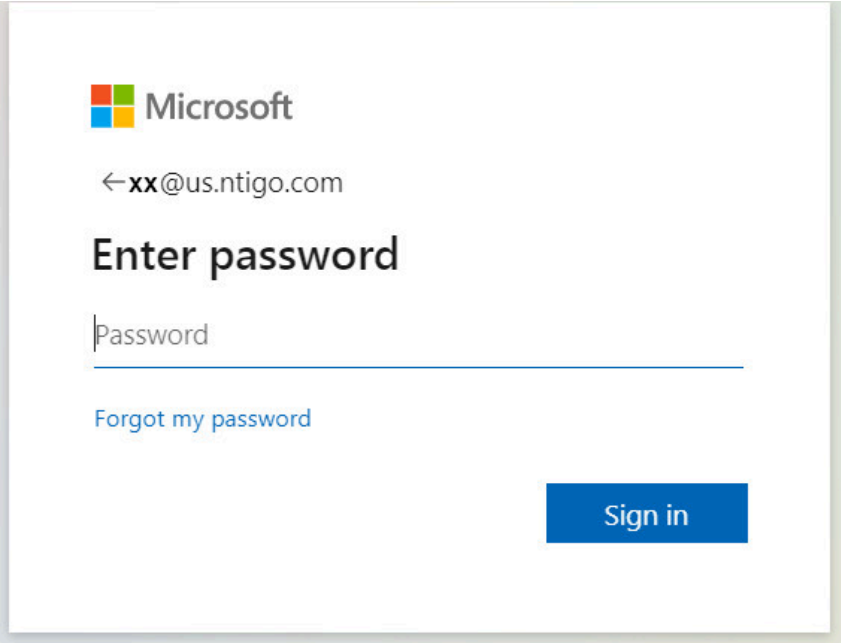
Figure 37- MS Office 365 server settings- before authorization

After saving, Click the "Authorize with Microsoft" button to complete the process. The following screens will pop-up.

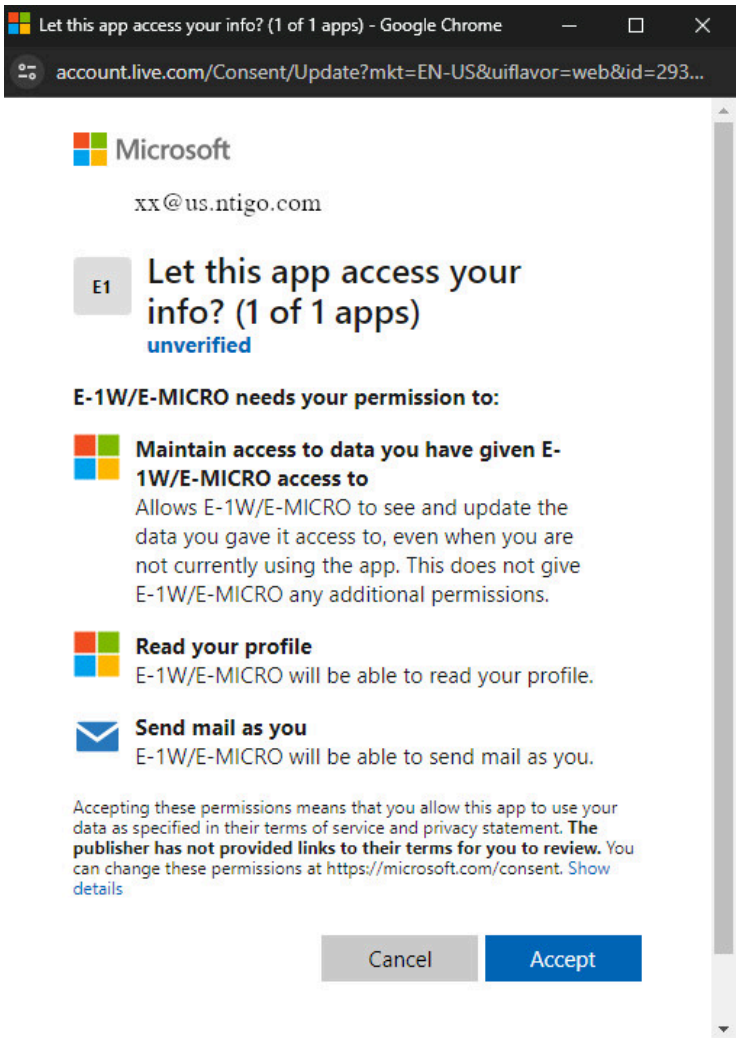


Sign in using your MS Office 365 email address.

Enter the password used for your MS Office 365 account.



Click "Accept" in the next screen to authorize the E-1W to send email through the provided email address.



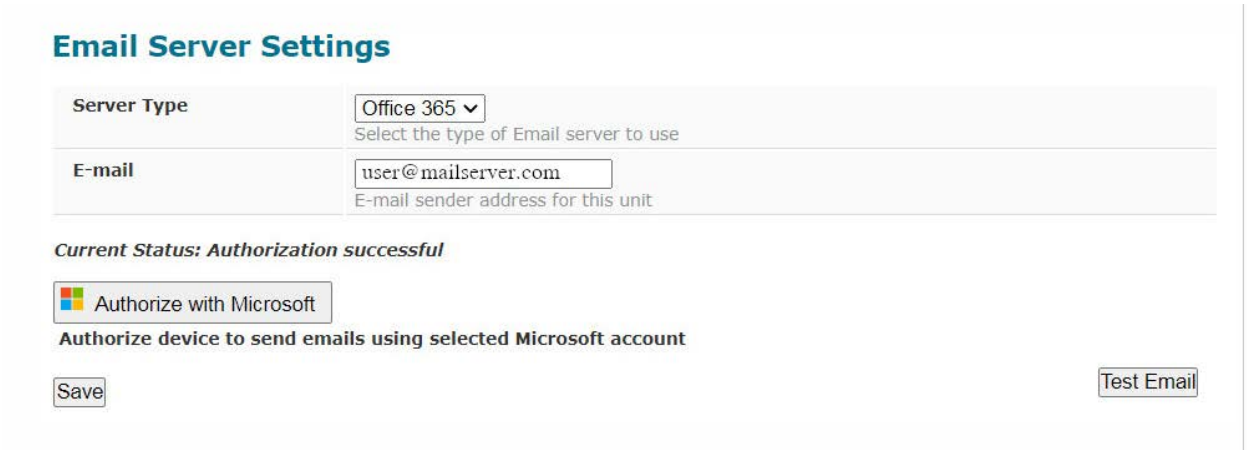


Figure 38- MS Office 365 server settings- after authorization

Authorization is complete and you are ready to test.

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.

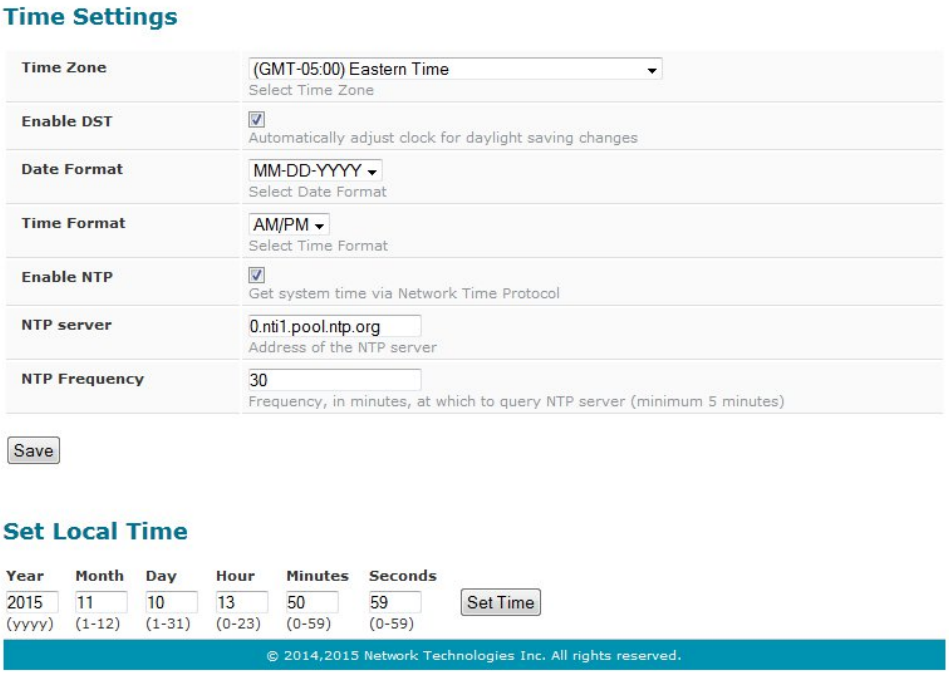


Figure 39- Time and Date Settings

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	Select date to be presented in desired format
Time Format	Set for AM/PM or 24 Hour 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.

Figure 40- Users List

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

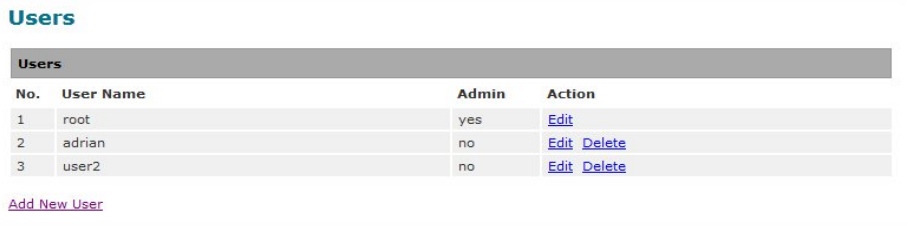


Figure 41- User2 added- ready to configure

Click "Edit" to bring up the User Settings.

