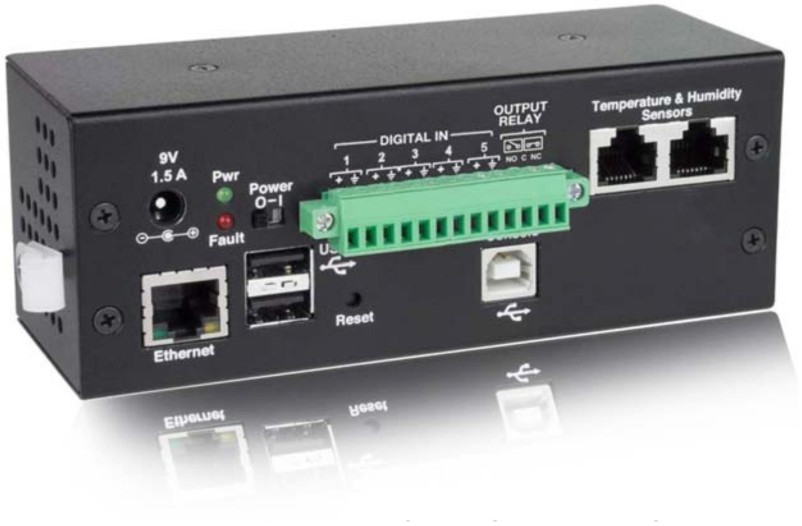
EMS200

Outdoor Electrical Enclosures Environment Monitoring systems

Installation and Operation Manual



Front View of EMS200

i-Tech Company LLC
TOLL FREE: (888) 483-2418
email: info@itechlcd.com
web: www.iTechLCD.com

TABLE OF CONTENTS

TABLE OF FIGURES

INTRODUCTION

The EMS200 (EMS200) are Server Environment Monitoring Systems designed to monitor, from a remote location, the critical environmental conditions in cabinets and rooms containing servers, hubs, switches and other network components. Remote monitoring is provided via a 10/100BaseT Ethernet web interface, secure web interface, SSH, or Telnet. The input data is filtered, collected, analyzed and processed to allow the user to configure it to meet individual requirements. The user is able to specify parameters for all monitored signals. When a sensor exceeds the configured threshold, the unit will signal an alert. Alert methods include email, SMS, SNMP traps (MIBs), web-page alerts, and a visual indicator (red LED).

The EMS200 will monitor temperature, humidity, and detect the presence of water on a flat surface (such as the floor). The unit also has four sets of terminal block pairs for the connection of contact-closure sensors.

Features and Applications

> Monitor and manage server room environmental conditions over IP.
> Monitors and operates at temperatures from 32°F to 122°F (0ºC and 50ºC) and 20% to 90% relative humidity.
  > Optional Industrial version (EMS200-**IND**) operates at 32 to 167°F (0 to 75°C).
> Sensors supported:
- 2 temperature/humidity sensors
- 5 digital input devices

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

Options:

> The EMS200 can be ordered with a DIN rail mounting bracket- Add “D” to the part number (i.e. EMS200-**D**)
> The EMS200 can be ordered with battery backup support and DC power monitoring installed, providing up to 2.3 hours of operation in the event of a power failure- to order, add “B” to the part number (i.e. EMS200**B**)
> The EMS200 can be ordered with a higher operating temperature range (32 to 167°F (0 to 75°C))- to order add “-IND” to the part number (i.e. . EMS200-**IND**)

SUPPORTED WEB BROWSERS

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

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

MATERIALS

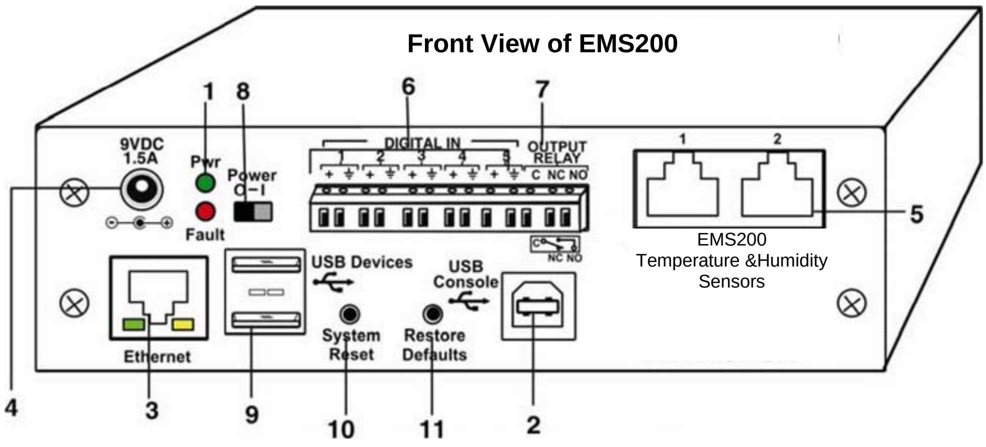
Materials supplied with this kit:

- NTI EMS200 Mini Server Environment Monitoring System
- 1- 120VAC or 240VAC at 50 or 60Hz-9VDC/1.5A AC Adapter (PS4074)
- 1- Line cord- country specific
- 1- USB2-AB-2M-5T 2 meter USB 2.0 male type A-male type-B transparent cable (CB4306)
- CD containing a pdf of this manual, a SNMP MIB file, and the NTI Discovery Tool

Additional materials may need to be ordered;

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

CONNECTORS AND LEDS



#	LABEL	CONNECTOR/LED	DESCRIPTION
1	**Pwr**	Green LED	green — indicates device is powered
	Fault	Red LED	red — illuminates if a sensor goes out of range of a configurable threshold
2	**USB Console**	USB Type B female connector	For connection of terminal for control through Text Menu
3	**Ethernet**	RJ45 female connector	for connection to an Ethernet for remote multi-user control and monitoring • Yellow LED- indicates 100Base-T activity when illuminated, 10Base-T activity when dark • Green LED – illuminated when Ethernet link is present, strobing indicates activity on the Ethernet port
4	**9V 1.5A**	2.1x5.5mm Power Jack	for connection of power supply
5	**Temperature & Humidity Sensors**	RJ45 female connectors	for connection of optional EMS200-T, EMS200-RH, or EMS200-TRH sensors (The left port is "#1", the right port is "#2" as listed in the Summary Page on Page 19.)
6	**DIGITAL IN**	Wire terminal block	For connecting dry-contact and liquid detection sensors
7	**OUTPUT RELAY**	Wire terminal block	For control of external devices (contacts rated up to 1A, 30VDC or 0.5A, 125VAC)
8	**Power**	Slide switch	For powering the EMS200 On (I) and Off (O)
9	**USB Devices**	USB Type A female connectors	For connecting USB Flashdrive and USB Modem
10	**System Reset**	Push button	For manually rebooting the EMS200 without power-cycling- a momentary press will activate
11	**Restore Defaults**	Push button	For manually restoring the EMS200 to factory default settings-press and hold for 5 seconds to activate

INSTALLATION

Connect Sensors

Connect the desired sensors (sold separately) to the available ports on the EMS200. Plug the RJ45 connectors to either of the two RJ45 ports marked "TEMPERATURE/HUMIDITY". Mount the sensors according to their individual operating characteristics. Power-cycle the EMS200 after sensors have been plugged-in.

Note: The maximum CAT5 cable length for attachment of temperature and humidity sensors in the EMS200 is 25 feet.

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

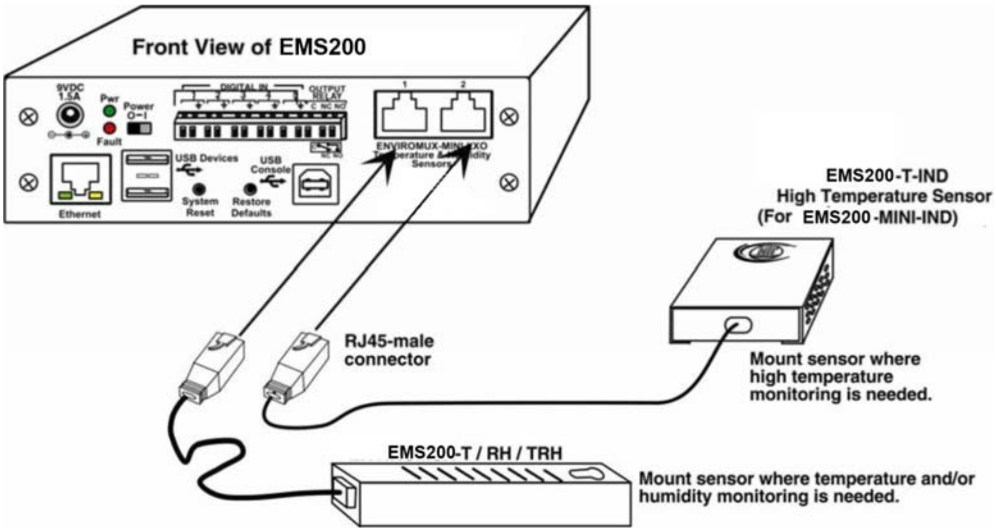


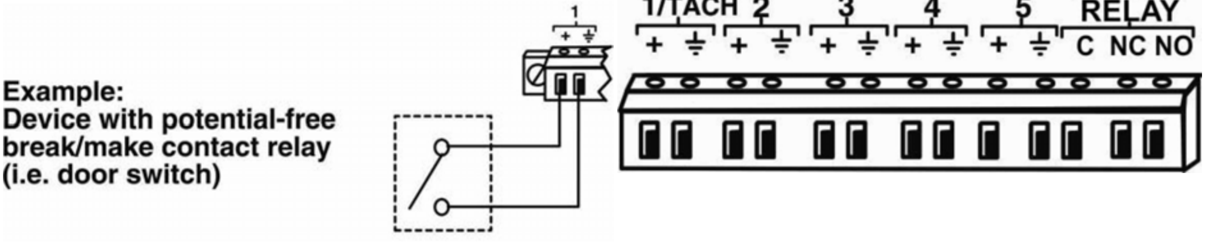
Figure 1- Connect Sensors

Up to five dry-contact sensors can also be connected. Sensors with 16-26 AWG connection wires, that operate on 5V at 10mA maximum current may be used. A contact resistance of 10kQ or less will be interpreted by the EMS200 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 EMS200 and the ground lead to the next terminal to the right that will correspond to a — marking on the EMS200. Tighten the set screw above each contact. Terminal sets are numbered 1-5.

B. Mount the sensors as desired.



Example:
Device with potential-free break/make contact relay (i.e. door switch)
1
+ ⏚
DIGITAL IN
1/TACH
2
3
4
5
OUTPUT RELAY
+ ⏚ + ⏚ + ⏚ + ⏚ + ⏚
C NC NO

Figure 2- Terminal block for dry-contact sensors ***Note: The terminal block is removable for easy sensor wire attachment if needed.***

Optionally, connect the two-wire cable from a liquid detection sensor (EMS200-LD shown below- sold separately) to a set of “DIGITAL IN” contacts.

The twisted orange sensing cable should be placed flat on the surface (usually the floor) where liquid detection is desired. If tape is required to hold the sensor in place, be sure to only apply tape to the ends, exposing as much of the sensor as possible. At least 5/8" of the sensor must be exposed for it to function. (See Figure 3)

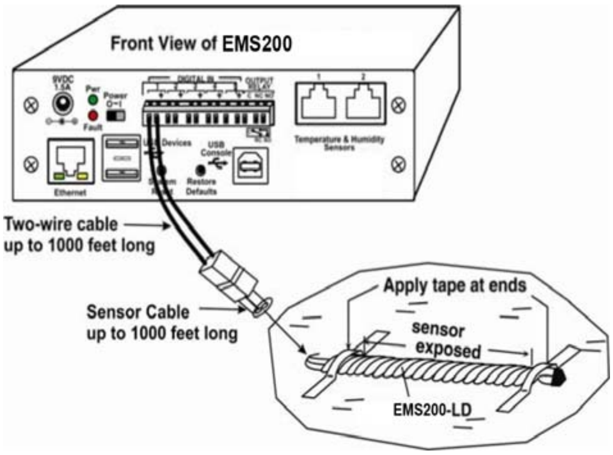
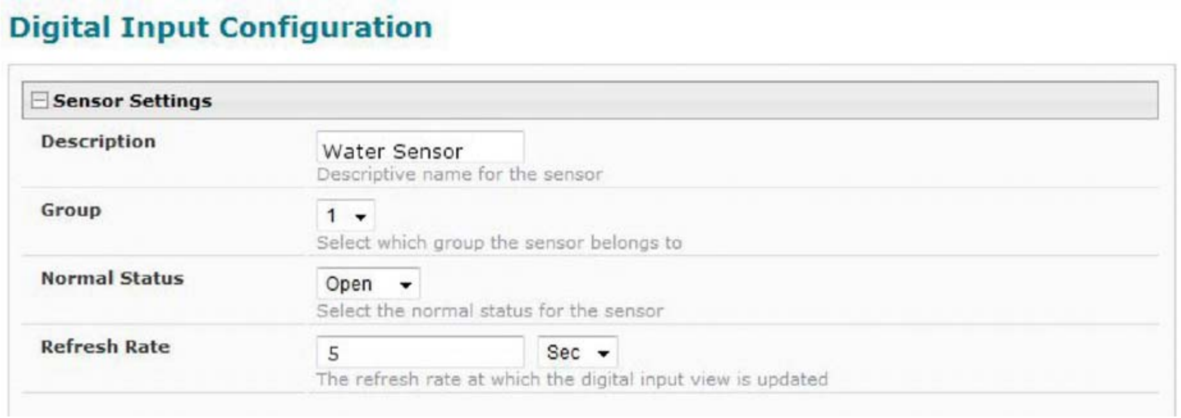


Figure 3- Secure liquid detection sensor with tape

To test the EMS200-LD;

1. Configure the sensor (page 26). (Normal Status set to “Open”, Refresh Rate set to 5 seconds.)
2. Submerge at least ½ inch of the exposed twisted orange wire (not the wrapped end) for up to 30 seconds. Do NOT use distilled water as water must be conductive.
3. Monitor the sensor (page 20) to see the sensor “Value” change from “Open” (dry) to “Closed” (wet).
4. Dry the exposed area of sensor and the sensor “Value” should change back to “Open” within 30 seconds.



Digital Input Configuration

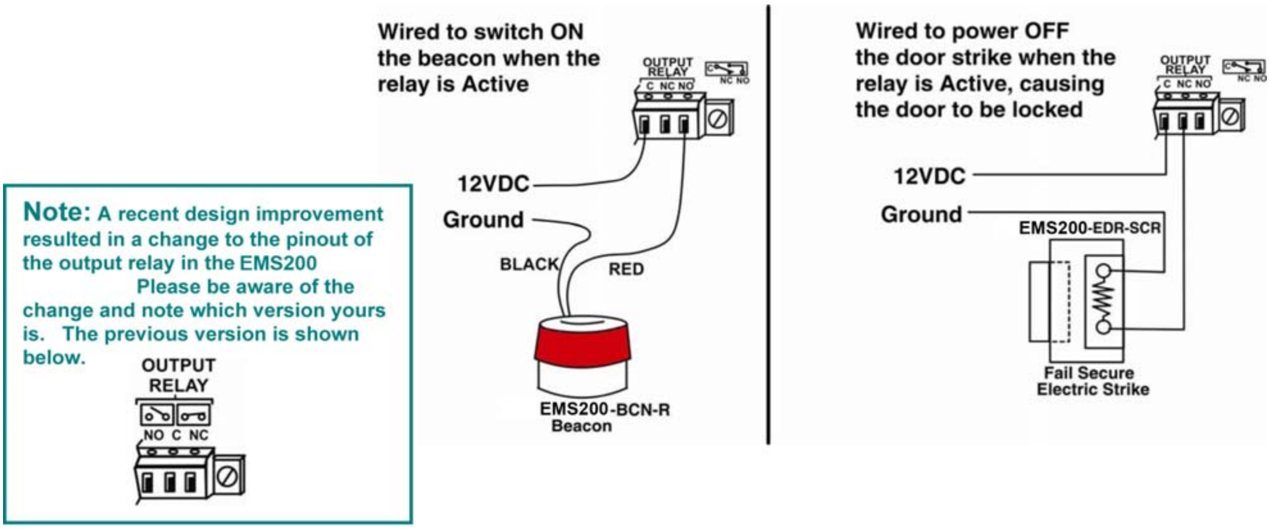
⊟ Sensor Settings

Description	Water Sensor Descriptive name for the sensor
Group	1 Select which group the sensor belongs to
Normal Status	Open Select the normal status for the sensor
Refresh Rate	5 Sec The refresh rate at which the digital input view is updated

Figure 4- Portion of Water Sensor configuration page

Output Relay

An output relay is provided to control an external device with a rating of up to 1A, 30VDC or 0.5A, 125VAC. Three terminals are provided to enable a normally-open connection (using the N.O. and C terminals) or a normally-closed connection (using the N.C. and C terminals). Using the web interface, this relay can be set to change state (close the normally-open connection, or open the normally-closed connection) either manually (page 29) or as a result of an alert state from one or more of the connected sensors (page 22). The terminals for these connections will accept 16-26AWG wire.



Note: A recent design improvement resulted in a change to the pinout of the output relay in the EMS200 Please be aware of the change and note which version yours is. The previous version is shown below.

Figure 5- Output Relay Application Examples

Ethernet Connection

Connect a CAT5 patch cable (RJ45 connectors on each end wired pin 1 to pin 1, pin 2 to pin 2 etc) from the local Ethernet network connection to the connector on the EMS200 marked "Ethernet".

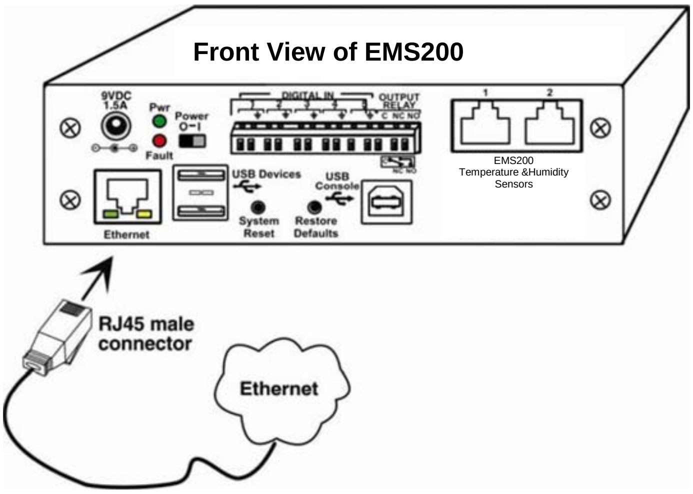


Figure 6- Connect EMS200 to the Ethernet

Note: A direct Ethernet connection can be made with a PC using a crossover cable. For the pinout of this cable, see page 102.

USB Console Port

Your EMS200 includes a USB Type B connector labeled "USB Console". If you connect a USB cable between the EMS200 and your PC you will be able to control your EMS200 serially from a terminal console using this connection.

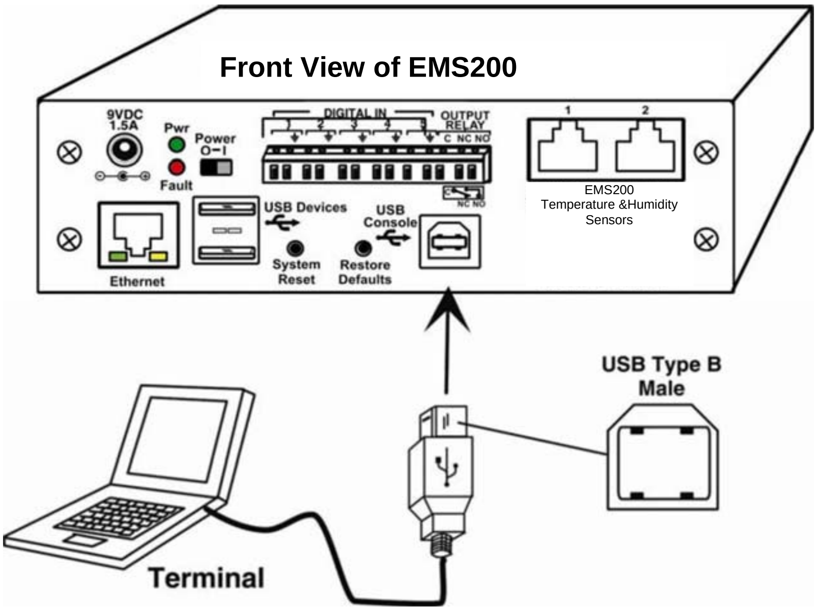


Figure 7- Connect terminal to USB Console port

Installing Drivers

You will only need to install drivers the first time the EMS200 is connected to your PC. After the first time, when the EMS200 is connected, your PC should recognize the EMS200 and re-assign the COM port. Follow the steps below to install the drivers.

1. Make sure the USB cable is connected between the EMS200 and your PC.

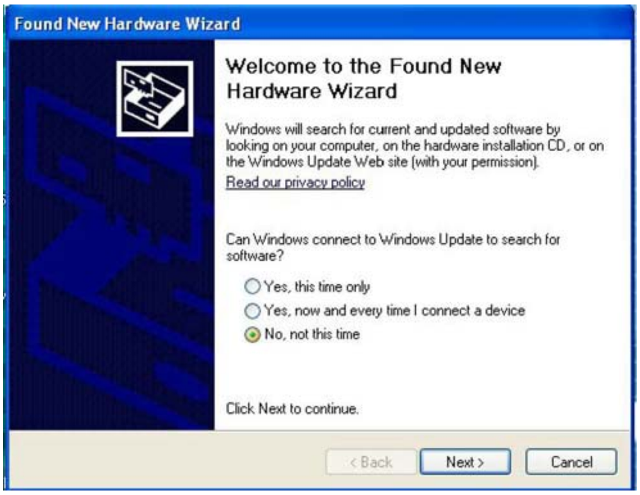
2. Power ON the EMS200. The PC will see the EMS200 as "New Hardware" and create a virtual COM port to communicate with it.

3. You will be prompted to load drivers. A driver file compatible with Windows XP, 2000, Vista and 7 (32 and 64 bit versions) can be found on the CD that came with your EMS200. Browse to the drive your Product Manual CD is in and locate and select the file named "**`EMS200.inf"`** in a directory named **`"windows-drivers\32bit or \64bit"`** depending upon your operating system.

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

Windows XP-32 bit Installation

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



Welcome to the Found New Hardware Wizard

Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).

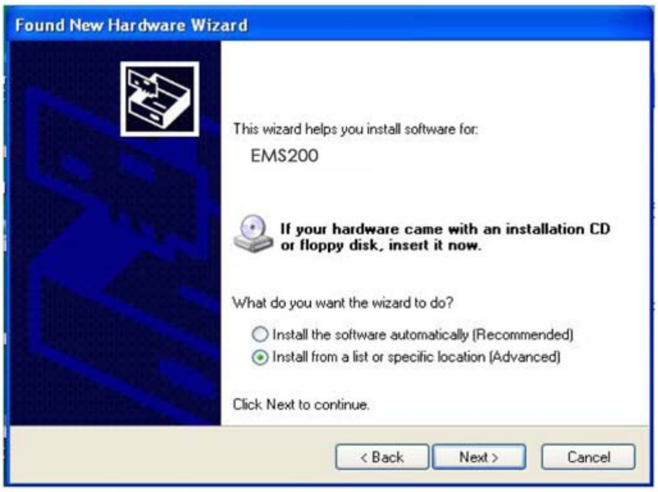
Read our privacy policy

Can Windows connect to Windows Update to search for software?

○ Yes, this time only
○ Yes, now and every time I connect a device
● No, not this time

Click Next to continue.

A. Windows will want to check the internet for drivers. Choose “**No, not this time**” because the drivers are unique to the EMS200.



This wizard helps you install software for:

EMS200

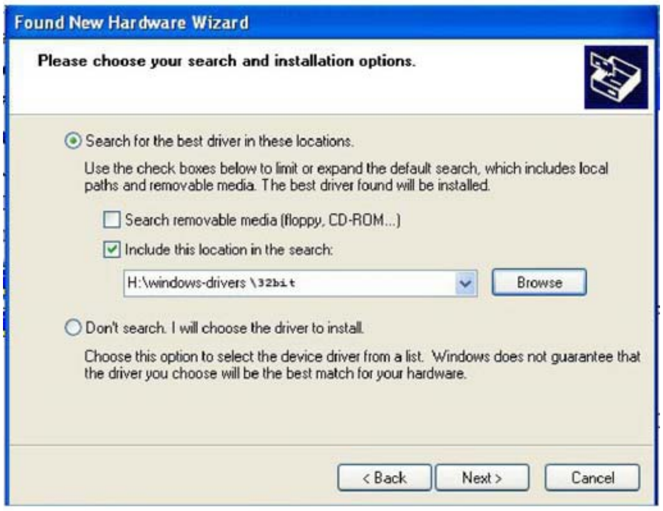
If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

○ Install the software automatically (Recommended)
● Install from a list or specific location (Advanced)

Click Next to continue.

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



Found New Hardware Wizard

Please choose your search and installation options.

● Search for the best driver in these locations.

Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.

□ Search removable media (floppy, CD-ROM...)

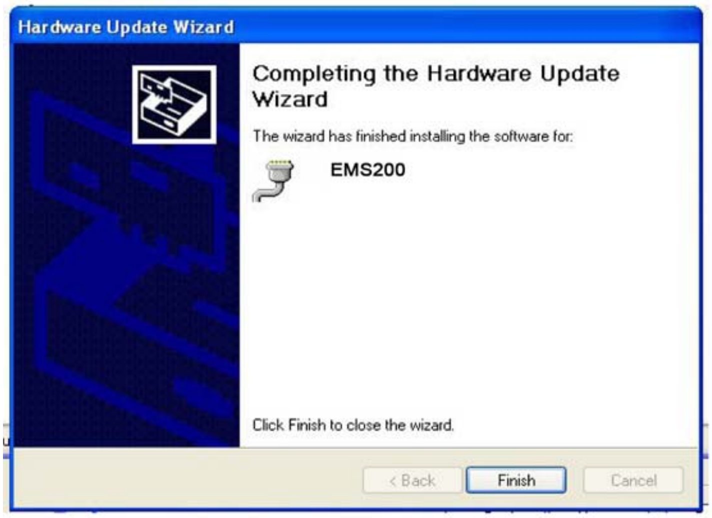
☑ Include this location in the search:

H:\windows-drivers \32bit

○ Don't search. I will choose the driver to install.

Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.

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



Hardware Update Wizard

Completing the Hardware Update Wizard

The wizard has finished installing the software for:

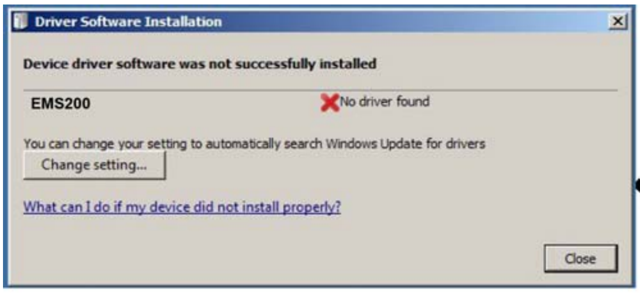
EMS200

Click Finish to close the wizard.

D. Once the driver is installed, you will get this screen and the EMS200 USB Console Port will be ready to use.

Windows 7-64 bit Installation

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



Driver Software Installation

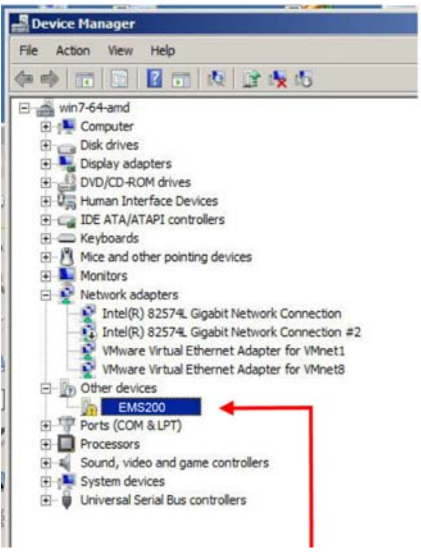
Device driver software was not successfully installed

EMS200 ✗No driver found

You can change your setting to automatically search Windows Update for drivers

What can I do if my device did not install properly?

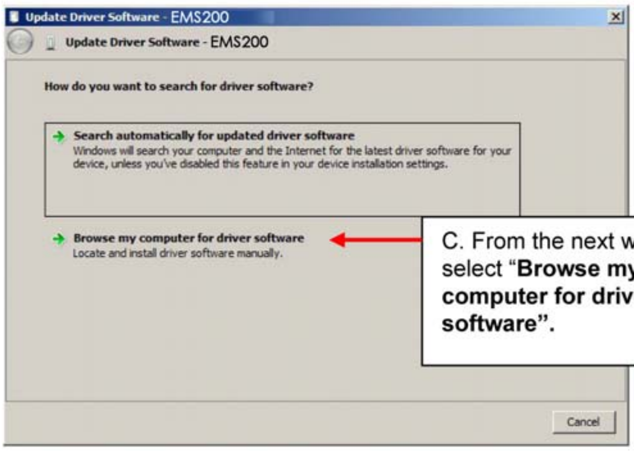
A. Upon EMS200 power ON, the driver cannot be found. Press “**Close**”.



- win7-64-amd
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
    - Intel(R) 82574L Gigabit Network Connection
    - Intel(R) 82574L Gigabit Network Connection #2
    - VMware Virtual Ethernet Adapter for VMnet1
    - VMware Virtual Ethernet Adapter for VMnet8
  - Other devices
    - EMS200
  - Ports (COM & LPT)
  - Processors
  - Sound, video and game controllers
  - System devices
  - Universal Serial Bus controllers

B. Open the Device Manger and select the EMS200 in the device list. Right-click and open “Properties”. Select “Update Driver Software”.

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



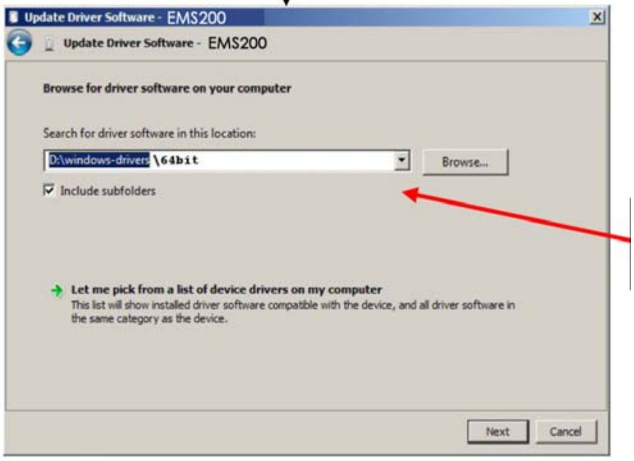
Update Driver Software - EMS200

How do you want to search for driver software?

→ **Search automatically for updated driver software**
Windows will search your computer and the Internet for the latest driver software for your device, unless you've disabled this feature in your device installation settings.

→ **Browse my computer for driver software**
Locate and install driver software manually.

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



Update Driver Software - EMS200

Browse for driver software on your computer

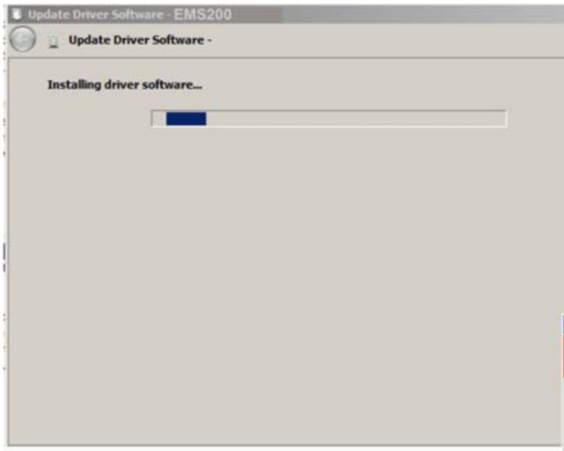
Search for driver software in this location:

D:\windows-drivers\64bit

☑ Include subfolders

→ **Let me pick from a list of device drivers on my computer**
This list will show installed driver software compatible with the device, and all driver software in the same category as the device.

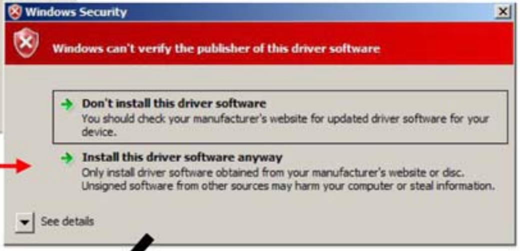
D. In the next window, enter the path to the .inf driver file (on the Product Manual CD). Press “Next”.



Update Driver Software - EMS200

Update Driver Software -

Installing driver software...



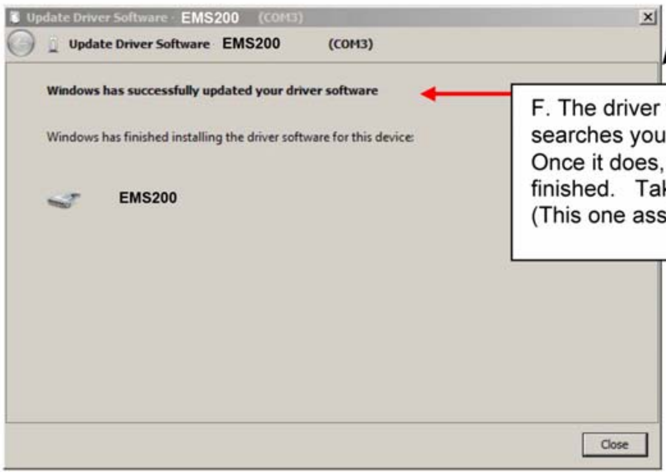
Windows Security

Windows can't verify the publisher of this driver software

→ **Don't install this driver software**
You should check your manufacturer's website for updated driver software for your device.

→ **Install this driver software anyway**
Only install driver software obtained from your manufacturer's website or disc. Unsigned software from other sources may harm your computer or steal information.

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



Update Driver Software - EMS200 (COM3)

Update Driver Software EMS200 (COM3)

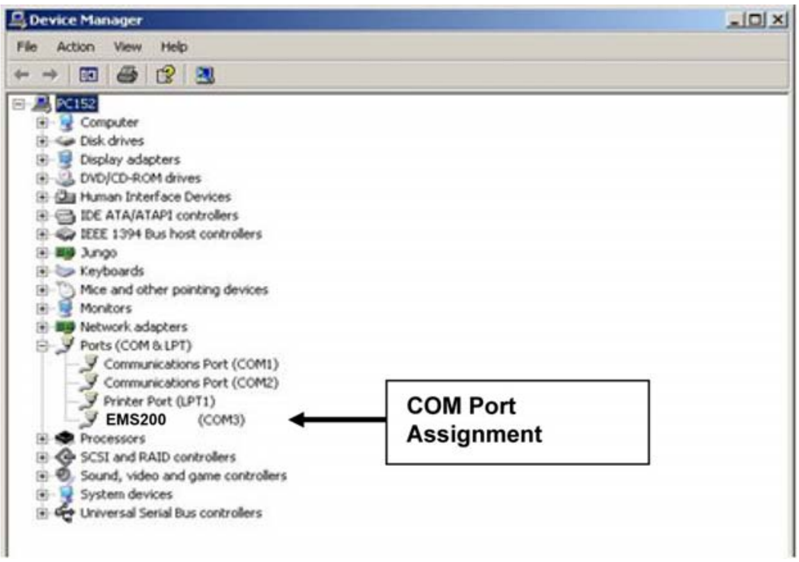
Windows has successfully updated your driver software

Windows has finished installing the driver software for this device:

EMS200

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

4. During the installation, your PC will assign a COM port number to the USB port attached to the EMS200. You will need to identify the COM port number assigned. This information can be viewed in your Device Manager list (below) if you didn’t take note of it during installation.



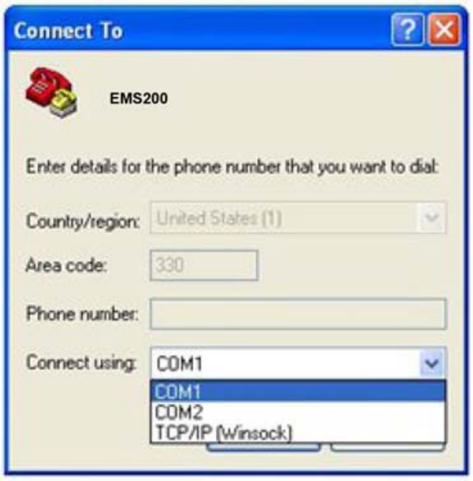
PC152
- Computer
- Disk drives
- Display adapters
- DVD/CD-ROM drives
- Human Interface Devices
- IDE ATA/ATAPI controllers
- IEEE 1394 Bus host controllers
- Jungo
- Keyboards
- Mice and other pointing devices
- Monitors
- Network adapters
- Ports (COM & LPT)
  - Communications Port (COM1)
  - Communications Port (COM2)
  - Printer Port (LPT1)
  - EMS200 (COM3)
- Processors
- SCSI and RAID controllers
- Sound, video and game controllers
- System devices
- Universal Serial Bus controllers

COM Port Assignment

Figure 8- COM port assigned to EMS200

Using the USB Console Port

The virtual COM port will be used to enable serial control over the EMS200 (see Operation Via Text Menu on page 59). When you open a terminal program be sure to use the correct COM port (see Figure 8 and Figure 9).



EMS200

Enter details for the phone number that you want to dial:

Country/region: United States (1)

Area code: 330

Phone number:

Connect using: COM1

COM1
COM2
TCP/IP (Winsock)

Figure 9- Configure COM port in HyperTerminal

Connect the Power

Note: Sensors should be connected before supplying power to the EMS200.

1. Connect the AC adapter to the connection marked "PWR" on the EMS200 and plug it into an outlet.

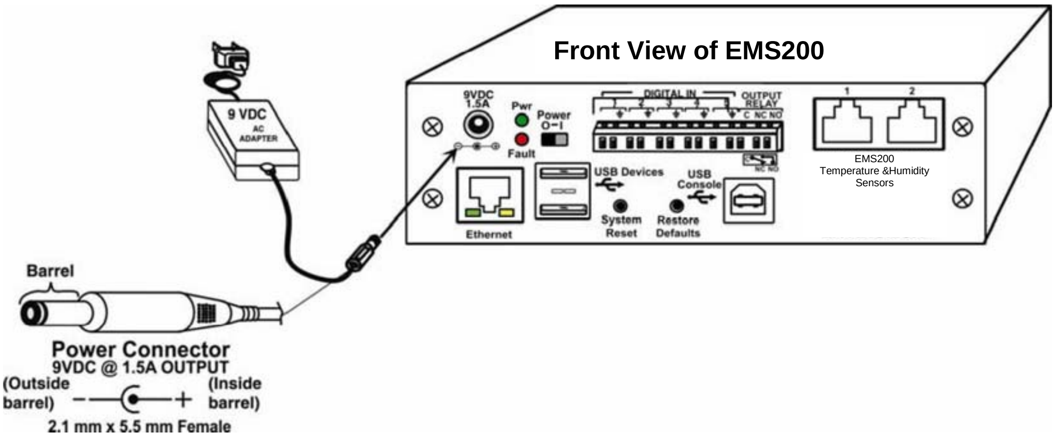


Figure 10- Connect the AC adapter and power-up

2. Use the NTI Discovery Tool (page 17) to configure network settings.

Front Panel LEDs Indicate Status

With proper connections made, the EMS200 is now ready to power ON. With the power cord attached and plugged into an AC outlet, the “Power” green LED should be illuminated on the front of the EMS200. The red “Fault” LED will illuminate when power is first applied and while the EMS200 boots up (for up to 60 seconds). Once the red LED goes OFF, the EMS200 is ready for use. After a completed boot-up, the red LED will only illuminate when one of the connected sensors is in alert.

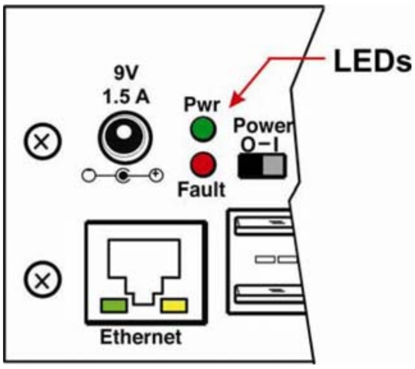


Figure 11- LEDs on front of EMS200

Connect a Modem

A USB GSM modem may be connected (EMS200-3GU) to use to send SMS alert messages to a contact's cell phone. The EMS200-3GU modem will connect to the EMS200 at the "USB Devices" port (either USB Type A connector, it doesn't matter which one) . The remaining USB Type A connector on the EMS200 is available for the connection of a USB Flash Drive for data logging (page 57).

The phone number to be called for each user is configured under "User Configuration-Contact Settings" (page 41).

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

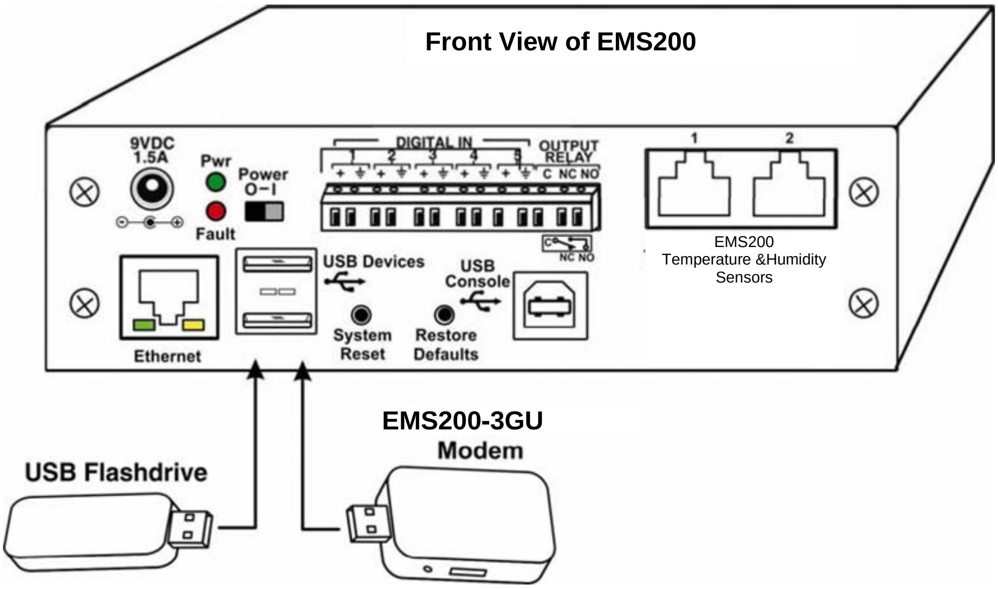


Figure 12- Connect a Modem

Cell phone Mini SIM card for GSM modem

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

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

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

Note: The EMS200-3GU will send SMS messages only.   No access to the EMS200 is possible through the modem.

OVERVIEW

Administration

The EMS200 can be administered in any one of the following ways:

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

The following administrative controls are available in the EMS200, thru the menu.

- View or modify the administrator & user parameters (passwords, sensor alert subscriptions, admin access, etc.)
- View or modify the network parameters (e.g. IP Address, Gateways, DNS, etc.)
- View and clear system event logs
- Clear, import, export and restore configuration parameters
- Firmware upgrades for the EMS200 (over Ethernet)
- View or modify sensor, and IP device configurations

General Functions

Sensor Alerts

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

IP Monitoring & Alerts

Individual IP addresses can be monitored. The EMS200 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 EMS200 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 EMS200 can also be configured to monitor the IP addresses of the network switches and routers to which these devices are connected, so as to determine if the problem is due to a lack of response from the device or a network failure. Alert notifications will be provided through four main methods: visible notification via one of the user interfaces (red "Fault" LED on front panel, alert on webpage, alert in text menu), emails, syslog messages, SMS messages and/or SNMP traps.

Event Log

The EMS200 maintains an event log. The event log includes power-ON, system, and alert notifications, as well as user login/logout, and user alert handling. The maximum number of log entries is 1000, and these entries are sorted in chronological order. The log can be viewed at any time through the web interface or text menu, and can be saved as a text file. Log entries can be removed individually or all at once.

Data Log

The EMS200 maintains a data log. The data log includes readings taken from sensors, IP devices, and connected accessories being monitored. The maximum number of log entries is 1000, and these entries are sorted in chronological order. The log can be viewed at any time through the web interface or text menu, and can be saved as a text file. Log entries can be removed individually or all at once.

Email

The EMS200 can access an SMTP server to send outgoing email. Outgoing email would contain pre-formatted alert notifications. SMTP server information can be configured using one of the interfaces. Email addresses can be configured through web pages or text menu. Each user (up to 15) can have their own email address.   For assistance in setting up Email, see page 103.

The email messages sent by the EMS200 have a fixed format. Alert emails contain 6 fields and will have a configurable title. The title is configurable for each sensor, device, or IP address. The title is the “email subject” in all configuration pages.   A sample message is shown below:

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

SNMP

The EMS200 can send alerts as SNMP traps when a sensor or IP device enters/leaves alert mode and for all log events. Using an SNMP MIB browser, a user can monitor all sensor statuses and system IP settings.

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

Note: The SNMP MIB file (mini-lx-v1-xx.mib), for use with an SNMP MIB browser or SNMP trap receiver, can be found on the manual CD. Click on the link to open the file, then save the file to your hard drive to use with the SNMP MIB browser or SNMP trap receiver.

GSM Modem

An external GSM modem can be connected to allow the system to send alert notifications via SMS messages. When a sensor crosses a threshold or IP device become inactive, an alert notification can be formatted to SMS message (see page 24) and the modem can transmit the message to all users that subscribe to the applicable sensor group.

Security

User Settings

In order to configure and operate the EMS200, each user must login with a unique username and password. The Administrator can configure each user’s settings as User or Administrator. An Administrator has access to all configurations and controls. A user can monitor sensors, accessories, and IP devices. A user can edit his/her own account. Users cannot configure the sensor settings.

IP Filtering

The EMS200 allows the administrator to block access to the device from certain IP addresses. The EMS200 can accept or drop requests based on the IP filter settings. IP Filtering provides an additional mechanism for securing the EMS200. Access to the EMS200 network services (SNMP, HTTP(S), SSH, Telnet) can be controlled by allowing or disallowing connections from various IP addresses, subnets, or networks.

Secure Connections

The EMS200 supports secure connections using SSHv2 and HTTPS.

Authentications

The EMS200 supports local authentication with up to 16 character usernames and passwords, and it also supports LDAPv3.

Encryption

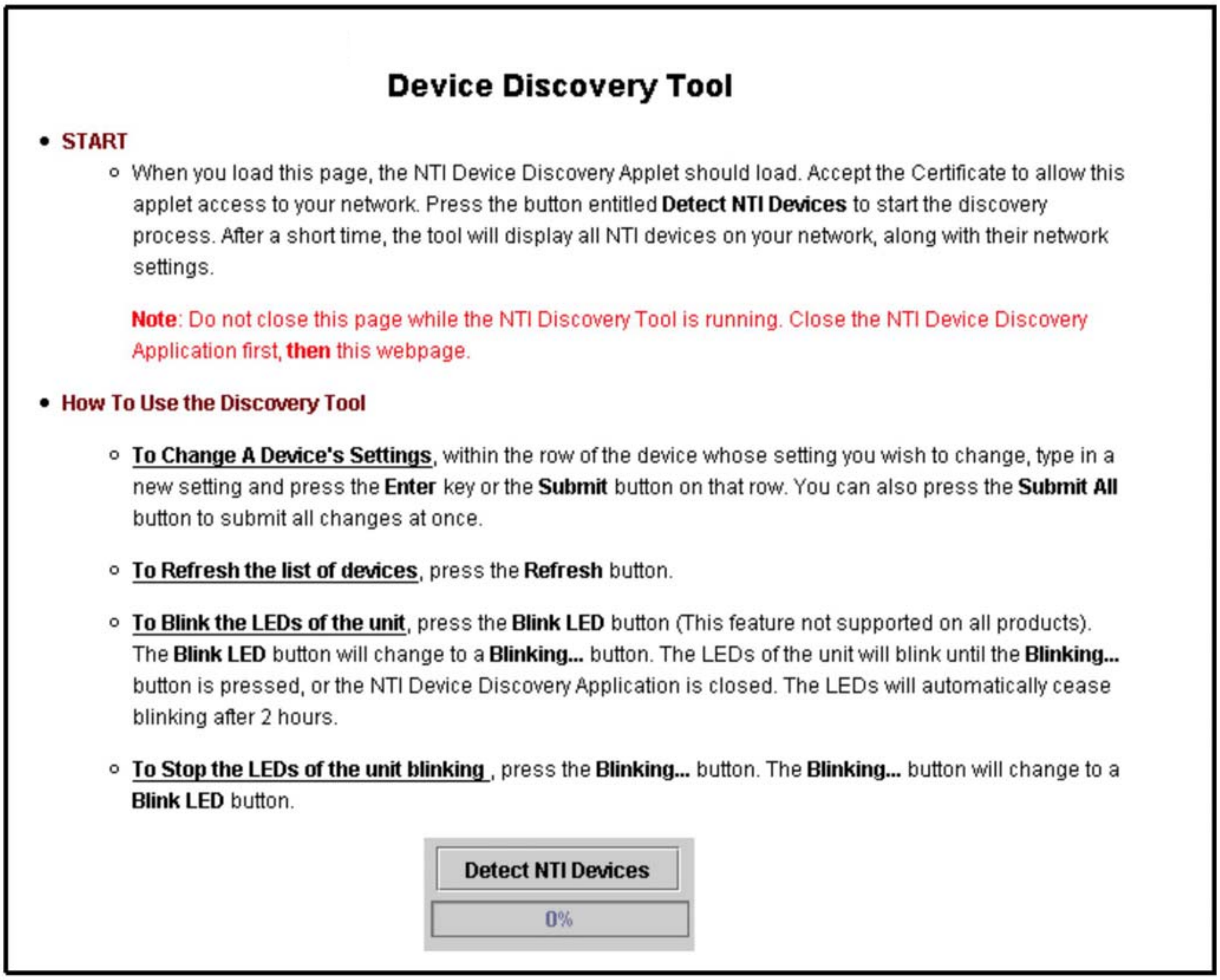
The EMS200 supports 256-bit AES encryption.