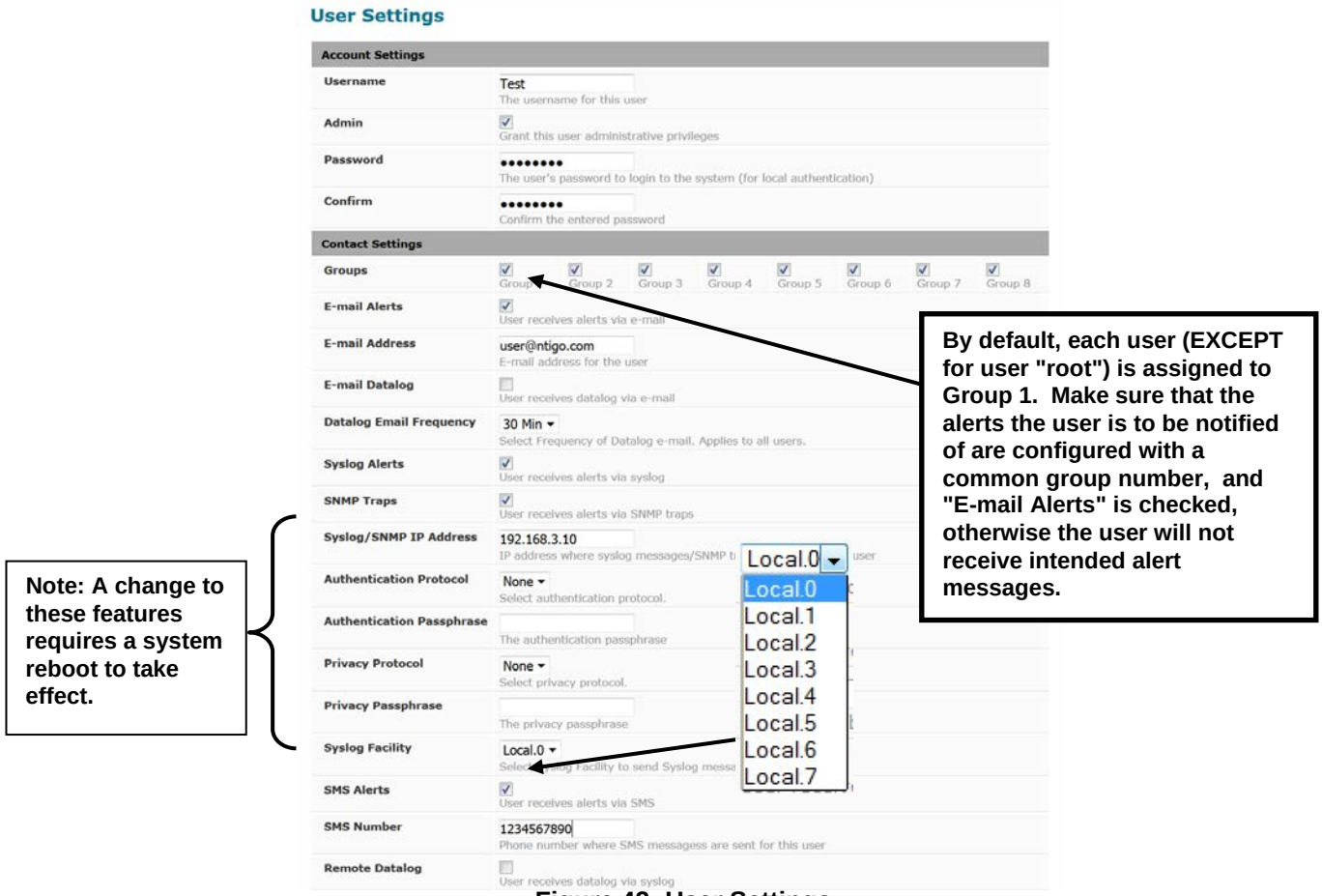


Figure 42- User Settings

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

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
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 22 and 47 for group assignments)
Email alerts	Place a checkmark if the user should receive messages via email **Tip:** Address can be user's telephone number and carrier to receive SMS messages on their cell phone (i.e. 1234567890@pushover.net)
Email address	Enter a valid email address if this user should receive email alert messages
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- the email will include the most current report)
Syslog alerts	Place a checkmark if the user should receive alerts via syslog messages
SNMP traps	Place a checkmark if the user should receive alerts via SNMP traps
Syslog/SNMP IP address	Enter a valid syslog/SNMP IP address for the user to receive syslog/SNMP messages (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 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

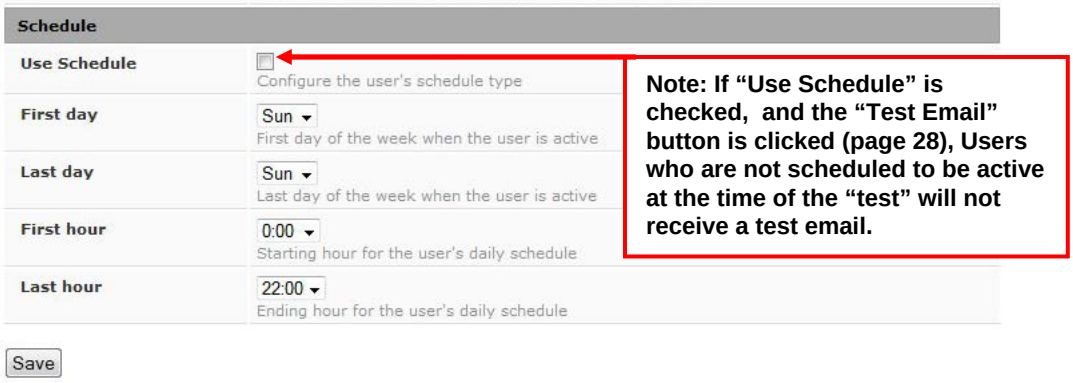


Figure 43- Scheduling parameters

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-1W(P) to take effect.

IP Cameras

Contact an NTI product consultant for IP cameras compatible with E-1W.

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.

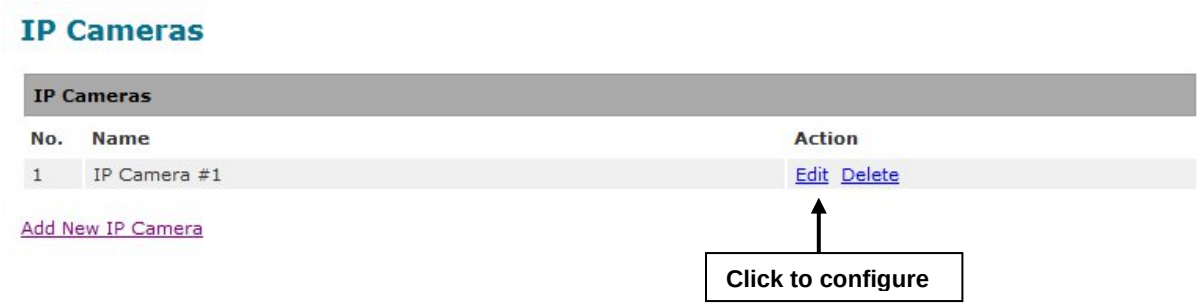


Figure 44- IP Camera Monitoring

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

Figure 45- 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 the **Summary** page 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-1wire.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.

Note: To perform a firmware update, first change the "Web Server Type" to HTTP on the Network Settings page (page 30).

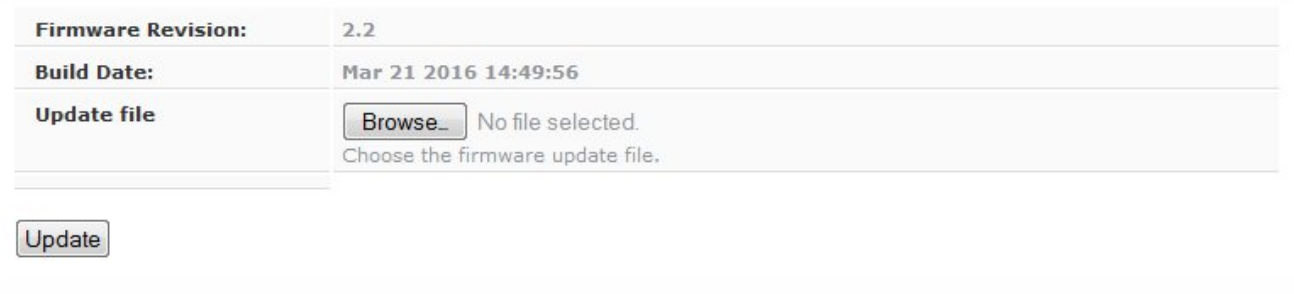


Figure 46- Update Firmware page

1. Download the most current firmware file from http://www.networktechinc.com/download/d-environment-monitor-1wire.html to a location on your PC.
2. Click on the "Browse" button and locate and select the firmware file for the ENVIROMUX (***E-1W-v2-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:

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

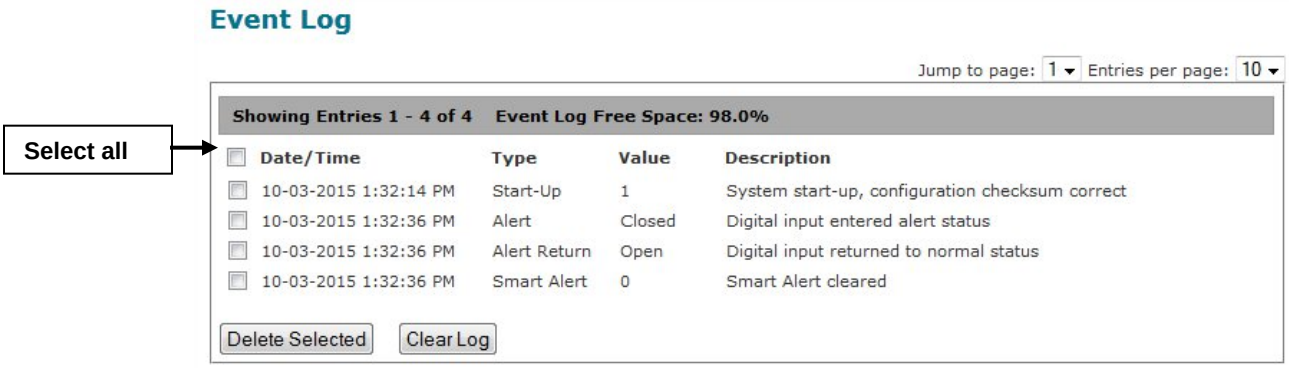


Figure 47- Event Log page

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.

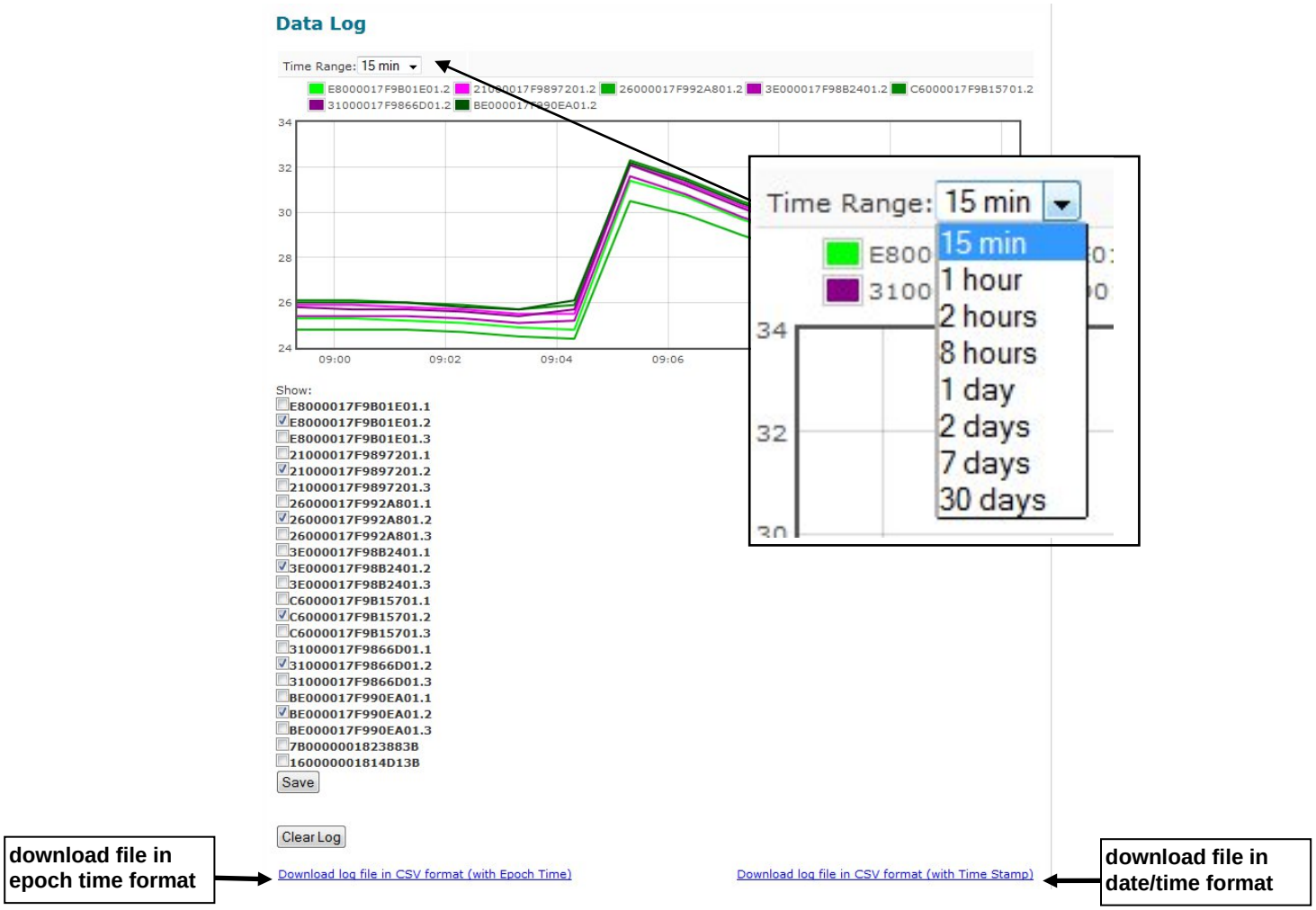


Figure 48- Data Log page

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 as15 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 39) will be in Epoch Time CSV format and will include data for all sensor ports whether they are in use or not. The log receives a report once each minute, and the data emailed will only include the most recent report (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".