DEVICE DISCOVERY TOOL

In order to easily locate the EMS200 on a network, the NTI Device Discovery Tool may be used. A link to the Discovery Tool is provided on the web page that appears when you insert the instruction manual CD provided into your CD ROM drive. Click on the link or browse the CD and click on the file *discover.html* . This will open your browser and display the Device Discovery Tool page.

Note: The Device Discovery Tool requires the Java Runtime Environment to operate. A link to the web page from which it can be downloaded and installed is provided on the CD.

Note: The computer using the Device Discovery Tool and the EMS200 must be connected to the same physical network in order for the Device Discovery Tool to work.



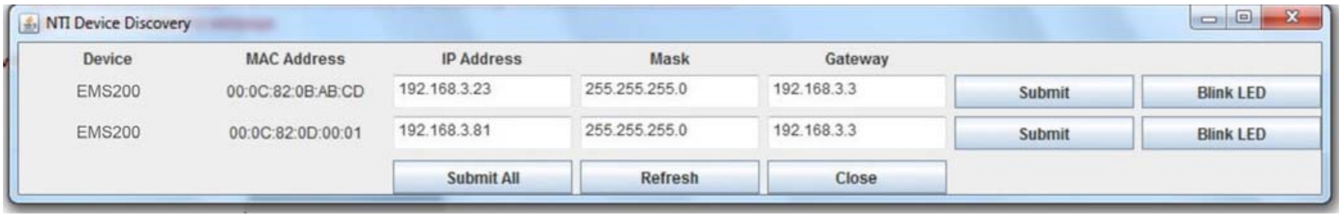
Device Discovery Tool

- **START**
  - When you load this page, the NTI Device Discovery Applet should load. Accept the Certificate to allow this applet access to your network. Press the button entitled **Detect NTI Devices** to start the discovery process. After a short time, the tool will display all NTI devices on your network, along with their network settings.

    Note: Do not close this page while the NTI Discovery Tool is running. Close the NTI Device Discovery Application first, **then** this webpage.
- **How To Use the Discovery Tool**
  - **To Change A Device's Settings**, within the row of the device whose setting you wish to change, type in a new setting and press the **Enter** key or the **Submit** button on that row. You can also press the **Submit All** button to submit all changes at once.
  - **To Refresh the list of devices**, press the **Refresh** button.
  - **To Blink the LEDs of the unit**, press the **Blink LED** button (This feature not supported on all products). The **Blink LED** button will change to a **Blinking...** button. The LEDs of the unit will blink until the **Blinking...** button is pressed, or the NTI Device Discovery Application is closed. The LEDs will automatically cease blinking after 2 hours.
  - **To Stop the LEDs of the unit blinking** , press the **Blinking...** button. The **Blinking...** button will change to a **Blink LED** button.

Figure 13- Device Discovery Tool page

Use the Device Discovery Tool to display all NTI EMS200 units on the network, along with their network settings. Follow the instructions on the Device Discovery Tool page to use the tool and to change the device settings if so desired.



NTI Device Discovery

Device	MAC Address	IP Address	Mask	Gateway		
EMS200	00:0C:82:0B:AB:CD	192.168.3.23	255.255.255.0	192.168.3.3	Submit	Blink LED
EMS200	00:0C:82:0D:00:01	192.168.3.81	255.255.255.0	192.168.3.3	Submit	Blink LED

OPERATION VIA WEB INTERFACE

A user may monitor and configure the settings of the EMS200 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 EMS200 to the Ethernet (page 6). Use the Device Discovery Tool (page 17) to setup the network settings.   Then, to access the web interface controls, the user must log in.

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://192.168.1.21

Note: If "Allow HTTP Access" (page 36) is not checked to be enabled (disabled by default) , only an SSL-encrypted connection will be possible. The software will automatically redirect to an HTTPS (secure) connection. The user will likely see a warning about the SSL certificate and a prompt to accept the certificate.   The EMS200 uses a self-signed NTI certificate.   Accept the NTI certificate.

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

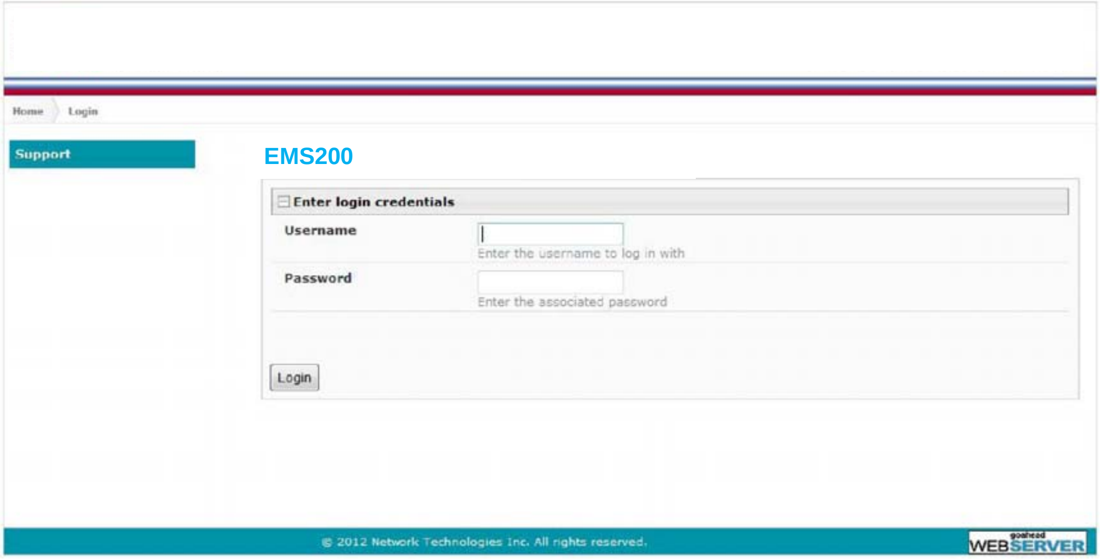

Home
Login
Support
EMS200
Enter login credentials
Username
Enter the username to log in with
Password
Enter the associated password
Login
© 2012 Network Technologies Inc. All rights reserved.
goahead WEBSERVER

Figure 14- Login prompt to access web interface

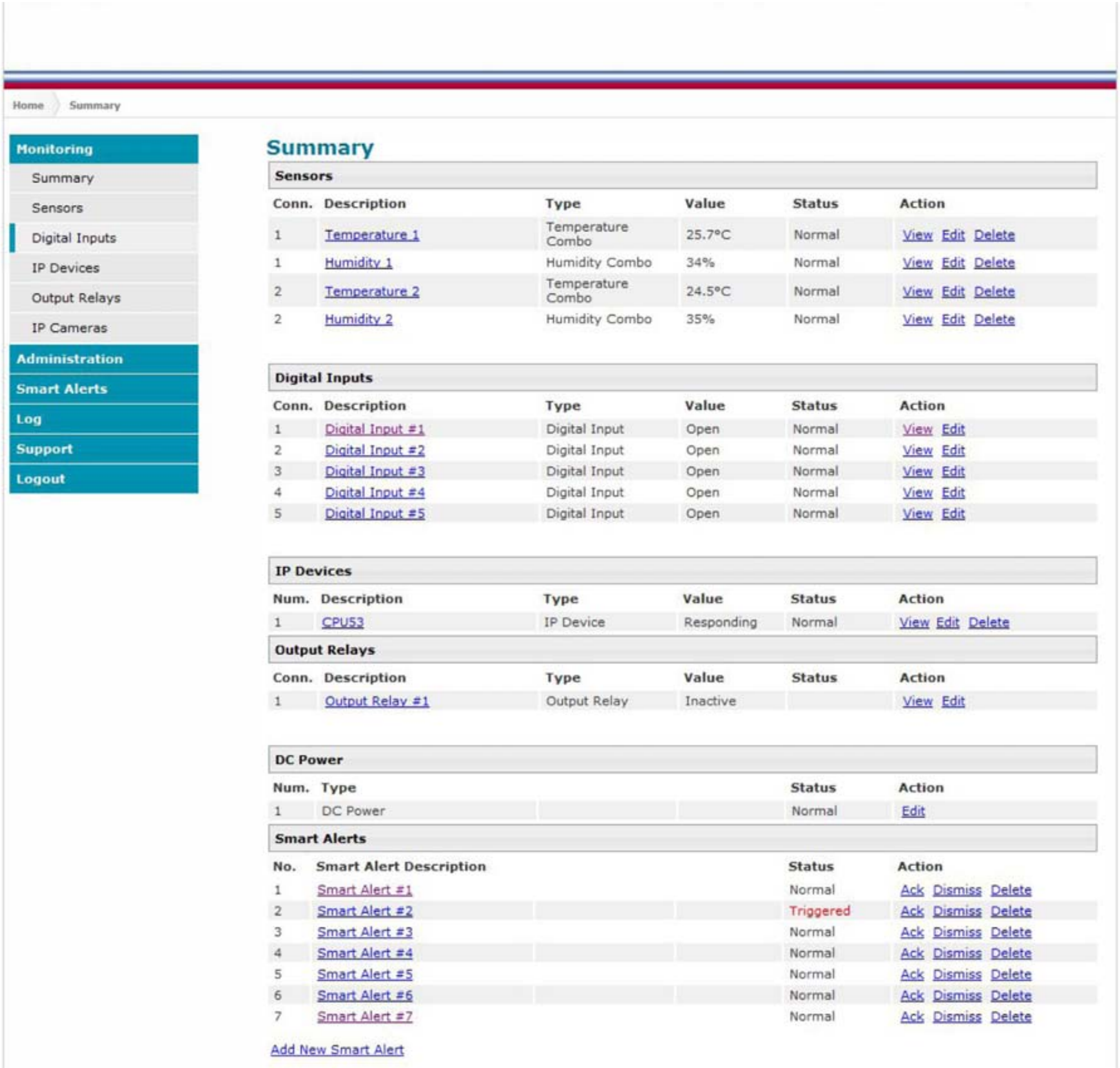
Username = root

Password = nti

(lower case letters only)

Note: usernames and passwords are case sensitive

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



Summary

Sensors

Conn.	Description	Type	Value	Status	Action
1	Temperature 1	Temperature Combo	25.7°C	Normal	View Edit Delete
1	Humidity 1	Humidity Combo	34%	Normal	View Edit Delete
2	Temperature 2	Temperature Combo	24.5°C	Normal	View Edit Delete
2	Humidity 2	Humidity Combo	35%	Normal	View Edit Delete

Digital Inputs

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

IP Devices

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

Output Relays

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

DC Power

Num.	Type	Status	Action
1	DC Power	Normal	Edit

Smart Alerts

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

Add New Smart Alert

Figure 15- Summary page

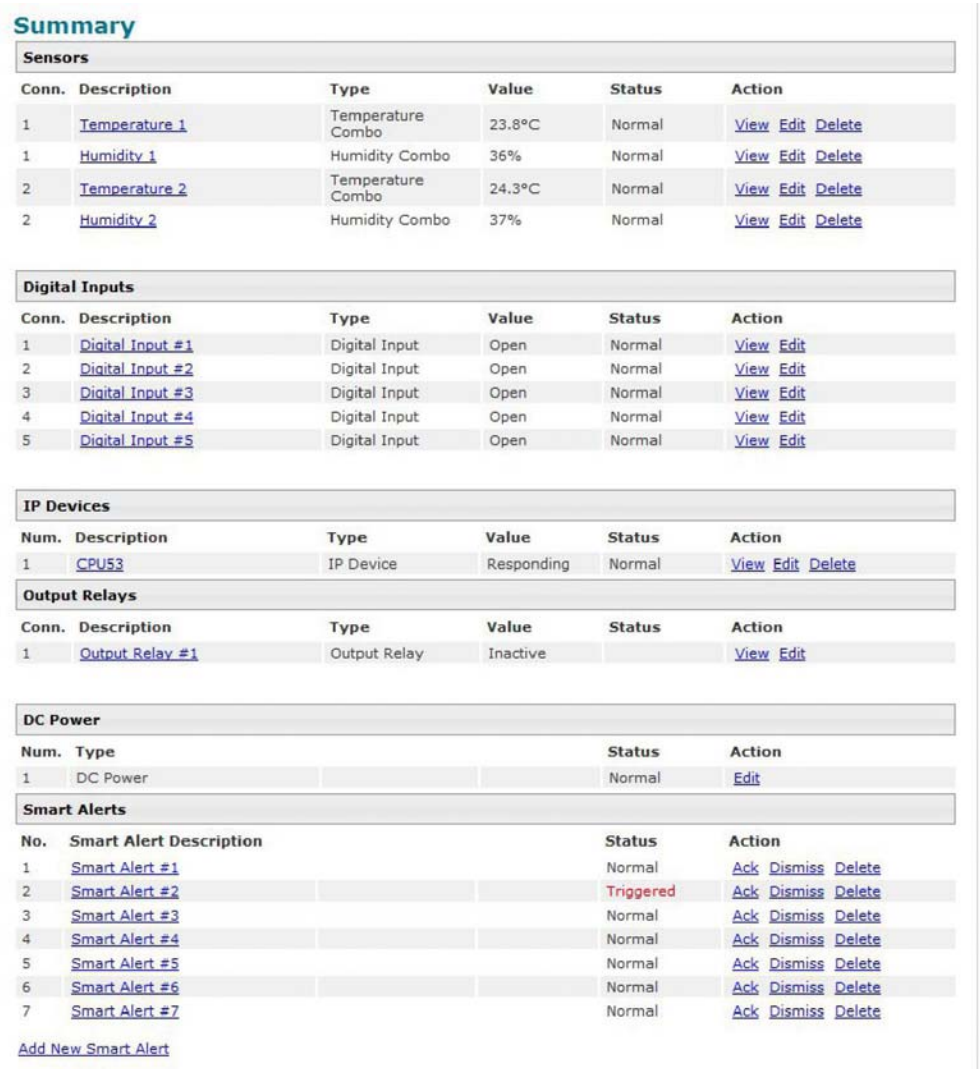
From this initial page, the user can use the menu to the left to manage all the functions of the EMS200.

Function	Description
MONITORING	Monitor the sensors, accessories, and IP devices of the EMS200 (next page)
ADMINISTRATION	**Configure all system, network, multi-user access, and security settings as well as upgrade firmware (page 33)**
SMART ALERTS	View and configure the Events used for Smart Alerts and the Smart Alerts themselves (page 48)
LOG	View and configure the Event and Data Logs (page 55)
SUPPORT	Links for downloading a manual, the MIB file, or firmware upgrades
LOGOUT	Log the user out of the EMS200 web interface

Monitoring

Under Monitoring, there are links to view the status of all sensors and IP Devices being monitored by the EMS200.

Link	Description
Summary	Lists all items being monitored, including their description, type, value, and status
Sensors	Provides a link to view the status of only the Sensors and a link to add them (page 22)
Digital Inputs	Provides a link to view the status of any sensors connected to the CONTACT terminals (1-5) a link to view or edit their configuration (page 22)
IP Devices	Provides a link to view the status of only the IP Devices and a link to add them (page 27)
Output Relay	Provides a link to view the status of the output relay and a link to edit the configuration (page 29)
IP Cameras	Displays an image from up to 8 webcams with links to connect to each (page 31)
DC Power	Provides status of the external DC power supply (page 32) (only applicable on models with battery-backup feature)
Smart Alerts	Displays the status of each Smart Alert configuration (page 48) and provided link to respond when triggered



Summary

Sensors

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

Digital Inputs

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

IP Devices

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

Output Relays

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

DC Power

Num.	Type	Status	Action
1	DC Power	Normal	Edit

Smart Alerts

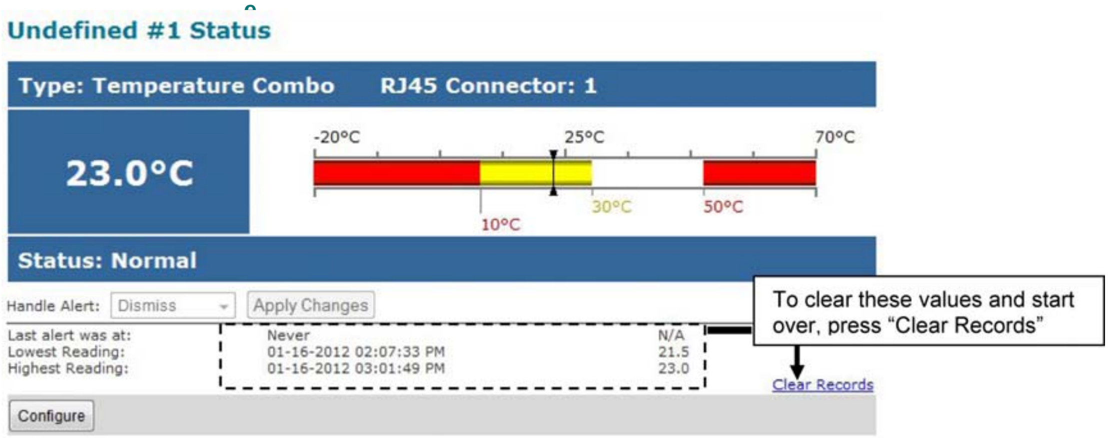
No.	Smart Alert Description	Status	Action
1	Smart Alert #1	Normal	Ack Dismiss Delete
2	Smart Alert #2	Triggered	Ack Dismiss Delete
3	Smart Alert #3	Normal	Ack Dismiss Delete
4	Smart Alert #4	Normal	Ack Dismiss Delete
5	Smart Alert #5	Normal	Ack Dismiss Delete
6	Smart Alert #6	Normal	Ack Dismiss Delete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

Add New Smart Alert

Figure 16- Summary page and the Monitoring menu

From the Summary page, the user can view the status of all sensors and the IP Devices being monitored by the EMS200. Each item listed has a link that when selected will open the status page for that item.

U
n
d



Undefined #1 Status

Type: Temperature Combo RJ45 Connector: 1

23.0°C

Status: Normal

Handle Alert: Dismiss Apply Changes

Last alert was at:	Never	N/A
Lowest Reading:	01-16-2012 02:07:33 PM	21.5
Highest Reading:	01-16-2012 03:01:49 PM	23.0

To clear these values and start over, press “Clear Records”

Clear Records

Configure

Figure 17- Status page for a temperature sensor

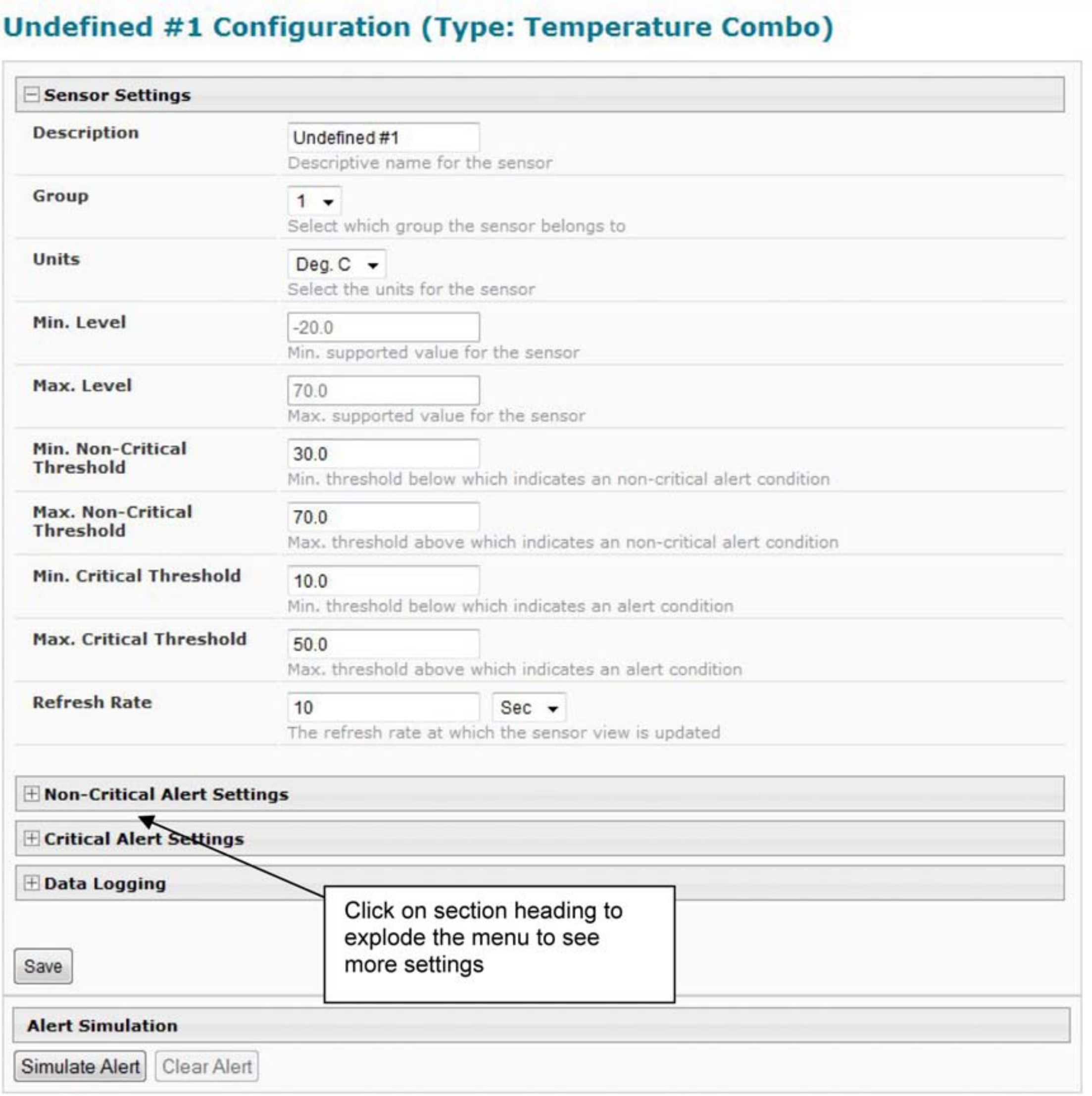
If the temperature sensor is in alert status, the user has the option to either **acknowledge** the alert or **dismiss** it. If the user acknowledges the alert, no additional alert messages will be sent during that alert status cycle. If the user dismisses the alert, another alert message will be sent once the “notify again after” time designated on the configuration page (page 23) elapses.

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

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

Configure Sensors

The Sensor Configuration page is broken into three sections; Sensor Settings, Alert Settings and Data Logging. To explode the window to see settings for a section, click on the section heading (Figure 18).



Undefined #1 Configuration (Type: Temperature Combo)

⊟ Sensor Settings

Description	Undefined #1 Descriptive name for the sensor
Group	1 Select which group the sensor belongs to
Units	Deg. C Select the units for the sensor
Min. Level	-20.0 Min. supported value for the sensor
Max. Level	70.0 Max. supported value for the sensor
Min. Non-Critical Threshold	30.0 Min. threshold below which indicates an non-critical alert condition
Max. Non-Critical Threshold	70.0 Max. threshold above which indicates an non-critical alert condition
Min. Critical Threshold	10.0 Min. threshold below which indicates an alert condition
Max. Critical Threshold	50.0 Max. threshold above which indicates an alert condition
Refresh Rate	10 Sec The refresh rate at which the sensor view is updated

⊞ Non-Critical Alert Settings

⊞ Critical Alert Settings

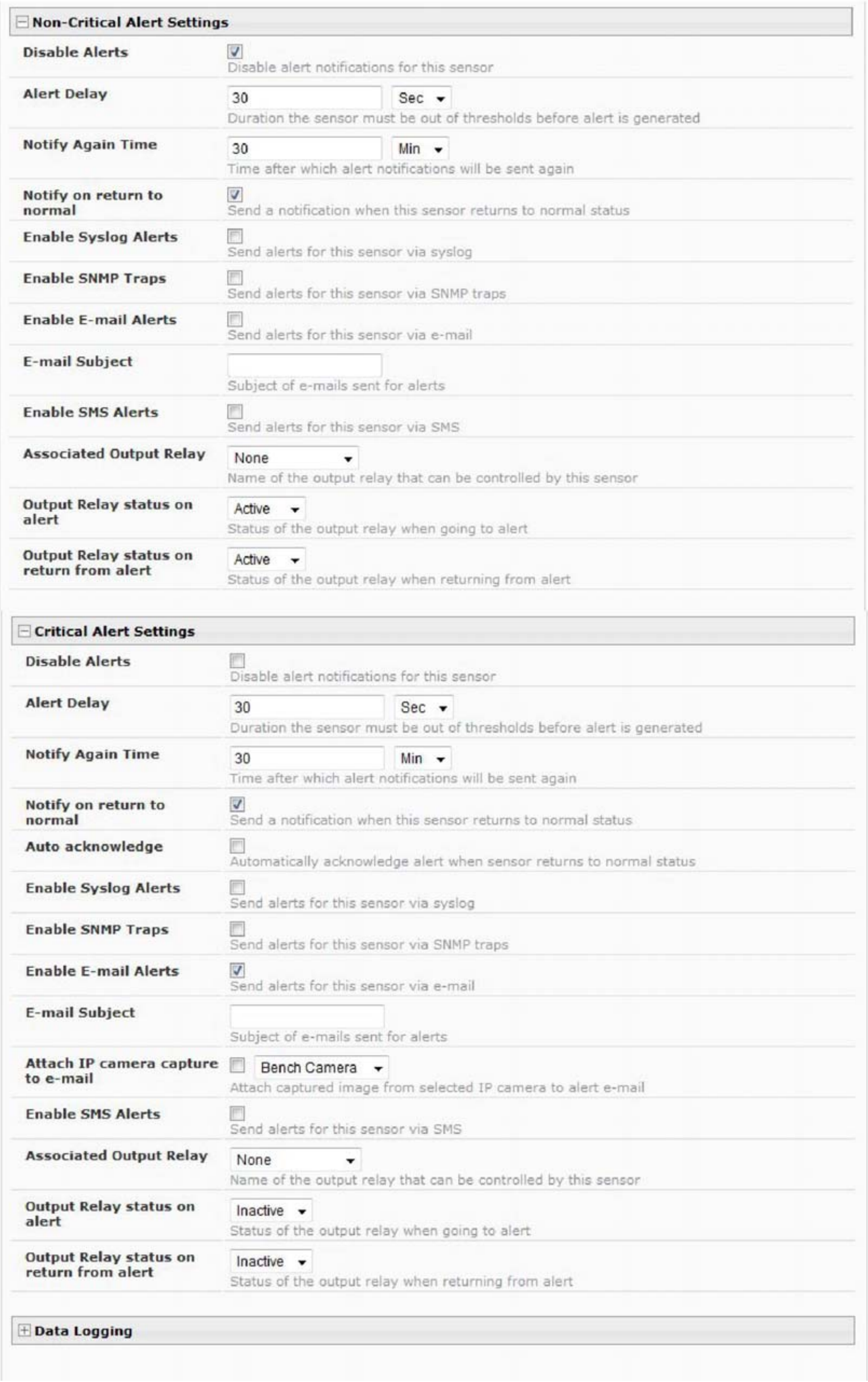
⊞ Data Logging

Click on section heading to explode the menu to see more settings

Figure 18- Sensor Configuration page

Threshold Settings

A sensor designed for connection to the RJ45 ports often has a range of reporting values (for example EMS200-T has a range of 32°-104°F). Two levels of threshold values for each end of that range can be configured (above) to initiate two different alert messages, depending upon the severity of the alert. These levels are identified as “Non-critical” and “Critical”. Use these variations in alert communication as needed to inform users of the severity of sensor reading changes. Each level of alert has its own configuration for how or if the user will be alerted as to a sensor’s status (see Figure 19).



⊟ **Non-Critical Alert Settings**

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

⊟ **Critical Alert Settings**

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

⊞ **Data Logging**

Figure 19- Sensor Configuration- exploded view of additional settings

Sensor Settings	Description
Description	The description of the sensor that will be viewed in the Summary page and in the body of alert messages
Group	Assign the sensor to any group 1 -8 (see also page 39)
Units	This lets the operator choose between Celsius and Fahrenheit as the temperature measurement unit.
Min. Level	Displays the minimum value that this sensor will report
Max. Level	Displays the maximum value that this sensor will report
Minimum Non-Critical -Threshold	The user must define the lowest acceptable value for the sensors. If the sensor measures a value below this threshold, the sensor will move to non-critical alert status. The assigned value should be > within the range defined by Minimum Level and Maximum Level and > lower than the assigned Maximum Threshold value. If values out of the range are entered, and error message will be shown.
Maximum Non-Critical Threshold	The user must define the highest acceptable value for the sensors. If the sensor measures a value above this threshold, the sensor will move to non-critical alert status. The assigned value should be > within the range defined by Minimum Level and Maximum Level and > higher than the assigned Minimum Threshold value. If values out of the range are entered, and error message will be shown.
Minimum Critical Threshold	The user must define the lowest acceptable value for the sensors. If the sensor measures a value below this threshold, the sensor will move to alert status. The assigned value should be > within the range defined by Minimum Level and Maximum Level, > lower than the assigned Maximum Threshold value, and > lower than the Minimum Non-Critical Threshold value. If values out of the range are entered, and error message will be shown.
Maximum Critical Threshold	The user must define the highest acceptable value for the sensors. If the sensor measures a value above this threshold, the sensor will move to alert status. The assigned value should be > within the range defined by Minimum Level and Maximum Level, > higher than the assigned Minimum Threshold value, and > higher than the Maximum Non-Critical Threshold value. If values out of the range are entered, and error message will be shown.
Refresh Rate	Determines how often the displayed sensor value is refreshed on the Sensor page. A numeric value and a measurement unit (minimum 1 seconds, maximum 999 minutes) should be entered.
Alert Settings (Applies to Critical and Non-Critical Alerts except where noted)	
Disable Alerts	Place a checkmark in the box to prevent alerts from being sent when this sensor's status changes
Alert Delay	The alert delay is an amount of time the sensor must be in an alert condition before an alert is sent. This provides some protection against false alarms. The Alert Delay value can be set for 0-999 seconds or minutes.
Notify Again Time	Enter the amount of time in seconds, minutes, or hours (1-999) before an alert message will be repeated
Notify on Return to Normal	The user can also be notified when the sensor readings have returned to the normal range by selecting the "***Notify when return to normal***" box for a sensor.
Auto Acknowledge	Place a checkmark in this box to have alert notifications in the summary page return to normal state automatically when sensor readings return to normal. **Note**: The Non-Critical alert settings do not have this option. Instead, non-critical alert notifications are always auto-acknowledged when sensor readings return to normal
Enable Syslog Alerts	Place a checkmark in this box to have alert notifications sent via Syslog messages
Enable SNMP traps	Place a checkmark in this box to have alert notifications sent via SNMP traps (v2c)
Enable Email Alerts	Place a checkmark in this box to have alert notifications sent via Email
Email Subject	Enter the subject to be viewed when an email alert message is received

Alert Settings (Applies to Critical and Non-Critical Alerts except where noted)	
Attach IP Camera capture to email	Associate a sensor with a IP camera. Select an IP camera from the drop-down box. An image will be captured and sent with the alert message when an alert is sent via e-mail. IP cameras that are monitored by the EMS200 (page 31) will be available for this purpose. ***Note: To be able to send IP camera captures as e-mail attachments, viewer security (in your camera's configuration) needs to be disabled. Consult your IP camera manual to see if this feature is present and for instructions on how to do this.***
Enable SMS Alerts	Place a checkmark in this box to have alert notifications sent via SMS messages (requires a modem)
Associated Output Relay	Associate the sensor with the operation of the output relay, or not ***Note: Only one sensor should be associated with the Output Relay at a time. Contradicting commands from two or more sensors will result in the output relay responding to the state directed by the last command received.***
Output Relay Status on Alert	State the output relay will be in when sensor goes to an alert
Output Relay Status on Return from Alert	State the output relay will be in when sensor is no longer in alert
Data Logging	
Add to data log	This is a check-box that lets the user decide if the data sampled should be recorded in the Data Log.
Logging Period	Enter the time period between logged measurements

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

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

More about Groups

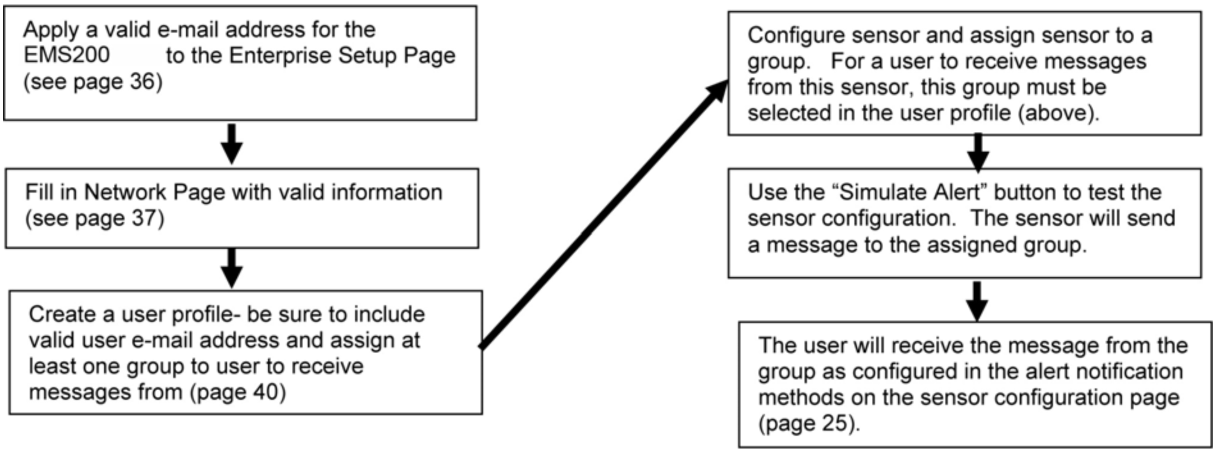
Groups are used to create a common relationship between sensors, IP devices, etc. and their alert messages. Each item being monitored is assigned to one group of 8 possible. Users (a maximum number of 16 including the root user) can receive alert messages from items in one or more groups (see user configuration on page 39).

Test Alerts

With all the configuration settings completed, each sensor and how the EMS200 will react to an alert condition can be tested. Press the **Simulate Alert** button at the bottom of the configuration page to test each of the notification methods configured. To cancel the simulation, press the **Clear** button.

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

To perform a test, the EMS200 must be properly setup for a user to receive alert messages. Use the chart below to make sure the EMS200 is setup properly.



Apply a valid e-mail address for the EMS200 to the Enterprise Setup Page (see page 36)

Fill in Network Page with valid information (see page 37)

Create a user profile- be sure to include valid user e-mail address and assign at least one group to user to receive messages from (page 40)

Configure sensor and assign sensor to a group. For a user to receive messages from this sensor, this group must be selected in the user profile (above).

Use the "Simulate Alert" button to test the sensor configuration. The sensor will send a message to the assigned group.

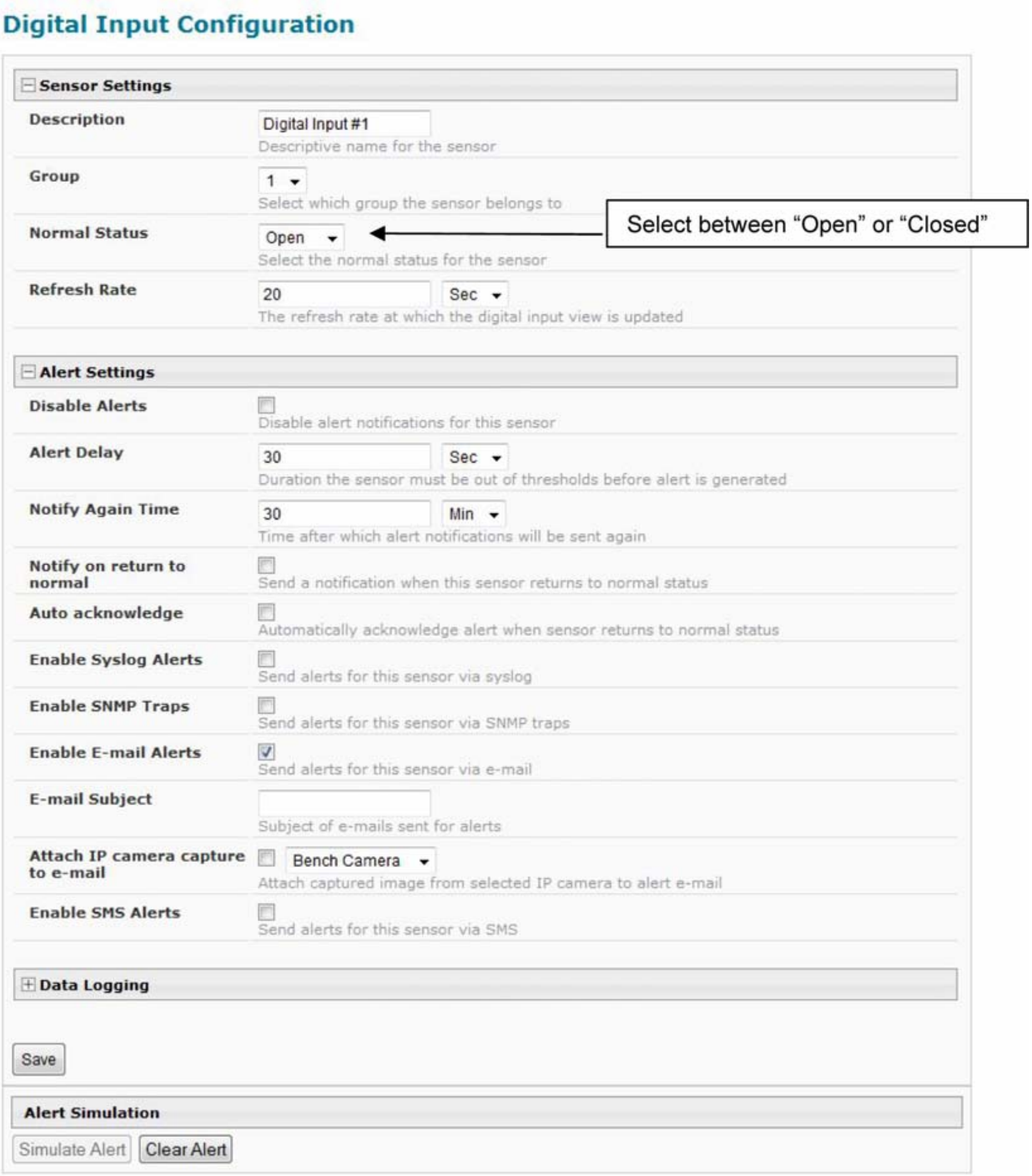
The user will receive the message from the group as configured in the alert notification methods on the sensor configuration page (page 25).

Figure 20- Chart to setup alert notification

Configure Digital Inputs

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

Alert settings and data logging features are the same as those described on page 24.



Digital Input Configuration

⊟ Sensor Settings

Description	Digital Input #1 Descriptive name for the sensor
Group	1 ▾ Select which group the sensor belongs to
Normal Status	Open ▾ Select the normal status for the sensor
Refresh Rate	20 Sec ▾ The refresh rate at which the digital input view is updated

Select between "Open" or "Closed"

⊟ Alert Settings

Disable Alerts	□ Disable alert notifications for this sensor
Alert Delay	30 Sec ▾ Duration the sensor must be out of thresholds before alert is generated
Notify Again Time	30 Min ▾ Time after which alert notifications will be sent again
Notify on return to normal	□ Send a notification when this sensor returns to normal status
Auto acknowledge	□ Automatically acknowledge alert when sensor returns to normal status
Enable Syslog Alerts	□ Send alerts for this sensor via syslog
Enable SNMP Traps	□ Send alerts for this sensor via SNMP traps
Enable E-mail Alerts	☑ Send alerts for this sensor via e-mail
E-mail Subject	 Subject of e-mails sent for alerts
Attach IP camera capture to e-mail	□ Bench Camera ▾ Attach captured image from selected IP camera to alert e-mail
Enable SMS Alerts	□ Send alerts for this sensor via SMS

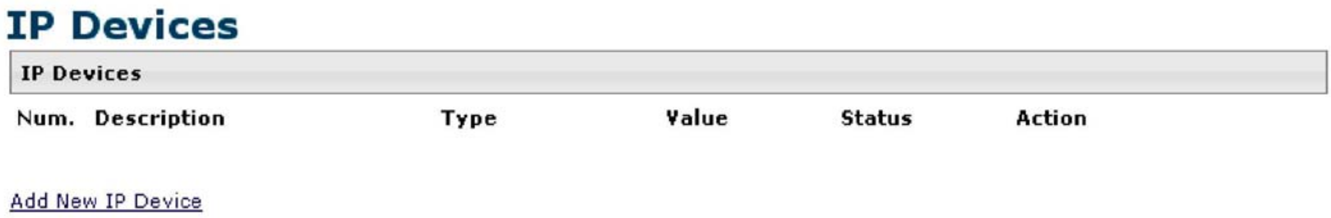
⊞ Data Logging

Alert Simulation

Figure 21- Sensor Configuration for Digital Inputs

Monitor IP Devices

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



IP Devices

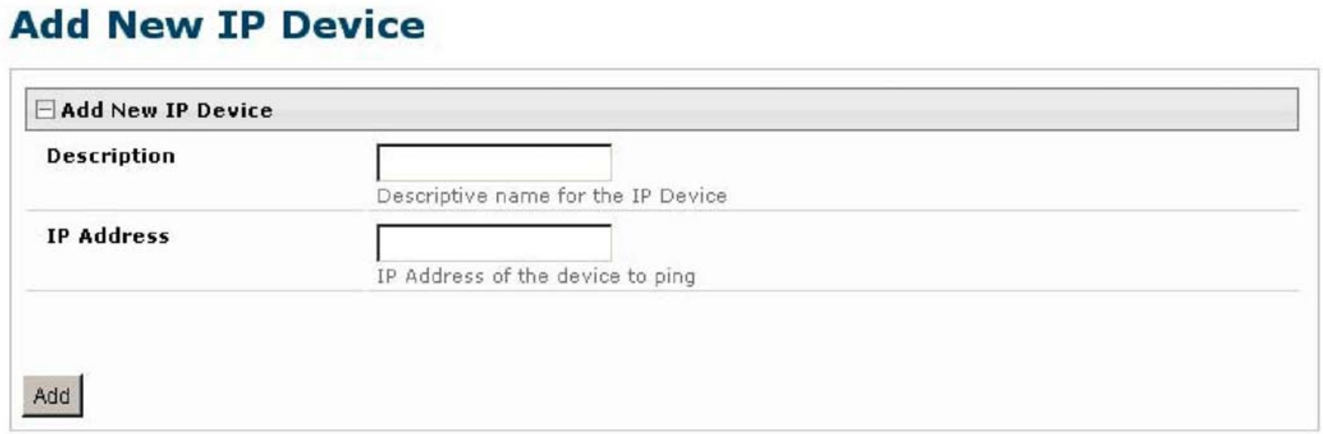
IP Devices

Num.	Description	Type	Value	Status	Action

Add New IP Device

Figure 22- IP Devices listing-none monitored yet

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



Add New IP Device

⊟ Add New IP Device

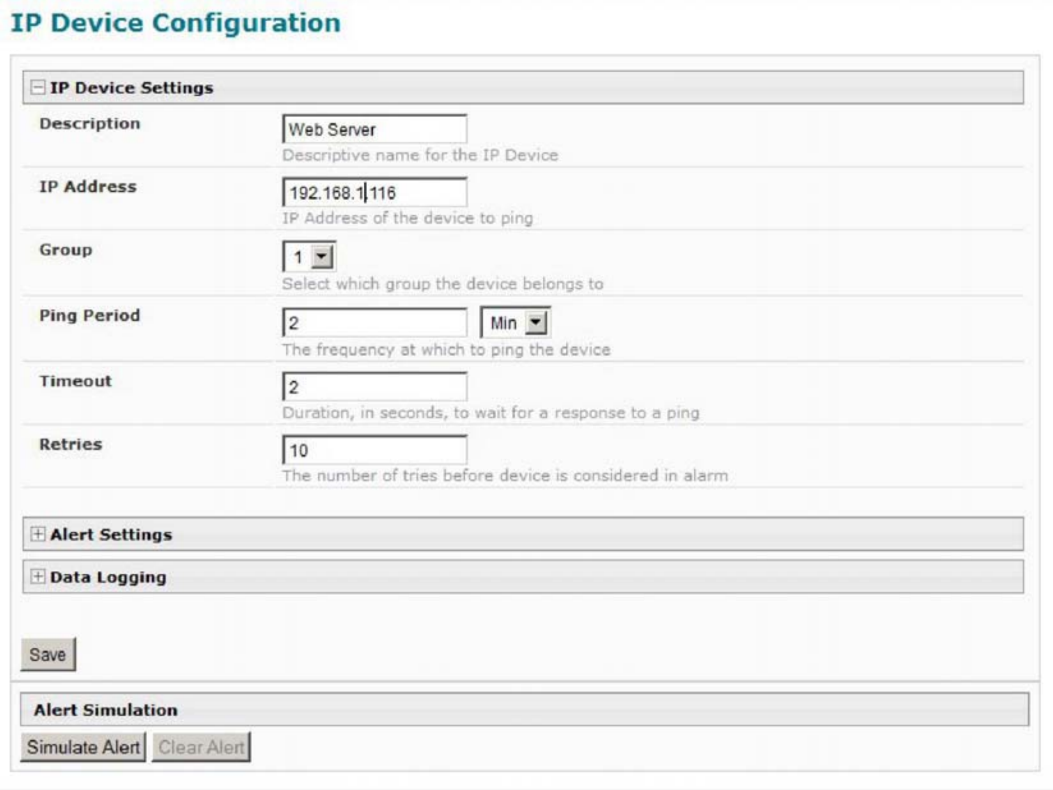
Description: Descriptive name for the IP Device

IP Address: IP Address of the device to ping

Figure 23- Add New IP Device page

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

The IP Device Configuration page will immediately open. Here you can configure the EMS200 to ping the IP Device as often as desired and to react to a lack of response by sending alert messages.



IP Device Configuration

⊟ IP Device Settings

Description: Web Server
Descriptive name for the IP Device

IP Address: 192.168.1.116
IP Address of the device to ping

Group: 1
Select which group the device belongs to

Ping Period: 2 Min
The frequency at which to ping the device

Timeout: 2
Duration, in seconds, to wait for a response to a ping

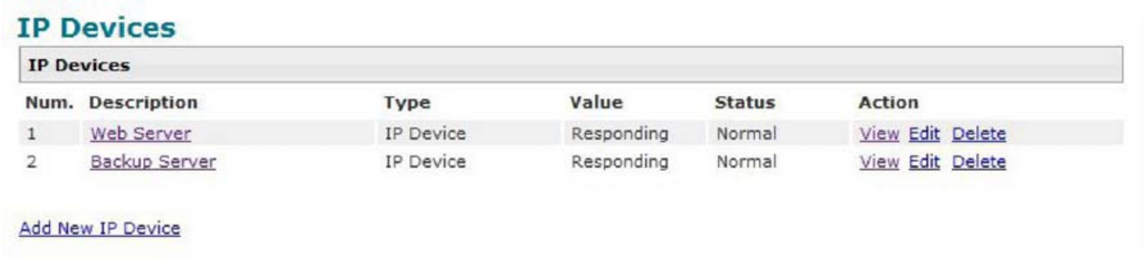
Retries: 10
The number of tries before device is considered in alarm

Figure 24- IP Device Configuration page

IP Device Settings	Description
Description	The description of the IP Device that will be viewed in the Summary page and in the body of alert messages
IP Address	The IP address of the IP Device
Group	Assign the IP Device to any group 1 -8
Ping Period	Enter the frequency in minutes or seconds that the EMS200 should ping the IP Device
Timeout	Enter the length of time in seconds to wait for a response to a ping before considering the attempt a failure
Retries	Enter the number of times the EMS200 should ping a non-responsive IP device before changing its status from normal to alarm and sending an alert

The alert settings and data logging are the same as for sensor configuration, described on page 24.