Example of Data Log email:

```
Subject: Message from E-1W P02 [Datalog]
Date: Tue, 20 Aug 2019 16:09:46 -0400

1566331783,78.12,78.29,46.91,56.34,78.46,n/a,n/a,O,C
```

Tip: When an automatic reporting of data from the ENVIROMUX is needed, it is recommended that the SNMP features of the E-1W be used with an SNMP program to sense, accumulate and provide analysis for configurable periods of time.

The E-1W will store up to 30 days worth of data at a time for each connected sensor, presenting that data in the graph and CSV file as per the configuration. After 30 days, old data is overwritten by new data. To erase all data and restart recording, click on "**Clear Log**".

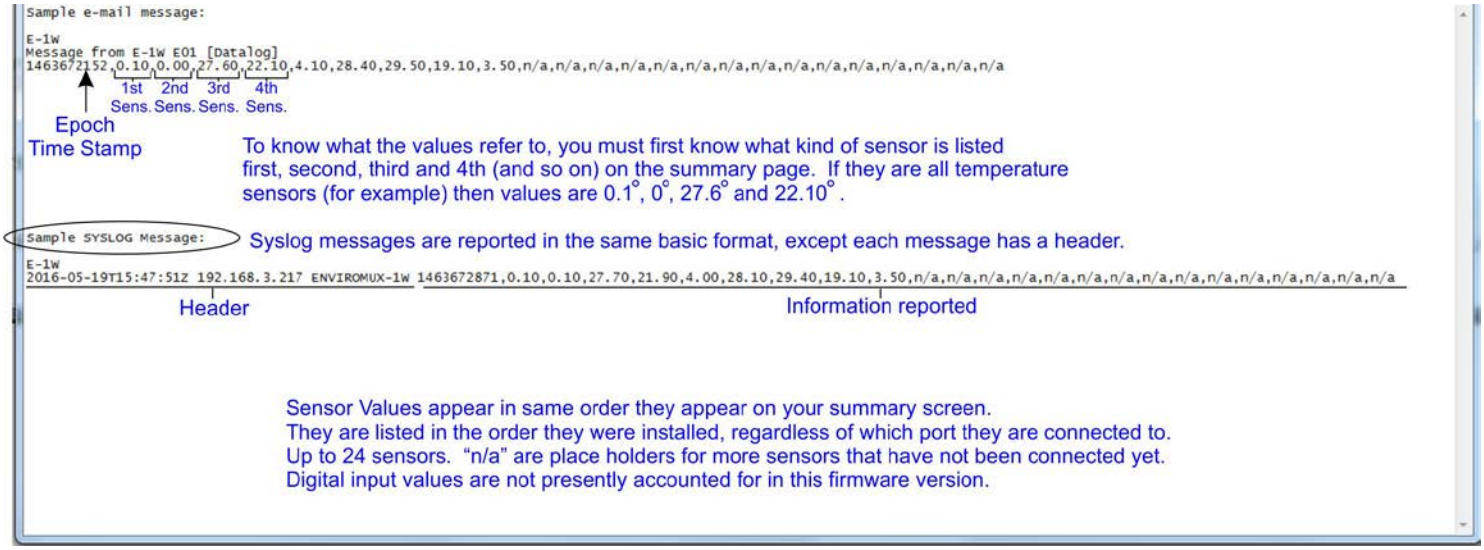


Figure 49- Datalog message interpretation

IP Devices

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

Figure 50- 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 as often as desired and to react to a lack of response by sending alert messages.

Figure 51- 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:

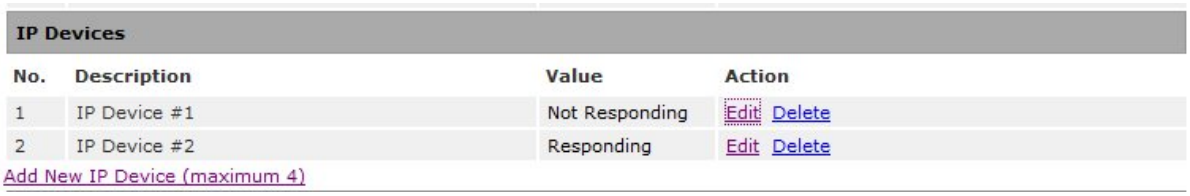
Ping Period = 10 sec Timeout = 2 sec Retries = 5

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 20.

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 52- 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.

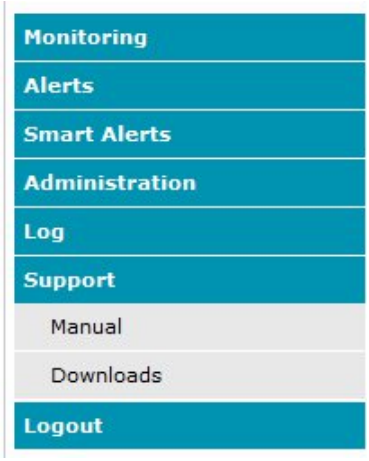


Figure 53- Support

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 54- Logout

OPERATION VIA TEXT MENU- ENVIROMUX

The ENVIROMUX can be accessed through a text menu using the Telnet provided a connection has been made to the Ethernet Port (page 10). 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 15).

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, Putty, etc.. provided the ENVIROMUX is properly connected to your LAN through the Ethernet port (page 10).

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".

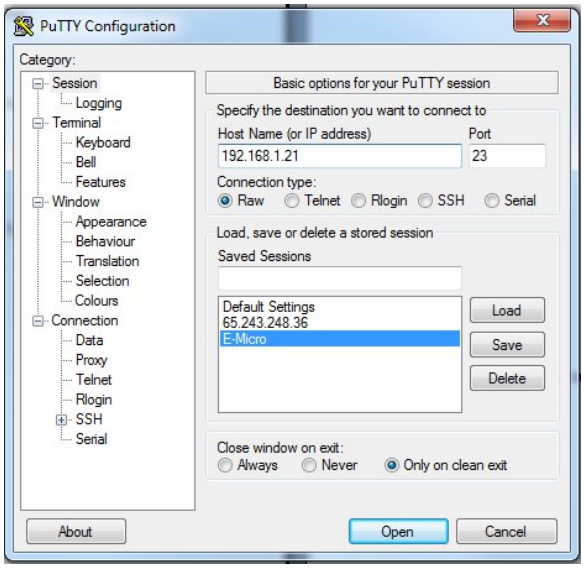


Figure 55- Terminal connection through Ethernet port

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

Figure 56- 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 10).

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.

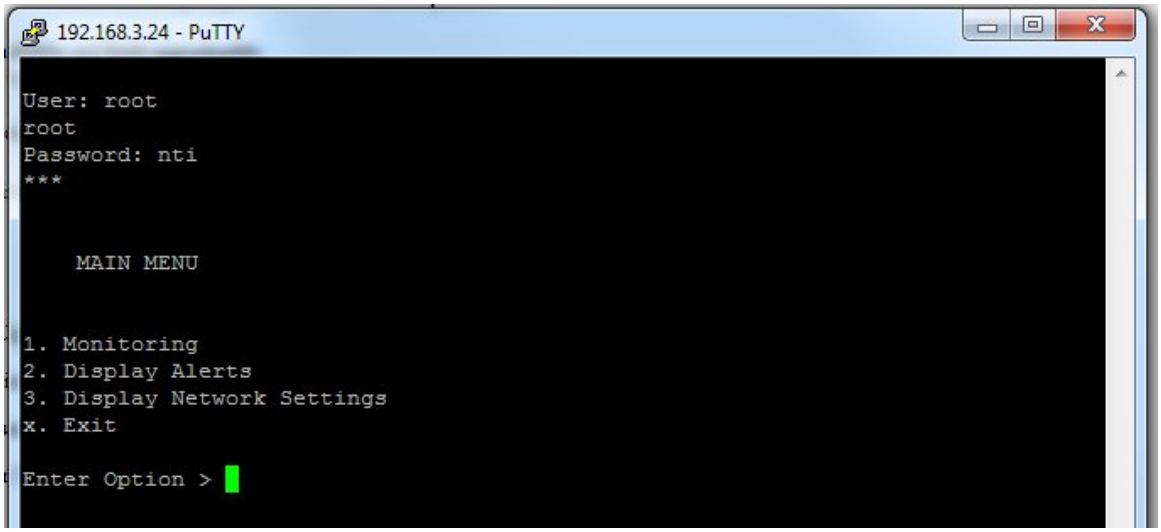


Figure 57- Text Menu- Administrator Main Menu

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.

Disregard item 1. "Integrated Sensors". This does not apply to the E-1W.