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



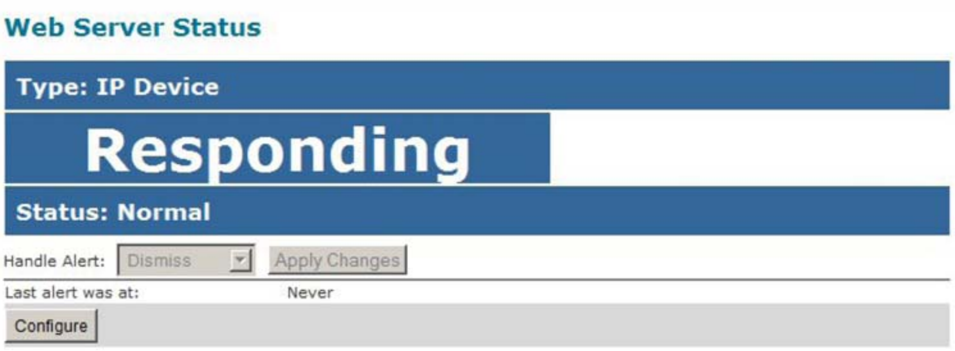
IP Devices

IP Devices

Num.	Description	Type	Value	Status	Action
1	Web Server	IP Device	Responding	Normal	View Edit Delete
2	Backup Server	IP Device	Responding	Normal	View Edit Delete

Figure 25- IP Device list with new devices added

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



Web Server Status

Type: IP Device

Responding

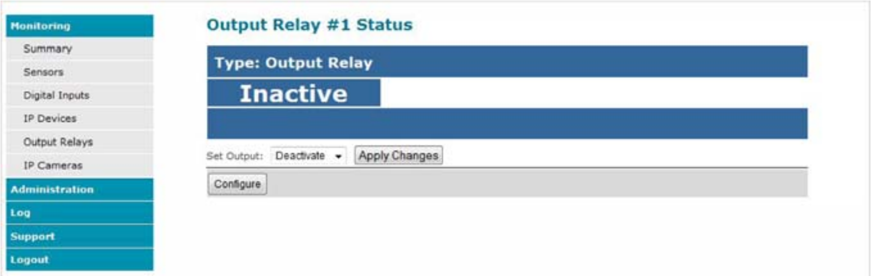
Status: Normal

Handle Alert: Dismiss

Last alert was at: Never

Monitor Output Relay

An output relay is provided to control an external device with a rating of up to 1A, 30VDC or 0.5A, 125VAC. The relay state is monitored to be either inactive (relay is at rest; contacts as indicated by product markings) or active (relay is energized; contacts are opposite that of product markings). The status of the relay can be changed either manually through the web interface, or as a result of an alert (page 22).



Output Relay #1 Status

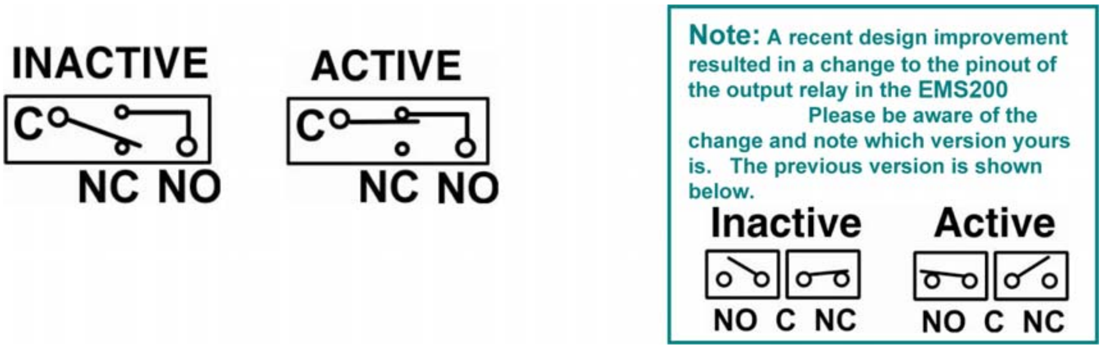
Type: Output Relay

Inactive

Set Output: Deactivate

Figure 27- Output Relay Status

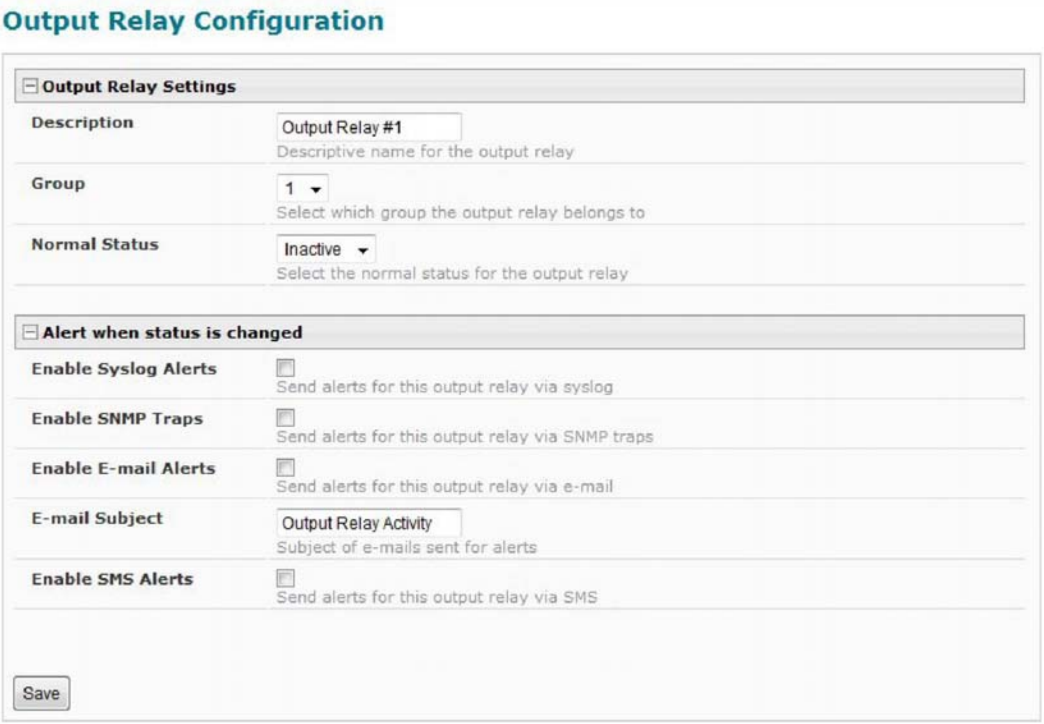
To set the state of the relay manually, from the relay status page (Figure 27), select the arrow next to “Set Output” to drop down the window and select either “Deactivate” or “Activate”. Then click the “Apply Changes” button.



Note: A recent design improvement resulted in a change to the pinout of the output relay in the EMS200 Please be aware of the change and note which version yours is. The previous version is shown below.

Figure 28- Output Relay Contact State

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



Output Relay Configuration

⊟ **Output Relay Settings**

Description	Output Relay #1 Descriptive name for the output relay
Group	1 Select which group the output relay belongs to
Normal Status	Inactive Select the normal status for the output relay

⊟ **Alert when status is changed**

Enable Syslog Alerts	□ Send alerts for this output relay via syslog
Enable SNMP Traps	□ Send alerts for this output relay via SNMP traps
Enable E-mail Alerts	□ Send alerts for this output relay via e-mail
E-mail Subject	Output Relay Activity Subject of e-mails sent for alerts
Enable SMS Alerts	□ Send alerts for this output relay via SMS

Figure 29- Configure Output Relay

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

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

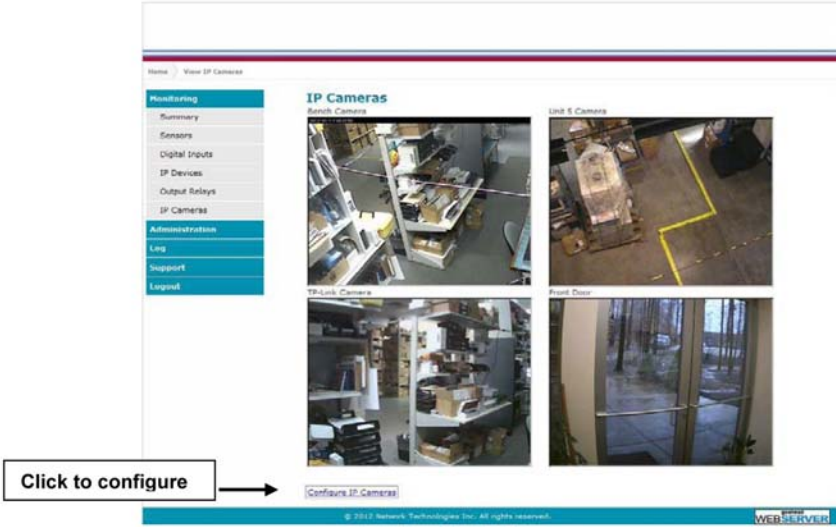
Choose the Normal Status for the relay, between Inactive or Active. When the status changes from what is defined as “normal”, an alert will be sent if so configured.

When the relay is an alert state, the EMS200 can be configured to send an email, syslog and SMS alerts, as well as an SNMP trap to the users subscribing to alerts in the selected group. Place a checkmark in the box for those features you wish to enable.

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

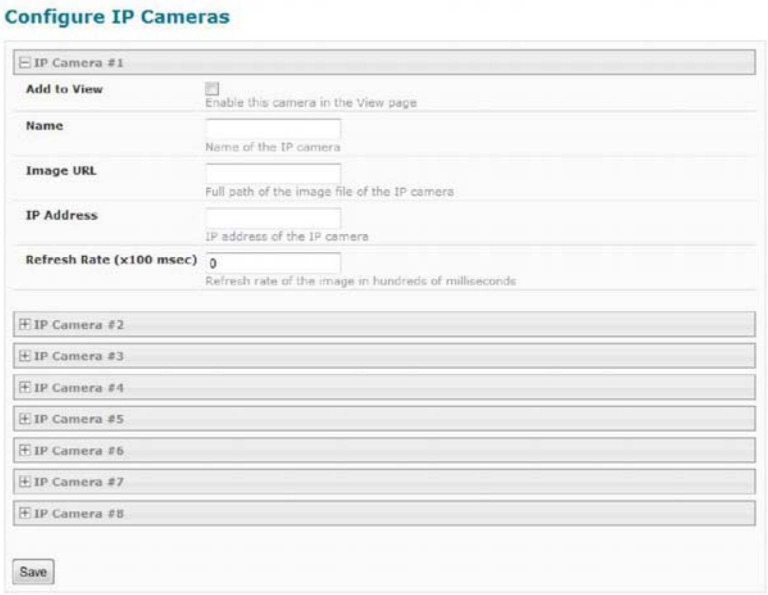
Monitor IP Cameras

The IP Cameras page displays the video snapshots of up to 8 monitored IP cameras. EMS200 will display the video from specified IP addresses and provide images at 320 x 240 resolution. To configure the IP cameras to be monitored, click on the “Configure IP Cameras” link.



Click to configure

Figure 30- IP Camera Monitoring



Configure IP Cameras

⊟ IP Camera #1

Add to View	□ Enable this camera in the View page
Name	Name of the IP camera
Image URL	Full path of the image file of the IP camera
IP Address	IP address of the IP camera
Refresh Rate (x100 msec)	0 Refresh rate of the image in hundreds of milliseconds

⊞ IP Camera #2

⊞ IP Camera #3

⊞ IP Camera #4

⊞ IP Camera #5

⊞ IP Camera #6

⊞ IP Camera #7

⊞ IP Camera #8

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

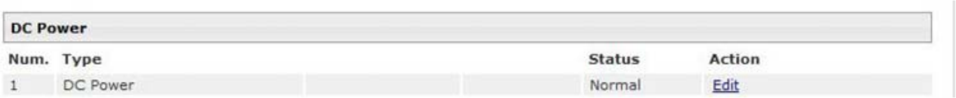
Figure 31- Configure IP Cameras

The images from IP cameras can also be associated with alert messages. When configured (page 22), an image from a IP camera can be taken and sent along with a sensor alert message via email.

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

DC Power

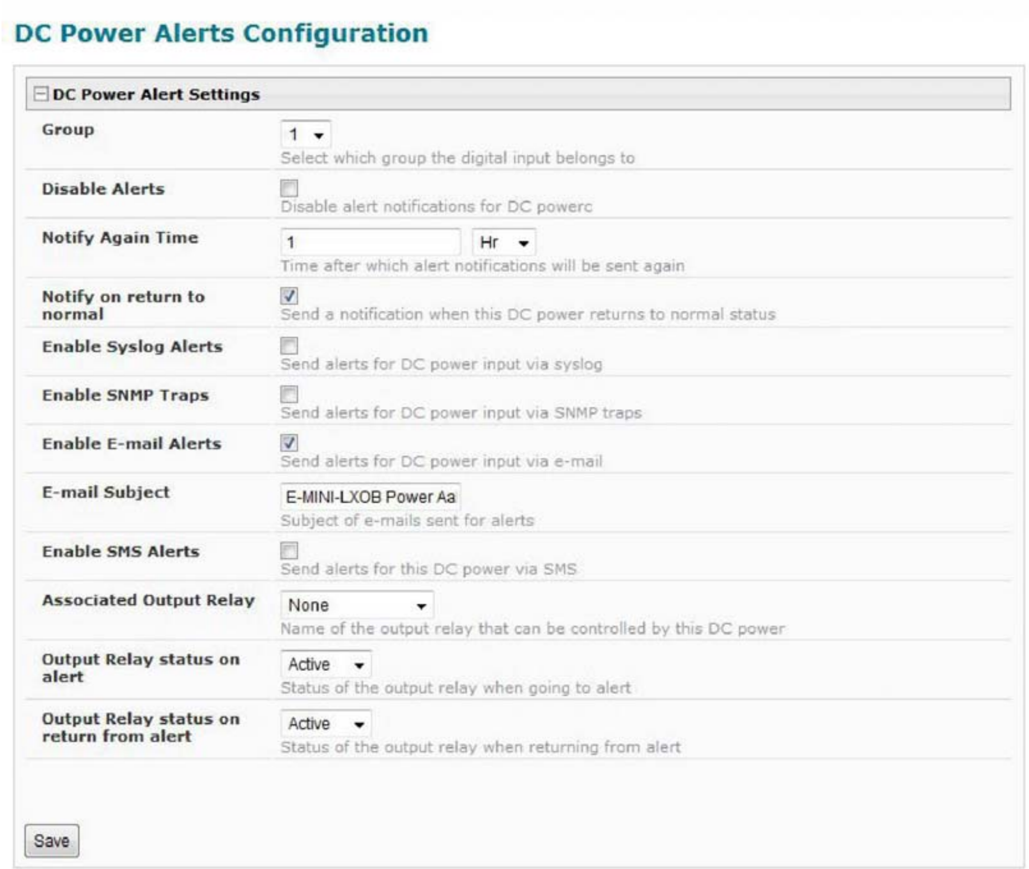
On the Summary Page (under Monitoring), the status of the DC power supply can be found (only applicable for models with battery backup). The EMS200 will monitor the power coming into the EMS200 and can be configured to send an alert in the event that power supply fails. Click on “Edit” to configure how the EMS200 should respond.



DC Power

Num.	Type	Status	Action
1	DC Power	Normal	Edit

Figure 32- Excerpt from the Summary Page showing DC Power monitoring



DC Power Alerts Configuration

⊟ **DC Power Alert Settings**

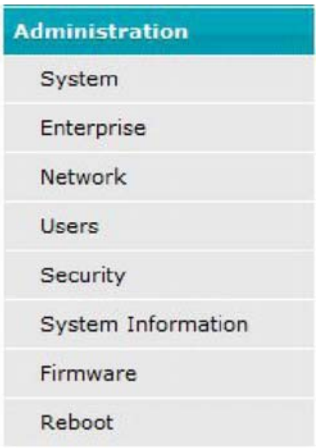
Group	1 ▾	Select which group the digital input belongs to
Disable Alerts	□	Disable alert notifications for DC powerc
Notify Again Time	1 Hr ▾	Time after which alert notifications will be sent again
Notify on return to normal	☑	Send a notification when this DC power returns to normal status
Enable Syslog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

Figure 33- DC Power Alert Configuration

Many of the same options that apply to sensor alerts (page 22) can be configured for DC Power alerts. The battery backup will keep the EMS200 on line for up to 2.3 hours in the event of a power failure.

Administration

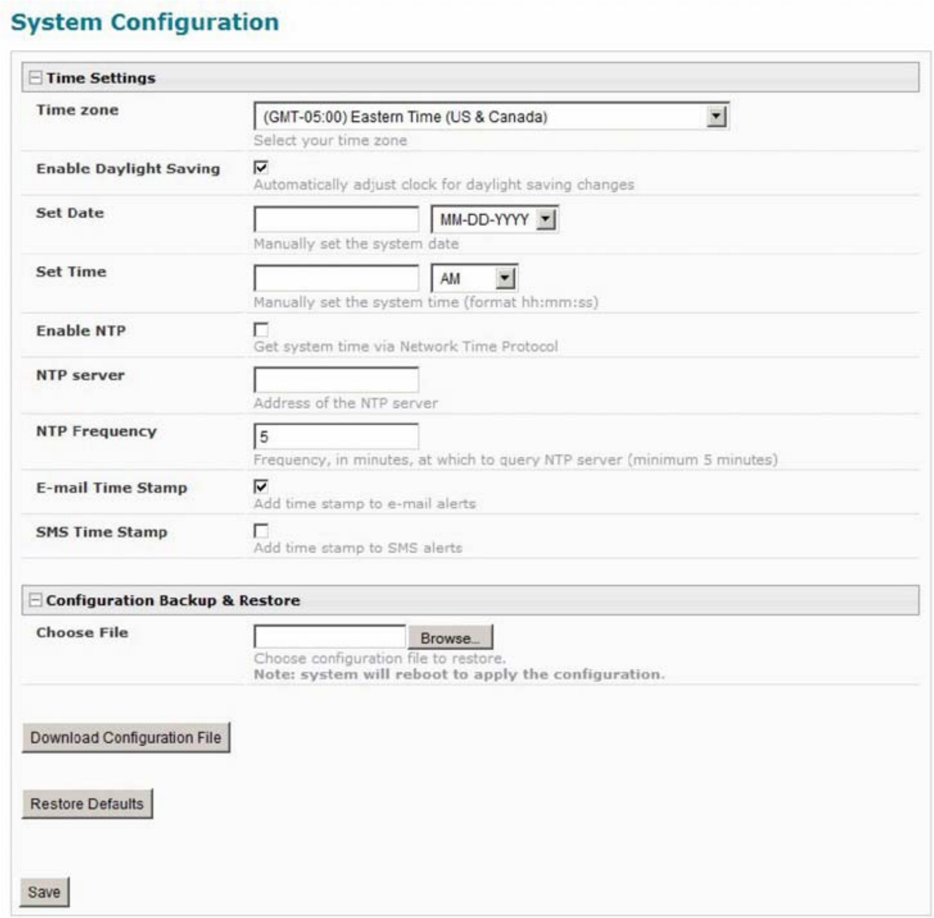
From the Administration section there are several sub sections for configuring the EMS200:



System	Fields for applying time zone, date, time, NTP server, and backup and restore configuration settings
Enterprise	Fields for assigning the unit name, address, contact person, the EMS200 email address, and phone number of a contact person
Network	Fields for providing all the network settings the EMS200 including IP address, DNS, SMTP and SNMP settings
Users	Fields for assigning users, access privileges, passwords, contact settings, and schedule settings
Security	Fields for setting authentication method and IP Filtering
System Information	For viewing EMS200 system information
Firmware	For updating the firmware of the EMS200 when improved software becomes available.
Reboot	Enables user to reboot the EMS200 using the web interface

System Configuration

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



System Configuration

⊟ Time Settings

Time zone	(GMT-05:00) Eastern Time (US & Canada) Select your time zone
Enable Daylight Saving	☑ Automatically adjust clock for daylight saving changes
Set Date	MM-DD-YYYY Manually set the system date
Set Time	AM Manually set the system time (format hh:mm:ss)
Enable NTP	□ Get system time via Network Time Protocol
NTP server	Address of the NTP server
NTP Frequency	5 Frequency, in minutes, at which to query NTP server (minimum 5 minutes)
E-mail Time Stamp	☑ Add time stamp to e-mail alerts
SMS Time Stamp	□ Add time stamp to SMS alerts

⊟ Configuration Backup & Restore

Choose File	Browse... Choose configuration file to restore. Note: system will reboot to apply the configuration.

Figure 34- System Configuration page

The Date and Time of the EMS200 can be either manually setup to use an onboard clock or set to be synchronized with an NTP server. The configuration of the EMS200 can also be easily backed up to a file on your PC and restored from that file as needed.

Time Settings	**Description**
Time Zone	Enter the appropriate time zone
Enable Daylight Saving	Apply a checkmark to have the time change according to Daylight Saving Time rules
Set Date	Enter the system date in MM-DD-YYYY format
Set Time	Enter the system time of day in hh:mm:ss format
Enable NTP	Place a checkmark to enable the EMS200 to automatically sync up with a time server via NTP
NTP server	If the NTP is enabled, enter the Domain Name or IP address of the NTP server
NTP Frequency	Enter the frequency (in minutes) for the EMS200 to query the NTP server (minimum is 5 minutes)
E-mail Time Stamp	Place a checkmark to have the EMS200 apply a time of day stamp in the alert message sent via email
SMS Time Stamp	Place a checkmark to have the EMS200 apply a time of day stamp in the alert message sent via SMS
Configuration Backup & Restore	
Choose file	Browse for a saved configuration file to be restored to the EMS200. Upon selection, the EMS200 will restore the configuration settings and reboot. Allow 1 minute before trying to reconnect and log in again. ***Note: The IP address will be set to the IP address in the file and may be different***
Download Configuration File	Click this button to save the configuration of the EMS200 to a location on your PC. This file can be restored using the "Choose file" field in the event you wish to return the EMS200 to a former state
Restore Defaults	Click this button to restore the EMS200 to the configuration settings it had upon receipt from the factory. **Be careful!** This will erase all user configuration settings. Upon restoration, the EMS200 will reboot. Allow 1 minute before trying to reconnect and log in again. **Confirmation is required**.

Note: If "Restore Defaults" is used, the IP address will also be restored to its default address of 192.168.1.21 with a login name "root" and password "nti". To restore the root password to "nti" without having to restore all default settings, contact NTI for assistance.

To identify the IP address of the EMS200 without restoring defaults, use the Discovery Tool (page 17). Click on

Save when finished with Time Setting changes.

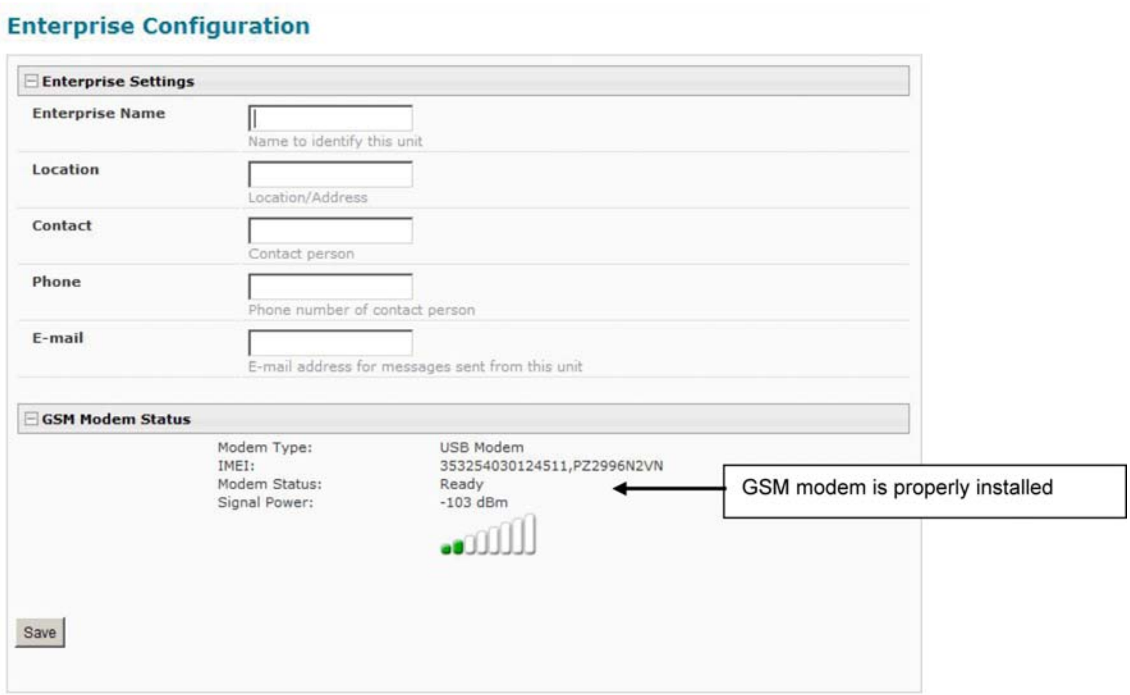
Default settings can also be restored using the "Restore Defaults" button on the front of the EMS200 (page 101) or through the serial interface via text menu (page 78)

Enterprise Configuration

The Enterprise Configuration page is used to enter basic company information to be applied to the body of alerts. To view the Enterprise Configuration, click on **Enterprise** from the **Administration** section of the menu. Enter in the blocks your unit name, location, the contact person that alert e-mails should refer to, the phone number to reach them, and the e-mail address assigned to the EMS200.

If a GSM modem is properly installed (page 14), the "Modem Status" found in the GSM Modem Status section will indicate "Connected" and the IMEI number for the modem will be indicated. Once the modem makes connection with the cell tower, "Connected" will change to "Ready" (as seen below).

Note: It may take several minutes for the GSM modem to be detected by the EMS200.



Enterprise Configuration

⊟ Enterprise Settings

Enterprise Name	Name to identify this unit
Location	Location/Address
Contact	Contact person
Phone	Phone number of contact person
E-mail	E-mail address for messages sent from this unit

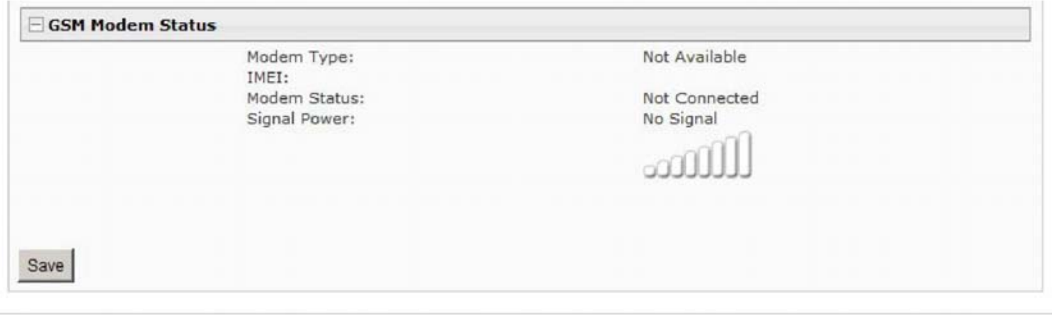
⊟ GSM Modem Status

Modem Type:	USB Modem
IMEI:	353254030124511,PZ2996N2VN
Modem Status:	Ready
Signal Power:	-103 dBm

GSM modem is properly installed

Figure 35- Enterprise Configuration- Modem Status "Ready"

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



⊟ GSM Modem Status

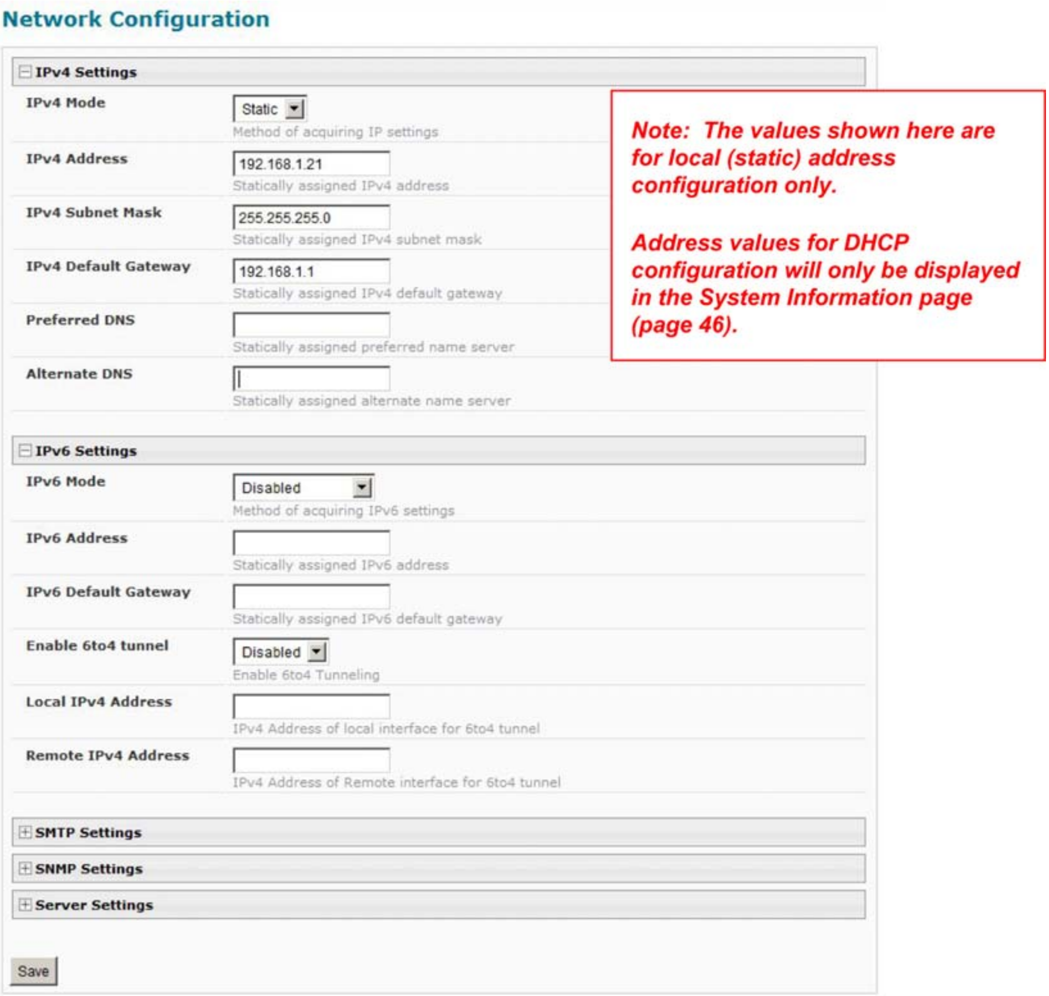
Modem Type:	Not Available
IMEI:	
Modem Status:	Not Connected
Signal Power:	No Signal

Figure 36- No Modem Installed

Network Configuration

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

Note: If you select "DHCP", make sure a DHCP server is running on the network the EMS200 is connected to.



Network Configuration

⊟ IPv4 Settings

IPv4 Mode: Static ▾ — Method of acquiring IP settings

IPv4 Address: 192.168.1.21 — Statically assigned IPv4 address

IPv4 Subnet Mask: 255.255.255.0 — Statically assigned IPv4 subnet mask

IPv4 Default Gateway: 192.168.1.1 — Statically assigned IPv4 default gateway

Preferred DNS: — Statically assigned preferred name server

Alternate DNS: — Statically assigned alternate name server

⊟ IPv6 Settings

IPv6 Mode: Disabled ▾ — Method of acquiring IPv6 settings

IPv6 Address: — Statically assigned IPv6 address

IPv6 Default Gateway: — Statically assigned IPv6 default gateway

Enable 6to4 tunnel: Disabled ▾ — Enable 6to4 Tunneling

Local IPv4 Address: — IPv4 Address of local interface for 6to4 tunnel

Remote IPv4 Address: — IPv4 Address of Remote interface for 6to4 tunnel

⊞ SMTP Settings

⊞ SNMP Settings

⊞ Server Settings

Note: The values shown here are for local (static) address configuration only.

Address values for DHCP configuration will only be displayed in the System Information page (page 46).

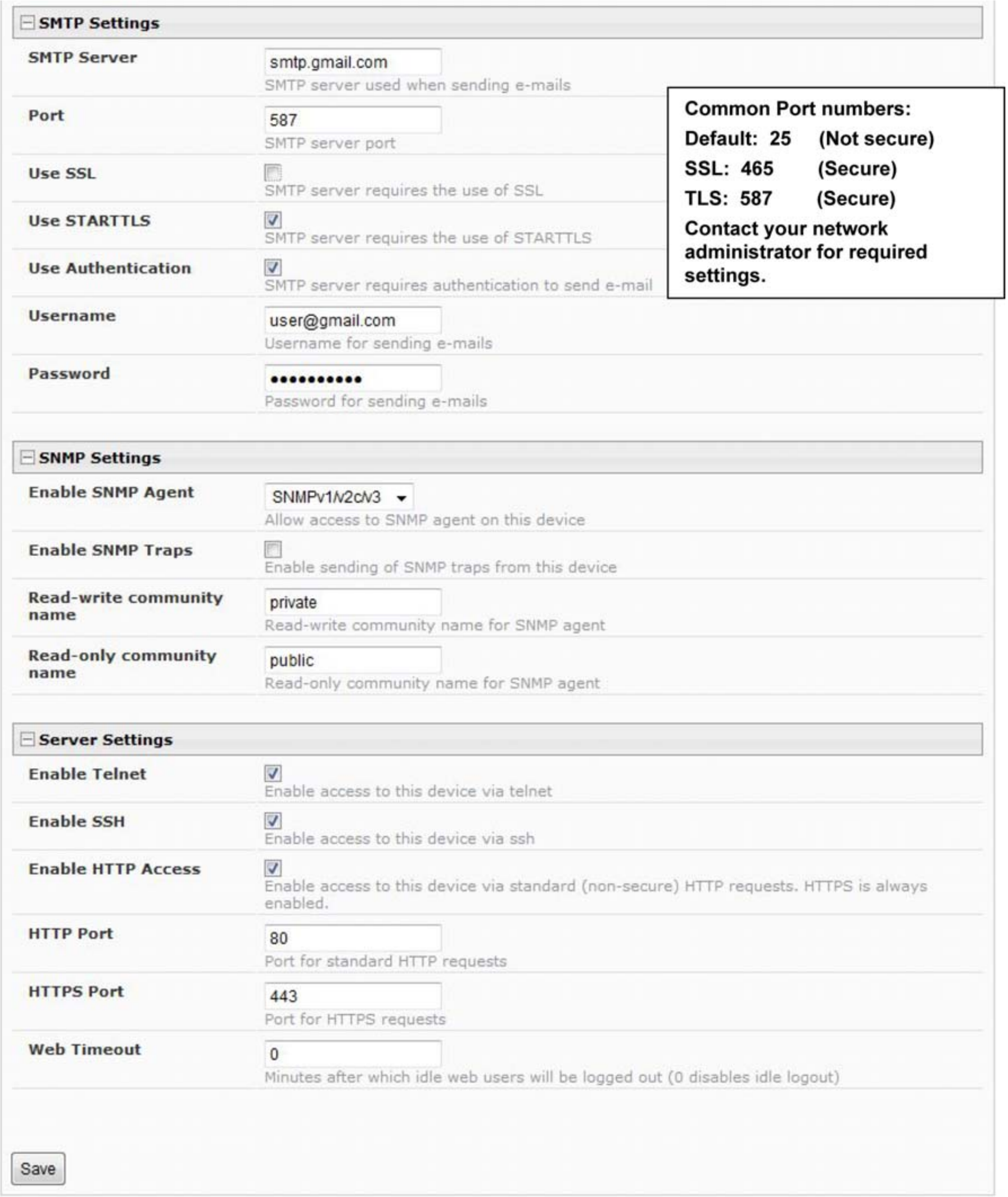
Figure 37- Network Configuration page

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

Enter IPv6 settings as applicable.

For descriptions of SMTP, SNMP, and Server Settings, see page 38.

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



⊟ SMTP Settings

SMTP Server	smtp.gmail.com	SMTP server used when sending e-mails
Port	587	SMTP server port
Use SSL	□	SMTP server requires the use of SSL
Use STARTTLS	☑	SMTP server requires the use of STARTTLS
Use Authentication	☑	SMTP server requires authentication to send e-mail
Username	user@gmail.com	Username for sending e-mails
Password	●●●●●●●●●●●	Password for sending e-mails

Common Port numbers:
Default: 25 (Not secure)
SSL: 465 (Secure)
TLS: 587 (Secure)
Contact your network administrator for required settings.

⊟ SNMP Settings

Enable SNMP Agent	SNMPv1/v2c/v3 ▾	Allow access to SNMP agent on this device
Enable SNMP Traps	□	Enable sending of SNMP traps from this device
Read-write community name	private	Read-write community name for SNMP agent
Read-only community name	public	Read-only community name for SNMP agent

⊟ Server Settings

Enable Telnet	☑	Enable access to this device via telnet
Enable SSH	☑	Enable access to this device via ssh
Enable HTTP Access	☑	Enable access to this device via standard (non-secure) HTTP requests. HTTPS is always enabled.
HTTP Port	80	Port for standard HTTP requests
HTTPS Port	443	Port for HTTPS requests
Web Timeout	0	Minutes after which idle web users will be logged out (0 disables idle logout)

Figure 38- Network Configuration- more settings

More Network Settings (see Figure 38)

SMTP Settings	Description
SMTP Server	Enter a valid SMTP server name (e.g. yourcompany.com)
Port	Enter a valid port number (default port is 25, for SSL most use 465, for STARTTLS most use 587)
Use SSL	Place a checkmark in the box if the SMTP server supports SSL
Use STARTLS	Place a checkmark in the box if the SMTP server supports TLS
Use Authentication	Place a checkmark in the box if the SMTP server requires authentication to send email
Username	Enter a valid username to be used by the EMS200 to send emails
Password	Enter a valid password assigned to the EMS200 username
Enable SNMP agent	Place a checkmark in the box to enable access to the SNMP agent
Enable SNMP traps	Place a checkmark in the box to allow SNMP traps to be sent
Read-write community name	Enter applicable name (commonly used- “private”) **Not applicable as of this printing**
Read-only community name	Enter applicable name (commonly used- “public”)
Enable Telnet	Place a checkmark in the box to enable access to the EMS200 via Telnet **The default is disabled.**
Enable SSH	Place a checkmark in the box to enable access to the EMS200 via SSH
Enabe HTTP access	Place a checkmark in the box to enable access to the EMS200 via standard (non-secure) HTTP requests
HTTP Port	Port to be used for standard HTTP requests
HTTPS Port	Port to be used for HTTPS requests
Web Timeout	Number of minutes after which idle web uses will be logged-out (enter 0 to disable this feature)

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 EMS200.

Note: The SMTP server port number is shown in Figure 38 as "25".   This is a common port number assigned, but not necessarily the port number assigned to your SMTP server.   For SMTP servers that support SSL, the common port number is 465, and for those that support TLS, the common port number is 587.

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

Note: If the port number is changed and forgotten, to determine what it has been changed to connect the EMS200 for control using the text menu (page 59) and review the Miscellaneous Service Settings (page 82).

Read-Only Community Name

The SNMP Read-only community name enables a user to retrieve "read-only" information from the EMS200 using the SNMP browser and MIB file.   This name must be present in the EMS200 and in the proper field in the SNMP browser.

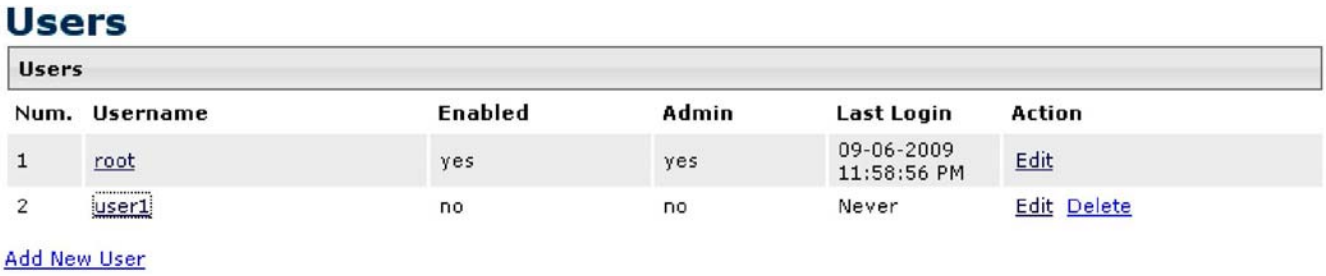
Read-Write Community Name

(not applicable as of this printing)

The SNMP Read-Write community name enables a user to read information from the EMS200 and to modify settings on the EMS200 using the SNMP browser and MIB file. This name must be present in the EMS200 and in the proper field in the SNMP browser.

User Configuration

The Users page is a list of all configured users of the EMS200. A maximum of 15 users (other than root) can be configured. From this page the user can choose to add more users, go to the user configuration page to edit a user's access to the EMS200, or delete a user from the list. To view the Users page, click on **Users** from the **Administration** section of the menu.



Users

Users

Num.	Username	Enabled	Admin	Last Login	Action
1	root	yes	yes	09-06-2009 11:58:56 PM	Edit
2	user1	no	no	Never	Edit Delete

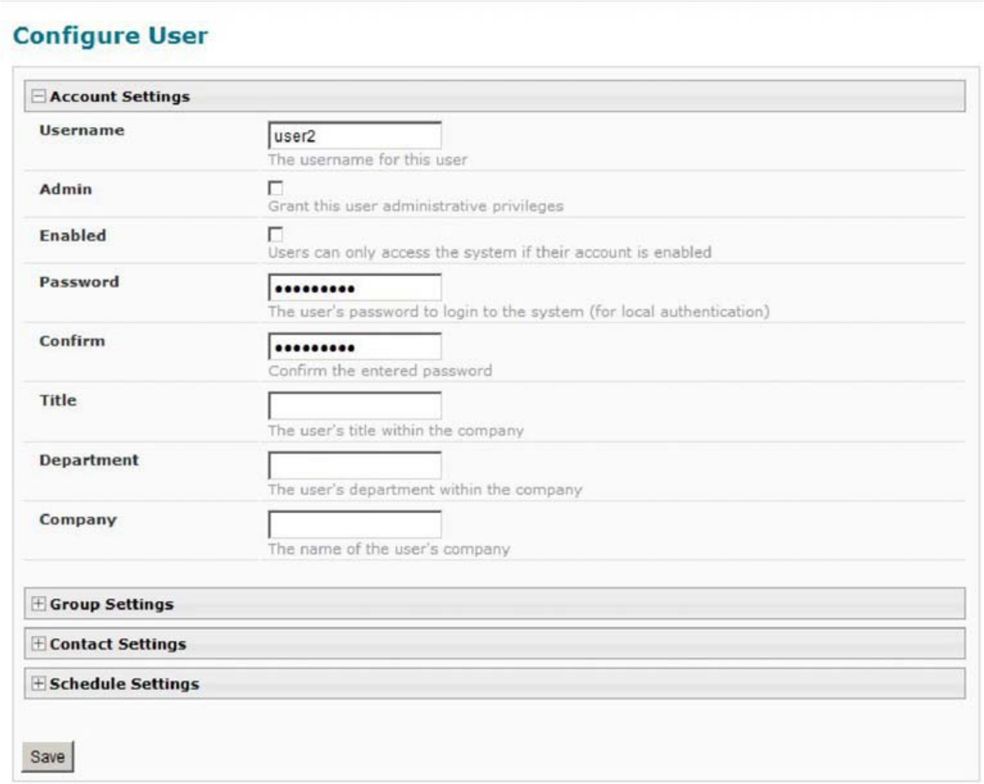
Figure 39- Users page

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

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

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

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

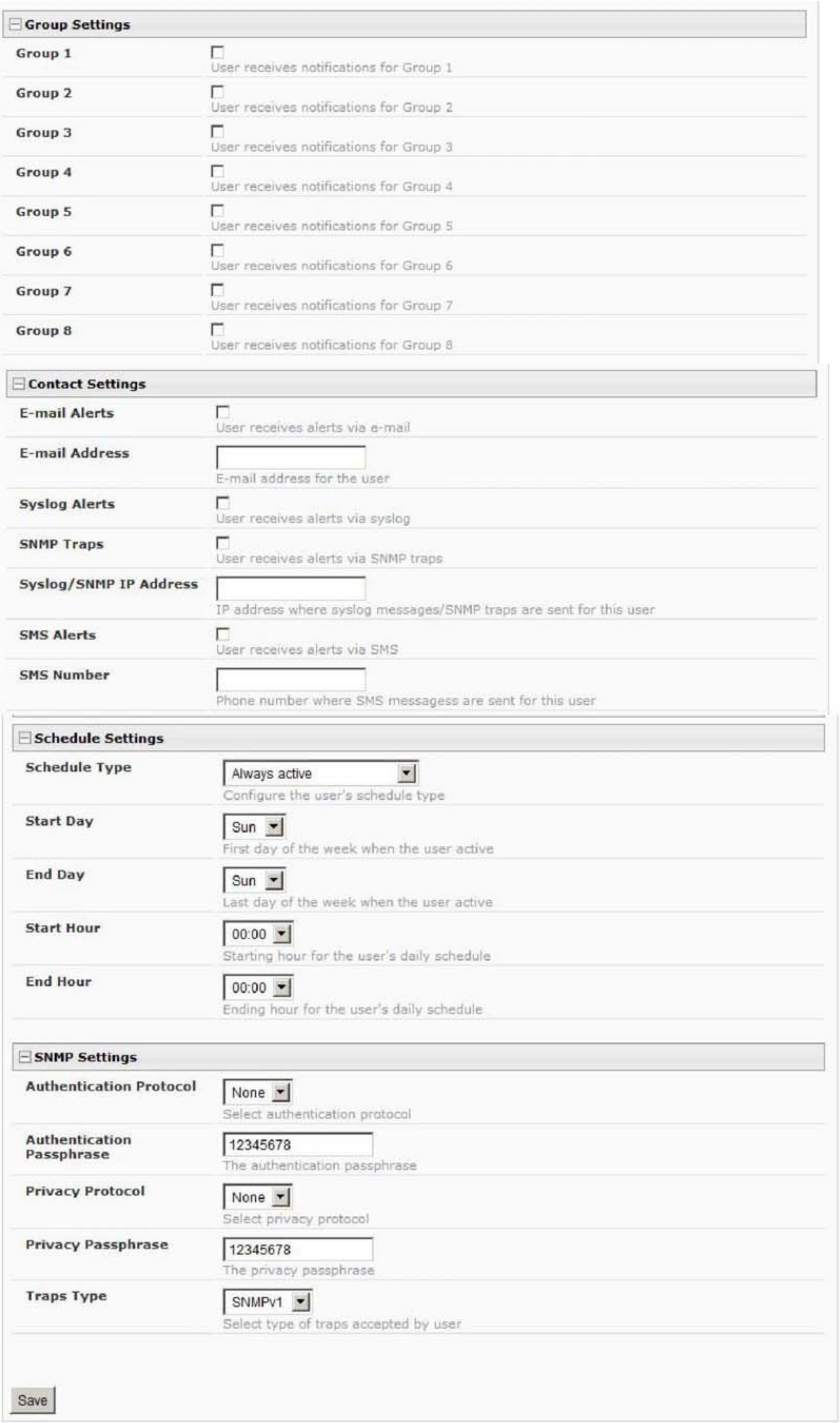


Configure User

⊟ Account Settings

Username	user2	The username for this user
Admin	□	Grant this user administrative privileges
Enabled	□	Users can only access the system if their account is enabled
Password	•••••••••	The user's password to login to the system (for local authentication)
Confirm	•••••••••	Confirm the entered password
Title		The user's title within the company
Department		The user's department within the company
Company		The name of the user's company

Figure 40- Configure Users page



⊟ Group Settings

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

⊟ Contact Settings

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

⊟ Schedule Settings

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

⊟ SNMP Settings

Authentication Protocol	None Select authentication protocol
Authentication Passphrase	12345678 The authentication passphrase
Privacy Protocol	None Select privacy protocol
Privacy Passphrase	12345678 The privacy passphrase
Traps Type	SNMPv1 Select type of traps accepted by user

Figure 41- Configure User- more options

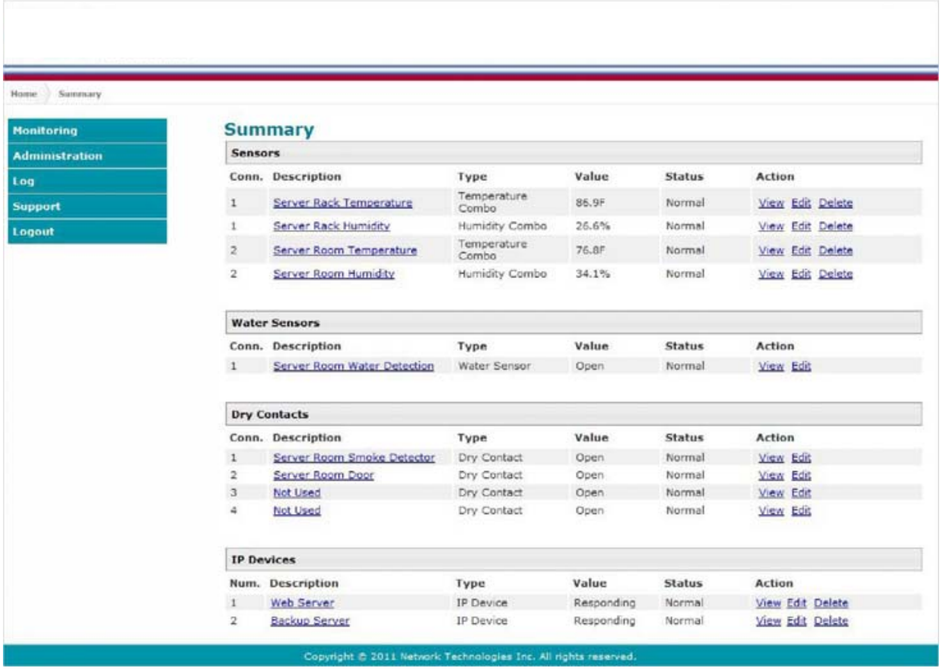
Account Settings	Description
Username	Enter the desired username for this user
Admin	Place a checkmark here if this user should have administrative privileges
Enabled	Place a checkmark here to enable this user to access the EMS200
Password	Enter a password that a user must use to login to the system **A password must be assigned for the user's login to be valid** **Passwords must be at least 1 keyboard character.**
Confirm	Re-enter a password that a user must use to login to the system
Title	Enter information as applicable
Department	Enter information as applicable
Company	Enter information as applicable
Group 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 24 and 28 for group assignments)
Email alerts	Place a checkmark if the user should receive messages via email
Email address	Enter a valid email address if this user should receive email alert messages
Syslog alerts	Place a checkmark if the user should receive alerts via syslog messages
SNMP traps	Place a checkmark if the user should receive alerts via SNMP traps
Syslog/SNMP IP address	Enter a valid syslog/SNMP IP address for the user to receive syslog/SNMP messages
SMS Alerts	Place a checkmark if the user should receive alerts via SMS messages
SMS Number	Enter a phone number for the GSM modem to call to alert the user via SMS message
Schedule Type	**Always active**- user will receive messages at all hours of each day **Active during defined times**- user will only receive alert messages during times as outlined below
Start Day	First day of the week the user should begin receiving messages
End Day	Last day of the week the user should receive messages
Start Hour	First hour of the day the user should begin receiving messages
End Hour	Last hour of the day the user should receive messages
Authentication Protocol	Choose between MD5 or SHA to require authentication, or none to disable it
Authentication Passphrase	Assign the passphrase to be used to enable the receipt of SNMP v3 messages
Privacy Protocol	Choose between DES or AES to encrypt SNMP readings or traps or none to disable encryption. If encryption is enabled, then the Authentication Protocol must also be set at "MD5" or "SHA".
Privacy Passphrase	Assign the passphrase to be used to open and read readings or alert messages received via SNMP v3
Traps Type	Choose between SNMPv1, SNMPv2C, or SNMPv3

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

More about User Privileges

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

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



Summary

Sensors

Conn.	Description	Type	Value	Status	Action
1	Server Rack Temperature	Temperature Combo	86.9F	Normal	View Edit Delete
1	Server Rack Humidity	Humidity Combo	26.6%	Normal	View Edit Delete
2	Server Room Temperature	Temperature Combo	76.8F	Normal	View Edit Delete
2	Server Room Humidity	Humidity Combo	34.1%	Normal	View Edit Delete

Water Sensors

Conn.	Description	Type	Value	Status	Action
1	Server Room Water Detection	Water Sensor	Open	Normal	View Edit

Dry Contacts

Conn.	Description	Type	Value	Status	Action
1	Server Room Smoke Detector	Dry Contact	Open	Normal	View Edit
2	Server Room Door	Dry Contact	Open	Normal	View Edit
3	Not Used	Dry Contact	Open	Normal	View Edit
4	Not Used	Dry Contact	Open	Normal	View Edit

IP Devices

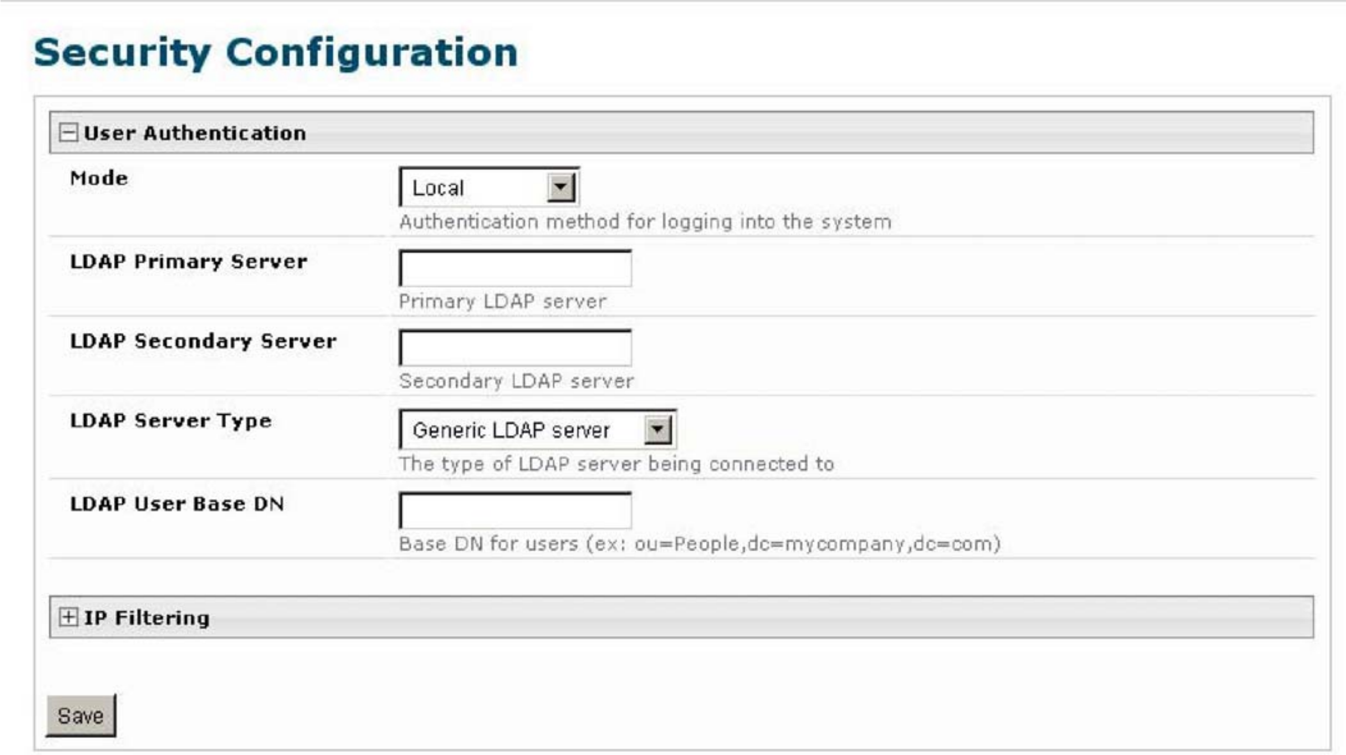
Num.	Description	Type	Value	Status	Action
1	Web Server	IP Device	Responding	Normal	View Edit Delete
2	Backup Server	IP Device	Responding	Normal	View Edit Delete

Copyright © 2011 Network Technologies Inc. All rights reserved.

Figure 42-Summary page for User without Admin privileges

Security

Security in the EMS200 can be managed one of two ways; through the local settings (passwords assigned in user settings on page 41) or through an LDAP server. If security is configured to use LDAP mode, then the passwords for users must be those found on a configured LDAP server. To view the Security Configuration page, select **Security** in the **Administration** section of the menu.



Security Configuration

⊟ User Authentication

Mode: Local
Authentication method for logging into the system

LDAP Primary Server:
Primary LDAP server

LDAP Secondary Server:
Secondary LDAP server

LDAP Server Type: Generic LDAP server
The type of LDAP server being connected to

LDAP User Base DN:
Base DN for users (ex: ou=People,dc=mycompany,dc=com)

⊞ IP Filtering

Figure 43- Security Configuration page

When in LDAP mode, usernames on the LDAP server must match those in the user settings of the EMS200 or access will be denied.

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

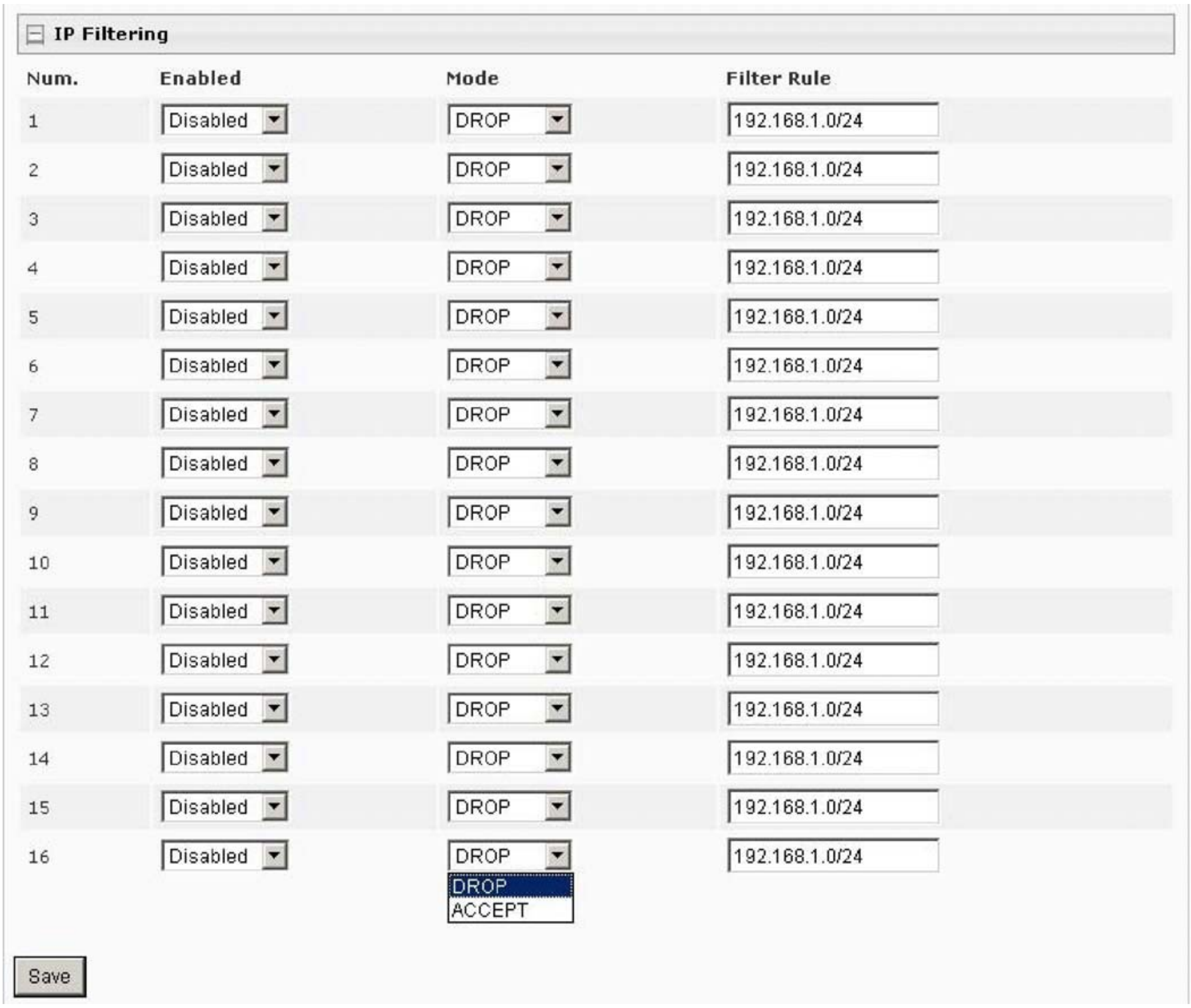
User Authentication Mode	Select Local to use authentication based on passwords in the EMS200 Select LDAP to use authentication based on passwords in an LDAP server	user configuration
LDAP Primary Server	Enter Hostname or IP address of Primary LDAP Server	
LDAP Secondary Server	Enter Hostname or IP address of Secondary LDAP Server (optional)	
LDAP Server Type	Choose from drop down list: Generic LDAP server Novell Directory server Microsoft Active Directory	
LDAP User Base DN	Enter the Base DN for users (ex: ou=People,dc=mycompany,dc=com)	

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

Included in the Security Configuration options is IP Filtering.   IP Filtering provides an additional mechanism for securing the EMS200. Access to the EMS200 network services (SNMP, HTTP(S), SSH, Telnet) can be controlled by allowing or disallowing connections from various IP addresses, subnets, or networks.

Up to 16 IP Filtering rules can be defined to protect the EMS200 from unwanted access from intruders. Each rule can be set as Enabled or Disabled. Rules can be set to explicitly drop attempts to connect, or to accept them.

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



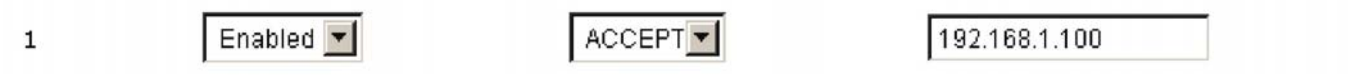
Num.	Enabled	Mode	Filter Rule
1	Disabled	DROP	192.168.1.0/24
2	Disabled	DROP	192.168.1.0/24
3	Disabled	DROP	192.168.1.0/24
4	Disabled	DROP	192.168.1.0/24
5	Disabled	DROP	192.168.1.0/24
6	Disabled	DROP	192.168.1.0/24
7	Disabled	DROP	192.168.1.0/24
8	Disabled	DROP	192.168.1.0/24
9	Disabled	DROP	192.168.1.0/24
10	Disabled	DROP	192.168.1.0/24
11	Disabled	DROP	192.168.1.0/24
12	Disabled	DROP	192.168.1.0/24
13	Disabled	DROP	192.168.1.0/24
14	Disabled	DROP	192.168.1.0/24
15	Disabled	DROP	192.168.1.0/24
16	Disabled	DROP	192.168.1.0/24

Figure 44- Security Configuration- IP Filtering Rules

More on IP Filtering

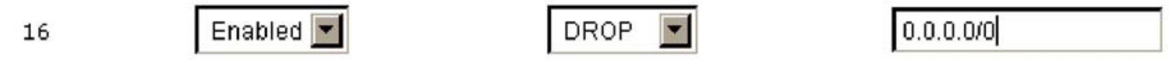
The most common approach is to only allow “white-listed” IP addresses, subnets, or networks to access the device while blocking all others. The IP Filters are processed sequentially from top to bottom, so it is important to place the most precise rules at the top of the list and the most generic rules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

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



1	Enabled	ACCEPT	192.168.1.100

Then, to block all other IP addresses from connecting to the EMS200, we add a rule to drop all other connections.



16	Enabled	DROP	0.0.0.0/0

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

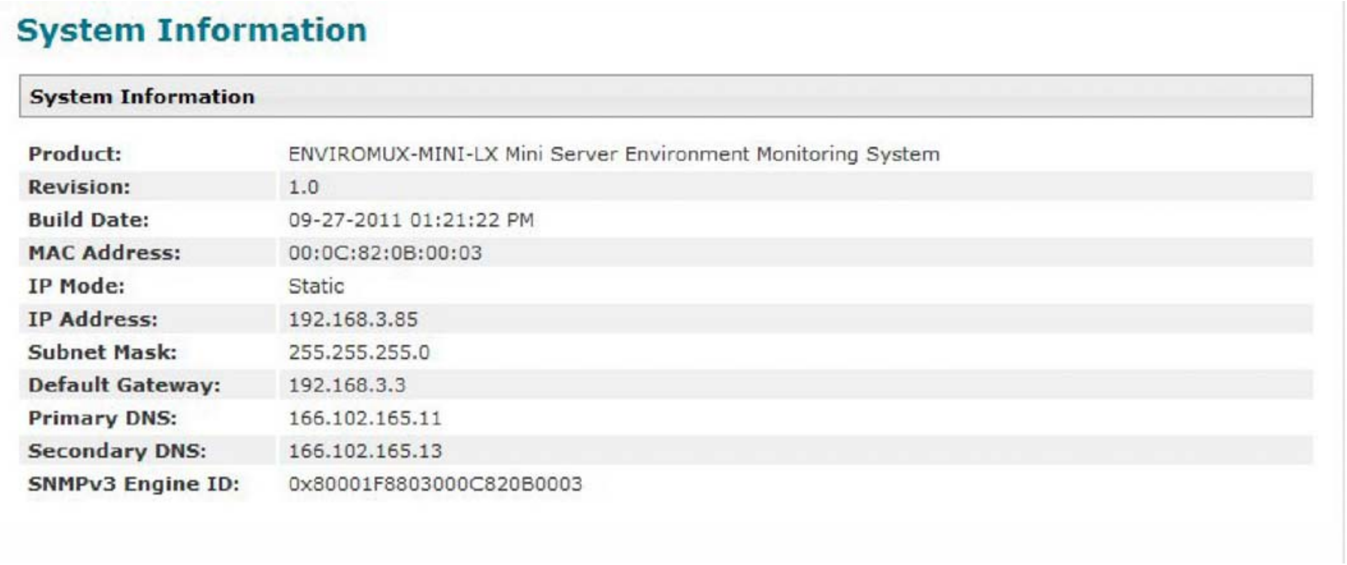
To match a particular IP address, simply enter in the desired IP address (e.g. 192.168.1.100).

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

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

System Information

The system information page displays the model name of the EMS200, the firmware version in the EMS200, the MAC address of the Ethernet port, the IP mode, and the network configuration. To view the System Information, select **System Information** in the **Administration** section of the main menu.



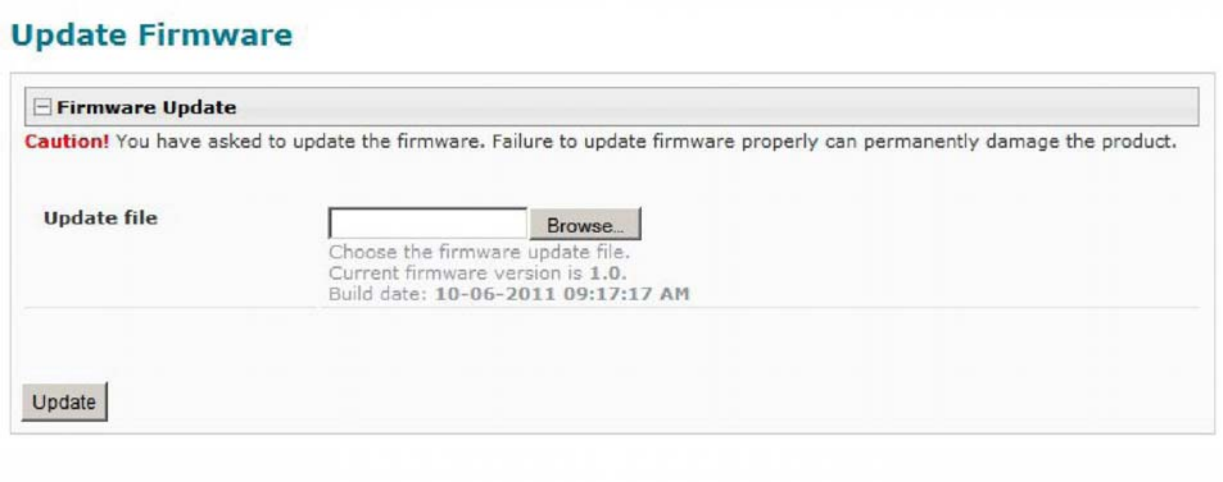
System Information

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

Figure 45- System Information page

Update Firmware

The Update Firmware page is used to change the firmware of the EMS200. Occasionally new features or changes to existing features will be introduced and new firmware with these changes will be made available on the NTI website (http://www.networktechinc.com/download/d-environment-monitoring.html). To view the Update Firmware page, select **Firmware** in the **Administration** section of the main menu. Once a user has downloaded the required file for firmware upgrade, this page will be used to upload it to the EMS200.



Update Firmware

Caution! You have asked to update the firmware. Failure to update firmware properly can permanently damage the product.

Update file

Choose the firmware update file.
Current firmware version is 1.0.
Build date: 10-06-2011 09:17:17 AM

Figure 46- Update Firmware page

1. Download the most current firmware file from http://www.networktechinc.com/download/d-environment-monitoring.html to a location on your PC.
2. Click on the “Browse” button and locate and select the firmware file for the EMS200 (***`EMS200-vx-x.bin, for example`***).
3. Click on the “Update” button to perform the firmware update. The firmware update process will take approximately 5 minutes while the EMS200 installs the firmware. Once the update file has been installed, the unit will automatically reboot and the login screen will appear.

Reboot the System

The EMS200 can be remotely rebooted by anyone with administrative privileges.   To view the Reboot System page, select **Reboot** in the **Administration** section of the main menu.   Click the **Reboot Now** button to cause the EMS200 to reboot. This will disconnect any user and shut down all activity.

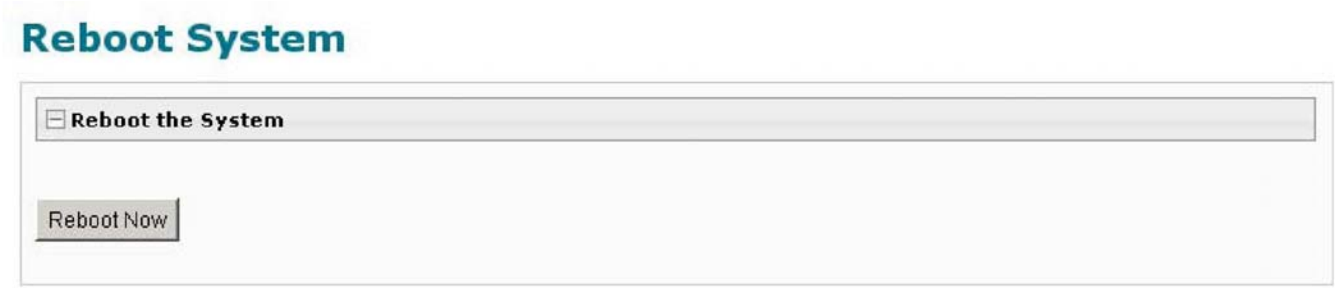
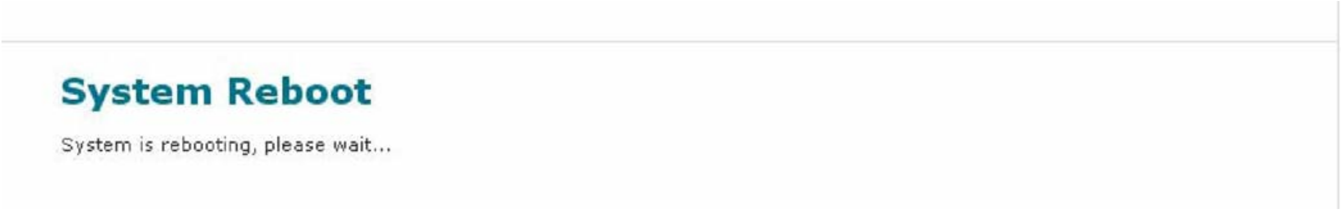


Figure 47- Reboot System page

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



System Reboot

System is rebooting, please wait...

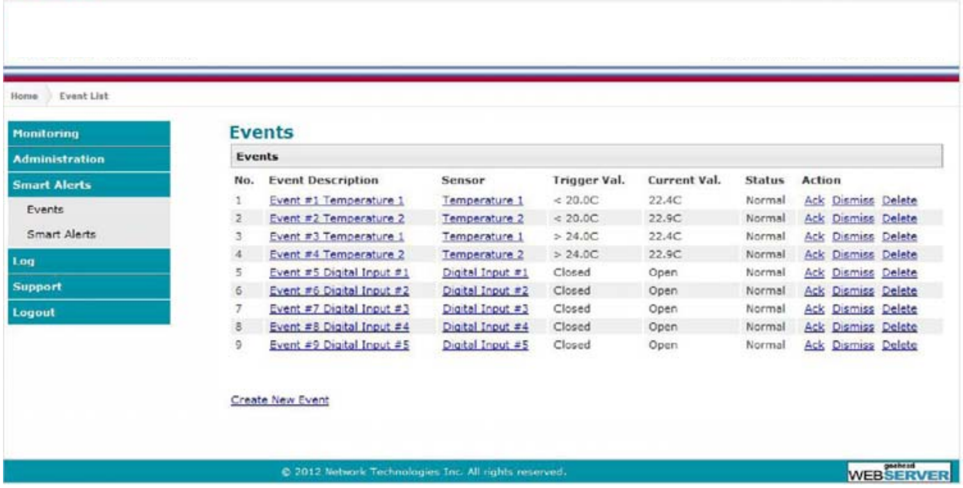
Figure 48- System is rebooting

Smart Alerts

Smart Alerts enable the EMS200 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 22.

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

To begin, Events must be defined and configured. Events are sensor conditions to be notified of. Events logged based on the sensor configurations described on page 22 will be managed separately from events logged by these pre-defined Events. Sensor configuration for these Events will have no impact on the general configuration of your sensors. Pre-defined Events provide more control over what you want to be notified of.



Events

Events

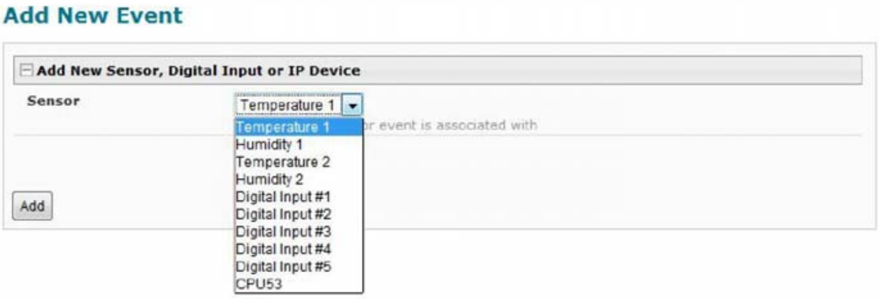
No.	Event Description	Sensor	Trigger Val.	Current Val.	Status	Action
1	Event #1 Temperature 1	Temperature 1	< 20.0C	22.4C	Normal	Ack Dismiss Delete
2	Event #2 Temperature 2	Temperature 2	< 20.0C	22.9C	Normal	Ack Dismiss Delete
3	Event #3 Temperature 1	Temperature 1	> 24.0C	22.4C	Normal	Ack Dismiss Delete
4	Event #4 Temperature 2	Temperature 2	> 24.0C	22.9C	Normal	Ack Dismiss Delete
5	Event #5 Digital Input #1	Digital Input #1	Closed	Open	Normal	Ack Dismiss Delete
6	Event #6 Digital Input #2	Digital Input #2	Closed	Open	Normal	Ack Dismiss Delete
7	Event #7 Digital Input #3	Digital Input #3	Closed	Open	Normal	Ack Dismiss Delete
8	Event #8 Digital Input #4	Digital Input #4	Closed	Open	Normal	Ack Dismiss Delete
9	Event #9 Digital Input #5	Digital Input #5	Closed	Open	Normal	Ack Dismiss Delete

Create New Event

© 2012 Network Technologies Inc. All rights reserved.

Figure 49- Events used for Smart Alerts

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



Add New Event

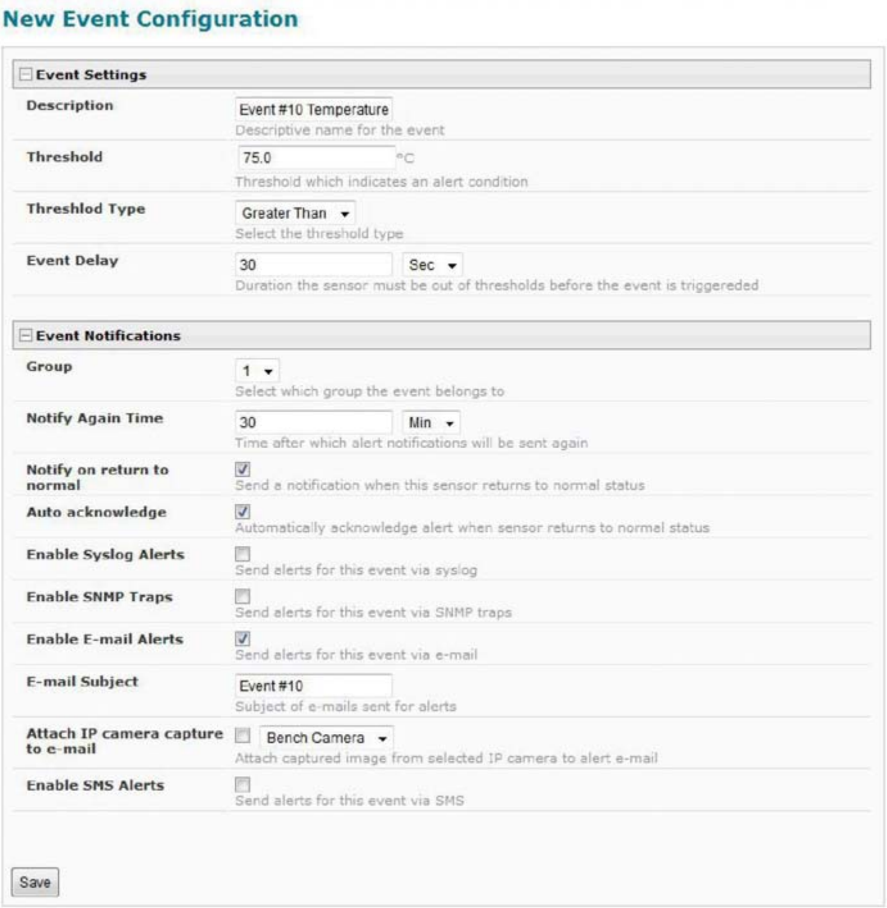
⊟ Add New Sensor, Digital Input or IP Device

Sensor: Temperature 1

…r event is associated with

Figure 50- Sensor to be used for a predefined event

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



New Event Configuration

⊟ Event Settings

Description: Event #10 Temperature
Descriptive name for the event

Threshold: 75.0 °C
Threshold which indicates an alert condition

Threshlod Type: Greater Than
Select the threshold type

Event Delay: 30 Sec
Duration the sensor must be out of thresholds before the event is triggereded

⊟ Event Notifications

Group: 1
Select which group the event belongs to

Notify Again Time: 30 Min
Time after which alert notifications will be sent again

Notify on return to normal: ☑
Send a notification when this sensor returns to normal status

Auto acknowledge: ☑
Automatically acknowledge alert when sensor returns to normal status

Enable Syslog Alerts: □
Send alerts for this event via syslog

Enable SNMP Traps: □
Send alerts for this event via SNMP traps

Enable E-mail Alerts: ☑
Send alerts for this event via e-mail

E-mail Subject: Event #10
Subject of e-mails sent for alerts

Attach IP camera capture to e-mail: □ Bench Camera
Attach captured image from selected IP camera to alert e-mail

Enable SMS Alerts: □
Send alerts for this event via SMS

Figure 51- Configuration options for new event

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

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

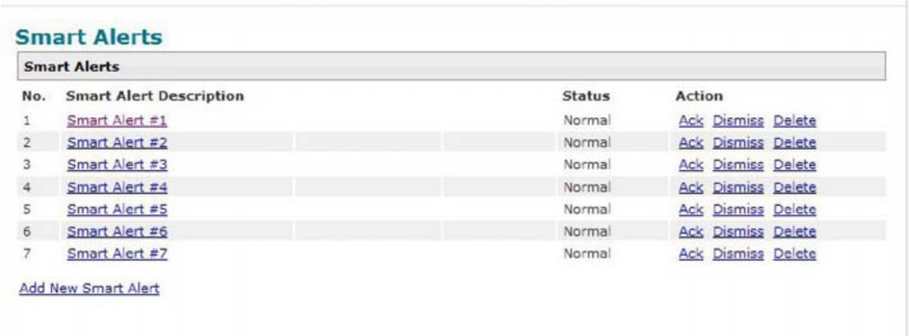
Event Notifications can then be configured to be sent, with the options described in the following table.

Event Settings	
Description	The description of the sensor that will be viewed in the Summary page and in the body of alert messages
Threshold (for RJ45 sensors)	The threshold value of the measured unit that will trigger an event ***Note: The trigger value can be a value that is considered a sensor's "normal" state, or its "alert" state.***
Threshold Type	The type of variation from the threshold value that indicates a condition (greater than or less than)
Trigger Status (for digital inputs)	The condition of the sensor that indicates a triggered state (open or closed)
Event Delay	The amount of time the event must be triggered before an event is logged. This provides some protection against false alarms. The Event Delay value can be set for 0-999 seconds or minutes.
Group	Assign the Event to any group 1 -8 (see also page 39)
Notify Again Time	Enter the amount of time in seconds, minutes, or hours (1-999) before an alert message will be repeated
Notify on Return to Normal	The user can also be notified when the Event has returned to a non-triggered state by selecting the "***Notify when return to normal***" box for an Event.

Event Notification Settings (Continued)	
Auto Acknowledge	Place a checkmark in this box to have alert notifications in the summary page return to normal state automatically when an Event is no longer being triggered.
Enable Syslog Alerts	Place a checkmark in this box to have alert notifications sent via Syslog messages
Enable SNMP traps	Place a checkmark in this box to have alert notifications sent via SNMP traps (v2c)
Enable Email Alerts	Place a checkmark in this box to have alert notifications sent via Email
Email Subject	Enter the subject to be viewed when an email alert message is received
Attach IP Camera capture to email	Associate an Event with an IP camera. Select an IP camera from the drop-down box. An image will be captured and sent with the alert message when an alert is sent via e-mail. IP cameras that are monitored by the EMS200 (page 31) will be available for this purpose. ***Note: To be able to send IP camera captures as e-mail attachments, viewer security (in your camera's configuration) needs to be disabled. Consult your IP camera manual to see if this feature is present and for instructions on how to do this.***
Enable SMS Alerts	Place a checkmark in this box to have alert notifications sent via SMS messages (requires a modem)

After all options are selected, click the “Save” button. This Event will now be added to the Events page (Figure 49). Up to 50 events can be defined. Events can be configured to trigger alerts by themselves, and/or be used in combination with other events to trigger Smart Alerts.

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



Smart Alerts

Smart Alerts

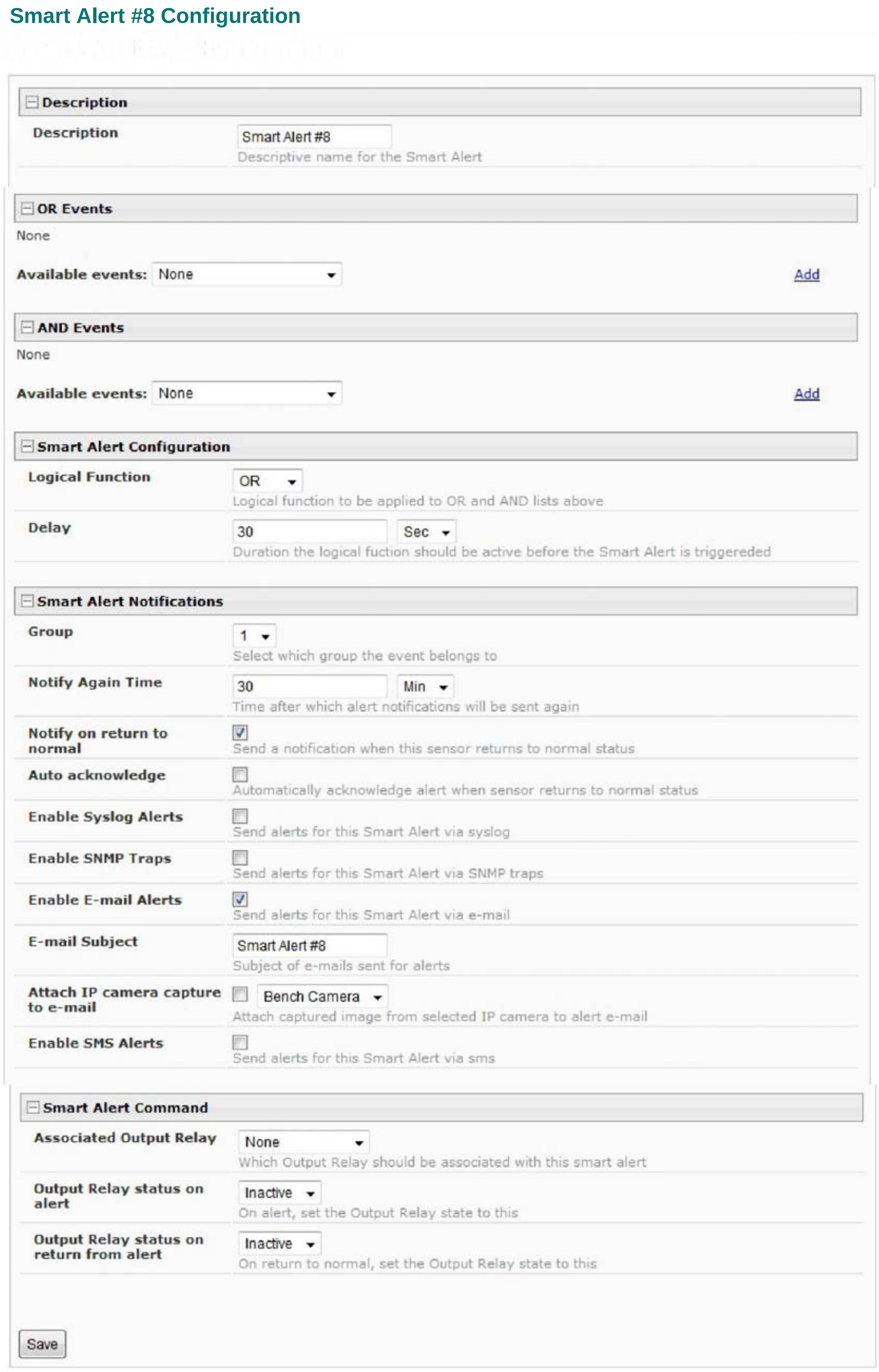
No.	Smart Alert Description	Status	Action
1	Smart Alert #1	Normal	Ack Dismiss Delete
2	Smart Alert #2	Normal	Ack Dismiss Delete
3	Smart Alert #3	Normal	Ack Dismiss Delete
4	Smart Alert #4	Normal	Ack Dismiss Delete
5	Smart Alert #5	Normal	Ack Dismiss Delete
6	Smart Alert #6	Normal	Ack Dismiss Delete
7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

Add New Smart Alert

Figure 52- Smart Alert summary page

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

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



Smart Alert #8 Configuration

⊟ Description

Description: Smart Alert #8
Descriptive name for the Smart Alert

⊟ OR Events

None

Available events: None ▾ Add

⊟ AND Events

None

Available events: None ▾ Add

⊟ Smart Alert Configuration

Logical Function: OR ▾
Logical function to be applied to OR and AND lists above

Delay: 30 Sec ▾
Duration the logical fuction should be active before the Smart Alert is triggereded

⊟ Smart Alert Notifications

Group: 1 ▾
Select which group the event belongs to

Notify Again Time: 30 Min ▾
Time after which alert notifications will be sent again

Notify on return to normal: ☑
Send a notification when this sensor returns to normal status

Auto acknowledge: □
Automatically acknowledge alert when sensor returns to normal status

Enable Syslog Alerts: □
Send alerts for this Smart Alert via syslog

Enable SNMP Traps: □
Send alerts for this Smart Alert via SNMP traps

Enable E-mail Alerts: ☑
Send alerts for this Smart Alert via e-mail

E-mail Subject: Smart Alert #8
Subject of e-mails sent for alerts

Attach IP camera capture to e-mail: □ Bench Camera ▾
Attach captured image from selected IP camera to alert e-mail

Enable SMS Alerts: □
Send alerts for this Smart Alert via sms

⊟ Smart Alert Command

Associated Output Relay: None ▾
Which Output Relay should be associated with this smart alert

Output Relay status on alert: Inactive ▾
On alert, set the Output Relay state to this

Output Relay status on return from alert: Inactive ▾
On return to normal, set the Output Relay state to this

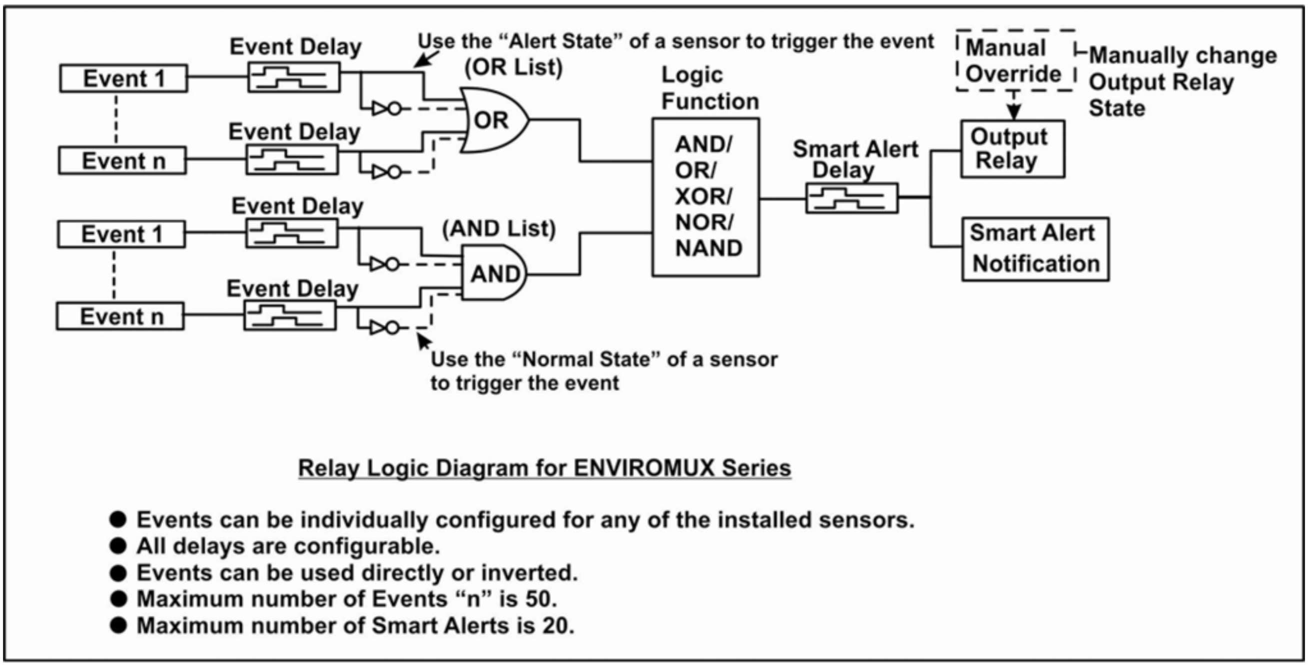
Save

Figure 53- Smart Alert configuration

DESCRIPTION	
Description	Use the default description provided or enter the description you want to see on notifications received.
OR Events	
Available Events	Select from the predefined available Events (Figure 49) to have OR logic applied to a triggered Event
Available Events	Select from the predefined available Events (Figure 49) to have AND logic applied to a triggered Event
Logical Function	Logical function to be applied to the output of the logical status of the OR and AND lists to determine when a Smart Alert should be generated. Options include OR, AND, XOR, NOR and NAND
Delay	The amount of time the Smart Alert Event status must be in an alert condition before a Smart Alert message is triggered. This provides some protection against false alarms. The Delay value can be set for 0-999 seconds or minutes.
Group	Assign the Smart Alert to any group 1 -8 (see also page 39)
Notify Again Time	Enter the amount of time in seconds, minutes, or hours (1-999) before an alert message will be repeated
Notify on Return to Normal	The user can also be notified when the Smart Alert conditions have returned to the normal (non-triggered state) by selecting the "***Notify when return to normal***" box.
Auto Acknowledge	Place a checkmark in this box to have alert notifications in the summary page return to normal state automatically when Smart Alert conditions return to normal.
Enable Syslog Alerts	Place a checkmark in this box to have alert notifications sent via Syslog messages
Enable SNMP traps	Place a checkmark in this box to have alert notifications sent via SNMP traps (v2c)
Enable Email Alerts	Place a checkmark in this box to have alert notifications sent via Email
Email Subject	Enter the subject to be viewed when an email alert message is received
Attach IP Camera capture to email	Associate a Smart Alert with an IP camera. Select an IP camera from the drop-down box. An image will be captured and sent with the alert message when an alert is sent via e-mail. IP cameras that are monitored by the EMS200 (page 31) will be available for this purpose. ***Note: To be able to send IP camera captures as e-mail attachments, viewer security (in your camera's configuration) needs to be disabled. Consult your IP camera manual to see if this feature is present and for instructions on how to do this.***
Enable SMS Alerts	Place a checkmark in this box to have alert notifications sent via SMS messages (requires a modem)
Smart Alert Command	
Associated Output Relay	Associate the Smart Alert with the operation of the output relay, or not ***Note: Only one sensor or Smart Alert should be associated with the Output Relay at a time. Contradicting commands from two or more sensors or Smart Alerts will result in the output relay responding to the state directed by the last command received.***
Output Relay Status on Alert	State the output relay will be in when a Smart Alert is triggered
Output Relay Status on Return from Alert	State the output relay will be in when a Smart Alert is no longer being triggered

More on Logical Functions

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



- Events can be individually configured for any of the installed sensors.
- All delays are configurable.
- Events can be used directly or inverted.
- Maximum number of Events "n" is 50.
- Maximum number of Smart Alerts is 20.

Figure 54- Event Logical Function Diagram

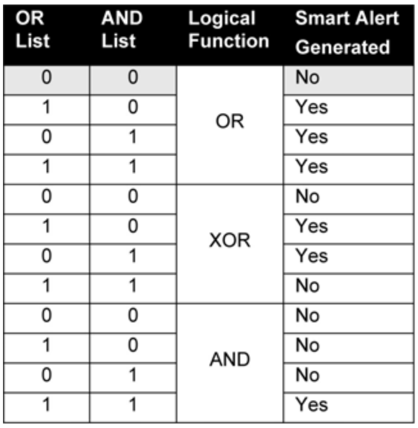
Smart Alert Rules:

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

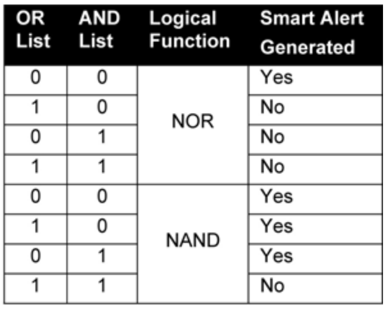
  - If **any** Event in the OR list is triggered, the output value of the OR list will be 1.