Figure 58- Text Menu-Monitoring Menu

View Sensors

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

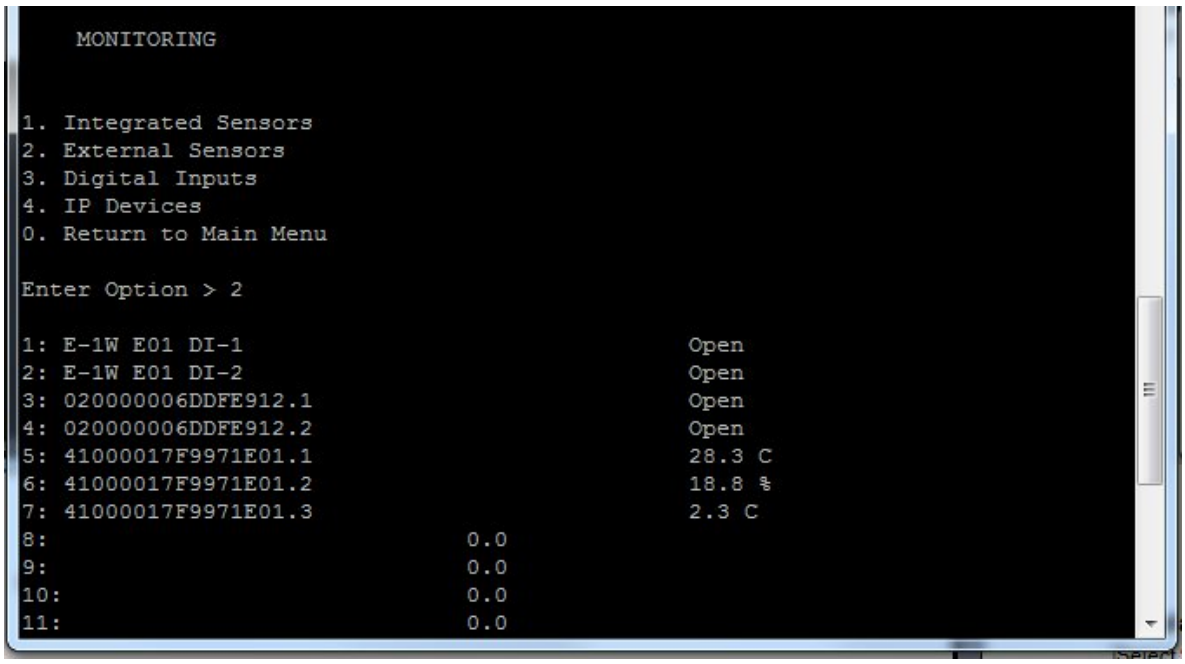


Figure 59- Text Menu-Sensor Status

Digital Inputs

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

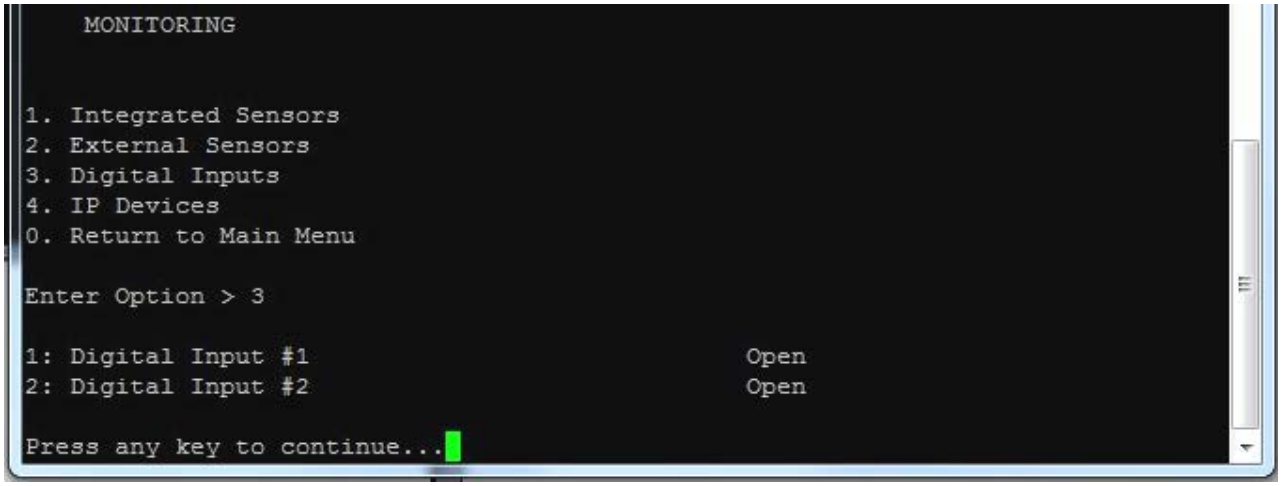


Figure 60- Text Menu- Digital Input Status

IP Devices

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

Figure 61- 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.

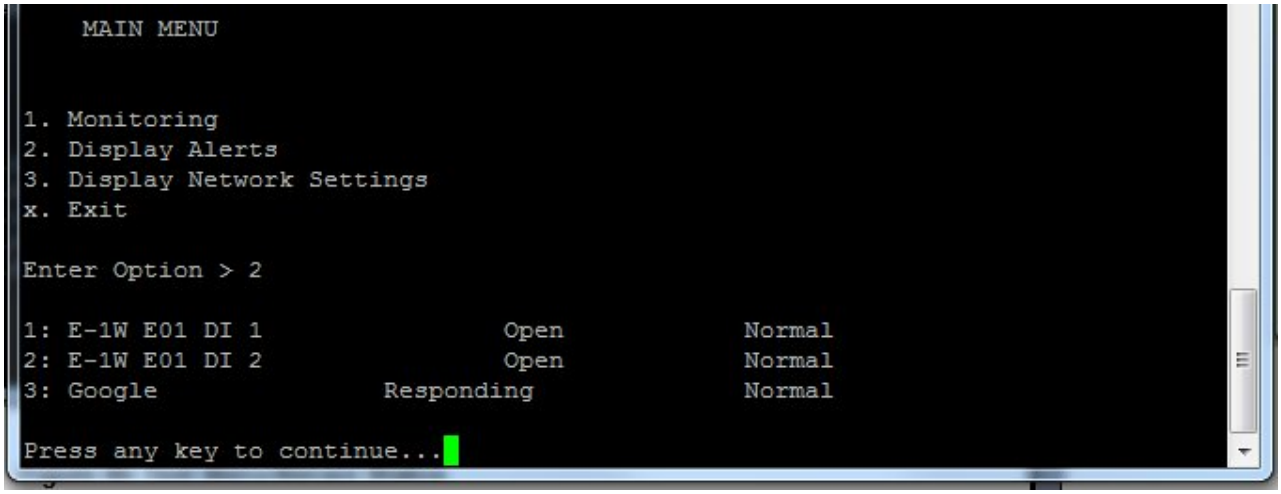


Figure 62- Text Menu-Configure Sensors list

Display Network Settings

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

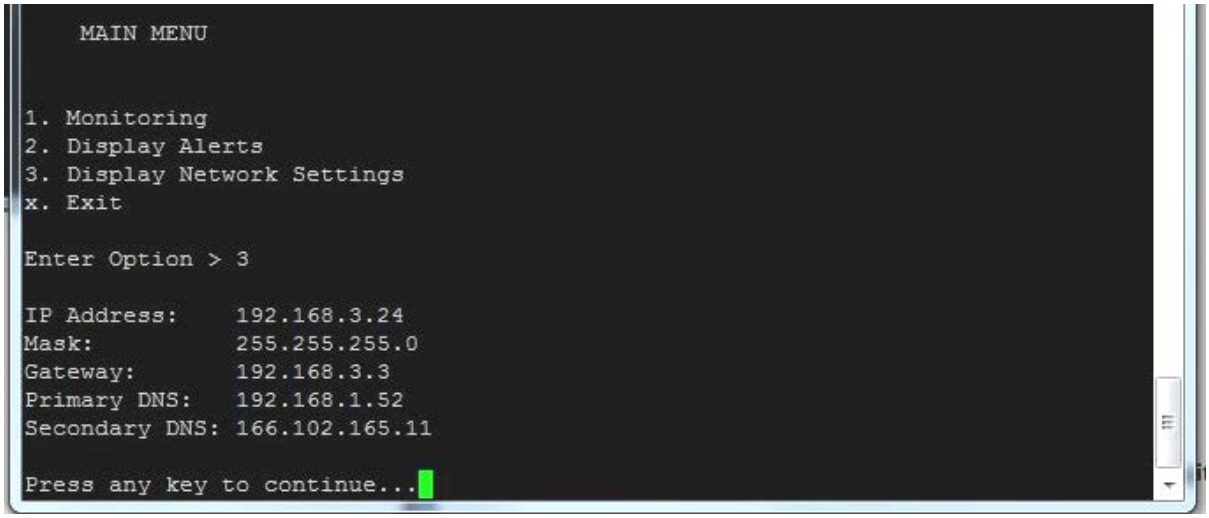


Figure 63- Text Menu-Network Settings

Press <**x**> to exit the text menu.

RESTORE DEFAULTS BUTTON

A “Restore Defaults” button is located on the front of the E-1W(P). 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.

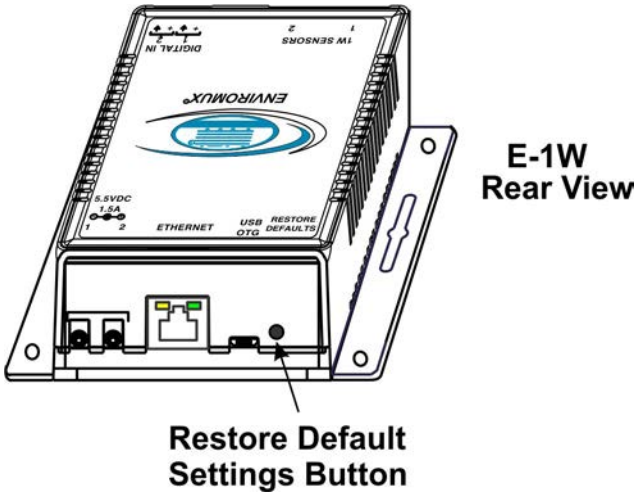


Figure 64- Location of Restore Defaults button

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 14).

USB PORT

The ENVIROMUX is equipped with a “USB OTG” Micro USB female port. This is reserved for future use.

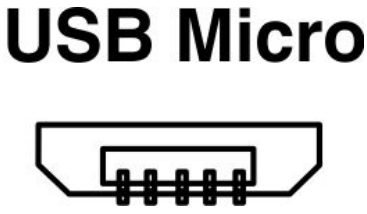


Figure 65- USB OTG port

HOW TO SETUP EMAIL

Use this guide to assist in the configuration of the ENVIROMUX to send email messages. Be sure each user is assigned to at least one group and that "Email Alerts" is checked before using the "Test Email" button.

1. Apply a valid email address for the ENVIROMUX to the Email Server Settings Page (see page 32).

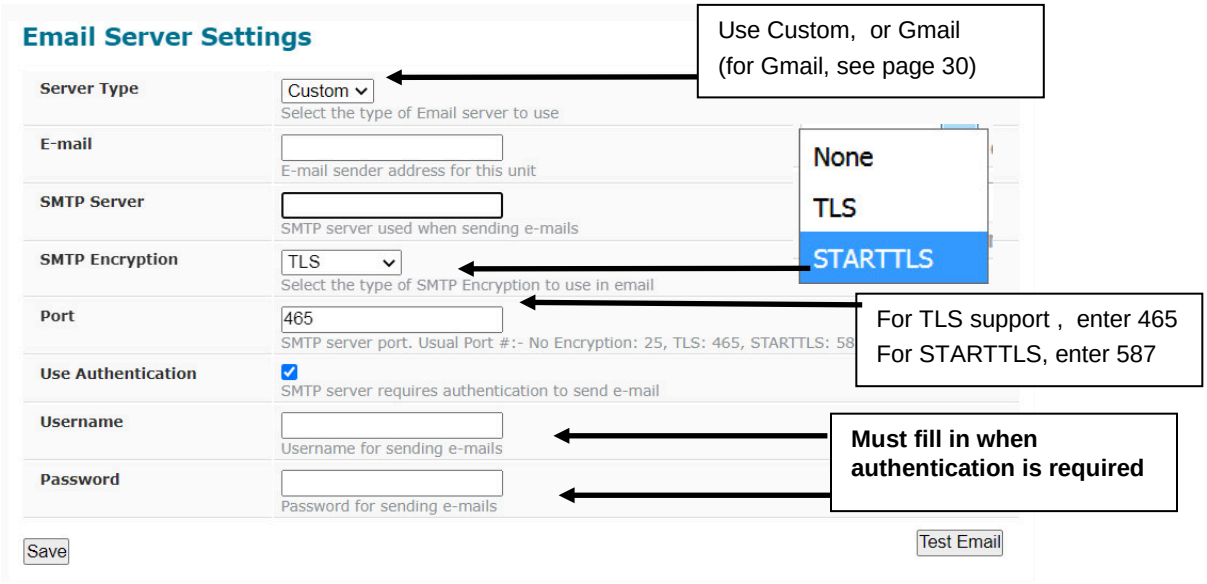


Figure 66- Email Server Settings example

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

2. Fill in Email Settings (page 30) 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) . For MS Office 365, use smtp.office365.com.

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 STARTLS, 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.