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

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



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



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

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

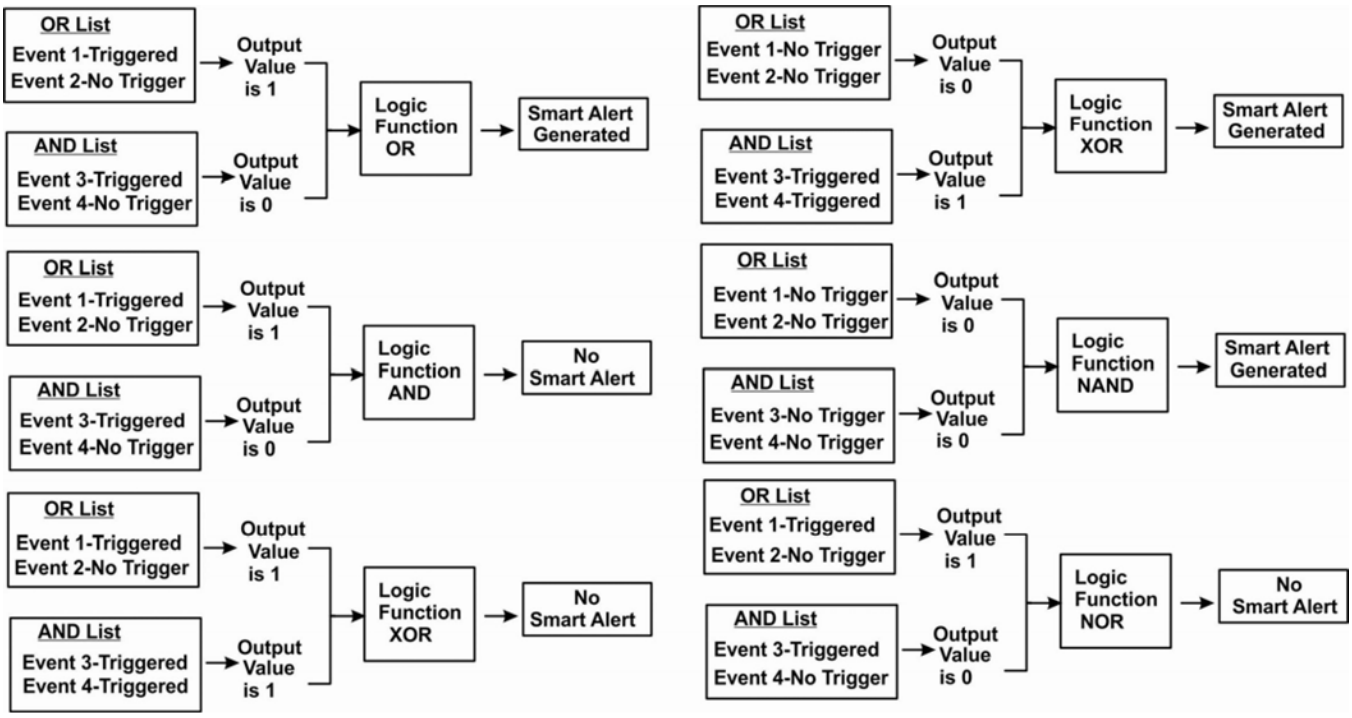
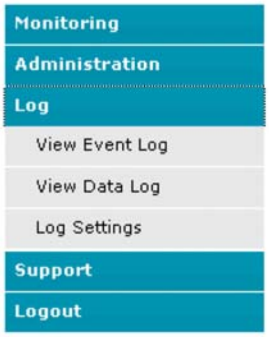


Figure 55- Examples of Smart Alert conditions

Log

From the Log section there are three sub sections for configuring the EMS200:

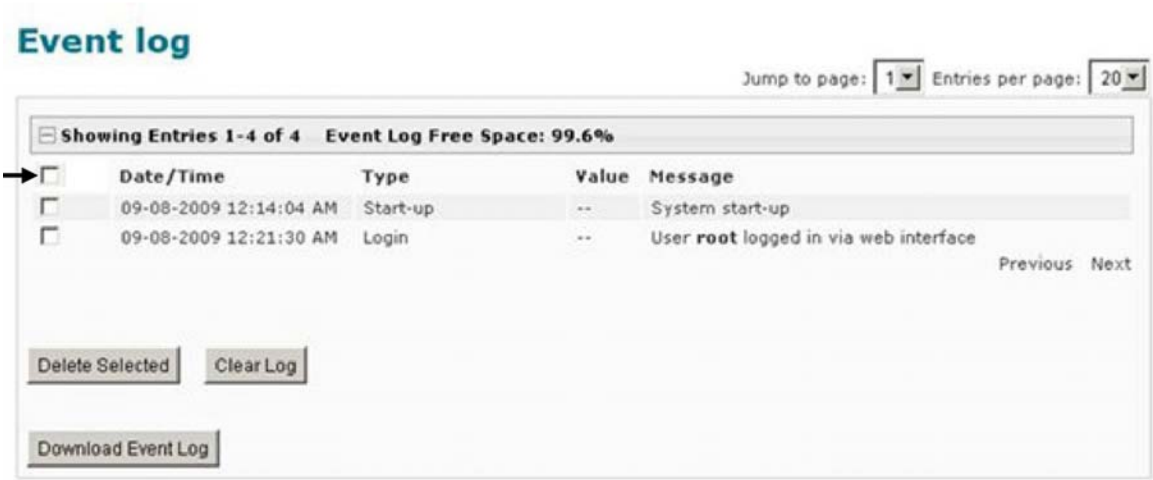


View Event Log	View a log listing the date and time of events such as startups, shut downs, user logins
View Data Log	View data readings from sensors and IP addresses
Log Settings	Configure how the logs are sent to users, how they handle reaching capacity, which users will be notified that it has reached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

View Event Log

The Event Log provides the administrative user with a listing of many events that occur within the EMS200. The event log will record the date and time of:

- each EMS200 startup,
- each user login and logout time,
- any time an unknown user tries to login,
- sensor and IP device alerts
- an alert handled by a user



Event log

Jump to page: 1 Entries per page: 20

Showing Entries 1-4 of 4 Event Log Free Space: 99.6%

□	Date/Time	Type	Value	Message
□	09-08-2009 12:14:04 AM	Start-up	--	System start-up
□	09-08-2009 12:21:30 AM	Login	--	User **root** logged in via web interface

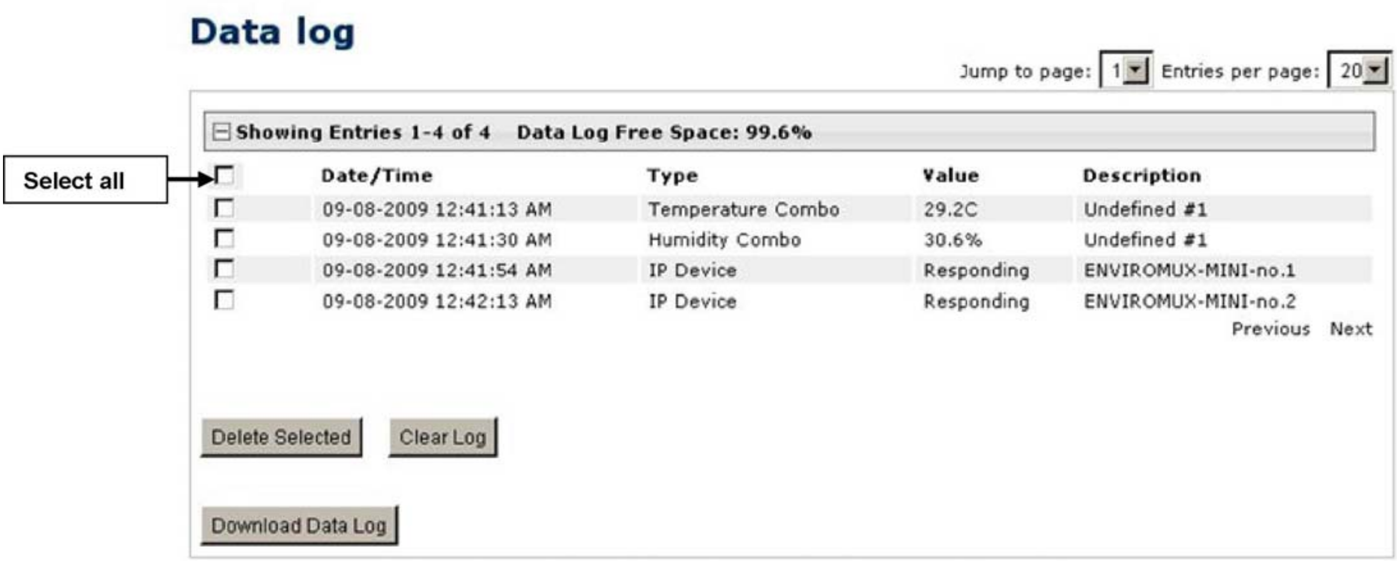
Figure 56- Event Log page

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

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

View Data Log

The Data Log provides the administrative user with a listing of all the readings taken by the EMS200 pertaining to the sensors and IP Devices being monitored. The event log will record the date and time of each reading.



Data log

Jump to page: 1 Entries per page: 20

⊟ Showing Entries 1-4 of 4 Data Log Free Space: 99.6%

□	Date/Time	Type	Value	Description
□	09-08-2009 12:41:13 AM	Temperature Combo	29.2C	Undefined #1
□	09-08-2009 12:41:30 AM	Humidity Combo	30.6%	Undefined #1
□	09-08-2009 12:41:54 AM	IP Device	Responding	ENVIROMUX-MINI-no.1
□	09-08-2009 12:42:13 AM	IP Device	Responding	ENVIROMUX-MINI-no.2

Figure 57- Data Log page

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

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

Log Settings

The Log Settings page (Figure 58) provides settings for how the EMS200 will react when its Data and Event logs reach capacity.

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

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

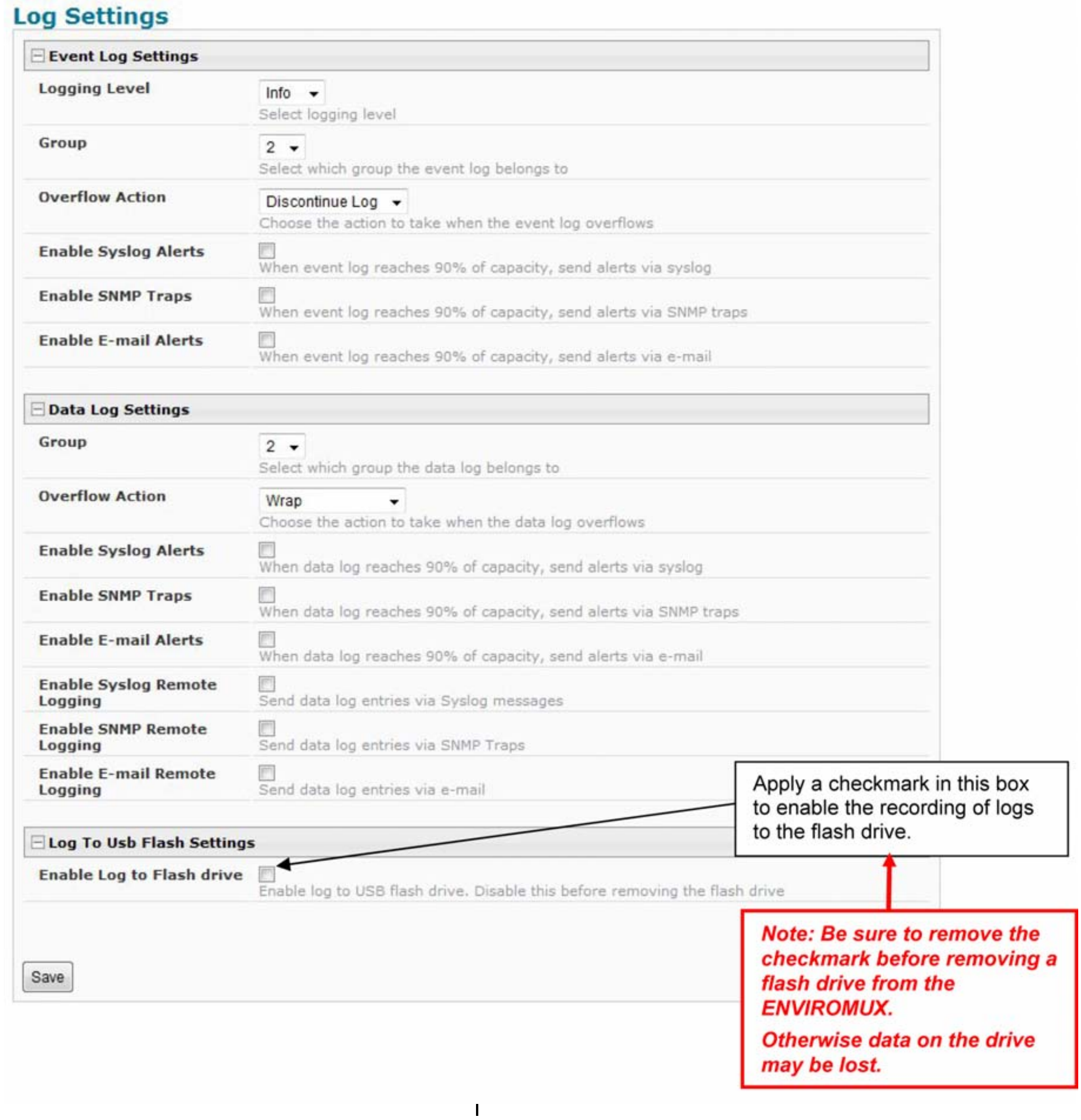
Each log can be assigned to a group and any user that receives messages from that group can be notified when capacity is being reached.

The log can be set to either :

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

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

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



Log Settings

⊟ Event Log Settings

Logging Level: Info ▾ — Select logging level

Group: 2 ▾ — Select which group the event log belongs to

Overflow Action: Discontinue Log ▾ — Choose the action to take when the event log overflows

Enable Syslog Alerts: □ When event log reaches 90% of capacity, send alerts via syslog

Enable SNMP Traps: □ When event log reaches 90% of capacity, send alerts via SNMP traps

Enable E-mail Alerts: □ When event log reaches 90% of capacity, send alerts via e-mail

⊟ Data Log Settings

Group: 2 ▾ — Select which group the data log belongs to

Overflow Action: Wrap ▾ — Choose the action to take when the data log overflows

Enable Syslog Alerts: □ When data log reaches 90% of capacity, send alerts via syslog

Enable SNMP Traps: □ When data log reaches 90% of capacity, send alerts via SNMP traps

Enable E-mail Alerts: □ When data log reaches 90% of capacity, send alerts via e-mail

Enable Syslog Remote Logging: □ Send data log entries via Syslog messages

Enable SNMP Remote Logging: □ Send data log entries via SNMP Traps

Enable E-mail Remote Logging: □ Send data log entries via e-mail

⊟ Log To Usb Flash Settings

Enable Log to Flash drive: □ Enable log to USB flash drive. Disable this before removing the flash drive

Apply a checkmark in this box to enable the recording of logs to the flash drive.

Note: Be sure to remove the checkmark before removing a flash drive from the ENVIROMUX.

Otherwise data on the drive may be lost.

Figure 58- Log Settings page

Log to USB Flash Settings

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

The number of logs that can be recorded depends on the capacity of the flash drive installed. To begin recording to the flash drive, place a checkmark in the "Enable Log to Flash drive" box.   Be sure to remove the checkmark before removing the flash drive from the EMS200 or the data on the drive may be lost.

Support

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

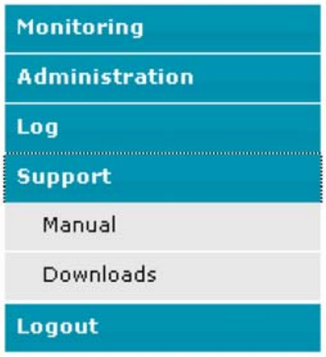


Figure 59- Support

The Manual link will open the pdf manual for the EMS200 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 EMS200 on the NTI website. All versions of firmware and MIB files for the EMS200 will be found there, available for immediate download to your PC.

Logout

To logout of the EMS200 user interface, click on the “Logout” section in the menu. A gray menu label will drop down. Click on the gray label to be immediately logged out. The login screen will appear, at which you can close your browser or log back in.

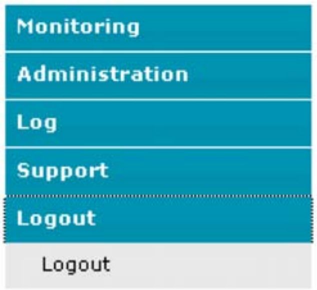


Figure 60- Logout

OPERATION VIA TEXT MENU- EMS200

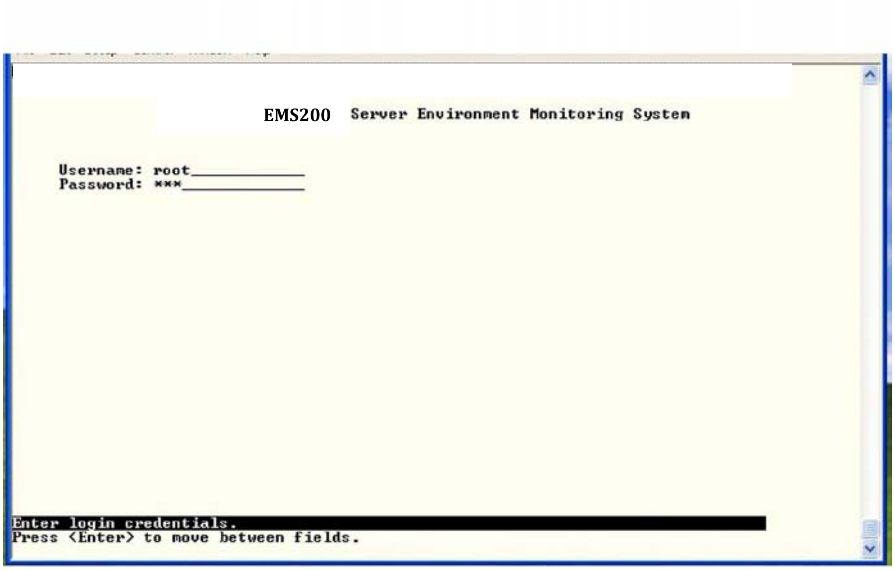
The EMS200 can be controlled through a text menu using a terminal program (e.g. HyperTerminal) connected to the USB Console Port (page 7), or using the Telnet or the SSH protocol provided a connection has been made to the Ethernet Port (page 6). Either of these methods will work to access the EMS200 text menu. The text menu can be used to control all functions of the EMS200 as an alternative to the Web Interface (page 18).

Connect to EMS200 from a Terminal Program

The following instruction will enable the user to quickly make connections using a terminal connected to the "USB CONSOLE" port after the drivers have been loaded (page 7). For instruction to make quick connection using the Ethernet port and Web Interface, see page 18.

Note: Drivers must first be installed on the PC (page 7) before the terminal program and USB CONSOLE port can be used.

1. Make sure the EMS200 is powered ON.
2. Using the serial console device connected to the port labeled "USB CONSOLE", start the terminal program (e.g. Windows HyperTerminal) and configure it as follows:
   - direct connection (using the appropriate CPU local serial Com port)
   - 115200 bps
   - 8 bits
   - no parity
   - 1 stop bit
   - no flow control
   - VT100 terminal mode.
3. Press <**Enter**> and a login prompt will appear- "**minilxo login:"** , type <**root**> (all lowercase letters) and press <Enter>.
4. At "Username: " type <**root**> (all lowercase letters) and press <**Enter**>.
5. At "Password" type <**nti**> (all lowercase letters) and press <**Enter**>.



```
                    EMS200  Server Environment Monitoring System


     Username: root____________
     Password: ***_____________





Enter login credentials.
Press <Enter> to move between fields.
```

Figure 61- 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.

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

Connect to EMS200 from Command Line

To access the Text Menu from the command line, the EMS200 must first be connected to the Ethernet (page 6).

Connect Via Telnet

Note: Telnet must be enabled for a connection via Telnet to be possible (page 37)

To open a telnet session to the EMS200, Issue the following command from the command line:

telnet *<EMS200 hostname or IP address>*

<*EMS200 hostname*> is the hostname configured in the workstation where the telnet client will run (through /etc/hosts or DNS table). It can also be just the IP address of the EMS200 (default is 192.168.1.21).

The user will be prompted for username and password to connect to the EMS200.

Connect Via SSH

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

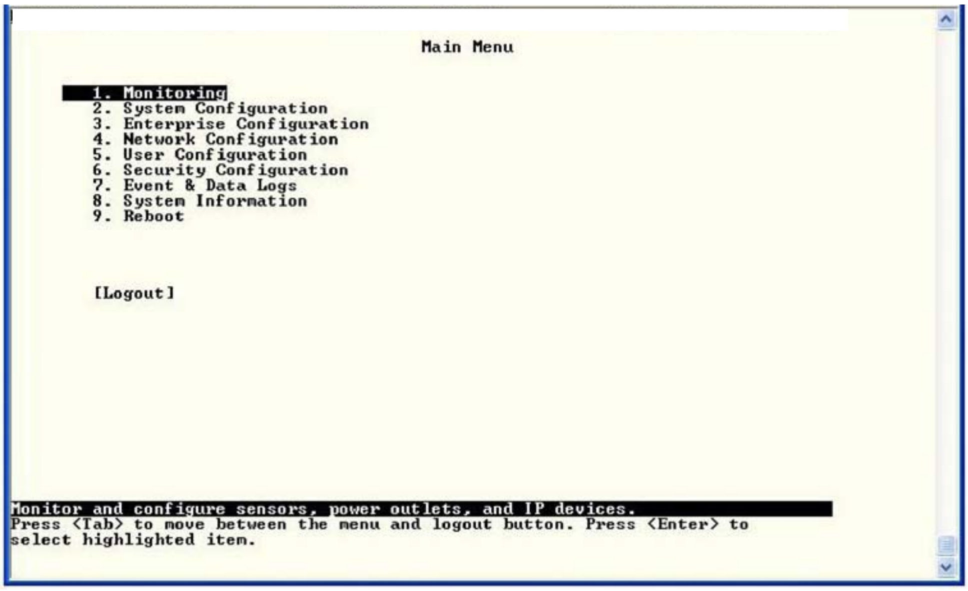
ssh -l *<Username> <EMS200 hostname or IP address>*

<*Username*> is any user configured to access the EMS200 (as defined in the list of users (page 39).

<*EMS200 hostname*> is the hostname configured in the workstation where the SSH client will run (through /etc/hosts or DNS table). It can also be just the IP address of the EMS200 (default is 192.168.1.21).

The user will be prompted for a password to connect to the EMS200.

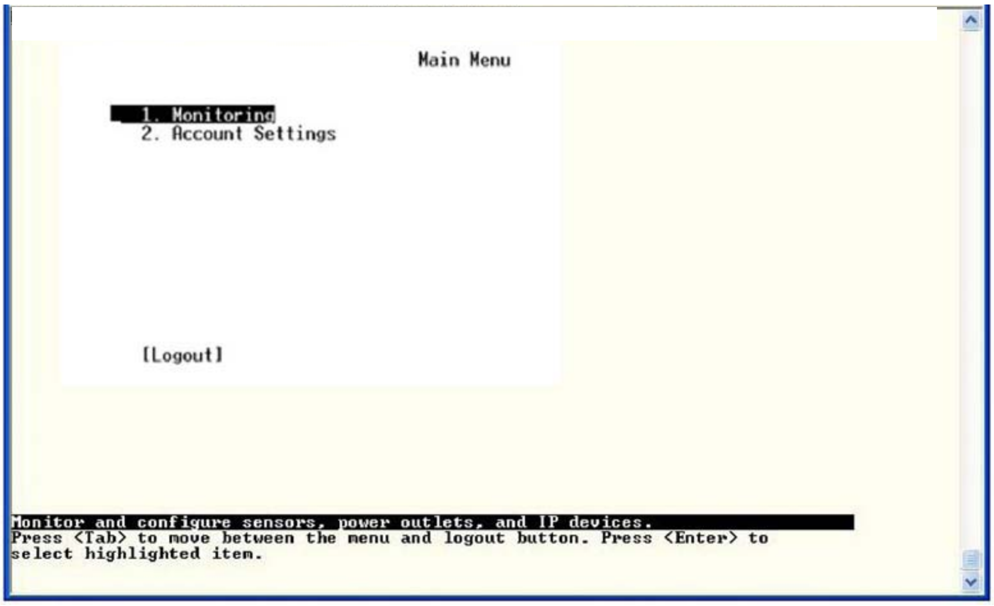
The main menu of the Text Menu will be displayed whether you are connecting via USB Console,Telnet, or SSH.



```
                                 Main Menu

      1. Monitoring
      2. System Configuration
      3. Enterprise Configuration
      4. Network Configuration
      5. User Configuration
      6. Security Configuration
      7. Event & Data Logs
      8. System Information
      9. Reboot


      [Logout]

Monitor and configure sensors, power outlets, and IP devices.
Press <Tab> to move between the menu and logout button. Press <Enter> to
select highlighted item.
```

Figure 62- Text Menu- Administrator Main Menu

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



```
                    Main Menu

   1. Monitoring
   2. Account Settings




   [Logout]


Monitor and configure sensors, power outlets, and IP devices.
Press <Tab> to move between the menu and logout button. Press <Enter> to
select highlighted item.
```

Figure 63- Text Menu- User Main Menu

For more on the Text Menu options for non-administrative users, see page 95.

Using the Text Menu

Text Menu Navigation

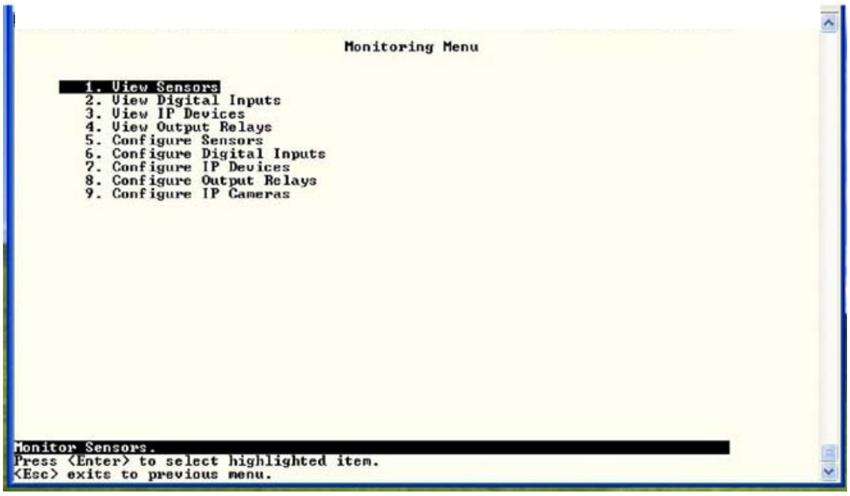
- To move up and down the numbered menu items or toggle through field options, use the arrow keys.
- To jump from menu item to another quickly, press the numbered key above the QWERTY keys (**the numberpad number keys are not used**).
- To move from menu list to action key (such as “Logout” in Figure 63 above), press <`Tab`>.
- To exit an action or menu, press <`Esc`>.
- To select a highlighted item or move to another field in a configuration page, press <`Enter`>.
- Be sure to Tab to “**Save**” and press <`Enter`> when configuration changes are made.
- To return from “Save” back to a field on the configuration page, press <`Tab`>.

The Administrators Main Menu is broken into 9 categories:

Function	**Description**
Monitoring	Monitor and configure the sensors, accessories and IP devices
System Configuration	Set the EMS200 time settings or reset the unit to factory default settings
Enterprise Configuration	Configure system settings
Network Configuration	Configure network settings
User Configuration	Configure user access settings
Security Configuration	Configure security settings
Event and Data Logs	View and configure the Event and Data Logs (page 91)
System Information	View system and network settings
Reboot	Enables the user to reboot the EMS200

Monitoring

The Monitoring menu lists choices for viewing the status of items monitored by the EMS200 as well as for configuring how they are monitored and how or if alert messages will be sent.



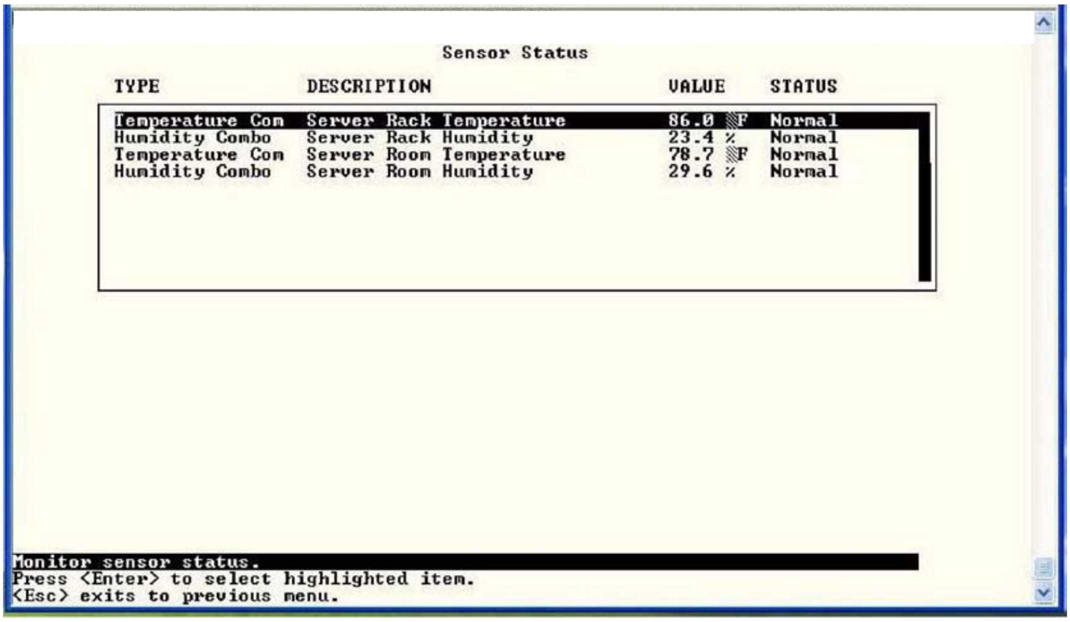
```
                              Monitoring Menu

        1. View Sensors
        2. View Digital Inputs
        3. View IP Devices
        4. View Output Relays
        5. Configure Sensors
        6. Configure Digital Inputs
        7. Configure IP Devices
        8. Configure Output Relays
        9. Configure IP Cameras

Monitor Sensors.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 64- Text Menu-Monitoring Menu

View Sensors

The View Sensors selection will show the present status of each analog sensor connected to the EMS200.

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



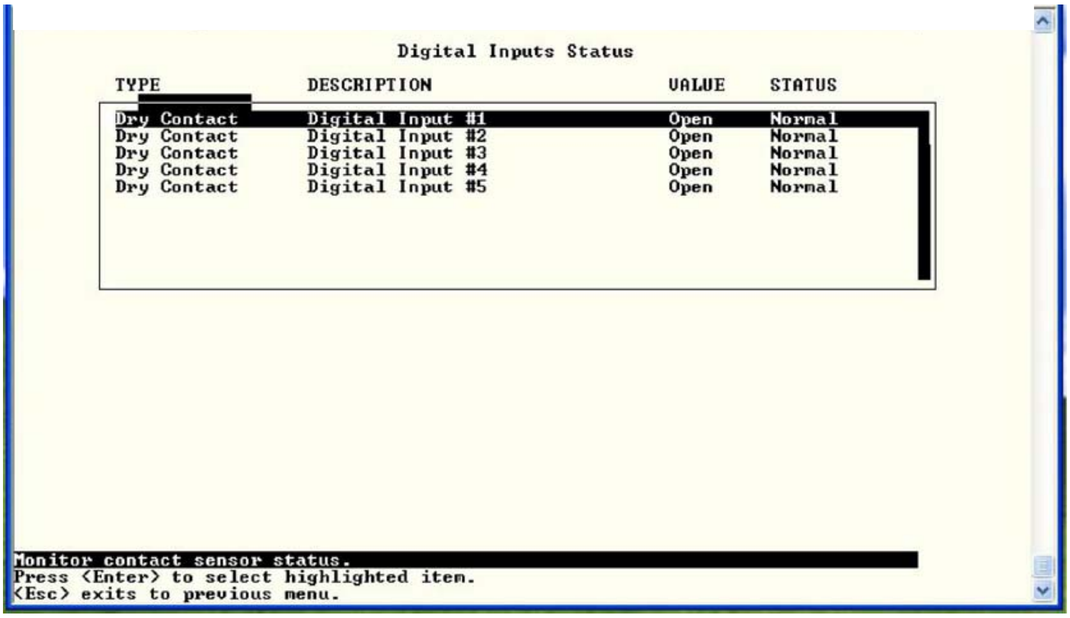
```
                                 Sensor Status

         TYPE              DESCRIPTION                    VALUE    STATUS

         Temperature Com   Server Rack Temperature        86.0 ▒F  Normal
         Humidity Combo    Server Rack Humidity           23.4 %   Normal
         Temperature Com   Server Room Temperature        78.7 ▒F  Normal
         Humidity Combo    Server Room Humidity           29.6 %   Normal

Monitor sensor status.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 65- Text Menu-Sensor Status

View Digital Inputs

The View Digital Inputs selection will show the present status of each dry contact sensor connected to the EMS200.

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



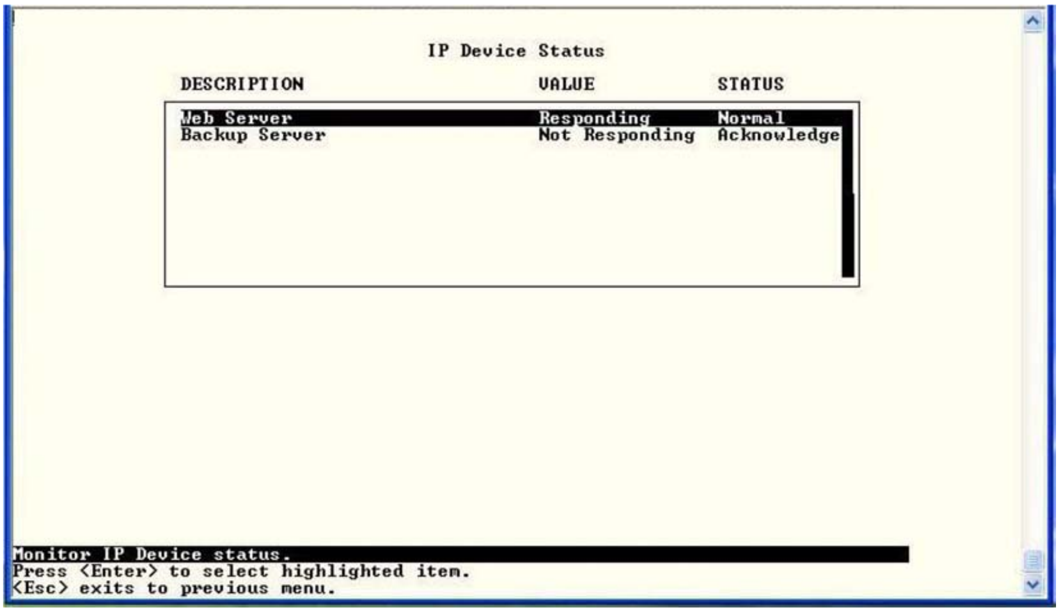
```
                              Digital Inputs Status

         TYPE              DESCRIPTION                    VALUE    STATUS

         Dry Contact       Digital Input #1               Open     Normal
         Dry Contact       Digital Input #2               Open     Normal
         Dry Contact       Digital Input #3               Open     Normal
         Dry Contact       Digital Input #4               Open     Normal
         Dry Contact       Digital Input #5               Open     Normal

Monitor contact sensor status.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 66- Text Menu- Digital Input Status

View IP Devices

The View IP Devices selection will show the present status of each IP Device monitored by the EMS200.

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

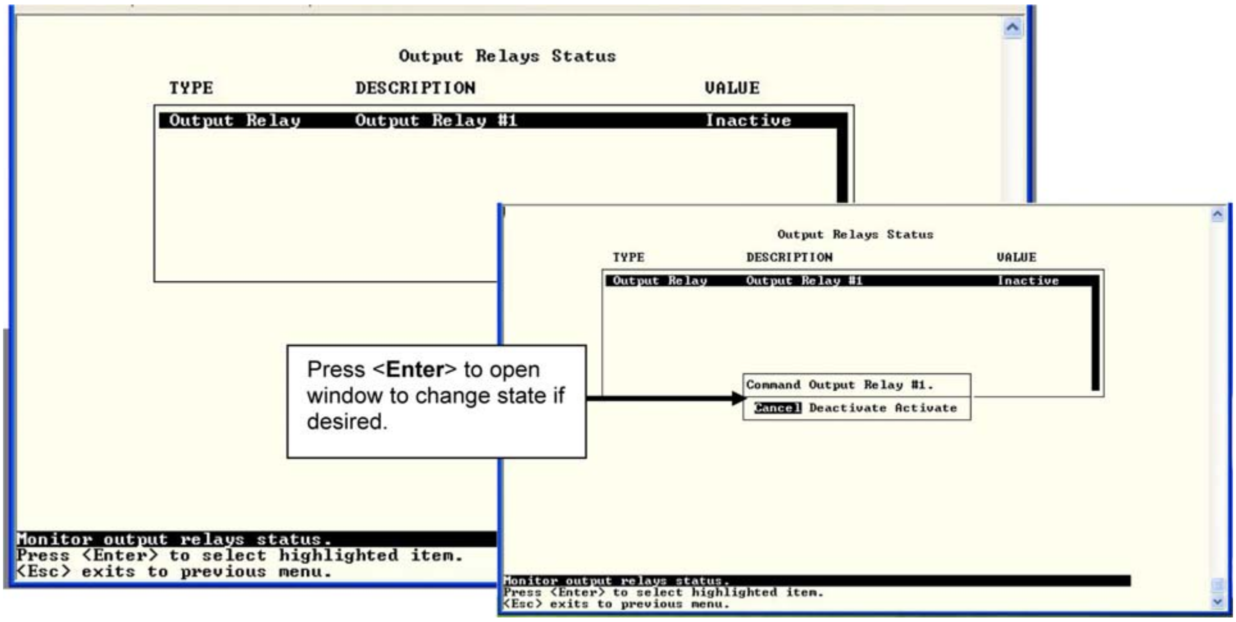


```
                         IP Device Status
     DESCRIPTION                       VALUE            STATUS
     Web Server                        Responding       Normal
     Backup Server                     Not Responding   Acknowledge

Monitor IP Device status.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 67- Text Menu-View IP Devices

View Output Relay

The View Output Relay selection will show the present state of the Output Relay on the EMS200.   To manually change its state, press <**Enter**> and select between Inactive and Active.



```
                         Output Relays Status
     TYPE             DESCRIPTION                    VALUE
     Output Relay     Output Relay #1                Inactive

Monitor output relays status.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

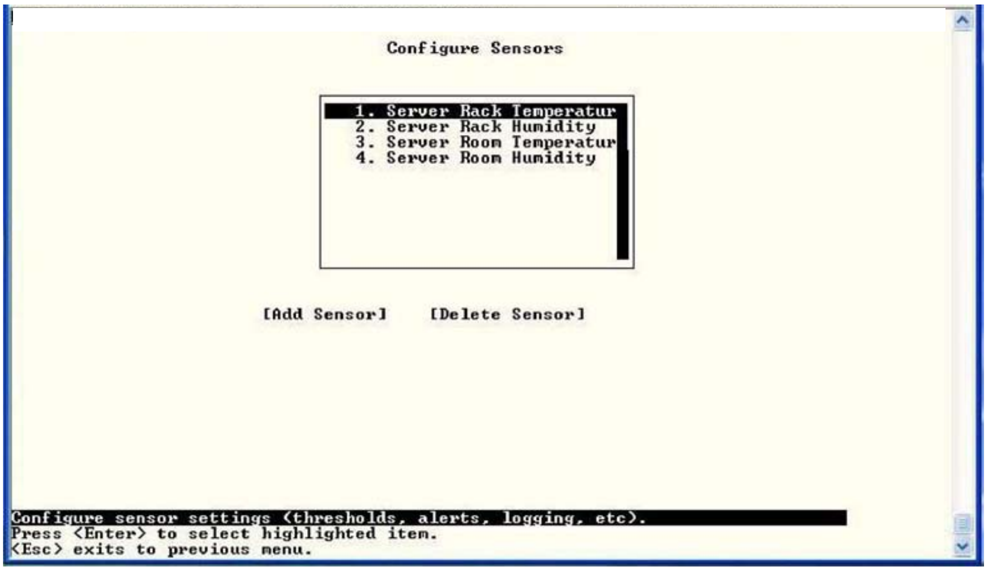
Press <**Enter**> to open window to change state if desired.

```
                         Output Relays Status
     TYPE             DESCRIPTION                    VALUE
     Output Relay     Output Relay #1                Inactive

                   Command Output Relay #1.
                    Cancel Deactivate Activate

Monitor output relays status.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 68- Text Menu- View Output Relay Status

Configure Sensors

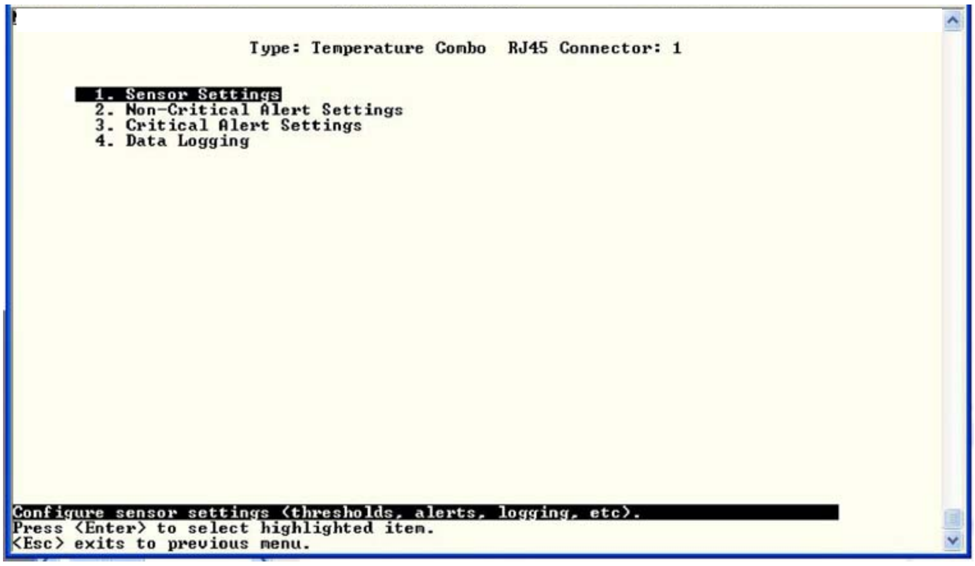
The Configure Sensors menu lists the temperature and humidity sensors connected to the EMS200. Press <**`Enter`**> to open the configuration menu for the selected sensor.



```
                         Configure Sensors

                   1. Server Rack Temperatur
                   2. Server Rack Humidity
                   3. Server Room Temperatur
                   4. Server Room Humidity

              [Add Sensor]    [Delete Sensor]

Configure sensor settings (thresholds, alerts, logging, etc).
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 69- Text Menu-Configure Sensors list

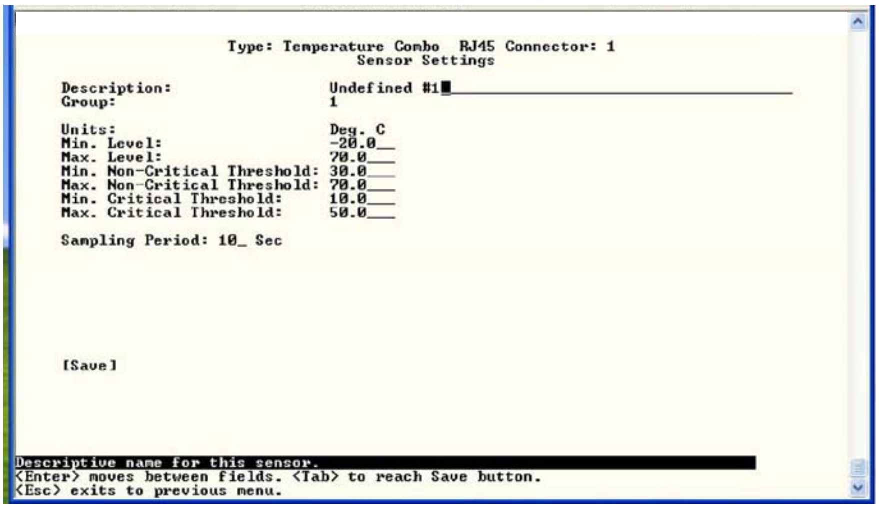
The configuration menu for the sensor includes options to enter the Sensor Settings, Non-Critical Alert Settings, Critical Alert Settings, and Data Logging.



```
              Type: Temperature Combo  RJ45 Connector: 1

      1. Sensor Settings
      2. Non-Critical Alert Settings
      3. Critical Alert Settings
      4. Data Logging

Configure sensor settings (thresholds, alerts, logging, etc).
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 70- Text Menu-Configuration Menu for Sensor

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



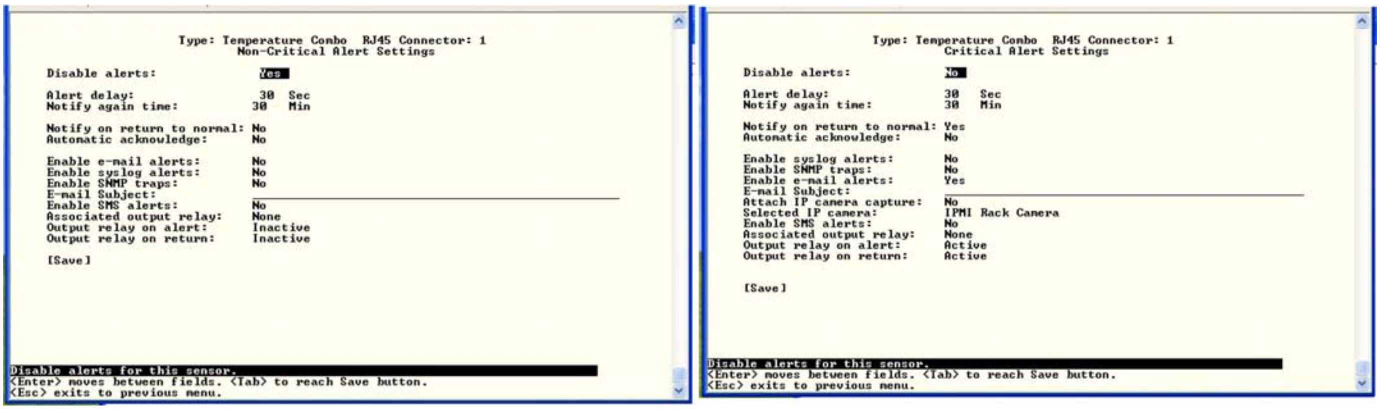
```
                    Type: Temperature Combo  RJ45 Connector: 1
                                  Sensor Settings

     Description:                 Undefined #1█______________________________
     Group:                       1

     Units:                       Deg. C
     Min. Level:                  -20.0__
     Max. Level:                  70.0___
     Min. Non-Critical Threshold: 30.0___
     Max. Non-Critical Threshold: 70.0___
     Min. Critical Threshold:     10.0___
     Max. Critical Threshold:     50.0___

     Sampling Period: 10_ Sec




     [Save]



Descriptive name for this sensor.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 71- Text Menu-Sensor Settings

Sensor Settings	Description
Description	The description of the sensor that will be viewed in the Summary page and in the body of alert messages
Group	Assign the sensor to a group (1 -8) (see also page 85)
Units	This lets the operator choose between Celsius and Fahrenheit as the temperature measurement unit.
Min. Level	Displays the minimum value that this sensor will report
Max. Level	Displays the maximum value that this sensor will report
Minimum Non-Critical - Threshold	The user must define the lowest acceptable value for the sensors. If the sensor measures a value below this threshold, the sensor will move to non-critical alert status. The assigned value should be > within the range defined by Minimum Level and Maximum Level and > lower than the assigned Maximum Threshold value. If values out of the range are entered, and error message will be shown.
Maximum Non-Critical Threshold	The user must define the highest acceptable value for the sensors. If the sensor measures a value above this threshold, the sensor will move to non-critical alert status. The assigned value should be > within the range defined by Minimum Level and Maximum Level and > higher than the assigned Minimum Threshold value. If values out of the range are entered, and error message will be shown.
Minimum Critical Threshold	The user must define the lowest acceptable value for the sensors. If the sensor measures a value below this threshold, the sensor will move to alert status. The assigned value should be > within the range defined by Minimum Level and Maximum Level, > lower than the assigned Maximum Threshold value, and > lower than the Minimum Non-Critical Threshold value. If values out of the range are entered, and error message will be shown.
Maximum Critical Threshold	The user must define the highest acceptable value for the sensors. If the sensor measures a value above this threshold, the sensor will move to alert status. The assigned value should be > within the range defined by Minimum Level and Maximum Level, > higher than the assigned Minimum Threshold value, and > higher than the Maximum Non-Critical Threshold value. If values out of the range are entered, and error message will be shown.
Sampling Period	Determines how often the displayed sensor value is refreshed on the Sensor page. A numeric value and a measurement unit (minimum 1 seconds, maximum 999 minutes) should be entered.

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

From the Non-Critical or Critical Alert Settings menu, the user can enable/disable alert messages to be sent when the sensor is in an alert state and configure when and how alert messages are sent. Additionally, from the Critical Alert Settings menu, the user can configure the EMS200 to capture a snapshot from an IP camera and attach the image to the alert message sent via email.



```
                    Type: Temperature Combo  RJ45 Connector: 1
                           Non-Critical Alert Settings

     Disable alerts:                Yes

     Alert delay:                    30  Sec
     Notify again time:             30   Min

     Notify on return to normal: No
     Automatic acknowledge:         No

     Enable e-mail alerts:          No
     Enable syslog alerts:          No
     Enable SNMP traps:             No
     E-mail Subject:                _______________________________________________
     Enable SMS alerts:             No
     Associated output relay:       None
     Output relay on alert:         Inactive
     Output relay on return:        Inactive

     [Save]

Disable alerts for this sensor.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

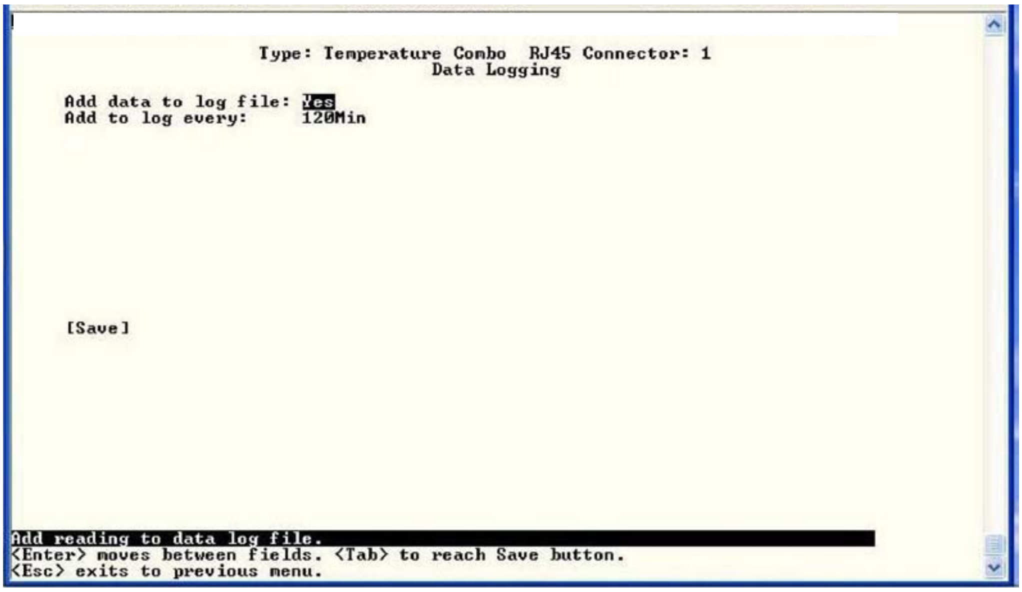
```
                    Type: Temperature Combo  RJ45 Connector: 1
                             Critical Alert Settings

     Disable alerts:                No

     Alert delay:                   30   Sec
     Notify again time:             30   Min

     Notify on return to normal: Yes
     Automatic acknowledge:         No

     Enable syslog alerts:          No
     Enable SNMP traps:             No
     Enable e-mail alerts:          Yes
     E-mail Subject:                _______________________________________________
     Attach IP camera capture:      No
     Selected IP camera:            IPMI Rack Camera
     Enable SMS alerts:             No
     Associated output relay:       None
     Output relay on alert:         Active
     Output relay on return:        Active


     [Save]

Disable alerts for this sensor.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 72- Text Menu-Non-Critical and Critical Alert Settings

Disable alerts	Change to “Yes” to prevent alerts from being sent when this sensor’s status changes
Alert Delay	The alert delay is an amount of time the sensor must be in an alert condition before an alert is sent. This provides some protection against false alarms. The Alert Delay value can be set for 0-999 seconds or minutes.
Notify Again Time	Enter the amount of time in seconds, minutes, or hours (1-999) before an alert message will be repeated
Notify on Return to Normal	The user can also be notified when the sensor readings have returned to the normal range by changing to “Yes” for "***Notify on return to normal***" for a sensor.
Auto Acknowledge	Change to “Yes” to have alert notifications in the summary page return to normal state automatically when sensor readings return to normal.
Enable Email Alerts	Change to “Yes” to have alert notifications sent via Email
Enable Syslog Alerts	Change to “Yes” to have alert notifications sent via Syslog messages
Enable SNMP traps	Change to “Yes” to have alert notifications sent via SNMP traps (v2c)
Enable SMS Alerts	Change to “Yes” to have alert notifications sent via SMS (requires GSM modem)
Email Subject	Enter the subject to be viewed when an email alert message is received
Attach IP camera capture	Change to “Yes” to enable a snapshot to be taken from an IP camera and attached to the alert message (for critical alert messages only.)
Selected IP camera	Select which IP camera to take a snapshot from to be attached to an alert message (for critical alert messages only)
Associated output relay	Choose which output relay to change state when sensor is in alert
Output relay on alert	Choose the state the output relay should be in when the sensor is in alert
Output relay on return	Choose the state the output relay should be in when the sensor returns to normal

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

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

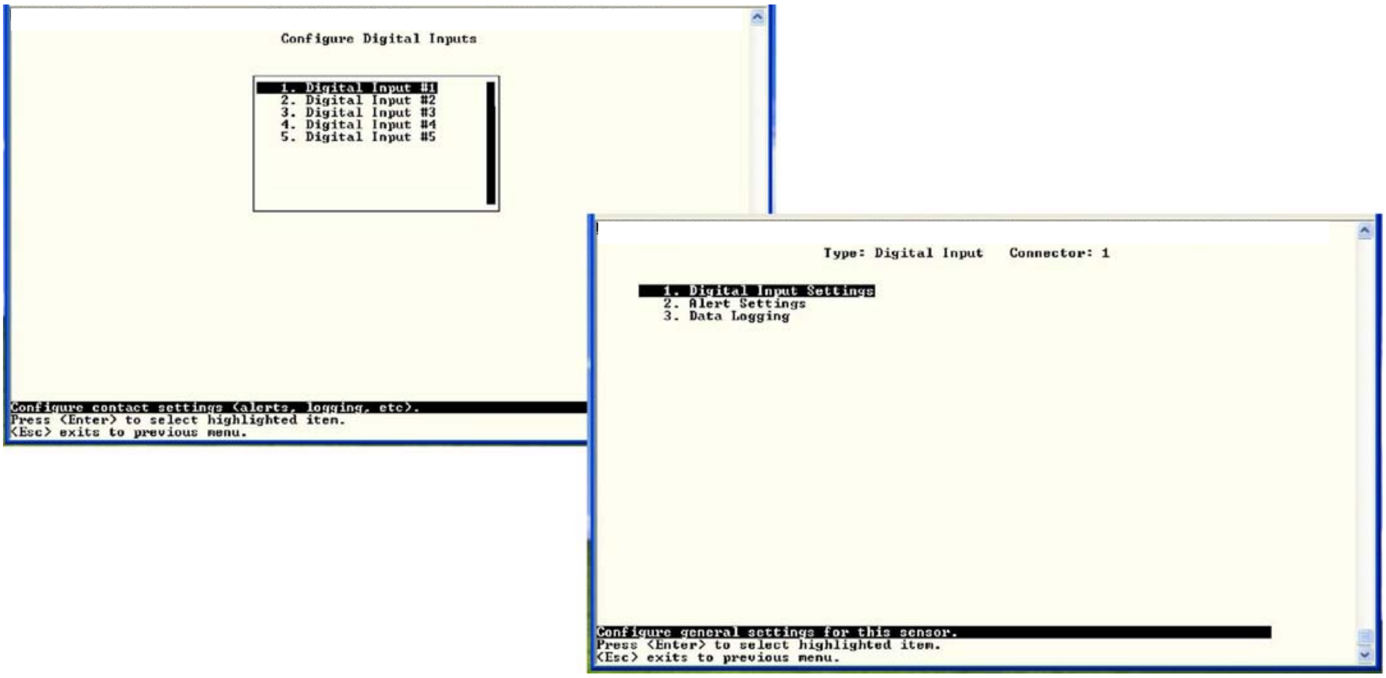


```
                    Type: Temperature Combo  RJ45 Connector: 1
                                  Data Logging

   Add data to log file: Yes
   Add to log every:     120Min





   [Save]




Add reading to data log file.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 73- Text Menu-Sensor Data Logging

Configure Digital Inputs

The Configure Digital Input Sensors menu lists the contact sensors connected to the EMS200.   Press <**Enter**> to open the configuration menu for the selected contact sensor.   (The Water Sensor menu contains the same options as the contact sensor menus.) The configuration menu for the Digital Inputs includes options to enter the Digital Input Settings, Alert Settings, and Data Logging.



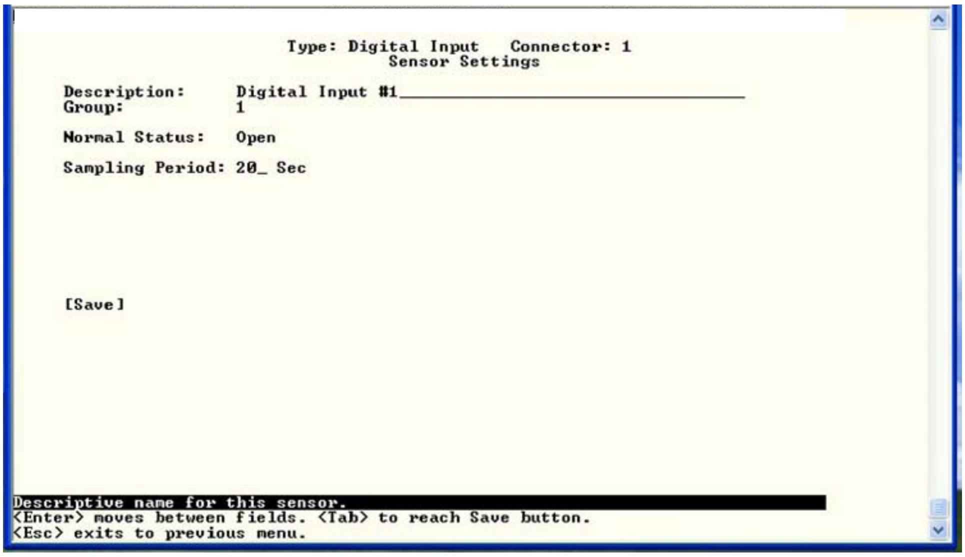
```
                    Configure Digital Inputs

                  1. Digital Input #1
                  2. Digital Input #2
                  3. Digital Input #3
                  4. Digital Input #4
                  5. Digital Input #5

Configure contact settings (alerts, logging, etc).
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

```
                    Type: Digital Input   Connector: 1

   1. Digital Input Settings
   2. Alert Settings
   3. Data Logging

Configure general settings for this sensor.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 74- Configure Digital Input Sensors

Water sensors and contact sensors are each configured much like the temperature and humidity sensors previously described. Only the Sensor Settings menu (below) is different. Alert settings and data logging menus are as seen in Figure 72 and Figure 73.

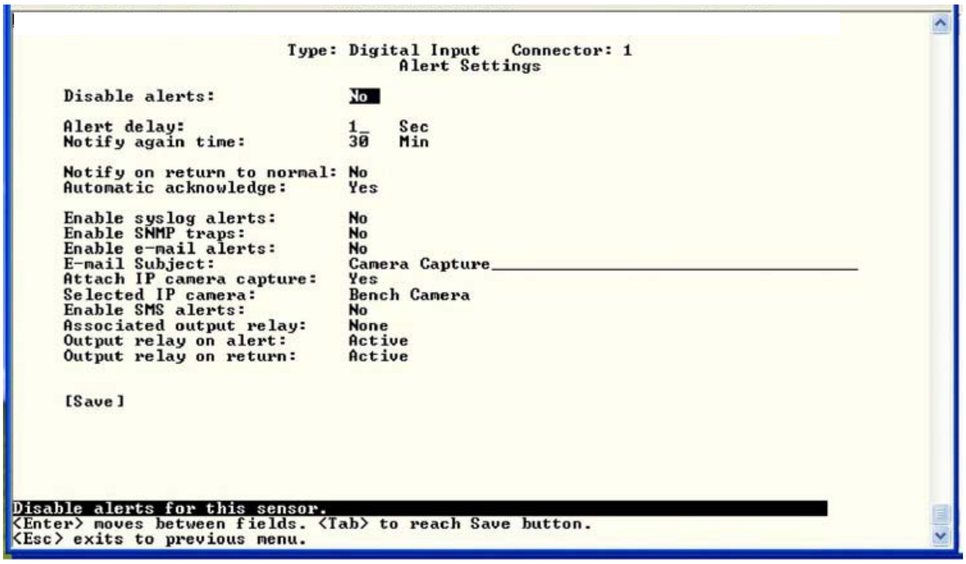
Instead of threshold and minimum/maximum levels settings, water sensors and contact sensors are either open contact or closed contact sensors. Therefore, the field “**Normal Status**” is provided to select the status of the sensor when it is not in an alert state. Select between **Open** contacts, or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



```
                    Type: Digital Input   Connector: 1
                                Sensor Settings

   Description:     Digital Input #1______________________________
   Group:           1

   Normal Status:   Open

   Sampling Period: 20_ Sec




   [Save]



Descriptive name for this sensor.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 75- Digital Input Sensor Settings Menu

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



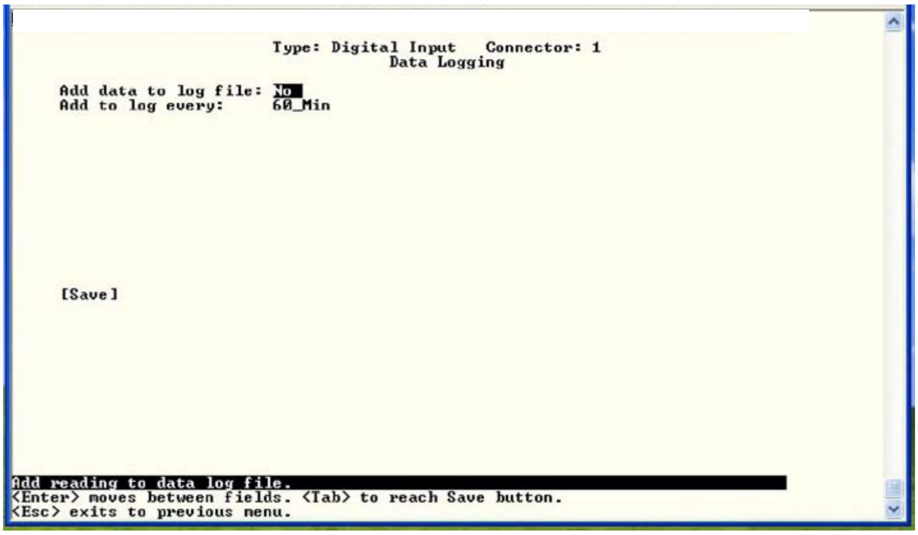
```
                    Type: Digital Input   Connector: 1
                                Alert Settings
   Disable alerts:              No

   Alert delay:                 1_   Sec
   Notify again time:           30   Min

   Notify on return to normal:  No
   Automatic acknowledge:       Yes

   Enable syslog alerts:        No
   Enable SNMP traps:           No
   Enable e-mail alerts:        No
   E-mail Subject:              Camera Capture____________________________
   Attach IP camera capture:    Yes
   Selected IP camera:          Bench Camera
   Enable SMS alerts:           No
   Associated output relay:     None
   Output relay on alert:       Active
   Output relay on return:      Active

   [Save]


Disable alerts for this sensor.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 76- Digital Input Alert Settings

Disable alerts	Change to “Yes” to prevent alerts from being sent when this sensor’s status changes
Alert Delay	The alert delay is an amount of time the sensor must be in an alert condition before an alert is sent. This provides some protection against false alarms. The Alert Delay value can be set for 0-999 seconds or minutes.
Notify Again Time	Enter the amount of time in seconds, minutes, or hours (1-999) before an alert message will be repeated
Notify on Return to Normal	The user can also be notified when the sensor readings have returned to the normal range by changing to “Yes” for "***Notify on return to normal***" for a sensor.
Auto Acknowledge	Change to “Yes” to have alert notifications in the summary page return to normal state automatically when sensor readings return to normal.
Enable Syslog Alerts	Change to “Yes” to have alert notifications sent via Syslog messages
Enable SNMP traps	Change to “Yes” to have alert notifications sent via SNMP traps (v2c)
Enable Email Alerts	Change to “Yes” to have alert notifications sent via Email
Email Subject	Enter the subject to be viewed when an email alert message is received
Attach IP camera capture	Change to “Yes” to enable a snapshot to be taken from an IP camera and attached to the alert message (for critical alert messages only.)
Selected IP camera	Select which IP camera to take a snapshot from to be attached to an alert message (for critical alert messages only)
Enable SMS Alerts	Change to “Yes” to have alert notifications sent via SMS (requires GSM modem)
Associated output relay	Choose which output relay to change state when sensor is in alert
Output relay on alert	Choose the state the output relay should be in when the sensor is in alert
Output relay on return	Choose the state the output relay should be in when the sensor returns to normal

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

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

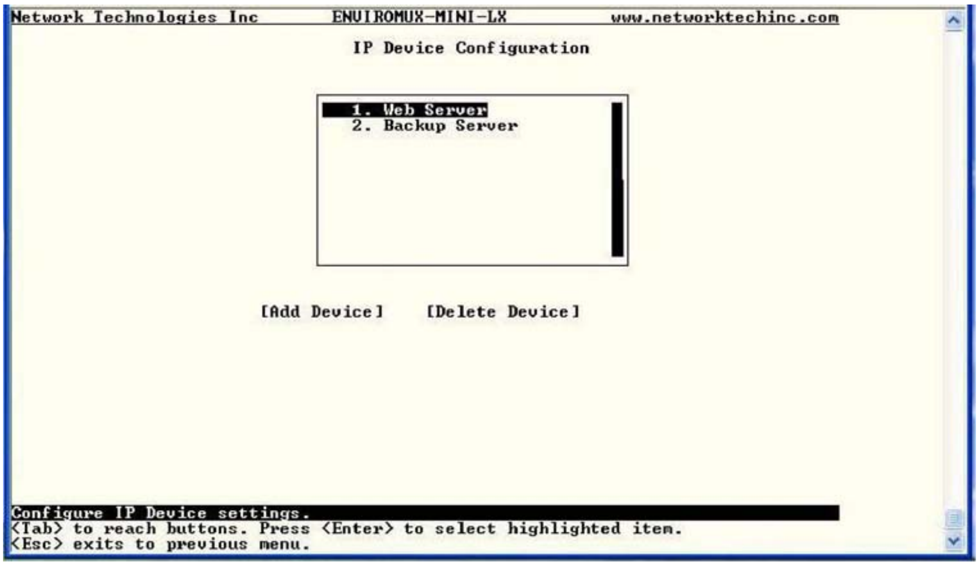


```
                         Type: Digital Input   Connector: 1
                                   Data Logging
     Add data to log file: No
     Add to log every:     60_Min




     [Save]




Add reading to data log file.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 77- Data Logging for Digital Input Sensors

Configure IP Devices

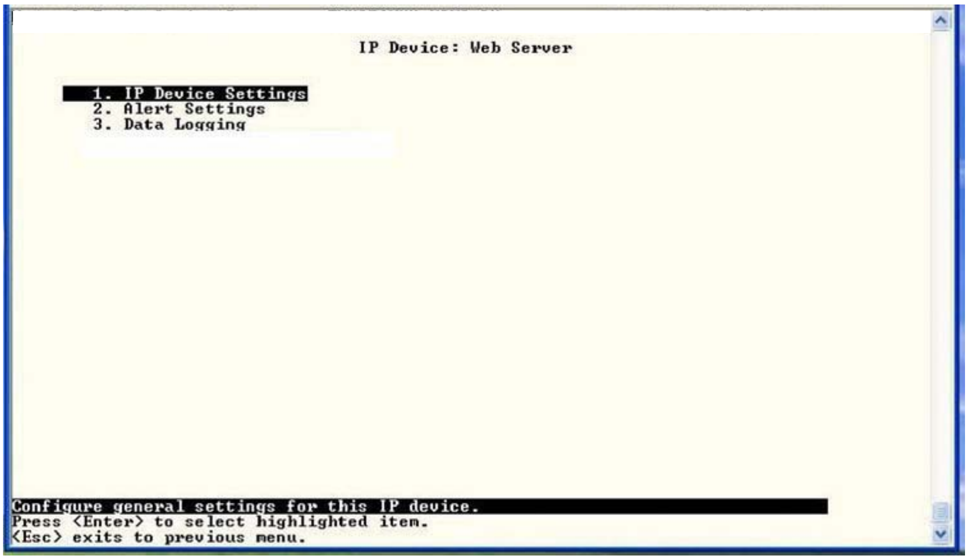
The Configure IP Devices menu lists the IP Devices monitored by the EMS200.   Press <**`Enter`**> to open the configuration menu for the selected IP Device.



```
Network Technologies Inc        ENVIROMUX-MINI-LX          www.networktechinc.com
                                 IP Device Configuration

                              1. Web Server
                              2. Backup Server


                       [Add Device]     [Delete Device]

Configure IP Device settings.
<Tab> to reach buttons. Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 78- Text Menu-Configure IP Devices List

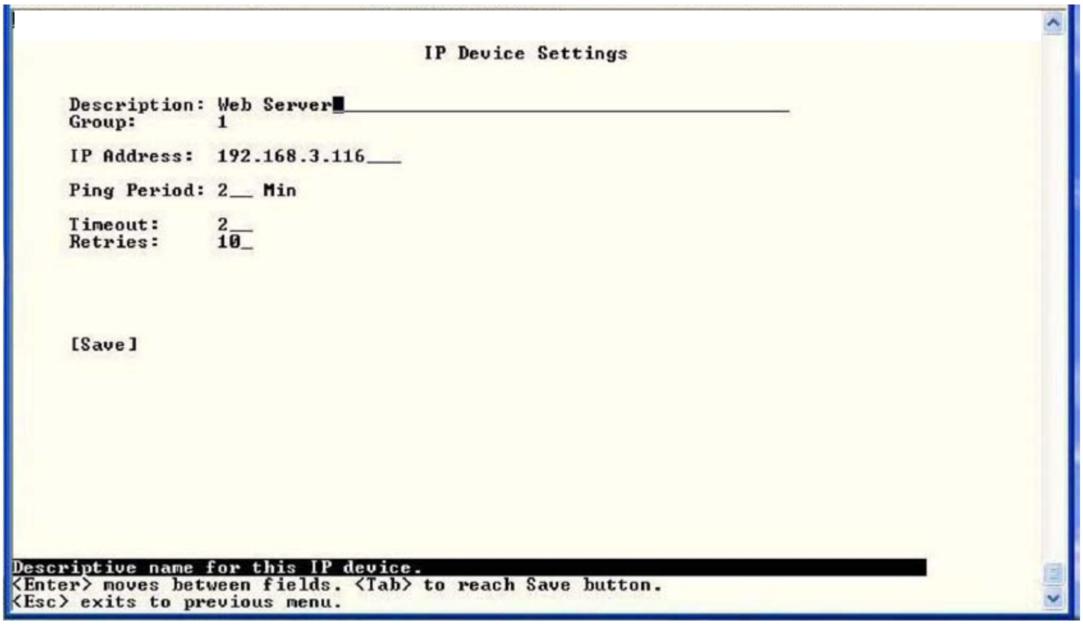
The configuration menu for the IP Device includes options to enter the IP Device Settings, Alert Settings, and Data Logging.



```
                                 IP Device: Web Server

     1. IP Device Settings
     2. Alert Settings
     3. Data Logging

Configure general settings for this IP device.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 79- Text menu-Configuration Menu for IP Devices

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



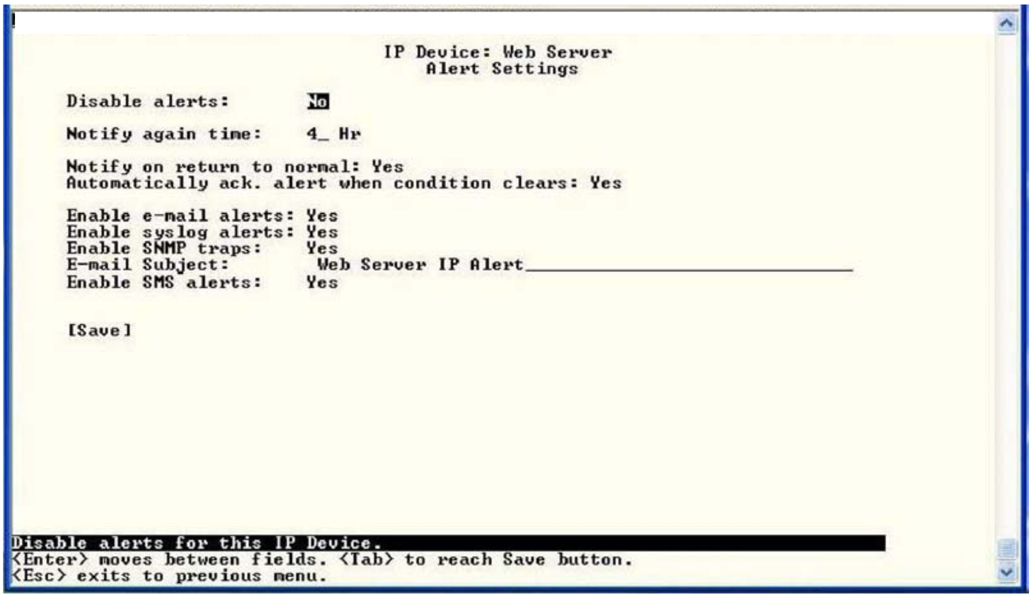
```
                              IP Device Settings

     Description: Web Server_________________________________________
     Group:       1

     IP Address:  192.168.3.116___

     Ping Period: 2__ Min

     Timeout:     2__
     Retries:     10_



     [Save]









Descriptive name for this IP device.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 80-Text Menu-IP Device Settings

IP Device Settings	Description
Description	The description of the IP Device that will be viewed in the Summary page and in the body of alert messages
Group	Assign the IP device to a group (1 -8)
IP Address	The IP address of the IP Device
Ping Period	Enter the frequency in minutes or seconds that the EMS200 should ping the IP Device
Timeout	Enter the length of time in seconds to wait for a response to a ping before considering the attempt a failure
Retries	Enter the number of times the EMS200 should ping a non-responsive IP device before changing its status from normal to alarm and sending an alert

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

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



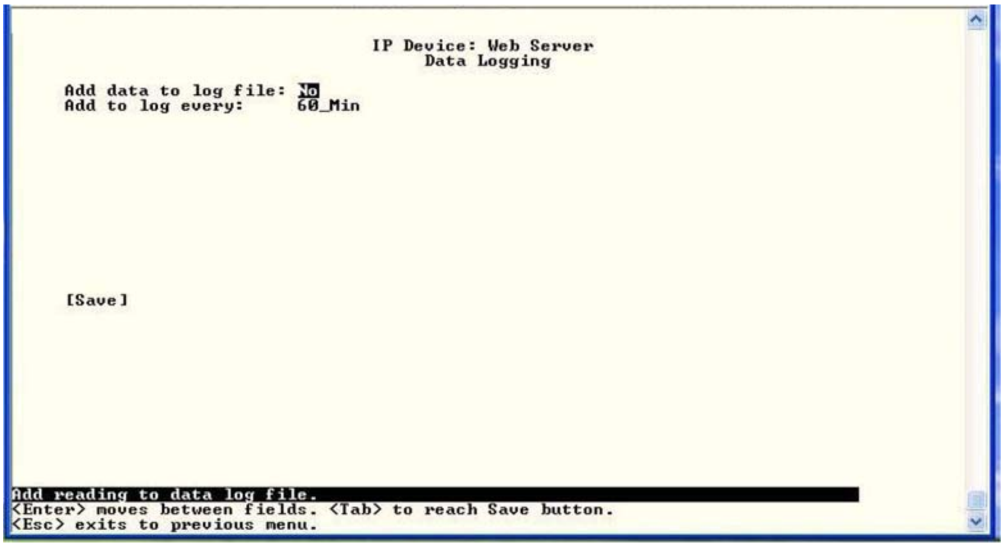
```
                    IP Device: Web Server
                      Alert Settings

   Disable alerts:        No

   Notify again time:     4_ Hr

   Notify on return to normal: Yes
   Automatically ack. alert when condition clears: Yes

   Enable e-mail alerts: Yes
   Enable syslog alerts: Yes
   Enable SNMP traps:    Yes
   E-mail Subject:        Web Server IP Alert______________________________
   Enable SMS alerts:    Yes

   [Save]

Disable alerts for this IP Device.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 81- Text Menu-IP Device Alert Settings

Alert Settings	Description
Disable alerts	Change to “Yes” to prevent alerts from being sent when this IP Device’s status changes
Alert Delay	The alert delay is an amount of time the IP Device must be in an alert condition before an alert is sent. This provides some protection against false alarms. The Alert Delay value can be set for 0-999 seconds or minutes.
Notify Again Time	Enter the amount of time in seconds, minutes, or hours (1-999) before an alert message will be repeated
Notify on Return to Normal	The user can also be notified when the IP Device’s state has returned to the normal by changing to “Yes” for "***Notify on return to normal***" for a sensor.
Auto Acknowledge	Change to “Yes” to have alert notifications in the summary page return to normal state automatically when sensor readings return to normal.
Enable Email Alerts	Change to “Yes” to have alert notifications sent via Email
Enable Syslog Alerts	Change to “Yes” to have alert notifications sent via Syslog messages
Enable SNMP traps	Change to “Yes” to have alert notifications sent via SNMP traps (v2c)
Enable SMS Alerts	Change to “Yes” to have alert notifications sent via SMS (requires GSM modem)
Email Subject	Enter the subject to be viewed when an email alert message is received

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

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

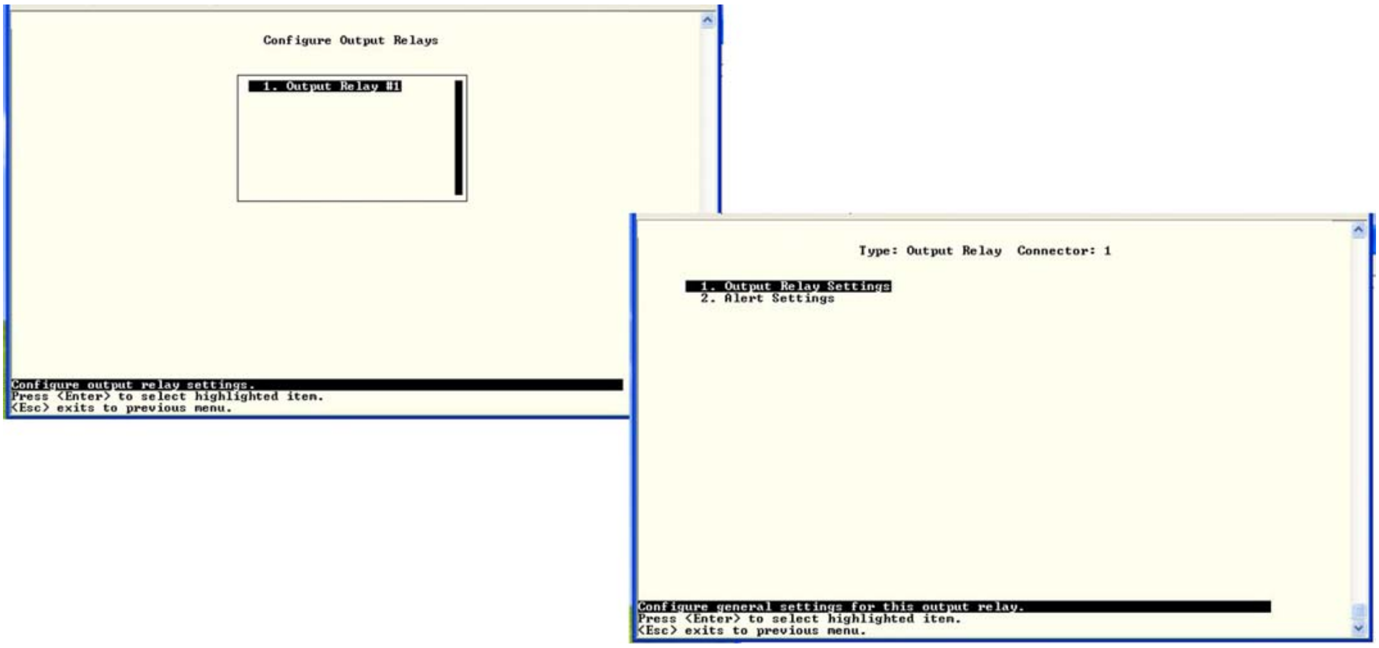


```
                    IP Device: Web Server
                        Data Logging

   Add data to log file: No
   Add to log every:     60_Min




   [Save]



Add reading to data log file.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 82- Text Menu-IP Device Data Logging

Configure Output Relay

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



```
                  Configure Output Relays

                  1. Output Relay #1



Configure output relay settings.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

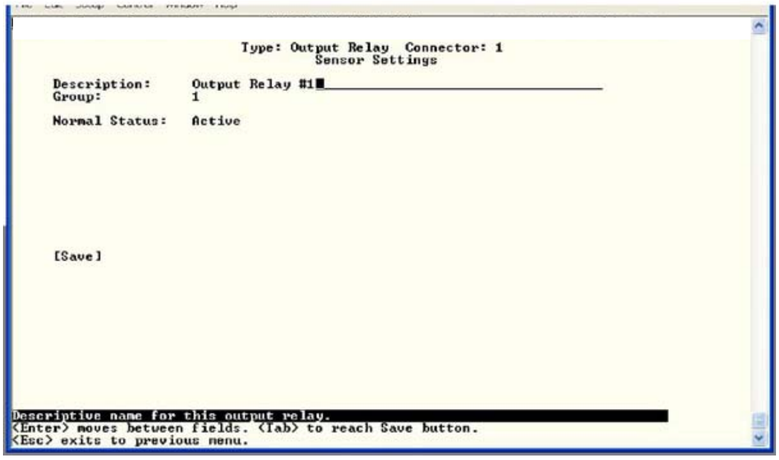
```
               Type: Output Relay  Connector: 1

     1. Output Relay Settings
     2. Alert Settings



Configure general settings for this output relay.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 83- Text Menu- Select Configure Output Relay

Select the Output Relay Settings to access a menu where the description of the Output Relay can be defined. This definition will be presented in the View Output Relays list as well as in the description field when viewing the list through the WEB interface (page 19).

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

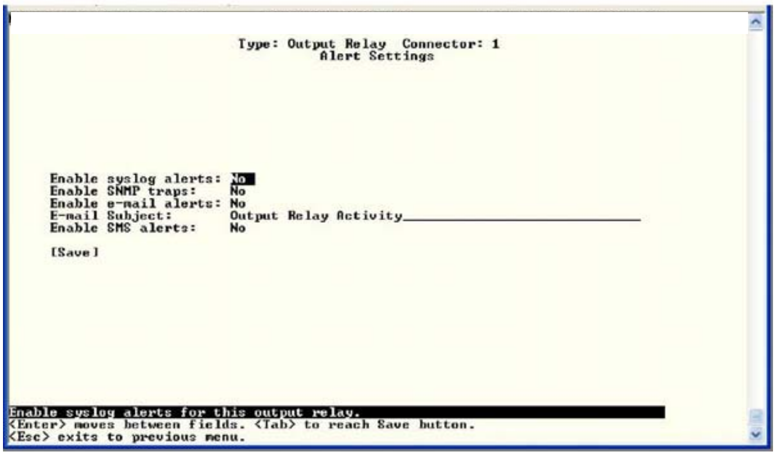
The "Normal Status" of the relay is defined here which determines what the EMS200 will consider a normal versus alert condition for the relay.



```
                    Type: Output Relay  Connector: 1
                           Sensor Settings

   Description:     Output Relay #1_________________________________
   Group:           1

   Normal Status:   Active




   [Save]




Descriptive name for this output relay.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 84- Text Menu- Output Relay Settings

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

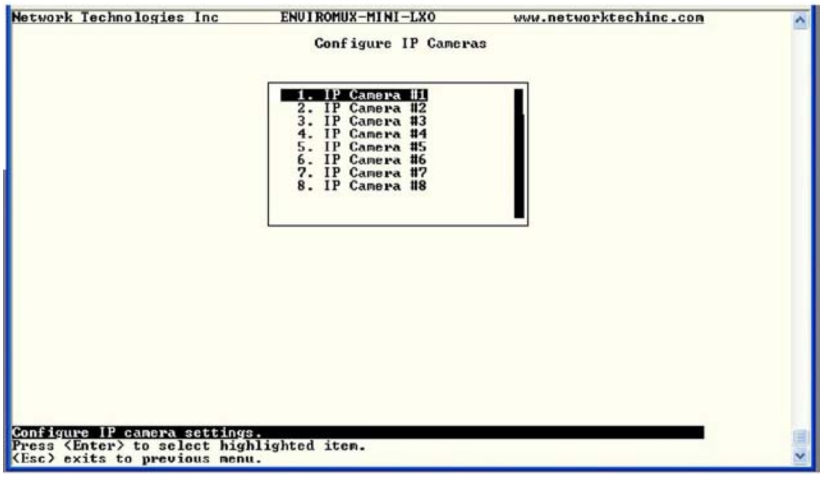


```
                    Type: Output Relay  Connector: 1
                           Alert Settings




   Enable syslog alerts: No
   Enable SNMP traps:    No
   Enable e-mail alerts: No
   E-mail Subject:       Output Relay Activity_____________________________
   Enable SMS alerts:    No

   [Save]




Enable syslog alerts for this output relay.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 85- Text Menu- Output Relay Alert Settings

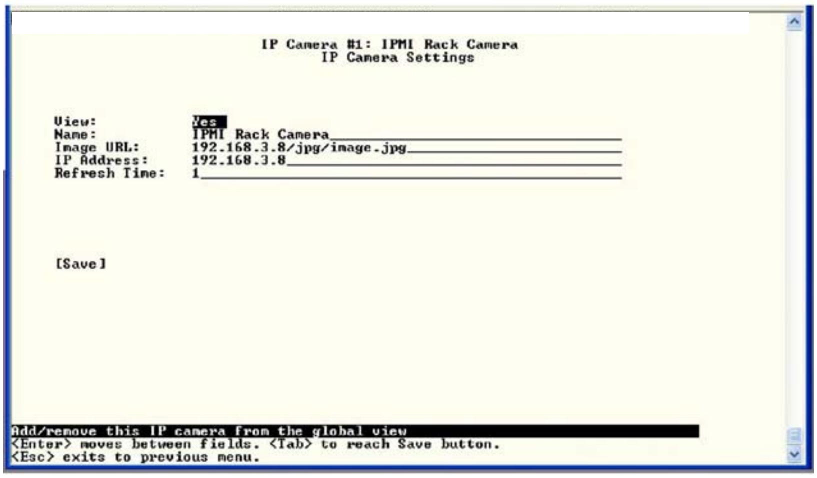
Configure IP Cameras

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



```
Network Technologies Inc        ENVIROMUX-MINI-LXO          www.networktechinc.com
                                 Configure IP Cameras

                              1. IP Camera #1
                              2. IP Camera #2
                              3. IP Camera #3
                              4. IP Camera #4
                              5. IP Camera #5
                              6. IP Camera #6
                              7. IP Camera #7
                              8. IP Camera #8

Configure IP camera settings.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 86- Text Menu- IP Camera List for Configuration



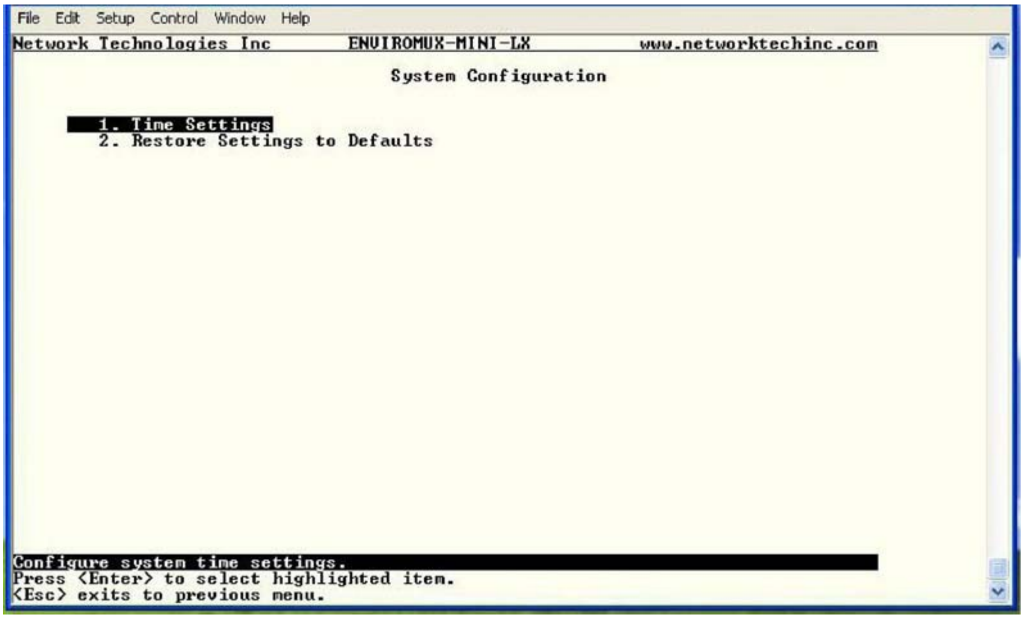
```
                         IP Camera #1: IPMI Rack Camera
                              IP Camera Settings

   View:              Yes
   Name:              IPMI Rack Camera_____________________________
   Image URL:         192.168.3.8/jpg/image.jpg____________________
   IP Address:        192.168.3.8__________________________________
   Refresh Time:      1____________________________________________



   [Save]

Add/remove this IP camera from the global view
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 87- Text Menu- IP Camera Settings

Camera Settings	Description
View	Change to "Yes" to enable images from the IP Camera to appear in the view when selecting the IP Cameras from the Monitoring menu in the WEB interface (page 20).
Name	Characters entered will appear in any listing of the IP camera selection.
Image URL	Enter the full path to the image file captured by the IP camera under "Image URL".
IP Address	the IP address for the IP camera.
Refresh Time	Enter a refresh time period in increments of 100 msec (milliseconds). That is, a value of 1 = 100 msec, 5 = 500 msec , 10 = 1000 msec (or 1 second). The images can be set to be refreshed every 100 msec (.1 second) up to 99,900 msec (almost 100 seconds).

System Configuration

Under System Configuration (from the Main Menu), select “Time Settings” to enter the time of day, time zone, enable daylight saving time, or NTP server settings. Also, select “Restore Settings to Defaults” to clear all configuration and user settings and restore the EMS200 to settings as received from the factory.

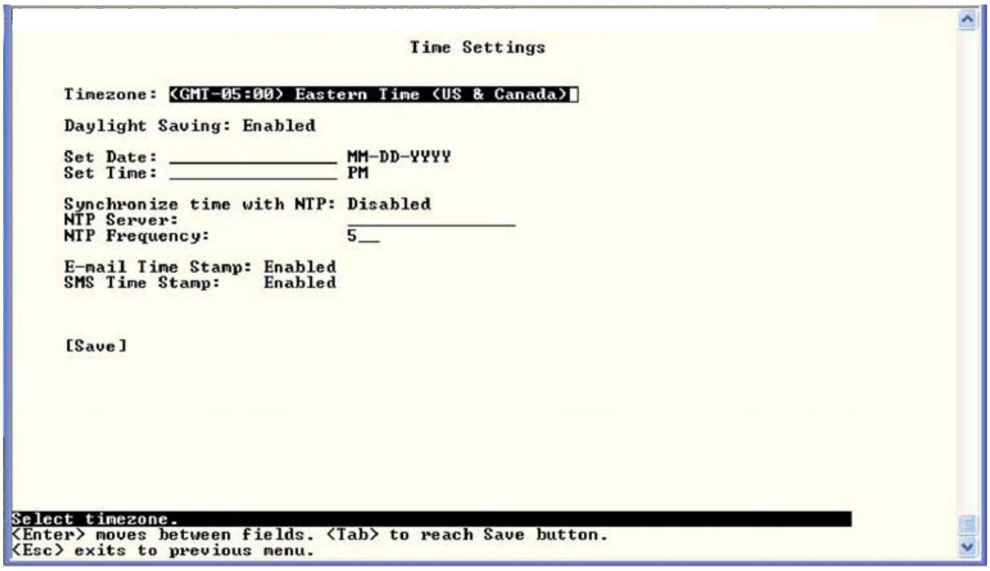


```
Network Technologies Inc        ENVIROMUX-MINI-LX          www.networktechinc.com

                                System Configuration

     1. Time Settings
     2. Restore Settings to Defaults

Configure system time settings.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 88- Text Menu- System Configuration

Time Settings

On the Time Settings menu, the user can designate what time zone the unit is associated with, set the date and time manually or configure the EMS200 to get this information from an NTP server.



```
                                Time Settings

     Timezone: <GMT-05:00> Eastern Time (US & Canada)

     Daylight Saving: Enabled

     Set Date: ________________ MM-DD-YYYY
     Set Time: ________________ PM

     Synchronize time with NTP: Disabled
     NTP Server:                ________________
     NTP Frequency:             5__

     E-mail Time Stamp: Enabled
     SMS Time Stamp:    Enabled


     [Save]

Select timezone.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

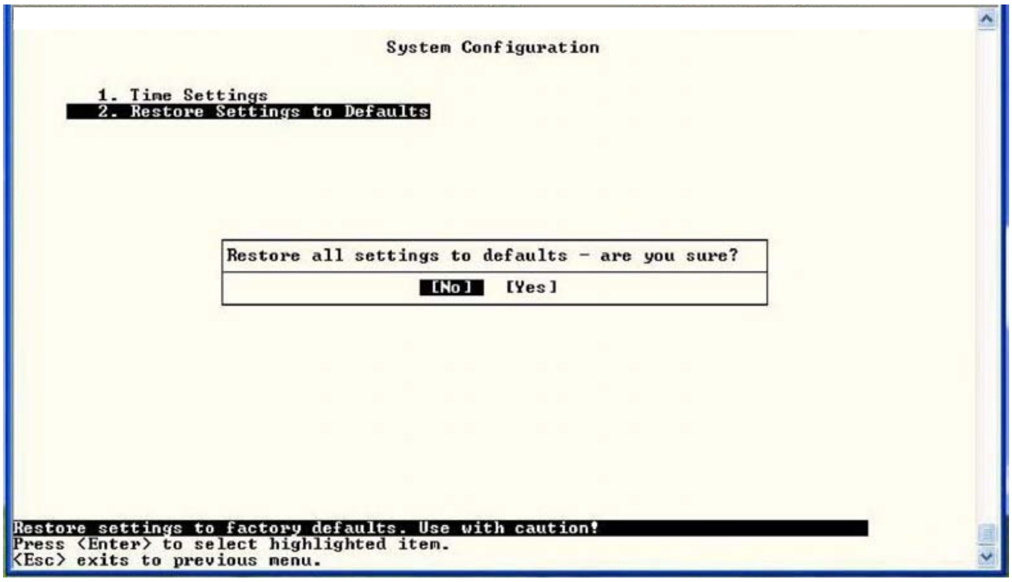
Figure 89- Text Menu-Time Settings menu

Time Settings	Description
Time Zone	Enter the appropriate time zone
Enable Daylight Saving	Change to “Yes” to have the time change in accordance Daylight Saving Time rules
Set Date	Enter the system date in MM-DD-YYYY format
Set Time	Enter the system time of day in hh:mm:ss format
Enable NTP	Change to “Enabled” to allow the EMS200 to automatically sync up with a time server via NTP
NTP server	If the NTP is enabled, enter the Domain Name or IP address of the NTP server
NTP Frequency	Enter the frequency (in minutes) for the EMS200 to query the NTP server (minimum is 5 minutes)
E-mail Time Stamp	Change to “Enabled” to allow the EMS200 to automatically apply a time stamp to e-mail messages sent to users
SMS Time Stamp	Change to “Enabled” to allow the EMS200 to automatically apply a time stamp to SMS messages sent to users

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

Restore Default Settings

Select this option to restore the EMS200 to the configuration settings it had upon receipt from the factory. **Be careful!** This will erase all user configuration settings. Upon restoration, the EMS200 will reboot. Allow 1 minute before trying to reconnect and log in again.



```
                         System Configuration

      1. Time Settings
      2. Restore Settings to Defaults



              Restore all settings to defaults - are you sure?
                             [No]   [Yes]



Restore settings to factory defaults. Use with caution!
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 90- Text Menu-Restore Default Settings

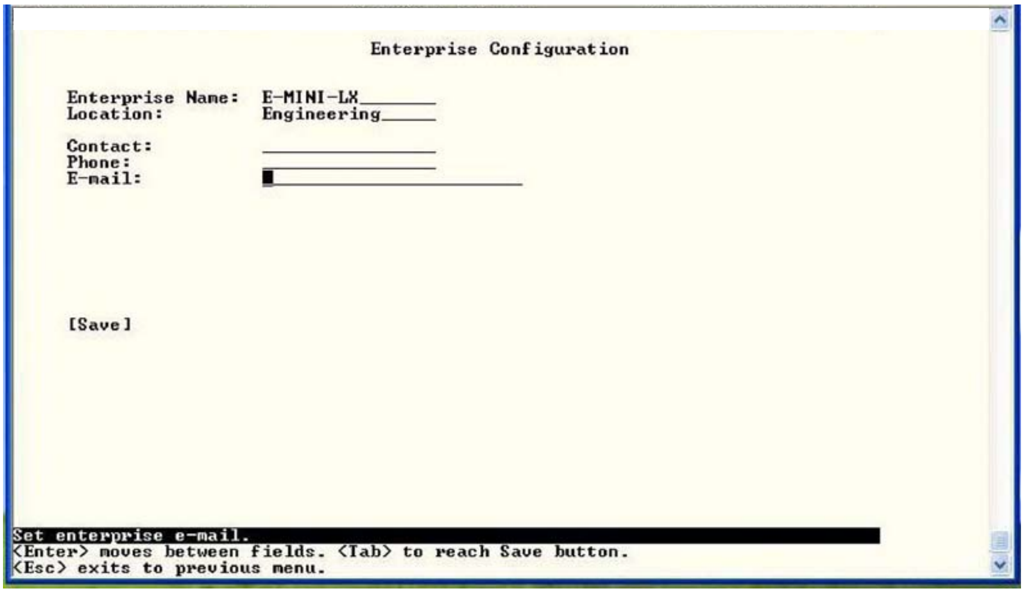
Note: If “Restore Defaults” is used, the IP address will also be restored to its default address of 192.168.1.21 with a login name “root” and password “nti”. To restore the root password to “nti” without having to restore all default settings, contact NTI for assistance.

To identify the IP address of the EMS200 without restoring defaults, use the Discovery Tool (page 17).

Default settings can also be restored using the “Restore Defaults” button on the front of the EMS200 (page 101) or through the web interface (page 34)

Enterprise Configuration

Under Enterprise Configuration (from the Main Menu), enter the unit name, location, the contact person emails should refer to and their phone number, and the email address of the EMS200 to be used for outgoing alert messages.

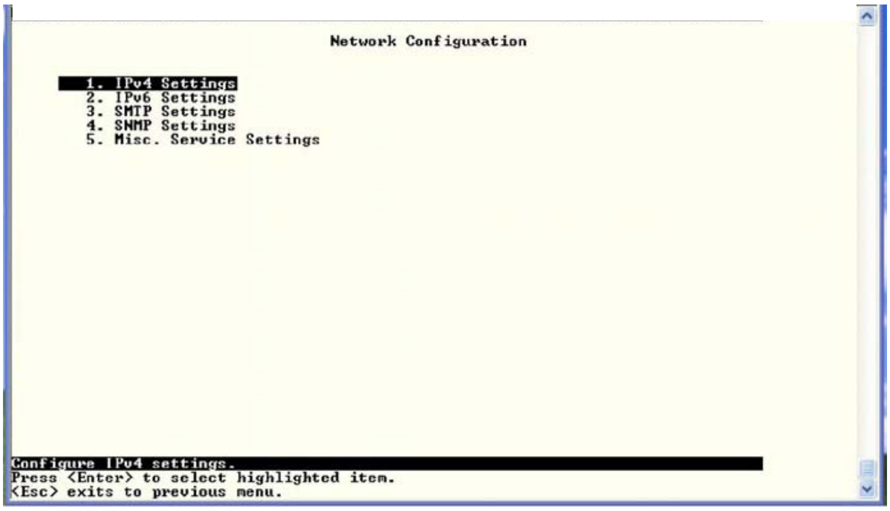


```
                         Enterprise Configuration

     Enterprise Name:  E-MINI-LX_______
     Location:         Engineering_____

     Contact:          ________________
     Phone:            ________________
     E-mail:           ________________________

     [Save]

Set enterprise e-mail.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 91- Text Menu-Enterprise Configuration

Network Configuration

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



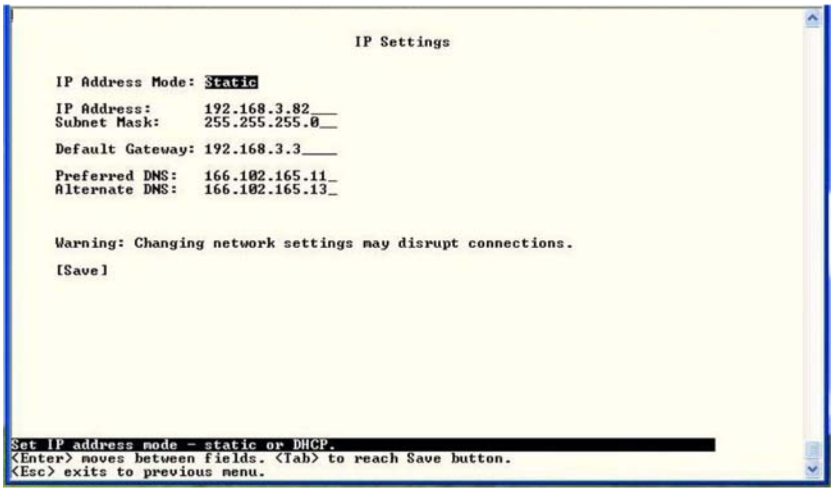
```
                              Network Configuration

      1. IPv4 Settings
      2. IPv6 Settings
      3. SMTP Settings
      4. SNMP Settings
      5. Misc. Service Settings

Configure IPv4 settings.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 92- Text Menu-Network Configuration

Figure 93- Text Menu-IPv4 Settings Menu

IPv4 Settings

The IP Settings menu contains the network connection settings for the EMS200.



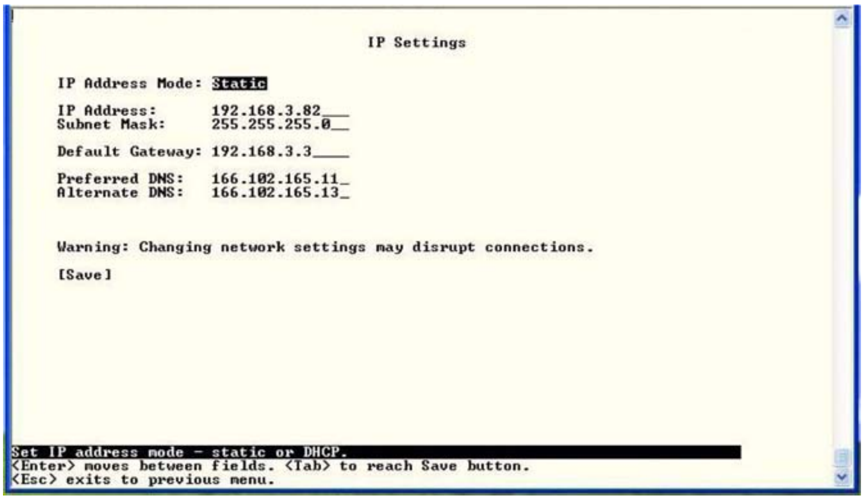
```
                    IP Settings

IP Address Mode: Static

IP Address:      192.168.3.82___
Subnet Mask:     255.255.255.0__

Default Gateway: 192.168.3.3____

Preferred DNS:   166.102.165.11_
Alternate DNS:   166.102.165.13_


Warning: Changing network settings may disrupt connections.