Example Email Server Settings for MS Office 365:

SMTP Server: smtp.office365.com

SMTP Encryption: STARTTLS

Port: 587

Place checkmark in for "Use Authentication"

Username: Enter the account e-mail address

Password: Enter the account password **NOTE: THIS IS CASE SENSITIVE**

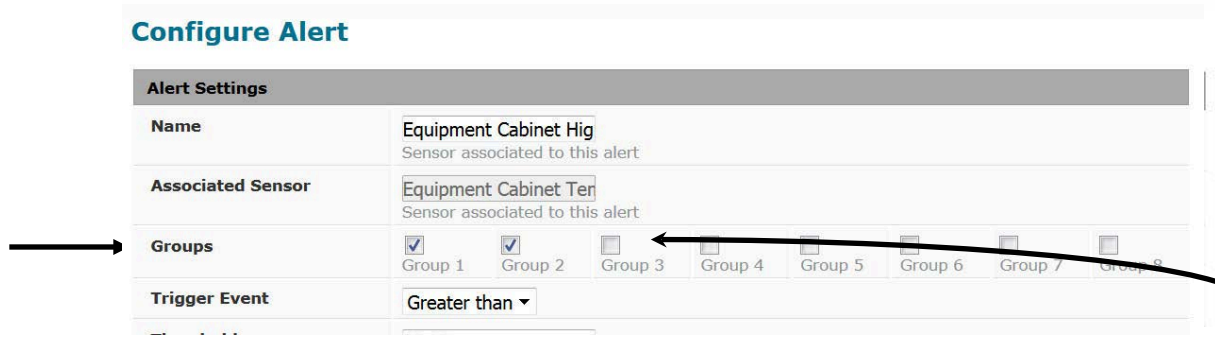


Figure 67- Configured alert to send to at least one group

3. Make sure the alert is configured to send messages to one or more groups.

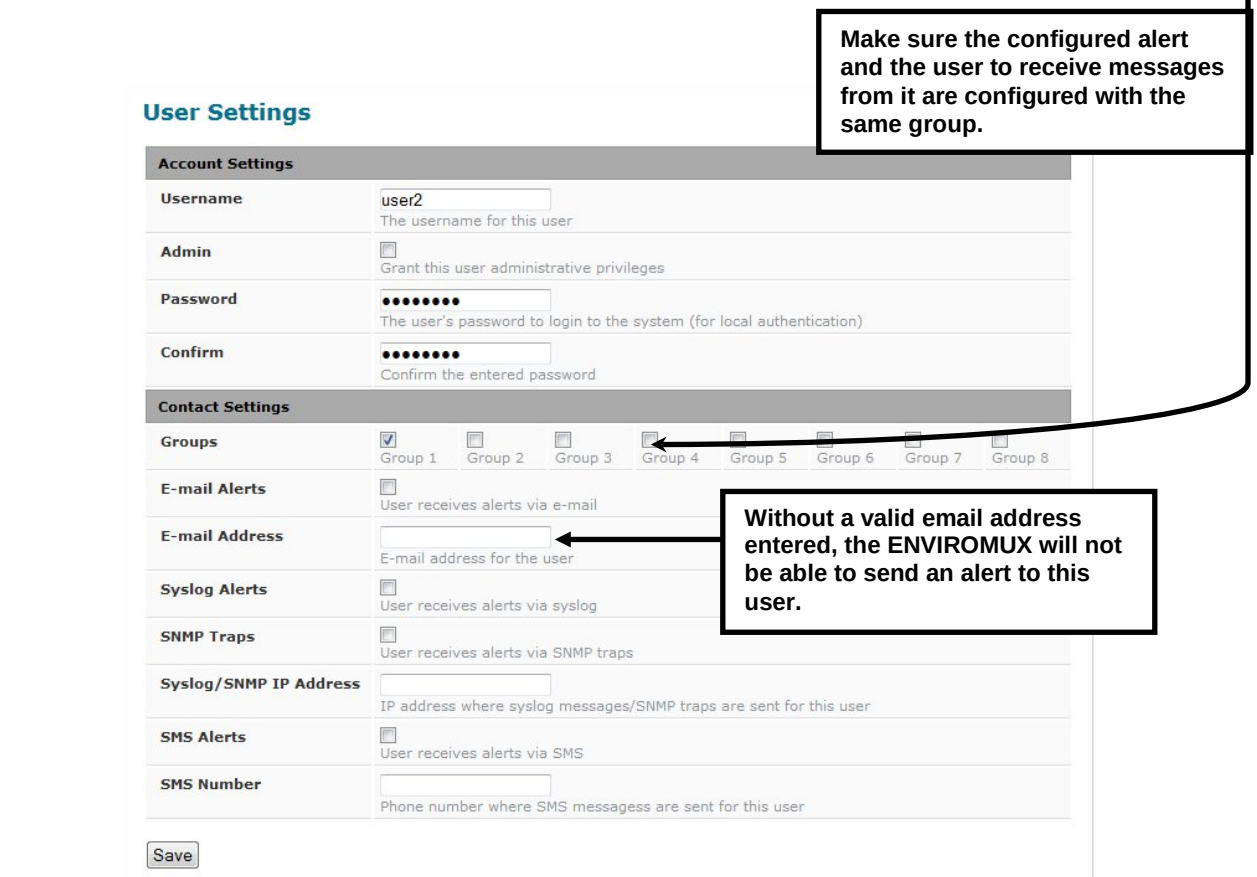


Figure 68- Configure user to receive alerts via email

4. Verify the User is configured to receive notifications from at least the same sensor group that the alert is configured to send alerts to.
5. Make sure that "E-Mail Alerts" is selected and has a valid E-Mail address to send the notifications to.

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 40). 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 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-1wire.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.

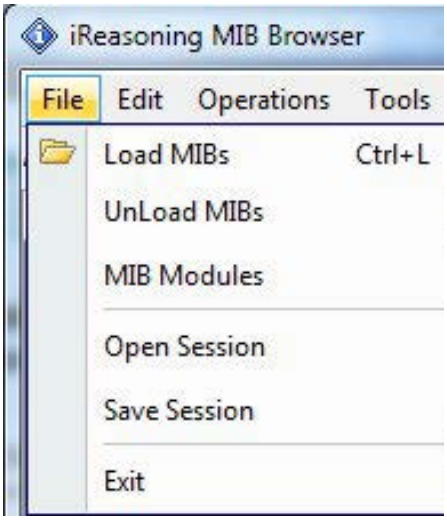
View OIDs

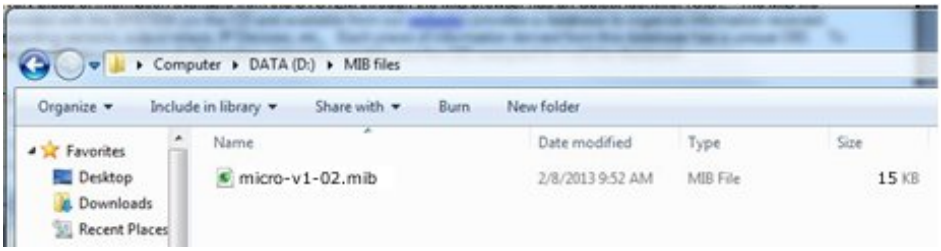
To view this information, you must do the following:

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.

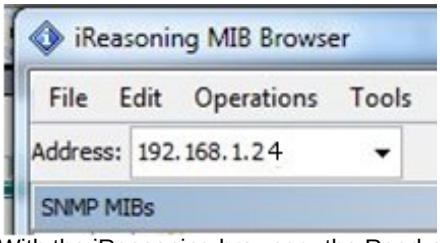




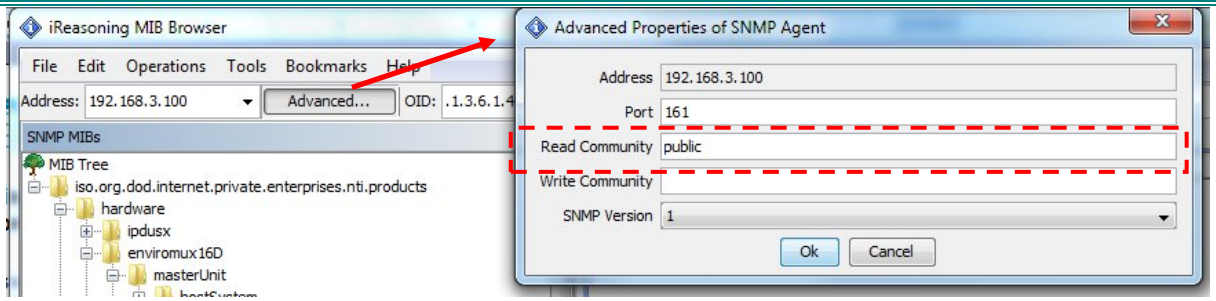
Select "Load MIBs" and locate the MIB file on your PC.

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.



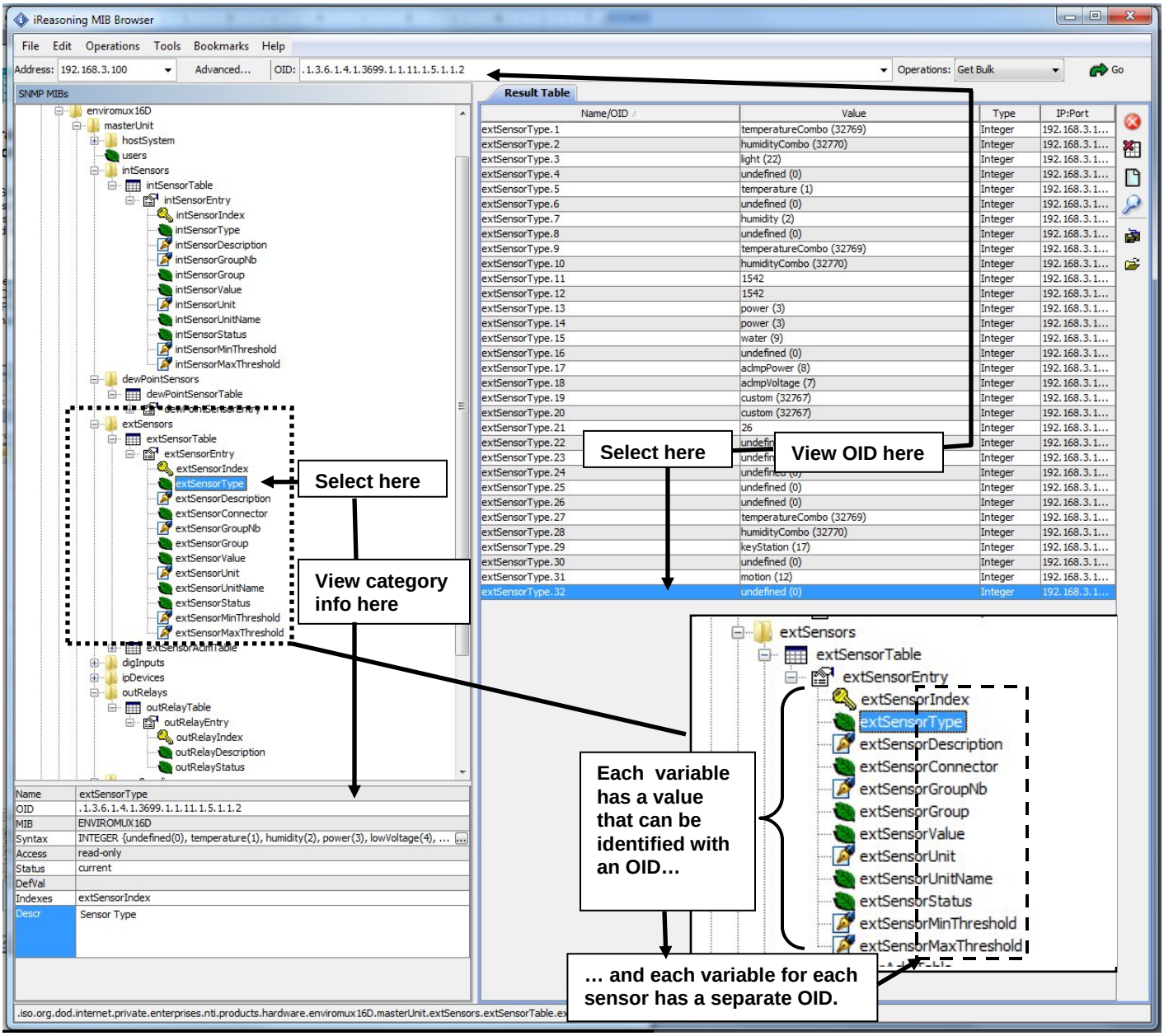
5. With the iReasoning browser, the Read-only Community Name (default is "public") was automatically sensed and applied when the IP address was entered, but if this doesn't happen in your browser, make sure the "Read Community" field in the agent properties includes the name "public" (or whatever you have changed it to in the SNMP 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 31 and your browser manual to apply the required additional settings.

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



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

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

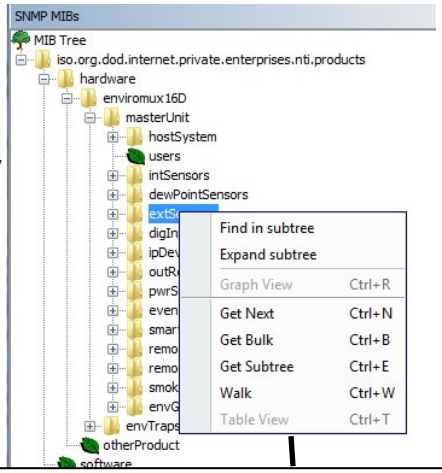
To get specific results in the Result Table, right click on an item in the MIB Tree and choose the type of search ("operation") you want.

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

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

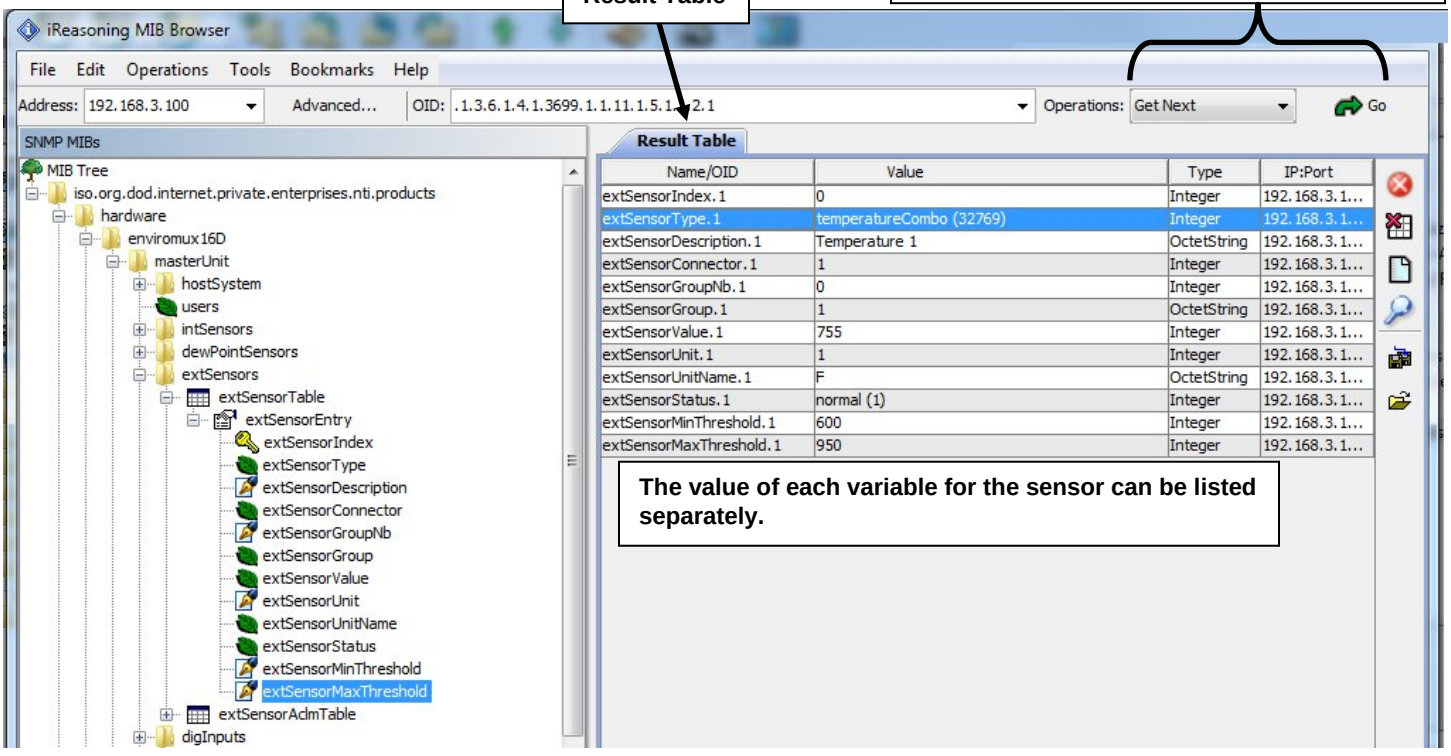
Get Subtree- will result in OIDs of that category and any sub-categories in the tree

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



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

Result Table



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

REST API SUPPORT

E-1W Firmware Version 2.8 (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.

REST API can be used to communicate with E-1W by any device including PLC. The PLC has to trigger the REST API to get sensor data.

API Request Details:

NOTE: API commands are case sensitive

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

Note: API Endpoint needs to use the http or https protocol as set in the E-1W 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://147.0.27.206/appAll.json"
```

API Response Details:

Response content type: 'application/json'

Response Sample Format:


```
{
  "data": {
    "all": [
      {
        "device": {
          "unit": "Server Rack E-1W",
          "model": "E-1W",
          "uptime": "0 hours, 33 mins, 16 sec",
          "firmware": "3.2"
        }
      },
      {
        "network": {
          "mac": "00:0c:82:17:00:01",
          "dhcp": 0,
          "addr": "147.0.27.206",
          "mask": "255.255.255.224",
          "gtw": "147.0.27.193",
          "dns1": "8.8.8.8",
          "dns2": "209.18.47.61"
        }
      },
      {
        "esens": [
          {
            "idx": 0,
            "desc": "Server Rack Temperature",
            "type": 1,
            "unit": 1,
            "val": "84.5 F"
          },
          {
            "idx": 1,
            "desc": "Server Room Temperature",
            "type": 1,
            "unit": 1,
            "val": "79.5 F"
```

```
      },
      {
        "idx": 2,
        "desc": "Server Room Humidity",
        "type": 2,
        "unit": 0,
        "val": "37.3 %"
      },
      {
        "idx": 3,
        "desc": "Server Room Dew Point",
        "type": 24,
        "unit": 1,
        "val": "51.2 F"
      },
      {
        "idx": 4,
        "desc": "Server Room Door",
        "type": 19,
        "unit": 0,
        "val": "Closed"
      },
      {
        "idx": 5,
        "desc": "Server Rack Door",
        "type": 19,
        "unit": 0,
        "val": "Closed"
      }
    ]
  },
  {
    "diginp": [
      {
        "idx": 0,
        "desc": "Server Room Smoke Detector",
        "type": 19,
        "val": "Open"
      },
      {
        "idx": 1,
        "desc": "Server Rack Water Sensor",
        "type": 19,
        "val": "Open"
      }
    ]
  },
  {
    "ipdev": [
      {
        "idx": 0,
        "desc": "DNS Server",
        "ip": "209.18.47.61",
        "val": "Responding",
        "retries": 3,
        "timeout": 5,
        "repeat": 600
      }
    ]
  },
  {
    "alerts": [
      {
        "idx": 0,
        "sensor": "Server Rack Temperature",
        "status": "0",
        "alertMsg": "",
        "alertStatus": "Normal",
        "val": "84.5 F",
        "sensorType": 1,
        "sensorClass": 1,
```

```
            "sensorId": 0
          },
          {
            "idx": 1,
            "sensor": "Server Room Temperature",
            "status": "0",
            "alertMsg": "",
            "alertStatus": "Normal",
            "val": "79.5 F",
            "sensorType": 1,
            "sensorClass": 1,
            "sensorId": 1
          },
          {
            "idx": 2,
            "sensor": "Server Room Temperature",
            "status": "0",
            "alertMsg": "",
            "alertStatus": "Normal",
            "val": "79.5 F",
            "sensorType": 2,
            "sensorClass": 1,
            "sensorId": 1
          },
          {
            "idx": 3,
            "sensor": "Server Rack Water Sensor",
            "status": "0",
            "alertMsg": "",
            "alertStatus": "Normal",
            "val": "Open",
            "sensorType": 825634359,
            "sensorClass": 2,
            "sensorId": 1
          },
          {
            "idx": 4,
            "sensor": "Server Room Smoke Detector",
            "status": "0",
            "alertMsg": "",
            "alertStatus": "Normal",
            "val": "Open",
            "sensorType": 0,
            "sensorClass": 2,
            "sensorId": 0
          }
        ]
      },
      {
        "smalerts": []
      }
    ]
  },
  "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
esens	External Sensor
diginp	Digital Inputs
ipdev	IP Devices
alerts	Alerts
smalerts	Smart Alerts
unit	Device name given by user
model	ENVIROMUX model type
mac	MAC address of Ethernet adapter in E-1W
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(smartalert)	Status string of the smart alert (Normal, Alarm, Acknowledged, Dismissed, Disconnected, Unknown)

Sensor Class ID's

Value	Description
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	E-ACLM-V	24	Dewpoint
7	E-ACLM-V of -P	25	Noise Level Sensor
8	E-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		

REST API Notes:

The idx value is determined by the order in which the sensors are detected by the software. It has nothing to do with a sensor's physical location.

The unit value refer to measurement unit, so 0 = Celsius, 1 = Fahrenheit. Therefore, this will only vary with Temperature sensors and Dewpoint sensors.

Newly added sensors will always be numbered at the end of the chain, regardless of where in the physical chain they have been placed.

CERTIFICATE CONVERSION TO DER FORMAT

The following procedure can be performed using a computer with Windows or Linux operating system, provided OpenSSL has been loaded and properly setup.

First, to Generate CA Certificate, Device key and certificate refer to https://www.networktechinc.com/pdf/sman154-04.pdf from pages 1 to 5 section I or section II. Once you get the required certificate files in PEM format, the following commands are to be entered at the command prompt for conversion.

To Convert Device or CA Certificate in PEM format to DER

openssl x509 –in <your_device_fqdn_or_ipaddress>.pem –inform PEM –out <your_device_fqdn_or_ipaddress>.der –outform DER

Example: # openssl x509 –in 192_168_1_24.pem –inform PEM –out 192_168_1_24.der –outform DER

To Convert Key in PEM format to DER

openssl rsa –in <your_device_fqdn_or_ipaddress>.key –inform PEM –out <your_device_fqdn_or_ipaddress>.der –outform DER

Example: # openssl rsa –in 192_168_1_24.key –inform PEM –out 192_168_1_24.der –outform DER

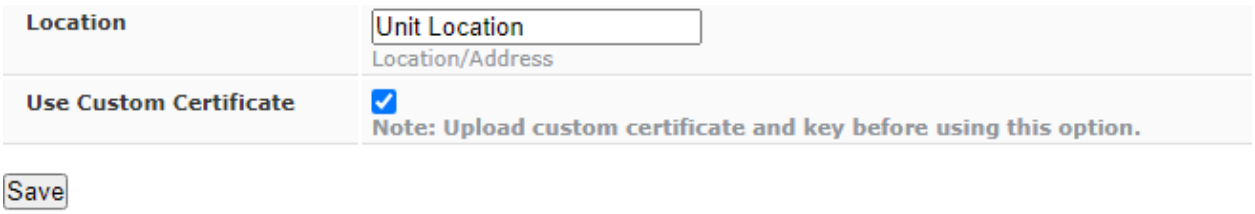
Uploading CA certificate, device certificate and device key to E-1W

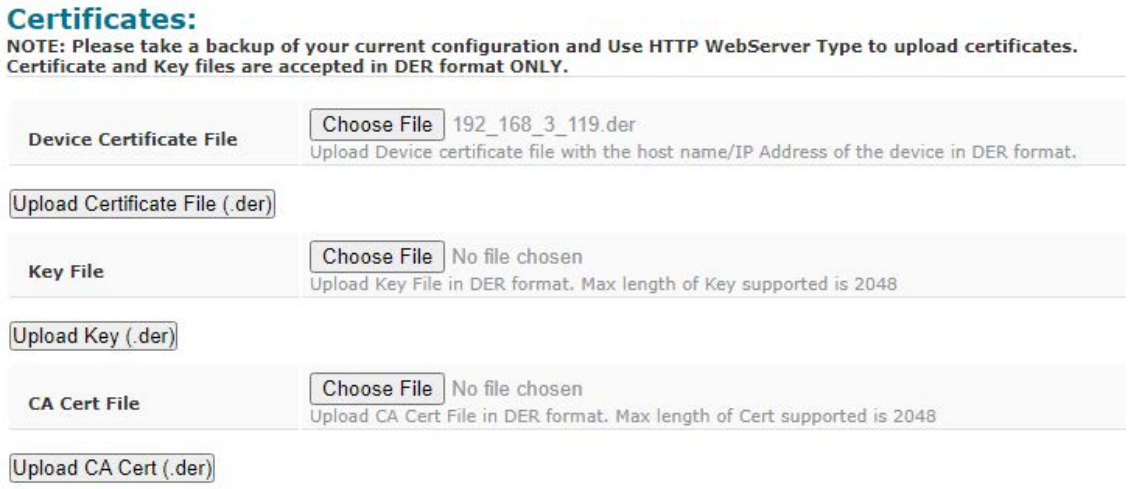
Device certificate can be added to the **E-1W(P)** along with device key. If applicable, you can also upload CA certificate as shown in the steps below.