[Save]

Set IP address mode - static or DHCP.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

IP Settings	Description
Mode	Select between Static (manual) , or DHCP (automatic IP and DNS) settings
IP Address	Enter a valid IPv4 address (default value is 192.168.1.21)
Subnet Mask	Enter a valid subnet mask (default value is 255.255.255.0)
Default Gateway	Enter a valid gateway (default gateway value is 192.168.1.1)
Preferred DNS	Enter a preferred domain name server address
Alternate DNS	Enter an alternate domain name server address

If the administrator chooses to have the DNS and IP address information filled in automatically via DHCP,   the SMTP server and port number still need to be entered for email alerts to work. If the SMTP server requires a password in order for users to send emails, the network administrator must first assign a user name and password to the EMS200.

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

IPv6 Settings



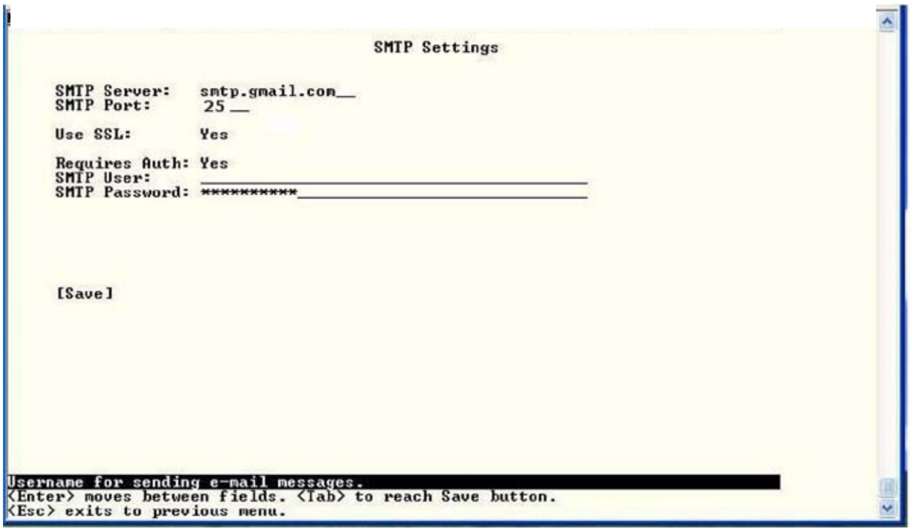
```
                    IP Settings

IP Address Mode: Static

IP Address:      192.168.3.82___
Subnet Mask:     255.255.255.0__

Default Gateway: 192.168.3.3____

Preferred DNS:   166.102.165.11_
Alternate DNS:   166.102.165.13_


Warning: Changing network settings may disrupt connections.

[Save]

Set IP address mode - static or DHCP.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 94- Text Menu-IPv6 Settings Menu

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

SMTP Settings

The SMTP Settings menu contains the SMTP server settings for the EMS200.



```
                              SMTP Settings

     SMTP Server:   smtp.gmail.com__
     SMTP Port:      25 __

     Use SSL:       Yes

     Requires Auth: Yes
     SMTP User:     ________________________________________
     SMTP Password: **********______________________________



     [Save]









Username for sending e-mail messages.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

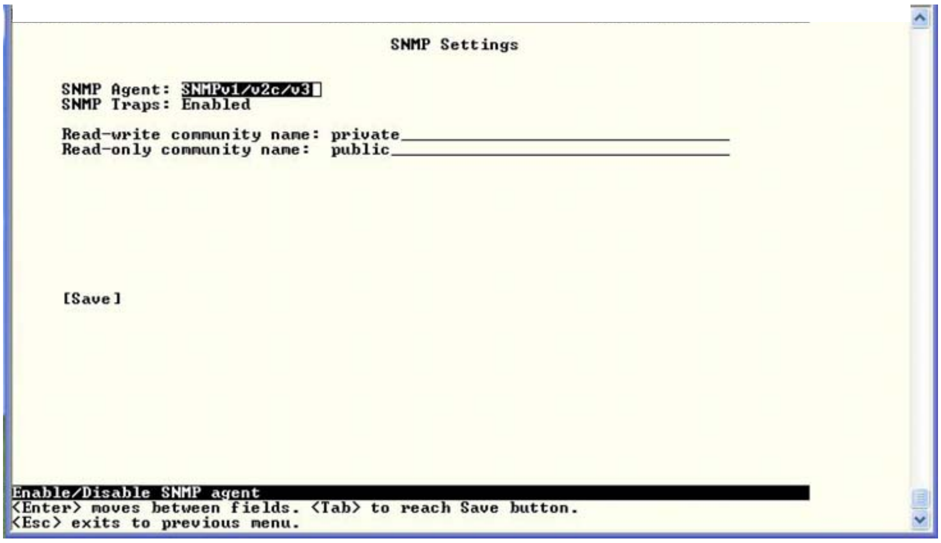
Note: The SMTP server port number is shown in Figure 95 as "25". This is a common port number assigned, but not necessarily the port number assigned to your SMTP server. For SMTP servers that support SSL, the common port number is 465.

Figure 95- Text Menu-SMTP Server Settings

SMTP Settings	Description
SMTP Server	Enter a valid SMTP server name (e.g. yourcompany.com)
Port	Enter a valid port number (default port is 25)
Use SSL	Change to “Yes” if the SMTP server supports SSL
Requires Authentication	Change to “Yes” if the SMTP server requires authentication to send email
SMTP User	Enter a valid username to be used by the EMS200 to send emails
SMTP Password	Enter a valid password assigned to the EMS200 username

SNMP Settings

The SNMP Settings menu contains the SNMP server settings for the EMS200.



```
                              SNMP Settings

     SNMP Agent: SNMPv1/v2c/v3
     SNMP Traps: Enabled

     Read-write community name: private__________________________________
     Read-only community name:  public___________________________________




     [Save]









Enable/Disable SNMP agent
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 96- Text Menu-SNMP Server Settings

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

Read-Only Community Name

The SNMP Read-only community name enables a user to retrieve "read-only" information from the EMS200 using the SNMP browser and MIB file. This name must be present in the EMS200 and in the proper field in the SNMP browser.

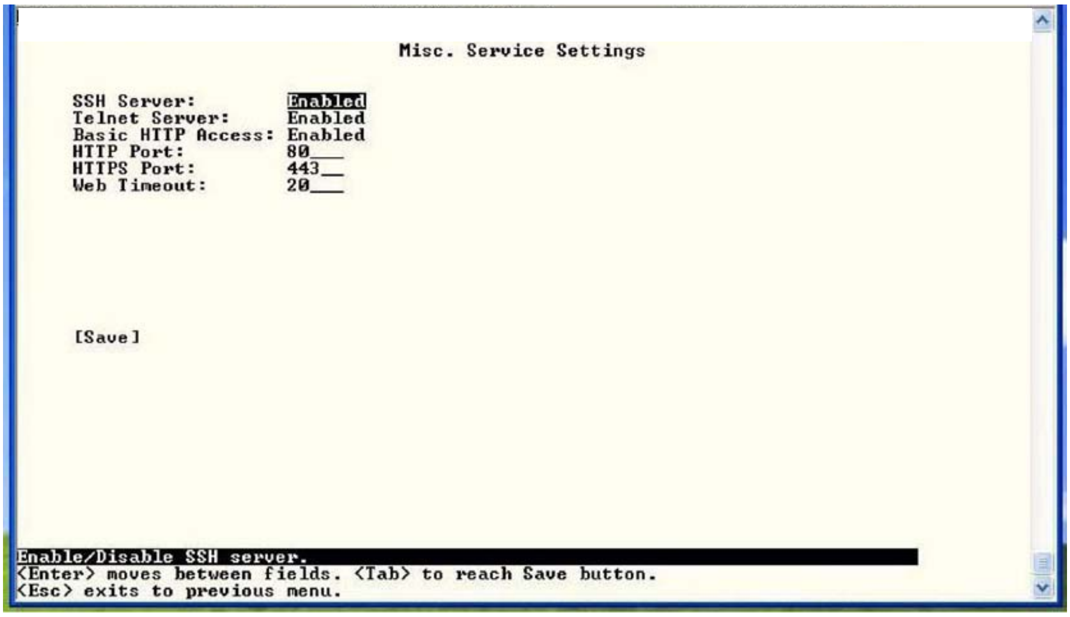
Read-Write Community Name

(not applicable as of this printing)

The SNMP Read-Write community name enables a user to read information from the EMS200 and to modify settings on the EMS200 using the SNMP browser and MIB file. This name must be present in the EMS200 and in the proper field in the SNMP browser.

Miscellaneous Service Settings

The Misc. Service Settings menu contains selections to configure services running on the EMS200.



```
                              Misc. Service Settings

     SSH Server:          Enabled
     Telnet Server:       Enabled
     Basic HTTP Access:   Enabled
     HTTP Port:           80___
     HTTPS Port:          443__
     Web Timeout:         20___





     [Save]






Enable/Disable SSH server.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

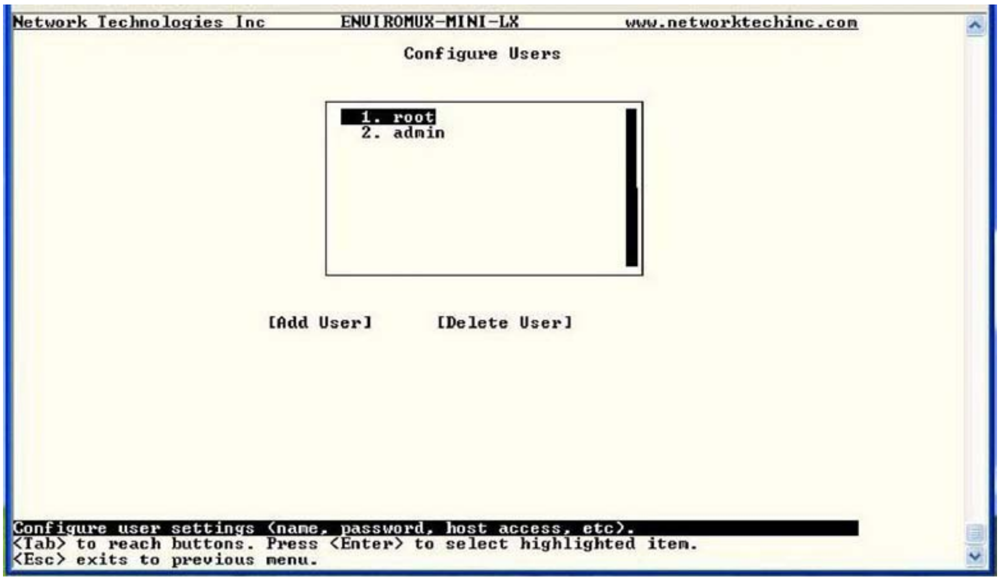
Figure 97- Text Menu-Misc. Service Settings menu

Enable SSH	Enable this to allow access to the EMS200 via SSH
Enable Telnet	Enable this to allow access to the EMS200 via Telnet **The default setting is Disabled.**
Enabe HTTP access	Enable this to allow access to the EMS200 via standard (non-secure) HTTP requests
HTTP Port	Port to be used for standard HTTP requests
HTTPS Port	Port to be used for HTTPS requests
Web Timeout	Number of minutes after which idle web uses will be logged-out (enter 0 to disable this feature)

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

User Configuration

The User Configuration menu lists all configured user names of the EMS200. A maximum of 15 users (other than root) can be configured. From this screen the administrative user can add users, go to the user configuration page to edit a user's access to the EMS200, or delete a user from the list.

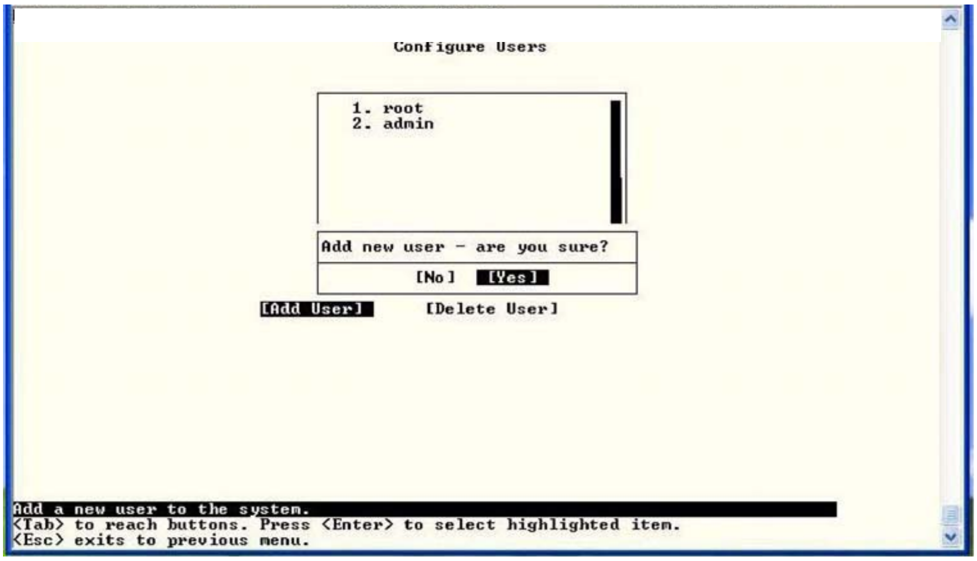


```
Network Technologies Inc        ENVIROMUX-MINI-LX          www.networktechinc.com
                              Configure Users

                     1. root
                     2. admin

                 [Add User]       [Delete User]

Configure user settings (name, password, host access, etc).
<Tab> to reach buttons. Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 98- Text Menu-User Configuration

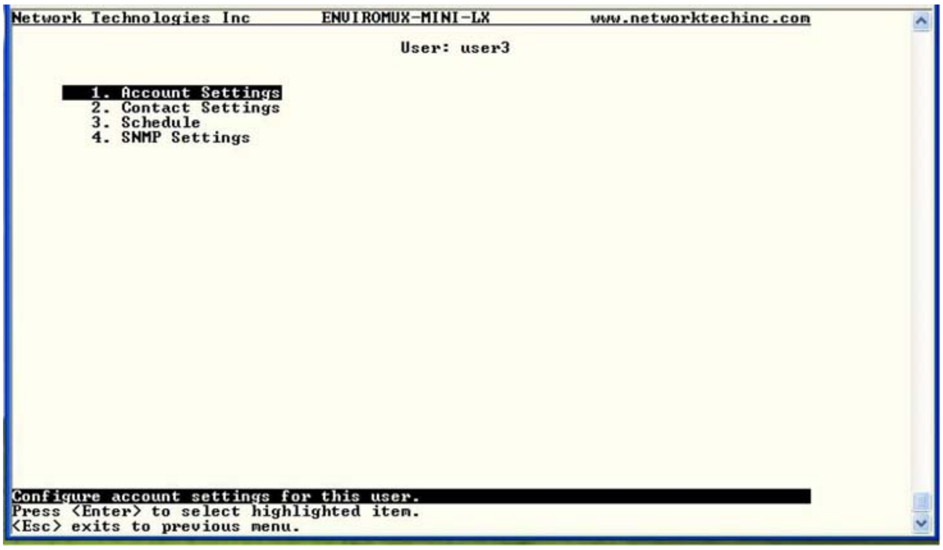
To add a user, Tab to "Add User" and press <`Enter`>.
To edit a user's configuration, select the listed username and press <`Enter`>
To delete a user and their configuration, select a listed username, Tab to "Delete User", and press <`Enter`>. You will be prompted for confirmation before deleting the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

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



```
                              Configure Users

                     1. root
                     2. admin

                    Add new user - are you sure?
                           [No ]  [Yes ]
                 [Add User]       [Delete User]

Add a new user to the system.
<Tab> to reach buttons. Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 99- Text Menu-Confirm to add new user

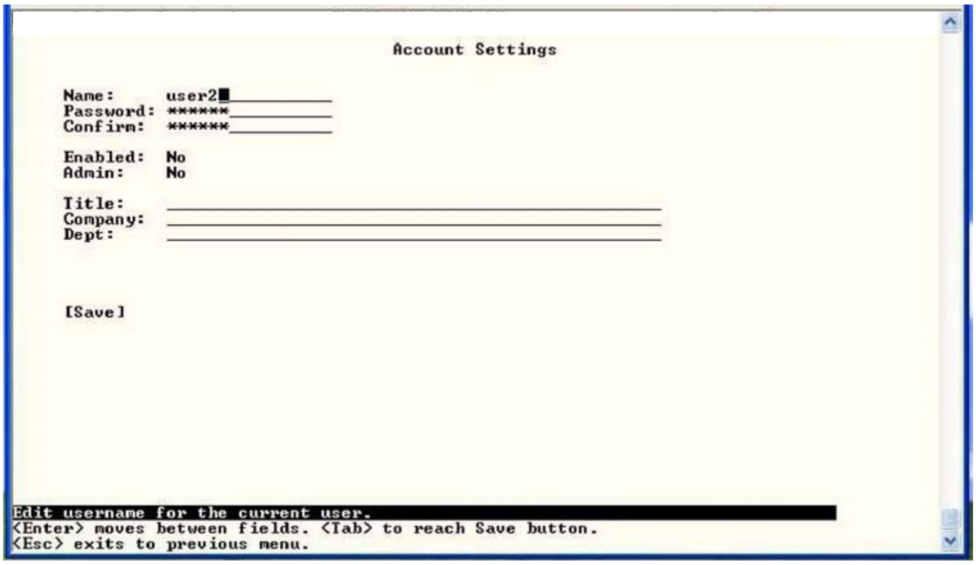


```
Network Technologies Inc        ENVIROMUX-MINI-LX          www.networktechinc.com
                                    User: user3

        1. Account Settings
        2. Contact Settings
        3. Schedule
        4. SNMP Settings

Configure account settings for this user.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 100- Text Menu-Configuration List for User

User Account Settings

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



```
                                  Account Settings

     Name:      user2█__________
     Password:  ******__________
     Confirm:   ******__________

     Enabled:   No
     Admin:     No

     Title:     ________________________________________________
     Company:   ________________________________________________
     Dept:      ________________________________________________


     [Save]

Edit username for the current user.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 101- Text Menu-User Account Settings

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

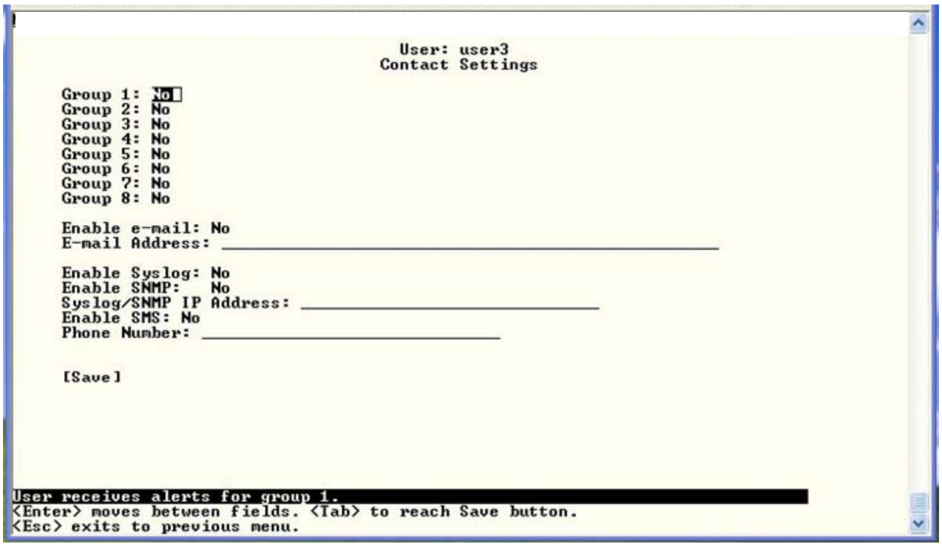
Account Settings	Description
Enabled	Change to “Yes” to enable this user to access the EMS200
Admin	Change to “Yes” if this user should have administrative privileges
Title	Enter information as applicable (optional)
Department	Enter information as applicable (optional)
Company	Enter information as applicable (optional)

More about User Privileges

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

User Contact Settings

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



```
                              User: user3
                            Contact Settings

   Group 1: No
   Group 2: No
   Group 3: No
   Group 4: No
   Group 5: No
   Group 6: No
   Group 7: No
   Group 8: No

   Enable e-mail: No
   E-mail Address: ___________________________________________

   Enable Syslog: No
   Enable SNMP:   No
   Syslog/SNMP IP Address: __________________________
   Enable SMS: No
   Phone Number: __________________________

   [Save]



User receives alerts for group 1.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

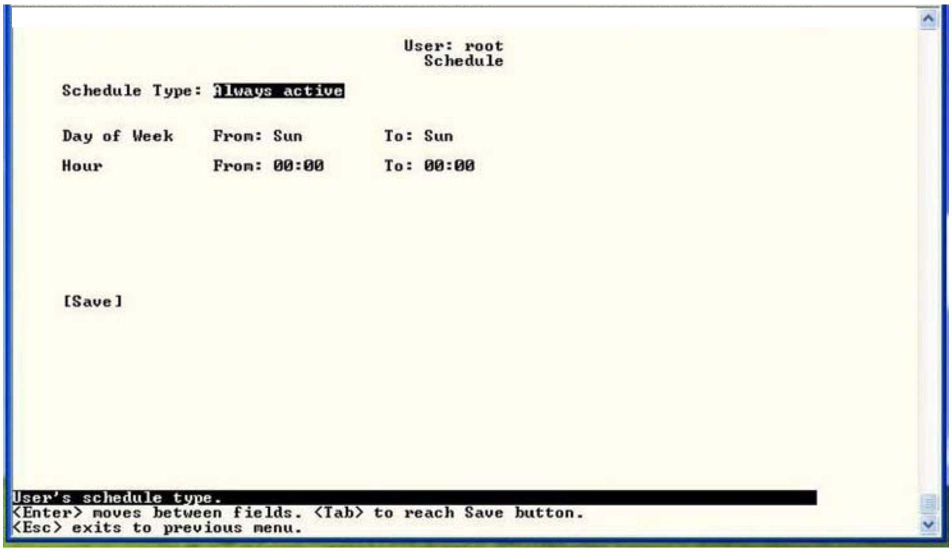
Figure 102- Text Menu-User Contact Settings

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

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

User Activity Schedule

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

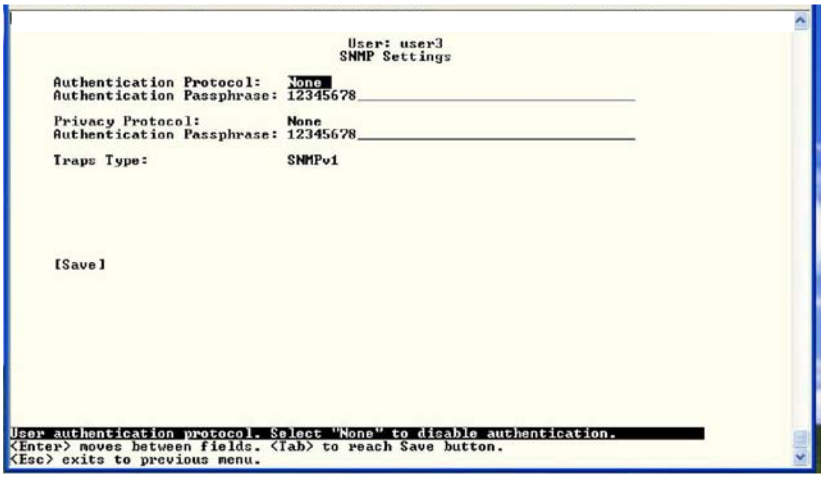


```
                                   User: root
                                     Schedule
  Schedule Type: Always active

  Day of Week    From: Sun        To: Sun
  Hour           From: 00:00      To: 00:00




  [Save]









User's schedule type.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 103- Text Menu-User Activity Schedule

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

User SNMP Settings



```
                                User: user3
                               SNMP Settings

    Authentication Protocol:   None
    Authentication Passphrase: 12345678________________________________

    Privacy Protocol:          None
    Authentication Passphrase: 12345678________________________________

    Traps Type:                SNMPv1




    [Save]









User authentication protocol. Select "None" to disable authentication.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 104-Text Menu- SNMP User Settings

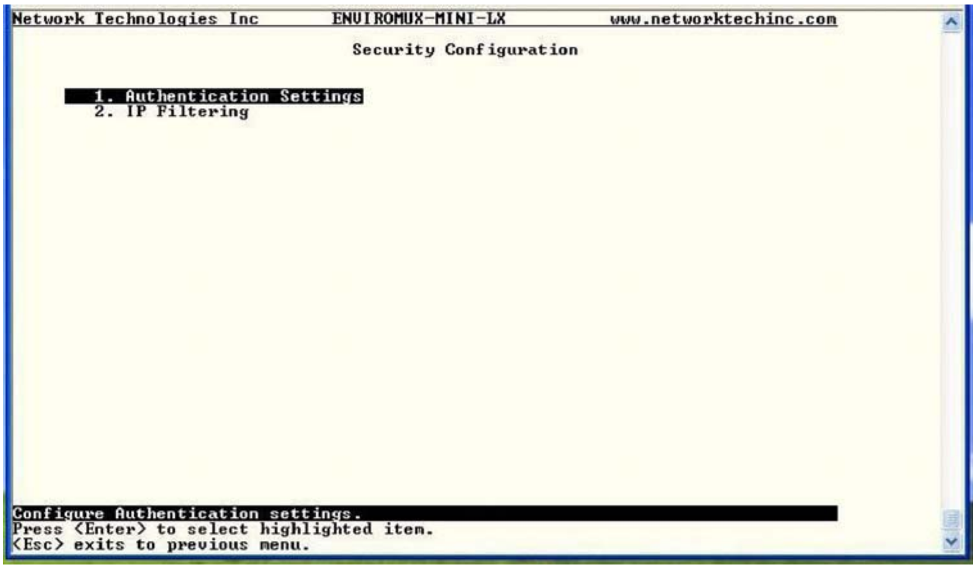
Security settings can be configured within each user configuration if the SNMP protocol has been selected for use (page 82).

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

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

Security Configuration

The Security Configuration menu provides two submenus for setting local versus LDAP authentication methods and for applying IP filtering rules to prevent unwanted access to the EMS200.



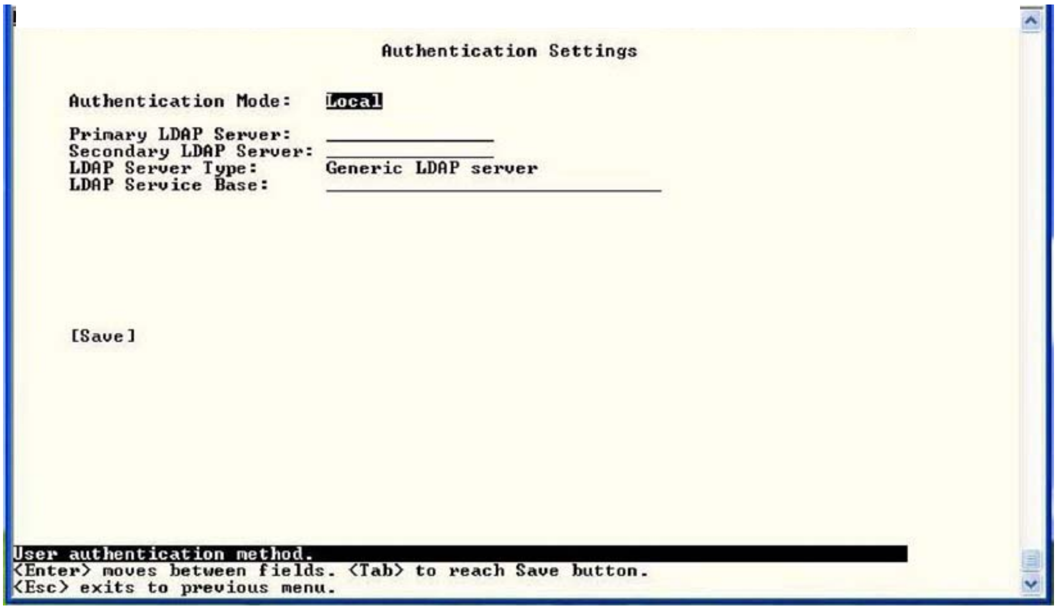
```
Network Technologies Inc        ENVIROMUX-MINI-LX          www.networktechinc.com
                               Security Configuration

         1. Authentication Settings
         2. IP Filtering

Configure Authentication settings.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 105- Text Menu-Security Configuration

Authentication Settings

Security in the EMS200 can be managed one of two ways; through the local settings (passwords assigned in user settings on page 84) or through an LDAP server. If security is configured to use LDAP mode, then the passwords for users must be those found on a configured LDAP server.
Select “Authentication Settings” from the list and press <**`Enter`**>. A menu providing an option to either user Local authentication or LDAP mode. When in LDAP mode, usernames on the LDAP server must match those in the user settings of the EMS200 or access will be denied.

Note: When the root user logs with the EMS200 in LDAP mode, if the LDAP server is not responding, local authentication will be tried.



```
                         Authentication Settings

  Authentication Mode:       Local

  Primary LDAP Server:       _______________
  Secondary LDAP Server:     _______________
  LDAP Server Type:          Generic LDAP server
  LDAP Service Base:         ______________________________

  [Save]

User authentication method.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 106- Text Menu-Authentication Settings

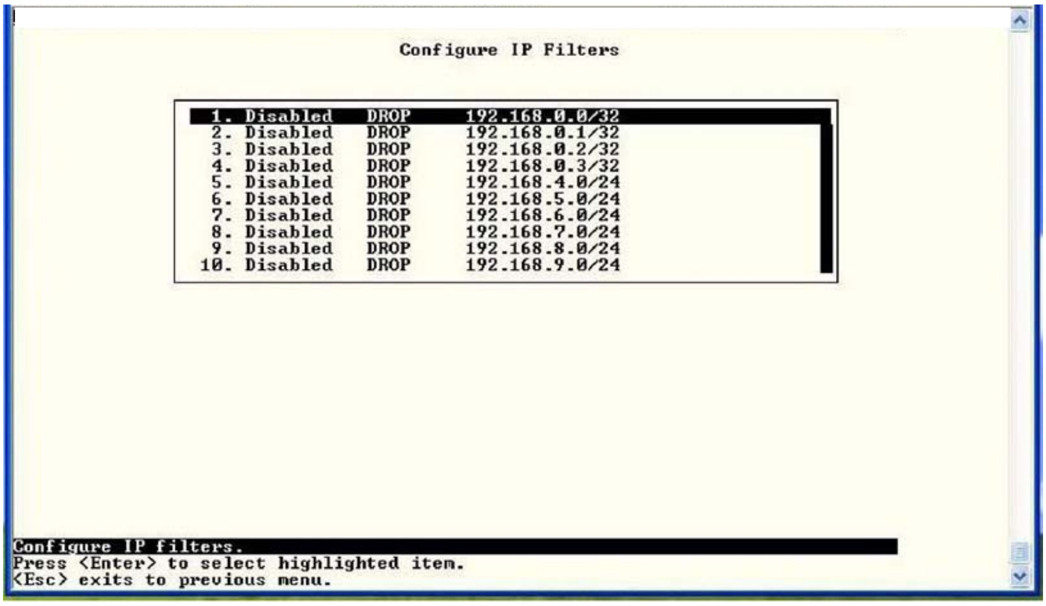
User Authentication Mode	Select Local to use authentication based on passwords in the EMS200 Select LDAP to use authentication based on passwords in an LDAP server	user configuration
Primary LDAP Server	Enter Hostname or IP address of Primary LDAP Server	
Secondary LDAP Server	Enter Hostname or IP address of Secondary LDAP Server (optional)	
LDAP Server Type	Tab to choose from the following: Generic LDAP server Novell Directory server Microsoft Active Directory	
LDAP Service Base	Enter the Base DN for users (ex: ou=People,dc=mycompany,dc=com)	

Even though LDAP authentication is being used, each user must also have a local account. User permission level is established by the local account.
Press <**`Tab`**> to highlight **Save** and press <**`Enter`**> to save before pressing <**`Esc`**> to exit.

IP Filtering

Included in the Security Configuration options is IP Filtering.   IP Filtering provides an additional mechanism for securing the EMS200. Access to the EMS200 network services (SNMP, HTTP(S), SSH, Telnet) can be controlled by allowing or disallowing connections from various IP addresses, subnets, or networks.

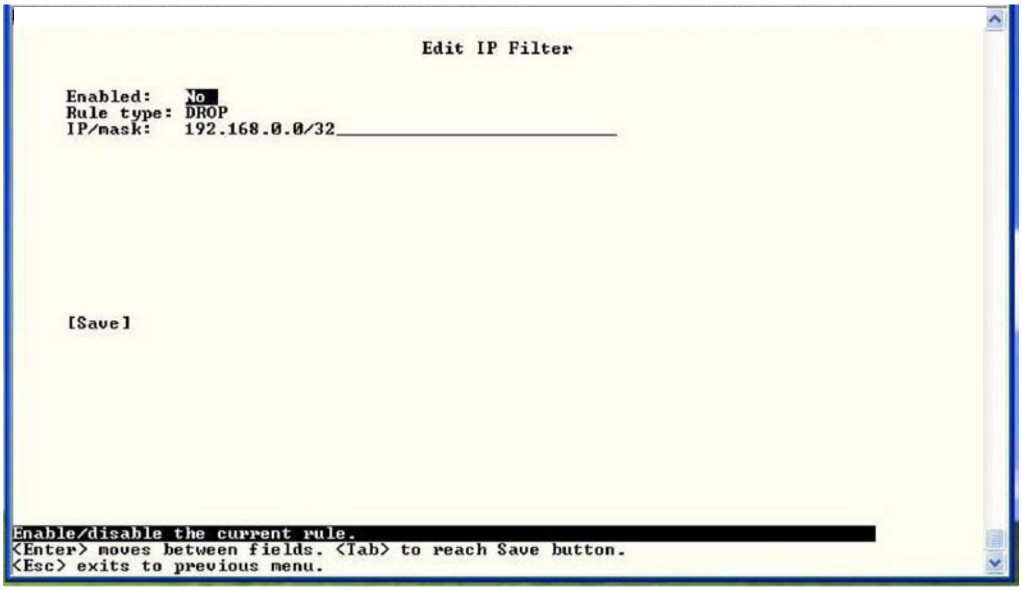
Up to 16 IP Filtering rules can be defined to protect the EMS200 from unwanted access from intruders. Each rule can be set as Enabled or Disabled. Rules can be set to explicitly drop attempts to connect, or to accept them.



```
                         Configure IP Filters

               1. Disabled   DROP     192.168.0.0/32
               2. Disabled   DROP     192.168.0.1/32
               3. Disabled   DROP     192.168.0.2/32
               4. Disabled   DROP     192.168.0.3/32
               5. Disabled   DROP     192.168.4.0/24
               6. Disabled   DROP     192.168.5.0/24
               7. Disabled   DROP     192.168.6.0/24
               8. Disabled   DROP     192.168.7.0/24
               9. Disabled   DROP     192.168.8.0/24
              10. Disabled   DROP     192.168.9.0/24

Configure IP filters.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 107- Text Menu-IP Filtering

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



```
                           Edit IP Filter

     Enabled:    No
     Rule type:  DROP
     IP/mask:    192.168.0.0/32__________________________



     [Save]



Enable/disable the current rule.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 108- Text Menu-Configure IP Filter rule

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

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

(Rule 1)

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

Then, to block all other IP addresses from connecting to the EMS200, we add a rule to drop all other connections.

(Rule 16)

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

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

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

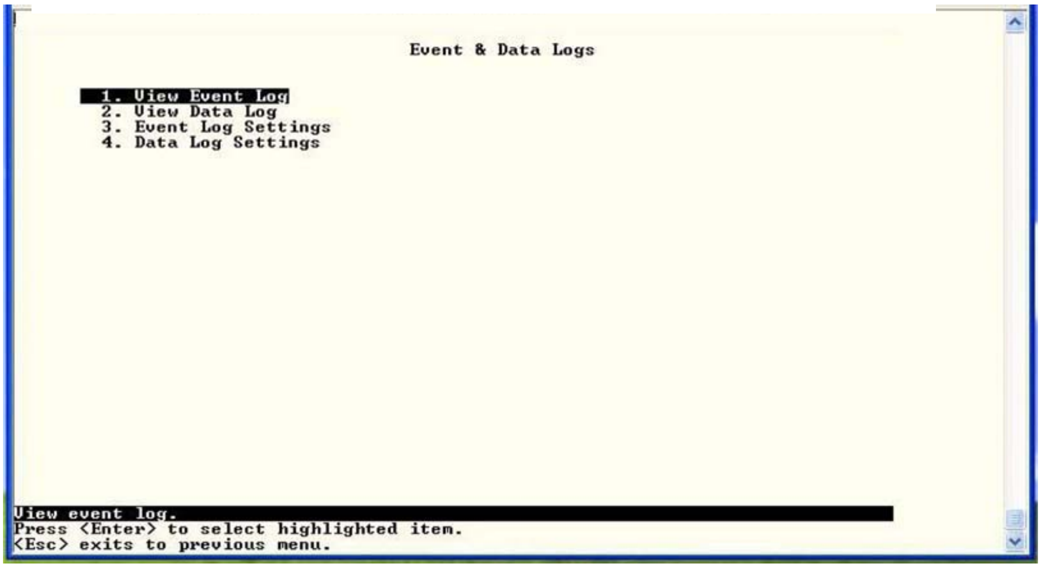
To match a subnet, enter in the subnet with the associated mask (e.g. 192.168.1.0/24).

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

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

Event and Data Logs

Under the Event and Data Logs menu find 4 submenus for viewing a log record of the events monitored by the EMS200 and configuring how the EMS200 will handle reaching the capacity of those logs.



```
                         Event & Data Logs

     1. View Event Log
     2. View Data Log
     3. Event Log Settings
     4. Data Log Settings




View event log.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

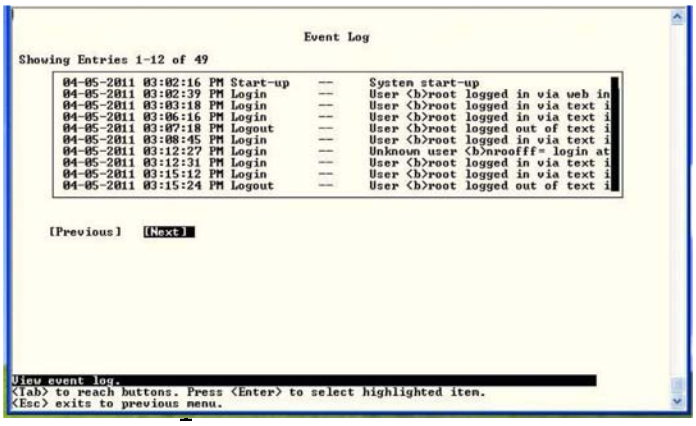
Figure 109- Text Menu-Event & Data Logs

View Event Log

The Event Log provides the administrative user with a listing of many events that occur within the EMS200. log will record the date and time of:

The event

- each EMS200 startup,
- each user login and logout time,
- any time an unknown user tries to login,
- sensor and IP device alerts
- an alert handled by a user



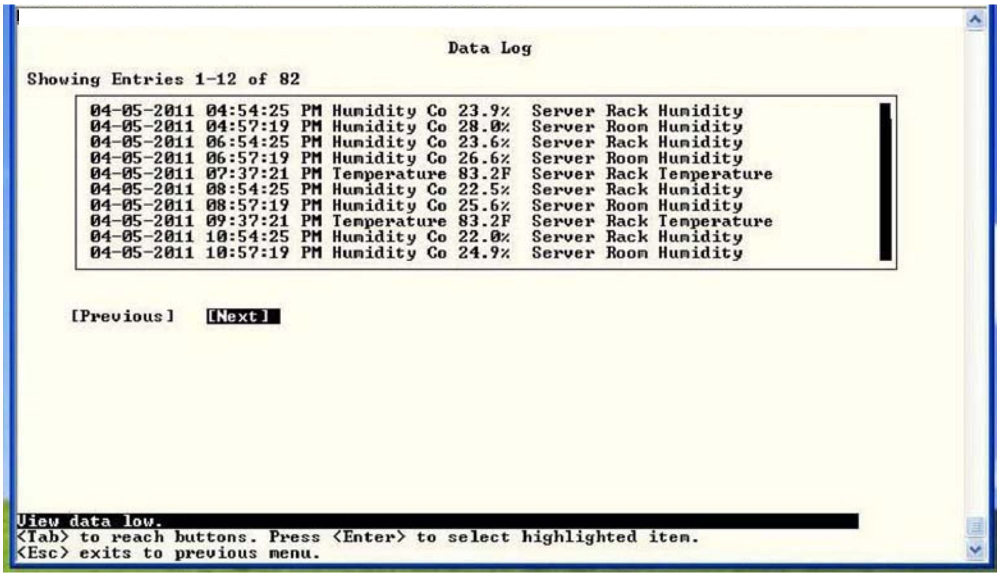
```
                              Event Log
Showing Entries 1-12 of 49

    04-05-2011 03:02:16 PM Start-up    --     System start-up
    04-05-2011 03:02:39 PM Login       --     User <b>root logged in via web in
    04-05-2011 03:03:18 PM Login       --     User <b>root logged in via text i
    04-05-2011 03:06:16 PM Login       --     User <b>root logged in via text i
    04-05-2011 03:07:18 PM Logout      --     User <b>root logged out of text i
    04-05-2011 03:08:45 PM Login       --     User <b>root logged in via text i
    04-05-2011 03:12:27 PM Login       --     Unknown user <b>nroofff= login at
    04-05-2011 03:12:31 PM Login       --     User <b>root logged in via text i
    04-05-2011 03:15:12 PM Login       --     User <b>root logged in via text i
    04-05-2011 03:15:24 PM Logout      --     User <b>root logged out of text i

   [Previous]  [Next]



View event log.
<Tab> to reach buttons. Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

1
1
0- Text Menu-View Event Log

From the Event Log the administrative user can view the logs. In order to clear specific logs, download log entries, or clear the entire log, use the Web Interface (see page 55). To navigate between pages of logs, pres <**`Tab`**> to move between **Previous** and **Next** and press <**`Enter`**>.

View Data Log

The Data Log provides the administrative user with a listing of all the readings taken by the EMS200 pertaining to the sensors and IP Devices being monitored. The data log will record the date and time of each reading.



```
                              Data Log
Showing Entries 1-12 of 82

     04-05-2011 04:54:25 PM Humidity Co 23.9%  Server Rack Humidity
     04-05-2011 04:57:19 PM Humidity Co 28.0%  Server Room Humidity
     04-05-2011 06:54:25 PM Humidity Co 23.6%  Server Rack Humidity
     04-05-2011 06:57:19 PM Humidity Co 26.6%  Server Room Humidity
     04-05-2011 07:37:21 PM Temperature 83.2F  Server Rack Temperature
     04-05-2011 08:54:25 PM Humidity Co 22.5%  Server Rack Humidity
     04-05-2011 08:57:19 PM Humidity Co 25.6%  Server Room Humidity
     04-05-2011 09:37:21 PM Temperature 83.2F  Server Rack Temperature
     04-05-2011 10:54:25 PM Humidity Co 22.0%  Server Rack Humidity
     04-05-2011 10:57:19 PM Humidity Co 24.9%  Server Room Humidity

    [Previous]   [Next]

View data low.
<Tab> to reach buttons. Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 111- Text Menu-View Data Log

From the Data Log the administrative user can view the logs.   In order to clear specific logs, download log entries, or clear the entire log, use the Web Interface (see page 56). To navigate between pages of logs, pres <**`Tab`**> to move between **Previous** and **Next** and press <**`Enter`**>.

Log Settings Menus

The Log Settings menus (Figure 112 and Figure 113) provide settings for how the EMS200 will react when its Data and Event logs reach capacity.

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

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

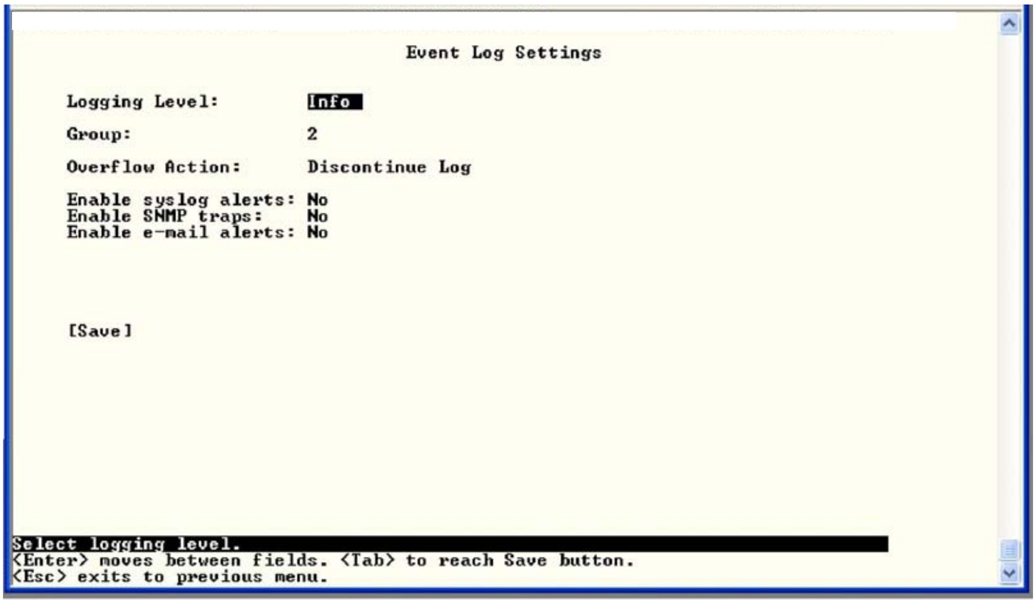
Each log can be assigned to a group and any user that receives messages from that group can be notified when capacity is being reached.

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

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

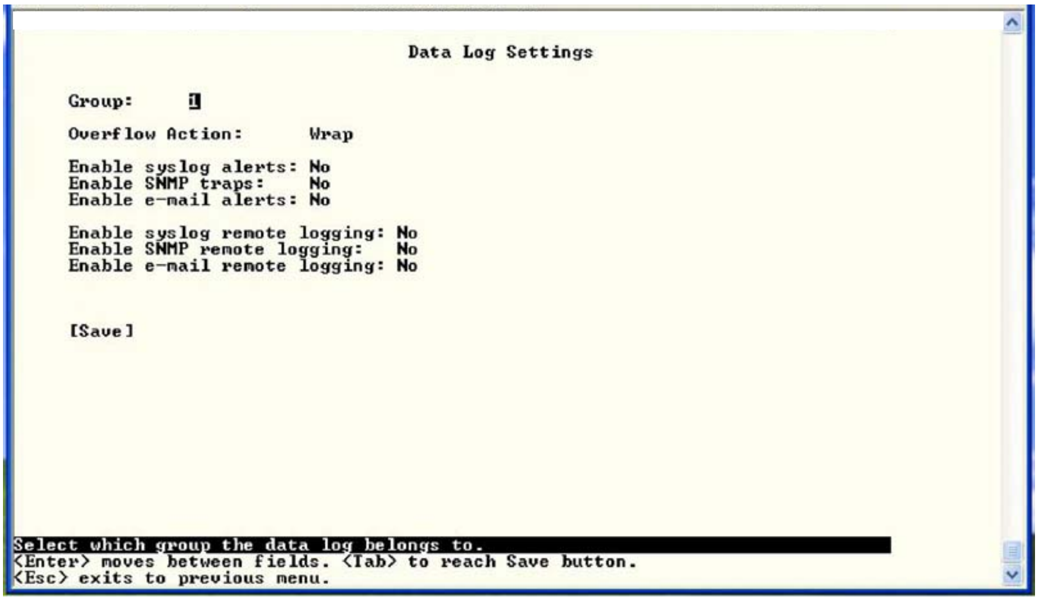
The Data and/or Event log can be set to sent alerts to users via email, syslog, and/or SNMP traps once it has reached 90% of capacity, allowing them time to react.

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



```
                         Event Log Settings

  Logging Level:          Info

  Group:                  2

  Overflow Action:        Discontinue Log

  Enable syslog alerts: No
  Enable SNMP traps:    No
  Enable e-mail alerts: No



  [Save]









Select logging level.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 112- Text Menu-Event Log Settings

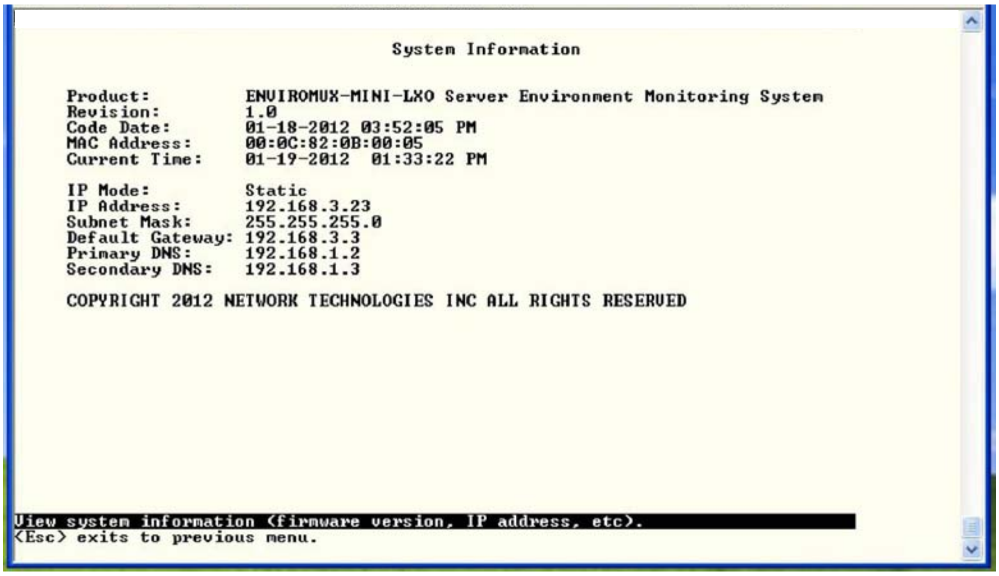


```
                         Data Log Settings

  Group:       1

  Overflow Action:       Wrap

  Enable syslog alerts: No
  Enable SNMP traps:    No
  Enable e-mail alerts: No

  Enable syslog remote logging: No
  Enable SNMP remote logging:   No
  Enable e-mail remote logging: No


  [Save]








Select which group the data log belongs to.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 113-Text Menu-Data Log Settings

System Information

The System Information page lists current firmware, time, and network settings for the EMS200. It also lists the EMS200 MAC address.

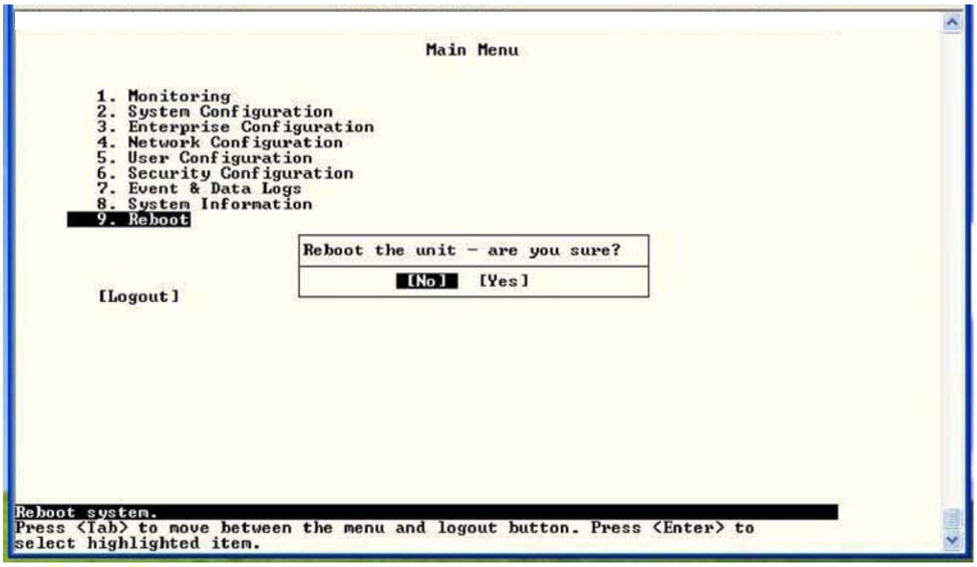


```
                              System Information

     Product:          ENVIROMUX-MINI-LXO Server Environment Monitoring System
     Revision:         1.0
     Code Date:        01-18-2012 03:52:05 PM
     MAC Address:      00:0C:82:0B:00:05
     Current Time:     01-19-2012  01:33:22 PM

     IP Mode:          Static
     IP Address:       192.168.3.23
     Subnet Mask:      255.255.255.0
     Default Gateway:  192.168.3.3
     Primary DNS:      192.168.1.2
     Secondary DNS:    192.168.1.3

     COPYRIGHT 2012 NETWORK TECHNOLOGIES INC ALL RIGHTS RESERVED

View system information (firmware version, IP address, etc).
<Esc> exits to previous menu.
```

Figure 114-Text Menu-System Information

Reboot

From the Main Menu the administrative user can initiate a reboot of the EMS200. By highlighting “Reboot” and pressing <**`Enter`**> (or <**9**> and <**`Enter`**>), you will be prompted to confirm that you want to reboot the EMS200. Press <Enter> to cancel, or press the <**`Tab`**> or either <**`arrow`**> key to highlight “Yes” and <**`Enter`**> to reboot. The EMS200 will reboot and a new connection must be initiated to reconnect, login, and resume operation.

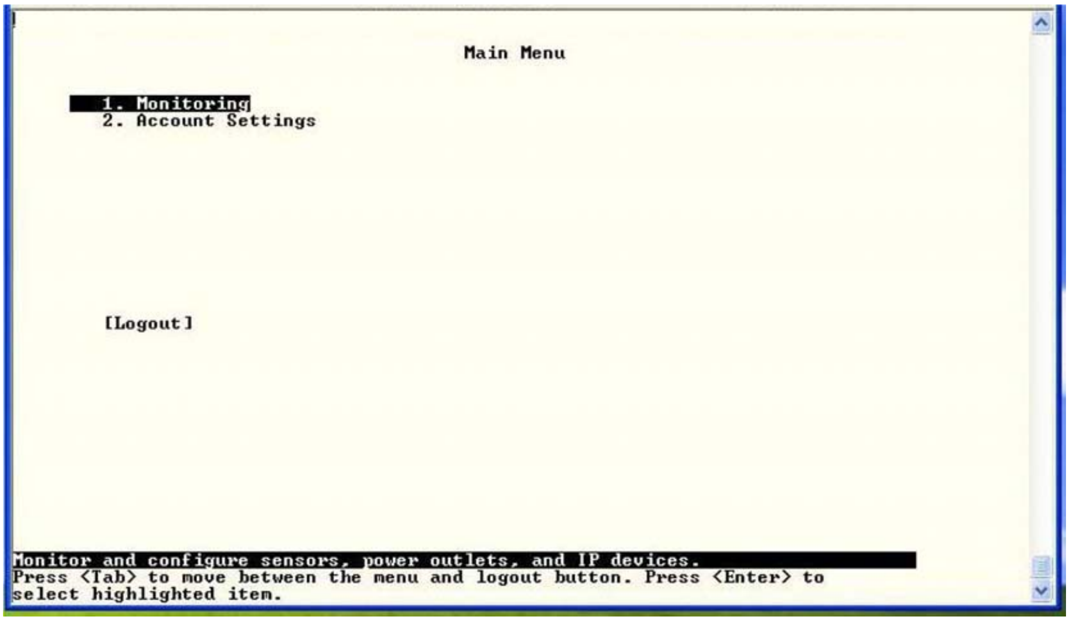


```
                              Main Menu

        1. Monitoring
        2. System Configuration
        3. Enterprise Configuration
        4. Network Configuration
        5. User Configuration
        6. Security Configuration
        7. Event & Data Logs
        8. System Information
        9. Reboot
                            Reboot the unit - are you sure?
                                     [No]   [Yes]
        [Logout]

Reboot system.
Press <Tab> to move between the menu and logout button. Press <Enter> to
select highlighted item.
```

Figure 115- Text Menu-Reboot the EMS200

Text Menu for Non-Administrative Users

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

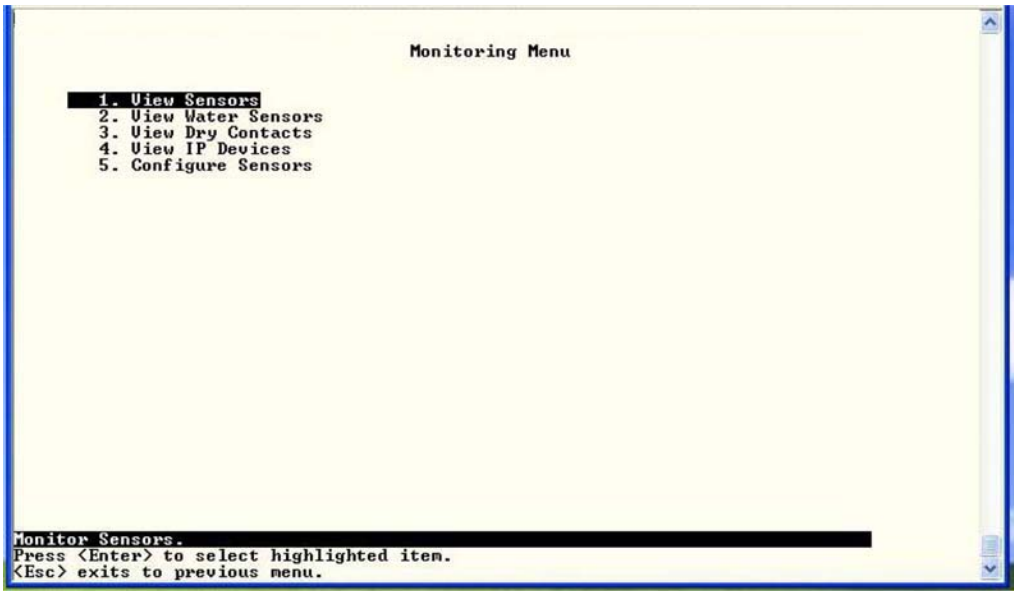


```
                              Main Menu

   1. Monitoring
   2. Account Settings





   [Logout]





Monitor and configure sensors, power outlets, and IP devices.
Press <Tab> to move between the menu and logout button. Press <Enter> to
select highlighted item.
```

Figure 116- Text Menu-User Main Menu

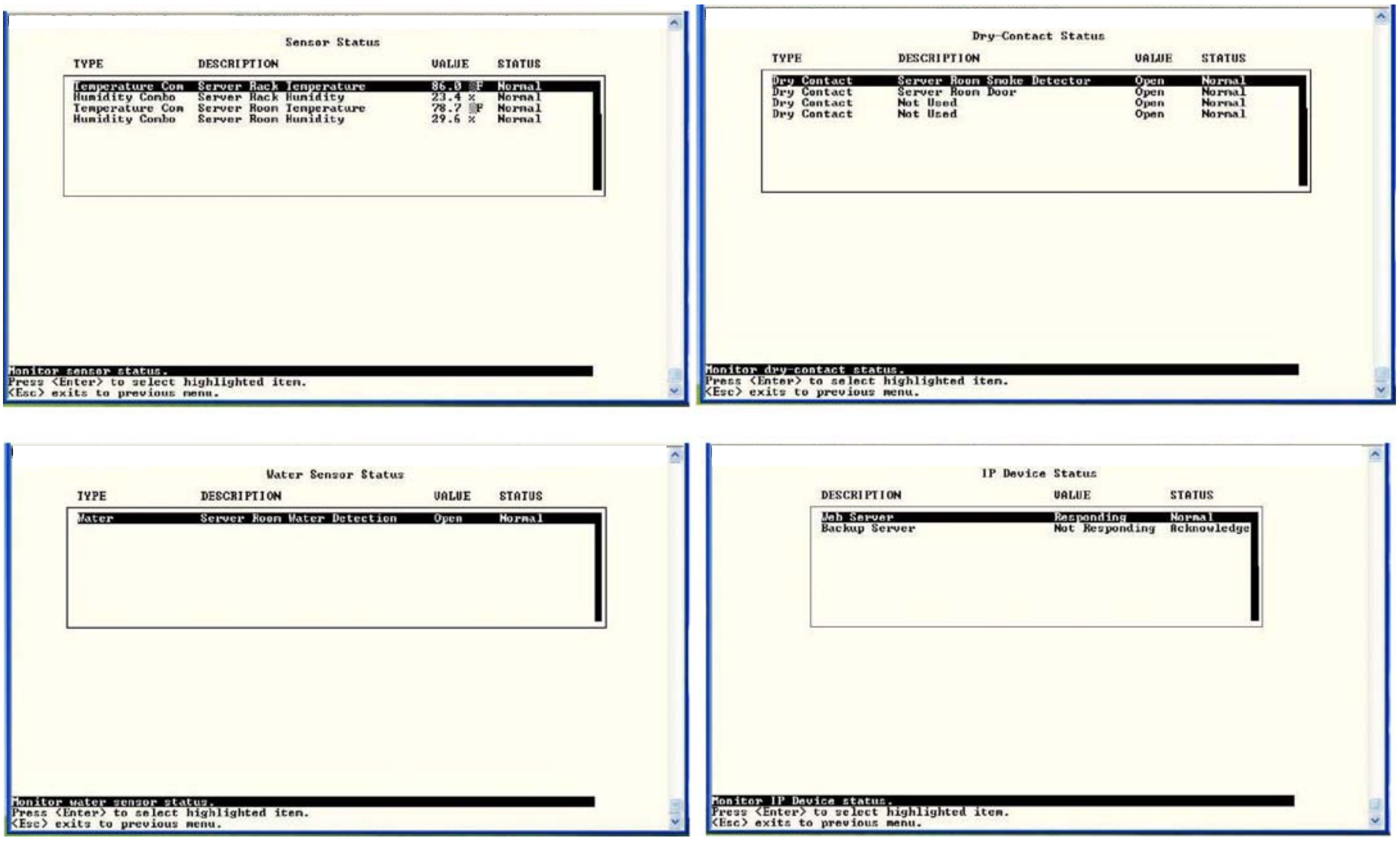
Monitoring

The Monitoring menu lists 4 options for viewing the status of the items monitored by the EMS200.



```
                           Monitoring Menu

    1. View Sensors
    2. View Water Sensors
    3. View Dry Contacts
    4. View IP Devices
    5. Configure Sensors









Monitor Sensors.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 117-Text Menu-User Monitoring Menu



```
                          Sensor Status
      TYPE              DESCRIPTION                  VALUE    STATUS

      Temperature Com   Server Rack Temperature      86.0 °F  Normal
      Humidity Combo    Server Rack Humidity         23.4 %   Normal
      Temperature Com   Server Room Temperature      78.7 °F  Normal
      Humidity Combo    Server Room Humidity         29.6 %   Normal

Monitor sensor status.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

```
                          Dry-Contact Status
      TYPE              DESCRIPTION                  VALUE    STATUS

      Dry Contact       Server Room Smoke Detector   Open     Normal
      Dry Contact       Server Room Door             Open     Normal
      Dry Contact       Not Used                     Open     Normal
      Dry Contact       Not Used                     Open     Normal

Monitor dry-contact status.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

```
                          Water Sensor Status
      TYPE              DESCRIPTION                  VALUE    STATUS

      Water             Server Room Water Detection  Open     Normal

Monitor water sensor status.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

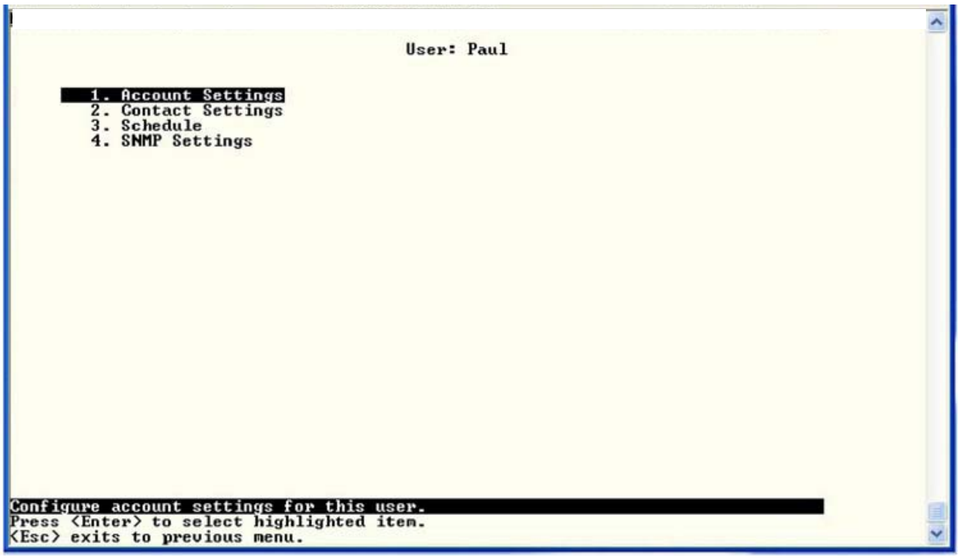
```
                          IP Device Status
          DESCRIPTION                   VALUE          STATUS

          Web Server                    Responding     Normal
          Backup Server                 Not Responding Acknowledge

Monitor IP Device status.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 118- Text Menu-User accessible status menus

If a monitored item is in alert status, the non-administrative user can enter a response to it. By pressing the <**`Enter`**> key with the sensor selected, the user will have the option to either **acknowledge** the alert or **dismiss** it. If the user acknowledges the alert, no additional alert messages will be sent during that alert status cycle. If the user dismisses the alert, another alert message will be sent once the "notify again after" time designated on the configuration page (one example on page 23) elapses.

User Accessible Settings

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

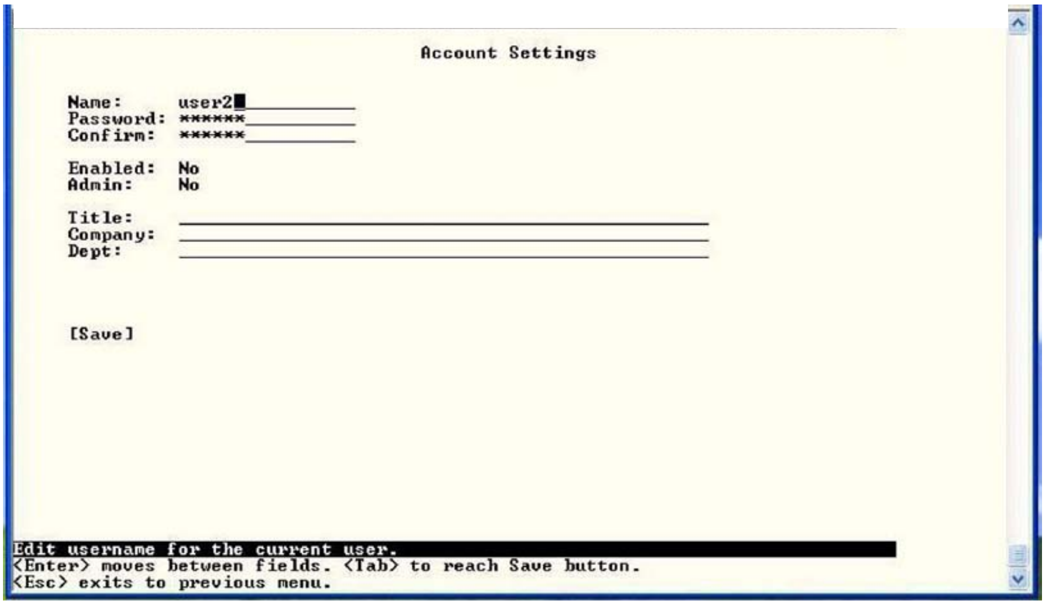


```
                              User: Paul

     1. Account Settings
     2. Contact Settings
     3. Schedule
     4. SNMP Settings

Configure account settings for this user.
Press <Enter> to select highlighted item.
<Esc> exits to previous menu.
```

Figure 119- Text Menu-User Accessible Settings

Account Settings

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

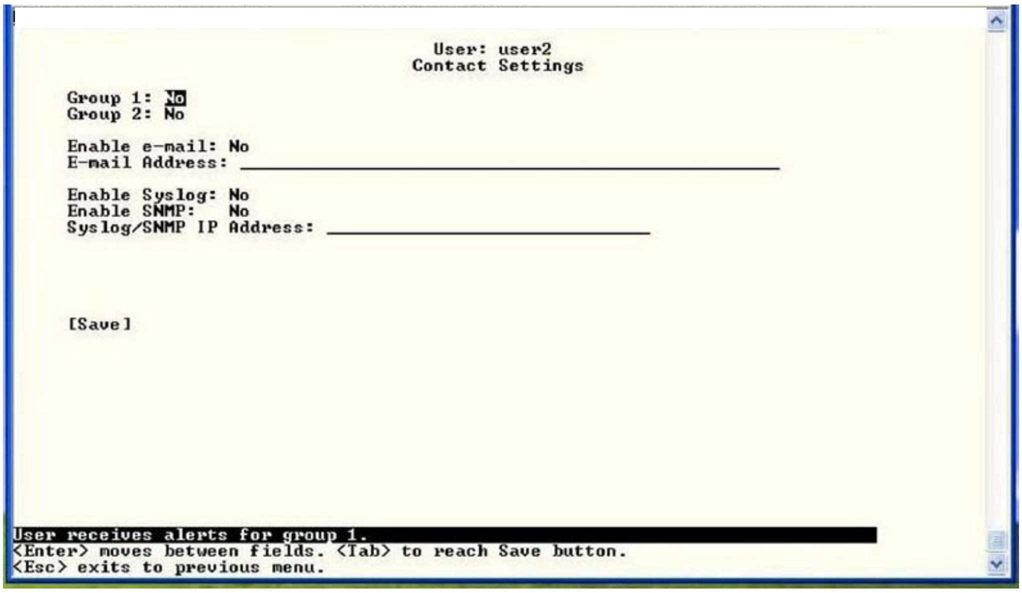


```
                           Account Settings

     Name:      user2
     Password:  ******
     Confirm:   ******

     Enabled:   No
     Admin:     No

     Title:
     Company:
     Dept:


     [Save]

Edit username for the current user.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 120- Text Menu-User Account Settings

Contact Settings

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



```
                              User: user2
                            Contact Settings

      Group 1: No
      Group 2: No

      Enable e-mail: No
      E-mail Address: __________________________________________________

      Enable Syslog: No
      Enable SNMP:   No
      Syslog/SNMP IP Address: ______________________________



      [Save]







User receives alerts for group 1.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

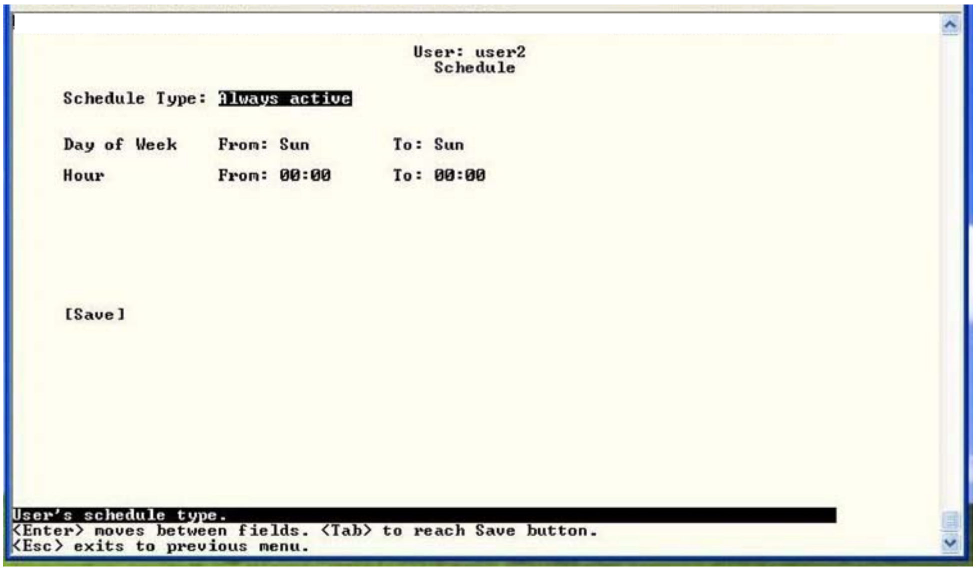
Figure 121- Text Menu-User Contact Settings

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

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

Schedule

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



```
                              User: user2
                                Schedule

  Schedule Type: Always active

  Day of Week      From: Sun        To: Sun
  Hour             From: 00:00      To: 00:00



  [Save]



User's schedule type.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

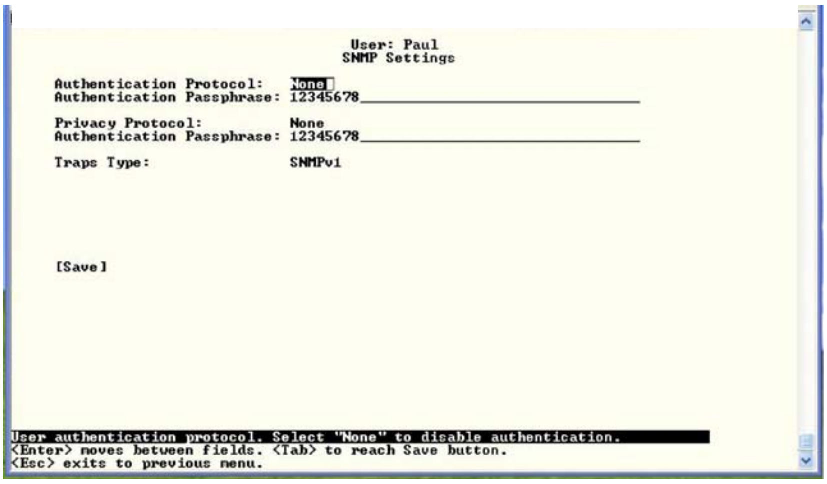
Figure 122- Text Menu-User Activity Schedule

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

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

SNMP Settings

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



```
                                User: Paul
                               SNMP Settings

   Authentication Protocol:    None
   Authentication Passphrase: 12345678_____________________________

   Privacy Protocol:           None
   Authentication Passphrase: 12345678_____________________________

   Traps Type:                 SNMPv1



   [Save]



User authentication protocol. Select "None" to disable authentication.
<Enter> moves between fields. <Tab> to reach Save button.
<Esc> exits to previous menu.
```

Figure 123- Text Menu-User SNMP Settings

Security settings can be configured within each user configuration if the SNMP protocol has been selected for use (page 82).

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

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

If any changes are made to the user’s SNMP Settings, the EMS200 must be rebooted (page 47) before they will take effect. If other users’ settings need to be changed, the reboot can be done after all users’ settings are complete.

SYSTEM RESET BUTTON

A System Reset push-button is on the front-panel and is recessed from the panel to prevent accidental use of the button. Pressing the System Reset button will cause the EMS200 to restart, just as if it were power-cycled. A momentary press of the System Reset push-button will activate this function. The reset button can be used at any time.

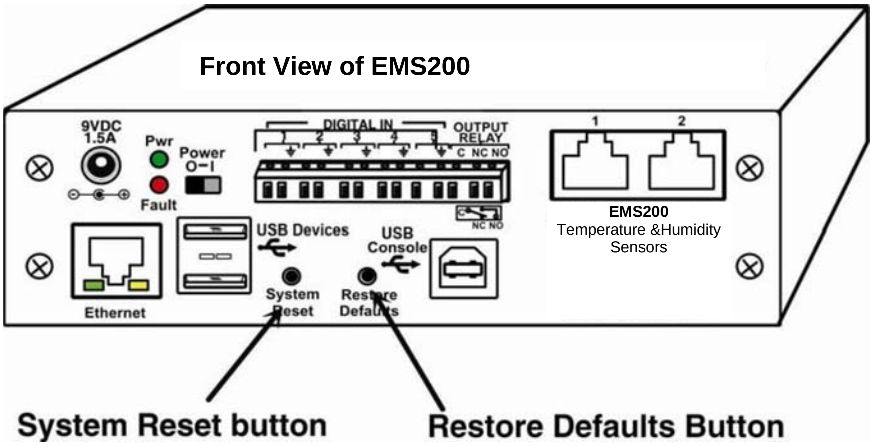


Figure 124- Location of Reset buttons

RESTORE DEFAULTS BUTTON

Another button, “Restore Defaults”, is located on the front of the EMS200 (see above). The button can be used to clear all configuration changes and restore the EMS200 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 EMS200 will reboot and be ready for login within its usual start-up time period. If possible, consider saving the EMS200 configuration before using this button (page 34).

USB PORTS

The EMS200 are each equipped with a USB Type A female ports for connection of a USB flash drive and a GSM modem (page 14) for receiving alert messages via SMS. The ports are compatible with USB 2.0 Full Speed flash drives. When enabled (page 57) and with the USB flash drive connected, the Event and Data Logs will be written to a text file on the flash drive in addition to the memory in the EMS200. When a modem is connected (page 14), it will automatically be sensed by the EMS200 (page 35).

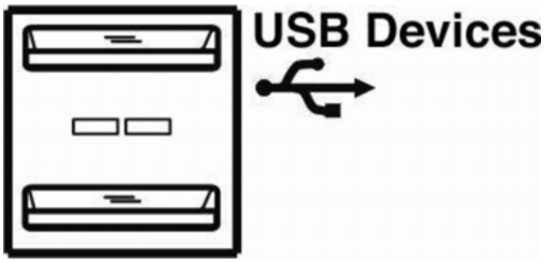


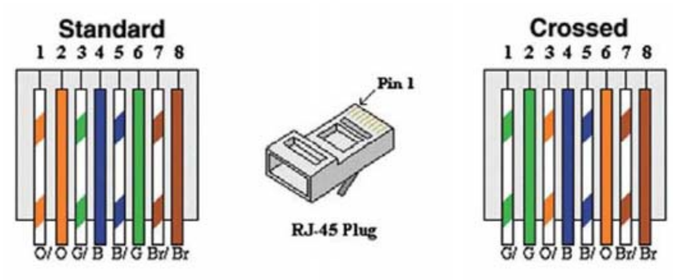
Figure 125- USB Flash Drive and GSM modem ports

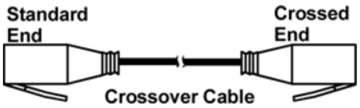
WIRING METHODS

PC-to EMS200 Crossover Cable

In order to make a direct connection between a PC and the ETHERNET connector of the EMS200, a crossover cable must be used. The cable is made with CAT5 cable terminated with RJ45 connectors and wired according to the chart below.

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

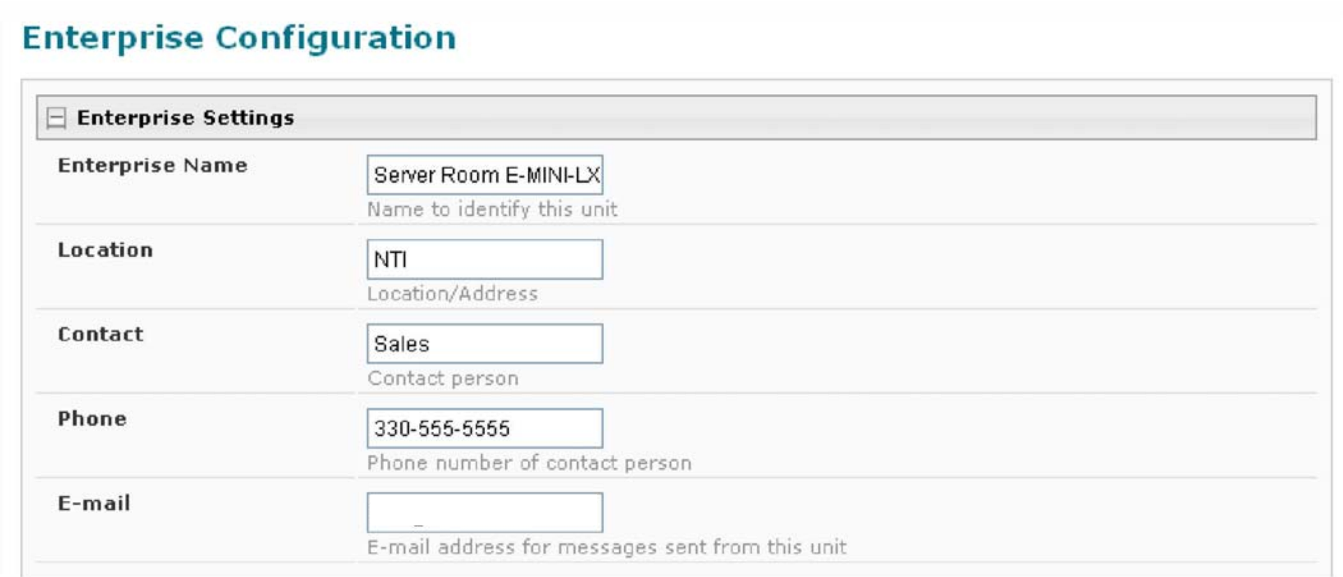




HOW TO SETUP EMAIL

Use this guide to assist in the configuration of the EMS200 to send email messages. 1. Apply a valid

email address for the EMS200 to the Enterprise Setup Page (see page 35).

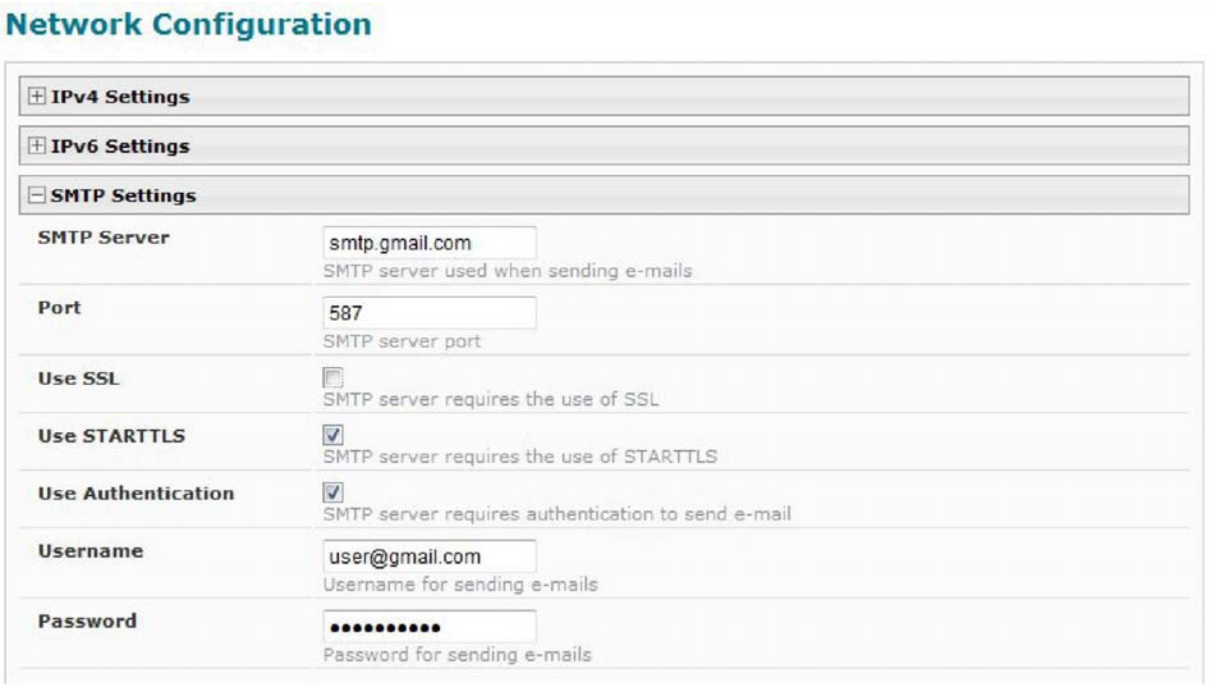


Enterprise Configuration

⊟ Enterprise Settings

Enterprise Name	Server Room E-MINI-LX	Name to identify this unit
Location	NTI	Location/Address
Contact	Sales	Contact person
Phone	330-555-5555	Phone number of contact person
E-mail		E-mail address for messages sent from this unit

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



Network Configuration

⊞ IPv4 Settings

⊞ IPv6 Settings

⊟ SMTP Settings

SMTP Server	smtp.gmail.com	SMTP server used when sending e-mails
Port	587	SMTP server port
Use SSL	□	SMTP server requires the use of SSL
Use STARTTLS	☑	SMTP server requires the use of STARTTLS
Use Authentication	☑	SMTP server requires authentication to send e-mail
Username	user@gmail.com	Username for sending e-mails
Password	●●●●●●●●●●	Password for sending e-mails

Figure 126- Example of configuration for Gmail server

2. Fill in Network Page (page 36) with valid information:

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

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

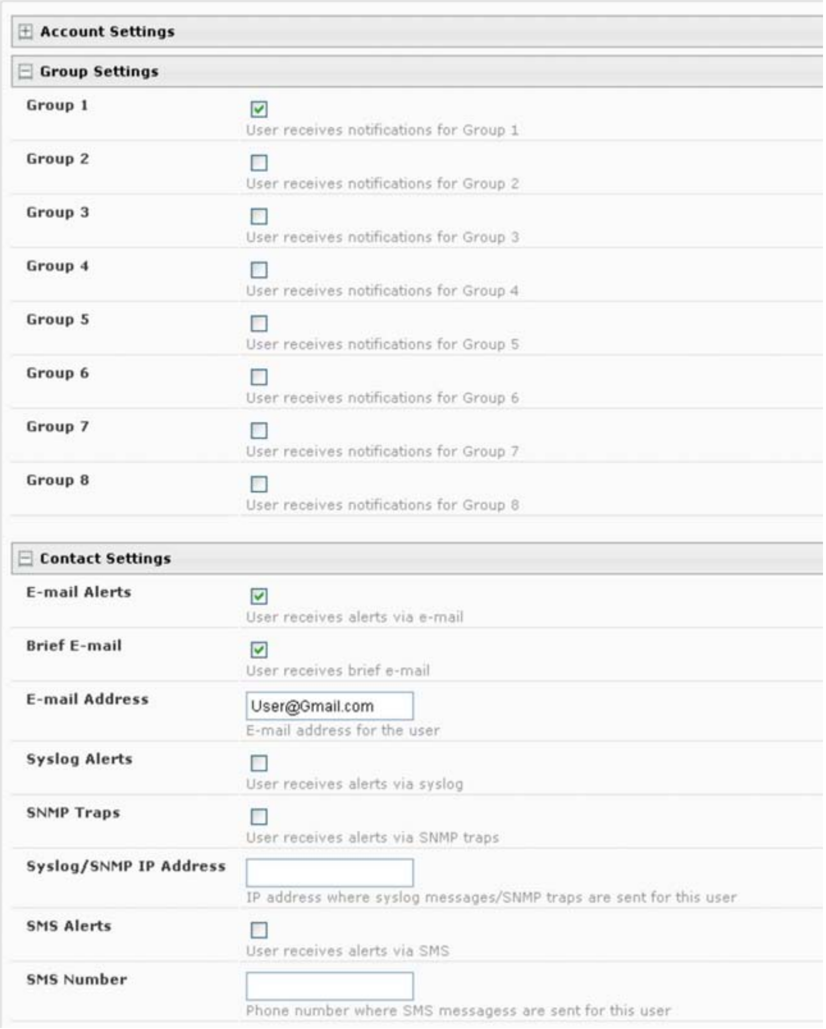
C. Check “Use SSL” if your SMTP server requires SSL, or “Use STARTTLS” if it requires TLS.

D. Check “Use Authentication” if SMTP server requires authentication to send emails.
a. If required, Enter “Username” and “Password” that has been assigned to EMS200. Make sure they apply to the email address applied in the Enterprise Setup Page.

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

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

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



⊞ Account Settings

⊟ Group Settings

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

⊟ Contact Settings

E-mail Alerts	☑ User receives alerts via e-mail
Brief E-mail	☑ User receives brief e-mail
E-mail Address	User@Gmail.com E-mail address for the user
Syslog Alerts	□ User receives alerts via syslog
SNMP Traps	□ User receives alerts via SNMP traps
Syslog/SNMP IP Address	IP address where syslog messages/SNMP traps are sent for this user
SMS Alerts	□ User receives alerts via SMS
SMS Number	Phone number where SMS messagess are sent for this user

Figure 127- Configure user to receive alerts via email

TECHNICAL SPECIFICATIONS

Ports	
Temperature/Humidity Inputs	Two female RJ45 connectors for connecting temperature sensors, humidity sensors, and/or combined temperature/humidity sensors.
Max. Sensor Cable Length	Temperature and Humidity Sensors- 25 feet Liquid and Contact Sensors- 1000 feet
DIGITAL IN Dry Contact Closures	Five screw terminal pairs for connecting dry contact devices and liquid detection sensors. * Potential-free. * Output voltage: +5 V DC * Current limited to 10 mA * Maximum contact resistance: 10K Ohm
Ethernet Port	One female RJ45 connector with LEDs. 10 BaseT Ethernet interface.
USB Console Port	Virtual Serial Port- USB Type B female connector
USB Devices Ports	Two female USB Type A connector Supports USB 2.0 Full Speed
Output Relay	SPDT relay- contacts rated for up to 1A, 30VDC or 0.5A, 125VAC
Environmental	
Operating temperature	32°F to 122°F (0°C to 50°C)
Storage temperature	-13°F to 149°F (-25°C to 65°C)
Operating and Storage Relative Humidity	0 to 90% non-condensing RH
General	
Compatible Modems	EMS200-GSM-3GU (NetComm N3GS003)
Protocols	HTTP, HTTPS,SNMP, SMTP, TCP/IP, UDP, Xmodem, SSHv2, SSLv3, IP Filtering, LDAPv3, AES 256-bit encryption, SNMPv1,v2c,v3
Power Supply	120VAC or 240VAC at 50 or 60Hz-9VDC/1.5A AC Adapter
Dimensions WxDxH (in.)	2.14x5.68x2.14
Approvals	RoHS

TROUBLESHOOTING

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

Problem	Cause	Solution
Cannot connect via telnet	telnet service not enabled	Enable telnet (page 38)
Cannot connect via web interface- no login screen	• wrong IP address • HTTP not enabled • HTTP moved from default (port 80)	• Use Discovery Tool to locate configured IP address (page 17) • Enable HTTP (page 36) • Identify port number assigned (page 36)
Cannot get Discovery Tool to work	Java not installed	Java Runtime Environment must be installed before the Discovery Tool can be used (page 17)
LDAP user cannot login	Login username and/or password does not match same in EMS200 user list	Make sure the username and password used in the LDAP server matches the username and password in the EMS200 user configuration (page 39)
Cannot login	cannot remember root password	Either restore default settings (page 78) or contact NTI for assistance

SMTP Error Codes:

Without SSL enabled:	Meaning	Comments
-1	SMTP_CONN_ERR,	Cannot establish a connection to the SMTP server. Possible reasons: bad setting for IP of SMTP server, firewall blocking the connection
-4	SMTP_SERVER_NOT_READY_ERR,	Server denied connection
-5	SMTP_EHLO_ERR,	Server did not answer to HELO command
-6	SMTP_AUTH_NO_SUPPORT_ERR,	Authentication method is not supported
-7	SMTP_AUTH_FAILURE_ERR,	Authentication failure (user or password rejected)
-8	SMTP_BAD_FROM_ERR,	SMTP Server did not accept the sender e-mail address
-9	SMTP_BAD_TO_ERR,	SMTP Server did not accept the destination e-mail address
-10	SMTP_DATA_ERR,	SMTP Server did not accept the DATA command
-11	SMTP_BAD_DATA_ERR,	SMTP Server did not accept the body of e-mail message
With SSL enabled:		
-100	SMTP_SSL_CONN_ERR,	Cannot establish a connection to the SMTP server. Possible reasons: bad setting for IP of SMTP server, firewall blocking the connection
-99	SMTP_SSL_CONN_ERR1,	
-98	SMTP_SSL_CONN_ERR2,	
-97	SMTP_SSL_PROTOCOL_ERR,	SMTP server connected but did not accept SSL connection
-95	SMTP_SSL_SERVER_NOT_READY_ERR,	Server denied connection
-94	SMTP_SSL_EHLO_ERR,	Server did not answer to HELO command
-93	SMTP_SSL_AUTH_NO_SUPPORT_ERR,	Authentication method is not supported
-92	SMTP_SSL_AUTH_FAILURE_ERR,	Authentication failure (user or password rejected)
-91	SMTP_SSL_BAD_FROM_ERR,	SMTP Server did not accept the sender e-mail address
-90	SMTP_SSL_BAD_TO_ERR,	SMTP Server did not accept the destination e-mail address
-89	SMTP_SSL_DATA_ERR,	SMTP Server did not accept the DATA command
-88	SMTP_SSL_BAD_DATA_ERR,	SMTP Server did not accept the body of e-mail message

INDEX