To upload custom CA, device certificates and key, Go to System page (page 27) in the Web Interface.

At this point save a backup configuration of your device. In the event the certificates are uploaded incorrectly and you cannot access the device, you can restore the configuration to default and reload the saved configuration file. Please note that the E-1W(P) works only in HTTPS mode or HTTP mode, but not both.

Select the checkbox “**Use Custom Certificate**” and click “Save”.





To upload a valid Device Certificate, click on “Choose File” next to “Device Certificate File” and select the appropriate `.der` file, (created in the previous steps). Next click “Upload Certificate File (.der)”.

Follow the same steps to upload a valid Device Key , and upload it by hitting “Upload Key (.der)”.

Uploading a CA Certificate is optional (if your device certificate was signed by CA). If you wish to upload a CA Certificate, upload the .der file of the CA certificate and click “Upload CA Cert (.der)” button.

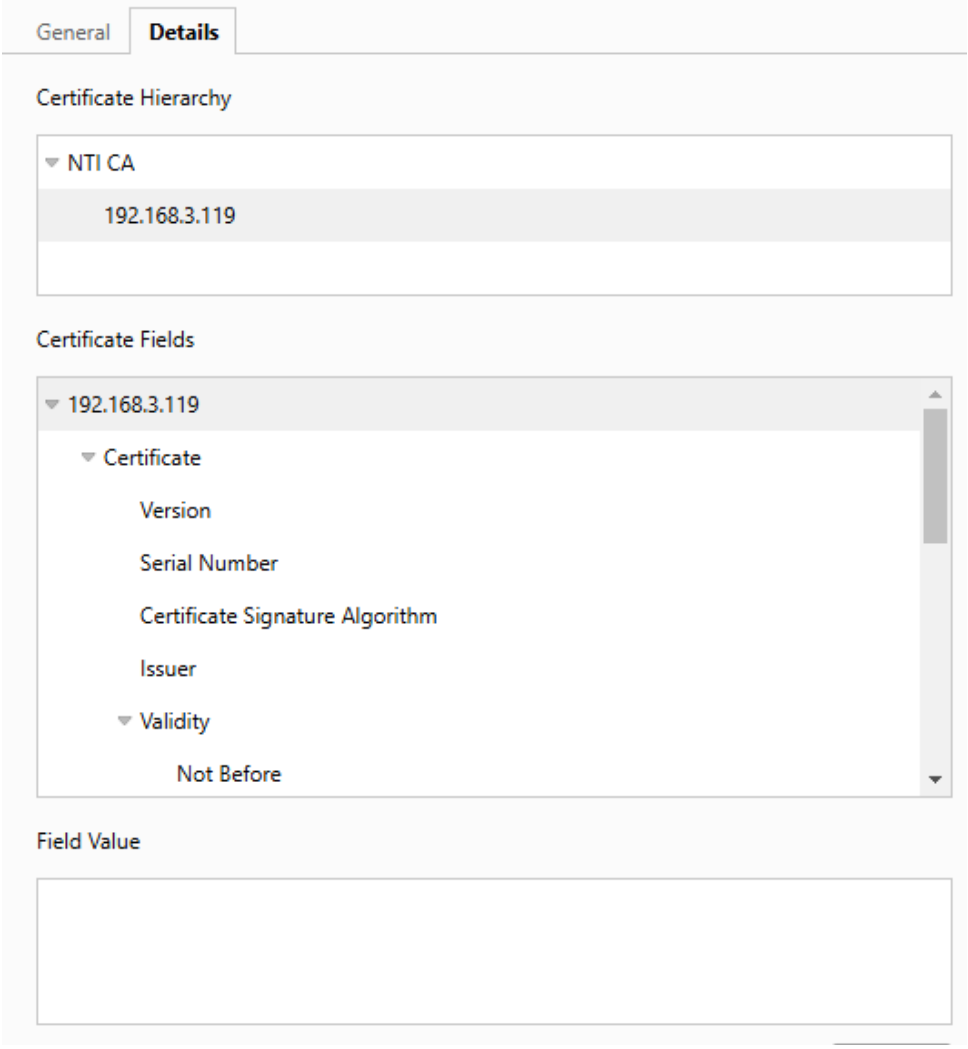
Files can be uploaded in HTTP mode only. If changing from default to or from Custom certificate when the device is already set to HTTPS mode, reboot the device for new certificates to take effect.

If you do not want to use custom certificates in the future, uncheck the “Use Custom Certificate” checkbox, and click “Save”.

TESTING PROCEDURE:

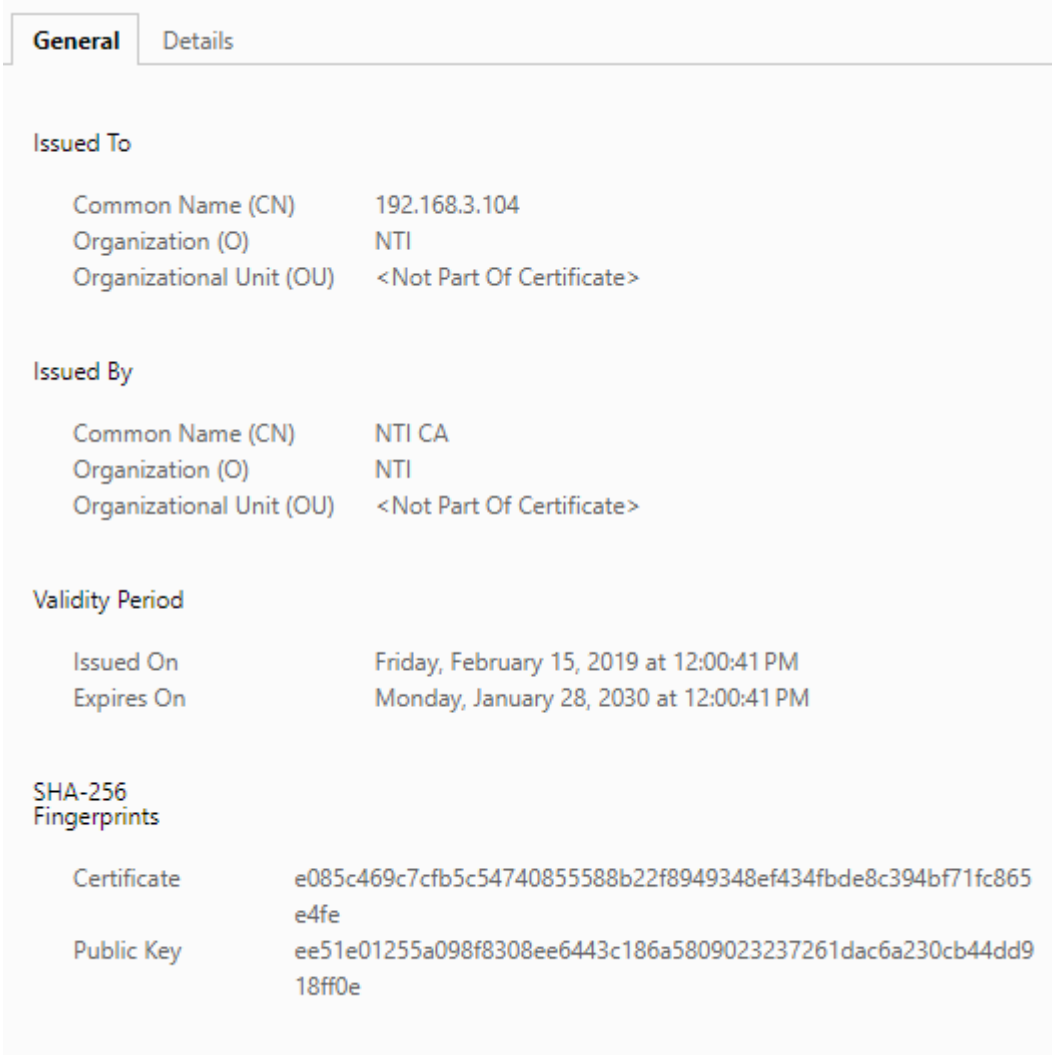
TEST 1: Testing Custom Certificates

1. Refer https://www.networktechinc.com/pdf/sman154-04.pdf documentation, from page 9 till 13 to generate CA Certificate, Device certificate and key.
2. Use the documentation above, to convert the PEM formatted certificates and key to DER format with correct extension.
3. Upload the Certificates and key as mentioned above and set to use custom certificate
4. From Administration > Network, change Web Server Type to HTTPS.
5. Reload your webpage and make sure to update the url to start with **"https:// "**
6. If correctly uploaded, you might get a "SECURE" or "Not Secure" Icon beside the url, depending on if the certificates and keys are verifiable. They are probably not verifiable in this scenario.
7. Click on the "Secure" or "Not Secure" > Certificate Details, and you should get the details of certificates, used.
8. If a CA Certificate is used, a hierarchy can be observed under the Details tab (below).



TEST 2: Test Default Certificate.

1. Go to Administration > System
2. Uncheck the box “Use Custom Certificate”, and save the settings.
3. From Administration > Network, change Web Server Type to HTTPS.
4. Reload your webpage and make sure to update the url to start with “https://”
5. Default certificate under “SECURE” or “NOT SECURE” on web browser, is issued by NTI CA. and will have details the same as in the image below.
6. Default device key and certificate do not have a CA cert and therefore no hierarchy will be shown under hierarchy in Details tab.



E-1W Email Error Codes

Below is list of email error codes specific to the E-1W (version 3.0 and later). Like the HTTPS connections on the E-1W, the email connections have a limitation of how many emails can be sent in parallel. We cannot be specific at 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: E-Micro keeps retrying old failed emails for a few hours and new email deliveries will be blocked until they clear. To quickly clear the pending emails in queue, please reboot your device.
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

More on -9 error: When setting up Email Server Settings, if there is an issue with settings and any email is undeliverable, the ENVIROMUX will continue retrying the failed email with delay of few hours, even after you have entered the correct settings. To clear the pending emails and start fresh, reboot the device.

MODBUS TCP/IP SUPPORT

The ENVIROMUX is equipped with Modbus TCP/IP support to enable PLC or any software-based controller to read the value/state of some of the sensors. Using the Modbus communication protocol devices can be programmed over TCP/IP to treat the ENVIROMUX as a Modbus slave device reacting to readings from available sensors as needed.

Note: Modbus communication protocol is supported provided only one client is active at a time.

Modbus TCP Function Codes Definition

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

Grayed-out codes are not applicable to this device.

Function Code 02 - Read the state of Digital Inputs

Description:

Function code 02 is used to read the status of Digital Inputs (Open/Closed) of the E-1W slave device in a binary data format (firmware version 3.3 or later).

Query:

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

Response:

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

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

Note: This is for the on-board Digital Inputs only (does not apply to Digital Inputs connected to E-DI2-1W).

Mapping:

Input # (Address)	E-1W
0	Digital Input #1
1	Digital Input #2

Function Code 04 - Read External Sensors and Digital Input values and status

Description:

Starting with firmware version 3.2 Function code 04 can be used to read the values of External Sensors and Digital Input sensors. Modbus Function code 04 to read input registers assigns 1 address register for each of 16 bit value. All responses here use 2 such 16 bit registers as a either a 32 bit signed integer or 32 bit float value. There are a total of 48 addresses for external sensors and 4 addresses for the on-board digital inputs.

Query:

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

Response:

The Modbus protocol has a single byte count which represents the number of bytes (2 bytes per 16 bit register).

Floating Point Format

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

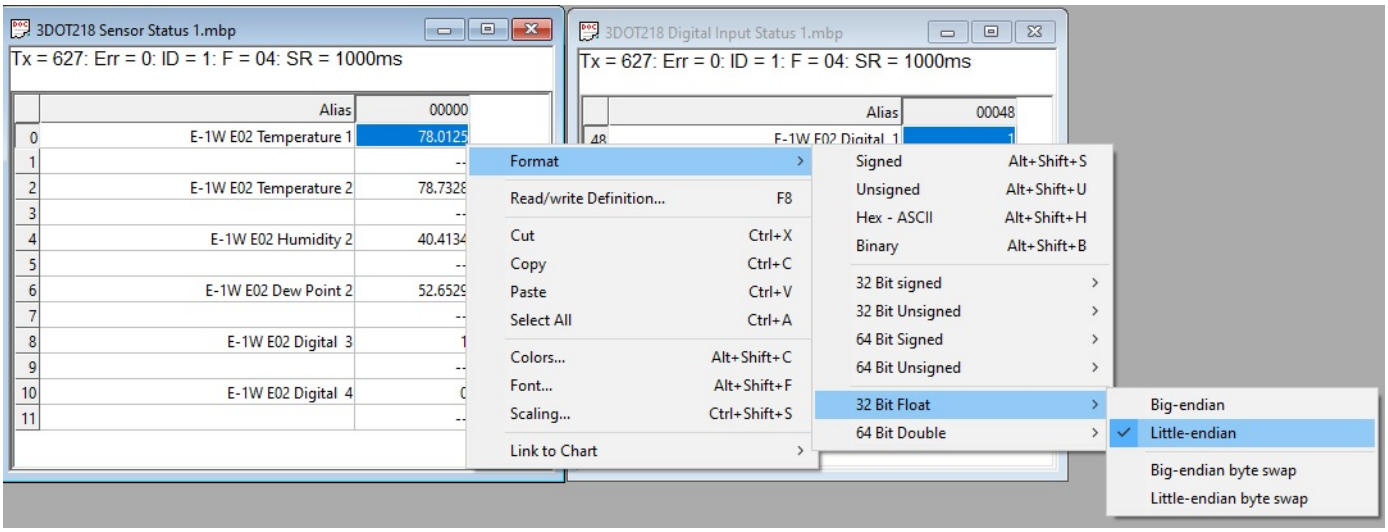
Starting with firmware version 3.2 input register mapping supports reading of external sensors and digital inputs.

If external sensors are of a contact type (i.e. E-DI2-1W), a value of "0" will represent a closed contact and a value of "1" will represent an open contact.

Sensor Mapping in the response is as follows:

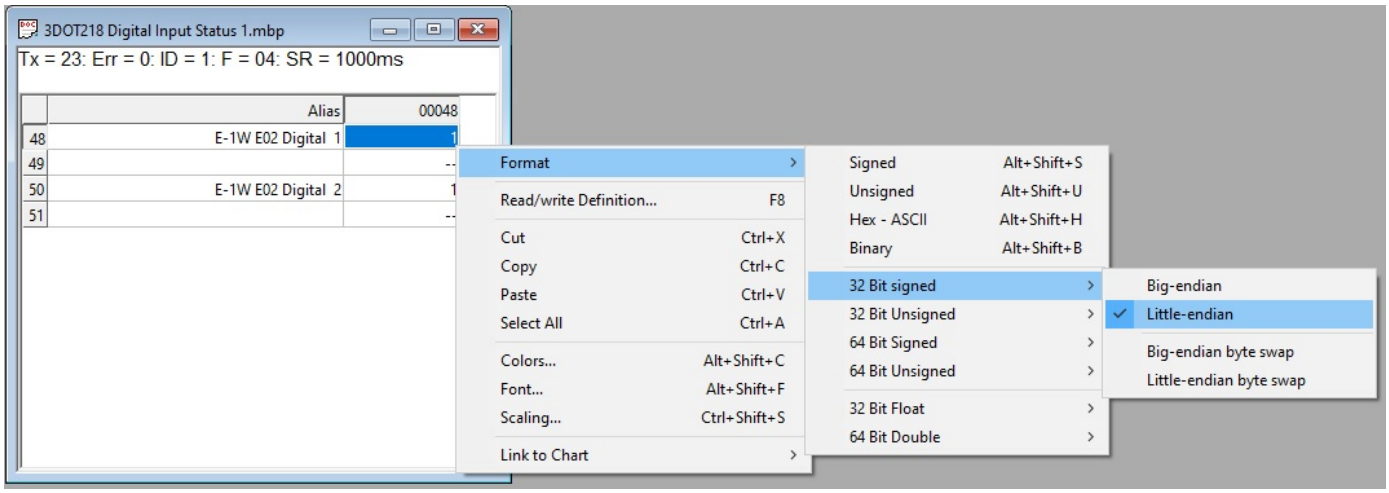
1. RJ45 Sensor values in 2X16bit registers each as 32bit float little endian mode are reserved for each E-1W.
   Sensors will be listed in order of appearance. Sensor(s) connected to 1W Sensor Device 1 first, followed by the 1W Sensor Device 2.

Note: E-1W sensors are listed in the order they are discovered, not by their physical position on the cable.

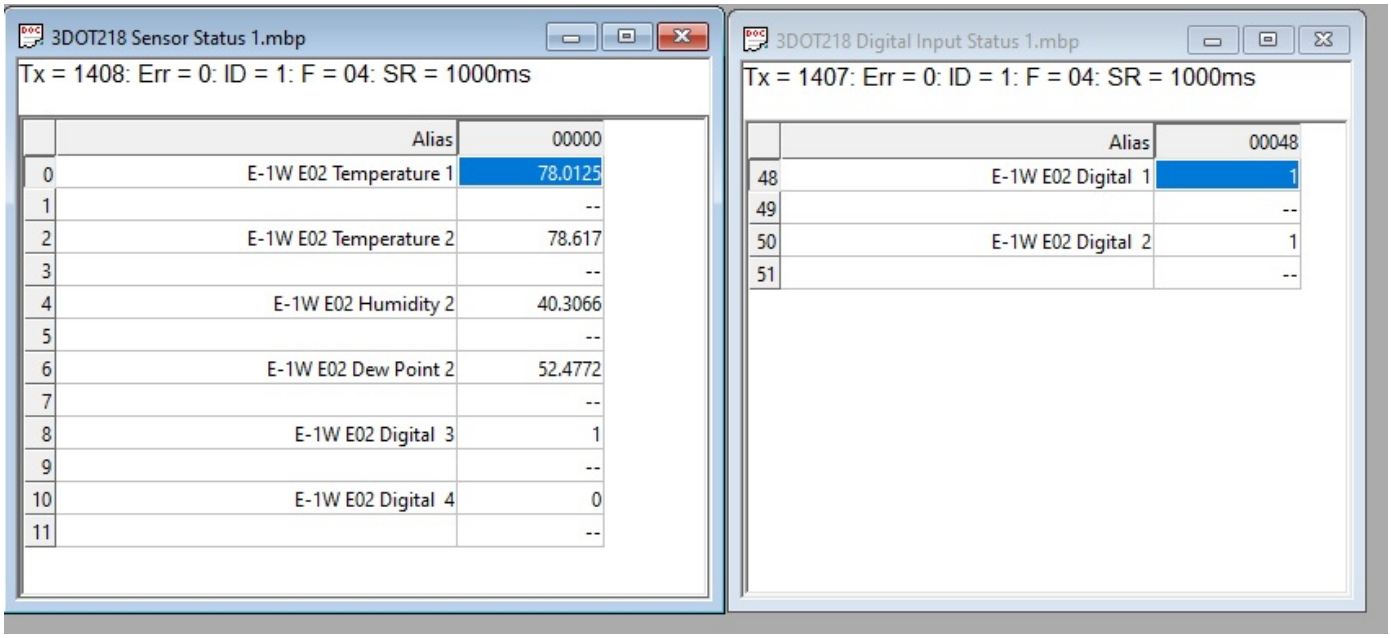


Note: E-DI2-1W digital inputs are treated the same as on-board digital inputs. 32-bit signed integer little endian format.

Digital Input status will be reported starting with register 48. These will be 32bit signed registers in little endian mode format. A value of "0" will indicate contact closure, and a value of "1" will indicate contact open.



A screenshot of the values displayed when polling input registers is shown here. All values shown in second column are displayed in 32 bit float little endian format. The integer numbers on the left of each row are the 16 bit register addresses. The 'Alias' column is shown for users reference



TECHNICAL SPECIFICATIONS

Ports	
Sensor Inputs	Two female RJ11 6P4C connectors for connecting 1-wire sensors
Max. Sensor Cable Length	Temperature Sensors- 7 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. * Potential-free. * Output voltage: +5 V DC * Current limited to 10 mA * Maximum contact resistance: 10K Ohm
Ethernet Port	One female RJ45 connector with LEDs. 10 BaseT Ethernet interface.
USB OTG Port **Reserved for future use**	Female Micro USB Type B connector Supports USB 2.0 Full Speed
Environmental	
Operating/Storage temperature	-4°F to 167°F (-20°C to 75°C)
Operating and Storage Relative Humidity	5 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
Operating System (E-1W)	Bare Metal Software using Microchip Harmony
PoE Support	IEEE 802.3af and 802.3at standards
Power consumption	5 Watts (Maximum)
Power Supply	120VAC or 240VAC at 50 or 60Hz-5.5VDC/1.5A AC Adapter
Dimensions WxDxH (in.)	4x3.65x1.37
Approvals	CE, RoHS

E-TH1W-7 Temperature/Humidity Sensor

- Temperature Accuracy:
  - ±0.72ºF (±0.4°C) from 14 to 185ºF (-10 to 80ºC)
  - ±0.90ºF (±0.5ºC) from -4 to 14º (-20 to -10ºC)
- Humidity Accuracy:
  - ±3% from 0 to 80% Relative Humidity
  - ±4% from 80 to 90% Relative Humidity
- Temperature range: -40°C to 85°C
- Dimensions: 2.125 X 2.5 X 1.0 in.

E-T1W-1M Temperature Sensor

- Temperature Range: -40ºC to 85ºC (-40ºF to 185ºF)
- Accuracy: ±0.5ºC(±0.9º F) from -10ºC to 85ºC (14ºF to 185ºF)
- Probe Size: 6mm Dia. X 30mm (0.24in Dia. X 1.18in)
- Connections to Sensor : 1 meter long 4 conductor signal cable with a RJ11/6P4C connector
- Ingress Protection Rating: IP67

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 14)
Cannot get Discovery Tool to work	Java not installed	Java Runtime Environment must be installed before the Discovery Tool can be used (page 14)
Not receiving alert messages	using email that doesn't support SSL encryption (like Gmail) or no-authentication	• If security is required, make sure email server supports SSLv3 Authentication Protocol. • If only using standard authentication (just requires username and password), make sure the username and passwords are entered correctly and that "SSL Required" is unchecked (see pages 28 or 46) • Make sure the port number entered is correct (check with the system administrator)
Cannot connect via Telnet	• Ethernet cable not connected • wrong IP address • wrong port number • telnet not supported via operating system	• check Ethernet cable connection • Use Discovery Tool to locate IP address (page 14) • Configure terminal to use port 23 • Use a terminal program instead of the command line
Cannot login	cannot remember root password	Either restore default settings (page 55) or contact NTI for assistance

INDEX

WARRANTY INFORMATION

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

MAN253 Rev. 5/13/25